



Brussels, 6.4.2016
SWD(2016) 115 final

PART 1/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Impact Assessment Report on the establishment of an EU Entry Exit System

Accompanying the document

Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011

and

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/xxx as regards the use of the Entry/Exit System (EES)

{ COM(2016) 194 final }
{ COM(2016) 196 final }
{ SWD(2016) 116 final }

Table of Contents

1.	INTRODUCTION.....	1
1.1.	Background.....	1
1.2.	Proof of concept	1
1.3.	Changed context	2
1.4.	Revised proposal	3
2.	PROBLEM DEFINITION	5
2.1.	The problems addressed by the Smart Borders package.....	5
2.2.	Implementation problems addressed by this impact assessment.....	8
2.3.	The drivers of the problems.....	10
2.4.	Who is affected, in what ways and to what extent?	10
2.5.	What is the EU dimension of the problem?.....	14
2.6.	How would the problem evolve, all things being equal?	14
2.7.	Conclusions of the evaluations of the existing policy	16
3.	WHY SHOULD THE EU ACT?	17
4.	OBJECTIVES	19
4.1.	General policy objectives	19
4.2.	Specific policy objectives.....	19
4.3.	Consistency with other EU policies and with the Charter for fundamental rights.....	20
5.	POLICY OPTIONS.....	23
5.1.	The architecture: how can the system be most effectively built?.....	24
5.2.	Biometrics: what biometric identifier(s) are required for the correct functioning of the system?.....	27
5.3.	Facilitation of border crossing.....	32
5.4.	Retention time for the storage of data	34
5.5.	Access for law enforcement purposes	37
6.	ANALYSIS OF IMPACTS.....	40
6.1.	Social impacts.....	40
6.2.	Economic impacts	46
6.3.	Impacts on SME's.....	48

6.4.	Impacts on Public Services.....	48
6.5.	Impact on International Relations	49
7.	COMPARISON OF OPTIONS.....	51
7.1.	Comparison in terms of effectiveness, fundamental rights, efficiency and coherence	52
7.2.	Preferred option	67
7.3.	Subsidiarity and proportionality of the preferred option.....	71
8.	MONITORING AND EVALUATION.....	73
8.1.	Practical arrangements of the evaluation: when, by whom.....	73
8.2.	Operational objectives and monitoring indicators for the preferred option.....	73
9.	ABBREVIATIONS.....	75
10.	GLOSSARY.....	77
11.	LIST OF ANNEXES.....	80

1. INTRODUCTION

1.1. Background

In February 2013, the Commission adopted a Smart Borders package consisting of three proposals: (1) a Regulation for an Entry/Exit System (EES)¹ for the recording of information on the time and place of entry and exit of third country nationals² travelling to the Schengen area³, (2) a Regulation for a Registered Traveller Programme (RTP)⁴ to allow third country nationals who have been pre-vetted to benefit from facilitation of border checks at the Union external border, (3) a Regulation amending the Schengen Borders Code⁵ in order to take into account the existence of the EES and RTP.

The Smart Borders proposals intended to contribute to the modernisation of Schengen area's⁶ external border management by improving the quality and efficiency of the management of border crossing processes. They aimed to help Member States dealing with ever increasing traveller flows without necessarily increasing the number of border guards, and to promote mobility between Schengen and third countries in a secure environment.

During the first examination of the package which was completed in February 2014, the co-legislators voiced technical, cost-related and operational concerns on the design of the systems. However the key choices made in 2013 – centralised systems based on biometrics – have not been questioned.

1.2. Proof of concept

In order to assess the technical, organisational and financial impact of possible solutions to the contentious issues, the Commission initiated with the support of both co-legislators a so-called 'proof of concept' exercise consisting of two stages:

- A Commission-led Technical Study on Smart Borders (published in October 2014, hereinafter '*The Technical Study*')⁷, and
- A testing phase led by eu-LISA (European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice) on the impact of the use of various biometric identifiers on the border control processes (report published in December 2015, hereinafter '*The Pilot*')⁸.

¹ COM(2013) 95 final

² A third country national is a person who is not holding the nationality of a Member State of the EU or of a Schengen associated country.

³ In 2015, the Schengen area is composed of all Member States of the European Union except Ireland and the United Kingdom and four Member States that do not yet fully implement the Schengen acquis: Bulgaria, Croatia, Cyprus, Romania. Four countries that are not part of the EU are also part of the Schengen area: Iceland, Liechtenstein, Norway and Switzerland. The Schengen area thus counts 22 EU Member States and 4 associated countries.

⁴ COM(2013) 97 final

⁵ COM(2013) 96 final

⁶ The Schengen Area covers 26 European countries which have decided to remove all internal border controls, so travellers can move freely within the area without having to show their passports. It includes most EU States, except for Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom (Bulgaria and Romania are currently in the process of joining). The non-EU states Iceland, Norway, Switzerland and Liechtenstein have also joined. For more information, please consult the following webpage: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen/index_en.htm

⁷ Technical Study on Smart Borders, European Commission, DG HOME, 2014. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm

⁸ Final Report of the Smart Borders Pilot Project, eu-LISA, December 2015. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm

The aim of the Pilot was to verify the feasibility of the options proposed in the Technical Study in operational environments with real travellers across the EU. Twelve different test cases were performed in 18 Border Crossing Points spread over eleven Member States, covering air, sea and land borders in different climatological situations, with different operational requirements. In total 78 tests were carried out. The pilot not only collected quantitative test case results but also sought feed-back from travellers as well as border guards.

In parallel to the Pilot, the Commission services engaged in a series of technical meetings on various topics with experts from Member States as well as with the Smart Borders' rapporteurs and shadow rapporteurs in European Parliament (EP).

The Commission hosted dedicated meetings with representatives of civil society, carriers and national law enforcement services. A particularly important consultation opportunity was organised by the LIBE Committee (Committee Civil Liberties, Justice and Home Affairs) of the EP (European Parliament) in February 2015, when a two-day inter-parliamentary hearing on Smart Borders took place, with the participation of national parliaments.

The question related to the protection of Fundamental Rights were discussed and analysed in dedicated meetings and workshops with experts of the European Data Protection Supervisor (EDPS)⁹ and the Fundamental Rights Agency (FRA). The EDPS also submitted comments in writing¹⁰.

The Commission conducted a public consultation on the Smart Borders Package, inviting citizens (both EU nationals and non-EU nationals) and organisations to contribute. The results of the consultation were published in December 2015¹¹.

1.3. Changed context

Today, like in 2013, the need for establishing an EU wide Entry Exit System is broadly recognised and supported by the Commission and co-legislators alike. If anything, public and political support for investing in the establishment of 'smart' border management solutions has further increased, also as a result of the current refugee crisis and recent terrorist attacks. Whereas it is important to underline that the proposal to establish an Entry Exit System is as such not related to these developments (the EES strictly deals with the recording of short-term legal stay of third country nationals; refugees are not included in the scope of this project), it is equally correct to stress that EES will contribute to the fight against irregular migration (e.g. the phenomenon of 'overstayers') and can provide an additional instrument for law enforcement authorities to prevent and combat terrorism.

The question whether an Entry Exit System is necessary and desirable is no longer in the centre of political debate. The real issue, which was addressed in the 'proof of concept' and forms the main part of this Impact Assessment, is how such a system should be developed: how would it relate to other, already existing, systems, how would it be integrated in existing border crossing processes, what biometrics should be used, how would data storage be organised, and how could the system contribute to law enforcement objectives, all of this in an efficient and cost-effective way.

⁹ See annex 16

¹⁰ <https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/Comments>

¹¹ http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/consulting_0030_en.htm

When discussing these questions some relevant developments since 2013 should be taken into account:

- The Visa Information System became fully operational. Its 'roll-out' to Member States consulates in all relevant third countries was concluded in November 2015. The biometric verification of visa-holders against VIS at Schengen external borders is now compulsory. Law enforcement authorities increasingly use VIS for identification and investigation purposes.
- Visa liberalisation dialogues with countries in the Western Balkan and at the Eastern and South-Eastern borders of the EU were concluded or have been accelerated, which will lead to an increasing proportion of visa-exempt travellers to the EU. It is expected that this trend will continue in the coming years.
- The Internal Security Fund (ISF-B) was adopted, which earmarked € 791 million financial reservation for the development of Smart Borders (to start after the adoption of the relevant legal basis).
- Rapid developments in the area of biometric technology opened up new possibilities for 'lighter' and 'faster' enrolment and verification of travellers, not only for fingerprints, but also for facial images.
- The Court judgment on the Data Retention Directive provided legal clarity on the conditions and safeguards that need to be respected for the storage and use of EES data.

These elements have partly changed the political, legal and institutional environment in which the Smart Borders proposals were discussed, and contributed to the need for a thorough review of the 2013 legislative package.

1.4. Revised proposal

Based on the findings of the Technical Study, the results of the Pilot and the numerous technical discussions with co-legislators and stakeholders as well as the outcome of the public consultation, the Commission has considered potential improvements and simplifications to the 2013 proposal. These will be explored in chapter 5 of this Impact Assessment.

The policy objectives of the 2013 proposals remain essentially unchanged¹², and so do several other features of the original proposals. This Impact Assessment is building on the 2013 Impact Assessments¹³ accompanying the 2013 proposals, and focusing on those elements of the 2013 proposals where changes are being proposed, notably (a) architecture of the system, (b) biometrics to be used, (c) the use of process facilitators, (d) the retention of data and (e) access by law enforcement authorities. Discussions in

¹² To improve the management of external borders and the fight against irregular migration; to facilitate the crossing by third country nationals of EU external borders through a semi-automated or automated system; to identify and detect overstayers (also within the territory); to support evidence based EU migration policy making. Should law enforcement authorities be granted access to the system, an additional policy objective would be to contribute to the fight against terrorism and serious crime, in line with the provisions in VIS and Eurodac.

¹³ SWD(2013)47 final and SWD(2013)50 final

Council and EP during the proof of concept phase largely focused on these options. They constitute the essence of how an effective and efficient EES can be built.

To ensure that this Impact Assessment can be read as a 'stand-alone' document, the problems to be addressed by the Smart Borders Package are recalled. However the establishment of an EES is not questioned and is assumed. This Impact Assessment addresses the specific question of 'how the EES should be established', focusing on the five aspects mentioned above, and taking account of the main relevant developments that occurred since 2013.

2. PROBLEM DEFINITION

Before defining the problem it is important to specify the scope of this Impact Assessment: the Schengen Borders Code¹⁴ stipulates that third country nationals have the right to enter in the Schengen area for a short stay of up to 90 days within any 180 day period. Third country nationals who are in possession of a valid residence permit or long-stay visa issued by a Member State ('residence permit holders') are not bound by this limitation. The same applies for third country nationals who are family members of a person that holds the nationality of a Member State of the EU or of a Schengen associated country¹⁵.

Unless stated otherwise, wherever this Impact Assessment speaks about third country nationals it refers to people that enter for a short stay¹⁶.

The border control processes at entry/exit according to current Schengen Borders Code are summarised in annex 5.

2.1. The problems addressed by the Smart Borders package

This section recalls the problems which the package, and notably the Entry-Exit system addresses.

Problem 1: The number of border crossings is increasing and lead to delays in border checks.

Passenger flows at the external borders¹⁷ of the European Union have been growing and will continue to increase in the future. On the basis of the survey done during the Technical Study¹⁸ it is expected that external border crossings in and out of the Schengen area will increase by approximately 28% by 2020 and 57% by 2025. The total number of border crossings in 2025 is forecast to rise to 887 million of which around one-third are expected to be by third-country nationals (TCN). Based on the travel patterns observed in 2014, it was estimated that around 127 million of these crossings would be by visa exempt travellers (TCN-VE) and 175 million by visa holders (TCN-VH). However it can be expected that the ratio between TCN-VH and TCN-VE will change substantially in the coming decade following the progress in 2015 on visa liberalisation dialogues between the EU and Ukraine, Georgia, Turkey, and Kosovo.

The total number of third country nationals involved (visa required and visa exempt) will be around 76 million per year in 2025.

While 'minimum checks' are currently performed on EU citizens and persons enjoying the right of free movement, third country nationals crossing the Schengen area external border are subject to 'thorough checks'. The Schengen Borders Code currently requires

¹⁴ Regulation (EC) 562/2006 of the European Parliament and of the Council establishing a Community Code on the rules governing the movement of persons across borders (Schengen Border Code)

¹⁵ Border checks on this category of persons shall be carried out in accordance with Directive 2004/38/EC, the Free Movement Directive.

¹⁶ or on the basis of a touring visa as proposed by the Commission on 1 April 2014 (COM(2014) 163 final)

¹⁷ The external borders of the EU include land borders with non-EU countries, as well as international air- and seaports.

¹⁸ Technical Study on Smart Borders, European Commission, DG HOME, 2014, chapter 7. In this study a counting was conducted during one week: the number of border crossings at land, sea and air borders was counted for European citizens, visa holders and visa exempt third country nationals and the figures extrapolated to a full year and till 2020 and 2025.

that thorough checks are made manually at borders (both at entry and exit) and do not allow the use of modern technologies for automated processes for third-country nationals.

The increasing traveller flows and the principle of a thorough border check on all third-country nationals have increased waiting times at borders in such a way that it constitutes already a problem for many Member States¹⁹.

On 15 December 2015, the Commission proposed an amendment to the Schengen Borders Code²⁰ in order to enforce systematic checks of EU citizens and persons enjoying the right of free movement against databases on lost and stolen documents as well as in order to verify that those persons do not represent a threat to public order and internal security. The implementation of these systematic checks will put further demands on the border management capacity and resources of Member States.

Problem 2: Control of authorised period of stay of Third Country Nationals is error prone, slow and not systematically implemented.

The Schengen Borders Code stipulates that third-country nationals have, as a general rule, the right to enter for a short stay of up to 90 days within any 180 day period²¹. There are however no provisions on the recording of travellers' cross border movements into and out of the Schengen area.

Currently the stamping of the travel document indicating the dates of entry and exit is the sole method available to border guards and immigration authorities to calculate the duration of stay of third-country nationals and to verify if someone is overstaying. Checking a traveller who has been making 10 visits to the Schengen area during the last months means verifying 20 stamps and using them to calculate the time spent in the area. These stamps can be difficult to interpret: they may be unreadable or the target of counterfeiting.

Difficulties affecting the legibility of the stamps as well as the absence of entry stamps were highlighted by the Member States in their replies to the questionnaire carried out by the Commission prior to the report on the operation of the provisions on the stamping of travel documents of third-country nationals²². Calculating time spent in the Schengen

¹⁹ E.g.: Estonia has implemented an electronic queuing system where travellers intending to cross the land border with Russia have to register to get a place in the virtual queue (i.e.: to get an appointment). This solution complements the system of waiting areas installed close to the border crossing points.

²⁰ COM(2015) 670 final.

²¹ However, it is to be noted that currently according to Article 20(2) of the Convention Implementing the Schengen Agreement (CISA), if a Member State concluded a bilateral visa waiver agreement with a third country on the list in Annex II of the Visa Regulation ('visa-free list') before the entry into force of the CISA (or the date of the Member State's later accession to the Schengen Agreement), the provisions of that bilateral agreement may serve as a basis for that Member State to 'extend' a visa-free stay for longer than 90 days in its territory for nationals of the third country concerned. This means that many third-country nationals can in theory remain for practically unlimited stays in the Schengen area, which is not compatible with a common visa policy. Furthermore, in the context of the introduction of Entry Exit System, it is even more important to note that the EES would not be able to take account of the potential impact of the bilateral agreements, which depends also on the travel pattern of each individual traveller (i.e. to which country he/she goes after which, how long he/she stays etc.). The system can calculate on which day the person will have used up the 90 days he/she is entitled to under Schengen rules, but cannot state whether the person is still staying legally, because that depends on the Member State he/she is staying in. Therefore, it would not be possible for the EES to flag an alert stating that these people are overstaying. In its proposal of 1.4.2014 (COM(2014) 163 final) the Commission proposed to solve this unsatisfactory situation by replacing this patchwork of bilateral agreements with a new visa type (touring visa), which is currently undergoing the legislative procedure.

²² COM(2009) 489 final. Report from the Commission to the European Parliament and the Council on the operation of the provisions on stamping of the travel document of third-country nationals in accordance with Article 10 and 11 of Regulation (EC) No 562/2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code)

area on the basis of stamps in the travel documents is thus both time-consuming and difficult with the consequence that often it may not be checked accurately.

Bilateral agreements between Member States and third countries authorising citizens from these third countries to stay for period of time longer than 90 days in the Member State bound by these bilateral agreement create exceptions to the short stay rule. These exceptions make border checks even more complex.

Similarly, it is difficult for consulates having to process visa applications to establish the lawful use of previous visas on the basis of the stamps present in the travel document²³.

Problem 3: Current border control process cannot report and identify overstayers systematically and easily and in a reliable manner, resulting in a lack of reliable information on irregular immigration and problems for return.

Irregular migration into the EU poses a challenge to every Member State. Irregular immigrants include both persons who crossed the borders irregularly – usually not at an official border crossing point - and so-called “overstayers”: persons having legally entered the EU at an official border crossing point but who stayed after their entitlement to do so expired. Up to 2013 and the beginning of the refugee crisis, it was estimated that the majority of irregular immigrants consisted of this second category. While accurate figures or estimates are not available, it is probable that ratio has evolved since then and will continue to change in the coming years. Overstayers can represent a burden for the Schengen area if, for example, they intend to stay in the Schengen area for a long period of time taking a job in the underground economy or participating in any kind of criminal activity. The category of overstayers may also include victims of human trafficking, including victims of labour or sexual exploitation.

Overstayers can be apprehended by means of inland controls. In 2014, the number of overstayers detected within the Schengen area amounted to 441.780, according to the regular collection by Frontex of data from Member State²⁴. As reported in the 2013 EES Impact Assessment, conservative and by now outdated estimates of the total number of irregular immigrants (both irregular arrivals and overstayers) in the EU vary between 1.9 and 3.8 million²⁵. More precise and updated figures are not available.

As border crossings by third country nationals are currently not registered, it is not possible to establish lists of overstayers. For the control of third country nationals present in the Schengen area, if the individuals do not present their travel documents (for example, because they claim to have lost them), it is impossible to determine accurately their entry date as well as their citizenship.

As a result immigration authorities have no effective and reliable means to identify and detect overstayers, which is a major shortcoming of the current EU policy against irregular migration.

Problem 4: The fight against international criminality, terrorism and other security threats needs to be further reinforced

²³ At border controls, the VIS is consulted for visa authenticity and validity verification and for the biometric identification of the traveller. The use of a visa is not recorded in VIS.

²⁴ Frontex, Annual Risk Analysis 2015 – Page 99. From 2011 till 2013 this figure was about 350.000 persons

²⁵ 'Clandestino', an EU-sponsored project implemented by the International Centre for Migration Policy Development give the date

The globalisation of criminality follows the globalisation of economics²⁶. International criminal organisations are developing their activities across borders²⁷. Criminal activities such as trafficking in human beings, smuggling of people or the smuggling of illicit goods involve numerous border crossings, which are facilitated by the absence of registration of the border crossings of the third country nationals concerned. Likewise, terrorist organisations and radicalised individuals can benefit from the absence of registration of border crossings.

Controls of third-country nationals at external borders involve identity checks and searches against various databases of known persons or groups posing a threat to public security that should be either apprehended or denied entry to the territory. Currently, all verifications are carried out based only on the travel documents presented by the third country national. Even though the alerts on these persons may have been recorded in the Schengen Information System (SIS), or other national and international databases, they can only be identified on the basis of the alphanumeric data that was introduced with the alert. This makes it difficult for the authorities to detect a person using different identities to cross the borders.

In general, identification is essential for law enforcement authorities in their mission to prevent and combat terrorism and other serious crime. However, in the event that a third country national destroys his/her official documentation once having entered the Schengen area, it can be very difficult for law enforcement authorities to identify that person in case he/she is suspected of a crime or is a victim of crime. While data on EU citizens exists in different databases in Member States that are in general accessible to law enforcement authorities, there is an information and verification gap concerning third country nationals who are not covered by the Visa Information System (VIS).

2.2. Implementation problems addressed by this impact assessment

During the first examination of the package which was completed in February 2014, the co-legislators voiced technical, cost-related and operational concerns, mainly on the feasibility of both systems and the practicability of certain features.

Concerns related especially to the limited number of potential users and administrative burden of implementing RTP, the length of the data retention period in the EES, the choice of the biometric identifiers, the extent to which the national entry exit systems could be integrated and/or reused, the need for enhanced synergies and/or interoperability with existing systems used during border controls and, last but not least, the possibility for law enforcement authorities to access the system.

In that context, the Commission proposed to initiate a two-step proof of concept exercise to cope with the identified concerns, the first step being a technical study and the second one a testing phase. The purpose of the proof of concept was to ensure that the two co-

²⁶ "Criminals capitalise on new opportunities to generate profit, especially when they are able to rely on existing infrastructures, personnel and contacts. This is particularly true for the groups involved in the transportation and distribution of illicit commodities. The ease of international travel and transport, the global emergence of the internet and other technological advances have made geographic considerations less relevant. Criminals act undeterred by geographic boundaries and the most significant groups are now global in terms of their range of activities, operating areas, levels of cooperation and nationality of membership." : Europol's EU Organised Crime Threat Assessment 2013 (OCTA 2013), p. 37.

²⁷ "Analysis of the nationality of criminals and the countries of main activities has demonstrated that **criminal groups are becoming increasingly international**. For example, both Belgium and Portugal reported criminal groups consisting of more than 60 nationalities of criminals. These two countries also reported criminal groups whose main criminal activities extend to more than 35 countries. This clearly indicates a significant level of international criminal **cooperation, mobility and reach**." : idem, p. 34.

legislators would be given a sound analysis containing the best possible options and solutions from a technical and a cost-benefit point of view.

On 4 February 2014, the Permanent Representatives Committee (COREPER) endorsed the "*Approach for the way forward on the Smart Borders Package*"²⁸ as proposed by the Commission as well as a list of questions to be addressed during the proof of concept: "*... there appears to be consensus on including 1) interoperability between EES and RTP and other existing systems used during border checks, 2) the technical aspects of law enforcement access, 3) biometrics and 4) feasibility of the token and other possible options. Other issues which have been mentioned by delegations include: 1) detailed and updated cost analysis of different options and technical solutions, including in relation to costs at national level, 2) integration of the national systems in the future EES and RTP, and 3) processing time at the border.*"²⁹

The European Parliament proposed to include in the list of questions to be studied the impact on border crossing time, the feasibility at all type of border (air, sea and land), a scope reduction for the RTP, an EES with law enforcement access and the interoperability of existing systems. The EP asked also for a cost analysis, statistics concerning border crossings and information concerning MS experiences with automated border control systems,

The Commission has invited experts of Member States as well as representatives of the EP to a meeting on 7 February 2014 to establish the objectives of the study. The participants in this meeting agreed to organise the questions to be addressed in five themes:

1. Architecture of the systems, including the possibility to develop EES and RTP as one single system, the possibility of developing EES/RTP as new VIS functionalities, the interoperability with VIS and SIS as well as the relation with the existing national systems.
2. Biometrics, which identifier should be used, impact on border crossing time and on border control process.
3. Impact on Border control processes, including automation, facilitation, process accelerators, impact for different border types, impact on border crossing point infrastructures and RTP enrolment process.
4. Data, including retention period, law enforcement access, impact on Fundamental Rights, data set minimisation and privacy by design.
5. Cost analysis of the various options and statistics on border crossing.

These five groups of questions addressed during the proof of concept have resulted in the options that are subject of this Impact Assessment, while the cost analysis is a cross-cutting issue.

²⁸ Doc. 5828/14

²⁹ Idem.

2.3. The drivers of the problems

The main drivers of these problems are:

- The absence of an EU wide IT system:
 - for recording travel movements of third-country nationals admitted for a short stay;
 - for identifying persons detected within the territory without travel documents who cannot be identified using the VIS;
 - helping in detecting persons subject to a SIS alert who use different identities to cross the borders.
- The very limited value of national entry exit systems in an area without internal border control between 26 countries.
- The lack of information in the area of migration management:
 - of who is in the Schengen area and who complies with the maximum allowed short stay of up to 90 days within a 180 day period;
 - that can support random checks within the Schengen area to detect irregularly staying persons;
 - on nationalities and groups (visa exempt/required) of travellers overstaying.
- The challenges posed by the current border control process:
 - which makes it difficult for the border guard to assess the authorised stay at the border check of the traveller;
 - which does not allow for the use of modern technologies for automated processes and border checks facilitation for third-country nationals.
- The lack of information in the area of law enforcement:
 - allowing the identification of a suspect who has destroyed his or her travel documents;
 - on cross-border movements of persons suspected of criminal activities or of victims of these activities.

2.4. Who is affected, in what ways and to what extent?

Where the problems mentioned above have an impact on the quality of border controls they affect border guards, visa/immigration authorities and authorities competent for carrying out checks within the territory.

Where they lead to a slow control process and long waiting times, they affect third-country nationals crossing the external borders of the Schengen area for short stays.

Carriers (airlines, buses, ferries), tourist agencies as well as infrastructure operators (airports, ferry terminals), whose activities involve third country national border crossings, are equally affected by the waiting time for border crossing.

EU regions close to the eastern external land border and major seaports or airports can be affected, in cases where retail activities are dependent on third country nationals travelling for shopping.

EU citizens crossing the external border of the Schengen area are not directly affected and use their specific lanes at border control posts. However, increasing number of third

country national border crossings combined with human resources limitations for border controls could in the future also have an impact on their waiting time at borders.

EU citizens, as well as Member State administrations, public services and private economic operators, are also affected by the fact that EU border management is currently insufficiently equipped to tackle the problem of overstaying (and hence irregular migration).

Finally, law enforcement authorities are also affected as they are facing difficulties for the identification and monitoring cross border movements of third country nationals involved in criminal or terrorist activities and for identifying criminals among suspects.

2.5. Experiences with EES and RTP systems

2.5.1. Entry Exit Systems

There are several Member States and third countries implementing their own national entry/exit systems. 13 Member States³⁰ currently have such a system in place and the only data collected are alphanumeric. The main purpose of these systems is to give law enforcement authorities the opportunity to store travel records of certain third-country nationals in accordance with security-related national legislation. Therefore these Member States give access to their national systems not only to border authorities but also to law enforcement authorities for the purpose of investigating crime.

If a person lawfully exits the same Member State through which he or she entered, then any overstayer would be detected by the relevant national EES systems. Beyond that, there are no possibilities for using such systems to detect overstayers as entry and exit records cannot be matched when persons leave the Schengen area via a different Member State from the one through which they entered and in which their entry was recorded.

As for non-Schengen countries, part of the UK's e-Borders programme aimed, among other things, to record entry and exit data based on the advance passenger information transmitted to government authorities by carriers transporting persons to the UK.

The Office of Biometric Identity Management—which has absorbed the former U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) system in 2013—requires most foreign nationals to provide fingerprints, photographs, or other biometric identifiers upon arrival in the United States. The automated biometric entry-exit system grew from a photograph and two-finger biometric system for immigration identification to the major identity management and screening system for the Department of Homeland Security.³¹

U.S. Customs and Border Protection (CBP) collects biographic information on all nonimmigrant arrivals to the United States through an inspection by a CBP officer. In the *air and sea environment*, CBP officers validate the manifest information provided by commercial and private aircraft operators. For many nonimmigrants, submission of biometric information is also required upon admission and is captured in the presence of a CBP officer. Since US airports do not have designated areas exclusively for travelers

³⁰ Finland, Estonia, Spain, Latvia, Lithuania, Poland, Slovakia, Hungary, Romania, Bulgaria, Cyprus, Portugal, Malta.

³¹ Congressional Research Unit. "Non-immigrant Overstays: Brief Synthesis of the Issue – January 22, 2014 on <https://fas.org/sgp/crs/homesecc/RS22446.pdf>".

leaving the United States, departures of travelers are recorded biographically using outbound passenger manifests provided by commercial carriers. Under regulations governing the Advance Passenger Information System, carriers are required to validate the manifest information against the travel document being presented before a traveler is permitted to board their aircraft or sea vessel.

In the *land environment*, there is no such requirement for advance reporting of arrivals and departures, as the majority of travelers cross the borders using their own vehicle or as a pedestrian. On June 30, 2013, Canada and the United States began exchanging entry data for third-country nationals, permanent residents of Canada, and U.S. lawful permanent residents, who enter through land POEs (Points of Entry) along the shared border, where information is collected electronically. As a result of this initiative, the United States now has a working land border exit system on its Northern border for non-U.S. and non-Canadian citizens. There is currently no equivalent entry/exit system operated with Mexico³².

Arrival and departure records of travellers to and from Australia are contained within the Movements Reconstruction database, set up in 1981. In Japan, a biometric border control programme for all non-Japanese citizens was introduced in 2007 as a measure for preventing terrorism and irregular immigration, while a system for recording biographical entry and exit data has been in place for several years.

At the high level conference on 2 and 3 February 2012³³, representatives from the responsible authorities in the USA and Australia described the new systems as a success and as an effective tool for the authorities to detect irregular migrants and to fight serious cross border crime. However precise figures on the number of apprehended irregular migrants were not presented.

Hong Kong SAR (Special Administrative Region) records entries and exits of both its own permanent residents using e-Gates (the so-called e-Channels) for 43% of cross-border movements and of non-residents whose use of automated means is increasing over recent years. Independently of the means used, Hong Kong has a full record of entries and exits of all travellers at all types of borders (air, land and sea). The increased efficiency of border controls using automated means is demonstrated by the fact that Hong Kong increased manpower of the immigration department only by 16% from 2003 till 2014, while traveller's throughput increased 81% over the same period.

2.5.2. Registered Travellers' Programme

Many non-EU countries such as the US, Canada, Australia and Singapore have also automated their border check procedures based by means of a Registered or Trusted Traveller's Programmes. The access granted for these programmes are limited. They are established only for their own citizens or their own citizens and neighbouring country citizens. Singapore eIACS system has three million users and the US system has one million users (see next).

Global Entry is a U.S. Customs and Border Protection (CBP) program that allows expedited clearance for pre-approved, low-risk travelers upon arrival in the United States.

³² Information from this section was updated following the document from the US Department of Homeland Security, "Entry/Exit Overstay Report Fiscal Year 2015" – January 19, 2016

³³ Conference on Innovation Border Management organised by the Danish presidency and the Netherlands on 2 and 3 February 2012 in Copenhagen reported under Council document 7166/12, Presidency summary of findings

Participants may enter the United States by using automated kiosks located at specific airports. At airports, program participants proceed to Global Entry kiosks, present their machine-readable passport or U.S. permanent resident card, place their fingertips on the scanner for fingerprint verification, and complete a customs declaration. The kiosk issues the traveler a transaction receipt and directs the traveler to baggage claim and the exit. Travelers must be pre-approved for the Global Entry program. All applicants undergo a rigorous background check and in-person interview before enrollment. While Global Entry's goal is to speed travelers through the process, members may still be selected for further examination when entering the United States. Global Entry is open to U.S. citizens, lawful permanent residents, citizens of Germany, the Netherlands, Panama, and South Korea, and Mexican nationals. Canadian citizens and residents may enjoy Global Entry benefits through membership in the NEXUS program. Membership fee is USD 100 (about € 92) for five years. Out of 1.070.142 participants 95% were US citizens and permanent residents, 4% Mexican residents and only 1% (so about 10.000) of other nationalities³⁴.

U.S. Customs and Border Protection (CBP) runs in total four trusted travellers programmes, Global Entry being one of them, each aimed for specific target groups (like NEXUS which is for US and Canadian citizens and permanent residents). On average 7% of arriving passengers in the US use the trusted traveller lanes³⁵.

In 2015, the United Kingdom implemented a new Registered Travellers' Scheme open to nationals of Australia, Canada, Japan, New Zealand or the USA, who are at least 18 years old and have visited the UK at least four times in the last 24 months before applying. The target is to enrol up to 200.000 persons at an annual fee of £70 (about € 92). As opposed to the schemes used in the US and Australia, neither UK nor other EU nationals need to enrol in such a scheme as they can cross the UK automated border lines using their biometric passport without any pre-enrolment. It is a national scheme as opposed to other ones specific to an airport such as Privium evoked in the next paragraph, in principle applicable to all types of borders although practically by its fee level and sort of advantage (use of automated control lanes in airports) it only provides a real benefit to frequent fliers.

The RTP scheme that is often cited is Privium, the Schiphol Airport's (Netherlands) automated border crossing programme for frequent fliers. The passport holders of all EU countries as well as Norway, Iceland, Liechtenstein and Switzerland are eligible to apply for the membership of the programme. Also US Global Entry members can use the Privium services. The majority of its members are business travellers, flying an average of 16 times a year through Schiphol Airport. During the pre-enrolment procedure the applicant has to fill in the commercial database so that the smartcard would be prepared for the final enrolment. The final enrolment includes application processing, biometrics capturing, check of blacklist databases etc. The Dutch Privium programme asks for a membership fee of €121 for the basic version and is reported to be mainly attractive for both its border crossing facilitation as well as the use of parking close to the terminal and of dedicated lounges. In 2014 the scheme had 48,000 members, which accounts for approximately 0.5% of the total targeted number of travellers.

³⁴ As reported by United States Government Accountability Office (GAO) in its report on TRUSTED TRAVELERS of May 2014 – See Figure 4 - <http://www.gao.gov/assets/670/663724.pdf>

³⁵ Cited in Smarter Borders, Biometrics, Facial, Recognition and Data: Talking about Smarter Borders with Ken Sava, U.S. CBP's Trusted Traveler Director, 23-25 November 2015.

2.6. What is the EU dimension of the problem?

The effective management of the external borders by the 26 countries³⁶ which are part of the Schengen area is a prerequisite for the free movement of persons within the area. A Member State could register third country nationals entering through its external border, but, as any of those third country nationals can and often do leave the Schengen area through a different Member State's external border, the relevance of such registration is very limited.

Where national entry exit systems³⁷ are in place today, their main objective is to support law enforcement. These different systems result in a redundancy of stored data (the same person's identity is stored in different databases) based on diverging national legislation, which is clearly undesirable from the perspective of data protection.

To address the EU-wide problems mentioned in section 2.1 any Schengen-wide solution needs to be uniformly applied at the 1800 external border crossing points of the Schengen Area.

2.7. How would the problem evolve, all things being equal?

The following elements are considered to be satisfactory and either will remain stable or evolve positively:

- An increasing proportion of EU citizens will use the Automated Border Control gates (e-Gates). Today these are mainly installed at airports but they will progressively also be used at sea and land borders. The deployment of additional e-Gates in the EU is promoted through the EU's Internal Security Fund (ISF).
- Following the recent completion of the roll-out of the EU's Visa Information System (VIS), all applications for a Schengen-visa will contain the ten fingerprints and a facial image³⁸ of the applicant. The enrolment of these biometric identifiers in VIS prevents visa fraud and allows identity verification at borders, as well as identification³⁹.
- Adoption of the Commission proposal for a touring visa⁴⁰ will resolve the unsatisfactory patchwork of bilateral agreements⁴¹.

The following elements are considered to be or to become unsatisfactory:

- To cope with the increased travellers' flow, in particular of third-country nationals, while remaining compliant with the existing Schengen Borders Code, the number of

³⁶ The notion Schengen Member State covers also the Schengen associated third countries: Iceland, Liechtenstein, Norway and Switzerland

³⁷ Bulgaria, Cyprus, Estonia, Finland, Hungary, Latvia, Lithuania, Malta, Poland, Portugal, Slovakia, Romania, Spain.

³⁸ A photo is the image of a person on a substrate (paper, plastic). A facial image is the digital representation of the image of a person.

³⁹ 'Verification' means the process of comparison of sets of data to establish the validity of a claimed identity (one-to-one check); 'identification' means the process of determining a person's identity through a database search against multiple sets of data (one-to-many check).

⁴⁰ Proposal for a Regulation of the European Parliament and of the Council establishing a touring visa and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 562/2006 and (EC) No 767/2008 (COM(2014) 163 final) with its annexes

⁴¹ COM(2014) 163 final

border guards will need to follow the same upward trend and the border crossing point infrastructures will necessitate enlargements and investments. This is not sustainable as it implies more budget and also more floor occupation which at air and especially at land borders can be physically impossible.

- As a result, the foreseen increase of border crossings will result in a waiting time increase for third country national travellers and as a side effect also for EU citizens as the border crossing points will reach saturation level. This could result in less thorough checks with direct consequences for the security of the Schengen Area.
- It will remain difficult for border guards to check compliance of the rule on the maximum duration of stay (no more than 90 days in any 180 day period) if border controls have to continue to rely on reading entry and exit stamps of the Schengen area. At the same time, it does not become easier for travellers to know their remaining duration of authorised stay as they can also only rely on reading these stamps.
- It will remain as difficult as it is today to identify overstayers and to implement the EU Return Policy⁴². Border guards can only identify an infringement of the rule on the maximum duration of stay by verifying the entry and exit stamps in the passport. In practice, at border, this check is often not performed given the time pressure. For irregular migrants, the absence of travel documents constitute a major obstacle to the effective return due the uncertainty about the identity of the person and the impossibility to define accurately the overstay period as there is not possibility to check any entry stamp.
- Visa applications will continue to be handled without systematic information on the travel history of the applicant and compliance of duration of previous stay. Each time a visa-required third country nationals applies for a visa, the consular officer from the Schengen Member State looks into previous visa applications of the same traveller in VIS. The consular officer is also required to verify whether the visa applicant is prohibited entry into the Schengen area. However, neither VIS nor other systems contain the information as to whether the visa applicant complied with the duration of stay; this can be ascertained only by checking the entry and exit stamps in the travel document used, assuming that the travel document has remained the same.
- While the use of the VIS will certainly continue to contribute to the security of the Schengen area, the successful finalisation of the ongoing visa liberalisation dialogues will also lead to a considerable increase in the number of visa exempt travellers crossing the external borders, placing additional challenges for the management of the external borders of the Schengen area.
- Law enforcement authorities will not have access to information on movements across the Schengen borders that could be used as a criminal intelligence or identification tool in the fight against terrorism and other forms of serious crime.

⁴² COM(2015) 453 final

2.8. Conclusions of the evaluations of the existing policy

At the moment, the entries and exits of third country nationals in the Schengen area are recorded only in their travel documents, which entails the limitations and consequences described above for border management and overstayers identification. This recording is materialised by the stamping of travel documents. The stamp indicates the location, date and direction (entry or exit) of the border crossing and is not machine readable. The existing EU policy does not foresee any register for entries and exits of third country nationals.

The existing policy cannot be adapted or modified to cope with the increasing traveller flows at external borders. A new approach relying on IT systems and automation has to be considered. Such entry exit systems are operational in the United Kingdom, Australia, Japan and several other countries, where they deliver the expected results of better border management and control of overstay. The International Organisation for Migration considers that a system correlating entry and exit data is required for an efficient and effective border management⁴³.

The VIS is an example of a successfully delivered EU large-scale IT system, where the use of biometrics, reliability and availability, and the management of access to its data by different groups of users having different access rights are amongst the main features. The VIS is in operation since October 2011 and its roll-out in all the consular posts of Schengen Member States was completed in November 2015. Systematic verification at the border by means of biometrics to check that the visa belongs to the traveller is mandatory since October 2014. Although a formal evaluation report of the VIS will only be available in 2016, some important observations can already be made:

(1) The use of biometrics has provided the expected benefits. "Visa-shopping" has stopped because any time a new visa application is created the "visa history" of the applicant is checked in the system. The biometrics captured is used to ascertain whether another visa-application is outstanding for the same person under another identity. Visa-fraud is excluded because the fingerprints taken at the border are matched with fingerprints provided at the moment of the visa application.

(2) The biometric verification of visa-holders at the border was not reported to have negatively affected border crossing time. Border control processes have not slowed down, but did become more secure.

(3) VIS was delivered on time and on budget. Although the VIS was delivered twelve months later than initially announced, this delay was entirely due to a well-evaluated and duly accepted change to its technical requirements. The VIS feasibility study estimated the multi-annual project budget⁴⁴ at €158 million while the project was delivered for €161 million.

⁴³ International Organisation for Migration, Border Management Systems, Section 3.3, page 14.

⁴⁴ The budget for VIS only included the cost for delivering the central system and did not include the development cost of national systems nor the cost for operations afterwards. In this Impact Assessment the cost of EES includes development costs of central and national systems, plus operations costs.

3. WHY SHOULD THE EU ACT?

Under Articles 74 and 77(2) of the Treaty on the Functioning of the European Union (TFEU), the Union has the power to adopt measures relating to the crossing of the external borders of the Member States. Under Articles 82 (1)(d) and 87(2)(a) TFEU the Union also has the power to adopt measures to strengthen police and judicial cooperation concerning the collection, storage, processing, analysis and exchange of relevant information.

The absence of internal borders in the Schengen area requires a sound management of external borders where each country has to control the external border on behalf of the other Schengen States. Consequently, no Member State alone is able to cope on its own with irregular immigration. A person may enter the Schengen area at a border crossing point in a Member State where a national register of entry/exit data is used, but exit through a border crossing point where no such system is used. The monitoring of compliance with EU rules on authorised stays can therefore not be done by Member States acting alone. Third-country nationals who enter the Schengen area are able to travel freely within it. In an area without internal borders, action against irregular immigration should be undertaken in common. Considering all this the EU is better placed than Member States to take the appropriate measures.

At the Justice and Home Affairs and European Councils in December 2015, Member States emphasised the need to improve the controls at external borders through the use of new technologies.

The European Agenda on Migration⁴⁵ identifies "*border management*" as one of the "*four pillars to manage migration better*". Securing external borders and managing them more efficiently implies making better use of the opportunities offered by IT systems and technologies. The use of the three existing EU large-scale IT systems (SIS, VIS and Eurodac (European Dactyloscopy)) brings benefits to border management. A new phase will come with the Entry Exit System implementation to increase the efficiency of border crossings, facilitating crossings for the large majority of '*bona fide*' third country travellers, whilst at the same time strengthening the fight against irregular migration by creating a record of all cross-border movements by third country nationals, fully respecting proportionality.

The implementation of an EU wide Entry Exit System will result, amongst other things, in the automation of certain tasks and activities related to border controls. This automation will ensure a homogeneous and systematic control of the authorised period of stay of third country nationals.

The use of EES in combination with new possibilities for using self-services systems and automatic or semi-automatic border control solutions will facilitate the work of border guards and help them absorbing the forecasted increase of border crossings. From the traveller's perspective this will result in a facilitation of border crossing, as the waiting time will be reduced and border checks will be faster.

An amendment to the Schengen Border Code will introduce the possibility for Member States to implement facilitation schemes at national level. This amendment will secure

⁴⁵ COM(2015) 240 final

facilitation schemes, existing or future, providing clear common rules consistent with the Schengen Border Code provisions.

Although Member States may retain their national systems in accordance with security-related national legislation, an EU Entry Exit System would allow Member State authorities to access data on third-country nationals who crossed the EU external border in one country and exited via another Schengen country.

Better information on cross border movements of third-country nationals at EU level would establish a factual basis to develop and adapt the EU migration policy, including its visa policy. It would help setting priorities for readmission agreements and visa facilitation agreement with third countries. It would contribute to a common understanding of immigration issues and priorities in policy dialogues with countries of origin and transit.

4. OBJECTIVES

4.1. General policy objectives

The general policy objectives are essentially the same as in the initial 2013 proposals. They are, in order of priority:

- (1) To improve the management of external borders
- (2) To reduce irregular migration, by addressing the phenomenon of overstaying.
- (3) To contribute to the fight against terrorism and serious crime and ensure a high level of internal security'

Improved border management can be measured by its effectiveness and efficiency. Effectiveness in border management is achieved if it facilitates the border crossing of legitimate travellers whilst at the same time preventing that travellers not meeting the entry conditions from entering the Schengen area or apprehending them at exit. Efficiency in border management is achieved when the increase of border crossings does not require a similar increase of border guards,

The fulfilment of the second objective is dependent on the first, but also requires utilisation of the Entry Exit System by relevant authorities within the territory of the Schengen area. The EES will contribute to the implementation of the EU policy on the return of illegally staying third-country nationals.

The implementation of EES will ensure a better identification of third country nationals and will allow for the detection of people using several identities. This will help to achieve to a certain extent the third policy objective. However, this objective can only be fully realised when access to the entry exit system is granted to law enforcement authorities (see section 5.5).

No new policy in new areas will be developed. The proposal is part of the continuous development of the Integrated Border Management Strategy of the European Union.

4.2. Specific policy objectives

The main policy objectives of the Entry Exit System and modifications of the Schengen Borders Code are, in order of priority, to:

- (1) Enhance the efficiency of border checks through monitoring of the rights to authorised stay at entry and exit;
- (2) Identify and detect overstayers (also within the territory) and enable national authorities of the Member States to take appropriate measures including to increase the possibilities for return;
- (3) Free up border control resources from performing checks that can be automated and enable better focus on traveller assessment;

- (4) Facilitate the crossing by third-country nationals of EU external borders through self-service systems and semi-automated or automated systems while maintaining the current level of security;
- (5) Enable consulates to have access to information on the lawful use of previous visas;
- (6) Inform third country nationals of the duration of their authorised stay;
- (7) Improve the assessment of the risk of overstay;
- (8) Support evidence based EU migration policy making;
- (9) Combat identity fraud.
- (10) To identify and apprehend terrorist, criminal suspects as well as of victims crossing the external borders;
- (11) To generate information on travel histories of third country nationals including crime suspects that would help investigations related to terrorism or serious crime.

4.3. Consistency with other EU policies and with the Charter for fundamental rights

The idea of establishing an EU Smart Borders System was first suggested in the Communication of 13 February 2008 *'Preparing the next steps in border management in the European Union'*⁴⁶. The proposal was endorsed in the Stockholm Programme agreed by the European Council in December 2009⁴⁷.

In October 2011 the Commission further developed this idea in a Communication on the implementation options for the EES and RTP⁴⁸. This was followed in February 2013, as already mentioned in the introduction of this Impact Assessment, by legislative proposals for a Smart borders package.

The proposals therefore build on a long-standing political mandate to undertake concrete action in this area.

4.3.1. Consistency with EU migration and security policy

In 2015 the revision of the legislative proposals on Smart Borders was announced in both the European Agenda on Migration⁴⁹ and the European Agenda on Security⁵⁰. The latter underlines that common high standards of border management are essential to preventing cross-border crime and terrorism and points out that the revised proposal on Smart Borders will help increasing the efficiency and effectiveness of border management. The Agenda on Migration stresses that in order to manage Schengen borders more efficiently

⁴⁶ COM(2008) 69 final. The Communication was accompanied by an Impact Assessment SEC(2008)153.

⁴⁷ 17024/09 and EUCO 6/09

⁴⁸ COM(2011) 680 final

⁴⁹ COM(2015) 240 final

⁵⁰ COM(2015) 185 final

there is a need to make better use of the opportunities offered by IT systems and technologies. It refers to the three existing systems: Eurodac (to deal with the administration of asylum), VIS (for managing visa applications) and SIS (for sharing of information on persons and objects for which an alert has been created). It announces a new phase will come with the Smart Borders initiative, which addresses objectives that are not met by the other three systems, and has a scope which is complementary to them.

The inter-relation between Eurodac, VIS, SIS and the future EES is further explained in the Communication 'Stronger and Smarter Borders' that will accompany the presentation of the revised proposals on Smart Borders.

As explained in the introduction of this Impact Assessment, there is no direct link between the EES proposal and the current refugee crisis. There are cases of third country nationals that apply for asylum after having arrived in Schengen in the framework of short-term legal stay (these people would be recorded in a future EES) or on arrival at a border crossing point; but the large majority of refugees arrives irregularly, not at a border crossing point, and are hence recorded only in Eurodac. Proposals to better adjust Eurodac to current challenges are currently being prepared and will be adopted by the Commission around the same time as the Smart Borders proposals.

The revised proposals on Smart Borders (as well as the proposal on Eurodac) are complementary to the Border Package that was presented by the Commission on 15 December 2015. This package proposed, inter alia, the creation of a European Border and Coast Guard, reinforced crisis prevention and intervention at external borders, the implementation of the hotspot approach, and an amendment of the Schengen Borders Code, to reinforce the border checks on EU citizens and other persons enjoying the right of free movement.

The revised proposals on Smart Borders will also support the implementation of the EU return policy. The EES will record refusal of entry data of third country nationals. More broadly, it will allow for the identification of undocumented third country nationals that at one point of time have legally entered the Schengen zone.

Finally, in the context of internal security, the EES will allow for the identification of third country nationals suspected of committing terrorist acts or serious crime, e.g. based on fingerprints found at the crime scene, or video surveillance images (again, assuming that these people at one point of time legally arrived in the Schengen zone). In addition, information on travel routes and travel history in- and out of Schengen of suspected individuals may be made available in the context of criminal investigations, thereby contributing to the fight against terrorism and serious crime.

4.3.2. Consistency with the Charter of Fundamental rights

The use of modern technologies can be beneficial to fundamental rights. Such technologies will reduce the risk of mistaken identities, of discrimination and of ethnic profiling. They will assist in the detection of missing children or of victims of trafficking in human beings. They can reduce the risk of people being wrongfully apprehended and arrested. It can also contribute to increased security of citizens residing in the Schengen area as it will help to combat terrorism and serious crime.

On the other hand, establishing an entry exit system, due to the personal data involved, has an impact on the right to the privacy and the protection of personal data, enshrined in

Articles 7 and 8 of the Charter of Fundamental Rights⁵¹ of the European Union. Therefore it should be examined in light of the Article 52.1 of the Charter. The legal basis for an EU Entry Exit System will therefore need to guarantee the right to an effective remedy before a tribunal, in line with Article 47 of the Charter, for challenging a notification of overstay, for example in cases of forced overstay, errors or when a migrant has a legal right to stay. Annex 13 'Impact Assessment on Fundamental Rights' contains a complete analysis of these impacts.

The proposals will include appropriate provisions limiting data processing to what is necessary for the specific purpose of the system and granting data access only to those entities that 'need to know'. The choice of limited data retention periods will be made depending solely on the principal objectives of the instrument. Mechanisms ensuring an accurate risk management and effective protection of data subjects' rights will be foreseen.

The system will have to comply with data protection principles and the requirements of necessity, proportionality, purpose limitation and quality of data. It will be developed in full respect of the *privacy by design*⁵² principles. All safeguards and mechanisms will be in place for the effective protection of the fundamental rights of travellers particularly the protection of their private life and personal data. Third-country nationals must be made aware of these rights.

In accordance with data protection legislation, access should be given to the data stored in the Entry Exit System only for specified, explicit and legitimate purposes. This means that the authorities who should have access to the Entry Exit System have to be designated for a specific limited purpose. Therefore, access for consulting the data should be reserved exclusively to duly authorised staff of the authorities of each Member State who are competent for the specific purposes of the Entry Exit System and limited to the extent that the data are required for the performance of the tasks in accordance with these purposes.

⁵¹ 2010/C 83/02. Charter of Fundamental Rights of the European Union

⁵² 'Privacy by design' means embedding personal data protection in the technological basis of a proposed instrument, limiting data processing to that which is necessary for a proposed purpose and granting data access only to those entities that 'need to know.'

5. POLICY OPTIONS

The impact assessments carried out for the 2013 proposals concluded that an EES and an RTP for third-country nationals should be established.

The proposals were based on a preferred solution of an EES system, as a centralised system containing both alphanumeric and biometric data. It was proposed that after a period of two years, the EES should be evaluated and, in this context the Commission would evaluate in particular the possible access to the system for law enforcement purposes as well as the retention period, also taking into account the experience of access for such purposes to the VIS.

As explained in the introduction, this Impact Assessment focuses on the most contentious elements of the 2013 proposals for which changes have been considered.

These elements relate to the concerns expressed by the co-legislators during the first examination of the package, notably the RTP, the length of the data retention period in the EES, the choice of the biometric identifiers, the extent to which the national entry exit systems could be integrated and/or reused, the need for enhanced synergies and/or interoperability with existing systems used during border controls and, last but not least, the possibility for law enforcement authorities to access the system.

In response to these concerns, five main areas were identified for which policy options need to be analysed. In each case the 2013 proposals are taken as the baseline scenario.

- (1) The architecture of the system
- (2) The biometrics used to identify travellers
- (3) The facilitation of border crossings
- (4) The retention time for the storage of data
- (5) The access for law enforcement purposes of the EES data.

The analysis in this section is based on the results of the 'proof of concept' exercise that took place in 2014 and 2015, consisting of a Technical Study on Smart Borders and a testing phase ('Pilot'). The analysis reflects where appropriate past experiences and potential synergies with existing large scale IT systems and the solutions they provide, notably with a view to contributing to reducing costs⁵³ and increasing efficiency.

Privacy by design, personal data protection and data set minimisation are principles sustaining the proposed options. All options are intended to respect the proportionality principle (see annex13 - Impact Assessment on Fundamental Rights).

All options would in principle apply to all third country nationals.

⁵³ When costs are cited from the Smart Border Technical Study, they refer to the cost model for building, maintaining and operating EES and RTP both centrally and for the national part directly communicating to it. When the reference is to four years this correspond to three years for building the system and one year of operation, in line with the current Multiannual Financial Framework (MFF) until 2020. When the reference is to seven years this corresponds to the original duration of the MFF and allows comparisons with the financial estimates of 2013 proposal.

5.1. The architecture: how can the system be most effectively built?

The 2013 proposals foresaw a separate Entry Exit System and Registered Travellers Programme system. The Technical Study has compared the advantages and inconveniences of building EES and RTP separately or as one single system. Two options have therefore to be considered:

- a) Separate EES and RTP systems (2013 proposal)
- b) One single EES/RTP system

One possible way of building a single system would be to combine the functionalities of EES and RTP **on the basis of VIS**. This option was promoted by several stakeholders as the preferred architectural option. Such 'upgrading' of VIS would create a complete system, relying on a single database where data required for VIS, EES and RTP functionalities are registered. VIS, EES and RTP data would remain logically separated in such a way that each type of data can be accessed exclusively through its own functionalities. This would have advantages from a business processes and data perspective point of view. With a single system, maintenance and development can be streamlined and costs will be lower, based on the fact that such developments benefit three systems rather than a single system at a time.

This option was analysed and discarded in the 2012 Impact Assessment, concluding however that biometric matching functionality could be performed by the existing Biometric Matching System, which already provides such a functionality for the VIS. The 2014 Technical Study⁵⁴, analysed in details this option and demonstrated that it would have a significant impact on the existing VIS, at national level in particular. The evolution of a complex system, already operational worldwide in the consulates and at the borders of all Schengen countries with high requirements of availability, will lead to an increase of the risks due to a much more complex testing phase and entry into operation, compared to the development of stand-alone systems. In addition, such an implementation of the EES/RTP starting from the existing VIS platform would also lead to a complex legislative process since the VIS legal framework would need to be significantly adapted. This option has therefore been discarded again. However, as explained hereunder, this is without prejudice to the fact that interoperability between EES/RTP and VIS will be maximised.

5.1.1. Description of the options

(a) If EES and RTP were to be developed as **two physically separated systems** each system would rely on its own database with its own data being separately registered. User access rights are managed separately for both systems. Both systems are using the same biometric matching functionalities as used by the Visa Information System.

(b) If **one single system was to be developed containing the functionalities of both EES and RTP**, this system would rely on a single database where data required for the EES and RTP functionalities are registered. EES and RTP data are logically separated in such a way that RTP data can be accessed exclusively through RTP functionalities while EES data can be accessed exclusively through EES functionalities. However, data used by both EES and RTP functionalities (e.g.: name, surname, date of birth, nationality, travel

⁵⁴ Technical Study, page 268 - 272

document number, biometrics) are shared. User access rights will define which transactions from EES and/or RTP can be used by which user.

For both options,

- Interoperability would be established between the EES/RTP and VIS (see details under point 5.1.3).
- The Schengen Information System⁵⁵ (SIS) can play a significant role with regard of overstayers as EES will notify the Member States competent for a record about the expiry date which will allow the Member State to take the appropriate measures, including the creation of an alert in SIS for the refusal of entry or stay in the Schengen area.
- Specific web services for travellers and carriers will be made available. Travellers will have the possibility to check when planning visiting the Schengen area if the intended visit is compatible with the right to enter for a short stay of up to 90 days within any 180 day period. Carriers will have access to a web service allowing them verifying whether the "traveller is eligible for transportation until destination"⁵⁶. These secured web services will be physically and logically separated from the central system. Users will be required to send the minimum data set required for their query and will receive an OK or non-OK answer.

5.1.2. What are the differences between the options?

The question of whether EES and RTP should be built as one or two systems does not have an impact on the operational processes: border crossing processes can be designed in an efficient and effective way in either case. The argument that the existence of two systems would make the work of border guards more complicated because they would access two systems is ill-founded because end-users do not access the central system directly but through an end-user's interface. The data originating from different systems are integrated in one single response. The real issue is where that integration layer is located. This has both technical and cost-related implications.

Technical considerations: The Technical Study looked at the commonality of processes, data and required technology between EES and RTP, and concluded in favour of one single system: *"Having a single, integrated system for EES and RTP would have multiple benefits. It aligns best with the process approach and the minimal dataset for EES and RTP which show the interweaving between them. There would also be a lowering of the infrastructure and development cost when choosing this option"*⁵⁷. This conclusion is independent of the biometric identifiers used, whether facial image or fingerprints. Simply said, the EES will contain data of all third country nationals, while RTP will contain the Registered Traveller's status (active or not) and application data of frequent

⁵⁵ The Schengen Information System (SIS) is a centralised information system containing alerts on persons and other categories of data for law enforcement and border check purposes. The SIS set up pursuant to the provisions of Title IV of the Convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders (Schengen Convention) (15) constitutes an essential tool for the application of the provisions of the Schengen acquis as integrated into the framework of the European Union.

⁵⁶ Under Article 26 of the Schengen Convention, carriers are obliged to ensure that an alien is in possession of the travel documents required for entry into the territories of the MS. They are not obliged to check the stamps in the passport of visa holders or non-visa holders to ensure that the aliens they transport still have the right to enter the Union as regards the authorised period of stay. However they do check in the case of a single entry visa holder that a stamp has not been entered in the passport in the page facing the one on which the visa is affixed to ensure that it is still valid.

⁵⁷ Technical Study, section 6.3.3 page 277

travellers. RTP can be considered as a subsystem of EES using the same identification data for those third-country nationals that have applied for RT status.

Associated costs: The cost analysis developed as part of the Technical study shows that if EES and RTP would be developed as one single system rather than as two separate ones this would entail a total saving of €49.4 million over 4 years and €69.2 million over 7 years⁵⁸. The savings result from reduced development costs, shared project infrastructure as well as lower recurrent operational costs.

Implementation considerations: The Technical Study clearly concluded in favour of building EES and RTP as one single system. However, one disadvantage of this option is that delivering one single system combining EES and RTP functionalities carries inherently a higher project management risk⁵⁹ than two projects delivering each a single system. This disadvantage however only relates to the time-restricted project phase (estimated to be three years) and not to the subsequent operations phase.

5.1.3. Interoperability between EES/RTP and VIS

The 2013 proposals consider already that EES and RTP should rely on the VIS biometric matching functionalities for all transactions based on the use of biometric data (biometric identification and biometric identity verification)⁶⁰.

The second option (one single EES/RTP) would achieve further interoperability as a direct communication channel between both systems would be established enabling EES/RTP to query VIS, acting in this case on behalf of the EES/RTP user, provided that this user has the required VIS access rights:

- A direct communication channel between EES functionalities and VIS is created. It will allow:
 - EES retrieving information from VIS concerning a traveller's visa;
 - biometric identity verification of visa holder travellers using fingerprints registered in VIS without having to register again these fingerprints in EES;
 - establishing a relation of trust between the systems: a biometric identity verification performed by one of the systems is recognised by the other system (which will avoid having to perform two biometric identity verification for visa holder travellers);
 - identification at the border crossing point (*see point 5.2 "Biometrics"*).
 - retrieving in EES information concerning the travel history (entry and exit records) of a visa applicant for the VIS processing of applications.
- This channel can be used under strictly defined conditions: access rights are defined for each system, meaning that for using the interoperability functionalities an end user needs to have the 'rights' required for accessing both systems.
- For both EES and RTP functionalities, the system is using the same biometric matching functionalities as used by the Visa Information System.

⁵⁸ Pages 8 and 9 of the Technical Study on Smart Borders – Cost Analysis. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_study_en.pdf

⁵⁹ Project management risk refers to the likelihood that a project does not deliver the IT services that are within the remit of the project with the required quality and performance, on time and within budget. So the main risks of a project is that the project either fails to deliver all the IT services, whether it fails on the quality or performance of these services and whether the project is completed on time and without significant budget overruns. The view is that a "small" project carries a lower risk than a "large" project.

⁶⁰ See annex 17 on existing EU large-scale IT systems.

This communication channel will enable both systems relying on each other for biometric identifications or biometric identity verifications, avoiding that the same biometric identifiers have to be enrolled twice (e.g.: a visa holder's fingerprints enrolled in VIS are not enrolled again in EES/RTP as this later system can rely on VIS data for any biometric identifications or biometric identity verification based on these fingerprints).

The implementation of such interoperability corresponds to the *privacy by design* principles as it will reduce the duplication of personal data as (biometric) data registered in one system can be used by the other system without having to register them again. The collection of personal information is thus limited to what is strictly necessary for the specified purposes. It will also reduce the amount of data circulating on the communication networks and transiting through national systems as the queries done on behalf of the user and the corresponding answers (mostly limited to 'HIT'/'NO HIT' or 'YES'/'NO') will use this direct communication channel.

Definition of interoperability and main options are explained in annex 9.

EES/RTP would also use the same communication infrastructure (network) as VIS, the respective data flows remaining logically separated.

5.2. Biometrics: what biometric identifier(s) are required for the correct functioning of the system?

Biometric identifiers are used to strengthen identity checks at external borders and to establish the relationship between an individual, his or her travel document(s) and the information registered in the database.

Biometric identifiers are used also for detecting identity frauds (e.g.: people using several identities), detecting travel document fraud (e.g.: look-alike people using the same travel document) and identifying undocumented people inside the Schengen area.

Biometric identifiers allow using self-service systems for the automation or semi-automation of border controls as explained under point 5.3 (c).

The 2013 proposals suggested using fingerprints as the sole biometric identifier (10 fingerprints for EES and 4 fingerprints for RTP) while the EES impact assessment acknowledged that enrolling 10 fingerprints of visa-exempt travellers would increase the border crossing time.

The Technical Study and the Pilot produced evidence on the feasibility of other options while maintaining a high level of reliability as an identification tool. The Study and the Pilot also took into account the diversity of border crossing types (air, sea or land) as well as the diversity of conditions (environment and climate, inside or outside building, in moving trains or vessels) for border control implementation. The following options are therefore considered:

- a) Fingerprints only (2013 proposal)
- b) Fingerprints and facial image combined.
- c) Facial image only.

Some stakeholders have mentioned the capturing of the **iris image**⁶¹ as a possible alternative biometric identifier, either alone, or in combination with facial image. The iris⁶² has the advantage that while it is captured a facial image can be taken at the same time: the device for capturing the iris is a dedicated camera integrated in the equipment for taking the facial image. 'Iris' would be enrolled in the same way as the facial image. Identity verification would be based on iris or on facial image, at border crossing.

Despite having some advantages, the iris option has been discarded. The Pilot has clearly demonstrated that⁶³:

- Iris capturing appeared to be more difficult for a larger share of the population than the other biometrics i.e. people with a hanging eyelid;
- Iris capturing can be very fast where fixed equipment is deployed (average of 4 seconds) but increases to 20 seconds on average with mobile equipment⁶⁴ which is not significantly faster than for a small fingerprint set. The process was also not easier to be done with mobile devices in moving trains or vessels;
- The implementation of iris as a biometric would require new investments in border posts and eliminates any possibility of re-use of existing equipment: the iris is taken at the same moment as the facial image but with a specific camera. The Smart Borders pilot report indicates that *"The simplest iris cameras costs approximately 1000€ but more sophisticated devices were indicated to cost significantly more. The addition of in-built software for verification and inclusion of anti-spoofing features in the hardware also results in higher device prices"*⁶⁵ which is significantly more per item and brings in a high uncertainty on final costs.;
- The accuracy level of iris technology used in outdoor conditions is currently not sufficient to achieve the objectives of the system as the false negative identification rate was estimated to be 2,5% which is significantly higher than for fingerprints⁶⁶;
- Finally, iris was perceived by travellers as more intrusive than any other biometric⁶⁷.

5.2.1. Description of the options

(a) Fingerprints only (2013 proposal):

For EES, 10 fingerprints of the visa-exempt third country national that is not yet (first entry) or no more (after the end of the data retention period) registered in EES will be enrolled at the border crossing point. For third country nationals registered in EES,

⁶¹ The Technical Study did not investigate this option in detail but identified the "iris" as a potential accelerator and was included in the Pilot project conducted by eu-LISA in 2015.

⁶² Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex random patterns are unique, stable, and can be seen from some distance

⁶³ Smart Borders Pilot Final Report volume 1, section 4.1.3, page 161

⁶⁴ See Annex 14, section "Iris enrolment", page 7

⁶⁵ Smart Borders Pilot Final Report volume 1, section 3.4.2.3, page 130

⁶⁶ Smart Borders Pilot Final report volume 1, section 2.3.5.2, page 53

⁶⁷ Smart Borders Pilot Final Report, volume 2, Annex 7, 'FRA survey in the framework of the eu-LISA pilot on smart borders – travellers' views on and experiences of smart borders', page 307

identity verification at border crossing will be based on a number of fingerprints to be approved by the committee established by the EES regulation. On the assumption that this committee would propose the same solution as in the case of VIS, verification would be done based on 1, 2 or 4 fingerprints.

For RTP, 4 fingerprints for all third-country nationals are enrolled at application. At border crossing, identity verification would be based on a number of fingerprints to be defined by the formal committee set up by the RTP regulation. With the same assumption as for EES, it is likely that verification would be done based on 1, 2 or 4 fingerprints.

For enrolling or verifying fingerprints, the third country national has to press the fingers on the glass of a scanner in the case of a contact scanner or to move the hand(s) in a contactless scanner.

(b) Fingerprints and facial image combined

In this option fingerprints and facial image are used in combination. The Technical Study has demonstrated that the best results in terms of security versus processing speed are achieved when combining the use of **four** fingerprints and facial image.

For EES, the fingerprints and the facial image are enrolled at the border crossing point for third-country nationals not yet (first entry) or no more (after the end of the data retention period) registered in EES. For third-country nationals registered in EES, identity verification based on fingerprints **or** on facial image is done at border crossing.

For RTP, the biometric identifiers are enrolled at application. At border crossing, identity verification based on fingerprints **or** on facial image is done.

The use of **one** biometric identifier is sufficient for identity verification.

For enrolling or verifying fingerprints, the traveller has to press the fingers on the glass of a scanner in the case of a contact scanner or to move the hand in a contactless scanner.

The facial image is enrolled using the picture contained in the chip of the electronic travel document or using a live camera. For verification, a picture from a live camera is compared with the image(s) registered in the system. If the verification is successful, this live-picture is also enrolled. The live-picture in the system is updated if a better quality live-picture is taken. If the image contained in the chip of the electronic travel document is not usable (broken chip, no image, bad quality) or if the travel document is not electronic, the use of a picture taken by a live camera is mandatory. The individual file of a person may contain multiple images, extracted from multiple electronic travel documents (in the case of a traveller using more than one travel document) and acquired from live cameras.

(c) Facial image only

For EES, the facial image of the third country national that is not yet (first entry) or no more (after the end of the data retention period) registered in EES will be enrolled at the border crossing point. For third country nationals registered in EES, an identity verification based on facial image is done at border crossing.

For RTP, the facial image is enrolled at application. At border crossing, identity verification is done on the basis of a facial image.

The processes for enrolling and verifying the facial image are identical to those described for option (b).

5.2.2. Use of biometrics for identity verification and for identification

Biometric identifiers will be used in the following situations:

- at first entry, for **enrolment in EES**, when the individual file is created in the system,
- for **enrolment in RTP**,
- at subsequent border crossings for **identity verification**,
- each time the **identification** of an individual is required.

Before entering into the details of using biometrics, it needs to be emphasised that visa-required third country nationals have their 10 fingerprints taken and registered in the Visa Information System (VIS) at the moment of making their first visa-application. When entering into the Schengen area, the identity of the visa-holder is authenticated by verifying the match of 1, 2 or 4 fingerprints vs. the 10 fingerprints stored in the VIS. The VIS also contains a picture of the applicant, which appears on the visa-sticker, but is not used by the biometric matching system. A visa-holder can therefore not be searched in VIS on the basis of /her picture only.

Enrolment in EES

At border crossing point, if the traveller is not yet (first visit to the Schengen area) or no more (visit after the end of the data retention period) registered in the EES, the traveller needs to be "enrolled" in the system so that his/her identity is recorded and can serve as the reference for any further checks.

If the facial image will be used as biometric identifier (alone or in combination with fingerprints) pictures of all third-country nationals (both visa-exempt and visa-holders) visiting the Schengen area will be registered in EES.

If fingerprints are used as biometric identifier (alone or in combination with facial image) the fingerprints of visa-exempt third-country nationals will be registered in EES while for visa-required third country nationals the EES will rely on the fingerprints already registered in the VIS.

As the enrolment process happens at the border it needs to be fast. At the same time it should produce high quality results, as the enrolled biometrics will be used for all subsequent verifications and identifications.

Enrolment in RTP

When a third-country national applies for Registered Traveller status, the traveller needs to be "enrolled" in the RTP so that his/her identity is recorded and can serve as the reference for any further checks.

Verification at the border

During the retention period of the EES and RTP individual files, the identity of the third-country national is verified before any border crossing at entry and exit. The traveller's biometrics are compared with the biometrics stored in his/her individual file in the EES database and in the VIS database for the fingerprints of visa holders. For this operation, called a '*one-to-one verification*', the biometric identifier of the traveller is compared *only* with his/her own biometrics enrolled in his/her individual file in the database. This identity verification allows establishing a link between the individual and his/her individual file in the database.

The biometric identity verification is an operation that happens for each and every crossing of the EU external border. It needs to be quick and reliable.

Identification

A biometric identification is performed if the identity of an individual needs to be determined because his/her travel documents are not available, or appear to be counterfeited or do not necessarily belong to the individual. Such a biometric identification can take place either at second line border control⁶⁸ when the individual seeks to cross the border, or within the Schengen area in the case of an identity check. In these cases a sample of the biometric identifier from the individual is compared with each biometric record of the reference database to find out against which recorded identity a match is found. This operation is called the '*one-to-n (or one-to-all) identification*'.

The biometric identification would also be used if the *identification at the border (deduplication)* is implemented. In that case, for each third-country national whose claimed identity is not yet recorded in EES, the biometric identifier is compared with each biometric record of the reference database to confirm that the individual is not yet recorded. If this is confirmed, the individual file is created and the biometrics are recorded in the database. If the individual is already registered in the database, it is because:

- the individual is using the same identity in more than one travel document issued by one or several countries (bi-nationals); in this case, the different travel documents have to be linked to the same individual file;
- the individual already registered in the database has legally changed identity (e.g.: change of name after marriage); in this case, the new travel document with the new identity has to be linked to the existing individual file;
- the individual is using several identities.

The biometric identification is a complex operation as in essence the biometric sample is compared with all stored samples. When this operation is performed for inland checks or second line border control operations, the volume of requests remains low compared to the verifications and a response time expressed in minutes is deemed acceptable. These two factors (volume and response time) combined do not therefore have a significant impact on the processing capacity (and cost) of the biometric matching system sized for the frequent 1-to-1 verifications.

⁶⁸ 'Second line' border control means a further check which may be carried out in a special location away from the location at which all persons are checked (first line). See annex 5.

When systematic identification is required for first-line border checks, the response time needs to be brought down to a few seconds. The volume of identifications then also becomes of the same order of magnitude as the number of enrolments. This requires a significant increase of the processing capacity (and cost) of a biometric matching system sized only for 1-to-1 verifications.

5.3. Facilitation of border crossing

One of the main objectives of the system is to facilitate border crossings for regular travellers. The 2013 proposal suggests setting up an RTP programme for pre-vetted third country nationals. The technical study considered potential simplifications to this approach. The following options are considered:

- (a) RTP (2013 proposal),
- (b) RTP with on-line registration,
- (c) The use of process accelerators

(a) RTP (2013 proposal)

In this option the application process for registered traveller status is very similar to the visa application process. Applicants can submit their applications for RTP status in a consular post of any Member State. The traveller has to submit an application file, present the required supporting documents (regarding the purpose of the intended journeys, the sufficient means of subsistence, and the applicant's occupational or family status) and pay the fee. At first application, the traveller is required to appear in person for fingerprint enrolment, interview and check of the travel document. The whole process requires additional resources in consular posts and border crossing points for application collection, as well as in Member States' central administration for the pre-vetting and again in border posts for its completion. Although it is not inherent to the described process, the 2013 proposal provided that all registered traveller's identity and their biometrics would be stored in a database distinct from the EES database. The RTP database would also contain some of the data collected during the application process.

At the border crossing, the third country national who has acquired the Registered Traveller (RT) status would have the possibility, to use dedicated ABC gates, if available, or lanes dedicated to EU citizens. The identity of the RT is verified (biometric verification), the RT status is checked and the person is subject to the checks applicable according to the Schengen Borders Code (the compliance with the rules concerning the authorised stay is verified and the VIS, SIS, Interpol database and national database are queried). However, due to the pre-vetting done during the RTP application process, RTs benefit at entry from three derogations to the thorough checks (no thorough scrutiny of the travel document for signs of falsification or counterfeiting; no questions on the point of departure and the destination and on the purpose of intended stay; no questions on the means of subsistence).

The technical study, where this option is called Target Operational Model "M" (TOM M), considers that such a Registered Traveller Programme could interest 5 to 7 million third-country nationals.

(b) RTP with on-line registration

This option was identified in the Technical Study as a 'lighter' and less resource-intensive alternative for option (a). It assumes that the RTP applicant is already enrolled in EES and has at least one entry and exit record. This ensures that the biometric information of the traveller already exists as it has already been collected for the EES or VIS. Travellers would apply via a secured website dedicated for RT applications. All supporting documents for the request would be provided as scanned versions. Fees would be collected on line.

Once the application is lodged, the pre-vetting would be performed by the competent Member State indicated as the Schengen country of main destination. The same supporting documents have to be submitted to obtain the RT status as for option (a). The conclusion of the vetting process would be communicated to the requester by e-mail. The RT status would be activated once the traveller has met with a border guard at the first visit to the Member State having processed the application. This would allow a final check and the verification of original documents if required by the Member State that vetted the application.

At border crossing, the process is the same as for option (a).

Option (b), called in the technical study Target Operational Model "N" (TOM N), is only possible when EES and RTP are built as one single system. The advantage of this option is that it relies systematically on electronic communication, which could also make it a more attractive proposition for visa exempt regular travellers.

(c) The use of process accelerators

This third option takes as a starting point that border controls should be facilitated for the largest possible group of travellers. Both option (a) and (b) require active advance application to undergo a pre-vetting process in view of obtaining a 'status' that allows the RT to cross the borders on the basis of his/her authenticated identity. Option (c) is based on the idea that following a risk assessment using the information provided at the border crossing, and the responses from the different databases consulted (including EES) and the answers provided by the travellers through self-service systems, the border guard may decide to relieve the traveller from additional questions when a 'face to face' border check is not necessary. This option does not require the development of a specific IT system or of specific functionalities in EES.

A detailed example of a border crossing process using accelerators is provided in annex 8 (*'New Smart Border processes at border crossing points'*). It assumes that third-country nationals would scan their travel document (passport) in a self-service kiosk, enrol their biometrics (if not yet registered in EES) or have a biometric verification of their identity (if already registered in EES) and answer the questions that are part of the thorough checks but reformulated as a set of closed questions. The kiosk application would trigger all queries to databases (VIS, SIS, Interpol database, national databases). The border guard would see on his/her working screen the results of these queries, of the operations done by the traveller and of the former entry/exit records in EES. On the basis of his/her risk assessment the border guard would then decide, whilst respecting the conditions set in the Schengen Borders Code, what further detailed questions are required for this traveller. In case there is no need for further controls, the border guard can decide to let the traveller leave using an automatic e-Gate where the exit record will be created. This

last possibility shall only be granted when all the conditions of entry or exit foreseen under the Schengen Borders Code are met. If the traveller is not yet registered in EES, a verification of the biometrics and the travel document performed by the border guard is mandatory.

Option (c) relies on the "ease of use" of self-service kiosks by the "average" traveller and concentrates the border guard work on value-adding tasks. Considering the evolution of technology, the self-services kiosks could be complemented or eventually be replaced by mobile "app" solutions.

5.4. Retention time for the storage of data

The functioning of the Entry Exit System requires the registration of data concerning

- the identity of the third country national (first name(s), surname, date of birth, current nationality, gender),
- the biometrics of the third country national,
- the travel document used by the third country national (document number, document type, document country code and expiry date),
- the visa in the case of a visa-required third-country national (visa sticker number, visa expiry date, number of authorised entries, authorised period of stay),
- the cross border movements (entry/exit) of the third country national (date and time of entry, entry authorising authority, entry Border Crossing Point, date and time of exit, exit Border Crossing Point),
- and the stay changes (revised expiry data of the authorisation of stay, date of change of limit of stay, place of change of limit of stay, ground for change or revocation).

The identity (first name(s), surname, date of birth, current nationality and gender) of the third country national is copied from the travel document.

Data concerning the identity of the third country national and the travel document are used for identifying the traveller. Biometrics are used for establishing a link between the individual and the database record as well as for detecting identity fraud. The visa information, the entry/exit records and stay changes are used for the calculation of the authorised stay.

Compared with the 2013 proposals, the number of data elements to be recorded in the system has decreased as 10 elements such as the name at birth or the place of birth will not appear anymore in the revised proposal.

In application of the *privacy by design* principles and in accordance with 2012 Commission's proposals for Data Protection, the data set detailed above is the minimum strictly required for the proper functioning of the Entry Exit System. It is limited to the minimum amount of information necessary for the specified purposes of the processing.

To answer the question of how long data need to be retained for the correct functioning of the system the following options are considered:

- (a) An EES data retention period of 181 days (5 years for overstayers) and a RTP data retention period of 5 years (2013 proposal).

- (b) An EES data retention period of 181 days and reduction of the data retention period for RTP.
- (c) An extension of data retention periods.

In all three options the question arises of what shall be done with the data on overstayers that have not yet left the Schengen area at the end of the data retention period. The legal proposals will suggest that in such case the identity of overstayers is removed from EES and, following a national decision, can be included as an alert in SIS for refusal of entry or stay. This will guarantee that the persons concerned can still be identified at inland checks or at border controls under the strict data protection and retention rules applicable to SIS data. SIS being systematically consulted at visa issuance, overstayers cannot have new visas or cannot pass borders without being identified.

In all three options, the recorded data are automatically erased after the retention period has expired. Conditions for the possible advance deletion of data (e.g. in case the third-country national marries an EU citizen) are also defined.

(a) An EES data retention period of 181 days (5 years for overstayers) and a RTP data retention period of 5 years (2013 proposal)

Under the 2013 EES legislative proposal, the minimum period to be taken into account for retaining entry and exit records for the purpose of EES is 181 days because it makes it possible to calculate all short stays during a period of 180 days and to verify whether the maximum 90-day period of stay has not been exceeded⁶⁹.

In the case of an overstay, the proposed retention period is 5 years after the last day of authorised stay. This retention period ensures that data are kept long enough to support the identification and return process, while remaining proportionate by setting an upper limit.

For RTP data, the retention period is 5 years after the end of RT status. The period is determined in order to meet the goal of facilitated border crossings: by keeping data (including fingerprints) for five years the registered traveller does not need to provide fingerprints again at each yearly renewal.

(b) An EES data retention period of 181 days and reduction of the data retention period for RTP and in the case of overstay

A reduction of the data retention period can be considered for the RTP only as any reduction of the data retention period proposed in 2013 for the EES would result in the impossibility of controlling the respect of the rule concerning the maximum duration of stay in the Schengen area.

Moreover, by having EES data deleted after a short period of time any third country national who comes back to the Schengen area beyond that period will again need to be re-enrolled. This operation is time-consuming whatever the choice of biometrics and would slow down considerably the border crossing processes.

⁶⁹ In the 2013 EES legal proposal there are two data retention rules. First the entry/exit records are kept for a maximum duration of 181 days. Second the individual file with the entry/exit records will be retained for a maximum of 91 days after the last exit record, if there is no entry record within 90 days following the last exit record. The consequences of applying these two rules are that if a third country national enters again after 90 days, but before the expiry of his/her right to stay in the Schengen territory, the whole individual file would need to be created again, which is the most time-consuming operation

For RTP, a reduction of the data retention period would not affect the functioning of the system. The fact that in the 2013 proposals data are kept after the end of the RT status allows the reusing of information for a possible RT status renewal application. Considering that part of the data is unlikely to change (identity, biometrics), their retention simplifies the application process for the RT status renewal for both the traveller and the application collection process. Consequently, the retention period for RTP could be reduced without consequence on the functioning of the system.

However, a short EES data retention period has an impact on Registered Travellers as, independently of the RT status, the data deletion will require frequent re-enrolment in EES, an operation that would reduce the advantages of the RTP. As a minimum the data retention period of registered travellers' data in the EES would have to be the same as that of their registered traveller status.

(c) An extension of the data retention periods

In this option the view is taken that the data retention period should also take into account facilitation aspects for the traveller and operational aspects for the border guard.

For the border guard the systematic deletion of the EES record after 181 days removes any trace of the traveller's recent history of entries and exits from the Schengen area which is required for a risk analysis. It would be a regression of useful information compared to what the border guard currently uses: consulting stamps in a travel document gives in many cases information that stretches a period of several years. A longer data retention period is thus necessary to allow the border guard performing the necessary risk analysis requested by the Schengen Border Code before authorising a traveller entering the Schengen area.

The processing of visa application in consular posts requires also analysing the travel history of the applicant to assess the use of previous visas and the respect of the conditions of stay. The abandoning of passport stamping will be compensated by a consultation of the EES. The travel history available in the system should therefore cover a period of time which is sufficient for the purpose of visa issuance.

A longer data retention period will reduce the re-enrolment frequency and will be beneficial for all travellers as the average border crossing time will decrease as will do the waiting time at border crossing points. Even for a traveller entering only once in the Schengen area, the fact that other travellers being already registered in the EES will not have to re-enrol will reduce the waiting time at border.

A longer data retention period will also be necessary to allow for facilitation at border crossing by using process accelerators (as described under point 5.3.1 c)) and self-service systems. Facilitation is dependent of the data registered in the system. A short data retention period would reduce the group of travellers that can benefit of such facilitation and thereby undermine the stated objective of EES to facilitate border crossing.

When considering the length of the data retention period, it should be noted that a period of five years would be consistent with the data retention period in VIS. In EURODAC, data concerning asylum seekers are stored for 10 years. Entry Exit systems operated by third countries usually involve a (far) longer retention period.

Extending the proposed data retention period for EES records to 5 years would correspond to the average duration of the validity of the passports used by third country nationals. As these passports have a maximum validity of 10 years the border guard views on average 5 years of travel history (brand-new passports having zero years of history and passports at the limit of their validity having 10 years history).

The data retention period of 5 years would also correspond to the maximum length of validity of multiple-entry visas (MEV). This retention period is thus required for the examination of visa applications when the "visa history" and the lawful use of previous visas by the applicant are checked.

A five year data retention period corresponds to the maximum duration of the RT status as foreseen in the 2013 RTP proposal. This 2013 proposal retained also a five year data storage period as it would be in line with the issuance of a multiple-entry visa for trusted travellers (maximum period 5 years) whose data is kept in the VIS for 5 years.

The data retention period for RTP would remain, like in option (a), equal to 5 years.

5.5. Access for law enforcement purposes

The 2013 proposals suggest that the option of access of law enforcement authorities to the data contained in the system will be evaluated two years after the entering into operation of the system. The following options are considered:

- (a) Evaluation after two years (2013 proposal)
- (b) Law Enforcement Access as secondary objective from the start
- (c) No Law Enforcement Access.

(a) Evaluation after two years (2013 proposal)

The Impact Assessment of 2013 recognized that EES data can be used by law enforcement authorities in the fight against terrorism and other serious criminal offences in specific cases both:

- as an identity verification tool and
- as a criminal intelligence tool (for investigations and prosecutions of terrorism and serious crime to construct evidence by tracking the travel routes of suspects).

The use of such data for identity verification would reduce the identification and verification gap concerning third country nationals who are not in the VIS.

However, when the proposal was issued in February 2013, based on an Impact Assessment developed before law enforcement authorities had the right of accessing VIS data, no evaluation could be made as to whether this access was really useful and proportionate. The proposal therefore contained the provision that during the first two years of operation of the Entry Exit System there would be no access to data for law enforcement authorities. After this period, an evaluation of the use of VIS data for law enforcement purposes and of the opportunity of granting such an access to EES data would take place. This evaluation would inform the assessment of the proportionality and

need of access to EES data for law enforcement authorities. Under this option, RTP is excluded from any possibility of data access for law enforcement purposes.

(b) Law Enforcement Access as a secondary purpose from the start

Based on the experience of operating VIS, the criteria and mechanisms provided for access to Member States' law enforcement authorities and Europol to Eurodac⁷⁰ and the actual use⁷¹ made by such law enforcement authorities of the right to access these databases under specific and strict conditions, this option proposes to grant access to EES data to law enforcement authorities *from the start*.

EES contains reliable data on entry and exit dates of all third country nationals at the external borders of the Schengen area. VIS contains the data on the visa application and on the visa-holder but does not record dates and places of entry and exit of the Schengen area. It would therefore meet the need of Member States' law enforcement authorities and Europol to complement their existing criminal intelligence sources with entry and exit dates and locations in duly justified cases. Like in option (a), RTP is excluded from the possibility of data access for law enforcement purpose.

Under this option EES data could be accessed for both identification and criminal intelligence purposes. For identification, a biometric sample would be compared with all biometric records of the database. For criminal intelligence, the information (travel history) concerning one or several individual(s) already identified would be retrieved.

To mitigate the data protection implications (see Annex 13 – Impact Assessment on Fundamental Rights, section 13.4), access for law enforcement purposes should be accompanied by strict conditions which could be modeled on the Eurodac recast Regulation and the VIS Decision:

- It must be necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences, which means there is an overriding public security concern which makes the searching of the database proportionate;
- It must be necessary in a specific case;
- There are reasonable grounds to consider that consultation of the EES data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question;
- If EES is accessed for identification purpose, there is a requirement for prior consultation of national criminal fingerprint databases and other Member States' criminal fingerprint databases via the Prüm system (Police co-operation

⁷⁰ Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. OJ L 180, 29.6.2013, p. 1.

⁷¹ On the basis of the access to VIS data for law enforcement purpose for the period January-August/2015, it can be extrapolated that around 16.500 searches would be launched in VIS for law enforcement purpose on a twelve months period. This number is calculated considering the actual use of VIS before the end of its roll out which occurred in December 2015.

mechanism for exchanging information on DNA, fingerprints and vehicle registration data);

- If EES is accessed for criminal intelligence purposes, a verifying authority verifies, in a functionally independent manner, in each case if the strict conditions for consulting the EES are fulfilled.

From a law enforcement point of view, and especially for the use of this data as a criminal intelligence tool, a travel record of a crime suspect would need to cover a commensurate period of retention, possibly with several entries and exit. In case the purpose of the system would be extended to include the fight against terrorism and serious crime, a retention period of 181 days would be too short. In order to construct in meaningful way evidence in criminal cases by analysing data on travel routes, law enforcement authorities have to be able to track the travel routes back for a period of several years⁷².

Consequently the retention period in relation to this policy option would be five years as this duration for keeping data presents a commensurate period of retention and is also one of the retention time options for immigration purposes. The impact assessment conducted for the 2013 proposal also considered a retention period of 5 years as necessary in case access by law enforcement authorities would be granted⁷³.

(c) No Law Enforcement Access

This option argues that EES is to be exclusively used as a border management tool.

⁷² E.g.: in the case of traffic of human being, a data retention limited at 181 days would result in the retention of information concerning the victims becoming overstayers while information concerning the criminals crossing regularly the borders would be erased after 181 days.

⁷³ SWD(2013) 47 final. See section 5.3 and 5.4

6. ANALYSIS OF IMPACTS

This section describes - where relevant - the anticipated impacts of the introduction of an Entry Exit System, in combination (or not) with a RTP. The various policy options described in section 5 do not fundamentally change the nature of the expected impact, but they may affect their magnitude.

6.1. Social impacts

6.1.1. *Impact on EU citizens*

The implementation of Smart Borders does not directly affect border crossings by EU citizens for any of the envisaged options. However, the policy options having an impact on the time spent at border by third country nationals could also have an indirect impact on EU citizens. Regarding particularly option 5.4(a) and 5.4(b) (facilitation schemes using a specific RTP application) the concern was raised whether the third country nationals would create queues when using the same lanes as the EU citizens for crossing the borders. This would not be the case given the limited expected number of registered travellers vs the number of EU citizens.

To be weighed against this very limited impact on EU travellers at borders is the contribution that the system will bring to the fight against irregular migration and the level of security of EU border management. This has an indirect, but arguably very positive effect on EU citizens.

If the access to EES data for law enforcement purpose is granted, this will further contribute to increasing the security of EU citizens when being in the Schengen area.

Contributions of EU citizens to the Public Consultation are summarised in annex 2. The questionnaire was divided in chapters corresponding to sets of options analysed in this impact assessment (excepted the 'Architecture' option). A majority of participants has indicated preferences for a biometric identifier combining fingerprints and facial image as well as for facilitation relying on self-service systems. The answers to questions concerning data retention and the access for law enforcement purpose are divided and do not make it possible to identify a trend in favour of or against any option.

6.1.2. *Impact on third country nationals*

The Entry Exit System will have a positive impact on the travel experience of third country nationals if one of the options for facilitation at border crossing is implemented. With options 5.3(a) and 5.3(b), a registered traveller programme would be implemented allowing pre-vetted third country nationals to benefit from extended facilitation at border. With option 5.3(c), the use of process accelerators for all third country nationals would allow most of these travellers to benefit from more limited facilitation at border. In both cases, the average waiting time for third country nationals would be reduced.

The impact of the Entry Exit System could be negative on the duration of the border crossing of third country nationals, as they would need to be enrolled at entry if they are not yet (first visit) or no more (after the end of the data retention period) registered into the system. In these cases, the registration process requires the enrolment of the biometric identifier(s) which needs time. However, this negative impact can be reduced by selecting a biometric identifier that can be enrolled rapidly such as option 5.2(c) (facial

image only). Having a longer data retention period (option 5.4(c) - five years) would also reduce this negative impact as it would allow a less frequent re-enrolment of the travellers.

The Entry Exit System will have an impact on the privacy and protection of personal data of third-country nationals. While currently personal data are only shown to the border guard, in the future these data will be recorded in a database. In addition biometrics are taken and stored in that database. The impact is the most substantial for visa-exempt third country nationals for whom no personal data is recorded up to now. On the other hand, currently, any person looking in the travel document of a third country national can see the stamps corresponding to the crossings of the external border of the Schengen area. The EES will limit the access to this information to authorised officials only.

The abandoning of passport stamping will prevent the travellers verifying their compliance with the rule of no more than 90 days of authorised stay in any 180-day period. This information is important both for third country nationals already in the Schengen area having to know about the end of their authorised stay and for third country nationals planning their travel to the Schengen area. It is foreseen that this information will be provided on request at entry and will be made available through a dedicated secure web service accessible by the travellers.

A very limited number (nine) of third country nationals participated in the Public Consultation. Most of them expressed their positive views on the use of one of the proposed solutions comprising the biometric identifiers. The number of respondents and the distribution of their answers do not allow concluding on their preferred biometrics.

The personal interest in RTP for border crossing and/or the use of self-service kiosks was confirmed by the majority of participants.

The outcomes of the far more substantial survey performed by the Fundamental Rights Agency in the framework of the Pilot present important elements concerning travellers' views and expectations of smart borders (see annex 15).

The results show that most respondents are comfortable with providing biometrics when crossing borders. Most respondents do not perceive biometric data collection as intrusive on their privacy. Trust in the reliability of biometric technologies is also high.

A key concern of respondents is however what happens if something goes wrong and the system does not function as expected. More than half of the respondents believe that they would not be able or do not know if they will be able to cross the border in case the technology does not work properly. Similar concerns emerged in relation to the right to correct wrong data. Half of the respondents believe that in case of an error in their personal data, it may be difficult to have this corrected.

The report shows also that third-country national travellers take data protection seriously and more than 80% consider it important to be informed on the purpose of collecting and processing their personal data.

There is a widely held view that automated systems could cause less discrimination compared to checks carried out in person by border guards. This might be based on the assumption that machines entail a lower risk of discriminatory profiling compared to checks by border guards.

Finally, most respondents believe that only adults (i.e. 18 years of age onwards) should be allowed to go through biometric checks.

6.1.3. *Impact on local border traffic*

The establishment of the Entry Exit System would not modify any of the aspects related to Local Border Traffic which is an exception to the Schengen Convention⁷⁴. This means that third country nationals with a local border traffic permit will not be submitted to the Smart Borders provisions for crossing the border between their country of residence and the specific country in the Schengen area which issued this permit.

6.1.4. *Impact on Protection of Personal Data*

An Entry Exit System would, due to the personal data involved, in particular have an impact on the right to the protection of personal data. The right to protection of personal data is established by Article 8 of the Charter and Article 16 TFEU and in Article 8 of the ECHR. As underlined by the Court of Justice of the EU⁷⁵, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society⁷⁶. Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter. This is reflected by Article 1(1) of Directive 95/46/EC which provides that Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.

Right to personal data protection

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the Regulation (EC) 45/2001 would apply to the processing of personal data carried out for the purpose of an EES respectively by the Member States and by the EU institutions, bodies and agencies involved.

According to the Commission Communication of July 2010 on Information management⁷⁷, data protection rules should be embedded in any new instruments relying on the use of information technology. This implies the inclusion of appropriate provisions limiting data processing to what is necessary for the specific purpose of that instrument and granting data access only to those entities that ‘need to know.’ It also implies the choice of appropriate and limited data retention periods depending solely on

⁷⁴ Regulation (EC) No 1931/2006. Third country nationals living in a border region can apply for and travel on the basis of a permit (called LBT) which simplifies border crossing, rather than using a short stay visa. With this LBT they may travel up to 30 km (or even up to 50 km) within the neighbouring Schengen country and stay in that area up to a maximum 3 months. The precise duration of the stay is determined in the Local Border Traffic agreement between the Member State and the neighbouring country. This permit and the conditions to be fulfilled in Local Border Traffic Agreements are defined in the cited Regulation. The local border traffic regime derogates from the general rules governing the border controls on persons crossing the external borders of the Member States of the EU which are set out in the Schengen Borders Code (Article 35 of the SBC). In 2015, eight Schengen countries (Spain, Hungary, Latvia, Norway, Poland, Romania, Croatia and Slovakia) issue LBT permits with at least one non-EU neighbouring country. The total number of LBT permits issued since 2009 is less than 500.000 at the end of 2014, accounting for an estimated 7.5 to 10 million border crossings per year.

⁷⁵ Court of Justice of the EU, judgment of 9.11.2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-0000.

⁷⁶ In line with Article 52(1) of the Charter, limitations may be imposed on the exercise of the right to data protection as long as the limitations are provided for by law, respect the essence of the right and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

⁷⁷ COM(2010) 385 final

the objectives of the instrument and the adoption of mechanisms ensuring an accurate risk management and effective protection of data subjects' rights.

The authorities who should have access to the Entry Exit System have to be designated for a specific purpose. Therefore, access to data should be reserved exclusively to duly authorised staff of the authorities of each Member State who are competent for the specific purposes of the Entry Exit System and limited to the extent the data are required for the performance of the tasks in accordance with these purposes.

All safeguards and mechanisms should be in place for the effective protection of the fundamental rights of travellers particularly the protection of their private life and personal data. Third-country nationals must be made aware of these rights. A number of safeguards would be integral to the core system:

- If there were errors on the identity checks of passengers, facilities would need to be made available for carrying out manual checks and for amending the data on entry and exit at all border crossing points. Regarding such facilities, the Schengen Borders Code currently requires that thorough second line checks for third-country nationals shall be carried out in a private area where the facilities exist and if requested by the third-country national.
- Individuals should have the right to access information held on them and to challenge and correct it, if the processing of this data does not comply with the provisions of Directive 95/46 and Regulation 45/2001, in particular because of the incomplete or inaccurate nature of the data. In case the information is held by law enforcement authorities following access to the EES, such rights shall be granted under Framework Decision 2008/977.
- Individuals should have the right to lodge a complaint with a data protection authority regarding the processing of their personal data and they should also have the right to effective administrative and judicial remedies (Article 47 of the Charter).
- Guarantees ensuring an effective remedy (Article 47 of the Charter) for third-country nationals that would enable them to challenge a notification of an overstay by the entry/exit system must be in place, for example in situations when they were forced to overstay, particularly if it appears that they overstayed for a valid reason (e.g. hospitalisation, change in travel arrangements), when errors were made in recording dates of entry or exit or to show that they have a legal right to stay (e.g. based on a new visa, marriage to an EU citizen, application for asylum, refugee status). Given the large numbers of new travellers affected and the new requirement for them to provide information, safeguards for data protection and mechanisms for ensuring an effective remedy would need to be visible and evident.
- In case the Entry Exit System notifies an overstay, this indication should not lead automatically to detention, removal or a sanction for the third-country national. Third-country nationals should have access to effective remedies in such proceedings in order to protect the right to liberty and security (Art. 6 of the Charter), right to asylum (Art. 18 of the Charter), respect for family life (Art. 7 of the Charter) and the obligation of non-refoulement (Art. 19(2) of the Charter). A decision to detain, remove or sanction a third-country national shall not be based solely on a notification of overstay by the entry/exit system. In addition the safeguards of Directive 2008/115/EC have to be respected.

- The supervision of all data processing activities should be carried out by Member States data protection authorities and the European Data Protection Supervisor which should be conferred with all the necessary powers to intervene and enforce compliance with data protection rules.
- The measures protecting rights of travellers, including right to an effective remedy, must also take into account the privileged position of non-EU family members of EU citizens whose right to enter and to stay depend on the right of the respective EU citizen in accordance with Directive [2004/38/EC](#).

The inclusion of these safeguards in the proposal will bring an adequate answer to an issue that was also identified in the FRA survey in the framework of the Pilot: the need to allow the immediate correction of obvious errors or omissions in the EES records, and to ensure that control mechanisms are in place to detect and report on these errors and omissions.

The conception of the Entry Exit System is based on the *privacy by design* principles⁷⁸:

- The approach is characterised by proactive rather than reactive measures and begins with an explicit recognition of the value and benefits of proactively adopting strong privacy practices, early and consistently;
- The privacy is built into the system, by default: specified purposes are clear, limited and relevant to the circumstances (purpose specification); the collection of personal information is limited to that which is necessary for the specified purposes (collection limitation); the collection of personally identifiable information should be kept to a strict minimum (data minimisation); the use, retention, and disclosure of personal information shall be limited to the relevant purposes (use, retention and disclosure limitation.);
- Privacy is embedded into the design and architecture of IT systems and business practices;
- Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. It avoids the pretence of false dichotomies, such as privacy versus security, demonstrating that it is possible, and far more desirable, to have both;
- Privacy must be continuously protected across the entire domain and throughout the life-cycle of the data in question: the security of personal information has to be ensured; applied security standards must assure the confidentiality, integrity and availability of personal data throughout its lifecycle including, inter alia, methods of secure destruction, appropriate encryption, and strong access control and logging methods;
- Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification: information about the policies and practices relating to the management of personal information shall be made readily available to individuals; complaint and redress mechanisms should be established, and information communicated about them to individuals;

⁷⁸ Privacy by Design, The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices, Ann Cavoukian, Ph.D., Information & Privacy Commissioner, Ontario, Canada

- Respect for User Privacy implies: accuracy (personal information shall be as accurate, complete, and up-to-date as is necessary to fulfil the specified purposes), access (individuals shall be provided access to their personal information and informed of its uses and disclosures; individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate), compliance (complaint and redress mechanisms must be established and information about them has to be communicated to the public, including how to access the next level of appeal).

An Impact Assessment on Fundamental Rights is included as annex 13.

6.1.5. Impact on other Fundamental Rights

Other potentially affected fundamental rights enshrined in the Charter are the following: the right to dignity (Article 1); the prohibition of slavery and force labour (Article 5); the right to liberty and security (Article 6); the prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21).

The right to dignity (Article 1) can be affected by the fact that third country nationals intending to cross the external border of the Schengen area will have to give their biometrics for enrolment in EES or for verification of their identity. This potential impact on dignity has been addressed by the Fundamental Right Agency survey.

Respondents were asked whether they feel comfortable with the use of the following biometric identifiers when crossing the border: fingerprints, iris-scan and facial image. Generally, third-country nationals travelling to the EU tend to feel comfortable with providing biometric data when crossing the border. For all three types of biometric identifiers (fingerprints, iris-scan and facial image) most respondents feel very comfortable. However, there are important differences: people feel more comfortable with providing fingerprints or facial image when crossing the border compared to having their iris scanned.

In the questionnaire, violation of human dignity has been operationalised as ‘humiliating behaviour’. In human rights law there is an intimate connection between the notion of human dignity and the notion of humiliation, and humiliation can be explained in terms of (violation of) human dignity. Respondents were asked whether they believed that giving their biometrics might be humiliating. Although the majority of all respondents do not feel that providing biometrics in the context of border control might be humiliating, more respondents find providing biometrics more humiliating compared to a check conducted by a border guard.

Provisions have to be foreseen for the cases where biometric enrolment is impossible or cannot be performed in the defined conditions.

The prohibition of slavery and force labour (Article 5) as well as the right to liberty and security (Article 6) can be positively affected by the implementation of an Entry Exit System. A better and more accurate identification (through biometrics) of third country national crossing the external border of the Schengen area will help detecting identity fraud, human being trafficking (including minors) and cross border criminality and thus will contribute to improving the security of the citizens present in the Schengen area.

The use of IT systems, ABC gates and self-service kiosks at border controls could be perceived as causing less discrimination than checks performed by human beings. The prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21) could consequently be positively affected by the revised proposals. This question has been addressed by the Fundamental Right Agency survey. The results show that there is a widely held view that automated systems could cause less discrimination – for example on the basis of race or ethnicity – as compared to checks carried out in person by border guards.

6.2. Economic impacts

6.2.1. Impact on tourism

During the consultations, the question was raised whether the Smart Borders proposal might have a negative impact on tourism as a more complex border crossing process may act as a deterrent to visit Schengen countries in comparison to simplification of visa issuing procedures or exemption from the visa requirement, which normally leads to a significant increase in the number of travellers during subsequent years. However, with the Entry Exit System the border crossing process remains in essence the same, with the main difference that passport data that were previously only shown to the border guard are now also recorded in a database. As a result, an Entry Exit System is not expected to have an impact on tourism.

6.2.2. Impact on airports, seaports and carriers

On the basis of Article 26 of the Schengen Convention⁷⁹, air and sea carriers need to check that third country nationals that are carried to the Schengen border are in possession of the travel documents required for entry. In case of refusal of entry, the carrier which brought them to the external border by air, sea or land shall be obliged immediately to assume responsibility for them again. At the request of the border surveillance authorities, the carrier shall be obliged to return the aliens to the third State from which they were transported and/or to the third State which issued the travel document on which they travelled or to any other third State to which they are certain to be admitted. In case the traveller does not have valid travel documents, the carrier is liable for a penalty that can go up to EUR 5000 per traveller.

Carriers are strictly speaking only bound to check that the travellers carry a valid passport and a valid visa. In practice carriers often also verify whether the traveller has still a sufficient duration of authorised stay in order not to be refused entry into the Schengen area.

Currently, air and sea carriers rely on the entry and exit stamps in passports and on whether or not the visa is stamped. To allow carriers to meet their obligations in a situation where passports will no longer be stamped, the Entry Exit System will include the functionality of a specific web service that will answer the question whether the "traveller is eligible for transportation until destination". Access to this secured web service will be granted to registered users only. In this way the Entry Exit System will

⁷⁹ "The carrier shall be obliged to take all the necessary measures to ensure that an alien carried by air or sea is in possession of the travel documents required for entry into the territories of the Contracting Parties"

have a positive effect for carriers as it facilitates the implementation of their legal obligation under article 26 of the Schengen Convention.

The changes to the border crossing process could have a negative impact on airport operators in case the time taken for for third country nationals to cross the border would become significantly longer. In that case the number of travellers queuing at the border could require the allocation of additional space which is scarce in busy airports and reduces the revenue from airport shops as travellers have less free time in the airport. A waiting time increase for border crossing in airports would have also consequences for travellers having a connecting flight and for airlines operating these flights.

In seaports where ferries or cruise ships are landing, each boat arrival corresponds to a very large number of travellers crossing the border. For ports where international ferry connections are landing, a longer waiting time would create space issues. A waiting time increase at border would decrease the cruise ship operator interest for stops in EU seaports.

As explained under point 5.1 (Description of the options), these potential negative impacts can be reduced if not avoided using the appropriate biometric identifier, extending the data retention period and implementing facilitation.

Eleven carriers and transport infrastructure operators or representatives participated in the Public Consultation. Seven respondents supported the necessity to use biometric data, with a clear preference for the use of facial image (FI) alone or in combination with fingerprints (FP). The use of the combination of FI and FP was considered as more secure, whereas FI is considered faster and easier by most of the respondents. Among those who rejected biometric identifiers in several cases the arguments were of a practical/operational nature (e.g. buses are not duly equipped to perform such verifications).

Ten out of eleven participants supported border crossing facilitation. Both RTP and self-service kiosks are perceived positively and the better speed for border crossing is mentioned by most of the respondents. These participants expressed also a strong support for a longer data retention period.

When asked about the consequences of the abolition of the stamping of passports of the non-EU citizens, a web service enabling them to verify if a single entry visa has not been used was confirmed by six participants as a necessary and sufficient solution. Some participants who replied negatively explained that in their activities they were not concerned by checking the documents. A cruise operator highlighted the importance of the information concerning the time their passengers can stay in the Schengen area.

6.2.3. Impact on retail activities close to border crossing points

At land borders, a non-negligible part of border crossings is due to travellers entering the EU for shopping purposes. This is also the case for a limited number of seaports and airports. An increase of the waiting time at the border would have direct consequences on the commercial activities depending of these travellers.

This negative impact can be reduced if not avoided using the appropriate biometric identifier, extending the data retention period and implementing facilitation.

6.2.4. Impact on the informal labour market

The Entry Exit System will provide the means for identifying overstayers. It is expected that this will have a preventive effect on overstaying, and will boost the effectiveness of the EU Return Policy. As a logical result the number of overstayers in the Schengen area is expected to reduce and so reduce one of the sources that fuel the informal labour market. It is very difficult to give precise projections on the expected reduction of the number of overstayers, as this is dependent on many factors. It is even more difficult to assess the impact this will have on the informal labour market, and the economic development of the EU as a whole. However, it seems safe to assume that one of the impacts of the introduction of an Entry Exit System will be that the supply of informal labour in the EU will decrease.

6.3. Impacts on SMEs

The Entry Exit System has as such no impact on Small and Medium Enterprises (beyond what is explained in section 6.2.3 Impact on retail activities close to border crossing points). The EES does not modify procedures or formalities SME's have to observe.

6.4. Impacts on Public Services

6.4.1. Impact on border control

The Entry Exit System has a significant and positive impact on the way border guards perform their checks. The eu-LISA Pilot has reported very positive experiences from border guards, regardless of the test cases considered.

Border guards (as well as consular officials) are relieved from the manual reading of entry and exit stamps and the calculation of the authorised duration of stay, as these tasks are performed automatically by the system. Any of the facilitation options (options 5.3 (a), (b) or (c)) will contribute to giving border guards more time and better tools to assess the potentially *non bona fide* travellers. This shift is maximised with option 5.3 (c) (use of process accelerators) as the repetitive actions of reading travel documents and verifying or enrolling biometrics are performed by the travellers using self-service systems for their pre-registration or pre-border checks while human intelligence can focus on the assessment of the traveller.

The positive impact on border guards assumes that border control tools are user-friendly and reliable, that the national border control application integrates relevant summary information on one screen for the border guard and that the central smart borders system has a very high availability and quick response time in all circumstances.

6.4.2. Impact on migration management

The Entry Exit System has a significant and positive impact on migration management. Currently the control of authorised period of stay (90 days in any 180 day period), cannot be done systematically in the absence of a central repository of in- and outgoing movements of the Schengen area. The Entry Exit System, independently of any of the options chosen, will provide the means for an effective enforcement of this long-established rule.

EES provides the means for identifying overstayers. The identity and facial image of overstayers will be known. Countries that already have an entry exit system in place

reported that these systems allow detecting overstayers as well as deterring the entry of persons who are likely to overstay⁸⁰.

EES will also allow the identification of apprehended irregular migrants without identity documents who legally arrived in the Schengen zone.

6.4.3. Impact on Law Enforcement Authorities

The Entry Exit System will have a positive impact on law enforcement authorities as it would provide unique information that could be used as a criminal intelligence tool. EES entry and exit records could be useful to exclude or maintain suspicions on persons known to law enforcement authorities on the basis of their presence in the Schengen area. It could allow re-constructing travel routes of suspected persons, known criminals/terrorists, but also victims. It could verify the concurrent presence of persons suspected to act jointly. To maximise the benefit of EES as a criminal intelligence tool, the data retention period should be sufficiently long. In this respect option 5.4(b) (data retention period of 5 years) would be the preferred option. Additionally, access to law enforcement authorities should be given from the start (option 5.5(b)) so that the positive impact of using EES data as a criminal intelligence tool will be effective as soon as possible.

EES has a second positive impact on law enforcement authorities as it would provide an additional source of criminal identification. Data enrolled in the Entry Exit System would allow the identification of suspects and known criminals on the basis of photographic material (pictures, videos) or on the basis of latent fingerprints found on a crime scene. This positive impact would be maximised under option 5.2(b) (fingerprints and facial image combined).

To mitigate the data protection implications, access for law enforcement purposes will be subject to the fulfilment of strict conditions as described under point 5.5.1 (b).

6.5. Impact on International Relations

The Entry Exit System will affect all third country nationals, and will thereby become a very visible feature of human mobility between all third countries and the EU. The EU EES will not be unique, as a substantial and increasing number of third countries have already invested in similar systems or intend to do so in the coming years. As a matter of fact, today EU citizens are fingerprinted or photographed and/or electronically registered when traveling to the USA, Japan, Canada, China, Australia, Ghana, Kenya, Jordan, Saudi Arabia and many more countries.

This being the case, it may still be expected that authorities of some visa-exempt countries will raise objections if their citizens would be fingerprinted at first entry into the Schengen area. It should therefore be explained through diplomatic channels and through tailor made information campaigns (as was done for the introduction of the VIS) that the establishment of the EES is part of a legitimate effort to strengthen the border management of the EU which is not targeting any country in specific. Pressure by some third countries aiming at negotiating exemptions from the system should be anticipated.

⁸⁰ E.g.: The Australian Government calculates non-return rates using an entry exit system (Movements Reconstruction database). These non-return rates are used as an indicator of Visitor visa compliance, and may be considered by decision-makers when assessing visa applications.

The proper functioning of the EES for all visa-free travellers will require the adjustment of the existing bilateral visa waiver agreements as explained at point 2.5. Major objections are not expected from the vast majority of third countries, as the proposed touring visa would provide a more adequate and legally clear solution for stays longer than 90 days in any 180-day period than the current "extension" of stays allowed by Article 20(2) of the Schengen Convention.

7. COMPARISON OF OPTIONS

Section 6 "Analysis of Impacts" assessed the broad impacts (like social impacts per affected stakeholder group, economic impacts, impacts on SME's, etc..) that result from the implementation of the Entry Exit System, regardless of the options chosen as this only affects the *magnitude* of the impact in some cases.

In this section the **effectiveness and efficiency** of each individual policy option (always referenced as (a), (b) and (c) when there are three) are compared for each of the five areas (architecture, biometrics, facilitation, data retention and law enforcement access) using the following model.

		Option (a)	Option (b)
Objectives	Better border management and facilitation		
	Overstayers: identifying at the border		
	Idem: inland identification.		
	Use as criminal intelligence tool		
	Use as criminal identification tool		
Impact on	Duration of border crossing		
	Travel experience of third country nationals		
	Border guard's workload		
	Fundamental Rights		
	Cost/benefit efficiency.		

The first part labelled "Objectives" and the second part "Impact on", both compare the **effectiveness** of the options. The last line "Cost/benefit efficiency" compares their efficiency.

The part marked "Objectives" links the options with the three general policy objectives of the Entry Exit System (see section 4.1). Therefore the comparison will assess to which extent each option allows:

- To improve the management of external borders expressed in the table as "Better border management and facilitation" for both border guards and travellers.
- To reduce irregular migration by addressing the phenomenon of overstaying, which the system can achieve by supporting identification of overstayers at the border and/or inland identification.
- To contribute to the fight against terrorism and serious crime by having the possibility to use the Entry Exit System as a criminal intelligence and/or criminal identity tool.

The second part of the table labelled "Impact on" looks at the criteria which differentiate the magnitude of the impacts described in section 6 "Analysis of impacts". These criteria are the impact on Fundamental Rights and on operational criteria:

- duration of border crossing,
- travel experience of third country nationals visiting the Schengen area. This refers to the possibility an option offers in terms of making the border crossing easier for *bona fide* travellers,
- border guard's workload.

The last line of the table compares the **efficiency** of the options using the cost/benefit ratio as the criterion.

For the purpose of the evaluation, the same scale is used as in the 2013 IA:

-√√√√	Highest negative impact/cost
-√√√	Significant negative impact/cost
-√√	Medium negative impact/cost
-√	Small negative impact/cost
0	No impact
+√	Small positive impact/savings
+√√	Medium positive impact/savings
+√√√	Very significant positive impact/savings
+√√√√	Highest positive impact/savings

7.1. Comparison in terms of effectiveness, fundamental rights, efficiency and coherence

7.1.1. *Architecture*

The following table provides an overview of the two options, all other options being assumed identical (same biometrics, data retention period, etc.), compared with the current situation without any new system.

		Option (a) EES and RTP as separate systems	Option (b) EES and RTP as one system
Objectives	Better border management and facilitation	All objectives can be met in either option	
	Overstayers: identifying at the border		
	Idem: inland identification.		
	Use as criminal intelligence tool		
	Use as criminal identification tool		
Impact on	Duration of border crossing	-√ to 0 as queries need to be directed to both systems and the answers combined	+√ as queries are handled faster
	Travel experience of third country nationals	Both options can deliver the same positive result	
	Border guard's workload	-√ to 0 according to the level of automation: a query needs to be sent from EES to VIS and to RTP	0 or +√ according to the level of automation: EES/RTP triggers query of VIS.

	Fundamental Rights	-√√ to -√ as personal information is stored twice	From -√
	Cost/benefit efficiency.	- √√√√	- √√√ Least expensive option.

Effectiveness. As explained in section 5.1 option (a) (Separate EES and RTP systems) and option (b) (One single EES/RTP system) are both capable of achieving the set objectives. However, option (b) does present an important advantage. EES and RTP developed as a single system will decrease the impact on data privacy as data concerning identity and travel documents as well as biometric identifiers will be registered only once and used for both EES and RTP functionalities, instead of being registered twice in two different IT systems;

In addition, if interoperability is established at the central level between EES/RTP and VIS this will:

- have a positive impact on border crossing time as some queries will be managed centrally without transiting through the national systems and the border crossing point;
- reduce the border guard's workload as the system will query automatically the VIS without requiring a specific intervention of the border guard.

Fundamental rights. While option (a) would require the duplication of all Registered Travellers personal data in EES, option (b) will allow the same records to be used for both RTP and EES functionalities. This corresponds to the data collection limitation and data minimisation principles detailed at point 6.1.4. This positive impact would be further reinforced if interoperability would be established between the EES/RTP and the VIS. This interoperability would make it possible to go further in the data collection limitation⁸¹ and the data minimisation⁸² (see the 'privacy by design principles' at point 6.1.4 'Impact on protection of personal data') due to the fact that the fingerprints of the visa holder travellers already registered in VIS will be used by EES/RTP avoiding an enrolment of the same biometric identifiers in both systems. The interoperability will also reduce the amount of data circulating on the communication networks and transiting through national systems as the queries done on behalf of the user and the corresponding answers (mostly limited to 'HIT'/'NO HIT' or 'YES'/'NO') will transit through a direct communication channel ensuring interoperability between the systems.

Efficiency. The cost analysis performed in the Technical Study has concluded that there would be a significant cost advantage in developing one single system rather than two. The cost of development would be €42,8 million lower (€49,4 million over 4 years⁸³ minus €6,57 million of one year of operations) and the recurrent yearly operations cost would be €6.57 million lower. The difference mainly stems from the synergy of similar functionalities between EES and RTP and the fact of having one single network for EES and RTP rather than two dedicated networks.

Coherence. The 2013 proposal to build EES and RTP separately was coherent with the previously made choices concerning other large scale IT systems (SIS II, VIS). The

⁸¹ The collection of personal information is limited to that which is necessary for the specified purposes.

⁸² The collection of personally identifiable information should be kept to a strict minimum.

⁸³ Pages 8 and 9 of the Technical Study on Smart Borders – Cost Analysis. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_study_en.pdf

choice for this option was furthermore based on a study⁸⁴ done in 2008 but where RTP was assumed to apply both on EU citizens and on pre-vetted third country nationals. Registration in RTP was seen as a condition for using e-Gates at that moment of the study. In the meantime this assumption was discarded as all EU citizens with an electronic passport and beyond an age or size limit can use e-Gates. Building one single system is coherent with this development and fits best with the objectives of the current proposal.

Preferred option. Option (b) is the preferred option. With this conclusion RTP functionalities are made part of EES. The comparison of options in section 0 concludes as preferred solution having no EU RTP. The additional element is that there is no need of EU RTP functionalities. At the same time it de facto confirms that there would be only a single system. Interoperability with VIS will need to be ensured.

7.1.2. Biometrics

Overview of the options

The table in annex 7 makes a comparison of the operational aspects of the various biometric identifiers. What this table shows is:

- Enrolment is the least time-consuming for the facial image alone. The more fingerprints are enrolled the more time-consuming and difficult this operation becomes.
- Verification requires only one biometric identifier: either facial image or iris or minimum one fingerprint meets the purpose.
- Identification for inland control can be done with facial image alone (provided that the part of the database to be searched has first been targeted on the basis of some criteria easy to identify (e.g. gender, the range of age). Identification can be done on the complete EES database using the facial image and four fingerprints.
- Systematic (and fast) identification at the border can only be sustained when at least a combination of four fingerprints and the facial image are used at the border. The more fingerprints are used together with the facial image, the faster and more accurate the process becomes. Systematic (and fast) identification at the border can also be realised with the iris alone.

In terms of costs, the systematic identification at the border adds a significant cost to the estimate for building and operating EES (and RTP). For other options the differences are limited.

Option (a), fingerprints only (2013 proposal), assumed that EES and RTP are built as two separate systems and hence can require different biometrics. The choice was made for enrolling visa-exempt third country nationals with 10 fingerprints and enrolling 4 fingerprints for all applicants to RTP. The difference was justified by the fact that as the RTP would contain about ten times less individuals than the EES database, a smaller biometric set is sufficient for all cases where biometrics are used. Anyhow, when EES and RTP are built as one system the biometric identifiers would be shared by both

⁸⁴ Entry/Exit Technical Feasibility study made by Unisys in 2008. Studies are published on the website: http://ec.europa.eu/home-affairs/doc_centre/borders/borders_schengen_en.ht

systems. The 10 fingerprints used in EES database would also allow all the biometric operations for RTP.

Option (b), fingerprints and facial image combined, proposes to enrol visa exempt third country nationals in EES and RTP on the basis of 4 fingerprints (for visa holders, EES/RTP relies on fingerprints already registered in VIS) plus the facial image. At subsequent border crossings, identity verification can use 1, 2 or 4 fingerprints or the facial image.

For visa holders, at first entry, an identity verification based on the fingerprints recorded in VIS is performed and the traveller's facial image is recorded in EES/RTP. At subsequent border crossings, identity verification based on facial image is sufficient also for visa holders, although fingerprints can also be used.

Option (c), facial image only, proposes to enrol all third country nationals in EES and RTP on the basis of the facial image only. Whether EES and RTP are built as one or two systems does not modify this. Verification of travellers at the border uses the facial image only.

Overview

With the assumption of one single system, the biometrics used for EES and RTP are shared.

		Option (a) Ten fingerprints	Option (b) Fingerprints and facial image combined	Option (c) Facial image only
Objectives	Better border management and facilitation	-√√√	+√√√√	+√√√
	Overstayers: identifying at the border	All three options fully meet the objective.		
	Idem: inland identification.	+√√√√		+√√√
	Use as criminal intelligence tool	All three options fully meet the objective		
	Use as criminal identification tool	+√√√	From +√√ to +√√√ depending on number of FP's	+√√
Impact on	Duration of border crossing	-√√√√ at first enrolment to 0/-√ at repeat visit	From -√ to -√√√ at first enrolment depending on number of FP's; 0/-√ at repeat visit	-√ at first enrolment; 0 at repeat visits
	Travel experience of third country nationals	-√√√√ at first enrolment to -√ at repeat visit	From -√ to -√√√ at first enrolment depending on number of FP's; 0 at repeat visit	-√/0 at first enrolment; 0 at repeat visits
	Border guard's workload	-√√√√ at first enrolment to 0/-√ at repeat visit	From -√ to -√√√ at first enrolment depending on number of FP's; 0 at repeat visit:	From -√/0 at first enrolment; 0 at repeat visits
	Fundamental Rights	-√√	From -√ to -√√ depending on number of FP's	-√

	Cost/benefit efficiency.	Both options are equally expensive. FP capturing devices in all MS to be renewed + digital cameras for option (b).	Least expensive option Digital cameras to be installed
--	--------------------------	---	---

Effectiveness. The case where there is a difference of effectiveness between options is further described here.

- **Better border management and facilitation:** At the core of this objective is the capacity to uniquely and reliably identify a person. All three options will achieve this. However the options (a) and (b) also allow performing a 1-to-n identification and therefore provide a simple (but computer resource intensive) way to avoid recording the same person twice in the EES. The issue stems from the fact that a traveller may change identity, legitimately (e.g. name change after marriage) or illegitimately, or in the worst case may maliciously use different passports to hide his/her identity. In the case of options (a) and (b), the system could be designed to identify the visa-exempt third country nationals at the border. This so-called 'de-duplication' does not need to be done for visa-required travellers as, in this case, it was done at the moment of the visa application. The biometric identification would very precisely confirm whether a person already exists in the database or not. The identification will nevertheless be useless at first entry of an individual using a non-detected forged identity as the enrolment happens on the basis of the identity stated in the travel document. The minimum biometrics set required to achieve this 'deduplication' would be four fingerprints and a facial image.

In the case of option (c), a search using a dedicated name search engine would be conducted on the fields that are part of the identification file (first name, surname, date of birth, gender) as provided on the passport but without using biometrics. This search would retrieve the cases where a traveller changed passports or where he/she uses multiple legitimately issued passports. The facial image would allow the border guard to confirm that the person is indeed the same as in an earlier record. In this option the conducted search would not be able to identify cases where a person changes name or uses a forged identity (provided the travel documents are genuine ones).

- **Inland identification.** The difference of effectiveness stems from the situation as mentioned above. In the case where an undocumented third country national has been apprehended as a result of inland controls, his/her identity needs to be confirmed. Where the person is cooperative, a classic search using biographic data (names, date of birth, etc.) can be performed and verified using the facial-image. For non-cooperative persons, options (a) and (b) allow the taking of the person's biometrics and looking for a match in the entire database. In the case of option (c), the process will be conducted step-wise in order to address only a segment of the database where the facial match can be done: first do a 1-to-n identification in VIS which would yield a result in case the overstayer is a visa-required traveller; second, if no result is found, search among the visa-exempt travellers that are currently in the Schengen area, specified on gender and estimated age group. With such a methodology, the search on a facial image can be made against a smaller portion of the database, with a large probability of an effective match.
- **Use as a criminal identification tool.** In the case of criminal identification the sample to be used is most often a (potentially incomplete) set of latent fingerprints found on an object or a facial image extracted from a video surveillance system. In the first case the chance of effective identification is obviously higher if more fingerprints are

stored in the database. For example: if four fingerprints are stored in the database and the criminal sample shows fingerprints from the other hand no match will be reported. It should however be recognised that the relative importance of fingerprints in criminal identification is diminishing. The ever-increasing amount of photo and video recordings made, also in the public domain, results in a higher probability of having facial images than fingerprints of an individual. Identification by means of facial matching for criminal investigations becomes essential. Therefore option (c) is also seen as having a positive impact for criminal identification.

- **Impact on border crossing time.** There is no difference between the respective options in required time for confirming the identity of a person (the so-called one-to-one verification). If fingerprints are used as a verifier, only one up to four are used, even if more fingerprints are stored. The differentiating element is the impact on the border crossing time for the visa exempt travellers who need to be enrolled. In this case, enrolling more fingerprints renders this task more time-consuming as concluded by the Smart Borders pilot: *"In a nutshell, enrolling eight fingerprints took roughly twice as long as enrolling four ($\approx +126\%$), while enrolling ten fingerprints took almost three times longer ($+185\%$)"⁸⁵.*

The results of the Smart Borders Pilot⁸⁶ show that enrolling ten or eight fingerprints from travellers is difficult and time-consuming in airports but is simply impossible in border crossing points where the conditions are less favourable like land borders and on moving trains or vessels.

Option (a) should therefore be discarded because it would be impossible to implement with the current state of technology. Option (b) can be implemented in all border crossing points provided that not more than four fingerprints are taken in combination with a facial image and with the condition that fingerprint scanners enrolling four fingerprints in one slap are implemented at all major border crossing points. It must be underlined that the enrolment of four fingerprints remains difficult in specific environmental conditions (high temperature, very low temperature) or in specific circumstances requiring the use of mobile devices. In option (c) only a good digital picture of the traveller is taken and enrolled. As confirmed in the Pilot *"Capture of the live facial image was typically possible in a short period - in less than 15 seconds at every type of BCP (except inside a train) - and should not have any noticeable impact on the overall duration of BCP operations. Furthermore, extraction of the facial image from the chip (as described fully in the chapter on chip reading) and the execution of the comparison software added only a couple of seconds to the overall process."*⁸⁷.

- **Impact on border guards' workload** goes in parallel with the increased duration of border crossing as all enrolments happen with border guard attendance except for border crossing points where self-service solutions are deployed and used for enrolment.
- **Travel experience of third country nationals:** The results of the survey performed by FRA in parallel with eu-LISA's pilot show that most travellers are comfortable

⁸⁵ Smart Borders Pilot, Final report volume 1, EU-LISA, November 2015, page 8

⁸⁶ Smart Borders Pilot Final report volume 1, Eu-LISA, November 2015, section 2.1.7.2 - page 36: "Using mobile equipment for enrolling eight FPs was also seen as difficult, in particular when performing the enrolment in a constrained space (e.g. in a train)" and section 2.1.7.3 - page 37: "The re-attempt policy was considered particularly burdensome for the users when ten prints were enrolled."

⁸⁷ Smart Borders Pilot Final report volume 1, Eu-LISA, November 2015, section 2.2.5.2 - page 44

with providing biometrics ("*approximately 1 in 10 travellers feels very uncomfortable with providing fingerprints or facial image*")⁸⁸ when crossing the border and do not perceive the provision of biometrics in the context of border control as compromising to their right to privacy and dignity. Trust in the reliability of biometric technologies is also high ("*more respondents (46.6%) have trust that biometric technologies will always properly identify who they are, compared to those who tend to have no trust (20.8%)*")⁸⁹. These results are similar for both fingerprints and facial image.

Fundamental Rights. As biometrics are considered as sensitive data, the more biometrics are enrolled and stored the bigger the intrusion in privacy is. The impact is rated -√ in case of option (c) (Facial Image only) to show that this is the minimum level of intrusion that can be reached for an Entry Exit System recording biometric identifiers. The facial image is already used by border guards who compare the face of the travellers standing in front of them with the picture printed in the travel document. However, using only the facial image as biometric identifier would not be sufficient to perform identifications of individuals in a database containing several tens of millions of records. Option (b) retains the 'lighter'/smaller' biometric identifiers necessary and sufficient for the specified purposes of identification of third country nationals crossing the Schengen area external border. The proposal will also provide that verification can be done on the basis of the facial image only. This difference in the use of biometric identifiers for identification or for identity verification contributes to a reduction of the personal data captures during border controls and transiting in the communication infrastructure. From a personal data protection perspective, option (a) would collect more information than necessary for the purpose of achieving the two primary objectives of the EES.

As explained at point 6.1.5, the FRA survey has reported that the majority of all respondents do not feel that providing biometrics in the context of border control affects their dignity. However, special provisions have to be included for people for whom biometric enrolment is physically impossible or cannot be performed in the defined conditions.

Efficiency. The cost to be borne by the EU budget for building a system with any of the biometric options proposed differs by a maximum 6%, which is significant in absolute numbers (€22,2 million over 4 years) even if it is not a strong differentiator (see annex 6 - Cost Model for EES System – 6.1.1, page 62).

Option (a) requires that all Member States adapt their existing fingerprint capturing devices to a four fingerprint scanner. Option (b) does not require this move to four fingerprint scanners as quickly although it remains a preferable situation when more than four fingerprints are taken. Option (b) and (c) require the installation of digital cameras to take the pictures which have a low price per unit (Smart Borders pilot estimates it at €100 per unit)⁹⁰ but would have to be implemented in many border posts⁹¹.

Coherence: Option (a) was introduced in the 2013 proposal to remain coherent with VIS. However the conditions and the time available for enrolling good quality fingerprints in consular posts or at border crossing points are not identical. The pilot results demonstrate that even if enrolling 10 fingerprints would be feasible at any type of border⁹², the impact

⁸⁸ See annex 15 - Fundamental Rights Agency survey – section 1.3.1

⁸⁹ See annex 15 – Fundamental Rights Agency survey – section 1.3.3

⁹⁰ Smart Borders Pilot Final Report volume 1, Eu-LISA, November 2015, section 3.4.2.2 - page 129

⁹¹ There are about (the numbers slightly vary over time) 1800 border crossing points at Schengen external borders. But less than 10% are large border crossing points.

⁹² This condition is far from being fulfilled. See Smart Borders Pilot Final report, EU-LISA, November 2015, section 2.1.5.1, page 29: "When enrolling 10 prints, success rates comparable to those obtained for four print enrolments were only obtained at a single air border crossing point". 10 prints could also not be taken on trains: see table 9 on page 27.

of this operation on border control duration is not acceptable. As the report of the Smart Borders pilot states: "It is clear that, overall, enrolling ten fingerprints has a significant negative impact on the throughput of the BCP, especially if stringent quality thresholds or re-attempt policies were to be enforced"⁹³. Option (a) needs therefore to be abandoned and replaced by either option (b) assuming four fingerprints and a facial image, or option (c).

Preferred Option. Option (b) is the preferred one as it meets all the objectives and combines positive or neutral (assuming four fingerprints) impacts. Option (c) could be considered but would not achieve entirely the objectives.

7.1.3. Facilitation

Overview

The assumption of one single system continues to be made. The registered traveller's (RT) status is simply an information element in the identification file of the traveller.

		Option (a) 2013 proposal. registration in consular post/airport before travelling	Option (b) on-line registration only after at least one visit to Schengen	Option (c) use of accelerators
Objectives	Better border management and facilitation	All three options achieve the objective of facilitation and focusing controls better.		
	Reducing the number of overstayers	The choice of option on facilitation has no impact on achieving this objective		
	Use as criminal intelligence tool	The choice of option on facilitation has no impact on achieving this objective		
	Use as criminal identification tool			
Impact on	Duration of border crossing	+√ for all travellers +√√ for registered travellers		+√√ for all travellers
	Border guard's workload	+√√		+√√√√
	Travel experience of third country nationals	+√		+√√√√
	Fundamental Rights	-√√√√		0
	Cost/benefit efficiency.	Marginal cost for an RTP system ⁹⁴ is €52,58 million development cost + €21,51 million yearly operations cost + additional cost of process in consular posts for option (a)		No additional central development. Cost for acquisition and deployment of accelerators

⁹³ Smart Borders Pilot Final Report volume 1, EU-LISA, November 2015, section 2.1.5.2 – page 32

⁹⁴ See the item "marginal cost of RTP" under Annex 6 –section 6.2, page 63

Comment

Both option (a) and (b) rely on a dedicated system of functionalities in EES to be developed. A new legal instrument is required, which will set the obligation for all Schengen states to receive, process and award RTP applications. Third country nationals with a RT status will benefit from the advantages related to their status at any border crossing point.

Option (b) requires also the development of a secure web service to collect applications and forward them to the responsible Member State.

Option (c) relies on self-service systems which do not necessitate the development of a new IT system and requires minor modifications to be included in the Schengen Border Code. The implementation of process accelerators is optional and would usually only be implemented at particularly busy border crossing points, to be decided by the Member States concerned.

Effectiveness

- **Impact on border crossing time.** This criterion looks at the average border crossing time for all third country nationals. The Technical Study concluded that in order to have a positive impact on the overall border crossing time of all third country nationals it would be necessary to have about 12-15% of border crossings made by RTP subscribers⁹⁵. Options (a) and (b) are therefore indicating a positive yet modest contribution to the overall border crossing time. Option (c) will have a more substantial positive impact because it is based on the installation of accelerators (essentially self-service systems) at all busy border posts and available for all third country nationals: "*.. approximately 35 seconds can be saved for each border guard-traveller interaction at the manual booth when the kiosks are deployed as in Madrid. Therefore, assuming continuous flow of passengers to a single manual booth, the throughput at the manual booth could double if enough kiosks are available for travellers to perform the pre-checks*"⁹⁶.
- **Impact on border guards' workload.** In option (a) and (b) registered travellers will require about the same amount of border guard supervision as EU citizens. The impact on border guard time is significant, but only when the population of Registered Travellers becomes sizeable, to precisely allow having continuously at least 12-15% of border crossings made by RTP subscribers. Option (c) will have a smaller impact per traveller but is however applicable to all third country nationals. The repetitive and administrative tasks required for border control will be automated while border guards will have more time to focus on traveller's assessment. Therefore option (c) is expected to have the highest impact.
- **Travel experience of third country nationals.** In option (a) and (b) the frequent traveller would obtain a "status" which would exempt him/her from the obligation to undergo a thorough check. Due to the pre-vetting done during the application process, RTs would at entry derogate from the thorough checks. This has a clear positive

⁹⁵ Technical Study on Smart Borders, European Commission, DG HOME, 2014, appendix J, section 2.2, chart on page 435 showing average dwelling time in manual lanes vs ABC lanes (case of an airport). To reduce average dwelling time from 2,9 minutes to 2,5 minutes (so by 24 seconds) at least 12-15% of TCN crossings need to be made by RTP subscribers. Even when 25% of TCN border crossings are made by RTP subscribers average dwelling time at manual lanes only goes down to 2,3 minutes (so reduction by 36 seconds).

⁹⁶ Smart Borders Pilot Final report volume 1, EU-LISA, November 2015, section 2.5.4.3 – page 76.

impact for this category of privileged travellers. Other third country nationals may benefit indirectly as queues may become shorter. In option (c), travellers will be given the opportunity to use their waiting time effectively by providing themselves the information that is necessary for the border check without having to rely on the direct intervention of a border guard. This will reduce the average time needed for the checks performed by the border guard, and may allow trusted (frequent) travellers to be authorised crossing the border without a "face to face" border check. This possibility shall only be granted when it has been verified through automated means that at all the conditions for entry or exit under the Schengen Borders Code are met.

Fundamental Rights. Options (a) and (b) both assume that the applicant for Registered Traveller's status provides a lot of information on the reasons of his/her frequent travels to the Schengen area. Although the Registered Travellers scheme is not compulsory, the traveller has to give up some of his/her privacy to undergo the pre-vetting process and obtain a benefit. In the case of option (c) no additional information would be collected as there is no Registered Traveller's status and the facilitation is based on information already registered into the EES.

The use of ABC gates and self-service kiosks at border controls as proposed in option (c) could be perceived as causing less discrimination as checks performed by human beings. The results of the FRA survey show that there is a widely held view that automated systems could cause less discrimination – for example on the basis of race or ethnicity – compared to checks carried out in person by border guards.

Efficiency. Options (a) and (b) assume an application or module to be built to manage the Registered Traveller's status. The investment cost for building this application on top of an Entry Exit System is about €74 million. This does not include the costs of the vetting process and the impact on human resources in the consulates of Member States. These costs may be higher than the foreseen €20 fee collected at the moment of the RT application. Increasing the fee would in principle be an option but would make the possibility to apply the RTP status less attractive for potential beneficiaries. In that respect, option (b) is viewed as more favourable than option (a) as its application process only relies on electronic communication and avoids additional tasks to be added to the existing ones in the consulates.

Both option (a) and (b) imply an obligation for all Member States to build a capacity for the reception and processing of RTP applications (whether at consulates, borders or online). Whereas the need for establishing RTP solutions is not equally felt by all Member States the workload and costs that come with the introduction of this solution would be equally imposed on all.

Option (c) does not assume any specific additional IT system⁹⁷: the already envisaged entry and exit functionalities are sufficient to operate this option. The costs of accelerators, if and where they would be installed, would be carried by Member States which can request partial financing from relevant EU programmes.

When looking at the results of existing national or airport-specific registered travellers' programmes, it appears that these programmes attract only a small percentage of travellers (like 1 or 2%), which does not come close to 10-12% envisaged for an EU RTP. These programmes also appear to be very resource intensive for those who organise

⁹⁷ The only additional application could be (without being mandatory) a smart phone "app". The investment was not quantified but is estimated to be very low.

it. The examples that currently exist target a very limited set of travellers, contain a high price tag (in the area of €120 per year) and combine fast border crossing with additional benefits such as exclusive access to lounges and easier parking.

Coherence. The RTP options aim at authorising the use of automated border control processes for low-risk third country nationals. However the workload resulting from the application process and pre-vetting process were identified as having an important impact on national administrations. The impact of the application process on the potential candidates was also analysed. The study proposed an alternative online solution allowing a reduction of the administrative burden associated to the application process and potentially more attractive for travellers. The ratio resulting from the comparison of the limited number of potential candidates, even if positively impacted by the possibility to apply online, with the development and operational cost of such a system suggested that a solution facilitating border crossing for a wider group of traveller at a lower cost should be promoted. The use of accelerators relies on automated border control processes, is open to most of the travellers and does not require the development of a new system.

Preferred Option. Option (c) is the preferred option as it combines many positive impacts, addresses a larger group of travellers and has the best cost/benefit efficiency.

This option could be complemented by national RTP schemes, introduced on a voluntary basis by those Member States that see a specific need for this additional and more targeted facilitation solution. In order to guarantee a harmonised approach and to ensure an appropriate level of security within the Schengen area, the minimum checks to be performed for the pre-vetting of the beneficiaries of such national RTP as well as the remaining mandatory checks at their border crossing have to be expressly foreseen by the Schengen Borders Code.

7.1.4. Data retention

Overview.

The table below summarises the three options considered.

		Option (a) max 181 days in EES in general, 5 years for RTP	Option (b) max 181 days in EES, less than 5 years for RTP	Option (c) more than 181 days (5 years) for EES and RTP
Objectives	Better border management and facilitation	0	-√√	+√√√
	Reducing the number of overstayers	+√√	0 to +√√	+√√
	Use as criminal intelligence or identification tool	0	0	+√√√
Impact on	Duration of border crossing	+√	+√	+√√√
	Border guard's workload	+√	+√	+√√√
	Travel experience of third country nationals	+√	+√	+√√√

		Option (a) max 181 days in EES in general, 5 years for RTP	Option (b) max 181 days in EES, less than 5 years for RTP	Option (c) more than 181 days (5 years) for EES and RTP
	Fundamental Rights	-√	-√	-√√
	Cost/benefit efficiency.	Minimal cost for EES but medium benefits (for option (b)) Requires development of RTP: marginal cost of RTP is €74 million over 4 years		Cost for EES in options (a) and (b) increases by €41,7 million over 4 years but no RTP required and larger benefits.

Comment

In the 2013 proposal, the EES is conceived to replace the stamping of passports for short-term stay by recording entries and exits in a central database, whereas the RTP intends to bring facilitation. The current integrated proposal aims to combine both objectives in one single system. This has an important impact on data retention periods.

For EES, both options (a) and (b) propose the minimal formal retention period allowing the functioning of the system. With these options, the border guard will have a limited view on the travel history of the third country national arriving at the border and the travellers will have to (re-)enrol frequently in the system. This period is also insufficient for the proposed "touring visa"⁹⁸, whose holders would be allowed to stay in the Schengen area for stays of up to one year.

Option (c) will enable border guards performing their tasks with the same level of information as currently available. Travellers will have to re-enrol less frequently, which has a direct impact on the average time necessary for border controls.

A longer retention period will also imply a larger database. The system needs to be capable of processing more data without increasing the response time.

For RTP, both options (a) and (c) propose the same data retention period as currently implemented for VIS. This is justified by the similarities that exist between a multiple entry visa and a RT status in terms of vetting conditions and application processing. Option (b) would imply a shorter data retention period for RTP, which has little consequences on the cost and performances of the system, but would create more work for the individual applicant and thereby undermine the attractiveness of applying for a RTP status.

Effectiveness

- **Better border management and facilitation:** Option (a) automates a border control step, but does not consider facilitation aspects. Option (b) would lead to an earlier deletion of RTP data, which reduces the attractiveness of such a programme. Under

⁹⁸ Proposal for a Regulation of the European Parliament and of the Council establishing a touring visa and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 562/2006 and (EC) No 767/2008 (COM(2014) 163 final) with its annexes.

option (c) providing a travel history will help tailoring the thoroughness of the border control. Avoiding the need for regular re-enrolment facilitates the border crossing process. There is therefore a significant impact of option (c) on meeting this objective.

- **Reducing the number of overstayers.** Option (a) and (b) keep entry/exit records for precisely the period of time required to detect overstayers when crossing the border. Option (a) keeps data of overstayers for five years, which has a positive impact on evaluating overstay risk. Option (b) keeps data of overstayers between a minimum of 181 days and five years, Option (c) keeps entry and exit records for 5 years for all travellers and not only for overstayers.
The impacts of options (a) and (c) are rated as "medium" as the system will allow for detecting the overstayers, but is in itself not sufficient to reach the objective of reducing the number of overstayers. For this, additional policies and actions will be necessary.
- **Use as a criminal intelligence tool.** The use of the system for criminal investigations to combat terrorism and serious crime will only be useful if data can be retrieved over a sufficiently long period of time. Considering that an official investigation can only start once an offence is committed and has become known to law enforcement authorities and can take several years to lead to results, it is considered that options (a) and (b) do not contribute to achieving this objective. The use of EES as a criminal intelligence tool would require having access to the travel history of suspected travellers and/or victims. To be relevant this travel history has to cover a commensurate period of time. As an example, for an investigation concerning trafficking of human being, in the case of a short retention period, consultation of the database would allow the retrieval of information concerning the victims being registered as overstayers while the information concerning the criminals would be deleted after six months. In such a case, options (a) and (b) would not be sufficient.
- **Use as a criminal identification tool.** The use of EES as a criminal identification tool would require the comparison of available information with all records of the database with a view of identifying an individual. In criminal investigations, the retrieval of information necessary for querying the database could take time. If the data deletion happens before this information is available, which is highly probable with options (a) and (b), the identification could become impossible. Only option (c) would be sufficient for this purpose.
- **Impact on border crossing time.** Options (a) and (b) have a positive impact on border crossing time as border guards do not have to read border control stamps to determine the duration of authorised stay, nor do they have to stamp documents anymore. Option (c) adds the benefit of also providing a rational basis for the border guard to decide on the level of thoroughness of the control.
In option (a) the biometric data which are stored with the personal identification data are deleted after 181 days. This requires biometrics to be enrolled again at a next repeat visit. A longer data retention period, like in option (c) is therefore beneficial for the average border crossing time as fewer travellers will have to undergo re-enrolment.
- **Impact on border guards' workload** goes in parallel with the increased duration of border crossing as the controls mentioned require border guard attendance.
- **Travel experience of third country nationals.** The options (a) and (b) applicable to data stored for use by the entry/exit functionalities will lead to the need of more frequent re-enrolment. The evaluation of both options is the same because it is the

data retention in EES that will drive the re-enrolment. Option (c) does not have this shortcoming.

Fundamental Rights. The longer data are stored, the more negative is the impact on the privacy of the visa-exempt traveller. For the visa-required traveller part of the personal data are anyhow stored in VIS and are kept for five years from the moment the visa has expired. EES will add information concerning the cross-border movements of these travellers. Consequently, the negative impact is the highest for visa-exempt travellers in the case of option (c). Data protection principles provide that the retention of personal information shall be limited to what is necessary for the relevant purposes. Option (b) would not allow achieving the two primary objectives of the EES while option (a) is sufficient for achieving the second objective (to reduce irregular migration, by addressing the phenomenon of overstaying) but would not be sufficient for facilitating the border crossing of bona fide travellers which is an essential element of the first objective.

Efficiency. The data retention time in EES has a significant influence on the costs for developing the central system. This is not so much because storage capacity increases, but mainly because some software products are priced according to the volume of data to be handled. Option (c) implies an additional cost of €41.7 million over 4 years ⁹⁹(3 year development and one year of operations) as compared to option (a). The data retention time in RTP which is the differentiating element between options (a) and (b) applies only to the data from RT travellers (estimated as about 10% of travellers). The cost difference for keeping RT data less than 5 years as in option (a) is therefore estimated to be marginal.

In this context it should however be noted that options (a) and (b) are far less successful in meeting facilitation objectives. For facilitation purposes it was proposed to develop and maintain RTP, which has a marginal cost (the cost on top of developing the EES part) of €74 million over 4 years. Options (a) and (b) do therefore not appear as very efficient solutions. Option (c) creates the opportunity not to develop a specific system for managing the RT status whose cost is superior to the additional cost induced by a longer data retention period. Therefore in terms of efficiency, option (c) scores also highest.

Coherence. Options (a) and (c) are coherent with the way facilitation is addressed in each case. Option (c) is coherent with the data retention period adopted in VIS and remains minimal and proportional to the way EES would function.

Preferred Option. Option (c) is the preferred option.

7.1.5. Law Enforcement Access

Overview

At the basis of the comparison is the assumption that, in case access to the Entry Exit System would be granted to law enforcement authorities, this would be under strict conditions in line with the relevant recent Court rulings. It is further assumed that law enforcement would in that case be a secondary purpose, whilst migration border management and facilitation remain the prime purpose of EES.

		Option (a) 2013 proposal	Option (b) from the start	Option (c) no law
--	--	-------------------------------------	--------------------------------------	------------------------------

⁹⁹ Cost Report of the Technical Study, section 4.3.3

		after an evaluation two years after start of operation	enforcement access
Objectives	Better border management and facilitation	LEA has no impact on this objective	
	Reducing the number of overstayers	LEA has no impact on this objective	
	Use as criminal intelligence tool	+√√√ (only when combined with a significant data retention period).	-
	Use as criminal identification tool	+√√ to +√√√ (only when combined with a significant data retention period and the availability of fingerprints and a facial image).	-
Impact on	Duration of border crossing	LEA has no impact on border crossing time as biometric choices are made to fit immigration purposes	-
	Travel experience of third country nationals	LEA has no impact on this as data submitted for justifying the RT status would not be accessed. Only exit/entry records would be accessed	-
	Border guard's work	LEA has no impact on this as the immigration related controls are not changed.	-
	Fundamental Rights	+√	0
	Cost/benefit efficiency.	The marginal cost of providing LEA to existing data is low: € 2,7 million over 4 years (0,5% of the total estimated cost for EES)	Zero cost but zero benefit

Comment

If option (a) is retained and LEA is granted after evaluation, the technical implementation complexity and costs will not increase dramatically, provided that the necessary data retention period is anticipated. An extension of the data retention period two years after entry in operation would constitute a major change to the system as it would require increasing the storage and processing capacities.

Option (b) has a limited technical impact on EES. Its cumulated cost over 4 years (period 2017-2020) is estimated at €2,7 million, the major part stemming from adding the possibility to identify persons on the basis of partial fingerprints. Nevertheless, this option is of little interest if it is not associated with a sufficiently long data retention period.

Option (c) is neutral for the EES system, but leads to an underutilisation of the potential of the system which may be difficult to justify from a public policy perspective. While the EES will contain entry and exit records of third country nationals, investigators

would be refused access to it. Time may be wasted on investigations on suspects that are no longer in the Schengen area. Reversely access to EES data would allow investigators to reconstruct travel routes whatever the means of transportation used (land, sea, air).

Effectiveness. Options (a) and (b) only differ in terms of the time when the access is provided. As mentioned earlier, the reasons justifying a two-year evaluation period are in the meantime no longer valid as both VIS and SIS are operational and VIS data are accessed by law enforcement authorities over a sufficiently long period of time to provide evidence that VIS is indeed effectively consulted (during the first 8 months of 2015, there were on average 1.400 consultations per month for law enforcement purposes), in addition to other sources of data and information, and such consultations are leading to successful resolution of serious crimes.

Fundamental Rights. Option (c) has the advantage of being more respectful of data protection than options (a) and (b). However, it is difficult to justify that no access is granted to data that can be helpful in preventing terrorist acts and stopping criminal activities, both having a deep negative impact on the fundamental rights of their victims (prohibition of slavery and force labour; right to liberty and security). From this perspective, option (b) should be retained.

The processing of personal data will be in line with Council Framework Decision 2008/977/JAI on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters and the Europol Decision 2009/371/JHA and the Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

Efficiency. Providing access to data to law enforcement authorities would add a marginal cost of €2,5 million over the development period¹⁰⁰, essentially because the biometric matching engine should also be able to match partial fingerprints collected on a crime scene with those registered in the EES (or VIS). It would further add €0,2 million of yearly operations cost. Over 4 years, law enforcement access accounts for €2,7 million or 0,5% of the cost for developing and maintaining EES over the same period.

Coherence. Providing access to data to law enforcement authorities from the start is coherent with the VIS Regulation.

Preferred Option. Option (b) is the preferred option.

7.2. Preferred option

7.2.1. Solution outline

The preferred options for the implementation of the Entry Exit System have the following characteristics:

- (1) Its scope should include border crossings by all third country nationals visiting the Schengen area for a short stay (maximum 90 days period in any period of 180 days), both visa-required and visa-exempt travellers, or stays on the basis of a touring visa (up to one year).

¹⁰⁰ Cost Report of the Technical Study, section 4.1.4

Family members of EU citizens enjoying the right of free movement or of third country nationals who enjoy the same rights of free movement equivalent to those of Union citizens and who do not yet have a residence card should be registered in the EES but are not subject to the short stay rule and checks on this category shall be carried out in accordance with Directive 2004/38/EC. Such family members in possession of a residence card referred to in Directive 2004/38/EC are excluded from the EES.

- (2) The system will collect data and register entry and exit records with the view of both facilitating the border crossing of bona fide travellers and being able to identify overstayers.
- (3) There will be one single system: the Entry Exit System (EES). Interoperability between the EES and the VIS is established at central level. Communications with Member States occur via a National Uniform Interface which is the same for all Member States and provides a set of generic message handling services.
- (4) The biometric identifiers for EES are four fingerprints used in combination with the facial image.
- (5) The approach for facilitation is based on the implementation of self-service systems which allow third country nationals to initiate border clearance which will be completed by providing additional information on border guard's request. In addition there will be a harmonised legal basis, to be introduced in the amendments to the Schengen Borders Code, for the establishment of national RTPs on a voluntary basis.
- (6) The retention time for stored data is five years. For overstayers not yet found at the end of the data retention period, following a national decision, an alert based on the EES data can be created in SIS, based upon a national decision, before deletion of the EES data.
- (7) From the start of operations, Member States' law enforcement authorities and Europol will have access to the EES, under strictly defined conditions

7.2.2. Cost of Preferred Solution

The cost of the preferred solution is composed of the cost for the EES system and the costs for Member States to comply with the Smart Border processes.

Cost for the EES System

The cost model applied is explained in Annex 6 - Cost Model for EES System. The **development cost** to be borne by the EU budget amounts to **€394,77 million, split as €222,10 million for the central system** (including the National Uniform Interface) **and €172,67 million for the (thirty) national systems** (including the technical integration of national systems with the National Uniform Interface). This is the cost accumulated over the estimated three years required to build the system. In addition, changes would be required to VIS (to establish interoperability between EES and VIS) and SIS (for the creation of an alert for overstayers not found at the end of the EES data retention period), which have been estimated as €40 million development cost and no additional operational cost.

The first year of operations the EU budget would bear a total operations cost €45,47 million split as €25,76 million for the central system and €19,71 million for the (thirty) national systems.

The cost to the EU budget amounts to €440,2 million + 40 million (for changes to VIS), equals **€480,2 million over 4 years (3 years development and 1 year operations)**.

Compliance Costs

These costs are computed (see Annex 10 – Implementation Costs at national level) independently of the source of funds as some Member States may not be eligible for EU programmes according to their status (EU Member States in Schengen or not and associated countries). However the incurred cost would remain the same.

The technical integration of NUI (National Uniform Interface) with national systems is already included in the estimate of the Smart Borders system. The national investments are computed as marginal costs on top of the existing personnel and infrastructure.

The implementation cost on Member States side would consist of:

- €57,0 million one-off set-up costs of new processes and infrastructure improvement over the 3-year development period;
- €109,5 million equipment cost for respectively small (€20,16 million) and large borders crossing points (€ 89,35 million) assumed to be done over the 3-year development period. These investments would induce an annual maintenance cost of €11 million once completely accomplished.

These costs are not included in the financial annex to the legal proposal.

Administrative burden

The Entry Exit System does not create any additional administrative burden to private or public organisations because all legal reporting obligations will be obtained from reports produced by the system. All data recorded in EES are taken from existing commonly used travel documents and the amendments to the Schengen Border Code do not introduce new controls but the impacts EES has on those controls.

7.2.3. Benefits of Preferred Solution

The benefits resulting from the preferred solution have been calculated (see annex 11 - Benefits of Smart Borders preferred solution) based on cautious assumptions.

The elements taken into consideration for this calculation are:

- The impact on third country nationals: the facilitation of border crossing has consequences on time spent at borders by third country nationals for border controls. To remain cautious only benefits were assumed for the share of third country nationals using the main (and therefore busiest) border crossing.,
- The impact for border control services: for some categories of travellers, the enrolment in EES will generate an additional workload while the use of self-services solutions will reduce the workload. This explains why at the beginning

the benefits are low as all visa-exempt third country nationals need to be enrolled with facial image and 4 fingerprints,

- The impact on migration management: EES will increase the possibility to identify overstayers and irregular migrants as well as the implementation of return decisions.

The financial benefits identified by this calculation amount at €16,24 million for the first year of operation and at €602,8 million for the seventh year of operation (= 10th year after project start).. The cumulated benefits over ten years equal 2,73 times the accumulated costs over the same period.

Not included in this amount are the benefits resulting from

- the possibility of accessing the EES data for law enforcement purpose,
- the impact of the introduction of facilitations of border control on airlines and ferries activities,
- effects on tourism
- impact on retail activities in airports and seaports and cross-border shopping
- impact on irregular labour market

7.2.4. Cost/benefit analysis

The detailed cost-benefit analysis is available in annex 12 - Cost/benefit analysis for preferred solution.

This analysis is produced using the results of calculations performed for:

- The cost model of the proposed Entry Exit System,
- The implementation costs at the national level,
- The benefits of the preferred solution.

Based on the costs estimated for 30 Member States and the benefits for only 26 Member States, the **net present value** at the beginning of the project has been computed for future costs and benefits using a discount rate of 4%.

The result of this computation is shown in the chart below.

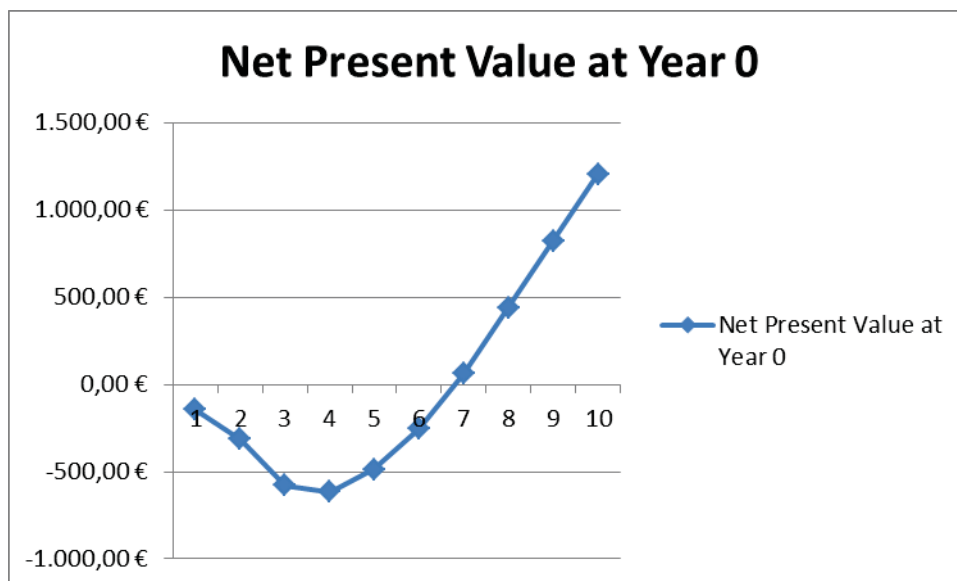


Chart showing the Net Present Value (in million €) after 1, 2, ..N years

The net present value decreases when costs and (zero) benefits of the first three years are discounted to the beginning of the project. As benefits outweigh more and more costs over the next years, **the net present value at the beginning of the project becomes positive after four years of operations** (which is in the course of year 7 after project start as operations begin after an estimated 3-year development period).

7.3. Subsidiarity and proportionality of the preferred option

Under Articles 74 and 77(2) of the Treaty on the Functioning of the European Union (TFEU), the Union has the power to adopt measures relating to the crossing of the external borders of the Member States. Under Articles 82 (1)(d) and 87(2)(a) TFEU the Union also has the power to adopt measures to strengthen police and judicial cooperation by collecting, storing, processing, analysing and exchanging relevant information.

No Member State alone is able to cope with irregular immigration and with combating international terrorism and serious crime. A person may enter the Schengen area at a border crossing point in a Member State where a national register of entry/exit data is used, but exit through a border crossing point where no such system is used. The monitoring of compliance with EU rules on authorised stays can therefore not be done by Member States acting alone. Third-country nationals who enter the Schengen area are able to travel freely within it. In an area without internal borders, action against irregular immigration should in principle be undertaken on a common basis. Considering all this the EU is better placed than Member States to take the appropriate measures.

Although Member States may retain their national systems in accordance with security-related national legislation and provided they comply with EU law, in particular data protection rules, an EU Entry Exit System would allow Member State authorities to access data on third-country nationals who crossed the EU external border in one country and exited via another Schengen country.

Better information on cross border movements of third-country nationals at EU level would also facilitate the negotiation and conclusion of visa agreements between the EU and third countries and contribute to a common understanding of immigration issues with third countries of origin.

The preferred option would create an instrument providing to the European Union the basic information on how many third country nationals enter and leave the territory of the EU. This information is indispensably needed for sustainable and reasonable policy making in the field of migration and visa.

Furthermore the preferred option would have significant added value in providing all Member States with clear and unambiguous data on overstayers and access to alerts on each individual, greatly contributing to the possibility of apprehending those persons and launching, where required, a return process. Compared to the baseline, with its reliance on the manual stamping of passports, and taking into account the size of the problem of overstayers at European level, the added value is apparent.

The preferred option will, compared to the national entry exit systems currently in operation, bring benefits in terms of counteracting irregular immigration by providing border authorities with more reliable and modern tools for carrying out border checks. The investments made into hardware and software for their national systems might not be

lost – some of the equipment and system software may be reused in the centralised solution. Member States will have the opportunity to discuss the specifications of the system in comitology procedures, and can argue to use a certain platform that they might have already proven useful. In any case, the national entry exit systems may be maintained for national security purposes in accordance with Member States' own security-related legislation.

The preferred option for facilitation privileges the use of automated border control means over the EU RTP solution which is more costly, would address only frequent travellers and implies the collection of additional data from third country nationals. The facilitation is based on the implementation of self-service systems which allow third country nationals to start border clearance which will be completed by providing additional information on border guard's request. In addition, there will be a harmonised legal basis, to be introduced in the amendments to the Schengen Borders Code in line with the requirements of that instrument, for the establishment of national RTPs on a voluntary basis.

The preferred option which conception is driven by the *privacy by design* principles is proportionate in terms of the right to protection of personal data in that it does not require the collection and storage of more data for a longer period than is absolutely necessary to allow the system to function and meet its objectives. In addition, all the safeguards and mechanisms required for the effective protection of the fundamental rights of travellers particularly the protection of their private life and personal data will be foreseen and implemented.

No further processes or harmonisation will be necessary at EU level to make the system work; thus the envisaged measure is proportionate in that it does not go beyond what is necessary in terms of action at EU level to meet the defined objectives.

The preferred option is also proportionate in terms of costs, taking into account the benefits the system will provide to all Member States in managing the common external border and progressing towards a common EU migration policy.

8. MONITORING AND EVALUATION

8.1. Practical arrangements of the evaluation: when, by whom

The Commission shall ensure that systems are in place to monitor the functioning of the Entry Exit System and evaluate them against the main policy objectives. Two years after the system starts operations and every two years thereafter, the Agency should submit to the European Parliament, the Council and the Commission a report on the technical functioning of the system. Moreover, two years after the Entry Exit System starts operations and every four years thereafter, the Commission should produce an overall evaluation of the system including on fundamental rights impacts and on examining results achieved against objectives and assessing the continuing validity of the underlying rationale and any implications for future options. The Commission should submit the reports on the evaluation to the European Parliament and the Council.

8.2. Operational objectives and monitoring indicators for the preferred option

The monitoring indicators in the next sections are essentially expected to be collected on an on-going basis by EES. For evaluation purposes yearly statistics will be computed and compared between successive years. Where possible, a comparison with a the baseline situation taken as the trend or average of the three years that precede the EES entry into operations can be used. However it should be noted that current statistics do not have the same level of detail as expected EES figures and that the comparison with baseline situation will often be possible only at a more aggregated level.

Operational objectives of the system include:

- (1) Proportionally, the yearly increase of the number of the full-time equivalent of border guards (data to be obtained from Member States) is inferior to the yearly increase of the number of border crossings by third country nationals (as reported by EES);
- (2) The percentage of border crossings by third country nationals based on electronic checks as reported by EES;
- (3) The number of overstayers identified and the number effectively apprehended as reported by Member States and correlated with access to EES for this purpose;
- (4) The percentage of return decisions that are executed based on Member State reporting;
- (5) The percentage of third country nationals for who the remaining authorised period of stay is effectively controlled as obtained from the availability figures of EES;
- (6) The average border crossing time for visa-exempt third-country nationals remains identical or decreases as reported by EES;
- (7) The impact on the average border crossing time of visa-required third-country nationals remains neutral or decreases as reported by EES.

- (8) Statistics on border crossing and overstay are systematic and provide breakdown per citizenship and other characteristics (e.g. traveller's age, gender and border crossing point) as reported by EES.
- (9) Statistics and case stories in relation to access by law enforcement authorities: access by EES can be reported according to purpose and access profile.

Monitoring indicators for the developments of the system result from project reporting and include:

- (10) The central part of the Smart Borders systems is put into operations within the time-span and budget of the development project defined after the adoption of the Regulation;
- (11) National Uniform Interface is delivered to Member States within the duration of the development project;
- (12) All Member States are connected to the Entry Exit System at the agreed date for "Entry into Operations";
- (13) All EES functionalities are delivered including the periodic delivery of reliable and precise statistics on border crossings and overstayers.
- (14) Process accelerators are implemented in the relevant border crossing points;

Monitoring indicators once the system is life essentially stems from systems operations reporting supplemented in some rare cases by specific data:

- (15) All third-country nationals are informed of the authorised duration of stay, of their rights and on appeal procedures in case of disagreement. The indicator can be assessed annually by looking at the processes and devices in place ;
- (16) The number of errors is minimal: errors refer to the number of incorrectly reported overstay cases due to the fact that exits were not matched with entries. This indicator to be based on Member State reporting;
- (17) Statistics on border crossings and overstay are available on demand and standard reports are regularly produced, on the basis of system operations reports;
- (18) All expired data are deleted. There is no unwanted loss or erasure of data based system operations reviews.;
- (19) All access to data was authorised. There are no cases of unauthorised access to data as observed from system operations reviews ;
- (20) Incidents on data access are reported, the origin of the problem analysed and a remedy provided as reported by system operations.

9. ABBREVIATIONS

ABC gates	Automated Border Control. Also referred to as e-Gates or electronic gates (see Glossary)
AFIS	Automated Fingerprint Identification System (see Glossary)
BCP	Border Crossing Point (see Glossary)
BG	Border Guard
BMS	Biometric Matching System
EDPS	European Data Protection Supervisor
EES	Entry-Exit System
EURODAC	European Dactyloscopy (see Glossary and Annex 17)
e-Gate	Electronic gate
eMRTD	Electronic MRTD (see below MRTD and Glossary))
ENISA	European Union Agency for Network and Information Security
EP	European Parliament
EU	European Union
eu-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
FAR	False Acceptance Rate (see Glossary)
FI	Facial Image(s)
FP	Fingerprint(s)
FRA	European Union Agency for Fundamental Rights
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
FRR	False Rejection Rate
ICAO	International Civil Aviation Organisation
LIBE	European Parliament Committee Civil Liberties, Justice and Home Affairs
MEV	Multiple Entry visa.
MRTD	Machine Readable Travel Document (see Glossary)

MRZ	Machine Readable Zone of a Machine Readable Travel Document
MS	Member State(s)
NUI	National Uniform Interface
Prüm system	Police co-operation mechanism for exchanging information on DNA, fingerprints and vehicle registration data (See Annex 17)
RT	Registered Traveller
RTP	Registered Traveller Programme
SBC	Schengen Border Code
SLA	Service Level Agreement
SIS (II)	Schengen Information System (of the 2nd Generation) (see Annex 17)
TCN	Third Country National
TCNVE	Third Country National - Visa Exempt
TCNVH	Third Country National - Visa Holder
TDN	Travel Document Number
VE	Visa Exempt
VH	Visa Holder
VIS	Visa Information System (see Annex 17)
VSN	Visa Sticker Number

10. GLOSSARY

AFIS	Automated system capable of capturing, storing, comparing, and verifying biometric data ABIS dealing only with fingerprints.
Automated Border Control (ABC) system	An automated system, which authenticates the eMRTD, establishes that the traveller is the rightful holder of the document, queries relevant systems and automatically determines eligibility for border crossing according to predefined rules.
Biometrics	Measurable, physical characteristic or personal behavioural trait used to recognise the identity, or verify the claimed identity of a person previously enrolled.
Border check	The checks carried out at Border Crossing Points, to ensure that persons, including their means of transport and the objects in their possession, may be authorised to enter the territory of the Member States or authorized to leave it. [Schengen Borders Code, Article 2.10]
Border Crossing Point (BCP)	Any crossing-point authorised by the competent authorities for the crossing of external borders. (Schengen Borders Code, Article 2.8).
De-duplication	Elimination of redundant data.
eMRTD / e-passport	Machine Readable Travel Document (e.g. passport) containing a Contactless Integrated Circuit (IC) chip within which data from the MRTD data page, a biometric measure of the passport holder, and a security object to protect the data with PKI cryptographic technology is stored, and which conforms to the specifications of ICAO DOC 9303, Part 1.
Enrolment	Process of collecting biometric samples and subsequent preparation and storage of biometric reference templates representing that person's identity
End to end duration	Time required for the entire border crossing process, from the moment the traveller cross the yellow line until the border crossing.
EURODAC	Central Automated Fingerprint Identification System (AFIS) containing fingerprints of asylum applicants and certain irregular third-country nationals. The primary current purpose is to determine which Member State is responsible for the asylum application in line with the Dublin regulation.
External borders	Schengen countries' land borders, including river and lake borders, sea borders and their airports, river ports and lake ports, provided they are not internal borders.
False Acceptance Rate (FAR)	Probability that a biometric system incorrectly identifies an individual or fails to reject an impostor.

False Rejection Rate (FRR) Probability that a biometric system fails to identify or verify the legitimate claimed identity of an enrolled individual.

First Line Check The border check conducted at the location at which all travellers are checked. See also “Second Line Check”.

FP scanner Device used to capture the fingerprints of an individual.

Identification (1:n) Process of comparing a biometric sample with a previously stored reference template.

Kiosk Self-service data collection station, configurable to perform different functionality, such as biometric enrolment and verification, or document reading.

Live capture Capturing a biometric sample by an interaction between an end user and a biometric system.

Manual verification A manual verification is made by a person and includes, in most cases, ocular inspection of a picture, from the travel document or displayed from another source, and comparing this picture to the person being checked.

Matching Successful comparison a biometric sample against a previously stored template, which implies that the level of similarity exceeds a given threshold.

MRTD Official document, conforming with the specifications contained in Doc 9303, issued by a State or organisation which is used by the holder of international travel (e.g. passport, visa,) and which contains mandatory visual (eye readable) data and a separate mandatory data summary in a format which is capable of being read by a machine.

Multimodal biometrics Combination of information from two or more biometric measurements. It is also known as “Fusion” and “multibiometrics”.

Pilot Small scale preliminary study conducted in order to evaluate different aspects in order to predict and help organizing the actual large-scale project in terms of feasibility, time, cost, adverse events, etc.

Schengen visa Uniform short stay visa that entitles the holder to stay in the territories of all Schengen States for a period of maximum of 90 out of 180days and that may be issued for the purpose of single or multiple entries.

Second line check A further check that may be carried out in a special location away from the location where all travellers are checked (first line). (Schengen Borders Code, Article 2.12)

Third Country National (TCN)	Any person who is not a Union citizen within the meaning of Article 20(1) of the Treaty on the Functioning of the European Union and who is not covered by the definition of persons enjoying the Community right of free movement outlined in Article 2.5 of the Schengen Borders Code. [Schengen Borders Code, Article 2.6].
Threshold	Decision threshold: the acceptance or rejection of biometric data depends on the quality or matching score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict.
Verification (1:1)	Process of comparing a biometric sample with a previously stored reference template.

11. LIST OF ANNEXES

This impact assessment is delivered with the following annexes:

Annex 1	Procedural information
Annex 2	Stakeholder consultation
Annex 3	Practical implications of the initiative for the affected parties.
Annex 4	Analytical models used in preparing the Impact Assessment.
Annex 5	Summary of processes at entry/exit according to current Schengen Borders Code
Annex 6	Cost Model for Smart Borders System
Annex 7	Comparison of Operational Aspects of different Biometrics
Annex 8	New Smart Border processes at border crossing points:
Annex 9	Interoperability
Annex 10	Implementation costs at National level.
Annex 11	Benefits of Smart Borders preferred solution
Annex 12	Cost/benefit Analysis for preferred solution
Annex 13	Impact Assessment on Fundamental rights.
Annex 14	Executive Summary of Results from 2015 Pilot
Annex 15	Fundamental Rights Agency survey – report
Annex 16	Preparatory work with the European Data Protection Supervisor (EDPS)
Annex 17	Existing EU large-scale IT systems



Brussels, 6.4.2016
SWD(2016) 115 final

PART 2/3

COMMISSION STAFF WORKING DOCUMENT
IMPACT ASSESSMENT

Annexes to the Impact Assessment report on the introduction of an Entry Exit System

Accompanying the document

Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011

and

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/xxx as regards the use of the Entry/Exit System (EES)

{ COM(2016) 194 final }
{ COM(2016) 196 final }
{ SWD(2016) 116 final }

Table of Contents

1.	ANNEX 1: PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES.....	1
1.1.	Identification.....	1
1.2.	Organisation and Timing.....	1
1.3.	Consultation and expertise	4
2.	ANNEX 2: STAKEHOLDER CONSULTATION.....	5
2.1.	Consultation Strategy	5
2.2.	Public consultation	6
2.3.	Meeting of the European Parliament with national Parliaments	8
2.4.	Stakeholder Consultations	8
2.5.	Survey from the Fundamental Rights Agency	11
2.6.	Results of the public consultation on Smart Borders	13
3.	ANNEX 3: PRACTICAL IMPLICATIONS OF THE INITIATIVE FOR THE AFFECTED PARTIES.....	25
4.	ANNEX 4: ANALYTICAL MODELS USED IN PREPARING THE IMPACT ASSESSMENT	40
4.1.	Simulation model used for the Technical Study.....	40
4.2.	Methodology used for Pilot Project.....	49
5.	ANNEX 5: SUMMARY OF PROCESSES AT ENTRY/EXIT ACCORDING TO CURRENT SCHENGEN BORDER CODE.....	57
6.	ANNEX 6: COST MODEL FOR SMART BORDERS SYSTEM.....	61
6.1.	Cost Model	61
6.2.	Marginal Cost of RTP	64
6.3.	Cost of Preferred Solution	65
7.	ANNEX 7: COMPARISON OF OPERATIONAL ASPECTS OF DIFFERENT BIOMETRICS	68
8.	ANNEX 8: NEW SMART BORDER PROCESSES.....	71
9.	ANNEX 9: INTEROPERABILITY	89
9.1.	Introduction	89
9.2.	Levels at which interoperability matters	90
9.3.	Starting point: no interoperability between central IT systems.....	91
9.4.	Reducing the impact of EES at national level.....	93
9.5.	Including the interoperability between VIS and EES.....	94

1. ANNEX 1: PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

1.1. Identification

Lead DG is Directorate General of Home Affairs and Immigration (DG HOME).

The agenda planning reference is 2016/HOME/001

1.2. Organisation and Timing

The Impact Assessment Steering Group was composed of: Secretariat General (SG unit E1), DG HOME (B3, A2), DG JUST (C3 and C1), Legal Service (SJ); DIGIT (B6); GROW (I4), DG BUDG (A3), JRC, and TAXUD (A1).

Chronology of events prior to the Impact Assessment

This chronology does not show all intermediate steps in working groups. Its purpose is only to help the reader of the Impact Assessment understand that the current document builds on a previous proposal and preparation work leading to a new proposal.

February 2013	Commission adopts Smart Borders package (called "2013 Proposal") consisting of: <ol style="list-style-type: none">(1) a Regulation for an Entry/Exit System (EES)(2) a Regulation for a Registered Traveller Programme (RTP)(3) a Regulation amending the Schengen Borders Code in order to take into account the existence of the EES and RTP.
March 2013 till February 2014	First reading in working groups of Council and Parliament.
February 2014	Commission initiates with the support of both co-legislators a so-called 'proof of concept' exercise consisting of two stages: <ol style="list-style-type: none">(1) A Commission-led Technical Study on Smart Borders (hereinafter 'the Technical Study') and,(2) A testing phase led by eu-LISA on a limited set of technical options.
February till October 2014	Execution of the Technical Study (published in October 2014). ¹
3 December 2014	Commission announces that modified proposals will be submitted early 2016.
19 December 2014	Terms of Reference of Pilot Project defined by Commission.

¹ Technical Study on Smart Borders, European Commission, DG HOME, 2014.

23-24 February 2015	Interparliamentary Committee meeting on Smart Borders organised by the European Parliament with national parliaments and participation by Commission including Commissioner D. Avromopoulos.
30 June 2015	Publication of the Inception Impact Assessment. No comments were received on this document.
29 July till 29 October 2015	Public consultation on Smart Borders
January till November 2015	Execution of testing phase by eu-LISA (report published in November 2015, hereinafter 'The Pilot') ² including site visits.
January till December 2015	Further discussion on a set of issues identified in the first reading of the "2013 Proposal" in the Council working group (Frontier's Working Party) and the LIBE Committee (committee of European Parliament dealing with Smart Borders).
September till October 2015	Meeting with technical experts from Member States on 24 September and 26 October 2015.
January till December 2015	As part of the preparation of a new legislative proposal, Commission conducts a set of informal meetings: <ol style="list-style-type: none"> (1) Meeting with Civil Society on 5 May 2015, (2) Meeting with Carriers on 28 May 2015, (3) Meeting with Law Enforcement Services from Member States on 13 July 2015, (4) Meeting with Fundamental Rights Agency on 22 June and 23 July 2015, (5) Workshops with European Data Protection Supervisor (EDPS) on 20 March and 21 September 2015.

Chronology of the Impact Assessment (IA):

This chronology only includes the steps related to formalising and completing the IA

Public consultation	12 weeks from 29 July until 29 October 2015, then extended till 31 October
---------------------	--

² http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_report_on_the_technical_conclusions_en.pdf.

First meeting of Impact Assessment Steering Group (discussion and comments on a first draft Impact Assessment)	4 November 2015
Written consultation of the Impact Assessment Steering Group on the draft Impact Assessment	14 December 2015
Meeting of the Impact Assessment Regulatory Scrutiny Board	20 January 2016

On 22 January 2016, the Impact Assessment Regulatory Scrutiny Board gave an overall positive opinion on the Impact Assessment and recommended the following points to be clarified under section B of its document:

Points to be clarified	How comments were implemented
1) How does this initiative relate (or not) to the refugee crisis and to the terrorists threat? What are the technical and practical problems identified in relation to the 2013 proposal which are being addressed by this initiative? What border management systems exist in third countries and what lessons can be learnt?	Sections 1.3. Changed context, 1.4.Revised proposal, 2.2. Implementation problems addressed by this impact assessment, 2.3. The drivers of the problems 2.5. Experiences with EES and RTP in third countries were added or redrafted.
2) How do the policy objectives address the outstanding technical/practical problems related to the entry/exit system? Why is access for law enforcement considered as a "secondary" objective	Section 4.1. General policy objectives reworded.
3) How would the entry/exit system work in practice and how would it fit into the context of other border management and security systems (e.g. VIS, Eurodac, etc.) and would these systems together cover all border crossings by third country nationals?	Introduction and chapter 1 redrafted Annexes 3 (Practical implications of the initiative for the affected parties) and 8 (New Smart Border processes at border crossing points) are better referenced.

The positive opinion included under section (C) the main recommendations for improvement and under section (D) the improvements on presentation.

Recommendations for improvement	Way it was addressed
(1) Clarify the policy context and the problems addressed	Introduction and chapter 1 redrafted
(2) Clarify/update the policy objectives	Sections 4.1 and 4.2 amended.

(3) Clarify the policy options.	Introduction and chapter 1 redrafted.
<p>Procedure and presentation</p> <p>The option description should be clearly separated from the impact analysis, and the report should be simplified by removing duplications. Furthermore, the report should be clarified by avoiding acronyms as far as possible and explaining used acronyms at their first appearance</p>	<p>Abbreviations explained, List of Abbreviations and Glossary added, option description shortened and comparisons of options moved to chapter 7.</p>

In addition specific questions sent were addressed by editing the document. The list above is not exhaustive for all the changes made.

1.3. Consultation and expertise

Use of external expertise

External expertise was used during the Technical Study:

- The consulting firm PwC was used for its expertise on analysing the technical issues (data and architecture), collecting statistical data and developing a new cost model for estimating the cost of the EES/RTP system. There was no expertise available as such on the contents and the way to perform the border control process as this would anyhow remain unchanged and compliant with the Schengen Border Code.
- During this study, the expertise from the Research and Development Unit of Frontex was used for the development and running of a simulation model assessing the impact of additional checks implied by Smart Borders on traveller's waiting time at border crossing points (expressed as "service level" and "dwelling time") and on the workload for border guards.
- Eu-LISA was associated to the study in order to understand the technical options that would be part of the Pilot phase they would have to conduct, and to collect relevant information on current systems operated by the Agency (resources required, best technical options, cost elements).

The Pilot was conducted by eu-LISA.

No external expertise was used during the Impact Assessment itself.

2. ANNEX 2: STAKEHOLDER CONSULTATION

2.1. Consultation Strategy

In line with the Commission's minimum standards regarding participation and openness to stakeholders' views presented in the Better Regulation Guidelines³, a consultation strategy has been developed to ensure a wide participation throughout the policy cycle of this initiative.

The strategy consisted in making sure all parties affected by the implementation of the Entry-Exit System would be consulted at least by the Public Consultation and the most affected parties (citizens, border guards) by another specific feed-back mechanism. Finally, a specific consultation was aimed for Law Enforcement authorities. The table below shows how the consultations were organised or the benefit taken from the one organised by the European Parliament.

	Type of Consultation				
	Public Consultation	Meeting of EP with national Parliaments	Specific Stakeholder consultation	Pilot test case feed-back	Survey from FRA ⁴
EU citizens	Specific questionnaire for individuals + Questionnaire for associations	European Parliament (EP) + National Parliaments representing EU citizens.	Specific consultation	-	-
Third-country nationals				Specific feed-back requested	Survey targeted this group
Border guards	Specific questionnaire for Authorities	Specific session in the meeting	-	Specific feed-back requested	-
Law enforcement authorities		Specific session during the meeting	Specific consultation	-	-
Authorities (in the generic sense)		-	-	-	-
Carriers and operators of infrastructure (airports, ports)	Specific questionnaire	-	Specific consultation	-	-
Industry	Questionnaire for associations includes industry	-	-	-	-

³ SWD(2015) 111

⁴ FRA stands here for Fundamental Rights Agency

	associations				
--	--------------	--	--	--	--

By these extensive consultations on top of the regular meetings with the working parties of the co-legislators⁵, the Commission has sought a wide and balanced range of views on issues covered by the Regulation by giving the opportunity to all relevant parties to express their opinions.

Results are reported as follows:

- The report of the public consultation is published on the Commission website and is summarised in section 2.2 and included in section 2.6.
- The outcome of the meeting of EP with national Parliaments is in section 2.3.
- The result of the specific stakeholder consultations is summarised in section 2.4 and takes also the feed-back from the Pilot into account.
- The executive summary of the survey from FRA is included as annex to the report of the Smart Borders pilot but some facts and figures are included in section 2.5.

2.2. Public consultation

The public consultation was launched on 29 July on a dedicated Commission website and was available during 12 weeks until 29 October 2015. The objectives of the public consultation were:

- to collect views and opinions on the policy options, their likely impact and hence testing existing ideas and options with all stakeholders and the general public;
- to gather new ideas and general relevant knowledge and
- to test existing ideas and analysis.

A total of 101 participants have provided answers to the questionnaire, in the following categories:

- 62 individuals, out of which 9 were non EU citizens
- 14 organizations (NGOs as well as industry representatives)
- 14 public authorities, all from EU countries
- 11 'carriers' (airlines, ferries, buses as well as airports or seaports operators)

The questionnaire was divided in chapters corresponding to sets of options identified in the road map and analysed in the impact assessment.

⁵ Smart Borders was a regular agenda item of the Frontier's Working Party (Council) and the LIBE Committee (European Parliament).

Biometrics

Participants have been requested to indicate their preferred option as biometric identifier: fingerprints (FP), facial image (FI), the combination of fingerprints and facial image or no biometric identifier

- 42 % of individuals have indicated that there should be no biometric identifier. 58 % of individuals have indicated that a biometric identifier should be used with a preference for the combination of FI and FP.
- 8 out of 14 organizations have indicated that there should be no biometric identifier. 6 out of 14 preferred the combination of FP and FI.
- Public authorities have favoured the combined use of FI and FP.
- 7 out of 11 carriers supported the use of biometric data, with a clear preference for the use of FI alone or in combination with FP. The need to use a biometric identifier was rejected by 4 out of 11.

Facilitation

The need for a process to accelerate border crossings was first addressed. In a second step, the participants had to answer questions on the different options for facilitation as well as their respective consequences.

There is a clear majority of respondents in favour of general facilitation of border crossings, as compared to more selective RTP type programmes. The use of alternative process accelerators such as self-service kiosks is largely supported.

Data retention

The participants had the choice between a 180 day retention period and a longer retention period (no duration specified in the questionnaire).

- Nearly half of the individuals are in favour of a data retention period of maximum 180 days while one third considers that the data retention period should be longer.
- Organisations are equally distributed.
- Public authorities are in favour of a longer data retention period.
- The majority of carriers are in favour of a longer data retention period.

Law Enforcement Access

The participants had the choice between authorising and refusing the access to EES data for law enforcement purpose.

The Public Authorities are in favour of the access to EES data for law enforcement purposes, while for the three other categories replies are equally distributed on the two possibilities.

2.3. Meeting of the European Parliament with national Parliaments

What was done. The European Parliament consulted the EU national Parliaments on the basis of the "2013 Smart Borders proposal" and LIBE held an interparliamentary committee meeting with representatives of national Parliaments on the Smart Borders from 23 till 26 February 2015. At that moment in time, the Technical Study was available and the Pilot was defined but no test cases were yet on-going.

The opinions expressed by the national Parliaments. Only seven national Parliaments (BE, CZ, ES, PT, RO, SL, RO, UK) replied with an opinion on the "2013 proposal". The national Parliaments are supportive to the idea of the introduction of an EES system, there are some doubts on the need of the RTP (CZ) and both the use of biometrics from the start and the access to EES by Law Enforcement Authorities is considered necessary from the beginning. The remaining most often cited concern is about the cost of the system (BE).

The opinions expressed during the meeting at the European Parliament (23 to 26 February 2015). During the debate Members of national Parliaments and the EP stressed the need to be clear on the purpose of the new systems (borders management and fight against irregular migration/secondary security purposes), maximise the use of existing instruments and a strictly respected budget. A large majority expressed their support for the proposal and the inclusion of the law enforcement element. In its conclusions, the EP Rapporteur for the EES called for a clearer definition of the EES's objective, with the improvement of passenger traffic as primary objective and security/access to law enforcement authorities as secondary objective. He pointed to the need to take into account the experience gained with VIS, to guarantee a robust data protection system in the respect of existing case-law and to ensure the interoperability with existing systems. The EP Rapporteur for the RTP, explained that the biggest concerns were on proportionality and costs, and reminded that the original objective is travel facilitation and increased attractiveness for the EU.

Whether/how comments were taken into account: The comments from the EP and national Parliaments have been addressed with the new proposal: primary and secondary objectives for EES are defined, the architecture of the EES/RTP has been simplified first by building both parts as one single system and later on by removing the need for a specific RTP component, costs have been reviewed and are substantially lower than in the 2013 proposal, benefits have been estimated in the Impact Assessment and show that the investment is justified, the Pilot results have validated operational solutions and in particular the use of four fingerprints and the facial image as biometric identifiers rather than ten fingerprints. The impact assessment contains a thorough impact assessment on fundamental rights of which the right to privacy is part of. Finally access by law enforcement authorities is granted from the beginning but under a set of conditions.

2.4. Stakeholder Consultations

2.4.1. EU-citizens and Third Country Nationals

What was done. The informal meeting on 5 May 2015 was attended by nine non-governmental organisations. The public consultation was responded by 62 citizens (nine of them being third country nationals) plus 14 non-governmental organisations. The feedback during the pilot was done by travellers actually passing a border control implementing the features of a border control as he/she would experience them. The pilot

received the feed-back of about 50% of the 58.000 travellers who participated. The FRA survey interviewed 1.234 randomly selected third country nationals (see section 2.5).

The opinions expressed. At the informal meeting, organisations essentially asked questions for understanding the proposal contents and also expressed their concerns that refugees and asylum seekers could be flagged as overstayers.

The public consultation shows a 50/50 split between those in favour or not of using biometric identifiers, of 5 years (or more) data retention periods and Law Enforcement Access (LEA). There is essentially an expectation of more justification and guarantees on independent control of the use of data and the right of redress.

The feed-back of travellers participating in the pilot was for a large majority very positive on the way border crossings would be done. The border crossing situations involving an enrolment/verification of biometrics achieved very high satisfaction rates (more than 80%). Where the satisfaction was lower it was related to equipment/technology problems resulting in a slow-down of the border crossing.

Whether/how comments were taken into account. The scope of the 2013 proposal remains unchanged: no residence permit holders are included, neither refugees nor asylum seekers.

The new proposal builds on the positive experience of the use of biometrics in VIS in particular and giving LEA in specific conditions. The justification is part of this Impact Assessment. The new proposal maintains all the positive measures contained in the 2013 proposal on the control of the use of data and on the right of redress.

2.4.2. Border guards

What was done. The opinion of border guards was collected during the pilot and at the occasion of a debriefing session at the end of the test case. In total the feed-back was collected from approximately 200 border guards split over the 12 test locations.

Opinion expressed. Feed-back of border guards is to a large extent unfavourable in the test cases where 8 or 10 fingerprints have to be collected. Feed-back was otherwise positive in the other test cases. The use of biometrics is viewed favourably provided the tools were user-friendly and reliable. Border guards had further suggestions for improving the traveller's flow or the ergonomics of the way the border post was set up as the time-scale for the pilot did not allow to introduce significant changes to existing premises.

Whether/how comments were taken into account: The proposal uses biometric identifiers that minimise the personal data and biometrics to be captured to comply with the principle of data protection by design. This principle at the same time concurs with the expectation from border guards to avoid capturing 8 or 10 fingerprints. The current proposal further assumes that user-friendly and reliable equipment is purchased and the cost/benefit computation includes significant amounts for equipment purchases.

2.4.3. Law Enforcement authorities

The informal meeting on 13 July 2015 was attended by delegates from 25 Schengen countries. None of these authorities answered the public consultation.

Opinion expressed. Law enforcement services (LES) are essentially in favour of having 10 fingerprints as biometric identifiers, having border guards recording additional information in EES than the data from the travel document, and having a data retention that "would be sufficiently long" given the duration between the moment a crime occurs and investigations are conducted on its circumstances. This duration would however not be longer than five years. LES themselves acknowledge the fact that access to personal data had to be justified on a case by case basis.

Whether/how comments were taken into account: As LEA is a secondary objective in the new proposal it cannot justify additional requirements on EES. Anyhow the pilot project showed that taking ten fingerprints at the border for all third country nationals is not feasible. For border control purposes there is no need and no time for collecting additional data than the ones on the passport. The data retention period to facilitate border control is however long enough (5 years) to meet the expectation from LES.

2.4.4. Authorities (in the generic sense)

MS authorities are consulted as part of the usual decision making process on legal proposals. However some authorities, essentially local ones, used the widely advertised public consultation to express their opinion.

Opinions expressed. On biometrics, the majority of authorities were in favour of using two biometric identifiers, as doing so reduces risk. Authorities also favour the existence of provisions that facilitate border crossing. Some of the opinions were expressed by authorities from regions where part of the economy rests on trade with neighbouring non-Schengen countries. Therefore, there is an expectation for having strong controls (security) but without creating a burden on travellers. The need to have a longer data retention period is understood. However it is unclear whether this longer duration is proposed in order to meet expectations of law enforcement authorities or to facilitate the process.

Whether/how comments were taken into account: The preferred solution meets the opinions expressed by local authorities although a longer data retention period is justified for other reasons than those expressed in the respondents' answers.

2.4.5. Carriers and operators of transport infrastructures

The informal meeting on 28 May 2015 was attended by seven organisations. Public consultation responded by 11 carriers and operators of transport infrastructures.

Opinion expressed. At the informal meeting carriers also essentially asked questions to understand the proposal. The public consultations showed a strong support for the use of biometrics and measures aimed at facilitating border control. Carriers and transport operators were the only group of stakeholders that made the link between a longer data retention period and facilitation of the process for a larger group of travellers. The majority of carriers consider that it is unfair that they are responsible for taking back travellers refused at the border.

Whether/how comments were taken into account: Most of the comments made correspond to what the new proposal contains. It also includes the use of a web-service where carriers will receive the answer that meets their current obligation ("Is this traveller eligible for transportation till destination?"). However there is no change to carrier's current obligations as this is outside the remit of border control.

Comments of airport and seaport operators are taken into account by using biometric identifiers that put a low burden on border crossing time and protects existing investments. Further the new legal package enables explicitly the use of self-service kiosks.

2.5. Survey from the Fundamental Rights Agency

In the framework of the eu-LISA Pilot, FRA has investigated the views of travellers on a number of fundamental rights (dignity, respect for private life and family life, right to protection of personal data, non-discrimination) related to the use of biometrics in the context of border control. FRA interviewed 1.234 randomly selected third-country nationals at BCPs.

The results show that the majority of persons are comfortable with providing biometrics when crossing the border and don't perceive the provision of biometrics in the context of border control as compromising their right to privacy and to dignity. Trust in the reliability of biometric technologies is also high. The majority of respondents believe that only adults (i.e. 18 years of age onwards) should be allowed to go through biometric checks.

The travellers, however, expressed concerns with regards to the proper functioning of the system (i.e. more than half of the respondents believe that they will not be able to or do not know if they will be able to cross the border if the system malfunctions). Similar concerns emerged in relation to the right to rectify the data, where half of the respondents believed that if there was a mistake in the data, it would be difficult to correct.

The results of the survey show that third-country national travellers take data protection seriously and more than 80% consider it important to be informed on the purpose of collecting and processing their personal data.

There is a widely held view that automated systems could cause less discrimination – for example on the basis of race or ethnicity – as compared to checks carried out in person by border guards. This might be based on the assumption that machines entail a lower risk of discriminatory profiling compared to checks by border guards.

Key findings

Acceptability of technology: Approximately 1 in 10 travellers feel very uncomfortable with providing fingerprints or facial image, while 38.7 and 39.6 percent respectively feel 'comfortable' and 'very comfortable'. The percentage of travellers feeling very uncomfortable is considerably higher for iris-scan: 21.3 percent chose this answer. This tendency is visible across all BCPs, across all regions of citizenship of travellers, gender and age groups.

Private life: 46.9% and 42.9% believe that providing fingerprints and facial image respectively is not intrusive to their privacy. Attitudes towards iris-scan are different, with a higher percentage (38.6%) believing that letting their iris be scanned is intrusive or very intrusive to their privacy.

Dignity: Almost one third (32.3%) believe that letting their iris be scanned might be humiliating, one in four (26.8%) finds that that providing facial image might be humiliating and slightly more than a fifth (22.8%) that providing fingerprints might be

humiliating. However, these results have to be put in relation with the fact that 15.9% of respondents are considering that any kind of border check is humiliating.

Accuracy of the data: Close to half of the respondents trust that biometric technologies will always properly identify who they are but there is a great amount of uncertainty about how well biometric systems work to properly identify people (20% have chosen the middle value).

Data protection: 83.9% of the respondents strongly agree, or agree, that it is important to be informed on why their biometric identifies are collected and used. Half of the respondents (50.8%) believe that their data could not be easily corrected in case of error. Only 17.2% believe that the data could be easily corrected. The majority (75%) of travellers trust that only legally authorised people can access biometric data. 55% of travellers agree or strongly agree with data access for law enforcement purpose.

Automated border control systems: Respondents were asked if they were to choose, whether they would go to a machine or a border guard. Approximately one third of the respondents reported they would go to a machine and another third reported they would go to a border guard. For one in every four respondents, it makes no difference. A large proportion of respondents (61%) consider that automated systems cause less discrimination than border guards because of the absence of human judgement selecting passengers for further checks.

Whether/how comments were taken into account: The results of the FRA are taken into account in the new proposal by including provisions for correction and redress of data to the data subjects. Otherwise the study results confirm the acceptability of biometrics and a wider support for fingerprints and facial image as opposed to the iris scan.

2.6. Results of the public consultation on Smart Borders⁶

2.6.1. Introduction

The objectives of the public consultation were:

- to collect views and opinions on the policy options, their likely impact and hence testing existing ideas and options with all stakeholders and the general public;
- to gather new ideas and general relevant knowledge and
- to test existing ideas and analysis.

For this purpose, the public consultation was published online on 29 July 2015 on a dedicated Commission website⁷ during 12 weeks (i.e. until 29 October 2015).

Seeking the highest number of participants possible, representatives of the civil society, carriers, and operators/organisations of the transport, tourism and transport infrastructure sectors were directly informed of the publication of the consultation by the services of the Commission. The information was also posted on Twitter and advertised on the Commission's general website and on the websites of EU Delegations abroad. Information on the consultation was furthermore disseminated by the the Fundamental Rights Agency (hereinafter *FRA*), which informed civil society actors, and eu-LISA, which shared information with the Members and Observers of the Management Board.

The public consultation consisted of four different questionnaires targeting respectively:

1. individuals;
2. organisations (non-governmental, civil society organisation, academia, research, social partner, interest group, consultancy, think-tank...);
3. public authorities;
4. carriers, transport and tourism operators/organisations and transport infrastructure operators/organisations.

The four questionnaires targeting the four different groups followed the same logic and presented the same structure:

1. General information;
2. The use of biometric identifiers;
3. The processes for accelerating the border crossings of non-EU citizens;
4. The data retention period;
5. The law enforcement access to the data (hereinafter *LEA*);
6. The consequences of the abolition of stamping of passports of non-EU citizens crossing the Schengen borders.

In total 101 responses were received. 62 replies came from individuals, 14 from organizations, 14 from public authorities and 11 from carriers, transport and tourism operators/organisations and transport infrastructure operators/organisations.

⁶ http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/docs/consultation_030/results_of_the_public_consultation_on_smart_borders_en.pdf

⁷ http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/consulting_0030_en.htm

2.6.2. General information

As regards individual persons, 9 replies were supplied by non-EU citizens. From these 9 non-EU citizens, three were holding a residence permit of a member state (hereinafter *MS*) while the remaining five held a multiple-entry visa. Five of the third country nationals (hereinafter *TCN*) who participated in the consultation could be considered as frequent travellers (i.e. they travel at least 3 to 5 times a year to the Schengen area).

As regards the organizations, the 14 replies represent organizations of different nature, such as international human rights associations, associations of commercial undertakings or churches.

As regards public authorities, 7 replies out of 14 came from Finland, the remaining replies were submitted by different national authorities (from the Netherlands, France, Estonia and Greece) and European organisations. The European organisations who replied to the consultation were the European Data Protection Supervisor (hereinafter *EDPS*) and the European Union Border Assistance Mission to Moldova and Ukraine (*EUBAM*).

As regards carriers, transport and tourism operators/organisations and transport infrastructure operators/organisations, from the 11 replies, 8 contributors are carriers or transport operators and 3 are transport infrastructure operators.

2.6.3. Presentation of the results

The use of biometric identifiers

Summary results:

The necessity to use biometrics was confirmed by the majority of the respondents from all the groups except “Organisations”.

“Individuals” and “Public authorities” showed their preference for the combination of the identifiers (FI and FP), whereas “Carriers” showed their preference for FI only.

Main advantages of biometrics that were mentioned: data reliability, certainty and speed of checks and security.

Main drawbacks mentioned: perceived intrusiveness of biometrics, issues related to proportionality of the measures, data security and a potential breach of fundamental rights

After a short introduction into the 2013 Smart Border proposals, the participants were invited to share their opinion on the preferred kind of biometric identifiers.

Individuals

A majority of the individuals (58%) were of the opinion that some kind of biometrics is necessary with a preference for the combination of fingerprints (hereinafter *FP*) and facial image (hereinafter *FI*).

Those who preferred the 'no biometrics' option were mainly concerned with the perceived intrusiveness of biometrics, the proportionality of the measures, the risks of a potential

data misuse or theft and questioned the need of biometrics on top of the information already included in the travel documents. The supporters of the combination of FP and FI mainly argued that this would bring a better data certainty and security. When explaining their choice for FP only or for FI only, the majority of the respondents highlighted their perception that the respective biometric identifier was less intrusive and also indicated the enhanced security and speed of checks.

It is worth mentioning that 7 out of the 9 participating TCN expressed their positive views on the use of one of the proposed solutions comprising the biometric identifiers. When asked if giving FP would discourage them from travelling to the Schengen area 4 out of 9 replied positively. Moreover, 3 positive replies were given to the similar question with reference to the FI.

When asked about the link between the biometric identifiers and reliability of border checks 43% of the individual respondents agreed with the improved reliability and 28% were of the opposite view. The majority of those in favour mentioned the security aspect in their justification whereas those with the opposite view highlighted the potential privacy infringements and the potential delays.

Organisations

As regards the organisations, 6 out of 14 respondents preferred the combination of FP and FI arguing that the use of two biometric identifiers was more reliable than the use of one. 8 participants replied negatively to the use of biometric identifiers, indicating in most cases a potential breach of fundamental rights and a potential threat to data security.

When asked about the link between the biometric identifiers and reliability of border checks 8 out of 14 participants agreed with the improved reliability stating that the checks using biometric identity verification are more reliable than the checks relying on “human-based” visual identification. The respondents considering that the use of biometric identifiers would jeopardize the reliability of border checks raised the issues of data security and “false-positive” incidents.

Public authorities

As regards the public authorities, a majority of the respondents (11 out of 14) favoured a combination of FI with a limited number of FP. The reasons indicated were a higher certainty of identification, an enhanced security and a lower error rate.

9 out of 14 public authorities supported the enhanced reliability of border checks if biometric identifiers were to be used. The only negative opinion came from the EDPS which stated that the need to use biometrics has still to be demonstrated and that an evaluation period is needed prior to the introduction of biometrics. They also expressed concerns stemming from the perceived intrusiveness of biometrics and its potential impact on the respect of the private life.

Carriers and transport infrastructure operators

As regards carriers and transport infrastructure operators, 7 respondents supported the necessity to use biometric data, with a clear preference for the use of FI alone or in combination with FP. The need to use a biometric identifier was rejected by 4 respondents. The use of the combination of FI and FP was considered as more secure, whereas FI is considered faster and easier by most of the respondents. Among those who

rejected biometric identifiers in several cases the arguments were of a practical/operational nature (e.g. buses are not duly equipped to perform such verifications). Other respondents who replied negatively mentioned their perceived limitation for air passengers or their preference for alphanumeric data as it would be more convenient for their passengers.

The majority of the respondents supported the enhanced reliability of border checks if biometric identifiers were to be used. They considered that the use of biometrics would lead to a better security and reliability of the border checks and would reduce the time spent for these checks. The necessity of reaching good quality for the biometric data was also highlighted.

Process to accelerate border crossing for non-EU Citizens

Summary results:

The necessity to accelerate border crossing for the TCN was supported by the majority of the respondents from all the groups. The majority of the respondents supported both the 2013 RTP proposal and the second simplified option without prior application (in both cases the support among the TCN was above the average).

Main advantages mentioned of the 2013 RTP proposal: time saving, mobility improvement, higher security due to pre-vetting, support to the EU economy.

Main drawbacks mentioned of the 2013 RTP proposal: segregation of TCN travellers, fees, security of the automated controls, excessive data collection and high costs.

Main advantages mentioned of a system without prior application: efficiency, celerity of the process and simpler procedure.

Main drawbacks mentioned of a system without prior application: fear that the automated controls would not be secure enough, fear of a breach of privacy, potential data hacking or potential errors in the biometric technology.

In this part of the survey, after having recalled the principle elements of the 2013 RTP proposal, the question was asked if there was a need for a process to accelerate the border crossings of non-EU citizens at the Schengen area's external borders. In the second part, the participants were asked to answer questions related to their preferences on the different options for facilitation as well as on their potential outcome.

Individuals

More than half of the participants (53%) replied that there was a need to accelerate the border crossing⁸.

Concerning the enrolment and facilitation process as envisaged in the 2013 RTP proposal, when asked if the RTP option should be available to non-EU citizens, 61% of the respondents replied positively (including 8 out of 9 of the participating TCN). Among supporters, the main reasons for implementing such facilitation process would be time

⁸ Including 6 out of the 9 non-EU citizens who participated in the consultation.

saving and mobility improvement⁹. 39% of respondents argued against an RTP. The main arguments against were that the process would segregate the travellers into classes, that it would be unfair to pay for the accelerated border crossings and the concerns surrounding the security of checks performed in the automated controls.

The personal interest in the scheme was confirmed by 7 out of 9 TCN participants. The replies highlighted the necessity for a reduction of time for border checks and the wish to use automated border gates. However, some concerns were raised concerning the security of the stored biometric data.

Concerning the use of self-service kiosks¹⁰, 61% of all respondents agreed that the self-service kiosks should be available for both the travellers holding a short-stay visa and the visa-exempt travellers whose data has been registered during a previous journey (if the retention period has not expired yet). The main argumentation provided by the respondents indicated efficiency gains and an acceleration of the border crossing process. The remaining 39% were against. The negative replies brought up the fact manual checks are sufficient, the fear that the automated controls would not be secure enough, the fear of a breach of privacy, potential data hacking or potential errors in the biometric technology.

When asked about the participants' opinion on the use of self-service kiosks, 7 out of 9 TCN confirmed their personal interest in the scheme. The main reason was the reduction of the time spent for border checks and, to a lesser degree, the fact the procedure did not require prior application.

If nevertheless the application was required in order to be able to profit from the facilitation (RTP proposal) 5 TCN confirmed that they could apply both online or personally at a consulate or at the border crossing point. In 3 cases online application was indicated. If fees were to be charged for the RTP the opinions were equally shared among those who agreed, those who were against and those do not have an opinion or are not sure. Concerning the maximum fee that could be accepted to benefit from the procedure, out of 3 positive replies the average amount was 40 euros.

One of the facilitation solutions to accelerate border crossing would be the use of self-service kiosks at the border crossing. After having explained the operations that the TCN travellers will have to carry out when using these kiosks, the TCN were asked if they would be interested in using them. The replies showed the acceptance rate of two thirds, with 2 participants not having opinion.

Organisations

More than half of the participants (53%) agreed that there was a need for a process to accelerate border crossings by non-EU citizens at Schengen area's external borders. A large proportion (5 out of 14) did not position itself regarding this issue.

When asked if the RTP process should be available to the non-EU citizens, 11 respondents agreed and highlighted the speed and gain on efficiency of checks, whereas

⁹ Other replies indicated also that it would constitute a better tool to tackle the growing passenger flow, to level the non-EU citizens' rights with those of the EU citizens and reported a good experience with the existing facilitation systems (Privium and Parafe).

¹⁰ To be used by the TCN already registered in the VIS system or, if not subject to the Schengen visa, those TCN whose data was still available in the EES.

the opponents indicated the risk of violation of the fundamental rights and of unjustified data collection.

Concerning the use of self-service kiosks, 11 of the respondents replied positively. The supporters brought up mainly time saving whereas opponents mentioned the potential infringement of the privacy due to the collection of the biometric data.

Then, the participants were asked if they envisaged any difficulties for the travellers, should the self-service kiosks be implemented. 7 of them replied positively and evoked potential problems if the devices are not sufficiently user friendly or if no assistance is provided to the traveller, especially at the beginning.

Public authorities

10 out of 14 respondents affirmed that there is a need for a process to accelerate border crossings by non-EU citizens at the Schengen area's external borders. When asked if the RTP process should be available to the non-EU citizens, 11 out of 14 respondents replied positively, 9 of them agreed that offering facilitation to its beneficiaries will effectively contribute to the overall facilitation of border crossings. 4 indicated that they considered the process as secure since it included pre-vetting. Additional arguments included positive economic impact for business (particularly for frequent travellers) and the necessity to limit a potentially higher procedural burden on border guards.

Concerning the use of self-service kiosks, 10 out of 14 respondents replied positively. Subsequently 7 of them agreed with the statement that facilitating border crossing for a wide range of users could contribute to the overall facilitation of border crossing. A single negative reply from the Estonian Ministry of Interior highlighted security concerns and the difficulty to introduce self-service kiosks at land borders. Some participants called for a balance of the security and the facilitation of the process to be maintained, for the use of web or mobile apps for the pre-checking and for the benefits of maintaining the RTP. While recognizing its increase in the process speed, it was highlighted that the use of self-service kiosks should be carried out under the supervision of the border guards. Lastly, the facilitation efforts for some travellers should not turn out to be detrimental for some other groups (e.g. for local traffic).

Carriers and transport infrastructure operators

10 out of 11 participants replied positively, in 8 cases indicating a strong support. When asked if the RTP process should be available to the non-EU citizens, 9 respondents agreed indicating as advantages: more expedite process, better security and positive impact on business. A bus operator wished that the accelerated procedure were available for all passengers as it was a condition for quicker border crossing of the entire bus. Among the 2 negative voices, the high costs of the system were pointed out. A cruise operator highlighted the need of a system that could tackle thousands of customers arriving in a short period of time.

Concerning the use of self-service kiosks, 10 respondents replied positively. The most frequent justification given by the supporters pointed out again to better speed for border crossing process (also due to the use of self-service kiosks) and a positive impact for the crew members who were already registered in VIS. The main requirement for the system that was highlighted was that it must be simple to use. The only negative reply pointed out towards scarcity of space for installing the kiosks.

Employing technology in the pre-check stage (self-service kiosks) would limit the waiting time. The procedures should be as light as possible both for the passengers and for the carrier's personnel. All types of borders should be taken into consideration (land, sea and air).

Data

Summary results:

The opinions concerning the length of the retention period were divided. For non-overstayers: the majority of "Individuals" and "Carriers" preferred 181 days or longer, the majority of "Organisations" were opposed to any type of data retention and the majority of "Public authorities" favoured a retention period longer than 181 days.

Reasons for 181 days retention period: sufficient to calculate the duration of the authorised stay, lesser impact on privacy.

Reasons for a shorter retention period (less than 181 days): risks of errors in the biometric identifiers (i.e. linked to a general reluctance to use biometric identifiers).

Reasons for an extended retention period (more than 181 days): faster border controls.

For overstayers: the majority of "Individuals" preferred shorter than 5 years or 5 years, the majority of "Organisations" less than 5 years. The majority of "Public authorities" preferred 5 years period or longer. "Carriers" were not consulted on overstayers.

Reasons mentioned to maintain the 5 years retention period: coherence with the validity of biometric passports and VIS.

Reasons mentioned for a data retention period shorter than 5 years: data protection and data collection concerns, erroneous data correction, reasons for overstay to be taken into account.

Reasons mentioned for a data retention period above 5 years: security reasons, better control of overstayers, improved mobility, data retention time used in other countries.

The third area that was consulted concerned the length of the EES data retention period. First, the data retention rules as envisaged in the 2013 proposals were presented and explained, and then with a reference to the revised proposal, the participants were asked to express their opinion on the length of time that the data could be kept after its collection at the entry/exit of the Schengen area's external borders. The proposed reply options were equally explained.

Individuals

Concerning the data retention period for the Entry/Exit System for non-overstayers (see the chart 4 below), 45% of participants favoured the option with a maximum data retention period of 181 days starting from the exit date (it was explained that 181 days is sufficient to calculate the duration of authorised short stays in the Schengen area), 31%

agreed with a longer retention periods in exchange for faster border controls, and 24% did not agree with either of the proposed replies.

The respondents who answered “other”, could further explain their preferences in an open question, 8 individuals explained that they would opt for a much shorter or no data retention period whereas 2 participants explained that they would opt for a longer/unlimited data retention period. One of respondents indicated maximum data retention of 181 days, increasing the share of those who chose this reply to 47%. Some of the participants appear to have misunderstood the link between the retention period and the rules for the short stay in the Schengen area.

For a similar question on data retention period but concerning overstayers, half of the participants (50%) voted for a data retention period shorter than 5 years. The reasons for favouring a shorter retention period were mainly related to data protection concerns, a general reluctance to data collection or a perceived difficulty to correct / update wrong or obsolete data. Some stated that the reason for overstay should be taken into account and that for a justified or very short overstay, a period of 5 years of data retention would be disproportionate. The majority of the supporters of a period of data retention longer than 5 years explained that such an option would lead to an improved security and to a better control of overstayers. For one of the respondents it would lead to better mobility. The example of longer data retention periods in other countries was also mentioned. One respondent wondered why the 5 years’ period was proposed. Those respondents who agreed with the 5 years period did not present additional arguments in favour of their choice.

Organisations

Concerning the data retention period for the Entry/Exit System for non-overstayers, the majority of the participants replied “other”, and provided their main argumentation for their opposition to the proposed data retention period: that the choice of a longer data retention period should be optional for facilitation reasons and that it might bring up risks of “false-positive” incidents. For the question on data retention period which concerned overstayers, the majority of the respondents preferred a data retention period shorter than 5 years, their choice justified by the risk of profiling and of misuse of data. The supporters of a longer data retention period justified their opinion mainly based on security concerns.

Public institutions

Concerning the data retention period for the Entry/Exit System for non-overstayers, 8 out of 14 participants agreed with a longer data retention period, with the aim of speeding up border controls by avoiding a re-enrolment into the EES, whereas 3 replies indicated that the retention period of 181 days is sufficient to calculate the duration of authorised short stay in the Schengen area and has a minor impact from a privacy protection perspective. For the question on the data retention period for overstayers, 7 out of 14 participants agreed with the proposed 5 year period following the last day of the authorised stay while 4 of the participants favoured a data retention period longer than 5 years. The detailed explanations that were submitted included a view that the 5 year data retention period would be equal to the 5 year validity of the biometric passports and that the data retention period should be in line with VIS. Those indicating data retention periods longer than 5 years had in mind LEA purposes. The EDPS in its contribution requested further justification for a 5 year retention period. Another issue mentioned was the need to correct the EES data once the stay was extended by the authorities.

Carriers and transport infrastructure operators

The replies received showed a strong support (8 out of 9 replies) for data retention periods longer than 181 days. Only 1 reply favoured a data retention period of maximum 181 days.

”Carriers” were not consulted on overstayers.

Law Enforcement Access (LEA) to the Entry/Exist System

Summary results:

The opinions on the law enforcement authorities' access to the future EES system were divided. Among “Individuals” and “Carriers” there were slightly more opponents than supporters, “Organisations” were equally divided and a majority of “Public authorities” supported LEA.

Reasons mentioned for granting access: security, detection, prevention and investigation of criminal and/or terrorist offences, international character of the threats.

Reasons mentioned against granting access: lack of proportionality, lack of trust, potential errors leading to the criminalisation of foreigners, insufficient data security, threat to the privacy.

The safeguards that were indicated concerned mainly the limitation of the searches, their scope and their access, as well as the necessity to authorise LEA access by courts or independent administrative bodies.

The subject of the access of law enforcement authorities to the data was already included in the 2013 proposals. The 2013 proposals suggested that the option of access of law enforcement authorities to the data contained in the system should be evaluated two years after the entering into operation of the system. With the increase of the security concerns and the experience obtained in other large scale IT systems, the Commission envisaged proposing such access from the start of the system while respecting the principles of necessity, appropriateness and proportionality.

Individuals

When asked, 40% of the respondents agreed on granting law enforcement authorities' access to the EES for the purpose of preventing, detecting or investigating terrorist and/or serious crime offences from the start. 44% of the respondents were against, 11% considered that the matter should be reconsidered 2 years after the implementation and the remaining 5% did not express an opinion. The respondents who agreed with granting the access from the start justified the need for such access from a security perspective.

The respondents who replied that no LEA should be granted to the EES mainly considered that such measure would not be proportionate. Some respondents highlighted the lack of trust, the potential errors that could lead to the stigmatisation of foreigners, or the insufficient level of data security.

The participants were then asked to choose from the list of conditions aimed at mitigating the impact on the fundamental rights, should LEA to the EES be granted. Having a

choice among numerous conditions and safeguards which were proposed, the 3 most popular replies were: (1) searches should only be possible in specific cases under clearly defined circumstances (excluding searches on a systematic basis) (35 replies), (2) a court or an independent administrative body should verify in each case if the required conditions for consulting the EES for law enforcement purposes are fulfilled (31 replies) and (3) access should be limited to the prevention, detection or investigation of terrorist offences or other serious criminal offences (27 replies).

Organisations

Out of 12 replies that were received in this area, there were 5 respondents supporting the access and 5 opposing it. The supporters highlighted a security need, whereas the opponents did not see a need for such access bringing up previously mentioned arguments: the threat to privacy and other fundamental rights and the criminalisation of non-EU citizens. The participants were then asked to choose from the list of conditions aimed at mitigating the impact on the fundamental rights, should LEA be granted to the EES. Having a choice among numerous conditions and safeguards which were proposed, the 3 most popular replies concerned: (1) a court or an independent administrative body should verify in each case if the required conditions for consulting the EES for law enforcement purposes are fulfilled (8 replies), followed by (2) access should be limited to the prevention, detection or investigation of terrorist offences or other serious criminal offences (7 replies) and (3) there should be reasonable grounds to consider that the specific envisaged consultation of the EES data will substantially contribute to the prevention, detection or investigation of any terrorist and/or serious criminal offences (7 replies). One contributor mentioned the need to avoid data transfer to third countries.

Public authorities

10 out of 14 participants supported granting LEA, as they considered it justified for security reasons. One respondent (the EDPS) preferred that LEA to the EES would be evaluated two years after the implementation of the EES and requested the Commission to carefully evaluate evidence presented by the MS. The reasons mentioned in support of LEA to EES data were that the access will substantially contribute to the detection, prevention and investigation of criminal and/or terrorist offences. Since the organised crime and terrorism have an international character, such access is necessary for the security of the EU citizens. An EU arrest warrant was evoked as a base for the definition of crimes for which investigation access to the EES should be granted.

The participants were then asked to choose from the list of conditions aimed at mitigating the impact on the fundamental rights, should LEA was to be granted access to the EES. Having a choice among various conditions and safeguards the most popular replies were: (1) access should be limited to the prevention, detection or investigation of terrorist offences or other serious criminal offences (7 replies) and (2) there should be reasonable grounds to consider that the specific envisaged consultation of the EES data will substantially contribute to the prevention, detection or investigation of any terrorist and/or serious criminal offences (7 replies). Additional comments pointed at the utility of the national EES systems, the necessity to respect fundamental rights, the necessity to establish the rules of data information sharing among the law enforcement authorities from the different MS, and maintaining the envisaged LEA as a secondary objective of the future Smart Borders package.

Carriers and transport infrastructure operators

The replies received were not conclusive, as 3 respondents supported the access, 4 either opposed or did not see the need and 3 did not have an opinion.

Stamping

Summary results:

The majority of non-EU citizens confirmed the need for having access to the information provided by the stamps, mainly to be able to respect the 90/180 days rule of stay. If stamps were discontinued some of them favoured the creation of an online website and others the delivery of a ticket when crossing the border. A majority of the replies received from “Organisations” agreed with such need. “Public authorities” indicated the need to grant access to several national services or service providers. As for “Carriers”, the majority of those directly impacted by the abolition of stamping confirmed the need to access the information previously provided by the stamp via alternative solutions.

The paragraph began with the explanation of the main purpose of stamping passports (which is the location and date of entry/exit) and based on this information, the calculation of the authorised length of a short stay. The main disadvantages of that method are the cumbersome calculation of the length of stay and the potential forgery of stamps. It was reminded that the Commission already proposed to abolish stamping in their 2013 proposals.

Individuals

When asked about the consequences of the abolition of the stamping of passports of the non-EU citizens crossing the external borders of the Schengen area, 7 out of 9 of the TCN who participated in the consultation confirmed the need to access to the information that the stamps currently provide. The main justification concerned certainty of respecting the 90/180 days rule during a stay or future stay. Some also indicated a need to prove their absence from the country of residence.

If stamps on passports were to be discontinued, the preferred alternatives to access the information that stamps currently provide (i.e. data and location of entry/exit to/from the Schengen area) were: the creation of an online website giving access to the relevant information (mentioned in 3 replies) and the delivery of a printed receipt when crossing the external borders (mentioned in 3 replies).

Organisations

If stamps on passports were to be discontinued, 9 out of 14 participants expressed as their opinion that the TCN should have access to the data that is currently provided by the passport stamp. On this issue, 1 respondent considered that TCN should not be granted access to this information and 4 did not have an opinion.

Public authorities

If stamping of passports were to be discontinued, the majority of respondents (8) agreed that public authorities other than border management authorities should have access to

the information currently provided by stamps (i.e. data and location of entry/exit to/from the Schengen area). Three respondents had no opinion and one was against.

When asked which public authorities would need access to this information and for which purposes the participants indicated: the police (identification of TCN without documents), the social services (to identify the welfare applicants), immigration authorities (to identify asylum seekers), the labour inspection (to determine legality of stay), the consulates (to verify visa applicants), the carriers (to check if a TCN fulfils the conditions for entry) as well as the accommodation providers (to check the legality of stay).

Carriers and transport infrastructure operators

If a web service was made available to carriers to enable them to verify if a single entry visa has not been used, 6 out of 10 confirmed this solution as necessary and sufficient. Some participants who replied negatively explained that in their activities they were not concerned by checking the documents.

As an alternative to the above presented solution, a carrier proposed a SMS service which would confirm the validity of a visa based on a visa sticker number or an integration into the into the departure control system of airports. A cruise operator highlighted the importance of the information concerning the time their passengers can stay in the Schengen area.

Comments

All the respondents from “Organisations”, “Public authorities” and “Carriers” had the opportunity to submit their additional comments and suggestions under section 7: “Comments/other questions” of their respective questionnaires. Their comments and suggestions are directly available in their respective contributions.

3. ANNEX 3: PRACTICAL IMPLICATIONS OF THE INITIATIVE FOR THE AFFECTED PARTIES

This annex describes the implications of the initiative for the affected parties and in particular the implications of the preferred solution.

The description of the practical implications of the initiative (column 2) refrains from explaining the operations that are not visible to the affected party. A more detailed description of the future process at the border at entry and at exit is described in annex 8 - New Smart Border processes.

The term "practical implications" is also understood as only dealing with the mainstream cases.

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
<p>EU citizens</p> <p>Number of persons concerned : 550 million</p>	<p>Entry and exit of the Schengen area is not modified at all. There are no practical implications of the initiative for EU citizens.</p>	<p>Same as in previous column.</p>
<p>TCN-VE</p> <p>Third-country nationals coming from countries that are exempted of the obligation to obtain a visa.</p> <p>Number of persons concerned: 39 million persons in 2020 (start of EES operations)</p>	<p>At first entry into the Schengen area or at an entry after the period of retention of his/her data in EES:</p> <ul style="list-style-type: none"> • Border control will be done as today but his/her individual file will be created by having the data from the biographical page of the passport (or from the chip of an electronic passport) stored in the EES and biometrics taken. This additional step will take more time depending on the biometrics used and on the congestion (or not) and organisation of the border control post. <p>At return visits into the Schengen area during the retention period of his/her data in EES:</p> <ul style="list-style-type: none"> • Border control will be done as today and the date and place of entry into the Schengen area recorded in the EES. His/her correspondence with the identity stored in EES will be checked by means of a biometric verification. This additional step will take less than 15 seconds and can be done concurrently with other border control steps and 	<p>At first entry into the Schengen area or at an entry after the 5 years (= the retention time) since the last exit:</p> <ul style="list-style-type: none"> • The biometric referred to will consist of 4 fingerprints and a facial image taken with a digital camera. • The time this would take is estimated at 30 seconds plus the waiting time dependent on congestion (or not) and organisation of the border control post. • The traveller will also be able to prepare border clearance him/herself at a kiosk in the border crossing points equipped with this (this is Member State dependent) followed by a face-to-face time with the border guard. <p>At return visits into the Schengen area within the 5 years period since his/her last visit:</p> <ul style="list-style-type: none"> • The biometrics referred to in the previous column will consist of 1, 2 or 4 fingerprints checked vs the biometrics stored in EES, or the picture taken with a digital camera compared with the picture stored in EES. • The traveller will also be able to prepare border clearance

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	<p>hence should not slow down the border control process.</p> <ul style="list-style-type: none"> The remaining duration of stay in the Schengen area will be provided to him/her: display, printed form, orally. <p>At exit:</p> <ul style="list-style-type: none"> Border control will be done as today and the date and place of exit from the Schengen area recorded in the EES. His/her correspondence with the identity stored in EES will be checked by means of a biometric verification. This additional step will take less than 15 seconds and can be done concurrently with other border control steps and hence should not slow down the border control process. <p>General: the traveller's passport will not contain Schengen entry/exit stamps anymore.</p>	<p>him/herself at a kiosk in the border crossing points equipped with this (this is Member State dependent) followed by face-to-face time with the border guard.</p> <p>At exit:</p> <ul style="list-style-type: none"> The biometrics referred to in the previous column will consist of either 1, 2 or 4 fingerprints checked vs the biometrics stored in EES, or the picture taken with a digital camera compared with the picture stored in EES. The traveller will also be able to use an e-gate in the border crossing points equipped with this (this is Member State dependent). <p>General:</p> <p>If the traveller wants to know the remaining duration of authorised stay he/she needs to access a web service, enter passport number and issuing country, answer a question related to his/her last trip, enter the intended entry and exit data and he/she will receive a YES or NO answer. This is only necessary if the traveller stays frequently in the Schengen area as the rules on short stay (90 days in any period of 180 days) are not affected.</p>
TCN-VH Third-country nationals	Border control will be done as today including the verification by means of a biometric check of 1, 2 or 4 fingers that the visa belongs to the traveller (this is part	At first entry into the Schengen area or at an entry after the 5 years (= the retention time) since the last exit:

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
<p>coming from countries that are required to obtain a visa.</p> <p>Number of persons concerned: 24 million persons in 2020 (start of EES operations)</p>	<p>of the control on visas).</p> <p>At first entry into the Schengen area or at an entry after the period of data retention in EES:</p> <ul style="list-style-type: none"> • In addition, a picture will be taken with a digital camera and the picture stored in the EES. This additional step will take less than 15 seconds and can happen concurrently with other steps. <p>At return visits into the Schengen area during the retention period of his/her data in EES:</p> <ul style="list-style-type: none"> • No additional steps are required in addition to the one required. <p>At exit:</p> <ul style="list-style-type: none"> • Border control will be done as today and the date and place of exit from the Schengen area recorded in the EES. His/her correspondence with the identity stored in EES will be checked by means of a biometric verification. This additional step will take less than 15 seconds and can be done concurrently with other border control steps and hence should not slow down the border control process. 	<ul style="list-style-type: none"> • The traveller will also be able to prepare border clearance him/herself at a kiosk in the border crossing points equipped with this (this is Member State dependent) followed by face-to-face time with the border guard . <p>At return visits into the Schengen area within 5 years since his/her last visit:</p> <ul style="list-style-type: none"> • The traveller will also be able to prepare border clearance him/herself at a kiosk in the border crossing points equipped with this (this is Member State dependent) followed by face-to-face time with the border guard. <p>At exit:</p> <ul style="list-style-type: none"> • The biometrics referred to will consist of either 1, 2 or 4 fingerprints checked vs the biometrics stored in EES, or the picture taken with a digital camera compared with the picture stored in EES. • The traveller will also be able to use an e-gate in the border crossing points equipped with this (this is Member State dependent). <p>General:</p> <p>If the traveller wants to know the remaining duration of authorised stay he/she needs to access a web service, enter passport number and issuing country, answer a question related</p>

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	<p>General: the traveller's passport will not contain Schengen entry/exit stamps. Also the single/double entry visas will no longer be stamped.</p>	<p>to his/her trip, enter the intended entry and exit data and he/she will receive a YES or NO answer. This is only necessary if the traveller stays frequently in the Schengen area as the rules on short stay (90 days in any period of 180 days) are not affected.</p>
<p>Air, land and sea carriers</p> <p>Number of carriers on travel routes to and from Schengen area estimated to a few thousands.</p>	<p>Carrier's obligations do not change. In practice, they will continue to check that each traveller carries with him the required documents to enter the Schengen area. Like now, carriers therefore will check whether each third country national has a passport and a valid visa.</p> <p>The items the carrier has to check are :</p> <ul style="list-style-type: none"> • whether the passport is valid, • whether a multiple-entry visa is still valid by means of the date mentioned on the sticker in the passport, • whether a single or double entry visa has been used by accessing a web-service. <p>Carriers will be granted credentials to access a webservice that will answer the question: "Is this traveller eligible for transportation till destination?" on the basis of the passport number and the issuing country.</p> <p>The web-service will only give a Yes/No answer when at least one day of stay is left when the date of entry is</p>	<p>Same as in previous column.</p>

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
<p>Airports and seaport operators</p> <p>Number of operators affected in the Schengen area are estimated between 100 and 150</p>	<p>given. The webservice will only access a report generated daily by EES. No transfer of data to carriers will occur.</p> <p>Operators or airports and seaports will face a situation where border crossing in and out of the Schengen area follows a modified process and at the same time contains opportunities to happen in a more automated way.</p> <p>Border clearance at entry for visa-exempt travellers has a risk to be more time-consuming as an enrolment step is added at first entry (or re-entry after data retention expired). There is much less risk of added duration for verification during return visits within the data retention period.</p> <p>Duration of border clearance at entry for visa-required travellers is not going to be significantly impacted by EES.</p> <p>Duration of border clearance at exit can be shortened since the opportunity exists to have most of the steps automated.</p> <p>Airports where a large share of travellers is visa-exempt need to organise the new border clearance process as efficiently as possible. If this was not the</p>	<p>Compared to the general situation described in the previous column, the preferred solution has the following practical implications:</p> <ul style="list-style-type: none"> • As the data retention period is proposed to be 5 years, the proportion of visa-exempt travellers who need to be enrolled will be low once the system is in operation. During the first one or two years of operations however there will be a significant proportion of visa-exempt travellers who will have to be enrolled. • The biometric identifiers chosen (4 fingerprints and a facial image) only require on average 30 seconds for being captured and are not sensitive to environmental conditions. • The possibility of automating part of the border clearance process (use of self-service kiosk) at entry creates the opportunity to avoid that travellers spend more time at the border and that therefore more space is required as compared to the current situation. • The possibilities for automating the major part of the border clearance process at exit for all third country nationals, is another opportunity to avoid that travellers spend more time

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	<p>case, the increased border crossing duration would lead to require more space for the higher number of travellers waiting.</p> <p>The same would apply for seaports except that the proportion of visa-exempt travellers in seaports is on average low.</p> <p>In the same way as is the case now dedicated solutions need to be worked out for travellers and crew on cruise ships. The problem of the large group of persons (up to 4.500 persons) to be controlled is mitigated by the fact that all travellers are identified, that cruise ship operators have dedicated staff for security and immigration questions, and that all entries and exits on and off the ship are recorded.</p>	<p>at the border crossing point and that hence a bigger waiting area is required.</p>
<p>Border guards</p> <p>Total number of border guards in the first line is estimated at 25.000 persons</p>	<p>The practical implications for border guards are the mirror image of the implications for travellers.</p> <p>What does not change: border control of visa-exempt and visa-required travellers do the same checks as today. What changes is adding the recording of the entry and exit date and place.</p> <p>Border guards will read the passport by means of the passport reader which will trigger the same database checks as today plus check whether the traveller is</p>	<p>Compared to the general situation described in the previous column the preferred solution brings the following additional elements:</p> <ul style="list-style-type: none"> • At enrolment the personal file is completely create by data from the passport and does not include data that the travellers would declare and the border guards would record manually. • The biometrics stored in VIS are re-used for visa-exempt

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	<p>known in EES and/or VIS.</p> <p><u>At entry</u></p> <p>Most frequent case once the system is in operation: the traveller is known in EES and/or VIS</p> <ul style="list-style-type: none"> • If he/she is known in EES and is visa-exempt, a biometric verification is done: facial image or 1, 2 or 4 fingerprints are matched with the one in the database. If it yields an OK, the EES provides the duration of authorised stay. Upon verification that the other conditions for entry are met), the border guard authorises entry and the EES records the entry date and place. • If he/she is known in EES and is visa-required, a biometric verification is done as today. Without the border guard necessarily being aware of it, 1, 2 or 4 fingerprints are matched with the ones in VIS. If it yields an OK the EES provides the duration of authorised stay. Upon verification that the other conditions for entry are met, the border guard authorises entry and the EES records the entry date and place. <p>In case the traveller is not recorded in EES</p>	<p>travellers.</p> <ul style="list-style-type: none"> • The biometric identifiers are composed of 4 fingerprints and a facial image. This is a choice justified because it is fast, efficient, reliable and secure. • When the traveller uses the self-service kiosks, the border guard is relieved from the actions of reading the passport and taking biometrics, but he/she gets the replies on his screen and the history of entries and exits of the traveller over the last 5 years. This allows him/her to adapt the questions according to his/her assessment of the risk of overstay. • At exit, travellers can use e-gates (when available as to install e-gates or not is a Member State's decision). Border guards carefully watch what is happening in and around the e-gates and intervene for any unusual situation.

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	<ul style="list-style-type: none"> • If he/she is not known in EES and is visa-exempt, the border guard enrolls the traveller, meaning that he/she creates a personal file: <ul style="list-style-type: none"> – The border guard takes 4 fingerprints and a facial image and requests the system to check whether these biometrics already exist in EES and VIS. The answer should be "no". A "yes" would indicate that the person already exists in EES or VIS but that he/she has more than one passport. Entries and exits should then be linked to that existing identity. – When the person does not yet exist in EES, the border guard creates the personal file in EES by copying (automatically) the passport data (name, date of birth etc.) to EES and does the usual checks as per the Schengen Border Code. – Upon authorisation to enter, the entry date and place are recorded for that person • If he/she is not known in EES and is visa-required, then he/she will still be known in VIS, and the border guard enrolls the traveller in EES, meaning that he/she creates a personal file: <ul style="list-style-type: none"> – The border guard takes 4 fingerprints and a 	

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	<p>facial image and requests the system to check whether these biometrics already exist in EES. The answer should be "no". A "yes" would indicate that the person already exists but with another identity. Entries and exits should continue to be linked to that existing identity.</p> <ul style="list-style-type: none"> – When the person does not yet exist in EES, the border guard creates the personal file in EES and adds the facial image to the personal file in EES and does the usual checks as per the Schengen Border Code. – Upon authorisation to enter, the entry date and place are recorded for that person. <p>At exit: In this case all travellers exist in EES as there must be an entry record created.</p> <ul style="list-style-type: none"> • Upon reading of the passport data, the EES retrieves the last entry record for that person. • The border guard does a biometric verification match of the traveller's identity with the one recorded in the EES: either the facial image or 1, 2 or 4 fingerprints are matched with the ones in the database. The EES calculates whether there is a situation of overstay or not. In the normal case this 	

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	<p>should be "no". Upon verification of the other exit conditions the EES records the exit date and place.</p> <p>General: the traveller's passport will not contain Schengen entry/exit stamps anymore and to assess the likelihood of overstay the border guards will see the history of entries and exits over the retention period of entries and exits.</p> <p>Border guards will no longer stamp passports and visas at entry and exit, nor compute durations of stay.</p>	
<p>Migration enforcement</p> <p>Total number of persons is estimated at about 25.000 persons</p>	<p>Migration enforcement refers to any service that has a responsibility for controlling and implementing migration legislation.</p> <p>Compared to the current way of working where no reliable or complete data is available on overstayers, the EES will contain the identification of overstayers and keep this data for five years. Further the EES will provide a tool for giving or checking the identity of apprehended overstayers and successfully send them back.</p> <p>There are mainly two practical implications:</p> <ul style="list-style-type: none"> • Migration enforcement can analyse the population of overstayers and identify patterns to better 	<p>In the preferred solution, the data of overstayers is kept for five years counting from their last entry record. However beyond five years, data is not simply destroyed but the possibility is offered to Member States to create a SIS alert for overstayers so that people can still be apprehended at the border and/or found during inland controls.</p>

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	<p>evaluate the risk of overstay and share it with border control authorities.</p> <ul style="list-style-type: none"> • Migration enforcement can currently find more overstayers than those it can handle the return procedure because when they are apprehended there is a difficulty to identify them with certainty. As long as the person's identity and country that issued the travel document is not established there are few chances that the return procedure will be successful. With EES, the identity of the apprehended person can be established: <ul style="list-style-type: none"> – Either the person apprehended is cooperative and gives his/her real identity. This identity is confirmed by a simple verification of 1, 2 or 4 fingerprints or the facial image with the one in EES, and can be sent back to the country of origin. – Either the person apprehended is not cooperative and refuses to give his/her real identity. In that case four fingerprints are taken and the facial image. This biometrics is then sufficient to find the identity back in EES provided the data are kept long enough. 	

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
<p>Migration management</p> <p>Total number of persons is estimated at about 5.000</p>	<p>Persons who have to monitor the status on illegal migration and within this on overstayers, can only rely on ad-hoc surveys to know basic information such as: where do overstayers come from, what is their profile, via which borders did they come, the date of entry/exit, etc.</p> <p>The EES contains the data of individual persons who are flagged as overstayers. As a system, EES has the possibility to provide non-personal statistics on a regular or on an ad-hoc basis.</p>	<p>The preferred solution proposes the existence of a specific statistical reporting module that can generate both regular and ad-hoc reports.</p> <p>This would also meet unexpected reporting requirements to suit infrequent requests.</p>
<p>Law enforcement authorities (police security services, ...)</p> <p>Size of personnel employed by law enforcement services is probably in the millions but the part of the investigation services that could use EES is limited to a fraction of it, estimated at say 60.000 persons.</p>	<p>Investigation services will practically use EES for two situations:</p> <ul style="list-style-type: none"> • Identification purposes. In this case the investigation service has a partial fingerprint and/or images from a video or from pictures taken. Investigation services will have to demonstrate that other means of identification have been used and yielded no useful answer and that access to EES may be useful given the case considered. The identification of a person can then be run based on the biometric material available vs the biometrics stored in EES. • Criminal intelligence. When the conditions for access are respected (essentially making sure it is 	<p>The data retention is 5 years which is a useful duration for investigation purposes which usually starts after the events occurred (typically one or two years later).</p> <p>The preferred solution contains safe-guards against the abusive use of data.</p> <p>When accessed for criminal intelligence purposes EES will <u>exclude</u> the possibility to establish profiles, meaning finding links/correlations between characteristics of persons (as opposed to specific cases) and border crossings over a period of time.</p>

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
	<p>for a specific case and EES can potentially be of use) the investigators are authorised to query EES using a mix of criteria. EES has the unique feature of recording entries and exits of all third country nationals authorised for a short stay, at <i>all borders</i> while other means are restricted to air or sea borders. Investigators could check whether a person suspected was indeed present in the Schengen area during a given period of time, the border crossing points used at entry or exit, correlate arrivals/departures of different suspects, and any similar query on data related to a specific case.</p>	
<p>Consular officers</p> <p>Total number of persons is estimated at about 25.000 persons (spread over 2.000 consulates around the world)</p>	<p>Consular officers handle the visa requests of visa-required travellers.</p> <p>For a new visa request the consular officer checks the visa application history and can see how many visas were issued over the retention period of visas (5 years from their expiry). With EES, consular officers will also see whether the durations of stay were respected and whether the traveller entered the Schengen area via the country whose consulate lodged the request.</p> <p>Especially the control of the duration of stay enables the attribution of visas to those who respect the rules.</p>	<p>The proposal intends to make the control on the use of visas very straightforward by ensuring the interoperability between the VIS and the EES.</p> <p>The result would be that when the consular officer consults the visa history he/she also accesses the entry/exit records directly without having to obtain data from VIS and then query EES.</p>

Type of Stakeholder and size of the group	Practical implications of the initiative	Practical implications of the preferred solution
<p>eu-LISA and IT services for border control / migration on Member State side</p> <p>eu-LISA employs 200 persons.</p> <p>An estimated 500 persons will be directly involved in the project on Member State side</p>	<p>eu-LISA</p> <p>The Agency will have to deliver a large-scale IT system in addition to operating and maintaining the SIS, VIS and Eurodac. This will require the resources (staff and budget) to be strengthened for the duration of the project (estimated at three years).</p> <p>Once EES is in operation, eu-LISA will have to operate and maintain the additional system. This will require resources to be strengthened on an on-going basis.</p> <p>The Agency will have to manage the credentials of operators on an on-going basis and the operations of the webservice.</p> <p>IT services for border control/migration on Member State side</p> <p>In the same way as the Agency, each Member State IT service for border control/migration will have to:</p> <ol style="list-style-type: none"> (1) Deliver the integration of national border management applications and EES; (2) Meet the availability requirements of EES; (3) Operate the system on an on-going basis. 	<p>The proposal provides a time-frame of three years for building and testing EES.</p> <p>eu-LISA is in charge of not only delivering the central system but also a National User Interface (NUI) which provides a common solution for connecting the national domain with the central system.</p> <p>The proposal covers financially a large share of Member State costs for the integration of the NUI with the national domain and its operations costs.</p>

4. ANNEX 4: ANALYTICAL MODELS USED IN PREPARING THE IMPACT ASSESSMENT

Appropriate analytical models were used for both the Technical Study (2014) and the Pilot (2015). For the Technical Study a simulation model was developed to assess the impact of additional checks implied by Smart Borders on traveller's waiting time at border crossing points. For the Pilot a methodology was developed for the assessment of results.

4.1. Simulation model used for the Technical Study

The model was developed by the Research and Development unit of Frontex for the specific purpose of the study.

4.1.1. Method for simulation

Discrete event simulation was used to assess the impact of any changes introduced in the border control process. The models used for air borders were customised versions of models previously used for simulations of actual air borders. The model for land borders was specifically built for this study.

Both models use real data from border crossing points that the concerned Member State's authorities have provided. The focus of the simulations was the EES processes at entry and exit. RTP is seen as a sub-case of the simulations. In addition to the real data provided there were estimates inserted, including added time for registration, verification, etc.

Appropriateness of the model

The model was considered to be the appropriate tool for simulating the impact on the border crossing time. While the study could estimate the impact on so-called "atomic" steps (the individual step in a border crossing process like taking a picture or reading the passport chip) for different biometric identifiers, a simulation tool is required to show the impact on a border crossing point. The reason is that the border crossing time is influenced both by parameters related to the border crossing point (e.g. the number of lanes), the travellers (e.g. the volume, the arrival rate, the proportions of EU citizens, VE¹¹ and VH¹²) and the duration of controls. In other words simply extrapolating the duration of atomic steps with the number of travellers does not yield a useful answer.

As an example, a VE at first entry could require 30 seconds more to cross the border than a VE who is already enrolled. If ten VE who need to be enrolled arrive at the same moment, there could be an added duration of 300 seconds for the last one in the queue. However, a simulation shows that this case seldom occurs as the arrival of VE to be enrolled is mixed with the arrival of EU citizens and VH. The outcome of the simulation is that the impact on the average duration for crossing the border will be dampened by the low proportion of VE.

The model has been extremely useful in understanding the impact of the duration of the atomic steps on the situation in a busy border post. The large possibilities for assessing

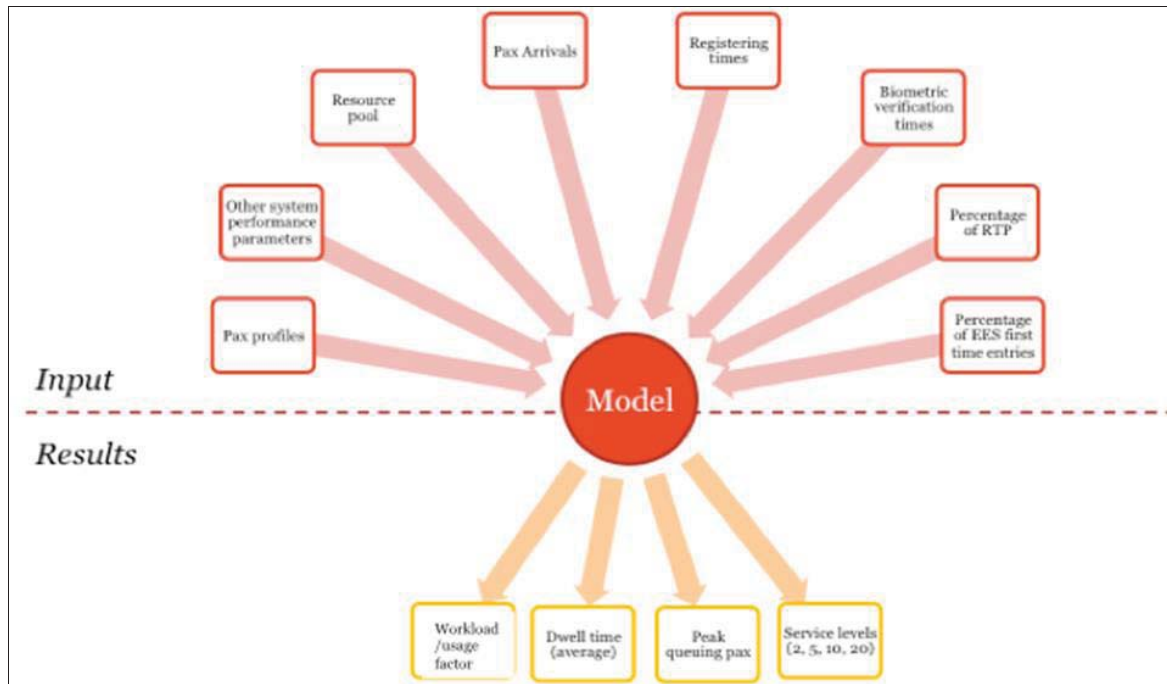
¹¹ Third-country nationals coming from countries that are exempted of the obligation to obtain a visa.

¹² Third-country nationals coming from countries that are required to obtain a visa.

the impact of changes to variables created awareness of which are the differentiating elements and which are the less differentiating. During the Pilot, the time values of atomic steps were assessed.

Model inputs and results

The picture below shows the type of parameters used for running the tool and the type of results that would come out of the simulation.



Input values

- The passenger profile, in this case the proportion of EU citizens, VE and VH.
- The "other performance parameters" refers to parameters like the proportion of travellers using ABC gates.
- The resources pool refers practically to the number of lanes and the number of border guards.
- The "pax arrival" refers to the pattern of arrival of travellers which is different per type of border. While the volume of travellers is a variable, the arrival rate is taken from real patterns.
- The registering time is the time for enrolling visa-exempt third country nationals at a first visit or after expiry of the retention period of data. This will be used as a variable meaning that the duration of this registration will be changed in successive computations.
- The biometric verification time is added as the so-called "overhead" for verification on top of the current border crossing time. This will be used as a variable as it is dependent of the type of biometric identifiers used.

- The percentage of RTP is the proportion of third-country nationals enrolled in the Registered Traveller's programme. RTP's border crossing time is equal to EU citizens'.
- The percentage of EES first time entries is the proportion of visa-exempt third country nationals at a first visit or after expiry of the retention period of data. This will be used as a variable meaning that the proportion of border crossings that require registration will be changed in successive calculations.

Service levels

The service level is in itself a time factor and the service level compliance is the percentage of travellers for whom each service level is fulfilled. What is calculated in the simulations is the service level compliance. The simulation shows how compliance changes for a range of added durations to the border checks. The graph also shows results for different volumes of travellers.

It should be noted that the service level time includes the total average dwelling time for the travellers, not only the time for the border check.

The service levels have different values for air and land borders.

Average dwelling time

The dwelling time represents the amount of time the traveller has to use to complete the border check clearance including the queuing time. It is computed from the moment the traveller arrives at the border check area, till the completion of the border check. The results are presented in relation to the same values of the service levels. It is the measurement that represents what the traveller experiences while "waiting for crossing the border".

Workload (air borders)

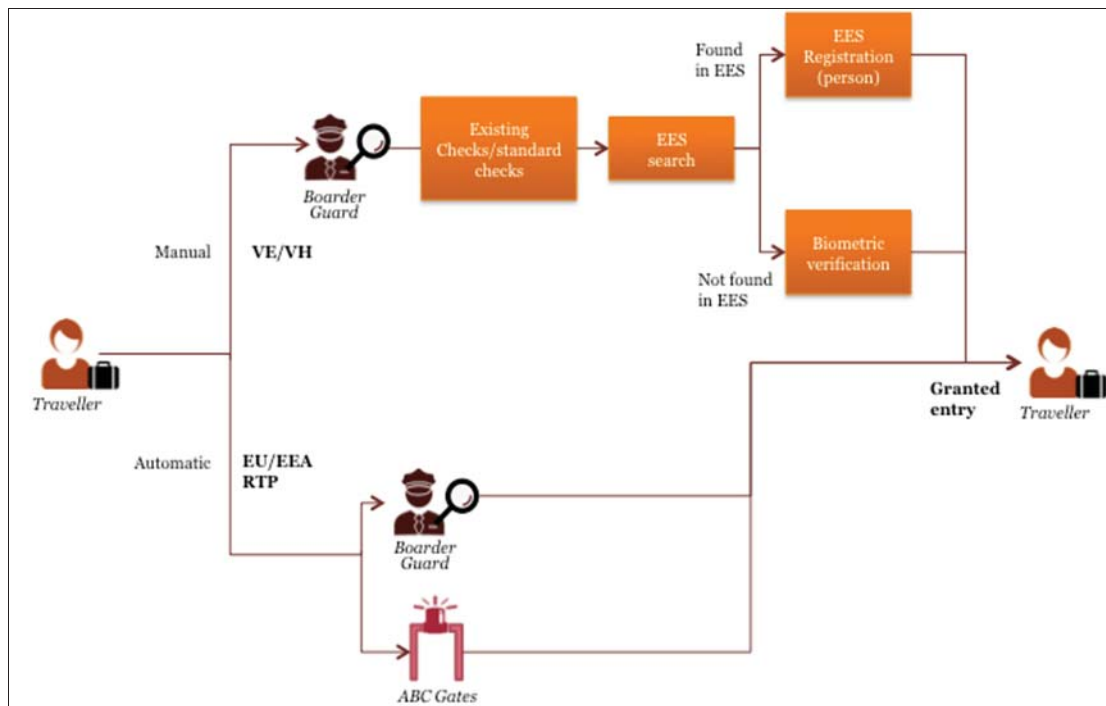
The workload included represents the total number of minutes of officer's time required to perform border checks at the manual booths in one natural day. The results were computed for workload related to the added time for the actual check.

Usage factor (land borders)

The measurement at land borders is not defined as workload but as something called a "usage factor" that shows the percentage of activity (i.e. when checks are being done) for the border guards. At land borders, the flow and peak patterns differ from air borders and there is a need for continuous manning of booths. The usage factors also indicate the need for resources to replace the person in the booth at certain intervals.

Model of the flow

The picture below shows the abstract model of the flow per category of traveller, including the EES and RTP. The picture shows the situation at entry. The only difference for the exit is that the step "registration in the EES" does not exist and only the step "biometric verification" takes place at exit. The "registration process" corresponds to what is called the "enrolment" of travellers.



The simulations were made for two types of borders: air borders and land borders. No simulation was run for sea borders due to practical constraints and the consideration that the majority of travellers pass via air (with a large proportion of VE) or land borders (with a large proportion of VH).

Model validation

In each case the model was applied to a real border crossing. In order to validate the simulation model the existing situation at the border was reproduced: current values for the parameters were introduced and the simulation produces current observed values of the outputs.

4.1.2. Simulation of air borders

Conditions

Real data from four filters¹³, two for arrival and two for departure, at a large airport within the Schengen area were put into the simulation tool. This data comes from an average day within the busiest month of the year.

Two filters (in the text named “Arrival filter B” and “Departure filter D”) could be seen as very busy border crossing points comprising both manual booths and ABC gates; and the other filters (in the text named “Arrival filter A” and “Departure filter C”) as border crossing points with more moderate volumes.

The simulation is performed for "incoming flows" at arrival (travellers entering the Schengen area) and "outgoing flows" at departure (travellers leaving the Schengen area).

The data used in the simulation is the following:

¹³ "Filters" is the word the model uses for border crossing points.

Volumes (traveller/day)		Simulations run
Arrival filter A No ABC gates, 5 manual booths	3 000	The volumes are estimated to increase up to 3500-4000 in the coming 5 years. This was taken into account in the simulation
Arrival filter B 6 ABC gates, 6 manual booths	10 000	The volumes are estimated to increase up to 11-12000 in the coming 5 years. This was taken into account in the simulation
Departure filter C No ABC gates, 6 manual booths	11 000	The volumes are estimated to increase up to 12-13000 in the coming 5 years. This was taken into account in the simulation
Departure filter D 6 ABC gates, 12 manual booths	21 600	The volumes are estimated to increase up to 24-25000 in the coming 5 years. This was taken into account in the simulation

The following split between categories of travellers was again taken from real data in that airport.

Categories (traveller)				
Arrival filter A	EU/EEA 69%	VE 15 %	VH 15 %	Premium 1%
Arrival filter B	EU/EEA 74%	VE 12.5 %	VH 12.5 %	Premium 1%
Departure filter C	EU/EEA 79%	VE 10 %	VH 10 %	Premium 1%
Departure filter D	EU/EEA 69%	VE 15 %	VH 15 %	Premium 1%

The term “Premium” (travellers) refers to fast-tracked travellers; they still go through the same checks however. Practically, it mainly refers to airline crews.

Variables explored

The variables to be explored in order to assess the impact of EES and RTP are presented in the table below.

Variables	Range of variation	Explanation
Percentage of border crossings of TCNs that require registration (called "enrolment step" in the process descriptions) of the individual file in EES	0-50 %	What is presented in the graph, in relation to this range are the values for 10% and 50 %.
Percentage of border crossings of TCNs who are already	0-10 %	The assumption is that RTP travellers have the

registered in the RTP

same border crossing time as EU/EEA travellers and that they use ABC gates when available

Time overhead for TCNs requiring registration of an individual file in the EES	Range of 0-180 sec	The values shown in the graphs are the average values of the potential additional time on top of the current border crossing time for performing the registration of the individual file in the EES.
Overhead for TCNs who need to be verified (not needing registration)	0-30 sec	This is the average value used for the potential added time to verify a TCN at entry/exit (the time for creating the entry/exit record is assumed to have a duration of 0 seconds)

The simulations were run for an extensive number of scenarios, exploring different values of the variants in the table above, to simulate what a day at an air border crossing point could look like after EES and RTP are implemented.

As an example, 1 400 simulations were run to obtain the data for airport filter A at arrival (entry). Up to 7 000 simulations were run, 5 times, in other cases, to capture the statistic variations.

Assumptions

Below are the values used for the time the border check takes today, not taking into account the implementation of EES and RTP:

EU/EEA	= 15 sec (manual)
EU/EEA	= 20 sec (ABC-gate)
VE	= 30 sec
VH	= 45 sec

These values are realistic values for the given airport. The simulation tool in addition attributes a duration to each border crossing that is stochastically distributed so that the mean value equals the values mentioned above for each category of traveller. This brings the simulation closer to the reality.

Results

The results were computed for the following areas:

- Service levels. For air borders the service levels used are the following:

- SL 2 = 2 minutes. This is a very challenging service level that is only used for ABC gates.
 - SL 5 = 5 minutes. This is a very high requirement for manual lanes.
 - SL 10 = 10 minutes. This is the most frequently used service level: having 85 or 90% of travellers served within 10 minutes is considered as a very good achievement.
- Average dwelling time.
 - Workload (air borders)

The results of the simulation are that an added duration of more than 60 seconds, at first entry, has the following impacts:

- A measurable impact on "service level 2", which has the objective of serving a traveller within 2 minutes. Once the additional tasks implied by EES equal 60 seconds, the decrease in service level becomes steeper;
- Service levels of 5 and 10 minutes are in principle not affected by the additional duration and very limited impact on the dwelling time;
- An impact of around 7% (at 60 seconds) on the workload necessary for the entry checks and around 11% (at 100 seconds).

The results further show:

- At first entry, an added duration of less than 60 seconds on average for the EES registration, using 30 seconds for verifications, shows a limited impact on the service levels defined for the case studied. The dwelling time increases by less than 16 seconds and workload increases by less than 9.4% (at 40 seconds the increase is around 4.5%);
- At subsequent entries and exits, an added duration of 30 seconds or less has in principle no impact on service levels, dwelling time or workload.

4.1.3. Simulation of land borders

The real data that was used represents one month of border traffic and comes from a 24h/24h operating land border crossing point with Russia. Only exit traffic was used in the simulation. Trucks and pedestrians are not included in the simulation for land borders. As regards trucks, the average checking time is around 30 minutes, mainly due to customs declarations and vehicle inspections, which makes it less relevant for the purposes of the simulation.

Three lanes with one booth per lane were used in the simulation and the vehicles were a combination of buses and private vehicles (motorbikes and private cars). Two lanes were used for private vehicles and one for combined buses and private vehicles. Checks take place while travellers stay in their vehicles (no need to step out). Most travellers are Russian citizens that are visa holders. It should be noted that neither the simulation nor the Study takes into account the potential change of this status. This is consistent with the assumption used throughout the Study that there are no (major) changes to the list of visa-exempt countries.

The land border concerned uses both a pre-reservation scheme (a border crossing timeslot is reserved in advance prior to arrival at the BCP) and a live queue (for those who show up at the BCP without a pre-reservation) for all vehicles.

Conditions

The set-up and conditions of the land border simulation are different from the air border simulation because a land border has different characteristics (a land border crossing point located on a road is used in this simulation).

The real data used in the simulation is the following:

Data used		Comment
Number of vehicles in month of observation	10 382	
Private vehicles	98%	The other vehicles (buses) have only a marginal occurrence, as at most land borders.
The chosen month's traffic in relation to the given year	9.1 % of yearly volume	The simulations were run for a month that is busier on average than the rest of the year, as the volume accounts for more than 1/12 th (8.3%) of the year.
Number of vehicles using the live queue	62%	
Number of vehicles using pre-reservation	38%	

The simulated border crossing is border checks at exit. Therefore, it is reasonable to use a potential added time of 30 seconds for the duration of the check against EES (biometric verification mainly) as a representative value. The time for added duration in the simulation is however per vehicle, which makes the comparison to the time it takes to verify 1 person more complicated. While preparing the simulation, it was seen that there was a certain degree of parallel activity and that the vehicles had an average occupancy of 1.5 to 2 persons. A value of 1 minute of added duration per vehicle could therefore be a representative value in this simulation. It should however be considered that if the occupants were to have to leave the car for such a verification, then the added time for the duration would presumably be longer.

Results

The simulation provides the results at exit as seen for the land border included in the simulation. This is a normal case because for the entry, the queue cannot be measured as it is occurring on the other side of the border in the neighbouring country. The results are related to service level fulfilment, dwelling time and workload and represent the results for the vehicles included in the simulation, passing through the specific border check.

The results were computed for the following areas:

- Service levels. In the case of land borders, the service levels are the following:
 - SL 10 = 10 minutes. This a very challenging service level for a land border of this type;
 - SL 30 = 30 minutes. This can be seen as the most representative service level for this type of land border.
 - For comparison, service levels of 60, 120 and 180 minutes were also simulated.
- Average dwelling time
- Usage factor (land borders)

The simulation is fully representative of the border crossing concerned, from where the real data and actual configuration of the border check were used.

The main result of the simulation is that for an added duration of 60 seconds per vehicle, at exit, has the following impacts would be measured:

- The impact on the situation at the border is dependent of whether the border crossing point already now is close to its nominal capacity or not;
- The impact is heavier when the border operates on 24h/24h basis as this eliminates situations of relief at the border post;
- The service level of 30 minutes decreases by around 2%, which represents around 35 seconds of added time for the total time of queuing and being checked (i.e. the so-called “dwelling time”);
- The dwelling time increases by around 3 %;
- The usage factor increases by 12 % points but this still leaves some margin to handle peak situations.
- A complicating factor, related to EES, would be if travellers needed to leave their cars for the biometric checks for instance.

4.1.4. Simulation of RTP

The simulation of the RTP could only be made at the air border. In this context RTP members are assumed to be able to use ABC-gates.

The summary takes into account the simulation conducted using arrival filter B and departure filter D (see section above on simulation of air border), with high volumes and equipped with ABC gates. The ABC-gate has a service level of 2 minutes and the manual service level is at 5 minutes, for comparison with the service level of the ABC-gate.

The simulated variable is the percentage of border crossings made by TCN travellers with RTP status. This value was changed from 0 to 25%.

Main results are:

- The use of ABC gates for RTP travellers makes it possible to keep a higher service level than at manual gates. The service level (2 min) used in the simulation includes dwelling time;
- The general trend is that the more crossings are made by RTP travellers, the more the service level compliance at manual gates improves, the shorter the dwelling time becomes and the lower the workload;
- The workload decrease when more than 12% of TCN border crossings is made by RTP subscribers can off-set part or the totality of the workload increase induced by the implementation of EES (additional first time enrolment and subsequent verification time).

4.2. Methodology used for Pilot Project

The Pilot (also referred to as Testing Phase or “the Project”) took place under responsibility of eu-LISA, with the objective of verifying the feasibility of the options identified in the Technical Study and validating the selected concepts for both automated and manual border controls.

4.2.1. Objective

The main objective of the Testing Phase was to test the limited technical options identified within the Technical Study against specific measurable criteria, notably accuracy, effectiveness and impact on the border crossing duration in operational and other relevant environments. The Testing Phase was not aimed at testing full end-to-end EES and RTP systems.

4.2.2. Requirements set by Commission

The Testing Phase of the Proof of Concept was based on the Terms of Reference (ToR) issued by Commission, which determined which options should be tested and conditions to be met.

The following conditions were outlined:

- The Testing Phase needs to be conducted as a continuation of the Technical Study as they both belong to the same Proof of Concept exercise. Practically this means that in the documents produced within the framework of the Testing Phase changes to concepts and abbreviations will be avoided. It also means that similar project management roles are followed and that all results of the Technical Study can be re-used or referred to in the Testing Phase.
- The Testing Phase should be carried out in such a way that the impact of the change introduced by an option can be identified. Where applicable, the reference values will be measured (e.g. duration of a process or process steps, quality) before a change occurs and after the change is implemented.
- The selected BCPs (air, land and sea borders) should be representative of the variety of Schengen border conditions (e.g. border type, ABC gate types, land border with personal cars). Particular attention should be given to the special conditions found at land borders.

- The biometric devices to be used for the tests should already be on the market.
- Adequate data protection measures should be in place. The data collected for the test should be depersonalised and saved only locally and the retention of those data should be limited to the time necessary to produce the relevant statistics and analysis.
- The Testing Phase needs to be conducted in compliance with data protection provisions. Insofar as personal data are to be processed in the tests, eu-LISA will have to comply with Regulation (EC) 45/2001 and the Member States' authorities will have to comply with Regulation (EC) 45/2001, Directive 95/46/EC and the national implementations of this Directive 95/46/EC or other applicable data protection rules. In this regard, the European Data Protection Supervisor as well as, if necessary, national supervisory authorities should be involved.
- The tests will be conducted in compliance with fundamental rights, particularly the right to respect for private life, protection of personal data, dignity, non-discrimination (on grounds listed in Article 21 of the Charter, e.g. sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, disability or age). They will also have to ensure respect for vulnerable groups (such as children, unaccompanied children, disabled people, elderly people, pregnant women, single parents with minor children, victims of human trafficking, persons with serious illnesses, persons with mental disorders and persons who have been subjected to torture or other serious forms of violence).
- In order to have personal data processed, the data subject shall be informed of the type of data collected, the purpose of the processing and the controller's identity. The data subject shall explicitly and freely give his/her consent to participate in the test. The data subject shall also be informed of his/her right as a data subject in accordance with data protection law.
- The Testing Phase needs to be conducted in compliance with the existing legislation (e.g. the SIS II and VIS regulations, the Visa and Schengen Borders Code).
- Some Test Cases could be complemented with a stand-alone installation connected to a system simulating the relevant EES/RTP processes.

4.2.3. Test Cases

The Test Cases that were tested during the Testing Phase were based on the options outlined in the ToR, and presented in the table below.

Categories of options	Test Cases
<ul style="list-style-type: none"> • Enrol biometrics for individual file in EES 	TC1 Enrol 4 fingerprints at first-line border check
	TC2 Enrol 8 fingerprints at first-line border check
	TC3 Enrol 10 fingerprints at first-line border check
	TC4 Enrol live facial image

	TC5 Enrol iris (including desk research regarding spoofing attempts and anti-spoofing measures for iris pattern enrolment)
<ul style="list-style-type: none"> • Capturing FI from e-MRTD and verifying it against another source 	TC6 Capture Facial Image from e-MRTD TC7 Verify FI captured from e-MRTD against live facial image
<ul style="list-style-type: none"> • Accelerators 	TC8 Search VIS by Travel Document Number TC9 Automated Exit Checks of TCNs TC10 Use of Self-Service kiosks TC11 Pre-border checks at Land Borders
<ul style="list-style-type: none"> • Technical options 	TC12 Web-interfaces to the carriers and to the travellers TC13 Fall-back options

4.2.4. Testing approach

The testing approach took into account compliance with fundamental rights during the execution of tests:

1. At borders, persons must be checked in a manner which respects human dignity, regardless of the volume of traffic or the behaviour of travellers;
2. All border guards should receive refresher training on how to treat travellers respectfully and professionally as well as on the importance of remaining polite and formal in all situations;
3. Border guards should also pay attention to cultural and language differences when communicating with travellers. As a result, the tests will emphasise the languages that border guards are most likely to use, particularly English and the languages of the relevant neighbouring countries.

Three types of methodologies were employed, each achieving different purposes:

- Desk Research;
- Partial operational testing;
- Operational testing integrated in border control process.

For each methodology type, the following items were identified, recorded and guaranteed by a quality control process:

- Data source (e.g. traveller), data capture equipment (e.g. fingerprint scanner) and data capture method;
- Required data (e.g. fingerprint template) and data evaluation tool and process (e.g. NFIQ);
- Output (e.g. quality score) and expected or actual outcome (e.g. FAR/FRR);

- Time: the duration of the border crossing process and the atomic steps integrating the new TC step;
- Security and accuracy: the confidence in the identification decisions (e.g. passport authentication, biometric verification, bearer verification) made before, after and at the border;
- User acceptance: the perception of the travellers and the border guards.

During the Testing Phase other indicators were also recorded, such as exceptions and observations on complexity from a technical or organisational viewpoint. These indicators were consolidated and evaluated to propose measurable results based on the criteria outlined by the ToR.

Most of the Test Cases were addressed by several methodologies depending on the relevant question. In general, a combination of operational testing and desk research was performed.

Desk research

Desk research complemented the real life testing performed and it was applied in the following particular cases:

- For specific topics as specified by the ToR (e.g. anti-spoofing methods for the iris enrolment);
- When other projects / experiences have already provided meaningful findings;
- When it is impractical or non-feasible to perform real-life testing;
- When the timing and budget of the Proof of Concept does not make it possible to perform real-life testing.

In light of the above, a number of questions for each TC were addressed as desk research. These questions were categorised in the following domains:

- Cost of the solutions;
- Security (i.e. anti-spoofing and required supervision);
- Equipment (e.g. minimum requirements, environmental conditions influencing the performances, etc.);
- Process (e.g. for what type of border the kiosks are a suitable solution, what operations can be performed in a self-service kiosk by the traveller).

Additionally, the following Test Cases were addressed only through desk research:

- Searching VIS by Travel Document Number;
- Fall-back options;
- Web interfaces to carriers & travellers.

Partial operational testing

Partial operational testing was applied:

- When integration of equipment / system was not manageable or not practical (e.g. integration of kiosk in existing system, set-up of new ABC-gates);
- When a technical study was been requested by the ToR.

Concretely, this methodology made it possible to introduce the option to be tested with minimal changes to the actual border crossing process and made it possible to test the feasibility of the option in real life conditions.

Full operational testing at BCP (Border Crossing Point)

Full operational testing was applied:

- When the testing of the option was feasible in an operational environment;
- When Member States provided the necessary resources to perform the adequate adaptations and measurements (human resources, infrastructure, required time, border guards and operators).

The following methods were used for full operational testing at BCP:

- Measurement of the baseline indicators, coming from the existing process when applicable;
- Adaptation of the existing border crossing process to integrate with the existing process an option of the EES/RTP;
- Measurement of the change indicators, coming from the new process;
- Calculation of the difference between the existing process and the new process.

4.2.5. Time Measurement

One of the main objectives of the testing was to assess the impact of the proposed changes to the current border crossing process in terms of duration.

Durations to be measured

Baseline measurement: in order to gauge the impact in terms of duration, it was necessary to also measure the baseline for the “as-is” process. The baseline measurement was mostly relevant for the end-to-end duration of a process; however, in some cases it appeared necessary to measure it for certain atomic steps, in order to correct the end-to-end time measured (either by adding or subtracting average durations). According to the ASQ Performance (ASQP) programme of Airports Council International¹⁴ (ACI) a minimum sample size of 100 is considered sufficient.

Duration of atomic steps: the duration of new or changed steps.

This includes:

- Biometric capture (FPs, FI, iris). The duration of the failed attempts will be also registered.
- Retrieval of the FI from the e-MRTD
- Verification of live FI against FI from e-MRTD

End-to-end duration: the duration of the entire border crossing process, from start to end, was measured where relevant (i.e. if the test is part of the real process and not

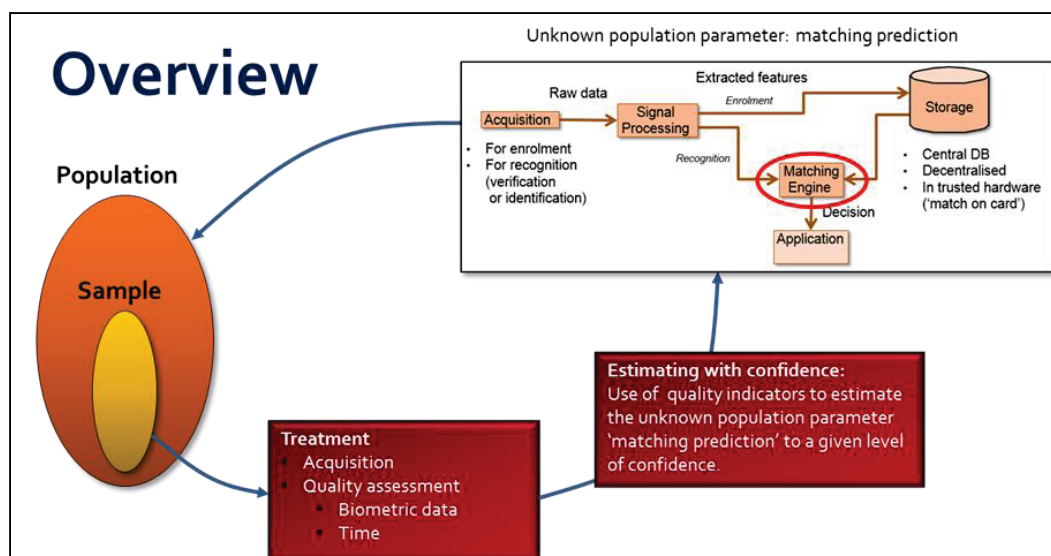
¹⁴ ACI World Facilitation and Services Standing Committee recommended practice 300A12: manual measurement of passenger services process time and KPI's drafted by ACI World secretariat and DKMA.

performed in an isolated and stand-alone manner). The main focus was to determine the differences obtained at various BCPs between the “as-is” process and the proposed “to-be” process.

4.2.6. Biometric Quality Measurement

The approach to biometric performance assessment can be summarised as “estimating with confidence”. Biometric data was acquired from a sample amount of travellers, which was sufficient to allow a reliable estimation of the performance of a biometric system. During the Pilot, as no actual matching was done (except for facial biometrics), estimation was based on the quality of the data captured. The approach was based on the following steps:

- The selection of quality indicators for the different biometric characteristics within the scope;
- The selection of confidence level and sample size;
- The preparation and execution of the data processing, i.e. the actual acquisition and quality assessment of biometric data;
- The estimation with confidence of the matching prediction for both verification and identification against galleries of different sizes.



Overview of the “estimating with confidence” approach for biometrics

When “estimating with confidence”, a confidence interval was used to estimate an unknown population parameter. It is an interval that has the form “estimate +/- margin of error” and has a confidence level property. In such a setting:

- The “estimate” is the guess for the unknown population parameter. The estimate is based on the outcome of the biometric quality assessment, e.g. NFIQ for fingerprints.
- The margin of error m reflects how accurate we believe our guess is. The margin of error of a confidence interval for the mean of a normal population is easily

calculated for a given confidence level (e.g. 99%) by $m = z * \frac{\sigma}{\sqrt{n}}$. The terms used are defined below¹⁵.

- If the population is not normal, a bootstrap can be used to understand the distribution. However, eu-LISA calculations indicated that, for the current BMS (Biometric Matching System) quality score data, the distribution is approximately normal. The assumption is therefore made that quality scores will generally be distributed normally irrespective of the algorithm used for quality assessment.

A confidence level expresses how frequently the observed interval contains the parameter. This value is represented by a percentage, so the statement, "we are 99% confident that the true value of the parameter is in our confidence interval" expresses that 99% of the observed confidence intervals (samples) holds the true value of the parameter.

4.2.7. Target sample size

The overall principle for the choice of sample size is finding the right balance between the available resources for the test, passengers' throughput per BCP and the desired accuracy¹⁶ to make conclusions about the population from the sample.

During the execution of the Testing Phase, the amount of passengers per each Test Case at each BCP was monitored and compared against the target sample size. This allowed the testing team to make any necessary adjustments during the execution (e.g. add extra staff, improve information activities).

The table below indicates a target sample size for each TC per each BCP in order to reach representativeness, as requested in the ToR.

		4FP + FI	8FP + FI	10FP + FI	Live FI	Iris	FI e-mrtd	of FI against other	ABC exit	Kiosk	Kiosks (waiting areas)
Country	BCP	TC1	TC2	TC3	TC4	TC5	TC6	TC7	TC9	TC10	TC11
Sea											
EL	Port of Piraeus	600	1000	1550	1550		1550	1600			
FI	Helsinki port	600	1000		1550		1550	1600	1000	1000	
FR	Cherbourg	600			1550	1550					
IT	Genova	600			1550		1550	1600			
Air											
DE	Frankfurt	600	1000	1550					1000		
ES	Madrid	600			1550		1550	1600		1000	
FR	Charles de Gaulle		1000		1550		1550	1600	1000		

¹⁵ σ = standard deviation, n = sample size and z^* = the value on the standard normal curve with the area corresponding to the confidence level between $-z^*$ and $+z^*$.

¹⁶ The desired accuracy of the population parameter is expressed as the width of the confidence interval or, equivalently, as the margin of error (half the width).

NL	Schiphol	600	1000	1550					1000		
PT	Lisbon airport					1550			1000	1000	
SE	Arlanda				1550		1550	1600			
Land: train											
FR	Gare du nord		1000		1550		1550	1600	1000		
RO	Vicșani		1000		1550		1550	1600	1000		
Land: road											
EE	Narva								1000		1000
EL	Kipoi Evrou	600	1000	1550		1550					
FI	Vaalimaa	600	1000	1550	1550		1550	1600			
HU	Udvar	600	1000	1550							
RO	Sculeni				1550	1550	1550	1600			

Target sample size for each TC per each BCP

5. ANNEX 5: SUMMARY OF PROCESSES AT ENTRY/EXIT ACCORDING TO CURRENT SCHENGEN BORDER CODE

EU citizens and persons enjoying the Union right of free movement

EU citizens and other persons enjoying the Union right of free movement (e.g. family members of EU citizens holding a visa or a residence card) crossing the external border are subject to a minimum check, both at entry and exit, consisting of the verification of the travel document in order to establish the identity of the person. Such a minimum check comprises the verification, where appropriate by using technical devices and by consulting, in the relevant databases, information exclusively on stolen, misappropriated, lost and invalidated documents, of the validity of the document authorising the legitimate holder to cross the border and of the presence of signs of falsification or counterfeiting.

In addition, on a non-systematic basis, national and European databases may be consulted in order to ensure that such persons do not represent a genuine, present and sufficiently serious threat to the internal security, public policy, international relations of the Member States or a threat to the public health.

The travel document of this category of persons is not stamped at entry and exit, with the following two exceptions which are subject to stamping:

- nationals of third countries who are members of the family of a Union citizen to whom Directive 2004/38/EC applies, who are admitted for a stay but who do not present the residence card provided for in that Directive
- nationals of third countries who are members of the family of nationals of third countries enjoying the right of free movement under Union law, who are admitted for a stay but who do not present the residence card provided for in Directive 2004/38/EC

Third Country Nationals (TCN) who do not exercise their right of free movement and who are admitted for a short-stay

Third Country Nationals (TCN) who do not have a residence permit or a long-stay visa issued by a Member State are admitted for a short stay of maximum 90 days within any period of 180 days (hereinafter referred as the "90/180 day" rule). This applies both for those who are subject to the visa obligation and those that are not. TCN admitted for short stays represent the majority of border crossings.

As described in the table below; these third-country nationals are subject, at entry, to a thorough check which, in addition to a bearer verification and more thorough travel document check, convey the following additional checks: that at their entry they still respect the "90/180 rule", their point of departure and destination and the purpose of their stay, the possession of sufficient means of subsistence, as well as a search in the Schengen Information System (SIS) and in relevant national databases.

- Verifying at entry (and also at exit) that the "90/180 rule" is met, currently the verification can only be based on the entry and exit stamps in the passport. In practice this is a very impractical exercise as stamps of Schengen countries may be mixed with stamps of other countries. Stamps may be difficult to read and anyhow different periods of stay might be combined.

- In addition, TCN with the citizenship of a country on the list of visa-required countries (TCN-VH)¹⁷ need to have a valid visa delivered by a Schengen Member State in accordance with the provisions of the Visa Code¹⁸. Accordingly, for these travellers, border guards perform an additional check as they verify the validity of the visa as well as the identity of the holder of the visa and the authenticity of the visa, by consulting the VIS, using fingerprints and the visa sticker number. Indeed, since 11 October 2014, border guards ascertain that each visa holder is the owner of the visa-sticker affixed in his/her passport by verifying whether one, two or four fingerprints of the traveller match with the fingerprint set enrolled in the Visa Information System (VIS). The fingerprints were enrolled at the moment of applying for the visa in the consular post of a Schengen Member State. By the end of 2015, the so-called VIS "roll-out" will be completed and all consular posts will register both the visa information and the required biometric information in the VIS.
- For all third country nationals, once the border guard authorises the border crossing, the passport is stamped marking the date and place of entry. In case entry is refused, the border guard affixes an entry stamp on the passport, cancelled by a cross in indelible black ink, and writes a code letter corresponding to the reason for refusing entry.
- At exit, the checks on TCN do not include the verification of their point of departure and destination and the purpose of their stay; nor the possession of sufficient means of subsistence. In addition, some checks are optional (the verification that the person is in possession of a valid visa; the verification that the person did not exceed the maximum duration of authorised stay in the territory of the Member States; and the consultation of alerts on persons and objects included in the SIS and reports in national data files). The verification that the third-country national is not considered to be a threat to public policy, internal security or the international relations of any of the Member States shall be carried out whenever possible;

Of relevance here is that the travel document is stamped at exit. It is by comparing the date of exit with the stamp at entry that overstayers are identified.

	Entry/ Exit	TCNVEs TCNVHs	Description
Bearer verification (Article 7(2) SBC)	Entry Exit	✓	Checks made to secure that the bearer of the travel document is the lawful owner of the document, where appropriate by using technical devices and by consulting, in the relevant databases, information exclusively on stolen, misappropriated, lost and invalidated documents.
Travel document check (Articles 7(3)(a)(i),	Entry Exit	✓	• Verification that the TCN is in possession of a valid travel document entitling the holder to cross the border satisfying the following criteria:

¹⁷ Council Regulation (EC) No 539/2001* of 15 March 2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement (OJ L 81, 21.3.2001, p. 1).

¹⁸ Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1)

7(3)(a)(ii),
7(3)(b)(i),
7(3)(b)(ii) and
5(1)(a) of the SBC)

- its validity shall extend at least three months after the intended date of departure from the territory of the Member States. In a justified case of emergency, this obligation may be waived;
- it shall have been issued within the previous 10 years.

- Verification that the travel document has not expired,
- Thorough scrutiny of the travel document for signs of falsification or counterfeiting.
- Verification that the travel document is accompanied, where applicable, by the requisite visa
- Verification of the validity of the visa
- Verification of the identity of the holder of the visa and of the authenticity of the visa, by consulting the VIS, using fingerprints and the visa sticker number.¹⁹

Visa check (if applicable)

(Articles 7(3)(a)(i), 7(3)(aa), 5(1)(b), 7(3)(c)(i) and of the SBC)

Entry *Only TCNVHs*
Exit -
optional

Stamp check

(Articles 7(3)(a)(iii) and 7(3)(c)(ii) of the SBC)

Entry ✓
Exit (optional)

Verification that the person has not already exceeded the maximum duration of authorised stay. For that purpose, entry and exit stamps are checked and the duration of previous stay is calculated manually

Questions

(Articles 7(3)(a)(iv) and (v) of the SBC)

Entry ✓

- Questions are asked as regards:
 - the point of departure and the destination;
 - the purpose of the stay;
 - sufficient means of subsistence for the duration of the stay and the return to the country of origin.
- If necessary, the concerned supporting documents are checked (e.g. tickets, hotel reservations or invitations to meetings).

Verification on the person, means of transport and objects transported (including SIS II consultation on alerts)

(Articles 7(3)(a)(vi), 5(1)(d), 5(1)(e) 7(3)(b)(iii) and 7(3)(c)(iii) of the SBC)

Entry ✓
Exit -
optional

Verification that the person, his/ her means of transport and the objects she/he is transporting are not likely to jeopardise the public policy, internal security, public health, or international relations of any of the Member States or that not allowed in the Schengen area

Verification that there is no alert on SIS II on the person for the purpose of refusing entry.

This verification includes a consultation of SIS II and other relevant systems

Stamping

(Articles 10(1) and 13 and Annex V, part A, paragraph

Entry ✓
Exit

The passport is stamped on entry and exit.

Where entry is refused, the border guard affixes an entry stamp on the passport, cancelled by a cross in indelible black ink, and write opposite it

¹⁹ Fingerprints are mandatory as of October 2014.

1(b)			on the right-hand side, also in indelible ink, the letter(s) corresponding to the reason(s) for refusing entry.
Second line checks and actions	Entry	✓	Depending on the results of the checks, further verifications may be carried out in a special location away from the location at which all persons are checked (first line).
	Exit		
(Article 7(5) of the SBC)			

- The average border crossing time at entry for visa-exempt TCN is estimated at 63 seconds at entry (so about four times more than for an EU citizen) and for a visa-required TCN at 104 seconds at entry (so about seven times more than for an EU citizen). The average border crossing time at exit for visa-exempt TCN is 53 seconds (3,5 times more than for an EU citizen) and 71 seconds for a visa-required TCN (so five more than for an EU citizen). As a consequence although 34% of border crossings are due to TCN, they account for more than 60% of the workload for border guards.

TCN with a long-stay visa

TCN with a long-stay visa issued by a Member State are also submitted to a thorough check. Long-stay visas are not submitted to the "90/180 days rule" of the short-stay visas as this duration of stay is precisely the differentiating factor. Long-stay visas are also not recorded in VIS, hence up to now the correspondence between the person who applied for the visa and the bearer is done on the basis of the photo. Long-stay visas are stamped at entry and exit. Like for all TCN, systematic checks are performed vs SIS II and national databases at the moment of border crossing.

TCN with a residence permit

TCN who travel with a residence permit are also submitted to a thorough check.

Residence permit holders are not submitted to the "90/180 days rule" of the short-stay. The permits are not recorded in VIS.

In addition, residence permit holders are as a general rule neither subject to the question on sufficient means of subsistence for the duration of the stay and the return to the country of origin, nor on the questions on the purpose of the stay.

Like for all TCN, systematic checks are performed vs SIS II and national databases at the moment of border crossing.

6. ANNEX 6: COST MODEL FOR SMART BORDERS SYSTEM

6.1. Cost Model

In 2014 as part of Technical Study a revised cost analysis was developed in order to provide up-to-date, reliable cost estimates of the EES and RTP systems to be borne at the European Commission (central) and Member State (national) level covered by a central envelope (ISF/Smart Borders line). The figure below details the split between the costs to be covered by the central envelope and those to be covered by Member States' budgets (National budgets or ISF/National programs).

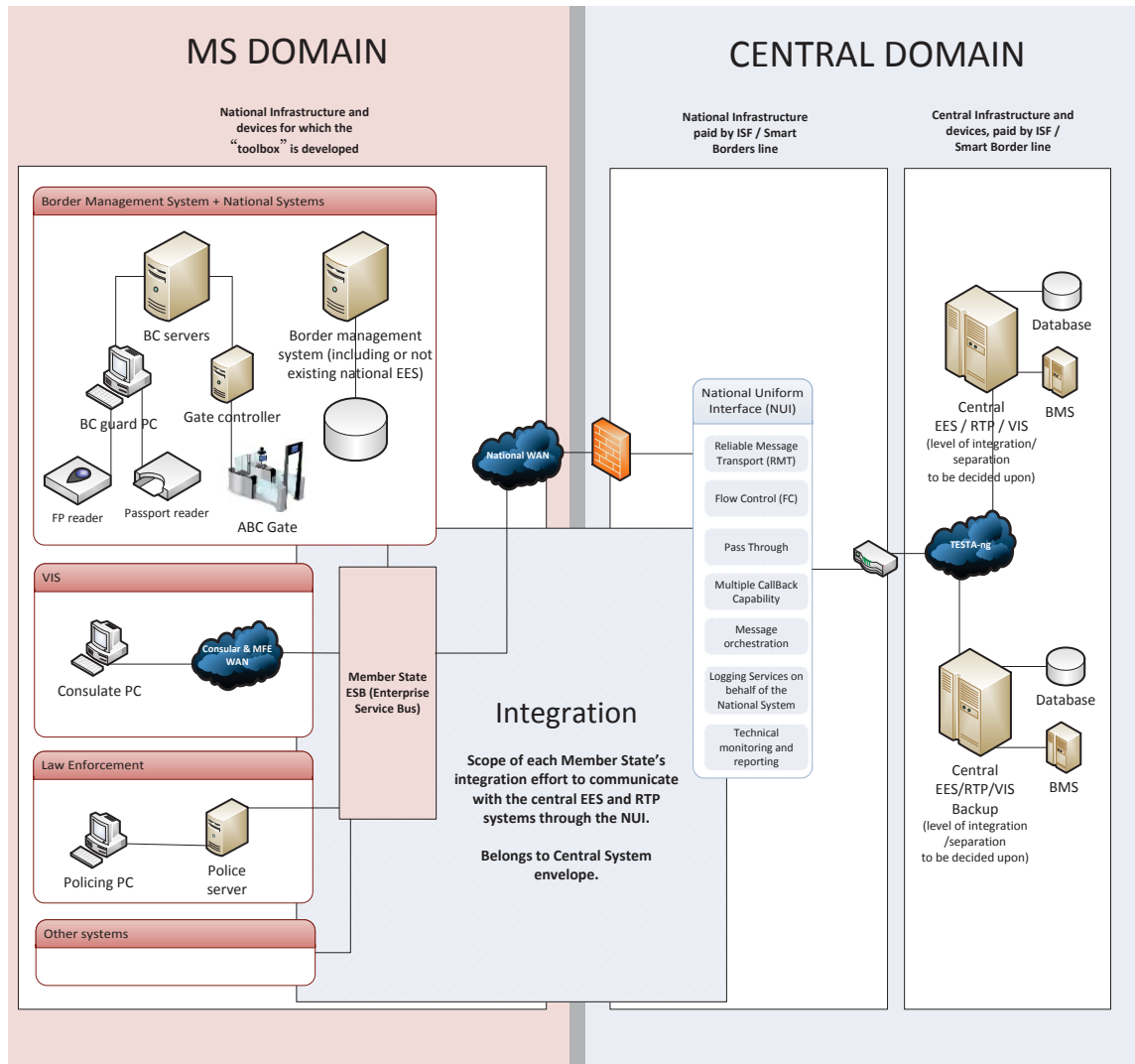


Figure: Split between the Central Envelope and Member States' budgets for the infrastructure of the EES and RTP systems. Blue sections (Central Domain and Integration) would be covered by the Central Envelope; pink sections would be covered by the Member State's own budgets or the National Programmes of the ISF borders/Smart Border Line.

The cost model developed and described in the Cost Report that is part of the 2014 Technical Study, contains a set of main assumptions and options.

Overall a cautious approach has been used throughout the report regarding cost estimation. This approach is aimed at avoiding underestimation of the final costs.

As this cost model is developed at a moment when only a concept of the Smart Borders system exists figures cannot be better estimated than with a 15 to 20% margin despite being accurate.

The following general assumptions were used for developing the model:

- Financial timeline: EES and RTP development period is expected to last three years, assumed to start in 2017 and ending in 2019. Both systems are expected to become operational in 2020.
- Benchmark with existing systems: The VIS and the SIS II provide benchmark data when relevant, as they operate in a comparable environment to that of the future EES and RTP. Experience values for contractor development cost were also taken from large-scale IT systems in other areas than Home affairs.
- National Uniform Interface (NUI): The assumption is that a NUI will be developed to provide the interface between the Member States (MS) and the Central System. The NUI enables Member States to connect to the Central System without having to develop and deploy their own infrastructure, reducing the complexity and the costs of the project. An envelope of €4 m is provisioned for each MS to cover the integration effort from their existing infrastructure to the central system. This option reduces the costs to be borne on Member States' side as the development costs of the NUI are shifted to the central side.
- SOA (Service Oriented Architecture)-based BMS (Biometric Matching System): the assumption is that a new SOA-based BMS serving the needs of VIS, EES and RTP will be developed.
- Number of Member States: 30 countries. This is the same assumption as in the 2013 proposal.
- Central Unit / Backup Central Unit (CU/BCU) configuration: the setup between two nodes is considered to be active/passive. This is also the current way the back-up sites of SIS II and VIS are designed. It means that only CU handles the transactions (active node) and that the BCU is only permanently updated so to remain in "hot" stand-by. In case the CU would be destroyed (or unavailable for a long time), the BCU takes over all operations. For cost purposes the investments in hardware and software are doubled compared to the situation where there is one single central unit and the cost for a redundant high-speed and high-capacity link between both sites is added to.

6.1.1. Cost comparison between different biometric options

The same study further identified three different TOMs (Target Operating Models) for EES and two TOMs for RTP. The three TOM's for EES correspond with the different biometric choices. The two TOMs for RTP correspond to the option (a) and (b) for doing the RT application.

EES:

- TOM A – Facial image from e-MRTD (Machine Readable Travel Document) as biometric identifier and relying on MRZ (Machine Readable Zone) (plus visa number for Visa Holders (VH)) as data for EES. Absence of systematic 1:N identification at first entry for TCNVE.

- TOM B – Facial image from e-MRTD and 4 fingerprints as biometric identifiers and relying on MRZ (plus visa number for VH) as data for EES. Systematic 1:N identification at first entry for TCNVE.
- TOM C – Facial image from e-MRTD and 8 fingerprints as biometric identifiers and relying on MRZ (plus visa number for VH) as data for EES. Systematic 1:N identification at first entry for TCNVE.

RTP:

- TOM M – Fingerprints (live)-only for VE- and photo (from e-MRTD) as biometric identifier for RTP. For VH, the FP used in the VIS will be used as the basis for verification and identification. In this TOM the enrolment of an RTP follows the process from the current legal proposal, which is very close to a visa application process: RT status is requested by the applicant (and this can be done via internet), interview with applicant takes place where his/her biometrics are captured (the number is equal to what the TOM A, B, C requires) and this cannot be done via internet, MS instructs the request and grants/refuses RT (this can also happen over internet).
- TOM N – No biometrics taken at enrolment (i.e. no physical visit necessary), existing biometrics (EES and VIS) used for verification purposes. In this TOM the enrolment of an RTP is only possible when the TCN has already travelled to EU Schengen area and is therefore recorded in the EES. The RT status is requested by the applicant via internet, no face to face meeting is necessary anymore as the applicant can provide all evidences via internet and the biometrics are in the EES personal file. Finally MS instructs the request and grants/refuses RT (this can also happen over internet).

TOM C and M are taken as the baseline for the calculation of the costs of the EES and RTP projects, as they are the most cautious in terms of costs as well as the closest to the existing legal proposals. In this section, the study evaluates the cost impact of the other TOMs on the overall project.

The general impact of TOMs is split between the cost components of the project. The study looked into each impacted cost component to provide an estimate of the cost impact of each TOM. The results will be presented as a fixed figure where possible, or as a percentage of the cost component.

The results are presented in the table below (comparison of costs over 4 years: 3 years development and one year operations):

	TOM A		TOM B		TOM C (baseline)	
	TOM M	TOM N	TOM M	TOM N	TOM M (baseline)	TOM N
EES	€214.3 m	€214.3 m	€225.2 m	€225.2 m	€226. m	€226. m
	95%	95%	100%	100%		100%
RTP	€194.6 m	€194.1 m	€204.4 m	€203.8 m	€204.4 m	€203.8 m
	95%	95%	100%	100%		100%
EES and RTP	€359.3 m	€358.8 m	€379.6 m	€378.3 m	€381. m	€379.1 m
	94%	94%	100%	99%		99%

This table supports the conclusion that the cost difference of the choice of the biometric identifier for EES and RTP enrolment solution is only significant when the facial image without fingerprints would be selected. The difference is however not more than 6% for the 4-year accumulated cost but which represents €22,2 million.

6.2. Marginal Cost of RTP

The cost model was developed in order to compute the cost for EES and RTP are each built as a system on its own and when EES and RTP are built as one system. In this last case, two major cost items being the BMS costs and the integration cost of the National Uniform Interface (NUI) are shared 50%-50% over both systems. The cost model does not provide the straightforward answer on how much RTP would cost if it was considered as "added" to the EES. In this case the major differences are that BMS and NUI development and integration costs are allocated 100% to EES, and that RTP network costs do not include the network set-up costs.

In order to compute the marginal cost of RTP, the difference needs to be made for the cost of EES and RTP built as one system and the cost for building EES alone. The cost model was first used to compute the cost of EES and RTP built as one system using 4 fingerprints and facial image as biometric identifiers and a data retention period of 5 years. Then the cost model was used for computing the cost of EES alone with the same assumptions of 4 fingerprints and facial image as biometric identifiers, a data retention period of 5 years, and costs for BMS (Biometric Matching System) and NUI (National Uniform Interface) allocated completely to this system. The results of both computations were then subtracted which gives:

Marginal of Cost of RTP (in million €)	Total (4 years)	Operational costs 2021 (2nd year)	Operational costs 2022 (3rd year)	Operational costs 2023 (4th year)	Total (7 years)
Total Central System	14,78 €	1,80 €	2,29 €	2,05 €	20,92 €
Total National Systems	59,31 €	19,71 €	19,71 €	19,71 €	118,44 €
Total envelope	74,09 €	21,51 €	22,00 €	21,76 €	139,36 €

Summary of the marginal costs of RTP obtained as the difference between the cost for EES and RTP as one system and the cost of EES alone

The result of this computation is that the **marginal cost of RTP** is estimated as € 74,09 million over four year (sum of € 52,58 million development cost and € 21,51 million operations costs for the first year - the details of this computation are not shown above). The cost of yearly operations is strongly impacted by the assumption that per Member State a small team of operators needs to be dedicated to RTP operations on a 365/24/7 basis (meaning to ensure a permanent service throughout the year).

The calculation of the marginal cost of the RTP system was done under the assumption of using TOM N (this is the operational model assuming the traveller has already been recorded in EES and therefore biometrics can be re-used). For the cost of the RTP system there is however only a marginal (like 1%) difference with the situation where TOM M would be used (this is the operational model where the traveller applies for Registered Traveller's status even before travelling, his/her biometrics are taken separately).²⁰

²⁰ See "Technical Study on Smart Borders – Cost Analysis" section 3.4 and accompanying tables: "TOM N does not have an important impact on the cost on the central envelope. The main purpose of TOM N being to rely on the EES for biometric matching of RTP members, and making online RTP enrolment compulsory, the impact is going to be felt on the national side as opposed to the central side, as RTP applications would be received directly online, reducing the need for administrative officers to deal with requests at the consular or administration post".

6.3. Cost of Preferred Solution

For computing the cost of the preferred solution, the following **specific assumptions** were applied to the cost model:

- Architecture: only one system is built (the Entry Exit System) and the development of a specific RTP is discarded. For the cost model this means that the EES has to bear the full BMS and NUI-related costs which were otherwise shared with RTP as these are two common architecture components.
- Architecture scope. The cost model has been amended to include the cost for having a fall-back solution whereby transactions are buffered at the level of the location(s) or Member State(s) from where the central EES was unavailable and released once the central EES can be accessed again. The cost model also includes the development and operations of a web-service for information to travellers and carriers.
- Architecture: the cost model has been adapted in order to take into account technical options for ensuring interoperability and system availability.
- Biometrics. The preferred solution assumes that the facial image and four fingerprints are taken as a biometric identifier. This corresponds to what is called the Target Operating Model B in the cost report. This model also assumes a systematic 1:n identification at first entry for visa-exempt third country nationals.
- Facilitation. The assumption is made that facilitation will use the "fast lane for all" concept. This concept does not impact the costs included in this model apart from giving the rationale for discarding a specific RTP.
- Retention time. A five-year data retention time for all travellers (visa-required and visa-exempted) is assumed. This has an important consequence on costs as the database accumulates data over 5 years and this impacts storage capacity and the cost of some specific software, like BMS, which evolves according to data volume.
- Law Enforcement access is granted from the beginning. This does not impact the cost model in an important way. The only significant cost impact stems from adding the capacity to BMS to also search on latencies.

The result of the cost model is provided on the following page. The **development cost** to be borne by the EU budget amounts to **€394,77 million, split as €222,10 million for the central system (including the National Uniform Interface) and €172,67 million for the (thirty) national systems (including the technical integration of national systems with the National Uniform Interface). This is the cost accumulated over the estimated three years required to build the system.** In addition, changes would be required to VIS (to establish interoperability between EES and VIS) and SIS (for the creation of an alert for overstayers not found at the end of the EES data retention period), which have been estimated as €40 million development cost and no additional operational costs.

The first year of operations the EU budget would bear a total operations cost of €45,47 million split as €25,76 million for the central system and €19,71 million for the (thirty) national systems.

When comparing with the MFF, the cost to borne by the EU budget amounts to €480,2 million over 4 years (3 years development and 1 year operations). This is the same amount as included in the financial annex to the legal proposal.

EES Development Cost

	2017	2018	2019	Total Develop- ment Cost	2020	Total over 4 years
Development Central System						
Contractor development	32.650.130	32.650.130	35.265.130	100.565.391	0	100.565.391
Software	8.051.249	0	46.559.996	54.611.245	3.555.000	58.166.245
Hardware	4.753.537	0	22.852.995	27.606.532	0	27.606.532
Administration	1.898.000	1.898.000	3.530.500	7.326.500	0	7.326.500
Set Up Data Center	219.336	0	0	219.336	0	219.336
Meetings/Training	816.000	816.000	1.740.936	3.372.936	327.370	3.700.306
	48.388.252	35.364.130	109.949.557	193.701.940	3.882.370	197.584.310
Maintenance Central System						
Contractor operations	0	0	1.734.254	1.734.254	1.748.254	3.482.509
Software	1.342.866	1.342.866	9.101.711	11.787.443	9.938.811	21.726.254
Hardware	568.525	568.525	2.925.348	4.062.397	3.585.748	7.648.144
Administration	0	0	0	0	4.208.000	4.208.000
Running costs Data Center	0	90.202	90.202	180.403	90.202	270.605
	1.911.391	2.001.592	13.851.514	17.764.497	19.571.015	37.335.512
Communication Infrastructure (Network)						
Network development	4.122.530	0	210.000	4.332.530	0	4.332.530
Network operations	1.995.303	1.995.303	2.310.303	6.300.908	2.310.303	8.611.210
	6.117.833	1.995.303	2.520.303	10.633.438	2.310.303	12.943.740
Total Central System	56.417.475	39.361.025	126.321.374	222.099.874	25.763.687	247.863.562
Integration in Member States						
Contractor development (integration of NUI)	40.000.000	40.000.000	40.000.000	120.000.000	0	120.000.000
Administration	16.236.000	16.236.000	20.196.000	52.668.000	0	52.668.000
Operations of National Systems						
Administration	0	0	0	0	19.710.000	19.710.000
Total National Systems	56.236.000	56.236.000	60.196.000	172.668.000	19.710.000	192.378.000
Total EES (including SIS/VIS adaptations)				394.767.874	45.473.687	440.241.562
SIS/VIS adaptations		20.000.000	20.000.000	40.000.000		40.000.000
Total EES (including SIS/VIS adaptations)						480.241.562

7. ANNEX 7: COMPARISON OF OPERATIONAL ASPECTS OF DIFFERENT BIOMETRICS

Option	Fingerprints (FP) only	Fingerprints (FP) and facial image (FI) combined	Facial image (FI) only	Iris and facial image (FI) combined
Stability	<p>FP are stable from the age of six years onwards.</p> <p>Enrolled FP remain valid for many years.</p>	<p>See column on the left for FP and on the right for FI.</p>	<p>FIs are more stable as the person gets older.</p> <p>FI loses its relevance as a reference biometric over time: 10 years is seen as a maximum while 5 years is the preferred option for renewal.</p>	<p>Iris is a stable biometric from a few days after birth and throughout life.</p> <p>See previous column for FI.</p>
Enrolment	<p>The more FP (1,2,4,8 or 10) are enrolled the more time it takes. Taking 8 FP's takes about two times more time than 4 FP's. Taking 10 FP's takes about three times more time than 4 FP's.</p> <p>Environmental conditions (weather, type of border) can make practically impossible the enrolment of more than 4 FP even with high performance equipment.</p> <p>Taking 1, 2 or 4 FP's takes about</p>	<p>The enrolment time and complexity is the combination of both. FI and FP can be taken at the same place and can even be combined to some extent so that enrolment time does not cumulate.</p>	<p>A quality FI can be taken fairly quickly in all situations.</p>	<p>When iris is taken at a distance, the enrolment time is fast and FI is the biometric that is considered to be "obtained for free" as the software driving the camera needs to recognise a face first before zooming in on the eyes to capture the iris pattern. The camera for FI and iris pattern capturing is not the same but both are combined in the same device.</p> <p>When iris is not taken at a distance the enrolment times of</p>

Option	Fingerprints (FP) only	Fingerprints (FP) and facial image (FI) combined	Facial image (FI) only	Iris and facial image (FI) combined
	the same time and is possible in all environmental circumstances.			taking the iris pattern and the facial image cumulate as they happen in front of different devices.
Verification	In practice, 1, 2 or 4 FP are sufficient for a reliable and fast verification. (Note: at least the same number of verified FP needs to have been enrolled)	Using both FP and FI does not improve verification. One of the two biometric identifiers is enough for that purpose.	FI is enough for a reliable and fast verification, because verification only matches the FI with the live picture of a particular person.	Using both iris and FI does not improve verification. One of the two biometric identifiers is enough for that purpose
Identification for inland controls	At least 4 FP are required for a reliable identification on a 100 million gallery size.	At least 2 FP and FI are required for a reliable identification on a 100 million gallery size	FI can only be used for identification on a 1 million gallery size.	The iris pattern taken at a distance and FI allow a reliable identification on a 100 million gallery size. However the reliability percentage is inferior to the obtained using 4FP's and a FI.
Identification at the border (when required processing capacity is available)	At least 8 FP are required for a fast and reliable identification on a 100 million gallery size	At least 4 FP and FI allow a fast and reliable identification on a 100 million gallery size	FI alone is not suited for that purpose. Increasing processing capacity does not solve the issue.	
Exceptions	Experience with VIS shows that about 2% of travellers have no FP mainly because these are worn out (result of heavy manual work).	See column on the left for FP's and on the right for FI. The FI acts as a "fall-back" in case no FP can be taken.	None: a facial image can be taken from all travellers ("everybody has a face")	Iris is difficult to take for a small portion of population. See column on the left for FI. The FI acts as a "fall-back" in case no iris can be taken.

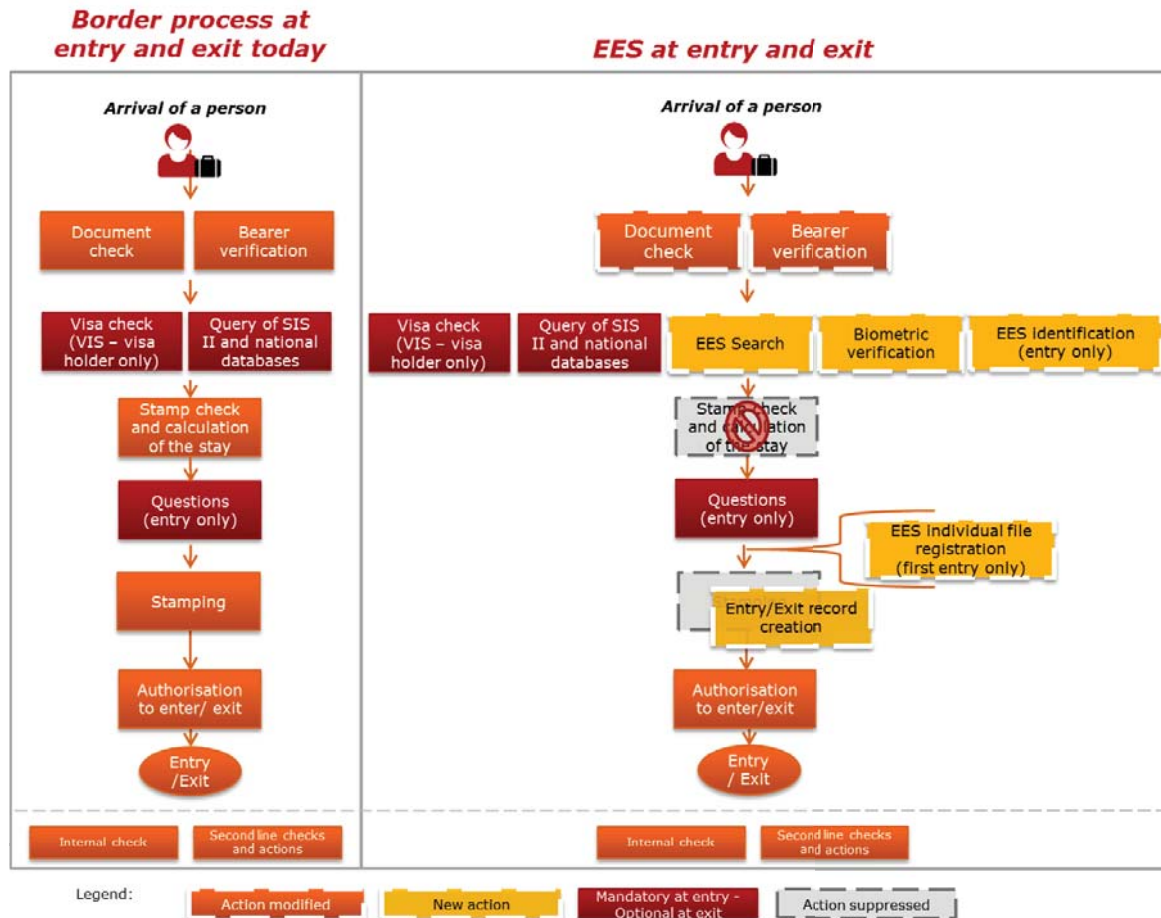
Option	Fingerprints (FP) only	Fingerprints (FP) and facial image (FI) combined	Facial image (FI) only	Iris and facial image (FI) combined
Risk of fraud	FP's can be spoofed and countermeasures are mandatory (liveness detection).	Multi-modal biometrics are less prone to be spoofed as two biometrics need to be counterfeited. Countermeasures remain mandatory.	FI can be spoofed and countermeasures are mandatory (liveness detection).	Multi-modal biometrics are less prone to be spoofed as two biometrics need to be counterfeited. Iris is not less nor more prone to be spoofed than other biometrics. Countermeasures remain mandatory.
Cost implications: cost for installing and operating the biometric capturing/reading devices at the border control points (this is what is borne by Member State budgets potentially co-financed by the Internal Security fund).	The devices implemented for the deployment of VIS checks at the border can be re-used as long as 4 or less FP are enrolled at the border, and therefore also used for verification. When 8 or 10 FP's are enrolled, all devices (mobile and fixed) must allow the enrolment of at least 2 FP's at once.	See column on the left for FP and on the right for FI. So there is an additional investment required for handling FIs.	Devices for taking and comparing FI will need to be installed at all borders. The cost per device is however low.	Iris at a distance requires an expensive device (a few thousand € a piece) and would require all border posts to be re-equipped.
Cost implications: cost for building and operating the central system and the national systems connected to it (this is what is paid for by the EU budget)	This cost is only marginally (a few percentages difference) affected by the choice of biometrics. The difference originates from the network costs for the message exchange between national and central systems: the more biometrics are used, the "heavier" the messages. However this effect is strongly counter-balanced by the fact that network costs are only one item among many. The biggest budget impact stems from the inclusion or not of a systematic <u>identification</u> at the border for all travellers			

8. ANNEX 8: NEW SMART BORDER PROCESSES

The contents of the pages in this annex are mainly taken from section 3.2.2 – Process description of the 2014 Technical Study report. A reference to that section would not have been sufficient as the description has now been adapted on the basis of the options selected for the preferred solution.

8.1.1. Overview

The following picture shows the major differences between the current and future processes at entry and exit.



The entry and exit processes for the EES would be integrated within the existing overall border control process, as regulated in the Schengen Borders Code. The main changes to the generic process would be the ones highlighted in yellow:

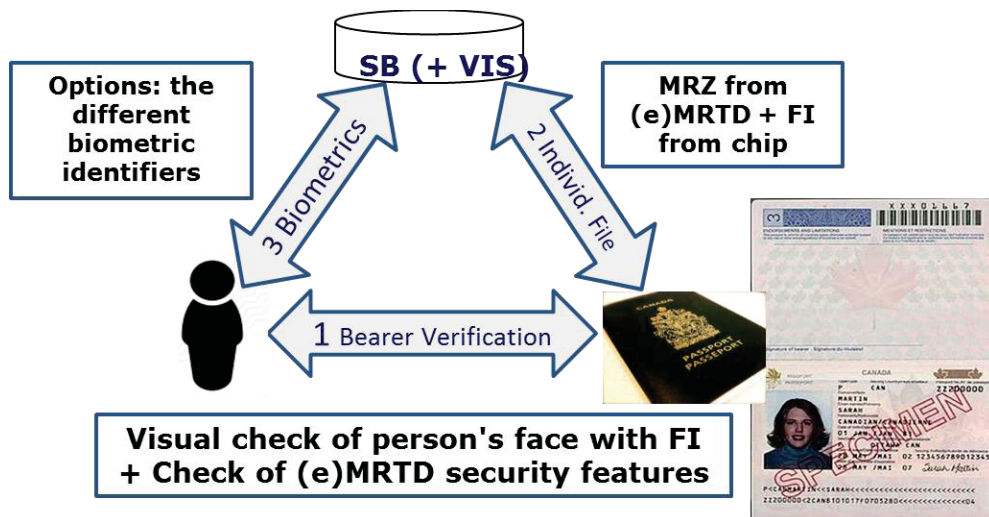
- **EES Search.** At every border crossing, as part of the verification, a search is run in the EES. The combination of issuing country and the document number, captured from the MRZ of the travel document are sufficient for doing this search.
- **EES FP's Identification.** A 1:N identification to the EES using 4 fingerprints and the facial image would help detect duplicates in the EES, to avoid that the same person would have more than 1 individual file registered.

- **Biometric verification.** When a person is found in the EES, further verification is made to secure the identity of the person, by electronic use of biometric data and/or by manual verification.
- **EES individual file registration.** In the case of a first entry, an individual file on the person will be registered in the EES. This would include an alphanumeric dataset and the addition of biometric data in the form of fingerprints and a photo.
- **Entry/exit record creation.** All entries/exits are recorded in the EES with data specific to the crossing (date, border crossing point, authority granting access).

Stamping and checking of stamps is abolished. The stakeholders concerned will be able to retrieve or receive information as regards the remaining number of days for the allowed stay.

The Identification Triangle

Whatever the way the process is described the key element is that the "identification triangle" remains. This "identification triangle" means that the consistency needs to be established at each border check between the person, the travel document (passport and visa) and the Smart Borders (SB) system, supplemented with VIS in case of visa-holders:



The first side of the triangle is the **"bearer" verification** which checks whether the traveller is the rightful owner of the passport (and visa). The most common way this is done is the border guard checking whether the passport is real (check of the optical security features of the passport and comparing the picture in the passport with the bearer). The introduction of e-Passports (e-MRTD's) allows this to be supported or even automated.

The second side of the triangle makes the **link between the travel document and the record in the Smart Borders (SB) system**. The most common way this is done is using part or all of the data in the MRZ (Machine Readable Zone) and querying the SB database. The result should be that either the system responds that the person does not exist in the system yet or that a person with that passport has already been recorded and that the MRZ data match with the ones in the individual file in the SB system. With e-Passports the data from the chip (which sometimes provides the advantage of not being truncated) can be used rather than the data from the MRZ.

The third side of the triangle is the **match between the person and the identity** that is recorded, the answer to the question *"is this person the one we know with that identity"*? This is done using biometric identifiers: a biometric reference sample needs to be taken at enrolment (the preferred choice is facial image and four fingerprints taken flat) and a new sample taken to verify whether it matches with that reference. While enrolment and verification of the facial image is the same operation (a digital picture is taken), there is a difference with fingerprints: enrolment needs to be done carefully for multiple fingerprints (four in this case) while verification can be done quickly with only one fingerprint.

8.1.2. Detailed Border processes at entry and exit

Table 1 Border processes at entry and exit today

	Entry/ Exit	TCN- VEs TCN- VHs	Description
Document check	Entry Exit	✓	Manual verifications of valid travel documents or other document authorising a traveller to cross the border and where applicable the requisite visa or residence permit. The documents are also checked to detect falsifications.
Bearer verification	Entry Exit	✓	Manual checks made to secure that the bearer of the travel document is the lawful owner of the document (side 1 of the identification triangle).
Visa check (VIS)	Entry Exit <i>optional</i>	<i>Only TCN-VHs</i>	Schengen visas are issued at consular posts around the world. The VIS is checked, using fingerprints (1, 2 or 4) and the visa sticker number ²¹ (side 2 using the visa-sticker number vs. VIS and side 3 of the identification triangle for visa-holders).
Stamp check	Entry Exit (optional)	✓	Stamps are checked and the stay is calculated manually.
Questions	Entry	✓	Questions are asked as regards: <ul style="list-style-type: none"> • the purpose of the stay; • sufficient means of subsistence for the duration of the stay and the return to the

²¹ Fingerprints are mandatory as of October 2014. By the end of 2015 all consular posts register the visa information in the VIS (the end of the so-called VIS roll-out).

			country of origin;
			<ul style="list-style-type: none"> • other supporting documents (e.g. tickets, hotel reservations or invitations to meetings).
SIS II check (and other databases)	Entry	✓	SIS II and other relevant systems are checked to verify that the person is not a threat to public policy, internal security, public health, or international relations of any of the Member States or not allowed in the Schengen area.
	Exit	- <i>optional</i>	
Stamping	Entry	✓	The passport is stamped.
	Exit		
Authorisation to enter/exit	Entry	✓	When the result of all checks can be approved, the passport is stamped and the person can be granted access to the Schengen area.
	Exit		
Internal checks		✓	After going through the border checks and gaining entry, a person can still be checked in the national territory (either as part of a police check or an identity check by authorities responsible for immigration).
Second line checks and actions	Entry	✓	Depending on the results of all the checks and on the questions and observations included at the border crossing, there could be alternative actions taken related to law enforcement, migration and asylum or to verify certain requirements (e.g. checking that the document is valid or that it is not a forgery). Those actions are not described here but can be seen as part of the overall Border Control Processes.
	Exit		





The following table describes the border processes at entry and exit as would result from the preferred solution. This process description does not detail the required tools. There is no absolute sequence of activities prescribed whether in the pictures or in the text. Some activities do have a sequence, guided by mere logic or by the Schengen Borders Code, and others can be done in parallel, depending on the routines and equipment at the specific border crossing point.


As the legend on the chart above indicates the overall border crossing process is modified in different ways:


- The actions related to the verification of the visa are not changed,
- The actions involving stamping of travel documents at entry and exit are replaced by a new action: the recording of the entry or exit in EES,
- The other actions in the border crossing process remain but are modified due to EES.

Table 2 Border processes with the use of EES

	Entry Exit	TCN-VE TCN- VH	Description
Document check	Entry	✓	<u>Action modified</u>
	Exit		Manual verifications of valid travel documents or other document authorising a traveller to cross the border and where applicable the requisite visa or residence permit. The documents are also checked to detect falsifications. <u>Modification</u> <i>For travellers with Electronic MRTD:</i> Both for manual and ABC gates, the Study and the Pilot confirmed the need and feasibility to include Passive Authentication (PA), which is a mandatory check according to ICAO standard 9303. PA verifies the integrity of the contents of the various on-chip Data Groups (containing biographic information, facial image, fingerprints, etc.). Furthermore, where feasible, the discretionary Active Authentication (AA) or Chip Authentication (CA) may be added. AA/CA verifies the authenticity of the chip on which the Data groups reside. <i>For travellers with Non-electronic MRTD:</i> In this case, the documentation check for falsifications is limited to manually checking the traditional document security safeguards (e.g. ink and optically variable elements).
Bearer verification	Entry	✓	<u>Action modified</u>
	Exit		Manual checks to ensure that the bearer of the travel document is the lawful owner of the document (side 1 of the identification triangle). <u>Modification</u> <i>For travellers with Electronic MRTD:</i> Both for manual and ABC gates, the Study and the Pilot concluded on the feasibility of doing a biometric verification of the live captured photo against the photo stored on the chip. For manual gates, this recommendation would imply that investments have to be made in camera equipment, since this type of equipment does not normally exist at manual gates today. This action applies for checks at first entry and for TCN-VEs. TCN-VHs are considered to be verified as part of the visa application process. <i>For travellers with Non-electronic MRTD:</i> In this case, the authentication check is limited to manually checking the picture on the document against the document holder.
VIS (VIS)	Entry Exit	<i>Only TCN- VHs</i>	<u>Action modified</u> The VIS is checked, using fingerprints (1, 2 or 4) and the visa sticker number (side 2 and 3 of the identification triangle for visa holders). At exit, the VIS check described above is not mandatory.

	Entry Exit	TCN-VE TCN- VH	Description
			<u>Modification</u> The document number and country code (from MRZ or from the e-Passport) is used to proceed with the check in the VIS.
SIS II check (and other databases)	Entry Exit	✓	<u>Action not modified</u> SIS II and other relevant systems (e.g. Interpol, national databases/watch lists) are searched (SIS II searches are optional at exit) to determine whether the person could be refused entry, is wanted and/or constitutes a threat to public security.
EES Search 	Entry/ exit	✓	<u>New action</u> A search is made in the EES using the issuing country and the document number, taken from the MRZ or from the data in the passport chip. The date of birth and the name can be used automatically for further searches, if needed (side 2 of the identification triangle).
Biometric verification 	Entry/ Exit	✓	<u>New action</u> If the person is found in the EES, a biometric verification is made by either using the facial image or the fingerprints stored in the traveller's individual file (side 3 of the identification triangle). At entry: For TCN-VHs - the biometric verification done via the VIS check is trusted. At exit: <ul style="list-style-type: none"> • For TCN-VHs, the check made against the VIS is trusted, if it is made (it is not mandatory at exit). If no VIS check is made, the verification related to EES is manual (ocular), using the photo of the travel document or a displayed stored photo from EES; • In ABC gates a) making an automated Document check (using at least Passive Authentication), b) making a Bearer verification using the e-MRTD and facial recognition and c) ensuring the EES and VIS data exist for the traveller would validate the chain of trust and so would be seen as sufficient, also without a biometric verification against the VIS.
EES fingerprint identification 	Entry	✓	<u>New action</u> If the person is not found in the EES on the basis of the travel document data, a biometric 1:N search for identification is launched using four fingerprints and the facial image taken live. The identification is for the purpose of finding duplicates in the EES database, meaning the same person appearing more than once, with different names and/or documents. This identification is done at <u>entry</u> and for <u>TCN-VEs</u> . TCN-VHs are identified as part of the visa application process and this should keep the risk of having duplicates to a minimum.

	Entry Exit	TCN-VE TCN- VH	Description
Questions	Entry	✓	<p><u>Action not modified</u></p> <p>Questions are asked as regards:</p> <ul style="list-style-type: none"> • The purpose of the stay; • Sufficient means of subsistence for the duration of the stay and for the return to the country of origin; • Other supporting documents (e.g. tickets or invitations to meetings); • The level of detail of questions and answers is adapted according to the travel history as shown in the EES.
<p>EES individual file creation</p> 	First entry	✓	<p><u>New action</u></p> <p>If the person is not found in the EES (by means of the search and the identification actions), a first-time registration of an individual file is made. This includes data from the MRZ (captured from e-MRTD or MRTD), and biometrics. This is creating the link between the travel document and the SB database.</p> <p>For TCN-VE, four fingerprints and a photo from the e-MRTD, or a live photo are stored in the individual file. This is creating the link between the traveller and the SB database. For TCN-VEs, using an MRTD, a live photo is stored. Only in a last resort would the printed photo from the MRTD be stored as this can only be used for manual verification (ocular, using a display of the stored photo) at subsequent entries/exits, since the quality is not good enough for current automated matching algorithms.</p> <p>For TCN-VHs, the fingerprints are already stored in the VIS and no enrolment is needed for these in the EES. A photo, preferably from the e-MRTD or a facial image taken live, is stored in the EES individual file.</p> <p>The use of photo in the EES</p> <p>The main reasons for the use of photo as a complementary biometric identifier in the EES process are the following:</p> <ul style="list-style-type: none"> • By using the photo of the e-MRTD (chip) it is possible to make a bearer verification against a live photo, which would highly improve the security of the border process in general; • Storing a photo from the e-MRTD or a live photo of sufficient quality in EES, means that there would be a biometric identifier that can be used in subsequent electronic and automatic (e.g. ABC-gates) verifications, in the border control process. The stored photo could also be used for manual (ocular) verifications, by displaying the photo and compare this to the traveller being checked; • Scanning and storing a printed photo in EES is of limited or no use for electronic or automated verifications, but can be useful in manual (ocular) verifications, where the photo can be displayed;

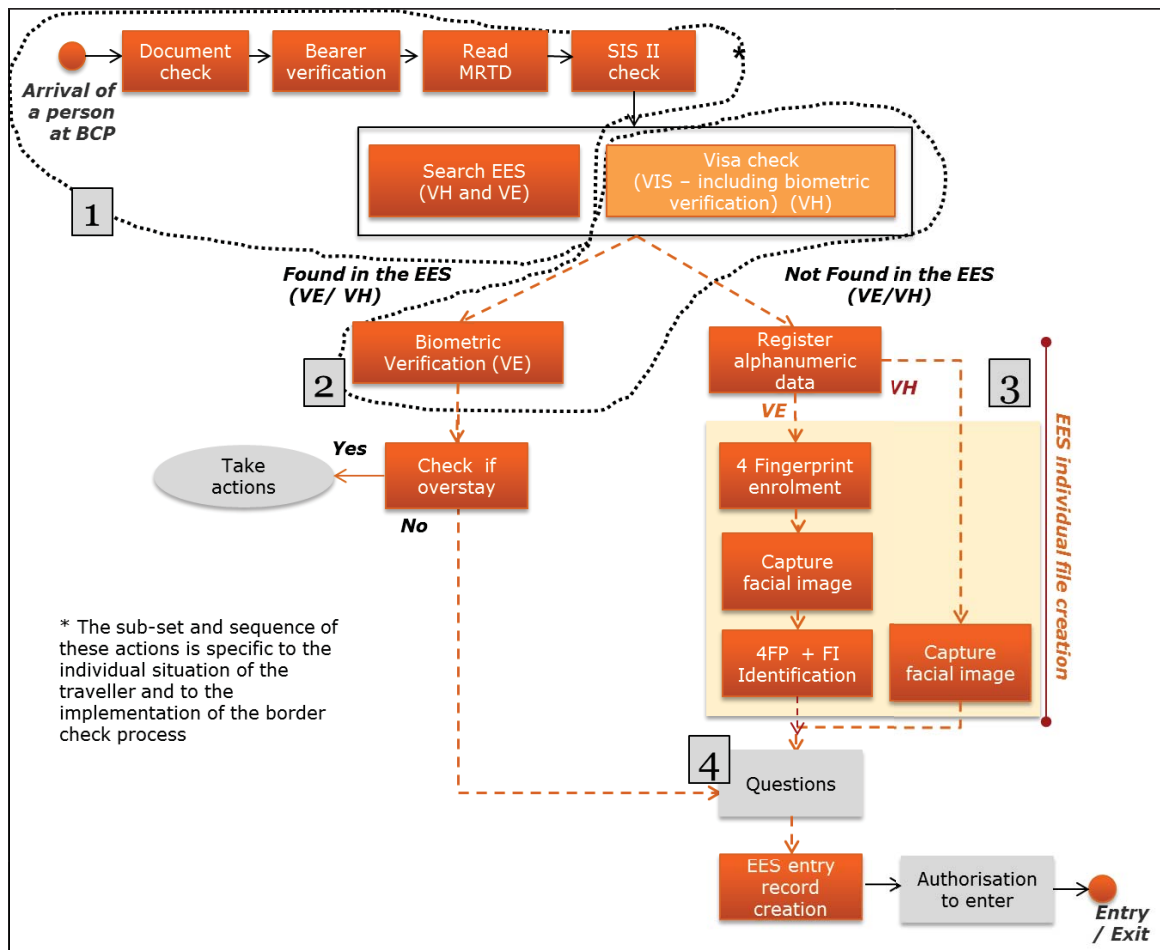
	Entry Exit	TCN-VE TCN- VH	Description
			<ul style="list-style-type: none"> • A stored photo in EES, from any of the sources mentioned, can always be used for identifying travellers believed to be overstayers.
EES entry/exit record creation	Entry/ exit	✓	<u>New action</u> Entry/Exit data is entered in the entry/exit record in EES. Data are either copied from the chip in the e-MRTD or from the Machine Readable Zone of the MRTD.
			
Authorisation to enter/exit	Entry Exit	✓	<u>Action modified</u> Once all checks have been made and approved, and once the EES record creation is complete, the person can be granted access to the Schengen Area. <u>Modification</u> If the person is not granted access the refusal of entry is recorded in the EES.
Second checks and actions	line and Entry Exit	✓	<u>Action not modified</u> Depending on the results of all the checks and on the questions and observations included at the border crossing, alternative actions could be taken in relation to LEA, migration and asylum. These are not described here but can be seen as part of the overall border process.
Internal checks	Entry	✓	<u>Action not modified</u> After going through the border checks and gaining entry, a person can still be checked in the national territory, either as part of a police check or security check.

8.1.3. Implementation of Processes at Entry

The description provided under the previous heading, can be split between the standard process at entry and at exit.

The mainstream process at entry can be represented in a flow diagram on the following chart. By "mainstream" is meant that the diagram does not show the actions when a step identifies a discrepancy between data.

The actions that are grouped by a dotted black line and numbered 1 to 4 are the group as actions that are distinguished by the traveller.



*Mainstream Smart Border Process Flow at Entry
 – (Group of) Actions 1 to 4 identifiable by the traveller
 VE= visa-exempt third country nationals; VH= visa-holder third country nationals*

The necessary sequence of actions is that:

- The process needs obviously to start with the document check and the bearer verification (refers always to the first check in the identification triangle).
- Once the travel document can be trusted, the traveller's personal data (taken from the MRZ or from the chip (passport or e-passport) can be used (action "Read MRTD") for querying different databases (SIS II, EES and VIS in the case of TCN-VH, but also Interpol and national databases). It can be noted that these queries can be launched simultaneously and have response times measured in at most a few seconds.
 The queries in EES (it is already the case with VIS) use an advanced search engine that retrieves identities despite spelling variations and thus can address the situation where the *same* person has a new or a different legally issued²² passport.
- The process differentiates the cases where VE and TCN-VH are found in EES and the cases where VE and TCN-VH travellers are not found in EES (but where the visa-application exists in VIS).

²² The cases referred here are the ones where a person has multiple passports issued by the same authority, multiple passports issued by different authorities because he/she has different nationalities, but where the biographical information is the same (same name, date of birth, etc.).

- The TCN-VH is authenticated by means of at least one fingerprint vs the fingerprints stored in the VIS application (side 3 of the identification triangle is confirmed) as part of the mandatory border crossing process for VH. This process assumes the VIS retrieves the visa application using the travel document number (and issuing country) read during the action "Read MRTD".

In the case the traveller is already recorded in EES (= side 2 of the identification triangle is established as an individual file matches the data from the travel document read) – part left on the slide:

- The process considers that the match between the biometrics (1, 2 or 4 fingerprints) of the VH and the reference sample (10 fingerprints) recorded in VIS is sufficient. In the case of a TCN-VE the facial image either taken live or taken from the passport chip or at least one fingerprint (according to the BCP set-up) is matched vs the biometric samples (4 fingerprints and a facial image) stored in EES. The biometric verification of the TCN-VE closes side 3 of the identification triangle and ensures the entry record is made for the same person as the one who was enrolled.
- The EES response provides also the status on the remaining number of days of authorised stay (action "Check overstay").

In the case the traveller is not recorded in EES – part right on the slide:

- The alphanumeric data from the travel document automatically populate a new EES record (action "Register alphanumeric data").
- In the case of a TCN-VH, only the facial image, either taken live or from the passport chip (action "Capture facial image"), is added to the newly created EES record.
- In the case of a TCN-VE, 4 fingerprints (of the right hand in the mainstream case) are enrolled (action "4 Fingerprints enrolment") as well as the facial image, again either taken live or from the passport chip (action "Capture facial image").
- For TCN-VE, both biometric identifiers are used to launch a process of identification (action "4FP and FI identification") where the reference samples are compared with all the samples in the database to find whether the same person has already been recorded under a different identity. This is not done for TCN-VH because it was part of the visa issuance process.

The next steps are again common for all TCN:

- The border guard asks the questions (action "Questions") in compliance with the "thorough investigation" required by the Schengen Border Code. The EES does not modify these questions.
- When the questions are satisfactorily answered, the border guard authorises the entry which creates the entry record in EES (steps "EES record creation" and "Authorisation to enter"). In the negative case (not shown on the chart), the refusal of entry is also recorded in EES together with the reason of the refusal.

From the description above it can be observed that all the steps performed except the questioning part (therefore mentioned in grey), are either triggered by reading the passport data or by providing biometrics. Therefore the proposal is made to use self-service kiosks for letting the traveller do this data and biometrics collection work himself.

From the traveller point of view as well as in order to estimate the duration for border clearance there are three steps to go through in case of a return visit and four steps at a first visit as can be seen on the chart above (the groups of actions surrounded by a black dotted line and with a number in a square).

In case of a return visit to the Schengen area (within the data retention period), there are three steps experienced by the traveller, where only step (2) is due to Smart Borders:

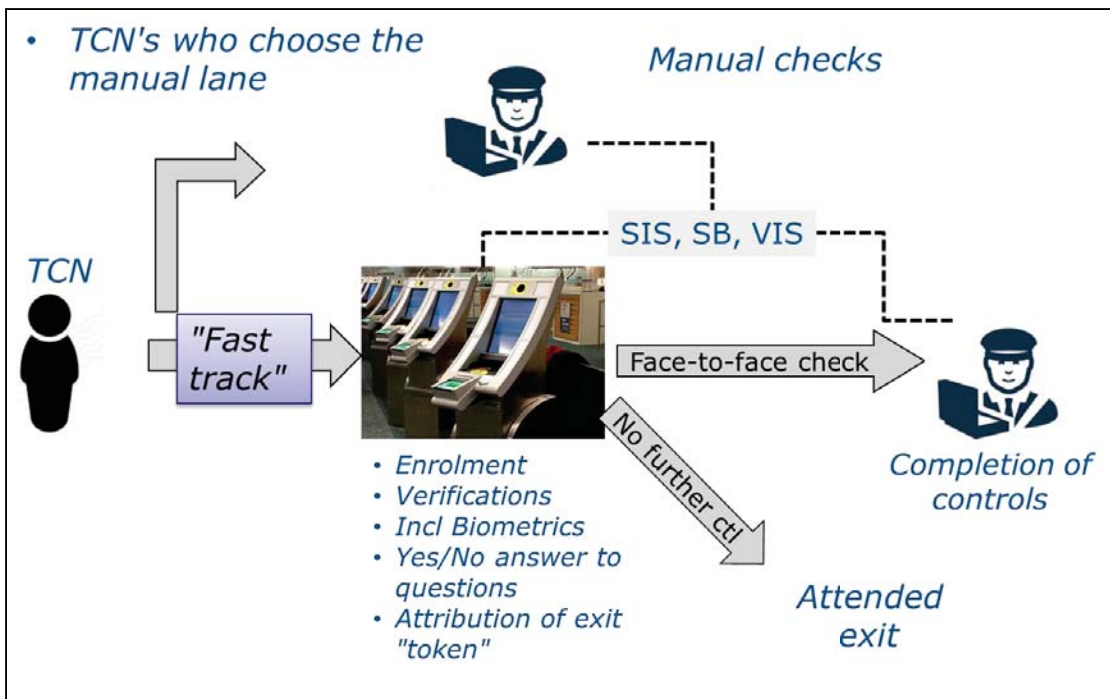
- (1) Hand over his/her passport which triggers the passport authentication, bearer verification and the query of the databases.
- (2) The biometric verification step.
For TCN-VH: put 1, 2 or 4 fingers for biometric verification (vs VIS).
For TCN-VE: put 1, 2 or 4 fingers for biometric verification or have a picture taken live or copied from the passport chip (vs EES).
- (3) Answer questions.

In case of a first visit to the Schengen area there are four steps experienced by the traveller, where only step 3 is due to Smart Borders:

- (1) Hand over his/her passport which triggers its authentication and the query of the databases.
- (2) The biometric verification for TCN-VH.
For TCN-VH: put 1, 2 or 4 fingers for biometric verification (vs VIS).
- (3) The biometric enrolment for TCN-VE and completion of enrolment for TCN-VH:
 - For TCN-VH: have a picture taken live or copied from the passport chip to be added to newly created EES record.
 - For TCN-VE: put 4 fingerprints of the right hand on the fingerprint scanner plate and have a picture taken live or copied from the passport chip to be added to the newly created EES record.
- (4) Answer questions.

8.1.4. Accelerated processes at Entry

The process at entry is more time-consuming than the exit process as there are more steps to be executed. The "Fast-track" or "Fast-Lane" process is built by proposing that the traveller performs routine border control tasks on a self-service kiosk (at its own pace) and that the border guard completes the border control, as defined in the current SBC (Schengen Border Code), using the information introduced by the traveller and the results of the queried databases. This general idea is now detailed further.



In what follows it should be understood that the travellers never see the results of operations but only the confirmation that the operation was done. This is the same for a manual control: the traveller does not see the border guard screen and mainly follows oral instructions.

The manual process is described as the "mainstream process". The following description only addresses the situation of the "fast track" process. The steps are not referred to on the picture.

Step 1: Reading the Travel Document

The traveller is requested to scan his/her passport by putting it on the kiosk passport reader.

In the case of an e-Passport, the passport reader accesses the chip, performs a passive authentication and reads the picture from the chip. On the basis of the data read from the chip, a query is launched simultaneously to the EES, the SIS, the Interpol database and the national databases and, in case of a TCN-VH, to the VIS.

In the case of a non-electronic passport, the passport reader scans the biographical page of the passport. The same query is triggered to the EES, the SIS, the Interpol database and the national databases and, in case of a TCN-VH, to the VIS.

In the case of an e-Passport, the check of the electronic security features of the passport confirms that the passport chip data is genuine. In the case of a non-electronic passport, the next steps are done assuming that the passport is authentic. This assumption will have to be confirmed by a border guard.

Step 2A - First entry: Enrolment

In the case of a first entry or a return visit beyond the data retention period, the EES has found no individual file and prompts immediately for an enrolment.

The kiosk camera takes a live picture from the traveller, scans the picture from the biographical page and stores both in EES. In the case of an electronic passport, the live picture is compared by means of facial matching software with the picture taken from the passport chip and provides a matching score. In the case of a non-electronic passport no comparison can be performed.

In the case of a TCN-VE, the traveller is requested to place four fingerprints on the kiosk fingerprint scanner. These fingerprints are recorded in EES and will be used as the reference sample for biometric verifications at return visits.

In the case of a TCN-VH, the traveller is requested to place one to maximum four fingers on the kiosk fingerprint scanner and these fingerprint scans are compared by the BMS (Biometric Matching System – the biometric system supporting VIS) with the fingerprints recorded in VIS at visa application. This operation confirms that the traveller is the TCN having been granted the visa.

After completion of the biometric enrolment, the traveller is invited to answer a series of questions on the points of departure and destination, purpose of the intended stay, means of subsistence and means of return.

The EES has created the individual file with the enrolled biometrics.

At the end of the process an "exit" token is created. The exit token allows identifying the traveller having completed the self-service process. This token can be material (printed piece of paper) or virtual (the traveller's picture or a fingerprint used as a token) and can therefore be decided on in each BCP.

In any case, the traveller is directed to a manual booth for completion of the control and enrolment process.

Step 2B - Return visit: Identity verification and check of entry conditions

In the case of a return visit within the period the data are kept, the EES has found the individual file and prompts immediately for the verification.

An identity verification (matching the traveller vs. the document and vs. the EES or VIS contents) is performed and the traveller is requested to answer a series of questions concerning the purpose of intended stay and the means of subsistence.

The kiosk camera takes a live picture from the traveller and compares it by means of facial matching software with the picture from the passport chip and with the picture retrieved from the EES. In the case of a non-electronic passport the live picture is compared only with the picture retrieved from the EES. Facial matching software compares the live picture with the picture in the EES record and provides a matching score.

In the case of a TCN-VH, the traveller is requested to place one to maximum four fingers on the kiosk fingerprint scanner and these fingerprint scans are compared by the BMS (Biometric Matching System – the biometric system supporting VIS) with the fingerprints recorded in VIS at visa application. This operation confirms that the traveller is the TCN having been granted the visa.

After completion of the biometric verification, the traveller is invited to answer a series of questions on the points of departure and destination, purpose of the intended stay, means of subsistence and means of return.

The EES computes the remaining number of days of authorised stay and displays it to the traveller.

At the end of the process an "exit" token is created. The exit token allows identifying the traveller having completed the self-service process. This token can be material (printed piece of paper) or virtual (the traveller's picture or a fingerprint used as a token) and can therefore be decided on in each BCP.

Depending of the results of the self-service process, the traveller is directed to an (automatic) gate or to a manual booth for completion of the control process.

Step 3A – Special case: Exit without further checks

On border guard decision, the traveller at the kiosk receives what has been called the "exit" token that indicates that s/he can leave without a face-to-face interview with the border guard. This token allows passing directly to the "attended exit" as mentioned on the slide. As mentioned in the title this is not expected to be the mainstream case for most border crossing points.

This exit needs to be attended to avoid that travellers having to go to a manual booth would use it and also to allow a border guard to perform random checks. The "attended exit" can be implemented by installing an automatic gate using facial recognition. The EES entry record is created at the moment of crossing the gate.

The minimum criteria to be met in order for the border guard to dismiss travellers from further controls are:

- The traveller is “known” in EES or VIS, so in all cases newly enrolled travellers do have to pass via a border guard.
- The traveller has an electronic passport whose electronic security features were checked with a positive result in the kiosk.
- All the queried databases render a favourable result: no hit in SIS, Interpol or national databases.
- The biometric matching scores (of the biometry used in EES and the one in VIS for TCN-VH) yield values that leave no doubt on the complete correspondence of the traveller's identity and the identity in the reference databases.
- The EES travel history does not show any overstay at the occasion of previous travels to the Schengen area.
- The TCN-VH does have a valid multiple-entry visa. This facilitation must not be given to visa-required travellers with single or double entry visas.
- The answers to all questions demonstrate full compliance with the conditions on thorough checks under SBC Art 7.3.(a) in particular points (iv), (v) and (vi).

The conditions mentioned above could then be dynamically updated by considerations on age of the traveller, travel route, place of departure, travel history in EES, etc. or simply left to the appreciation of the border guard.

Step 3B – Main case: Completion of controls by a Border guard

The mainstream case will be that either the traveller did not complete all the steps or that the border guard considers that some further checks are necessary. The traveller goes to a manual booth for the "face to face" check and is identified by his/her token.

When the traveller was enrolled for the first time the border guard:

- verifies that the fingerprints enrolled correspond with the one of the TCN-VE by checking at least one fingerprint with the sample in EES,
- verifies that the live facial image corresponds with the ones in the passport chip and/or on the biographical page,
- completes the thorough examination on the basis of the questions answered.

In the case of a return visit, the border guard sees on his display:

- the results of the passport authentication in case of an electronic passport (or the absence of it for a non-electronic passport),
- the results of the different database queries (SIS, Interpol, national databases) triggered,
- the EES history of previous entries/exits,
- the answers to the questions asked at the kiosk.

On the basis of this information and his risk assessment, the border guard can decide on which controls remain to be done. Similarly to the current situation, the extent of these controls is completely dependent on the border guard appreciation.

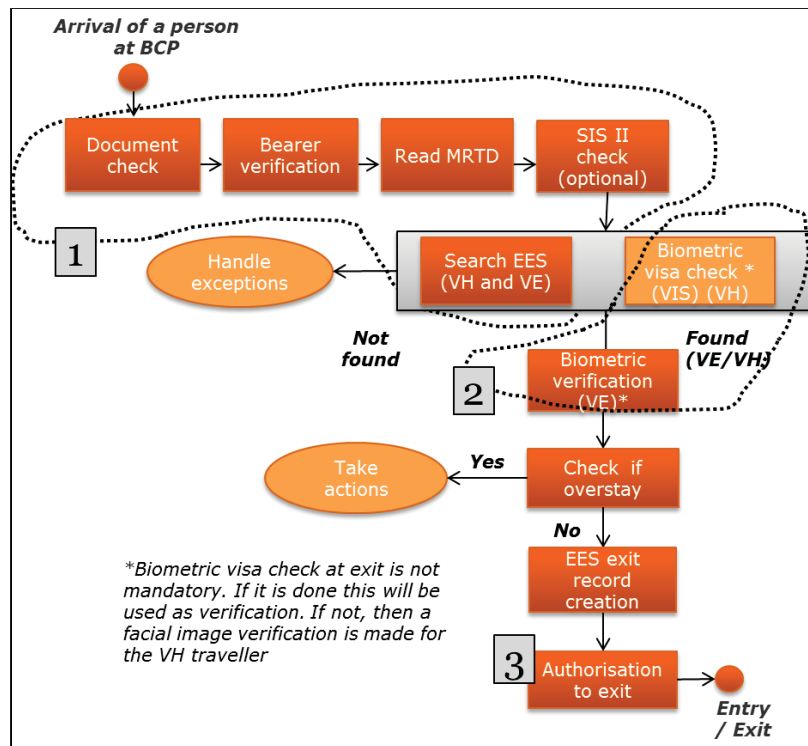
In the case of a non-electronic passport, the border guard needs to confirm that the passport is authentic and belongs to the holder by comparing the picture in the passport and the passport holder.

At the moment the traveller is authorised entering the Schengen area, the border guard clicks "OK for entry" on the display and the EES entry record is created.

*8.1.5. Implementation of Processes at **Exit***

The mainstream process at **exit** can be represented in a flow diagram on the following chart. By "mainstream" is meant that the diagram does not show the actions when a step identifies a discrepancy between data.

The actions that are grouped by a dotted black line and numbered 1 to 3 are the group of actions that are distinguished by the traveller.



Mainstream Smart Border Process Flow at Exit

– (Group of) Actions 1 to 3 identifiable by the traveller

VE= visa-exempt third country nationals; VH= visa-holder third country nationals

The necessary sequence of actions is that;

- (1) The process needs obviously to start with the document check and the bearer verification (refers always to the first check in the identification triangle).
- (2) Once the travel document can be trusted, the traveller's personal data (taken from the MRZ or from the chip (passport or e-passport)) can be used (action "Read MRTD") for querying different databases (EES and VIS in the case of TCN-VH, but also Interpol and national databases). Querying the SIS II database at exit is optional although recommended. It can be noted that these queries can be launched simultaneously and have response times measured in at most a few seconds.

At exit, in all normal cases the traveller is present in EES (= side 2 of the identification triangle is established: the database always contains an individual file that matches the data from the travel document as the database was necessarily updated at entry):

- (3) At exit, it is an optional step to authenticate the TCN-VH (action "Biometric visa check") by means of at least one fingerprint vs the fingerprints stored in the VIS application (side 3 of the identification triangle is confirmed). It could happen more easily as VIS would retrieve the visa application using the travel document number (and the issuing country) read during the action "Read MRTD".
- (4) In the case of a TCN-VH, if not done as part of the previous step, the biometric verification can be done matching the facial image either taken live or taken from the passport vs the facial image stored in EES. In the case of a TCN-VE the facial image either taken live or taken from the passport chip or at least one fingerprint (according to the BCP set-up) is matched vs the biometric samples (4 fingerprints and a facial image) stored in EES (action

"Biometric verification (VE)").

The biometric verification closes side 3 of the identification triangle and ensures the entry record is made for the same person as the one who was enrolled.

- (5) The previous steps allow creating the exit record for the right person. The EES checks whether the traveller overstayed (action "Check if overstay") and provides the remaining number of days of authorised stay.

From the description above it can be observed that all the steps performed are either triggered by reading the passport data or by providing biometrics. Therefore the proposal to use self-service kiosks or e-gates for letting the traveller do this data and biometrics collection work himself.

From the traveller point of view there are three steps to go through at exit (the groups of actions surrounded by a black dotted line and with a number in a square), where only step (2) is due to Smart Borders (similarly to when estimating the duration for border clearance):

- (1) Hand over his/her passport which triggers the passport authentication, bearer verification and the query of the databases.
- (2) The biometric verification step.
For TCN-VH: put 1, 2 or 4 fingers for biometric verification (vs VIS) or have a picture taken live or copied from the passport chip (vs EES).
For TCN-VE: put 1, 2 or 4 fingers for biometric verification or have a picture taken live or copied from the passport chip (vs EES).
- (3) Receive border clearance.

*8.1.6. Accelerated processes at **Exit***

The accelerated process at exit is very straightforward.

In case the TCN has an electronic passport an e-gate can be used:

- The e-MRTD data are read from the chip and the passport is authenticated by means of its electronic security features. This corresponds to document authentication.
- The passport data triggers the queries of the different databases including the EES. This corresponds to matching the document with the database (side 2 of the identification triangle),
- The biometric verification is done either by matching the facial image extracted from the chip with the picture taken live in the e-gate and the picture stored in EES (VE and VH), and/or a fingerprint taken live is compared with the fingerprints stored in EES (for VE) or VIS (for VH). This corresponds to the bearer verification and a biometric verification (sides 1 and 3 of the identification triangle).

It should be noted that in case of e-gates the exit is still attended. According to local set-ups, three to seven exit lanes are usually supervised by one border guard.

In case the TCN has a passport without a chip, a kiosk-based solution can be used because all the steps mentioned above can be performed, with the exception that the passport needs to be authenticated by its optical means, in which case the bearer

verification needs to be done by the border guard comparing the passport photo with the traveller.

9. ANNEX 9: INTEROPERABILITY

The purpose of this annex is to explain how the interoperability is conceived.

9.1. Introduction

In this annex, interoperability the interoperability between IT systems will be defined as the capacity of information technology services to allow for information exchange. The interoperability between IT systems is sometimes further refined as syntactic interoperability (data is exchanged in the same or in compatible formats) and semantic interoperability (the content of the information exchange requests are unambiguously defined: what is sent is the same as what is understood).

The question of interoperability is addressed as part of this Impact Assessment assuming that EES and RTP are built as one system, or that only one system is built (the EES as suggested in the preferred solution). The option of having EES and RTP as two different systems is no longer considered as an option for the purpose of this annex.

However, the single EES/RTP (further only EES will be considered as the preferred solution does not contains specific RTP functionalities) will be used by the same authorities (i.e. consular posts, border control, immigration and law enforcement authorities) that are already using VIS. If VIS and EES work next to each other, the same authorities will often have to duplicate tasks and data. The following example illustrates this: assume a visa-holder arrives at a Schengen border post with his valid passport and visa. This is one of the standard situations that occur a few million times per year taking all Schengen borders together.

In case the **VIS and EES are kept as separated systems**, the border crossing process (leaving out generic document controls) will be:

- Border guard scans the visa sticker. With this operation the VIS is queried on the existence of the visa sticker.
- If a visa exists in VIS, the traveller is asked to put 1, 2 or 4 fingers (depending on how the border crossing point is equipped) on the fingerprint scanner. These fingerprints are matched vs the fingerprints stored in VIS for the traveller to whom that visa was delivered in the consulate. This verification has the purpose of confirming that the traveller is the same person who obtained the visa.
- Assuming that the visa-holder is not yet recorded in EES, the border guard will request the traveller to enrol 4 fingerprints again (although 10 fingerprints are already stored in VIS) and a facial image. The passport biometric data is captured again and stored in EES (the same data is partially already recorded in VIS). Finally, the date and place of entry plus the authority authorising the entry are recorded for that traveller in EES.

At each and every new entry, having EES and VIS as separate systems will require each time to confirm the traveller's identity once vs VIS and once vs EES and add an entry record in EES.

The "obvious" answer would then appear to **combine EES and VIS and have one single system**. This option was examined in the Technical Study but has essentially three drawbacks:

- Adding EES data and volume of transactions requires VIS to handle a much higher capacity both in terms of data and transaction volume. *De facto* it means that an "upgraded" VIS would require a new IT infrastructure. This task is not impossible but building the EES "on top" of the VIS would anyhow require significant hardware and technology changes.
- The experience gained in operating VIS, since it went live on 11 October 2011, shows that some technical solutions implemented for VIS would have to be changed given the higher volumes that EES would add. So building EES "on top of" VIS would not happen on a VIS that is kept unchanged. Changes would essentially be required on message handling and on reducing the amount of work (and costs) it takes for Member States for combining the data exchanged with VIS in their national applications;
- The project of delivering EES built on the existing VIS appeared more risky than building EES next to VIS, albeit when re-using same technical components.

From the above it appears that building **EES separated from VIS duplicates work**, but building EES "on top" of VIS is not a "quick-win" solution and is maybe not even desirable because of project risks. The "third" and preferred way is therefore building EES next to VIS but in a way that both systems "speak" to each other, which is the intuitive way to ensure interoperability between the systems.

9.2. Levels at which interoperability matters

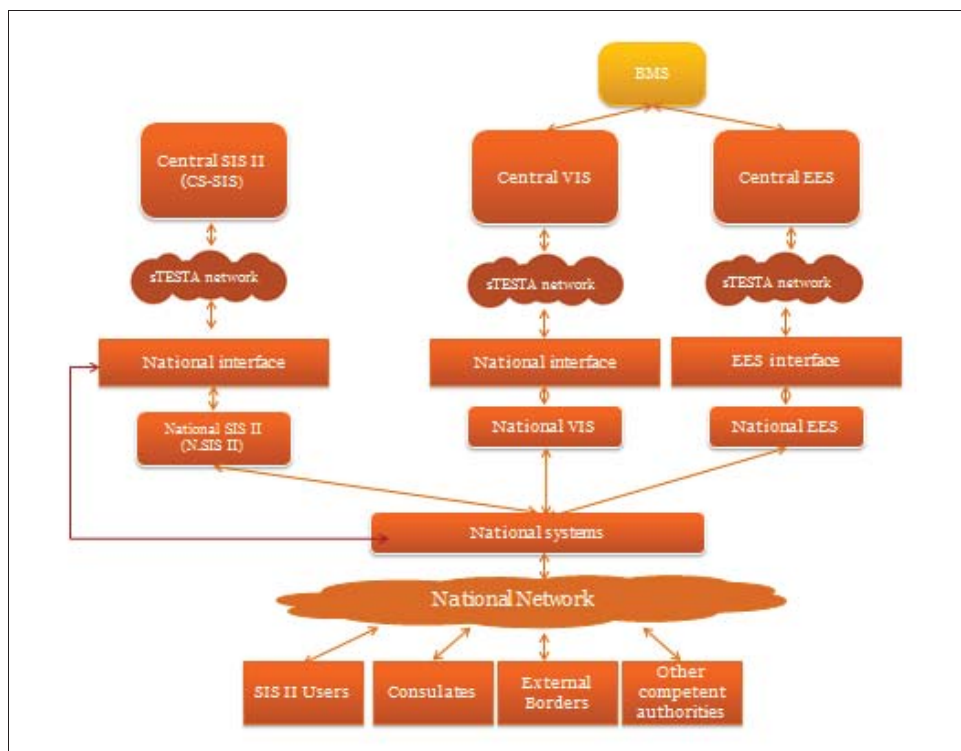
From the example mentioned above there are two levels where "interoperability" matters.

The first level concerns the **biometrics**. As the following example illustrates, biometrics (fingerprints) enrolled in a consular post of Member State A (and stored in VIS) on an equipment of a specific manufacturer need to be matched with biometrics taken at the border post of Member State A but using a different equipment (probably from another manufacturer), but also of a border post in Member State B. Biometrics (this time fingerprints and facial image) taken at the border of Member State A will certainly be used often for matching at exit at the border of Member State C, again each time using different equipment. The interoperability of the biometric identifiers means in this context that the samples taken at any place (consulate, border post, etc.) can be used at any other place (border post of the same or of a different Member State). This interoperability is no longer an issue provided that the biometric samples meet minimum quality requirements which will be specified during the EES development phase which in essence will repeat what has already proven to work well for VIS: VIS has already handled millions of operations with fingerprints and the biometrics are indeed interoperable.

The second level is about avoiding data to be duplicated in different central IT systems (SIS, VIS, EES), reducing the complexity for Member States to have their national systems "speaking" to these central IT systems and combining the use of data received from these systems.

9.3. Starting point: no interoperability between central IT systems

The situation is described as regards SIS, VIS and EES. This scenario is the one implied by the "2013 proposal" but where RTP is left out. In this situation, the interoperability of EES with existing systems is simply not addressed: EES is put next to VIS and SIS as another distinct system. EES simply benefits from re-using the solution developed for VIS.



Future situation when EES is added to the current SIS and VIS

The figure above shows how each IT system is conceived:

- In the case of SIS²³, the central system is connected over a European-wide value-added network to a National Interface in each Member State. This National Interface is identical for all Member States and is connected with a SIS national system whose main tasks are to handle the message flow between the central system and the specific national system that provides services to the end-user. In the case of SIS, there is the particular situation that 23 out of 28 Member States maintain a partial or complete copy (called national copy) of the data of the central system. The SIS national systems are different in each Member State because they need to "speak" with national systems that are different for each of them, despite the fact that the services rendered are the same.
- In the case of VIS, the same logic is applied as for SIS but in this case there is no national copy part of the national VIS.
- In the case of EES, the same logic as for VIS is applied.

For data protection reasons and because the legal basis is each time different, the communication networks for SIS, VIS and EES are separated. The services are procured

²³ The reference to SIS II has become redundant as SIS I+ was decommissioned on 8 May 2012.

to the same network services provider under the s-TESTA (secure Trans European Services for Telematics between Aministrations) contract which allows having "bulk tariffs". Nevertheless, from a cost point of view, having three networks is a very detrimental solution as for many connections the sum of the individual maximum load is still inferior to the minimum capacity that can be procured. At the end, each of the three networks has an important over-capacity for most of its network connections. Combining the load of at least two networks would be possible without increasing the capacity of most network connections (i.e. one network could take up the required load of two networks without extending the capacity of most of its connections). This would not create data-protection issues as it is not because messages use the "same lines" that they are mixed.

While the National Interface provides the same services for SIS, VIS and EES, a specific interface is configured for connecting respectively the SIS, VIS and EES to the national system.

When EES comes in the picture, the complex and expensive item for Member States is (1) that the national systems must be adapted so that the data exchanged with the national EES are handled in a way that is meaningful for the end-user, (2) its use is combined with data from SIS and VIS. This so-called "integration of EES data" in the national systems is Member State-specific.

As an example, a consular officer receives a visa-request of a third-country national. When EES will be available, there are three checks that the officer will perform:

- (1) use the biographical data of the visa-applicant's passport to send a request to SIS to know whether there is an alert recorded for that person,
- (2) use the biographical data and ten fingerprints enrolled from the applicant to check in VIS whether the visa-applicant has already initiated a request in for example another Schengen consulate,
- (3) use the biographical data of the visa-applicant's passport and its biometrics to check in EES whether the duration of authorised stay was respected during previous visits.

To ease the work of consular officers it is likely that these three actions will be hidden behind a single functionality called something like "check new visa-request". The answers from SIS (the expected case is a "no hit"), from VIS (the expected answer is "no other application pending") and from EES (the expected answer is either no history of entries/exits or a history of entries and exits without overstay) need also to be combined in a meaningful and practical way for the consular officer. Nevertheless, technically one message is sent to three different central systems and one answer from each of them is sent back via three different channels to be combined at the level of the national systems: total six messages triggered for one operation as seen by the consular officer.

It can be noted that at least three straightforward simplifications would have reduced this integration effort at Member State level:

- (1) biographical data and biometrics could be sent to VIS to check whether another pending application exists,

- (2) VIS would query the SIS central system for the existence of an alert using biographical data,
- (3) VIS could retrieve the traveller's EES history by accessing the EES central system.
- (4) one message is sent back to the Member State with a combined answer from SIS, VIS and EES.

The advantage is that it is much simpler to adapt national systems for handling the data contained in this message as data are already combined in a meaningful way. Technically, it also has the advantage that one operation triggers two messages (one question and one answer).

However, this simplification is not possible for the following reasons:

- When SIS and VIS were conceived a direct link between central systems has been discouraged for data protection reasons.
- Although it becomes simpler in this case to adapt national systems, it moves the complexity of combining data from different systems towards the central systems. Complexity does not disappear but is rather moved to the central level. Cost-efficiency would probably be improved by addressing complexity once rather than 28 times, but to reduce project risk the direct link between VIS and EES was also pushed back.

9.4. Reducing the impact of EES at national level

The Technical Study addressed the issue of reducing the impact on national systems of exchanging data with the central EES system. The idea is that while in VIS there is a standard National Interface doing nothing more than providing an encrypted access to the s-Testa network and a Member State specific national VIS system, in EES a centrally built standard system would take care of all message handling services that are necessary for all national systems. This is what is called the National Uniform Interface (NUI) and is therefore represented in another colour in the picture below. It is also this NUI concept that is included in the new legal proposal.

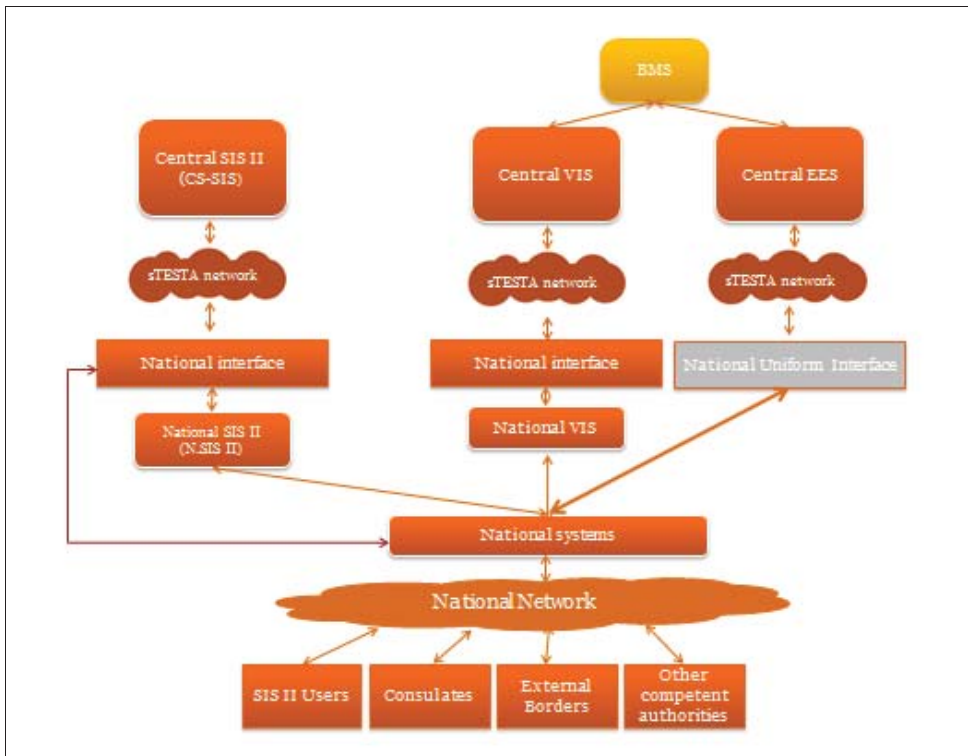


Illustration of the position of the NUI in the architecture

The message handling services of the NUI, refers to a set of services that do not deliver functionalities to the end-user but control the exchange of messages with the central system. To illustrate this concept, one of the most crucial services is called "Reliable Message Transport". This service ensures that a message sent by the national system is delivered to the central system: it records the identifier of each message and as long as it does not receive an acknowledgement of the central system the original message is re-sent according to a specific re-send strategy (e.g. in case the message is not delivered because of network congestion a re-send attempt is tried out every ten seconds). If these services were not provided by the NUI, each national system would have to include them in its modification of the national system in order to handle the exchange of data with the central EES.

The NUI concept does not address the interoperability between SIS, VIS and EES. It only addresses what is called the connectivity, but it nevertheless simplifies the effort (and cost) at national level of including the exchange of data with EES in the national applications. It also addresses the cost and connectivity concerns. The national systems can be considered to "call" the NUI services for handling the messages exchanged with the central EES. However, the national systems will still have to combine the data exchanged with VIS and EES. The example given of the consular officer initiating a new visa request would still imply the same message exchange.

As can be seen in the picture above, the SIS and VIS implementations remain unchanged. This is essentially seen as a benefit, as the EES project will therefore not impact current SIS and VIS operations.

9.5. Including the interoperability between VIS and EES

Building further on the solution described in the previous section that only addresses the connectivity between VIS and EES, the possibility that the central EES accesses VIS and that reciprocally VIS accesses EES is added.

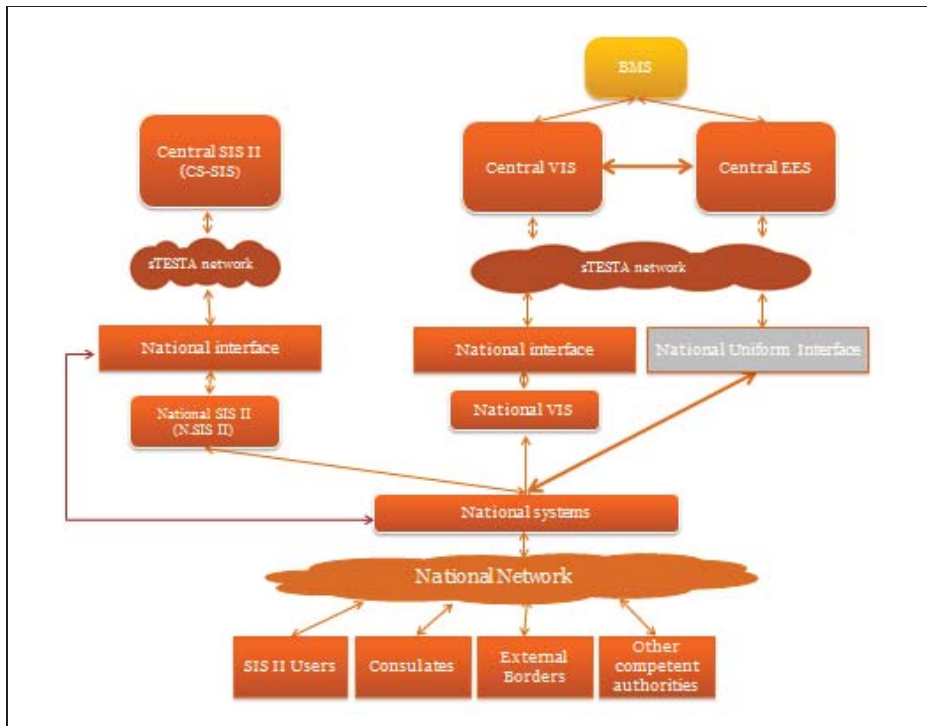


Figure with the proposed interoperability between VIS and EES

The interoperability of VIS and EES is based on the following assumptions:

- Interoperability of VIS and EES with SIS is not addressed. The reasons are mainly practical: it would require the amendment of the SIS legal proposal and, in the context of a legal proposal for EES, the data exchanges of this future system with SIS are not systematic. It is the interoperability of SIS and VIS that could provide further benefits but this could be handled independently.
- Although this was assumed from the beginning, in this case the Biometric Matching System (BMS) has to be the same for VIS and EES, while till now it was only a best option.
- The access to VIS and EES is bi-directional. As an example, VIS updates EES on the changes of visa status (annulment, revocation, extension of visa validity) of visa-holders and EES answers requests from VIS on the history of entries/exits.
- Identity verifications in VIS and EES are mutually trusted. This means that when the identity of a visa-holder is verified vs EES by means of his/her biographical data and facial image, the confirmed identity is also taken for granted by VIS. Otherwise a second identity verification would have to take place where this time at least one fingerprint would be matched with the biometrics stored in VIS. It would reduce the interest of interoperability.
- Since EES accesses VIS centrally and reciprocally, there is no justification of having a separate virtual network and the same network connections will convey EES and VIS messages. This will save network costs without any loss of data security.

As regards the systems on the Member State side, no additional changes compared to section 9.3 are assumed: messages to and from central VIS continue to be handled through the VIS national system and the National Interface, while messages to and from EES are handled through the NUI. There might be opportunities for simplifying the

architecture at the national level (like using the NUI also for handling the messages to and from VIS) but delivering EES is not dependent on changes to be first made to the VIS national implementation.

Referring to the example taken in section 9.3 of a consular officer receiving a visa-request of a third-country national, this is the way the described checks would be done:

- use the biographical data of the visa-applicant's passport to send a request to SIS to know whether there is an alert recorded for that person,
- use the biographical data and ten fingerprints enrolled from the applicant to check in VIS whether the visa-applicant has already initiated a request in another Schengen consulate. VIS sends a request to EES with the same biographical data and four fingerprints (taken from the set of ten) to check whether that person is known in EES. EES sends the travel history of that person back to VIS or the message of the absence of a travel history.

The answer from SIS will be sent to the national system used by the consular officer as one message and from VIS as a second message which also includes the EES data. Both answers will again need to be combined in a meaningful way to the end-user, however combining data coming from SIS and VIS is already taking place now. For sure more data is contained in the VIS message (in this case the travel history or the absence of travel history) but this is far easier to change than having to combine data from EES on top of the data from the other two systems. In this case, one message is sent to two different central systems (SIS and VIS) and one answer from each of them is sent back via two different channels to be combined at the level of the national systems: in total four messages triggered for one operation as seen by the consular officer. The consultation of EES by VIS represents two other messages which do not go over the s-Testa network. An access of one central system by another one is both faster and avoids network costs. The benefit may appear small but there are currently 17 million visa applications per year which will require the message exchange of this example to happen. Nevertheless the main benefit is essentially that it reduces the complexity at the national level.

The access of one central system is often viewed as an operation that has the inconvenience that it is more difficult to manage from the point of view of control on access rights and logs. However, this presumed disadvantage can be avoided by having EES access VIS by the same (existing) central interface that logs the messages and controls the access rights for consultations originating from Member States: EES messages would follow the same path as messages originating from Member State systems.

As an example, a border guard from Member State A sends the message to EES containing the passport data of a visa-holder to verify whether the traveller is already recorded in EES and whether there is a valid visa issued. The message hits EES which accesses VIS in order to find the valid visa (in this case on the basis of the travel document number). If it is designed like for VIS, the EES message will carry with it the information of the requesting authority and the access rights of this authority are checked by the VIS central interface. The access is also logged and is not recorded as "an EES request" but something like "border guard MS A identity check request" and therefore the control on access to data can remain as tight as it is currently.

In the reciprocal case of VIS accessing EES, the current message design is that the type of request plus the authority at the origin of the request remain identified and the corresponding access rights controlled. EES will have to implement a logically equivalent central interface as the one currently used for VIS.



EUROPEAN
COMMISSION

Brussels, 6.4.2016
SWD(2016) 115 final

PART 3/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Annexes to the Impact Assessment report on the introduction of an Entry Exit System

Accompanying the document

Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011

and

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/xxx as regards the use of the Entry/Exit System (EES)

{COM(2016) 194 final}

{COM(2016) 196 final}

{SWD(2016) 116 final}

Table of Contents

10.	ANNEX 10: IMPLEMENTATION COSTS AT NATIONAL LEVEL	98
10.1.	Set-up costs at Member State level	98
10.2.	Costs for Border Equipment.....	99
10.3.	Summary and timing of Implementation costs.....	101
11.	ANNEX 11: BENEFITS OF SMART BORDER PREFERRED SOLUTION	103
12.	ANNEX 12: COST-BENEFIT ANALYSIS	113
12.1.	Cost-Benefit of Preferred Solution.....	113
12.2.	Preferred Solution vs Building no Smart Borders system.....	115
13.	ANNEX 13: IMPACT ASSESSMENT ON FUNDAMENTAL RIGHTS.....	117
13.1.	Why is this impact assessment necessary.....	117
13.2.	Approach	118
13.3.	Impact Assessment of the preferred solution	119
13.3.1.	Legal ground of the data processing.....	119
13.3.2.	Respect of the essence of the right to privacy, objectives of general interest and proportionality.....	119
13.3.3.	Precision of the measures	121
13.3.4.	Purpose limitation.....	122
13.3.5.	Data processing is adequate, relevant and not excessive	123
13.3.6.	Proportionality test	127
13.3.7.	Protection of other fundamental rights	133
13.3.8.	Appropriate safeguards at EU level.....	133
13.3.9.	Rights to Access and Correction	134
13.3.10.	Control by an independent authority	134
13.3.11.	Need for security and data protection by design and by default	135
13.3.12.	Conclusion.....	135
13.4.	Impact assessment for Law Enforcement Access	136
13.4.1.	Necessity	136
13.4.2.	Proportionality	137
13.4.3.	Protection of other fundamental rights	138
13.4.4.	Specific Safeguards	138
13.4.5.	Conclusion.....	139
14.	ANNEX 14: EXECUTIVE SUMMARY OF RESULTS FROM 2015 PILOT.....	140
15.	ANNEX 15: FUNDAMENTAL RIGHTS AGENCY SURVEY - REPORT.....	141
16.	ANNEX 16: PREPARATORY WORK WITH THE EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)	142
17.	ANNEX 17: EXISTING EU LARGE-SCALE IT SYSTEMS	146

17.1. Overview	146
17.2. Legal instruments	146
17.3. Schengen Information System.....	148
17.4. Visa Information System.....	151
17.5. Biometric Matching System.....	153
17.6. Eurodac	153

10. ANNEX 10: IMPLEMENTATION COSTS AT NATIONAL LEVEL

For the implementation of Smart Borders in the 30 Member States, the structure used is the so-called "MS Toolbox" developed during the Technical Study in 2014. The cost computation is done independently of the funding, as it might very well be that some of the Member States considered would not be eligible for EU funding programmes. However the incurred cost would remain.

Given the scope of the proposed Smart Borders system there are only costs at the border and none at the consulates.

The technical integration of NUI (National Uniform Interface) with national systems is already included in the estimate of the Smart Borders system, which explains why these costs are computed here.

The national investments are computed as marginal costs on top of the existing personnel and infrastructure.

10.1. Set-up costs at Member State level

The following cost items are considered:

Nbr	Work/Description	Quantity	Unit Price (in k€)	Total (in k€)	One-off or recurrent
1	Project Management of transformation of each border type: processes, people and technology	46	462	21.252	One-off
2	Procurement of new border equipment installations	30	88	2.640	One-off
3	Training of 1 st line border guards	20.000	0.2	4.000	One-off
4	Changes to national border control application	30	220	6.600	One-off
5	Enhancement of national IT infrastructures	30	750	22.500	One-off
	Total			56.992	

Assumptions:

Item 1: use of two internal (€350/day) and two external staff (€700/day) during one year (220 days) (so $2 \times (350 + 700) \times 220 = 462$ k€). This number is multiplied by 46 which represents the number of Member States multiplied by the number of different types of border per country. When a country has multiple types of border, 50% and 25% of the cost is counted for second and subsequent border type.

Item 2: Use of two internal resources (€200/day) during one year (220 days) (in total 88k€) and multiplied by the 30 (one per Member State).

Item 3: Training of border guards in first line: two days at daily cost of €100/day (in total 0.2k€) applied to 20.000 persons.

Item 4: Changes to end-user systems to include Smart Border processes. Estimate of two persons (value €500/day each) during one year (220 days), for a total of 220k€ development cost per Member State.

Item 5: Enhancement of national network and infrastructure. Estimate of 750k€ to cope with increased network traffic per Member State.

10.2. Costs for Border Equipment

There are about 1.800 border crossing points for the 30 Member States considered. However many of them are of small and even very small size like airfields and harbours for leisure boats. The estimate is that there only 127 large border crossings (7% of the total): 40 sea border crossings, 27 airports, 40 land borders and 20 railway connections linking Schengen countries (including countries that do not yet completely implement the Schengen acquis) and third countries.

Equipment cost for small border crossings

For a small border crossing the assumption is made that there are only two desks (either entry/exit or EU/non-EU).

The equipment necessary for a small border crossing is:

Equipment	Quantity	Price (in €)	Total (in €)
Passport reader –fixed (including authentication)	2	1.500	3.000
Equipment for taking facial image	2	500	1.000
4 FP reader ¹	2	4.000	8.000
Total			12.000
Yearly maintenance of 10%			1.200

The **total cost for equipment of the small border crossing points** would amount to **€20,16 million** (1680 border crossing points @ 12.000€/case). This investment would induce an **annual maintenance cost of around €2 million**.

Equipment cost for large border crossings

For the large border crossing points the assumption differs according to the type of border crossing.

Equipment	Quantity	Price (in €)	Total (in €)
<i>Air border entry</i>			
Equipment for the manual lanes			
Passport reader –fixed (including authentication) -	0	Assumed to be already available	0
Equipment for taking facial image	6	500	3.000

¹ The unit price is a generous one as the information on average prices done as part of the Smart Borders pilot indicate ranges of average prices between €1.000 and €16.643. Differences relate to whether the device can be used standalone or integrated, and whether it is a contact device or a contactless one. In this cost computation the fingerprint reader is assumed to be a contact device.

4 FP reader	6	4.000	24.000
Sub-Total			27.000
Yearly maintenance of 10%			2.700
Equipment for automated lanes			
3 kiosks for each of 6 entry lanes for non-EU citizens	18	25.000	450.000
Yearly maintenance of 10%			45.000
Air border exit			
Additional e-gates for non-EU citizens.	6	75.000	450.000
Yearly maintenance			45.000
Total per Air border			927.000
Yearly maintenance			92.700

Equipment	Quantity	Price (in €)	Total (in €)
Sea border entry –fixed equipment			
Passport reader –fixed (including authentication)	0	Assumed to be available	0
Equipment for taking facial image	6	500	3.000
4 FP reader	6	4.000	24.000
Sub-Total			27.000
Yearly maintenance of 10%			2.700
Sea border entry mobile equipment			
Mobile stations	6	15.000	90.000
Yearly maintenance of 10%			9.000
Sea border exit			
Additional e-gates	6	75.000	450.000
Yearly maintenance			45.000
Total per Sea border entry			58.500
Assume 50% fixed and 50% mobile			
Yearly maintenance			5.850
Total per Sea border exit			450.000
Yearly maintenance			45.000

Equipment	Quantity	Price (in €)	Total (in €)
Land border entry –fixed equipment			
Passport reader –fixed (including authentication)	6	Assumed to be available	0
Equipment for taking facial image	6	500	3.000
4 FP reader	6	4.000	24.000
Sub-Total			27.000
Yearly maintenance of 10%			2.700
Land border entry mobile equipment			
Mobile stations	6	15.000	90.000

Yearly maintenance of 10%			9.000
Total per Land border entry			58.500
Assume 50% fixed and 50% mobile			
Yearly maintenance			5.850
Total per Land border exit			58.500
Yearly maintenance			5.850

Equipment	Quantity	Price (in €)	Total (in €)
<i>Railway border mobile equipment</i>			
Mobile stations	4	15.000	60.000
Yearly maintenance of 10%			6.000
Total per Railway border			60.000
Yearly maintenance			6.000

	Number of border crossings	Average investment cost (in k€)	Investment (in k€)	Yearly maintenance in k€
Air borders	27	927,0	25.029	2.502,9
Sea borders (entry and exit)	40	508,5	20.340	2.034,0
Land borders	40	117,0	4.680	468,0
Railway connections	20	60,0	1.200	120,0
Sub-Total	127	403,5	51.249	5.124,9
Integration cost (IT investment and infrastructure changes) at the level of the border post	127	300,0	38.100	0
Total	127	703,5	89.349	8.934,9

The total cost for equipment of the large border crossing points would amount to **€89,35 million**. This investment would induce an **annual maintenance cost of almost €9 million**.

10.3. Summary and timing of Implementation costs

The implementation cost on Member States side would consist of:

- €57,0 million set-up costs over the 3-year development period. This will be split as €10 mio the first year, €20 mio the second year and €27 mio the third year as the lead time for procurement under new contracts will make that the amounts of investment will mainly take place from the second year.
- €109,5 million (20,16 + 89,35) equipment cost for small and large borders to be done over the 3-year development period. This is a simplification these investments could also be done beyond the development period as the most expensive equipment are

process accelerators and could also be implemented only when the number of border crossings increases, meaning years 4 and 5. The investments would be split as €20 mio the first year, €40 mio the second year and €49,5 mio the third year. This investment would induce an annual maintenance cost of 10% on the accumulated investment and would reach €11 million (2+9) once completely accomplished.

In mio €	1 st year	2 nd year	3 rd year	4 th year	5 th year	6 th year	7 th year
	Development period			Operations period			
Investment	10	20	27	0	0	0	0
Equipment	20	40	49,5	0	0	0	0
maintenance		2	6	11	11	11	11
Total	30	62	82,5	11	11	11	11

11. ANNEX 11: BENEFITS OF SMART BORDER PREFERRED SOLUTION

This annex details the origin of the benefits of the preferred solution, an assessment of their magnitude and the assumption for "monetizing" (meaning computing a monetary value to it) them when possible.

The approach starts from the list of impacts in chapter 6 of the Impact Assessment, uses the assessment made in the comparison of options in chapter 7 and details the assumptions for estimating the magnitude of the benefit.

The computation of benefits is explained first and the benefits computed in a sheet.

	Category of impacts (from chapter 6 of the Impact Assessment)	Impact on	Estimation + Value and timing
1	<p>Social Impact impact on third country nationals (see 6.1)</p>	<p>Border crossing time at entry:</p> <ul style="list-style-type: none"> • No impact for visa-required travellers not using facilitation. • <i>Negative impact for visa-exempt travellers at first enrolment.</i> • No impact for enrolled visa-exempt travellers. • <i>Positive impact for travellers using the "Fastlane for All"</i> <p>Border crossing time at exit</p> <ul style="list-style-type: none"> • No impact on exit time for all travellers 	<p><i>Negative impact for visa-exempt travellers at first enrolment</i></p> <p>When a 5-year data retention period is assumed, all visa-exempt travellers will need to be enrolled the first year. The next years this number decreases quickly as data is retained for 5 years and only not yet registered travellers need to be enrolled.</p> <p>The Smart Borders pilot showed that enrolment using the preferred solution would add 30 seconds + system response of 10 seconds to the existing border crossing time. The enrolment process adds therefore about 40 seconds (0,7 minutes) to the border crossing time but about 10 minutes to the dwelling time in the busy border posts (which is a reasonable value). An estimated 70% of travellers use the busy border crossing points. The opportunity cost for the additional time spent for crossing the border is valued at a standard cost of €31² per hour.</p> <p>Value = proportion to be enrolled (from 1 to 0,20) x 0,70 x number of TCN-VE x 10 min x 31 €/60min</p> <p><i>Positive impact for travellers using the "Fastlane for All"</i></p> <p>An estimated 70% of travellers use the busy border crossing points. The percentage of travellers using the "Fastlane for All" would start from 30% in 2020 and reach 70% in 2025, which has been demonstrated to be realistic</p>

² Value taken from "Standard Inputs for Eurocontrol Cost Benefit Analysis" version 6.0 of September 2013, page 31 where the passenger value of time is rated at 31€/hour by General Aviation. This is below the recommended value of €47 to €60 per hours per passenger recommended by Eurocontrol.

	Category of impacts (from chapter 6 of the Impact Assessment)	Impact on	Estimation + Value and timing
			<p>based on implementations in Canada and USA. The benefit per traveller is estimated as 5 minutes less dwelling time (which is a cautious estimate and inferior to the added duration of enrolment), valued at the same rate as above.</p> <p>Value = (0,30 to 0,50) x 0,70 x number of TCN border crossings/year x 5 min x 0,50 €/min</p>
2	Economic impact on transit hubs (see §.2).	Fastlane for all reduces the cost of delay for lost connections.	There is no estimate for this benefit.
3	Impact for Border Control Services	<p>Workload for border guards:</p> <ul style="list-style-type: none"> • Additional workload for enrolling visa-exempt third-country nationals in congested border crossing points. • Reduced workload for controlling third country nationals using "Fastlane for All". 	<p><i>Additional workload for enrolling visa-exempt traveller.</i></p> <p>Only in congested border crossing points will an increased workload lead to a need for more staff. In a non-congested border crossing point will an increase in workload reduce the idle time.</p> <p>When a 5-year data retention period is assumed, all visa-exempt travellers will need to be enrolled the first year. The next years this number decreases quickly as data are retained for 5 years and only not yet known travellers need to be enrolled.</p> <p>The enrolment process adds 40 seconds (0,7 minutes) to the border crossing workload. Maximum 70% of travellers will use the congested border crossing point. The cost for the additional time spent for crossing the border is valued at a standard cost of €40 per hour.</p> <p>Value = proportion to be enrolled (from 1 to 0,20) x 70% x number of TCN-VE x 0,7 min x 40 €/60min =.</p>

Category of impacts (from chapter 6 of the Impact Assessment)	Impact on	Estimation + Value and timing
		<p><i>Reduced workload for controlling third country nationals using "Fastlane for All"</i></p> <p>About a third of the border crossing workload is shifted to the travellers. In busy/congested border crossing points a decreased workload per traveller will lead to the possibility to control more travellers per border guard.</p> <p>The percentage of travellers using the "Fastlane for All" would start from 30% in 2020 and reach 70% in 2026. This is a slow pattern of uptake. From the Smart Borders Pilot the benefit per controlled traveller is estimated between 0,60 minutes (36 seconds) and 1 minute per traveller³ at entry and 36 seconds (0,6 minutes) at exit, valued at the average rate of 40€/hour. To remain cautious the lower value of 0,60 minutes is kept at entry.</p> <p>Value in time = (0,30 to 0,70) x number of TCN border crossings/year et entry x 0,60 min x 40 €/60 min + (0,30 to 0,70) x number of TCN border crossings/year et exit x 0.6 min x 40 €/60 min</p>
4. Impact for Immigration Enforcement	<p>Identifying overstayers:</p> <ul style="list-style-type: none"> • Additional income from fines on identified overstayers <p>More efficient and effective and identification of irregular migrants:</p>	<p><i>Additional income from fines on identified overstayers</i></p> <p>As overstayers will be systematically identified at the border, the revenue of fines imposed by MS will increase. The assumption is made that 1 person out of 1.000 overstays more than 7 days and that the average fee amounts to €10 per day.</p>

³ One minute is the estimated upper limit of benefits according to the Smart Borders pilot result. This value corresponds to the benefit of 1 minute per border guard and per controlled traveller computed from the figures cited in a presentation by the US Customs and Border Protection in 2014, citing "Global Entry members have used the kiosks over 13 million times, saving 208.000 officer hours", which makes that 208.000 hours x 60 min/hour/13 million = 0,96 min/entry, rounded to 1 minute.

	Category of impacts (from chapter 6 of the Impact Assessment)	Impact on	Estimation + Value and timing
		<ul style="list-style-type: none"> The saved cost of not having to increase the Immigration enforcement services staff to identify more irregular migrants. <p>More efficient and effective implementation of return decisions:</p> <ul style="list-style-type: none"> Saved cost of executing a higher proportion of return decisions. 	<p>Additional revenue = (number of travellers per year) x 7 days x 10 /1000 = a figure comprised between €3 and 5 million for current Schengen countries.</p> <p><i>Saved cost of not having to increase the Immigration enforcement services staff to identify more irregular migrants.</i></p> <p>The number of regular migrants becoming irregular migrants by overstaying is estimated at 250.000 persons. The Smart Borders system would provide a reliable tool for identifying more overstayers without increasing the staff number. The assumption is made that after one year, 5%, than increasing from 10% till 16% more migrants in irregular situation will be identified per year and that currently 8 migrants are identified per immigration control staff and per year.</p> <p>The saved cost= (5% till 16%) x (250.000 per year) x Yearly cost of law enforcement officers /8. The yearly cost of law enforcement officers is estimated at €45.000/year⁴. This cost is consistent with the hourly cost used for calculating the cost of the additional work for border guards.</p> <p><i>Saved cost of executing a higher proportion of return decisions.</i></p> <p>Only 50% out of 250.000 return decisions are implemented. This number of return decisions is kept constant over time which is a cautious estimate. This means that the staff cost incurred for preparing and executing the return</p>

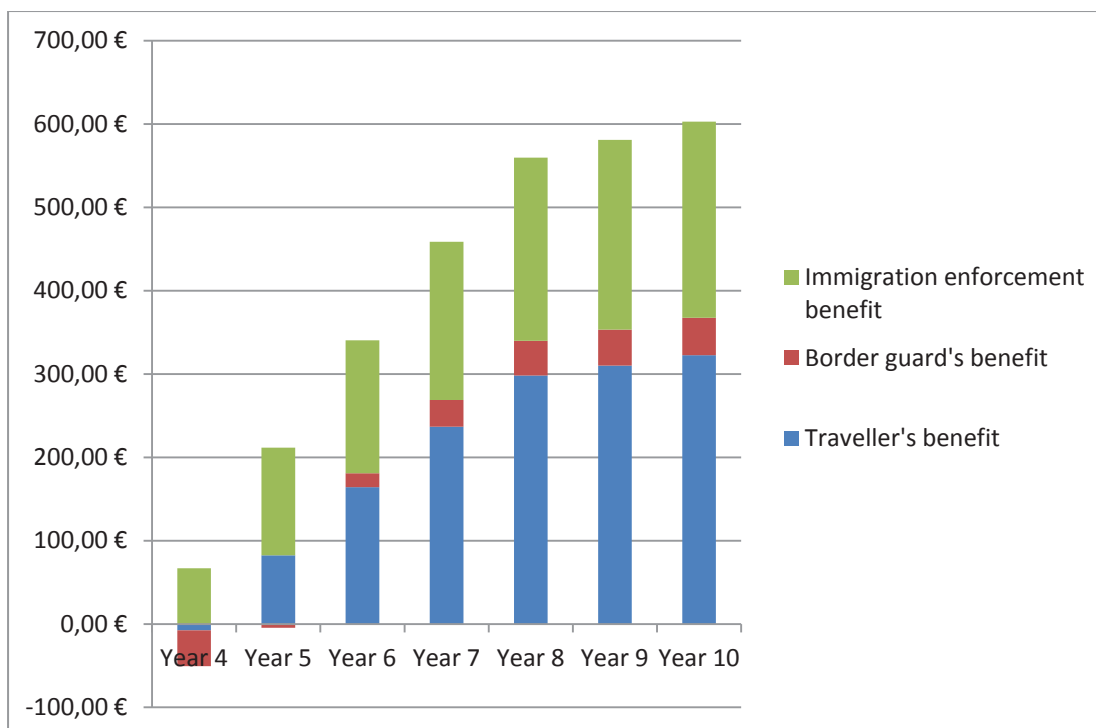
⁴ This figure is consistent with the value given in a presentation called "Risk Analysis and Electronic Lodgement to Improve Border Management where the identification of one overstayer was estimated to cost 60.000 AUD (Australian dollars), which equates €45.000. The figure was obtained by dividing the budget line for these activities by the number of people this activity applied to.

	Category of impacts (from chapter 6 of the Impact Assessment)	Impact on	Estimation + Value and timing
			<p>decision is lost in one case out of two. The assumption is made that the execution of a return decision requires 20 hours of work valued at €30 per hour. Assume the proportion of effectively executed return decisions increases from 4% to reach 33%, than the benefit is.</p> <p>Value= (4% to 33%) x 250.000 x 20 hours x €30/hour= €6 to 49,5 million according to the year.</p>
5	Impact for Law Enforcement	Use as criminal identification tool. Use as criminal intelligence tool	<p>The benefits of being able to use the system as a criminal intelligence tool and criminal identification tool are not expressed in a financial value. The benefits are</p> <ul style="list-style-type: none"> • As a criminal identification tool: reduce the cost of more resource-intensive means to identify persons. • As a criminal intelligence tool: contribute to faster crime resolution or avoidance of criminal acts. <p>There is no estimate for this benefit</p>
6	Air and sea carriers	Reduction of the risk of incurring a fine and a penalty for having transported travellers to the Schengen border who are refused entry	<p>The system will also include a web-site for carriers that will allow them to check whether the traveller meets the entry conditions for the Schengen area. However, the traveller can still be refused entry on the basis of other ground and the traveller is then case still liable for bringing the traveller back to the place of departure.</p> <p>There is no estimate for this benefit.</p>

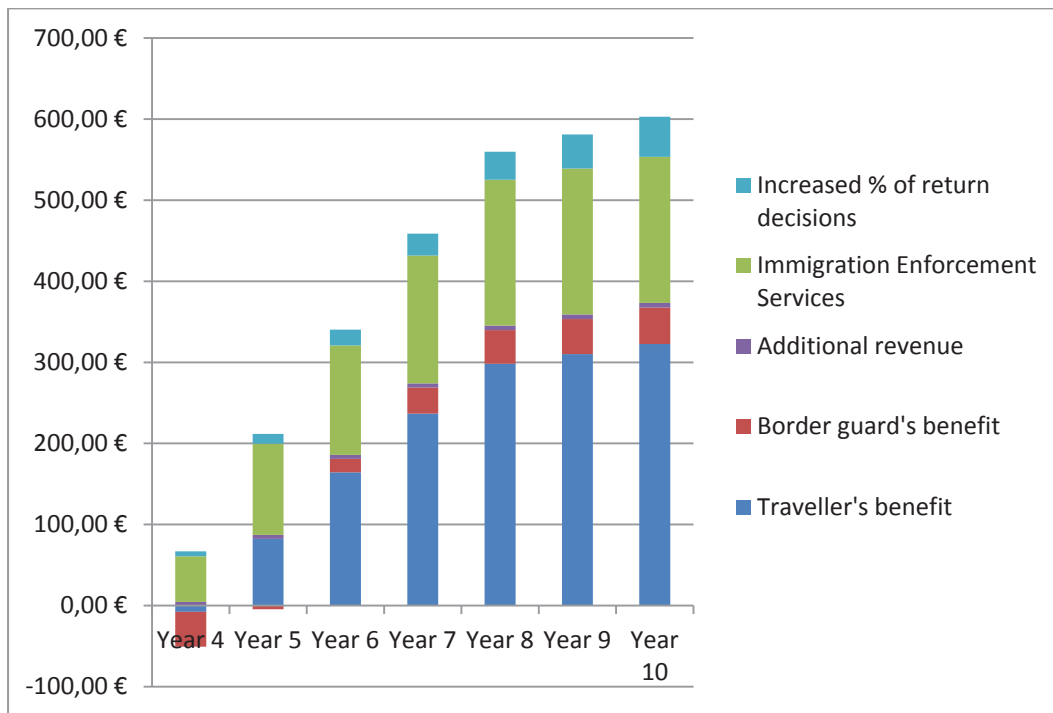
Graphical representation

The following graphs represent the distribution of benefits over time and split over the three main areas:

- Benefits for the traveller obtained as a reduction of the dwelling time despite an increase of border crossing time for the visa-exempt travellers who need to be enrolled again. The benefits stem from the use of self-service kiosks for an increasing proportion of travellers.
- Benefits for border guards in terms of saved workload. The first year this benefit is negative as a vast majority of visa-exempt travellers need to be enrolled. The second year this benefit is close to zero and becomes positive in the next years. This benefit pattern is the consequence of having to enrol a lower proportion of travellers.
- Benefits for immigration enforcement which has different components: additional income from fines on identified overstayers (additional revenue), the increased effectiveness of immigration enforcement services (Immigration Enforcement Services), the saved cost of better execution of return decisions. This detail is provided on the second chart.



X-axis: year after project start. First three years are for development and no benefits are generated over that time
Y-axis: benefits in million € per year.



X-axis: year after project start. First three years are for development and no benefits are generated over that time.
 Y-axis: benefits in million € per year.

Cost-Benefit Estimation	Development			Development			Operations			Operations			Operations		
	Year 1 2017	Year 2 2018	Year 3 2019	Year 4 2020	Year 5 2021	Year 6 2022	Year 7 2023	Year 8 2024	Year 9 2025	Year 10 2026	Year 11 2027	Year 12 2028	Year 13 2029	Year 14 2030	
Costs															
Development and Operations of Smart Borders															
Central System															
National systems															
Total	112,65	115,60	206,52	45,47	19,71	46,78	27,43	19,71	47,14	27,43	19,71	47,14	27,43	19,71	
Changes SIS II and VIS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Total Development and Operations of Smart Borders	112,65	115,60	206,52	45,47	46,03	46,78	47,14	47,14	47,14	47,14	47,14	47,14	47,14	47,14	
Compliance costs MS (see Annex 10)	30	62	82,5	11	11	11	11	11	11	11	11	11	11	11	
Total Costs	142,65 €	177,60 €	289,02 €	56,47 €	57,03 €	57,78 €	58,14 €	58,14 €	58,14 €	58,14 €	58,14 €	58,14 €	58,14 €	58,14 €	
Cumulated Costs	142,65 €	320,25 €	609,27 €	665,74 €	722,77 €	780,55 €	838,69 €	896,83 €	954,97 €	1.013,11 €					
Benefits															
Parameters															
TCN-VE border crossings per year (in million)	92	96	100	104	108	112	117	122	127	132	137	142	147	152	
TCN-VH border crossings per year	126	131	137	142	148	154	160	166	173	180	187	194	201	208	
TCN border crossings per year (in millions)	219	227	237	246	256	266	277	288	299	311	323	336	349	363	
TCNE-VE (in million)	34,7	36,1	37,5	39,0	40,6	42,2	43,9	45,6	47,4	49,3	51,2	53,1	55,0	56,9	
TCNE-VH (in million)	24,0	25,0	26,0	27,0	28,1	29,2	30,4	31,6	32,8	34,2	35,6	37,1	38,6	40,1	
TCN (in millions)	58,7	61,0	63,5	66,0	68,6	71,4	74,2	77,2	80,3	83,5	86,7	90,1	93,6	97,1	
Border crossing time at entry															
Proportion of VE travellers to be enrolled	0	0	0	1,00	0,70	0,50	0,40	0,40	0,40	0,40	0,40	0,40	0,40	0,40	
Proportion of travellers passing via busy BCP's	0	0	0	0,70	0,70	0,70	0,70	0,70	0,70	0,70	0,70	0,70	0,70	0,70	
Increased dwelling time (min)	0	0	0	10	10	10	10	10	10	10	10	10	10	10	
Average opportunity cost (per hour)	0	0	0	31 €	31 €	31 €	31 €	31 €	31 €	31 €	31 €	31 €	31 €	31 €	
- impact for VE travellers at first enrolment	0	0	0	141,05 €	102,68 €	76,28 €	63,46 €	66,00 €	68,64 €	71,39 €					
Proportion of border crossings using kiosks	0	0	0	0,30	0,40	0,50	0,60	0,70	0,70	0,70	0,70	0,70	0,70	0,70	
Reduction in dwelling time (min)	0	0	0	5	5	5	5	5	5	5	5	5	5	5	
- impact for travellers using fastlane	0	0	0	133,46 €	185,06 €	240,57 €	300,24 €	364,29 €	378,86 €	394,01 €					
Border crossing time benefit in million € - Traveller's benefit	0	0	0	-7,60 €	82,37 €	164,30 €	236,77 €	298,28 €	310,22 €	322,62 €					

Part highlighted represents the €480,2 million of financial annex

Impact for Border Control Services										
Proportion of VE travellers to be enrolled	0	0	1,00	0,50	0,30	0,20	0,20	0,20	0,20	0,20
Proportion of VE travellers enrolled at busy BCP's	0	0	0,70	0,70	0,70	0,70	0,70	0,70	0,70	0,70
Increased workload for border guards (min)	0	0	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,7
Average cost (per hour)	0	0	40 €	40 €	40 €	40 €	40 €	40 €	40 €	40 €
Cost of Additional workload for enrolling VE travellers (in millions)	0	0	63,70 €	33,12 €	20,67 €	14,33 €	14,90 €	15,50 €	16,12 €	
Proportion of travellers using kiosks	0	0	0,30	0,40	0,50	0,60	0,60	0,70	0,70	0,70
Reduction in workload for BG's per border crossing at entry (min)	0	0	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6
Reduction in workload for BG's per border crossing at exit (min)	0	0	0,6	0,6	0,6	0,6	0,6	0,6	0,6	0,6
Benefit of Reduced workload when TCN's using fast lane for all	0	0	20,66 €	28,65 €	37,25 €	46,49 €	56,41 €	58,66 €	61,01 €	
Benefit on Border Control Services (in million €)	0	0	-43,04 €	-4,47 €	16,58 €	32,16 €	41,50 €	43,16 €	44,89 €	
- Border guard's benefit										
Impact for Immigration Enforcement										
Number of travellers per year	0	0	66,0	68,6	71,4	74,2	77,2	80,3	83,5	
Proportion of overstayers	0	0	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001
Average duration of overstay (in days)	0	0	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0
Average fine per day	0	0	10,00 €	10,00 €	10,00 €	10,00 €	10,00 €	10,00 €	10,00 €	10,00 €
Additional revenue (in million €)	0	0	4,62 €	4,80 €	5,00 €	5,20 €	5,40 €	5,62 €	5,85 €	
Number of overstayers (persons) - medium value	0	0	250.000	250.000	250.000	250.000	250.000	250.000	250.000	250.000
% of overstayers identified	0	0	0,05	0,10	0,12	0,14	0,16	0,16	0,16	0,16
Cost of identification per person	0	0	4.500 €	4.500 €	4.500 €	4.500 €	4.500 €	4.500 €	4.500 €	4.500 €
Saved cost of not having to increase Imm. Enforcement Services (in million €) to identify more overstayers	0	0	56,25 €	112,50 €	135,00 €	157,50 €	180,00 €	180,00 €	180,00 €	
Number of return decisions	0	0	250.000	250.000	250.000	250.000	250.000	250.000	250.000	250.000
% of decisions implemented	0	0	0,50	0,50	0,50	0,50	0,50	0,50	0,50	0,50
additional % of return decision implemented	0	0	0,04	0,08	0,13	0,18	0,23	0,28	0,33	
Workload per return decision			20,00	20,00	20,00	20,00	20,00	20,00	20,00	20,00
Hourly cost			30,00 €	30,00 €	30,00 €	30,00 €	30,00 €	30,00 €	30,00 €	30,00 €
Saved cost on better execution of return decision	0	0	6,00 €	12,00 €	19,50 €	27,00 €	34,50 €	42,00 €	49,50 €	
Benefit for Immigration Enforcement (in million €)	0,0	0,0	66,9	129,3	159,5	189,7	219,9	227,6	235,3	
Total benefits	0,00 €	0,00 €	16,24 €	207,21 €	340,37 €	458,63 €	559,69 €	581,00 €	602,86 €	

12. ANNEX 12: COST-BENEFIT ANALYSIS

12.1. Cost-Benefit of Preferred Solution

In this section the Smart Borders system is synonym for the EES preferred solution.

The cost-benefit analysis is produced using the results developed in previous annexes:

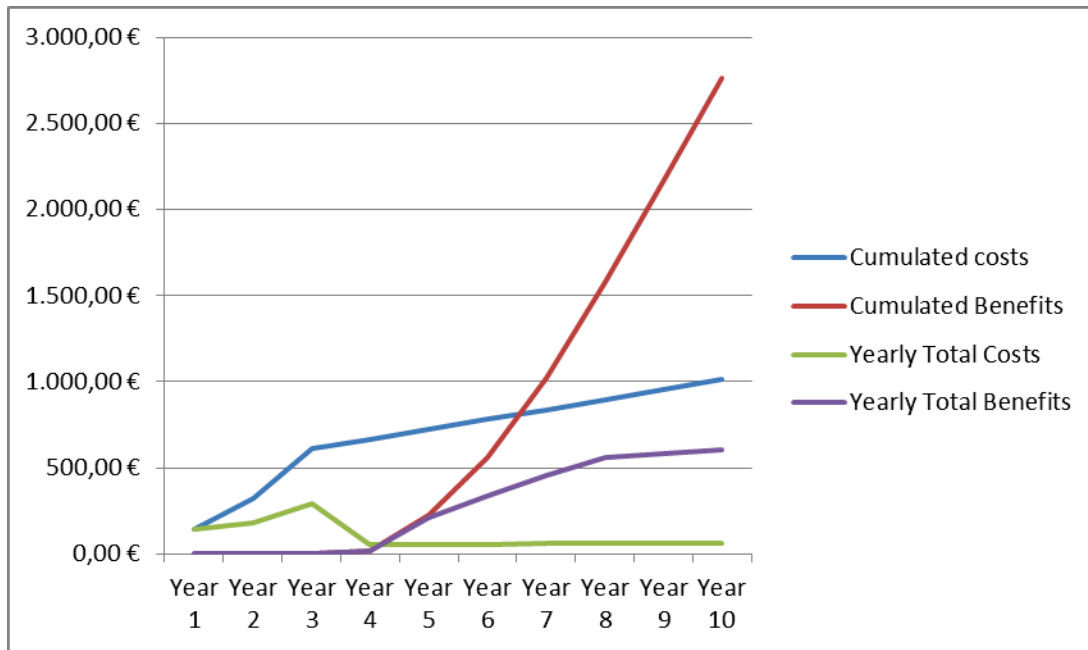
- "Annex 6 – Cost Model for Smart Borders system" contains the cost for the development and maintenance of the Smart Borders system, both the central and the national part. The model is based on cautious assumptions on cost components and does not take items of possible cost reductions into account, such as volume discounts on procured items. The model is also based on the assumption of 30 Member States in the Schengen area (both EU countries and associated countries) from the start.
- "Annex 10 – Implementation costs at National level" provides an estimate for the costs incurred within 30 Member States for the set-up of the system and in particular the investments in additional or renewed border crossing equipment.
- "Annex 11 – Benefits of Smart Borders of preferred solution" estimates the benefits systematically using cautious values. The benefits are also computed for the number of third country nationals entering or leaving the current Schengen area, which is only 26 Member States as Bulgaria, Croatia, Cyprus and Romania are not part of the Schengen area at the moment of this computation (2015).

The summary of these computations is shown in the chart below (all figures in million €):

Cost-Benefit Estimation	Development year 1 2017	Development year 2 2018	Development year 3 2019	Operations Year 1 2020	Operations Year 2 2021	Operations Year 3 2022	Operations Year 4 2023	Operations Year 5 2024	Operations Year 6 2025	Operations Year 7 2026
	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
Costs										
Development and Operations of Smart Borders										
Central System					26,32	27,07	27,43	27,43	27,43	27,43
National systems					19,71	19,71	19,71	19,71	19,71	19,71
Total	112,65	115,60	206,52	45,47	46,03	46,78	47,14	47,14	47,14	47,14
Changes SIS II and VIS	0			0	0	0	0	0	0	0
Total Development and Operations of Smart Borders	112,65	115,60	206,52	45,47	46,03	46,78	47,14	47,14	47,14	47,14
Compliance costs MS (see Annex 10)	30	62	82,5	11	11	11	11	11	11	11
Total Costs	142,65 €	177,60 €	289,02 €	56,47 €	57,03 €	57,78 €	58,14 €	58,14 €	58,14 €	58,14 €
Cumulated Costs	142,65 €	320,25 €	609,27 €	665,74 €	722,77 €	780,55 €	838,69 €	896,83 €	954,97 €	1.013,11 €
Benefits										
Border crossing time benefit in million € - <i>Traveller's benefit</i>	0	0	0	-7,60	82,37	164,30	236,77	298,28	310,22	322,62
Benefit on Border Control Services (in million €)	0	0	0	-43,04	-4,47	16,58	32,16	41,50	43,16	44,89
- <i>Border guard's benefit</i>										
Impact for Immigration Enforcement										
Benefit for Immigration Enforcement (in million €)	0,0	0,0	0,0	66,9	129,3	159,5	189,7	219,9	227,6	235,3
Total benefits	0,00 €	0,00 €	0,00 €	16,24 €	207,21 €	340,37 €	458,63 €	559,69 €	581,00 €	602,86 €
Cumulated benefits	0,00 €	0,00 €	0,00 €	16,24 €	223,45 €	563,82 €	1.022,45 €	1.582,14 €	2.163,14 €	2.766,00 €
Benefits - Cost	-142,65 €	-177,60 €	-289,02 €	-40,23 €	150,18 €	282,59 €	400,49 €	501,55 €	522,86 €	544,72 €
Cumulative	-142,65 €	-320,25 €	-609,27 €	-649,50 €	-499,32 €	-216,73 €	183,76 €	685,31 €	1.208,17 €	1.752,89 €
Discounting value (rate 4%)	1	0,96	0,92	0,89	0,85	0,82	0,79	0,76	0,73	0,70
Net Present Value (when (cost-benefit) are taken over 1,2, ..n years)	-142,65 €	-313,42 €	-580,63 €	-616,40 €	-488,03 €	-255,76 €	60,75 €	441,89 €	823,94 €	1.206,65 €

Evolution of Costs and Benefits

The result of this computation is shown more explicitly in the chart below.



Graph of yearly and cumulated costs and yearly and cumulated benefits for Smart Borders in million €

Yearly total costs are substantial at the beginning and reach a peak in year 3 as major investments need to be made before the beginning of operations. The line of cumulated costs has a steep slope over that period. Benefits being zero over that period of time, the cumulated benefits are also zero.

Once the system starts to be in operation, benefits start to accumulate. As the benefit computation model assumes a progressive uptake of potential benefits that Smart Borders creates (see line of Yearly Total Benefits), the slope of the yearly benefits is modest and becomes nearly flat from year 8 onwards. The benefits are however substantial and explain why the cumulated benefits line increases quickly and crosses the line of cumulated costs. Once the system is in operation, the yearly total costs almost stagnate (see line of Yearly Total Costs). The cumulated costs still grow but at slower pace as compared to years 1 to 3 (the slope flattens).

Net Present Value

Based on the costs estimated for 30 Member States and the benefits for only 26 Member States, the **net present value** at the beginning of the project has been computed for future costs and benefits using a discount rate of 4%.

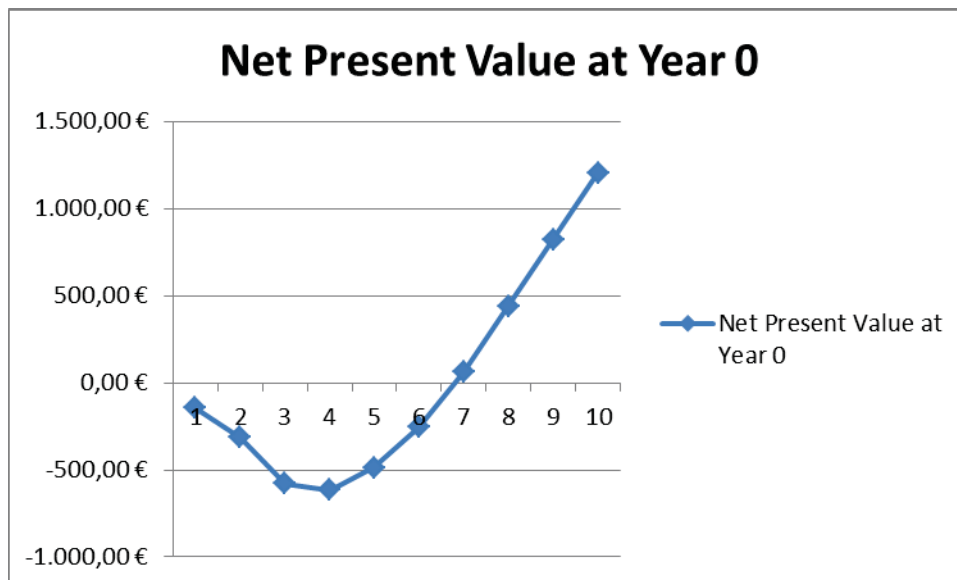


Chart showing the Net Present Value (in million €) after 1, 2... N years

The net present value decreases when costs and (zero) benefits of the first three years are discounted to the beginning of the project. As benefits outweigh more and more costs over the next years, the net present value at the beginning of the project becomes positive after four years of operations.

12.2. Preferred Solution vs Building no Smart Borders system

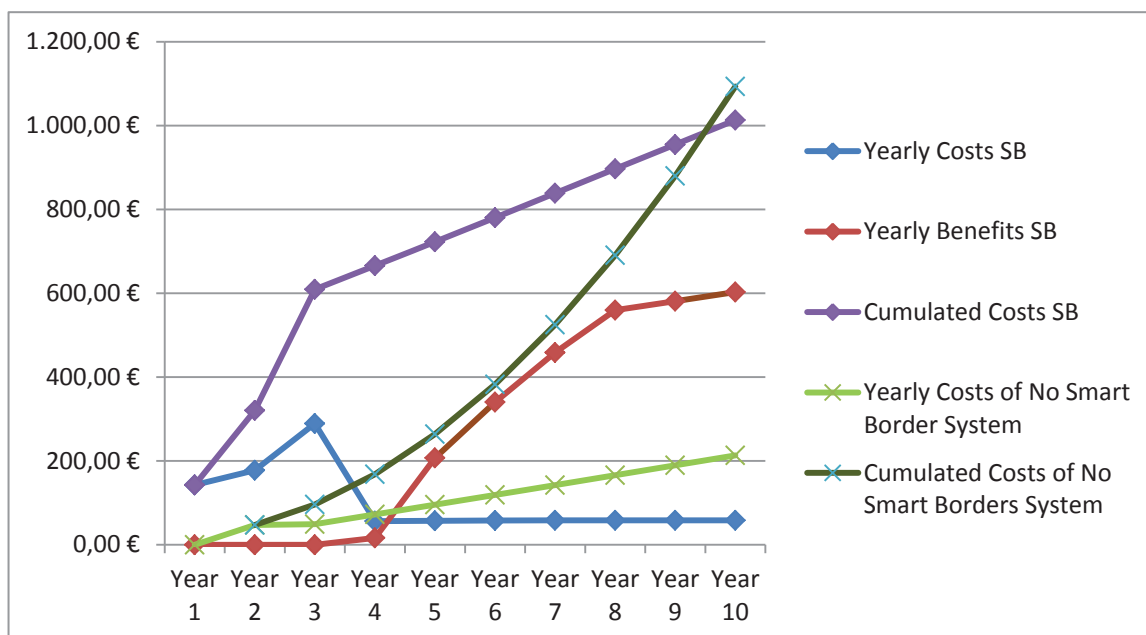
The scenario of the preferred solution has been compared with the alternative scenario in which the Smart Borders system was not introduced.

In this alternative scenario, Member States would incur a series of costs in order to:

- Keep the duration of border crossings unchanged. Considering that the number of border crossings increases, the number of border guards in first line would have to increase in the same proportion.
The recruitment of more border guards induces a recruitment cost and an equipment cost.
- Achieve an equal amount of return decisions from year 4 (first year of operations) as in the situation where the Smart Borders system is implemented. In order to do so, an increased number of staff in Immigration Enforcement services would have to be recruited with their corresponding associated costs.

The benefit of not building Smart Borders compared to the current situation is by definition zero.

The results of this computation are shown on the graph below and compared with the situation where Smart Borders is built:



*Horizontal axis as years after Smart Borders project start – Vertical axis in million €
Graph compares yearly costs and benefits and cumulated costs and benefits
when Smart Borders system is built with the situation
where no Smart Borders system would be built but same operational results are expected*

The picture shows:

- That the **yearly costs** with the Smart Borders system ("Yearly Costs SB") remains about half the yearly costs without Smart Borders ("Yearly Costs of No Smart Border System") for the years after the system is in operations (i.e. from year 5 onwards).
- The development and implementation of Smart Border is a cost-intensive operation. This is shown by the fact that the line "Cumulated Costs with SB" only becomes inferior to "Cumulated Costs of No Smart Borders System" at the end of year 9: the high initial cost of introducing SB is compensated over time by a lower yearly operational cost.
- The **yearly benefits** of the Smart Borders system are significantly higher than without assuming resources are provided to deliver the same results. The reason is that the Smart Borders system provides efficiency gains to travellers, border guards and immigration enforcement services ("less workload for more results"). Without Smart Borders there is no reduced dwelling time for travellers, no reduced workload for border guards when traveller use self-service kiosks and no increased number of return decisions for equal staff numbers.

13. ANNEX 13: IMPACT ASSESSMENT ON FUNDAMENTAL RIGHTS

The objective of this annex is to describe in detail the assessment of the impact on Fundamental Rights of the "preferred solution" of the proposal for a "Regulation establishing an EU Entry-Exit System and for a Regulation amending the Schengen Border Code.

13.1. Why is this impact assessment necessary

An Entry Exit System (EES) would, due to the personal data involved, in particular have an impact on Fundamental Rights and particularly on the right to the protection of personal data. The right to protection of personal data is established by Article 8 of the Charter of Fundamental Rights of the European Union and Article 16 of the Treaty of Functioning of the European Union. Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter and by Article 8 of the European Convention on Human Rights (ECHR). This is further reflected by Article 1(1) of Directive 95/46/EC which provides that Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to privacy with respect of the processing of personal data.

Therefore, the impact assessment on Fundamental Rights of the proposal is necessary because the proposed regulation for an EES will result in processing the following personal data:

- (1) the identity as recorded in the biographical page of the passport to be copied for all visa-exempt third country nationals (TCN-VE), including two biometric identifiers (four fingerprints and the facial image),
- (2) the identity of all visa-required third country nationals (TCN-VH) stored in VIS being used to identify the person and a facial image being taken,
- (3) the place, date and authorising authority to be recorded and stored at the entry into the Schengen area of each third country national,
- (4) the place and date to be recorded at exit from the Schengen area of each third country national,

The data listed above will be stored for a period of five years counting from the date of the last exit record.

The EES record would contain:

- (5) Five individual file data: first name, surname, date of birth, nationality or nationalities and gender. These data will all be taken from the Machine Readable Zone or the chip of the travel document;
- (6) Two biometric identifiers: the four fingerprints (FP) and the facial image (FI);
- (7) Four data elements from the travel document: document number, document type, document country code and expiry date. The data elements for documenting the refusals of entry will also be recorded as they are a key border crossing information;

- (8) Four visa-related data in case of visa-required third-country nationals (TCN): visa sticker number, visa expiry date, number of authorised entries and authorised period of stay;
- (9) Five data elements for registering stay changes: the revised expiry data of the authorisation of stay, the date of change of limit of stay, the place of change of limit of stay and the ground for change or revocation;
- (10) Five data elements for each entry/exit record: date and time of entry, entry authorising authority, entry BCP, date and time of exit and exit BCP;
- (11) Two data elements for each RTP scheme the traveller has been entitled to: the unique RTP reference number (this is assumed also identify the RT scheme) and the RTP status information.

There are in total 27 data elements as compared to the 36 data elements of the 2013 proposal.

The items above demonstrate that the EES will record and store a small amount of personal data including biometrics from a large amount of people (order of magnitude of 50 million people per year) as well as their entry and exit record(s) stored over the duration of the retention period.

13.2. Approach

The approach followed covers an impact assessment on all rights that are part of the Charter of Fundamental Rights (the Charter), focusing on Articles 7 and 8 as the impact on these rights is the most obvious.

Under Article 7 of the Charter: "*Everyone has the right to respect for his or her private and family life, home and communications*".

This article must be read in conjunction with Article 52(1). Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be (1) provided for by law, (2) respect their essence and, (3) subject to the principle of proportionality, (4) limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.⁵

Concerning the principle of proportionality three elements must therefore be assessed in combination:

- (1) the measure must be appropriate (suitable),
- (2) the measure must be necessary (requisite), which includes an assessment to determine whether there is no less intrusive alternative,
- (3) the measure must be proportionate.

Article 8 is a proactive horizontal right to protection that is not limited to interferences by the State. It gives individuals the right that their personal data can only be processed if the requirements set out in paragraphs 2 and 3 of Article 8 are met:

⁵ See Judgment of the Court of Justice of the EU, judgment of 9.11.2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-0000, paragraph 65.

- (4) the data is processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law,
- (5) transparency is ensured by giving the individuals rights to access and correction,
- (6) control by an independent authority is ensured.

The sequence of items addressed in this Impact Assessment essentially follows the presentation done by the EDPS (European Data Protection Supervisor) during the workshop with DG HOME on 20 March 2015 as part of the consultations in preparation of the modified legal proposal. In this approach, the way the impact of measures on Articles 7 and 8 of the Charter of Fundamental Rights is assessed, reflects the European Court of Justice ruling on the Data retention directive on telecommunication data.

The assessment is first made **without assuming access to data by law enforcement authorities** (see point 14.3) and then separately **when this access is granted** (see point 14.4).

13.3. Impact Assessment of the preferred solution

13.3.1. Legal ground of the data processing

The regulation for an Entry-Exit System provides the legal ground of the data processing including the collection, storage, use and deletion of the data enumerated under section 13.1. The EES regulation has been developed in full respect of the *privacy by design*⁶ principles.

13.3.2. Respect of the essence of the right to privacy, objectives of general interest and proportionality

So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by the EES Regulation constitutes an interference with those rights, it is not such as to adversely affect the essence of those rights given that the Regulation only permits the use of the EES data to officials from competent authorities for border and migration control.

Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because the EES Regulation provides, in relation to data protection and data security, that certain principles of data protection and data security must be respected by Member States. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted to amend data which it has introduced into the EES, by correcting or deleting such data in accordance with the EES Regulation.

From the above the conclusion is that the "essence" to the right of privacy is not altered: the EES does not record an amount of data that would correspond to a permanent tracing of traveller movements. The frequency of the recording is also low as it only happens at entry and exit of the Schengen area and no intra-Schengen movements are included.

The proposed regulation pursues two objectives of general interest:

⁶ Privacy by design means embedding personal data protection in the technological basis of a proposed instrument, limiting data processing to that which is necessary for a proposed purpose and granting data access only to those entities that 'need to know.'

- (1) Improve the management of external borders.
- (2) Reduce irregular migration, by addressing the phenomenon of overstaying.

Improved border management pursues increased effectiveness and efficiency of border controls at the external borders. Effectiveness in border management is achieved if it facilitates the border crossing of bona fide travellers whilst at the same time prevents that "non-bona fide" travellers enter the Schengen area or are apprehended at exit. Efficiency in border management is achieved when the increase of border crossings does not require a similar increase of border guards. The objective of improved border management means that the level of detail is adapted according to an individual risk assessment performed by the border guard. But such a risk assessment is based, like it is the case today, on identifying the traveller, as a starting point, and on information about the traveller's past behaviour as regards immigration rules.

The second objective is achieved by the EES computing the remaining duration of stay at entry and verifying the overstay status at exit. The EES provides the Schengen area with the tool that systematically verifies whether the basic rule on the duration of stay and applicable to all third-country nationals entering Schengen for a short stay is respected.

The principle of proportionality is met for the following reasons:

- The scope of the measure addresses only the third-country nationals entering the Schengen area for a short stay. The measure does not include third-country nationals with long-stay visas or residence permits. It also excludes third-country nationals crossing the land borders of the Schengen area with a Local Border Traffic permit. It further excludes EU nationals and persons enjoying the right of free movement. Although the group of impacted persons is a large group it represents roughly less than 1/3 of border crossings and less than the same proportion of persons crossing the border as a significant proportion of them travel frequently to the Schengen area.
- A further narrowing of the scope of persons whose personal data would be collected is not possible without introducing discrimination on the basis of nationality. Currently identified overstayers stem both from visa-required and visa-exempt countries but with numbers varying according to a mix of circumstances in their home country and evolving over time. Further, the scope of persons strictly corresponds to the one on which the rule on duration of short stay applies according to the Schengen Border Code.
- The data that are recorded are all justified by the need to uniquely identify the person and to establish compliance with the duration of stay. There are no data recorded for other purposes and that would infringe the privacy of the person like indications on who is accompanied by whom or the means of transport used. These examples of data are currently recorded by national occurrences of entry-exit systems serving law enforcement purposes but are excluded from EES.
- The identification data are copied from the travel document and the biometrics from the traveller. The entry and exit data are taken at the moment of the border crossing. As a consequence, there are no data collected without the traveller knowing about, nor on the basis of traveller declarations or subjective appreciation of border guards.
- Although it does not diminish the need for the current privacy Impact Assessment, it is a reassuring element for the traveller to know that authorities that will have access

to EES data will not see more information about him/her than is currently the case when handing over his/her travel document.

The principle of proportionality is respected as the data stored strictly meet the legitimate objectives pursued by the Regulation listed above and as the group of persons to whom it applies strictly corresponds to the ones affected by the applicable rule on duration of short stay.

13.3.3. Precision of the measures

The proposed measure is extremely precise both in terms of the group of persons whose personal data will be recorded, the data themselves, the processing of data and the exchange of data.

The group of persons whose data will be recorded are third country nationals who enter the Schengen area for a short stay (defined under the Schengen Border Code as "no more than 90 days within any 180 days period"). It therefore excludes third-country nationals entering the Schengen area with a long-stay visa, the residence permit holders (so third country nationals living in a Schengen country), residence card holders (these are the persons enjoying the right of free movement) and the persons crossing the border on the basis of a Local Border Traffic Permit.

The data themselves are defined up to the level of the data element. Each data element is itself very accurately specified either in the regulation, in the legislation referred to (the VIS Regulation), or by internationally recognised standards (the definition of the contents of ICAO compliant travel documents).

The processing of the data is also extremely precise:

- For visa-exempt third country nationals, data are recorded at the border crossing point of entry into the Schengen area and at the border crossing point of exit.
- For visa-required third country nationals, identification data from the visa-application are retrieved and referenced in the Entry-Exit system. Entry and exit data are recorded in the same circumstances as for visa-exempt third country nationals.
- Consultation of personal data is only possible by officials from competent authorities for migration control or enforcement.
- When other authorities or private operators (this is the case for carriers) need to ascertain that a third-country national is lawfully staying within the Schengen area, the solution retained is that a "YES/NO" answer is given by a web-site which accesses a report from the Entry-Exit database. With this mechanism the privacy of travellers is increased compared to the current situation. Currently travellers hand over their passport containing the history of all their entries and exits to any request while with the proposed solution the passport data will only allow receiving the confirmation that the person is staying lawfully in the Schengen area.
- The EES will either compute durations of stay, flag cases of overstay and produce statistics. Statistics can only be produced for specific stakeholders (Member States competent authorities, European Commission and Frontex) and does not require a direct access to the individual data. Production of statistics contains also a safeguard mechanism that avoids statistics to be produced for such small numbers of affected

persons that de facto individual persons can easily be identified (example a report on the number of persons who overstayed in a narrowly defined time period coming from a third country with a very small number of citizens coming to the Schengen area may be so small that it is clear who these persons could be). This last provision is referred to in the legal proposal by the fact that the development of the system will take security of the system and protection of its data into account.

- The conditions for correcting and/or deleting data from EES are also defined in the regulation. It can be noted that the correction of data either by competent authorities or on the request of the data subjects takes into account the feed-back received from travellers during the survey carried out by the Fundamental Rights Agency. It appeared from this survey that travellers were mainly concerned on how potentially wrongly recorded data could be corrected. Further, the conditions for deleting data are also specified and address cases where third country nationals request asylum or refugee status after having entered the Schengen area for a short visit as well as the cases where a traveller falls under the conditions where entry-exit data are not recorded (example: the third country national obtains a long stay visa or becomes the family member of an EU citizen). The deletion of all data (identification data and entry-exit records) becomes automatic and non-reversible for all third-country nationals whose last exit date reaches the data retention period. For third-country nationals who are still identified as overstayers at the end of the data retention period in EES, data are removed from EES, and handed over to each Member State for possible introduction into SIS. From that date onwards, these personal data are subject to the data retention provisions for SIS data.
- The processing of data is performed by eu-LISA, the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. As such, the data are stored in the EU and remain submitted to EU legislation on data protection.
- The exchange of EES with third countries or with private companies is excluded in the regulation.

13.3.4. Purpose limitation

The objectives pursued for collecting the personal data, as listed under section 13.3.2 above, are extremely clear:

- (1) Improve the management of external borders.
- (2) Reduce irregular migration, by addressing the phenomenon of overstaying.

Improved border management pursues increased effectiveness and efficiency of border controls at the external borders. The effectiveness of border management can only be increased by differentiating the intensity of the thorough control required by the Schengen Border Code according to an assessment of individual migration risk. As an example, the migration risk for a visa-exempt traveller who was refused entry a previous time is different than for another traveller who visits relatives every year during holidays. This migration risk, which is the only risk addressed by this proposed regulation, cannot be assessed quickly and clearly enough when the border guard needs to read Schengen stamps among the stamps of other destinations. In addition the traveller is left the opportunity to hide past events (like a refusal of entry) simply by changing passport. It is abnormal that up to now the appreciation of migration risk happened exclusively on the

basis of the information contained in a travel document carried by the traveller with no equivalent information owned by the authorities in charge of migration. The traveller is up to now left with the decision of changing passport (which can be easily done by pretending a loss or voluntarily destroying it) or by using another one in the case of persons having more than one passport, from the same or from different countries, which is not uncommon.

The second objective is achieved by the EES computing the remaining duration of stay at entry and verifying the overstay status at exit. The EES provides the Schengen area with the tool that systematically verifies whether the basic rule on the duration of stay and applicable to all third-country nationals entering Schengen for a short stay is respected.

The first objective leads to store entry and exit records over a sufficiently long retention period. By analogy with the current de facto average retention period of information in a passport, the retention period is five years. The second objective does not add additional requirements as regards the data to be collected.

Both objectives however require establishing the identity of the traveller first. If this would not be done, entries and exits could be wrongly attributed to homonyms after a passport changed or when multiple passports are used by a same person. Biometrics are used in order to avoid an unacceptable level of inaccuracy in establishing the identity.

The only further processing of data occurs for overstayers at the end of the date retention period. Five years after the last entry date, which by definition is not matched with an exit date, personal data are removed from EES and on Member State's decision included in SIS. This is the only further processing of a percentage-wise small amount of the EES data. This further processing is compatible with the original purpose as it remains an immigration control measure. By storing these data into SIS, overstayers are not criminalised but continue to be registered in order to remain identifiable and to be removed from the Schengen territory and not be authorised to enter again.

13.3.5. Data processing is adequate, relevant and not excessive

The proposed data processing consists in recording the entries and exits of all third country nationals entering Schengen for a short stay.

The data that are proposed to be recorded can be split into three main categories: the data that establish the identity of the person including his biometrics, the data that establishes the entitlements to stay (like the availability of a visa or the extensions of duration of stay), the successive entry and exit dates that are the basis for computing the authorised duration of stay.

Adequacy and relevance for improved border management

The first objective pursued is improved border management. The problem at stake is that third country nationals represent 200 million border crossings in 2014 and an estimated 300 million border crossings in 2025. At the same time the number of border guards is not expected to grow within the same proportions. The way this can be done is by automating controls and by focusing the depth of the controls on the travellers representing a migration or security risk.

Automating border controls of third-country nationals for a short stay is possible with current technology. The border control schematically involves three steps: establishing

the identity of the person, verifying whether entry (or exit) conditions are fulfilled, authorising the entry for a specific duration of stay. Current technology improves the precision and speeds up the identity verification and can help determine the authorised duration of stay. Verifying the entry (or exit) conditions is currently done by asking a set of questions. This questioning part can be targeted according to the migration risk assessed by looking into the past history of entries and exits, and relevant information about the country of origin. The security risk is addressed by the systematic control vs SIS and national databases.

The envisaged data processing allows recording identities, linking a history of entry and exit movements and automating the computation of the authorised duration of stay. The only part that is not automated is the questioning part which can be prepared using automated means or can be replaced by a pre-vetting in a nationally defined trusted travellers scheme.

The proposed data collection is not to reduce necessarily the duration of the border crossing for the traveller as this duration is already very low but to decrease the work effort for border guards so that their number can increase less quickly than the number of border crossings. Both the technical study and the pilot have demonstrated the relevance of the proposed data collection provided the enrolment of travellers in EES (in practice this enrolment is only required for visa-exempt travellers) does not need to be repeated frequently as this is the only process step taking longer than the current one. Improved border management therefore relies on a sufficiently long data retention period of the data set containing 27 data elements described earlier.

Adequacy and relevance in reducing overstay

In order to assess whether the proposed measure is not excessive, the magnitude of the existing problem needs to be evoked. The current way of doing border controls in accordance with the Schengen Border code has not prevented that an estimated 1,9 to 3,8 million persons⁷ are irregular migrants. This amount is assumed to increase by another 250.000 persons on a yearly basis. The majority of these irregular migrants have not smuggled into Europe but have simply used regular migration paths and overstayed. The recent migration waves in Europe via the Mediterranean Sea and the Balkans essentially concern refugees fleeing war circumstances and are different from the overstayers mentioned before.

The EU has developed a return policy to curb the volume of overstayers but this policy is hampered by the fact that the date and place of entry into the Schengen area are unknown. As the return needs to be done towards the country of origin or from where the overstayer came from the current policy reaches its goal for only 50% of returns as the required information is currently not recorded. Only visa-required travellers can be identified vs VIS on the basis of their fingerprints, but even for these travellers the place and date of entry are not recorded.

When the proposed data are collected for all travellers concerned by the measure, migration authorities are given the tools to get a grasp of the situation. Authorities will start to be able to identify the overstayers, estimate their number and where they come from. When overstayers are "picked up on the street" their identity can be established and

⁷ Estimates from the Clandestino project, an EU-sponsored project implemented by the International Centre for Migration Policy Development. More precise and updated figures are not available.

a return successfully executed. The data processing is therefore adequate, relevant and proportionate with the migration problem at stake.

The relevance of the data collection is objected by stating that as the EES does not locate overstayers (no addresses are recorded), authorities will only be able to identify overstayers but not apprehend them. The argument is not very relevant as the problem today is not finding overstayers but establishing their identity as they often destroy their travel document and/or try to acquire EU documents to secure their situation. Finding overstayers is done by investigating the places where they seek jobs and not by collecting addresses.

A second objection to the relevance of the data collection is that Europe needs more workers with its declining demography and that overstayers should therefore not be tracked but welcomed. The argument is not relevant either because the EU has opted for a chosen migration and not for having to accept overstayers who impose their presence. Treating overstayers the same way as persons following regular migration schemes means that a premium is given to irregular migration and completely undermines the chances of success of controlled migration.

Relevance of biometric data

At the kernel of the EES identity file are the biometrics. The biometrics are only a tool for establishing the identity of a person accurately. The following question needs to be answered: why biometrics need to be stored on top of the biographical information of the traveller? The reasoning could be made that recording entries and exits of third country nationals is adequate, relevant and not excessive for the objectives pursued and there is no need for storing the biometric identifiers.

The biometric identifiers of the preferred solution are the facial image and four fingerprints at enrolment. These identifiers are used in three situations:

- Situation 1: verification at the border. Verifying that the identity on a passport matches the identity in the EES so that entries and exits are recorded for the right person. For this purpose one identifier like the facial image is enough or one fingerprint from the set of four recorded.
- Situation 2: identification at the border. Identifying whether a person was already recorded so that entries and exits are not allocated to a new individual file while the person was already enrolled. For this purpose the identification is conducted using the facial image and the four fingerprints to obtain a sufficient accuracy.
- Situation 3: identifying a non-documented traveller. This is the situation where the identity of a person (often an overstayer) needs to be established potentially in the absence of any travel document. Like in situation 2, the identification is conducted using the facial image and the four fingerprints.

There are three reasons why only biographical information would not be sufficient for the first situation which is the situation most often encountered:

- There is a high proportion of homonyms among the names of third country nationals. The only strong identifier⁸ is the combination of passport number and issuing country.

⁸ A strong identifier in IT means an identifier that is unique and stable. In a personnel database, the strong identifier is the personnel number but not the first and last name as both can have homonyms.

This identifier is however not stable over time as the passport can be changed following expiry, loss, theft, or involuntary destruction to cite the most common cases. The proportion of homonyms is much higher among the names of third country nationals⁹ than of citizens of Schengen countries which makes that relying solely on name matching or biographical data is very error prone. The biometric data provide the unsurpassed benefit of linking in a stable and reliable manner an identity to a same physical person.

- The situation of homonyms is worse as names that are originally not spelled in Latin alphabet are transliterated. This transliteration maps differently spelled names potentially to a same transliterated name. However, the transliteration rules are not necessarily stable over time and are not consistently applied, which makes that successive passports of a same person do not spell a name in exactly the same way. Linking entry/exit records on the basis of first and last name as well as any other key based on this appears even more error prone.
- Persons do not necessarily keep the same name. Only a limited number of countries try to consider the name as a strong identifier. In many countries the name changes according to the marital status and to other events in life. For perfectly lawful reasons, a same person can therefore appear at two successive moments with different names. Again, name matching appears to be very error prone.

The situation 2, where a person has different travel documents for legal reasons (example: a significant minority of persons has two nationalities or two passports for convenience reasons), needs to be detected. Otherwise, a same person could stay indefinitely in the Schengen area by being enrolled twice but with a different passport and alternating its use in order never to exceed the duration of stay. Given that not all cases would be detected by only relying on name searches a biometric identification is required.

The situation 3, where a person has no travel document, is the most obvious case where only biometric identifiers can be used to search the EES database. The experience of VIS has demonstrated the importance of this capability as on a yearly basis about 14.400 (about 1.200 per month)¹⁰ are done and follow an upward trend as more biometrics are available now than before.

It can be noted that at the level of a single EU Member State, citizens are not identified by means of their first and last name but by means of a so-called "concatenated key" composed of "first names (plural), last name, date of birth (day/month/year) and place of birth". However, even in this case the risk of confusing persons was still deemed too high and a unique national identifier was introduced (e.g. a social security number or a national register number). There is no such universal identifier available and the "concatenated" key used at the level of an EU Member State would not work for third-country nationals as their passports do not contain the place of birth and the date of birth is often simply a year.

⁹ As an example there are ten names shared by 100 million Chinese citizens. A similar situation exists in other Asian countries.

¹⁰ Obtained from regular statistics on the use of VIS produced by eu-LISA. Values used refer to March 2015.

As a conclusion, biometric identifiers are adequate and relevant for identifying travellers accurately. They therefore reduce significantly the risk of confusion between identities as there is no other universal unique and stable identifier of individuals.

Why these biometric identifiers?

The minimum set of biometric identifiers (i.e. the facial image and 4 fingerprints at enrolment) has been chosen for the intended use in the three situations mentioned above (i.e. verification at the border, identification at the border, documenting undocumented persons). This choice represents the minimum set of identifiers that can establish identity with a high accuracy given the number of travellers who will be recorded (i.e. the 'lighter'/'smaller' biometric identifiers necessary and sufficient for the specified purposes of identification of third country nationals crossing the Schengen area external border). The proposal will also foresee that verification can be done on the basis of the facial image only. The other potential options would consist in recording 8 or 10 fingerprints in addition to the facial image. Capturing 8 or 10 fingerprints at all borders increases precision for identification but only marginally while, at the same time, it becomes operationally very burdensome and it has a significant negative impact on waiting times for travellers.

13.3.6. Proportionality test

The questions to be answered under this heading are:

Need for an additional border control measure

The question raised is whether existing data collections do not or could not fit the purposes pursued by the EES. It is different from the technical question whether the EES needs to be built as an extension of an existing system (the VIS is usually cited) or by reusing components of another one. What matters here is whether a new (important) collection of personal data needs to be created on top of the existing ones.

There are currently three large-scale IT systems in operation in the area of Justice and Home affairs. The table below summarises their purpose, data content and data retention period.

Instrument	Purpose(s)	Personal data coverage	Data retention
Visa Information System (VIS)	To help implement a common visa policy and prevent threats to internal security.	Visa applications, fingerprints, photographs, related visa decisions and links between related applications.	5 years.

Instrument	Purpose(s)	Personal data coverage	Data retention
Schengen Information System (2nd generation) (SIS)	To ensure a high level of security in the area of freedom, security and justice and facilitate the movement of persons using information communicated via this system.	The data categories in SIS plus fingerprints and photographs, copies of European Arrest Warrant, misused identity alerts and links between alerts. SIS alerts relate to several different groups of persons.	Personal data entered in SIS for the purpose of tracing persons may be kept only for the time required to meet the purpose for which they were supplied, and no longer than three years. Data on persons subject to exceptional monitoring on account of the threat they pose to public or national security must be deleted after one year.
EURODAC	To assist in determining which Member State should assess an asylum application.	Fingerprint data, sex, the place and date of the application for asylum, the reference number used by the Member State of origin and the date on which the fingerprints were taken, transmitted and entered in the system.	10 years for asylum-seekers' fingerprints; 2 years for those third country nationals apprehended in connection with the irregular crossing of an external border.

Visa Information System (VIS)

The main purpose of the Visa Information System (VIS) is to permit the verification of the visa application history and to verify whether the person presenting the visa at the border is the same person to whom the visa has been issued at entry.

It concerns only those third-country nationals who are required to hold a visa. The VIS was not developed to keep track of entries and exits of third-country nationals nor is it meant to allow checking whether a person, after entering the EU legally, has or has not complied with the authorised stay according to the visa. Therefore the possibility of including entry/exit functionality in the VIS itself and the storage related to non-visa holders in the VIS can be discarded.

However, there would be major technical and functional links between the VIS and the EES. Besides the same technical features and a common matching functionality, VIS is the repository of the biometric identifiers of visa holders who will be registered in the EES. The fingerprints of the visa holders would not be stored in the EES as they already exist in the VIS. The EES would re-use the visa holder fingerprints already captured for the benefits of VIS, without duplicating the effort and avoid storing the fingerprints of visa holders twice.

Schengen Information System

The Schengen Information System (SIS) provides access to alerts on persons and objects to a large set of authorities including migration and border control, law enforcement and judicial authorities.

The main categories of alerts are:

- Persons wanted for arrest for extradition purposes;
- Third-country nationals to be refused entry to the Schengen territory;
- Missing persons (children and adults);
- Witnesses and persons required to appear before the judicial authorities in connection with criminal proceedings;
- Persons or vehicles to be put under discreet surveillance or for specific checks;
- Certain categories of objects (e.g. stolen identity cards, vehicles, firearms, bank notes).

The SIS operates on the principle that the national systems cannot exchange computerised data directly between themselves, but instead only via the central system. The SIS enables authorities to check persons and objects both at external borders and within the territory of the Schengen States. The SIS provides law enforcement authorities with information on why a certain individual is wanted, what action is to be taken and whether the person is presumed violent and armed.

However, as the information contained in the SIS is only sufficient for the authorities on the ground to take the correct initial actions, it is necessary for the Member States to be able to exchange supplementary information, either on a bilateral or multilateral basis, as required for implementing certain provisions of the Schengen Convention, and to ensure full application of Title IV of the Schengen Convention for the SIS as a whole.

The description above evidences that the SIS is not designed to record entry and exit data and compute durations of stay.

Eurodac

Eurodac is a fingerprint database that stores and compares the fingerprints of asylum applicants and irregular immigrants and which allows Member States to identify the State responsible for examining an asylum application in accordance with the Dublin II regulation. The Eurodac central unit operates a central database comparing fingerprints, an automated fingerprint identification system (AFIS) and a secure communication system for data transmission from and towards the national units (National Access Points) in Member States.

Neither the purpose nor the type of data Eurodac contains come even close to the objectives pursued by EES. On the contrary, it is when a person entered the Schengen area for a short stay and subsequently requests asylum that Eurodac can be used to check whether the same person already applied for asylum elsewhere.

Advanced Passenger Information and Passenger Name Record

For the sake of completion, and although these are not large-scale systems, they belong to categories of data to which the competent authorities potentially have access to.

Information collected on travellers, via Advanced Passenger Information (API) and via Passenger Name Record (PNR), applies to air and sea travel only for API data and to air travel only for PNR data: there is no information collected for crossing of land borders by individual means (personal car, (motor)bike, etc.) or by train. It is therefore not directly relevant for the EES. In addition, as these data are normally collected from airlines, travel agencies or entered by the traveller himself, the quality of the data is inferior to the data that would be collected from the travel documents at border control.

Conclusion. The investigation of the existing data collections concludes that none of the existing systems meets the purpose and contains data that correspond with EES at the exception of the VIS. The VIS contains identification data including biometrics for visa-required travellers but contains no data on visa-exempt travellers. The regulation therefore proposes for visa-required travellers to re-use the identification data from VIS and add their entry/exit records in EES, and for visa-exempt travellers to record both the identification data and the entry/exit data in EES. SIS and Eurodac have a completely different purpose and functionality than EES.

Least privacy-intrusive measure

The question whether there would be a less privacy intrusive measure is understood as answering two sub-questions: (1) is there a way for the number of travellers whose personal data are recorded to be reduced and (2) is there a way where less data could be collected from each traveller.

The number of travellers whose personal data are recorded corresponds strictly to the span of application of the Schengen Borders Code. The EES regulation does not modify the nature of the checks of the SBC but changes how they are done. The data collection is therefore also organised at the level where the SBC is applied: the whole Schengen area and not the constituent countries.

The amount of data collected for each traveller has been kept for the minimum. The description of the different data elements stored in EES (see section 13.1) and of the processing of data (see section 1.3.3) show that all data included have a justification and that less data would not allow to pursue the two objectives for the regulation (improved border management and reduce irregular migration). The biometric identifiers of the preferred solution are also the minimum set of biometrics that provide the accuracy required for linking entry/exit data to a personal file for the three situations (verification at the border, identification at the border, identification of non-documented person) where EES would be used.

Proportionality

It is the assessment of proportionality that led the European Court of Justice (ECJ) to annul Directive 2006/24 as the Court otherwise considered that the directive did not affect the essence of the right to private life and pursued objectives of general interest.

Compliance with the principle of proportionality has already been addressed to some extent in section 13.3.2 above.

Differentiation, limitation or exception in data collected.

As indicated in section 13.3.2 above, the measure addresses only the third-country nationals entering the Schengen area for a short stay as these are all submitted to the

same border control as per the Schengen Borders Code which is not changed on the substance.

The measure contains exceptions on the data collected as it does not include third-country nationals with long-stay visas or residence permits. It also excludes third-country nationals crossing the land borders of the Schengen area with a Local Border Traffic permit. It further excludes EU nationals and persons enjoying the right of free movement.

The result of the measure is that for visa-required travellers no additional personal data will be collected than already required under the VIS regulation but that entry and exit records will be stored per traveller over the duration of the data retention period. For visa-exempt travellers the result will be that personal identifiers will be collected as well the individual entry and exit records over the duration of the data retention period

The scope of persons whose personal data are collected as well as the data themselves correspond to the objectives pursued. The first objective of improving border control applies as well to the border control of visa-exempt and visa-required travellers. This is not the largest group of travellers but the one that represents the highest workload for border guards and where current methods for recording entries and exits (i.e. use of manual stamping) prevent any form of automation. Improved border controls need to rely on the result of past controls and on the improved accuracy of the identification of the traveller. The second objective of reducing irregular migration and overstay in particular concurs with the first objective on the data to be collected but requires the process of EES to calculate automatically the remaining duration of stay.

Link with specific migration objectives

The measure addresses under its second objective a specific migration objective of reducing irregular migration.

Conditions of access to data

Access is given to the data stored in the EES only for specified, explicit and legitimate purposes. The regulation provides that the authorities who will have access to the EES have to be designated for a specific limited purpose. The regulation can rely for this aspect on the VIS regulation which implemented the same approach.

Access for consulting the data is reserved exclusively to duly authorised staff of the authorities of each Member State who are competent for the specific purposes foreseen in the EES. Such access is limited to the extent to which the data are required for the performance of the tasks in accordance with these purposes.

The use of process accelerators

Concerning the use of process accelerators foreseen in the impact assessment, no additional information would be collected as there is no registered traveller's status and the facilitation is based on information already registered into the EES.

Furthermore, the use of modern IT systems, ABC gates and self-service kiosks at border controls can be perceived as less prone to discrimination as compared to checks performed by human beings. The prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21) could consequently be

positively impacted by the introduction of the EES. This question has been addressed by the Fundamental Right Agency survey (see Annex 15). The results of the survey showed that there is a widely held view that automated systems could cause less discrimination (e.g. on the basis of race or ethnicity) compared to checks carried out in person by border guards.

Data retention period

The main criterion used for the data retention period is that officials dealing with migration matters should have the same visibility on the travel history as it is currently the case when scrutinising the entry/exit stamps contained in a passport.

The majority of current passports have a validity period of ten years and there is usually the requirement that passports remain valid six months beyond the date of return. On average, a passport at the moment of its inspection by an authority contains a history of previous travels ranging between zero (a brand new passport) and nine and a half years (a passport close to the end of its validity). Given the large number of passports, the average situation is that the passport contains five years of entry/exit stamps. Hence the retention period is five years for all travellers.

The relevance of this data retention period is further confirmed by the fact that in the case of visa-required travellers the visa application data are kept for five years after expiry of the visa. The entry and exit data can be considered as the complementary information on how this visa was used and thus it is logic that the data retention period of EES and VIS data would be aligned. The validity of multiple-entry visas (MEV's) is also five years. For assessing the renewal of MEV's the consular officer currently examines the Schengen entry and exit stamps in the passports. With EES these entry and exit stamps of the Schengen area would no longer exist and hence justify a data retention period of five years.

A differentiator occurs however at the end of the data retention period. In the "normal" case, at the expiry of the data retention period of each entry/exit record calculated from the date of exit, the record is deleted. In case there are no more recent entry/exit records, the whole personal file is deleted, as the purpose of a personal file is to have entries and exits linked to it. In the case where overstay occurs, at the expiry of the date retention period there is still an entry record without an exit record. In that case, after five years calculated from the last possible day of authorised stay, the personal data and the entry/exit data are not deleted but removed from EES, handed over to each Member State for possible introduction into SIS. From that moment the data retention rules of SIS become applicable.

Data protection principles foresee that the retention of personal information shall be limited to the relevant purposes. A short data retention period is sufficient for achieving the second objective of the EES (i.e. to reduce irregular migration by addressing the phenomenon of overstaying) but would not be sufficient for facilitating the border crossing of bona fide travellers which is an essential element of the first objective. Therefore, in light of the above, a data retention period of five years, similar to the personal data anyhow stored in VIS, is considered sufficient and proportionate to the objective of facilitating the border crossing of bona fide travellers.

The 5 year length of the data retention period is also beneficial to the traveller. By having personal data, and in particular biometric data, stored over a relatively long period of time, the traveller is relieved from having to enrol his/her identity again at each entry to

the Schengen area. The enrolment step for visa-exempt travellers is indeed an additional step within the border control process introduced with the use of EES and, as such, requires time. Although benefits will accrue to the traveller at return visits, by lengthening the time-span between enrolments, that inconvenience can be mitigated. The same reasoning was applied for VIS where biometrics only need to be enrolled again after five years for similar reasons of convenience for the data subject.

Protection of data against risk of abuse?

The protection of data against risk of abuse refers in particular to the access to data and/or the transfer of data to persons to whom that access was not granted.

The main protection measures included in the regulation are:

- Access to EES is restricted to specific persons within designated Competent Authorities;
- Transfer of data to third parties, whether private or public entities is prohibited;
- All data processing is done by eu-LISA and therefore do not leave the EU.

A set of technical measures will further be developed and implemented as part of the security plan that must be implemented during the development of EES.

13.3.7. Protection of other fundamental rights

The improved border control measures (aspects related to law enforcement are set out further) better implement:

- Article 5 ("The prohibition of slavery and forced labour"). Victims of trafficking in human beings have been found among the category of overstayers and such situation can be suspected on the basis of the characteristics (age category, gender, country of origin to cite the obvious ones) recorded in EES. With EES these data are recorded for all countries and identify the date and place of entry which can lead to better detection at the border crossing point where this trafficking is occurring.
- Article 15.3 ("Nationals of third countries who are authorised to work in the territories of the Member States are entitled to working conditions equivalent to those of citizens of the Union."). This fundamental right becomes less relevant when there is an uncontrolled influx of irregular migrants who will accept any working conditions. The size and rate of increase of the number of overstayers is detrimental to the use of this right by third country nationals who use means of legal migration to stay and work in the EU.

The impact of EES on these fundamental rights further justifies the proportionality of the data collection.

13.3.8. Appropriate safeguards at EU level

A number of safeguards are integral to the proposed regulation, in particular for complying with fundamental rights:

- If there are errors on the identity checks of passengers, facilities are made available for carrying out manual checks and for amending the data on entry and exit at all

border crossing points. Regarding such facilities, the Schengen Borders Code currently requires that thorough second line checks for third-country nationals shall be carried out in a private area where the facilities exist and if requested by the third-country national.

- Individuals have the right to access information held on them and to challenge and correct it, if the processing of this data does not comply with the provisions of Directive 95/46 and Regulation 45/2001, in particular because of the incomplete or inaccurate nature of the data.
- Individuals are given the right to lodge a complaint with a data protection authority regarding the processing of their personal data and they are given the right to effective administrative and judicial remedies (Article 47 of the Charter).
- The guarantees ensuring an effective remedy (Article 47 of the Charter) for third-country nationals enable them to challenge a notification of an overstay by the entry/exit system, for example in situations when they were forced to overstay, particularly if it appears that they overstayed for a valid reason (e.g. hospitalisation, change in travel arrangements), when errors were made in recording dates of entry or exit or to show that they have a legal right to stay (e.g. based on a new visa, marriage to an EU citizen, application for asylum, refugee status).
- In case the EES notifies an overstay, this indication does not lead automatically to detention, removal or a sanction for the third-country national. Third-country nationals have access to effective remedies in such proceedings in order to protect the right to liberty and security (Art. 6 of the Charter), right to asylum (Art. 18 of the Charter), respect for family life (Art. 7 of the Charter) and the obligation of non-refoulement (Art. 19(2) of the Charter). A decision to detain, remove or sanction a third-country national is not based solely on a notification of overstay by the entry/exit system. In addition the safeguards of Directive 2008/115/EC are respected.
- The measures protecting rights of travellers, including right to an effective remedy, must also take into account the privileged position of non-EU family members of EU citizens whose right to enter and to stay depend on the right of the respective EU citizen in accordance with Directive 2004/38/EC.

13.3.9. Rights to Access and Correction

The rights to access and correction have already been developed under the section on "Appropriate safeguards", which deals not only with the right to access and correction but also with safeguards as regards the consequences for data subjects even when data are correct.

13.3.10. Control by an independent authority

Under the proposed regulation, the supervision of all data processing activities is carried out by Member States data protection authorities and the European Data Protection Supervisor which is conferred with all the necessary powers to intervene and enforce compliance with data protection rules.

13.3.11. Need for security and data protection by design and by default

The principles of data protection by design¹¹ and data protection by default are taken into account by implementing a set of very efficient data protection techniques already used in other large-scale IT systems (VIS in particular):

- The network used for the transmission of data from the central to the national domain uses encryption;
- The minimal data set is stored in EES (data minimisation principle¹²);
- Access to data is governed by access controls;
- All access to data is logged;
- All changes to data produce an audit trail.

The need for security translates into the implementation of a security plan that addresses physical and logical security of the data.

13.3.12. Conclusion

The authorities who should have access to the Entry Exit System must be designated for the specific purpose of the system. Therefore, access for consulting the data is reserved exclusively to duly authorised staff of the authorities of each Member State who are competent for the specific purposes of the Entry Exit System and limited to the extent the data are required for the performance of the tasks in accordance with these purposes.

All safeguards and mechanisms are in place for the effective protection of the fundamental rights of travellers particularly the protection of their private life and personal data. Third-country nationals must be made aware of these rights.

The EES hence respects the essence of the right to privacy, meets clearly defined objectives of general interest and is proportionate as the data stored in the EES strictly meet the legitimate objectives pursued by the Regulation and as the group of persons to whom it applies strictly corresponds to the ones affected by the applicable rule on duration of short stay.

Finally, it should be reminded that the EES helps to safeguard the fundamental rights of the European citizens provided under Article 5 of the Charter ("The prohibition of slavery and force labour") and Article 15.3 of the Charter ("Nationals of third countries who are authorised to work in the territories of the Member States are entitled to working conditions equivalent to those of citizens of the Union."). Furthermore, the use of modern IT systems, ABC gates and self-service kiosks at border controls can lead to a system less prone to discrimination as compared to checks performed by human beings and hence constitute an additional safeguard in terms of prohibition of discrimination (e.g. on the basis of race or ethnicity) in the meaning of Article 21 of the Charter.

¹¹ Privacy and Data protection by Design – from policy to engineering, Enisa (European Union Agency for Network and Information Security, December 2014.

¹² The withdrawal of the proposal of having the EES and the RTP as separate systems, in favour of a unique system also contributes to compliance with the data collection limitation and data minimisation principles.

13.4. Impact assessment for Law Enforcement Access

The approach followed states that in case access is given to Law Enforcement Services, the fundamental rights impact assessment needs to specifically re-do the test on necessity and proportionality:

Unlike in the 2013 proposal, in this proposed measure the objective "to contribute to the fight against terrorism and serious crime" appears as a secondary objective of the proposal. To meet this objective the access to EES data collected for immigration purposes are made accessible to Law Enforcement Authorities under precise conditions. It can be noted that Law Enforcement Authorities are given an access to immigration data and that no data are recorded in EES for another purpose than immigration control.

All the safeguards and control measures that apply to the EES data and explained under section 13.3 therefore remain valid and are not repeated under this section again.

The assessment therefore concentrates on the question of necessity and proportionality and on additional measures that protects the data subjects.

13.4.1. Necessity

This secondary objective is achieved by granting access to the EES database to Member States' law enforcement authorities and Europol in order to pursue the fight against terrorism and serious crimes under very specific and strict conditions. It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest.¹³

The Entry Exit system is the only system that collects the entry/exit data of all third-country nationals entering the Schengen area for a short stay, whether via a land, sea or air border. No other existing or envisaged data collection would even by far match the completeness of entry /exit data recorded in EES. As such for the purposes of criminal investigations, only EES can provide data to confirm or not the presence of specific third country nationals in the Schengen area. The EES also uses the identification data to link entries and exits and can act as the database of last resort for identifying persons when more focused databases did not yield a result.

The necessity of giving an access to EES data by law enforcement services has already been demonstrated by the situation with VIS. Although access has been given only since two years to VIS data, there are more than 1.400 searches done on a monthly basis. Further thirteen countries have a national system in operations with entry-exit functionalities since many years. In all cases access to law enforcement authorities to the data recorded is granted and has demonstrated to fulfil a need.

The information contained in the Entry Exit system is necessary for the purposes of the prevention, detection and investigation of terrorist offences as referred to in Council Framework Decision 2002/475/JHA of 13 June 2002 on combatting terrorism or of other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.

¹³ See Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation v Council and Commission* EU:C:2008:461, paragraph 363, and Cases C-539/10 P and C-550/10 P *Al-Aqsa v Council* EU:C:2012:711, paragraph 130.

To meet the purposes mentioned in the previous paragraph there are two situations where the access to EES would be necessary:

- **Identification.** The data recorded in EES could support law enforcement authorities in the fight against terrorism and serious crime to establish the identity of a third country national both in cases where he/she destroyed his/her documents and when investigating a crime through the use of fingerprints or facial image. It should be noted that although the identification for law enforcement purposes is technically the same operation as the identification during inland control for immigration enforcement, the authority performing the check, the purpose (criminal responsibility vs verifying the right of stay) and the outcome of the control (potentially prosecution vs possible return decision) are very different in essence.
- **Criminal intelligence.** The data recorded in EES could also help to construct evidence by tracking the travel routes of a person suspected of having committed a crime or of a crime victim. Therefore, the data in the EES should be available, subject to the conditions set out in the regulation to the designated authorities of the Member States and the European Police Office (Europol).

"Cascade mechanism" for identification purposes. In case access to the EES is requested for identification of unknown suspects, perpetrators or victims of terrorist offences or other serious criminal offences, the principle is applied that more focused databases would be used before accessing the EES. In practice there is only the access to the data collected under the Prüm system that contains biometric data from known criminals that would meet this condition.

Data retention period. A data retention period of five years would be necessary also for the secondary purpose of the fight against terrorism and serious crime because in order to construct evidence in criminal cases by analysing data on travel routes, law enforcement authorities would have to be able to track the travel routes back for a period of several years. The data should be deleted after the period of five years, unless there are grounds to delete it earlier.

The data retention period has been determined on the basis of the experience gained with the use of the national systems recording entry/exit data at national level in thirteen Schengen Member States and which are all used, sometimes even primarily, by law enforcement authorities. The data retention periods range between five and twenty-five years and with one case where no deletion of data is envisaged at all. From Commission's evaluation and specific consultation of law enforcement authorities, the likelihood of having to access EES data beyond five years is not zero but follows a downward trend. The data retention period has therefore also been aligned to the ones for immigration purposes.

13.4.2. Proportionality

An essential element that meets the principle of proportionality is that access to data by law enforcement authorities would always be related to a specific case.

- Authorities could have access in well-defined cases, for identity verification and/or criminal intelligence purposes, when there is a substantiated suspicion that the perpetrator of a criminal offence could be registered in the EES. The proportionality principle requires that the EES be queried for such purposes only if there is an overriding public security concern, that is, if the act committed is so reprehensible that

it justifies querying a database that registers persons with a clean criminal record and the threshold for authorities responsible for internal security to query the EES must therefore always be significantly higher than the threshold for querying criminal databases.

- Access to the EES to request comparisons of data on the basis of a latent fingerprint, which is the dactyloscopic trace which may be found at a crime scene, is fundamental in the field of police cooperation. The possibility to compare a latent fingerprint with the fingerprint data which is stored in the EES in cases where there are reasonable grounds for believing that the perpetrator or victim may be registered in the EES will provide the authorities of the Member States with a very valuable tool in preventing, detecting or investigating terrorist offences or other serious criminal offences, when for example the only evidence at a crime scene are latent fingerprints.

13.4.3. Protection of other fundamental rights

Granting access to EES data by law enforcement authorities helps to safeguard the fundamental rights of the European citizen provided under the Chart:

- Article 2(1) ("Everyone has the right to life") Article 3(1) ("Everyone has the right to respect for his or her physical and mental integrity"), Article 5 ("Prohibition of slavery and forced labour") and Article 6 ("Everyone has the right to liberty and security of persons"). The type of criminal offenses (terrorism and serious crime) for which law enforcement authorities would have access to EES, when all other conditions are met, are the ones that pose a serious threat to the lives of the citizens in the EU.
- Article 45(1) ("Every citizen of the Union has the right to move and reside freely within the territory of the Member States"). This applies in particular to terrorist offenses where the difficulty to prevent and counter-act leads authorities to re-install controls on all travellers within the EU reducing the use of the right contained in Article 45(1). The possibilities given to law enforcement authorities for a more effective fight against terrorism therefore also protects this fundamental right of EU citizens.

13.4.4. Specific Safeguards

Independent control of the reasons for access. A specific safeguard mechanism is provided in the regulation that ensures the independence and control of the Central Access Points and the operating units that initiate the requests for access. Requests for access to data stored in the Central System should be made by the operating units within the designated authorities to the Central Access Point and should be reasoned. The operating units within the designated authorities that are authorised to request access EES data should not act as a verifying authority. The Central Access Points should act independently of the designated authorities and should be responsible for ensuring, in an independent manner, strict compliance with the conditions for access as established in this regulation. The duly authorised staff of the Central Access Points should then process the request to the Central System following verification that all conditions for access are fulfilled. In exceptional cases of urgency, where early access is necessary to respond to a specific and actual threat related to terrorist offences or other serious criminal offences, the Central Access Point should process the request immediately and only carry out the verification afterwards.

Processing by Member State authorities. The processing of personal data by the authorities of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences pursuant to this regulation should be subject to a standard of protection of personal data under their national law which complies with Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters .

Exchange of personal data. For the purpose of efficient comparison and exchange of personal data, Member States should fully implement and make use of the existing international agreements as well as of Union law concerning the exchange of personal data already in force, in particular of Decision 2008/615/JHA

Transfer of data to third parties. Transfers of personal data obtained by a Member State or Europol pursuant to this regulation for law enforcement purposes from the Central System to any third country or international organisation or private entity established in or outside the Union should be prohibited due to the potentially vast amount of data which could be shared and the risk of data mining. Certain third countries may also misuse access to data of their citizens for exercising repercussions on the members of their families still present in that third country.

13.4.5. Conclusion

Access to EES by law enforcement services fulfils a need that cannot be achieved by other measures, like access to another system. The data protection measures consist in granting this access only for specific categories of crimes (terrorism and serious crime), for specific purposes (criminal intelligence and criminal identification) related to specific cases, to specific authorities, using a specific control mechanism and in the case of criminal identification when the search was first conducted vs criminal databases before accessing the EES data. And on top of this, the independent control and safeguard mechanisms applicable to EES data continue to prevail.

Finally it should be reminded that granting access to EES data by law enforcement helps to safeguard the fundamental rights of the European citizens provided under Article 2(1) of the Chart ("Everyone has the right to life"), Article 3(1) of the Chart ("Everyone has the right to respect for his or her physical and mental integrity"), Article 5 of the Chart ("Prohibition of slavery and force labour") Article 6 of the Chart ("Everyone has the right to liberty and security of persons") and Article 45(1) of the Chart ("Every citizen of the Union has the right to move and reside freely within the territory of the Member States").

14. ANNEX 14: EXECUTIVE SUMMARY OF RESULTS FROM 2015 PILOT¹⁴



Adobe Acrobat
Document

¹⁴ http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_executive_summary_en.pdf

15. ANNEX 15: FUNDAMENTAL RIGHTS AGENCY SURVEY - REPORT¹⁵



Adobe Acrobat
Document

¹⁵ http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf (see section 7)

16. ANNEX 16: PREPARATORY WORK WITH THE EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)

On 12 December 2014, DG HOME consulted the EDPS in the context of the preparation of the Smart Borders Pilot. A meeting was organised to discuss the provisions concerning personal data protection to be foreseen in the delegation agreement entrusting the implementation of the Smart Borders pilot to eu-LISA. The outcomes of this meeting were inserted in the delegation agreement.

On 20 March 2015, DG HOME and EDPS jointly organised a workshop on the preparation of the Smart Borders proposals. The outcome of this workshop is summarised below.

On 21 September 2015, some questions related to the Smart Borders were discussed in an interactive workshop between DG HOME and EDPS focussing on "Data Protection and Privacy Considerations in Policies on Migration and Home Affairs".

* * *

Proceedings of the 20 March 2015 workshop on Smart Borders proposals.

1. Introduction by the EDPS

The EDPS gave a presentation on the impact of the judgment of the Court of 8 April 2014 in Joined Cases C-293/12 and C-594-12 Digital Rights Ireland and Seitlinger and Others for the Smart Borders proposals. The EDPS also pointed out that the EP Legal Services' Opinion sets out a method for reviewing the validity of acts under Articles 7, 8 and 52 of the Charter, which include a number of factors to be considered. The main issue will be the possible addition of a secondary purpose to the EES proposal, namely the use of entry and exit data and biometrics for law enforcement purposes. The necessity and proportionality test will have to be taken and passed separately for the two possible purposes of the EES proposal. DG HOME said its analysis of the data retention ruling was the same as that of the EDPS and said it looked forward to working with the EDPS on building the blocks of LEA for this and other files.

The EDPS touched upon Privacy by Design and emphasized as a first step the need for a specific legislative text to embed concrete appropriate safeguards as regards data protection and security. Those safeguards should lead to ensuring that the design of the IT system respects data protection principles. The specific technical and security measures required in developing and protecting the IT system need not be embedded in the legislative text itself, but preferably should be developed later in separate documents when the legislative text is near finalisation. With regard to the envisaged website for information to carriers and travellers, the EDPS said that there was a business need to do this and that the legal base should contain a high enough level of details on it.

2. Biometrics in the Smart Borders package

DG HOME gave a presentation on the use of biometrics in the Smart Borders package and the need thereof to improve border control processes, especially for third country

nationals from visa-free countries. DG HOME informed the EDPS that probably there will be no duplication of data for visa holders of whom 10 fingerprints should already be in the Visa Information System. Also the combined use of fewer fingerprints with facial images will be tested during the Pilot Project.

DG HOME and the EDPS had a preliminary discussion on data protection considerations and clarified important elements of their respective analysis. The importance of distinguishing the use of data for verification/control purposes from identification purposes was underlined in relation to the processing of biometrics data, in the sense that identification requires more biometric data (such as fingerprints and a facial image) and cannot rely on facial image only.

3. Data retention

DG HOME gave a presentation on the data retention rules in the 2013 proposals, the drawbacks of those rules, the main findings of the Technical Study and the different options proposed by the Study.

DG HOME and the EDPS discussed the possible extension of the initial data retention period for the objective of improving the management of the external borders in order to avoid frequent registration of travellers in the system. They also discussed the need for extending the data retention period for the secondary purpose of law enforcement access. The EDPS underlined that the first question to be answered is the length for which it is necessary to retain data in the EES in view of the original purpose pursued. Then as concerns law enforcement access, there should be a thorough evaluation of the necessity of law enforcement access to the data. Even if in theory one could imagine that the initial retention period could be increased for an additional time on the basis of law enforcement access demonstrated needs, the EDPS mentioned that such an extension could only be valid if it respects the conditions of necessity and proportionality and provided that appropriate safeguards are implemented.

4. Necessity of access to EES for law enforcement purposes

The EDPS gave a presentation of their Policy Paper “Analysing the impact of privacy and data protection of EU legislative proposals”, which outlines the different steps taken by the EDPS when consulted on a legislative proposal.

DG HOME gave a presentation on the necessity of access to the EES for law enforcement purposes and the foreseen requirements. DG HOME reported on the conclusions of the EES Impact Assessment and the findings of the Study. From those documents, it appears that a 5-years retention period would be appropriate should law enforcement access be granted. DG HOME also reported on the state of play of discussions in the Council on LEA to the EES proposal and noted that most delegations want to have access to all data stored in the EES for a period of 5 years. DG HOME referred to the explanations of MS on the added value of LEA to the national entry/exit systems and the VIS and the specific examples they had given of the added value of LEA in solving cases concerning murder, smuggling of irregular immigrants, procurement for prostitution and narcotics, stolen vehicles, human and drug trafficking, state security and terrorism. DG HOME and the EDPS exchanged their views on the possible extension of the data retention period to 5 years for law enforcement purposes, taking into account differentiated access. The EDPS noted that differentiated access could make sense and insisted on the need for adequate safeguards but did not express any views on the question by DG HOME on the possible use of the VIS or the Eurodac model for the

proposal and on possible improvements which could be considered the reason being that the access procedure will need to follow the needs determined as necessary (i.e. this cannot be answered in the abstract). The EDPS mentioned its Opinion of 2011 on the Evaluation report from the Commission on the Data Retention Directive, which contains useful indications as to what kind of evidence is expected in order to demonstrate the necessity of an interfering measure.

The representative of the LS underlined the need to understand the precise uses that the law enforcement authorities would want to make of the system and the type of researches that they could need to carry out in different types of investigation. He suggested as hypothetical examples that LEA in the context of criminal investigations regarding crimes closely linked to illegal immigration (such as trafficking in human beings) might be considered differently from LEA to the same database in the context of investigating other crimes (such as murder): in the first case one of the constituent elements of the crime is bringing third country nationals illegally into the Union, which includes the crossing of the external border which is registered in the EES, whereas in the second case one would presumably check the EES for the remote possibility that the fingerprints found next to the deceased body are present in the database. The LS underlined the urgency to get down to detailed conversations with law enforcement specialists to hear in which precise investigation contexts they considered LEA to the EES of very high utility.

5. Requirements for communication of data to third countries

DG HOME gave a presentation on the requirements for communication of data to third countries included in Article 27 of the current EES proposal and explained that Article 46 of the proposal provides that the question of whether access to EES data to LE authorities of third countries shall be granted should be part of the evaluation to be conducted two years after the EES entered into operation.

DG HOME asked the EDPS on the way the conditions foreseen in Article 27 of the 2013 EES Proposal could be further substantiated as it had suggested in its opinion on the EES proposal. As regards the possible granting of access to law enforcement authorities of third countries, the EDPS referred again to the guarantees under the DRD ruling. DG HOME also asked the EDPS whether there should be a prohibition of transfers to third-country LEAs as is the case in the Eurodac Regulation or whether such access should be allowed in exceptional cases as in the VIS decision. The EDPS replied that the implementation of the different legal instruments should be examined carefully and noted it was premature to make an evaluation in this regard.

6. RTP: Use of MRTD instead of the token : data protection issues

7. RTP on-line application process.

8. Option to improve RTP efficiency

The points 7, 8 and 9 of the agenda were discussed altogether.

DG HOME presented the different options analysed by the Study for the RTP and their pros and cons; i.e. the use of a separate token, of an e-MRTD or of a MRTD. DG HOME and the EDPS exchanged their views on the use of the e-MRTD as the token for the RTP. The EDPS would need to look at the details of the different options in order to make informed comments on the options.

With regard to the RTP on-line application process, DG HOME and the EDPS discussed the possibility of redirecting the data submitted by the applicants to the competent Member State. The different architectures for the Webservice were also touched upon during the discussion.

17. ANNEX 17: EXISTING EU LARGE-SCALE IT SYSTEMS

17.1. Overview

This annex gives an overview of currently existing European large-scale IT systems. There are three European Large Scale IT systems:

- SIS: the centralised database containing alerts on persons and other categories of data for law enforcement and border check purposes (SIS);
- VIS: the database on visa applications. VIS uses a Biometric Matching System (BMS) which is established as a service that could be used by other systems (like EES in the future);
- Eurodac: the database on asylum applicants.

The EU Agency for large-scale IT systems, euLISA, is responsible for the operational management of these three systems including the BMS.

A police co-operation mechanism for exchanging information on DNA, fingerprints and vehicle registration data has been established through the Prüm Decisions. However the exchanges are happening between Member States and there is no central system.

Advanced Passenger Information (API) and Personal Name Records (PNR) are data sent by carriers to national authorities but there is no European system where these data are stored.

17.2. Legal instruments

The legal instruments for the three existing large-scale IT system are presented in the table below.

	Instrument	Description
SIS (II)	Regulation (EC) No 1987/2006 of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)	<p>This Regulation establishes the conditions and procedures for the entry and processing in SIS II of alerts in respect of third-country nationals, the exchange of supplementary information and additional data for the purpose of refusing entry into, or stay in, a Member State.</p> <p>The Regulation also lays down provisions on the technical architecture of SIS II, the responsibilities of the Member States and of the management authority referred in to Article 15, general data processing, the rights of the persons concerned and liability.</p>
	Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)	<p>The Decision establishes the conditions and procedures for the entry and processing in SIS II of alerts on persons and objects, the exchange of supplementary information and additional data for the purpose of police and judicial cooperation in criminal matters.</p> <p>The Decision also lays down provisions on the technical architecture of SIS II, the responsibilities of the Member States and of the</p>

engagement authority referred to in Article 15, general data processing, the rights of the persons concerned and liability.

	<p>Regulation (EC) No 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)</p>	<p>The Regulation defines the purpose of, the functionalities of and the responsibilities for the Visa Information System as established by Article 1 of Decision 2004/512/EC. The Regulation sets up the conditions and procedures for the exchange of data between Member States on applications for short-stay visas and on the decisions taken in relation thereto, including the decision whether to annul, revoke or extend the visa, to facilitate the examination of such applications and the related decisions.</p>
VIS	<p>Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences</p>	<p>This Decision lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may obtain access for consultation of the Visa Information System for the purposes of prevention, detection and investigation of terrorist offences and of other serious criminal offences.</p>
	<p>Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention</p>	<p>The Regulation establishes the Eurodac system which aims to assist in determining which Member State is to be responsible pursuant to the Dublin Convention for examining an application for asylum lodged in a Member State, and otherwise to facilitate the application of the Dublin Regulation under the conditions set out in the Regulation.</p> <p>This Regulation has been repealed with effect from 20 July 2015 by Regulation (EU) No 603/2013 (Eurodac recast Regulation) quoted further down.</p>
Eurodac	<p>Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000</p>	<p>This Regulation establishes rules for the transmission of data, for carrying out comparisons and transmitting results, for the communication between Member States and the Central Unit and for other tasks of the Central unit.</p> <p>This Regulation has been repealed with effect from 20 July 2015 by Regulation (EU) No 603/2013 (Eurodac recast Regulation) quoted further down.</p>
	<p>Regulation (EU) No 603/2013 of 26 June 2013 on the establishment of Eurodac for the comparison of fingerprints for the effective application of</p>	<p>Eurodac amendment amending Regulation (EU) No 1077/2011</p> <p>Eu-LISA was entrusted with the Commission's tasks relating to the operational management of Eurodac and with certain tasks relating to the Communication Infrastructure in accordance with</p>

Regulation (EU) No 604/2013 and amending Regulation (EU) No 1077/2013	Article 5 of the Agency establishing Regulation. This provision has been amended by Article 38(1) of the Eurodac recast Regulation
---	--

17.3. Schengen Information System

The Schengen Information System (SIS) is a large-scale information system that supports external border control and law enforcement cooperation in the Schengen States. The SIS enables competent authorities, such as police and border guards, to enter and consult alerts on certain categories of wanted or missing persons and objects. A SIS alert not only contains information about a particular person or object but also clear instructions on what to do when the person or object has been found. Specialised national SIRENE Bureaux serve as single points of contact for any supplementary information exchange and coordination of activities related to SIS alerts.

Purpose of SIS

The main purpose of the SIS is to help preserving internal security in the Schengen States in the absence of internal border checks.

Which countries use SIS?

The SIS is in operation in all EU Member States and Associated Countries that are part of the Schengen Area. Special conditions exist for EU Member States that are not part of the Schengen Area.

- EU Member States that are part of the Schengen Area. The Schengen Area encompasses most EU Member States, except for Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom. The 22 EU Member States that are part of the Schengen Area fully operate the SIS.
- Associated Countries that are part of the Schengen Area. Four Associated Countries that are part of the Schengen Area (Switzerland, Norway, Liechtenstein and Iceland) fully operate the SIS.
- Bulgaria, Croatia, Cyprus, Ireland, Romania and United Kingdom. Bulgaria and Romania currently only operate the SIS only for the purpose of law enforcement cooperation. They will start using the SIS for the purpose of external border control as soon as the decision for lifting the internal border checks has entered into effect. Cyprus and Croatia are enjoying a temporary derogation from joining the Schengen Area. They are currently carrying out preparatory activities to integrate into the SIS. The United Kingdom operates the SIS within the context of law enforcement cooperation. Ireland is carrying out preparatory activities to integrate into the SIS for the purpose of law enforcement cooperation.

How does it work?

The SIS operates on the principle that the national systems cannot exchange computerised data directly between themselves, but instead only via the central system. The SIS enables the users to check persons and objects both at external borders and within the territory of the Schengen States. The SIS provides law enforcement authorities

with information on why a certain individual is wanted, what action is to be taken and whether the person is presumed violent and armed.

However, as the information contained in the SIS is only sufficient for the authorities on the ground to take the correct initial actions it is necessary for the Member States to be able to exchange supplementary information, either on a bilateral or multilateral basis, as required for implementing certain provisions of the Schengen Convention, and to ensure full application of Title IV of the Schengen Convention for the SIS as a whole.

Article 92(4) of the Schengen Convention provides that Member States shall, in accordance with national legislation, exchange through the authorities designated for that purpose (SIRENE), all information necessary in connection with the entry of alerts and for allowing the appropriate action to be taken in cases where persons in respect of whom, and objects in respect of which, data have been entered in the Schengen Information System, are found as a result of searches made in this System.

The Schengen States are the owners of the data they introduce into the SIS and bear the responsibility for their legality and accuracy.

What does the SIS contain?

The SIS only contains alerts on persons or objects falling under one of the following alert categories:

- Refusal of entry or stay (Article 24 of Regulation (EC) No 1987/2006) This alert category covers third-country nationals who are not entitled to enter into or stay in the Schengen Area.
- Persons wanted for arrest (Article 26 of Council Decision 2007/533/JHA) This alert category covers persons for whom a European Arrest Warrant or Extradition Request (Associated Countries) has been issued.
- Missing persons (Article 32 of Council Decision 2007/533/JHA) The purpose of this alert category is to find missing persons, including children, and to place them under protection if lawful and necessary.
- Persons sought to assist with a judicial procedure (Article 34 of Council Decision 2007/533/JHA) The purpose of this alert category is to find out the place of residence or domicile of persons sought to assist with criminal judicial procedures (for example witnesses).
- Persons and objects for discreet or specific checks (Article 36 of Council Decision 2007/533/JHA) The purpose of this alert is to obtain information on persons or related objects for the purposes of prosecuting criminal offences and for the prevention of threats to public or national security.
- Objects for seizure or use as evidence in criminal procedures (Article 38 of Council Decision 2007/533/JHA) This alert covers objects (for example vehicles, travel documents, credit cards, number plates and industrial equipment) being sought for the purposes of seizure or use as evidence in criminal proceedings.

Who can access SIS?

The Schengen Information System (SIS) provides access to alerts on persons and objects to the following authorities:

- authorities responsible for border checks;
- authorities carrying out and coordinating other police and customs checks within the country;
- national judicial authorities, inter alia, those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, in the performance of their tasks, as set out in national legislation;
- authorities responsible for issuing visas, the central authorities responsible for examining visa applications, authorities responsible for issuing residence permits and for the administration of legislation on third-country nationals in the context of the application of the Union *acquis* relating to the movement of persons;
- authorities responsible for issuing vehicle registration certificates.

It is up to each Member State to decide which national authorities are competent and shall have access to some or all categories of SIS alerts depending on that competence.

Europol and Eurojust also have access to certain categories of alerts. Europol may access data entered for alerts for arrest, alerts for discreet surveillance or specific check and alerts on objects for seizure or use as evidence in criminal proceedings. Eurojust may access data entered for alerts for arrest and alerts for a judicial procedure.

Which data on persons are stored?

In 2015, about one million records exist on wanted persons. The vast majority of alerts on persons are about third-country nationals who shall be denied entry to the Schengen area.

As regards these individuals, the SIS currently stores only alphanumeric data (letters and numbers):

- names, including aliases;
- sex;
- objective physical characteristics "not subject to change";
- date and place of birth;
- nationality;
- whether the persons are armed or violent;
- the reason for the alert; and
- the action to be taken.

The alerts on persons may contain a picture or biometric information but only as attachments to the file and this information is not searchable. This means that a person cannot be found back in SIS on the basis of his/her fingerprints or picture. But once a person is found the picture and/or fingerprints can be used to ascertain the identity.

17.4. Visa Information System

The Visa Information System (VIS) is a system for the exchange of short-stay visa data between the Schengen and the Schengen Associated States that was initially established in 2004.

The Visa Information System (VIS) allows Schengen States to exchange visa data. It consists of a central IT system and of a communication infrastructure that links this central system to national systems. VIS connects consulates in non-EU countries and all external border crossing points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes.

All functionalities of the VIS are based on visa applications or visa decisions attached to applications. After a first registration, a visa application can be amended, until a decision is made whether or not a Schengen visa should be issued. After visa issuance, further decisions can be made, for example, an issued visa can be revoked or annulled, or a visa can be extended. The VIS supports the storage, maintenance and retrieval of this information.

Purposes of the VIS

- Facilitating checks and the issuance of visas: VIS enables border guards to verify that a person presenting a visa is its rightful holder and to identify persons found on the Schengen territory with no or fraudulent documents. Using biometric data to confirm a visa holder's identity allows for faster, more accurate and more secure checks. The system also facilitates the visa issuance process, particularly for frequent travellers.
- Fighting abuses: While the very large majority of visa holders follow the rules, abuses can also take place. For instance, VIS will help in fighting and preventing fraudulent behaviours, such as "visa shopping" (i.e. the practice of making further visa applications to other EU States when a first application has been rejected).
- Protecting travellers: Biometric technology enables the detection of travellers using another person's travel documents and protects travellers from identity theft.
- Helping with asylum applications: VIS makes it easier to determine which EU State is responsible for examining an asylum application and to examine such applications.
- Enhancing security: VIS assists in preventing, detecting and investigating terrorist offences and other serious criminal offences.

How does it work in practice?

Ten fingerprints and a digital photograph are collected from persons applying for a visa. These biometric data, along with data provided in the visa application form, are recorded in a secure central database.

Ten finger scans are not required from children under the age of 12 or from people who physically cannot provide finger scans. Frequent travellers to the Schengen Area do not have to give new finger scans every time they apply for a new visa. Once finger scans are stored in VIS, they can be re-used for further visa applications over a 5-year period.

At the Schengen Area's external borders, the visa holder's finger scans may be compared against those held in the database. A mismatch does not mean that entry will automatically be refused - it will merely lead to further checks on the traveller's identity.

Who can access VIS?

Competent visa authorities may consult the VIS for the purpose of examining applications and decisions related thereto.

The authorities responsible for carrying out checks at external borders and within the national territories have access to search the VIS for the purpose of verifying the identity of the person, the authenticity of the visa or whether the person meets the requirements for entering, staying in or residing within the national territories.

Asylum authorities only have access to search the VIS for the purpose of determining the EU State responsible for the examination of an asylum application.

According to Council Decision 2008/633/JHA of 23 June 2008, law enforcement authorities from Member States and Europol have a restricted and indirect access to the VIS data for the purposes of preventing, detecting and investigating terrorist and criminal offences. Each Member State has to designate an authority responsible for controlling law enforcement access to the database and the police have to provide evidence that their query is necessary for criminal investigations.

Which data are stored?

According to the text of Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008, the VIS stores the following personal data from visa applicants:

- Data on the applicant (i.e. name, address, occupation);
- Data on the visa application process (date and place of the application, visas requested, issued, refused, annulled, revoked or extended);
- Biometrics (photographs and fingerprints).

Current Status

The VIS started operations in the first region on 11 October 2011. The operations started first at the consulates in North Africa and 20 days after go-live of the VIS also at the border crossing points (verification of visas against the VIS).

Biometric verification of the visas is mandatory at entry into the Schengen area since 11 October 2013.

Since 20 November 2015, the "roll-out" was completed, meaning that all visas issued by consulates from Schengen Member States are recorded in VIS and contain biometrics.

17.5. Biometric Matching System

The Biometric Matching System (BMS) developed for the VIS is an information search engine that can match biometric data from visa applications, identity management systems and policing systems.

The system performs one-to-one comparisons for biometric verifications and one-to-many searches for biometric identifications.

The BMS is developed using a service-oriented architecture approach, has the capability to connect with a number of IT systems and manage functions related to visas, immigration, border control and police cooperation. In addition, the technical architecture is flexible enough to accommodate new developments in EU policy as immigration and border control procedures evolve.

BMS does not store biometric information as such which is owned by the requesting system. As an example, since currently BMS only operates with VIS, fingerprints and photo are stored in VIS. For each fingerprint, the template¹⁶ is stored in BMS. BMS provides the service of matching fingerprints on the request of the systems that it is linked to, currently only VIS but this can be extended when authorised. The current BMS does not use the facial image as a biometric identifier. This means that while pictures are stored in VIS there is no template equivalent created in BMS. Hence with the current VIS and BMS, the facial image cannot be used to search for a person or match a picture taken live with a picture stored in VIS. However the existing BMS can be enhanced with this functionality and does not require to be replaced.

17.6. Eurodac

The Eurodac Regulation establishes an EU asylum fingerprint database. The previous version of the Regulation was still valid until 20 July 2015 when the new one became applicable. When someone applies for asylum, no matter where they are in the EU, their fingerprints are transmitted to the Eurodac central system.

Updates to the relevant legislation establishing Eurodac were required to reduce the delay of data transmission by the Member States, to precipitate the asylum procedure, to address data protection concerns as well as to help combatting terrorism and serious crime by allowing law enforcement access to Eurodac. The new requirements were laid down in the Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013, establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person ('recast regulation').

The Eurodac system enables Member States to identify asylum applicants and persons who have been apprehended while unlawfully crossing an external frontier of the Community. By comparing fingerprints, Member States can determine whether an asylum applicant or a foreign national found illegally present within a Member State has previously claimed asylum in another Member State or whether an asylum applicant entered the Union territory unlawfully.

¹⁶ A template is a stored record of an individual's biometric features. Typically, a "livescan" of an individual's biometric attributes is translated through a specific algorithm into a digital record that can be stored in a database. The formatted digital record used to store the biometric attributes is generally referred to as the biometric template

The Eurodac central unit operates a central database comparing fingerprints, an automated fingerprint identification system (AFIS) and a secure communication system for data transmission from and towards the national units (National Access Points) in Member States.

Data collected for any asylum applicants over 14 years of age include:

- Fingerprint and control images;
- Date of the asylum application;
- The Member State where the asylum application was filed;
- The gender of the applicant.



Testing the borders of the future

Smart Borders Pilot: The results in brief



Co-funded by
the Internal Security Fund
of the European Union



ISBN 978-92-95208-00-1
10.2857/598631

© European Agency for the operational management of large-scale IT systems
in the area of freedom, security and justice, 2015

Reproduction is authorised provided the source is acknowledged.
The opinions expressed are those of the author(s) only and should not be considered
as representative of the European Commission's official position.

Contents

Background	2
Smart Borders: a unique and large-scale EU pilot	3
Pilot results	4
Key findings from operational testing	4
Fingerprint (FP) enrolment	4
Facial-image (FI) enrolment and verification	6
Iris enrolment	7
ABC gates	8
Kiosk	9
Key findings from desk research	11
Survey conducted by the FRA – key findings	12
Conclusion	12

Background

Border management is currently going through significant transformation. To address the need for the Schengen Area to move towards more modern⁽¹⁾ and efficient border management by using state-of-the-art technology, the European Commission proposed the 'Smart Borders package' on 28 February 2013. This package contained legal proposals for establishing two systems that should help to speed up, facilitate and reinforce border-check procedures for third-country nationals (TCNs) travelling into the Schengen Area:

- **EES** – a central *entry/exit system* to record the time and place of entry and exit of all third-country nationals travelling to/from the Schengen Area;
- **RTP** – a uniform *registered traveller programme* to allow pre-vetted and frequent travellers from third countries to enter (and exit) the Schengen Area with minimal border checks.

In order to further assess the technical, organisational and financial impacts of the various possible ways to address border-management challenges, the Commission subsequently initiated – with the support of the European Parliament and the Member States – a proof-of-concept exercise aimed at identifying, assessing and testing technical options for implementing the Smart Borders package.

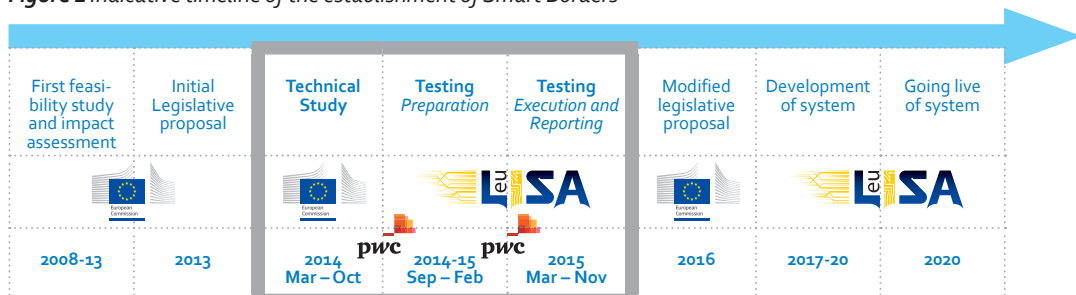
This exercise consists of two phases:

- **first phase – a Commission-led technical study** aimed at identifying and assessing the most suitable and promising options and solutions, as well as cost estimates. This study was delivered at the end of 2014;ⁱ and
- **second phase – a pilot (also called 'testing phase')** entrusted by the Commission to the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA).

The main objective of the pilot was to test a limited set of technical options (identified within the technical study) against specific measurable criteria in operational and relevant environments. These criteria are accuracy, effectiveness and impact on border-crossing duration. The testing phase aimed to contribute to defining the best technical solutions for faster and more secure border-control processes, respecting the highest principles on data protection and fundamental rights.

The Commission announced it would submit a modified legal proposal by early 2016 which – once adopted by the co-legislators – would allow eu-LISA to develop the system and start operations by 2020.

Figure 1 Indicative timeline of the establishment of Smart Borders



1 e.g. removing manual stamping and increased reliance on automated verification and identification methods.

Smart Borders: a unique and large-scale EU pilot

The targets and challenges set for the pilot were high and unique. More than 100 questions had to be addressed through either desk research or operational testing (or both). The limited technical options to be tested and researched amounted to 13 different test cases (TCs), such as the enrolment of four, eight and ten fingerprints, or the use of self-service kiosks⁽²⁾. It required the involvement of numerous stakeholders.

Therefore, eu-LISA involved the EU institutions and other agencies in both the preparation and execution phases, such as the European Data Protection Supervisor (EDPS), the Fundamental Rights Agency (FRA) and Frontex. Progress reports were regularly communicated to the European Commission, the Member States as well as to the European Parliament. The tests in the pilot were carried out successfully across Europe in 12 volunteering Member States between March and September 2015.

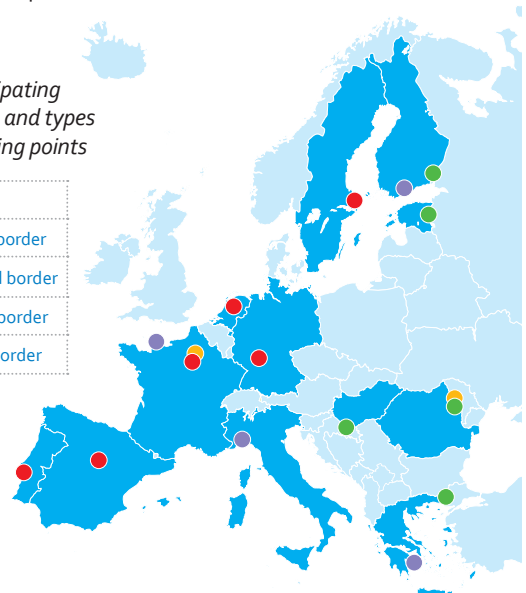
The scope did not include end-to-end⁽³⁾ testing with real data from travellers. The pilot was conducted in compliance with existing legislation. Traveller participation was completely voluntary. All the tests were conducted by the Member States under the close supervision and cooperation of national data-protection authorities.

The pilot lived up to expectations: it managed to deliver evidence-based results based on high participation rates from travellers, who were of various nationalities and all ages. One out of two travellers also provided feedback, and 89 % of respondents said that they were satisfied or very satisfied with their experience of the pilot. Participating border guards expressed positive feedback. eu-LISA also invited the FRA to look into the use of biometric technology on third-country nationals at the borders. The aim was to complement the third-country nationals' experience of the pilot with perceptions regarding the use of modern technology. Following this, the FRA carried out an independent small-scale survey at seven border-crossing points where the Smart Borders pilot took place to look into attitudes of third-country national travellers regarding the use of biometrics at BCPs and their opinions on various associated fundamental rights aspects.

Smart Borders Pilot in a nutshell	
Scope	Air, sea and land borders crossing points (BCPs)
Member States	12 (DE, EE, EL, ES, FI, FR, HU, IT, NL, PT, RO, SE)
Border crossing points	18
Test cases	78 test variations
TCN travellers	58 000
Border guards involved	About 350
Biometrics	Fingerprints (FP), Facial Image (FI) and iris
Process accelerators	ABC gates, kiosks
Desk research	Spoofing, VIS and travel document number, web service

Figure 2 Participating Member States and types of border-crossing points

Key	
	Sea border
	Land border
	Rail border
	Air border



² All 13 Test Cases are described in the Methodology chapter in an annex to the Final Report.

³ An end-to-end pilot would have encompassed recording personal data at entry into a central database simulating the EES and matching this data at exit. In that instance, the tests would have required a mock-up central EES system to be set up and personal data to be stored in that system. This would have required a specific legal framework allowing it.

Pilot results

This report presents the results of operational testing and desk research, providing **an important evidence** basis for the feasibility of the system(s) and processes proposed by the Smart Borders package.

Where possible, the results have been consolidated according to the same biometric identifiers. However, due to the differences in border crossings (e.g. conditions, volumes, processes, integration and set-up level of new testing equipment), not all the results from the same test cases at the different border-crossing points could be compared⁽⁴⁾. Instead, similarities and differences were considered from a duration, security or equipment-performance perspective.

Key findings from operational testing

Fingerprint (FP) enrolment

Table 1 Summary of locations per type of border where fingerprint enrolment was tested.

4 fingerprints (TC1) – at 11 border-crossing points, 8 FPs (TC2) – at 8 BCPs, 10 FPs (TC3) – at 6 BCPs	
Air	Frankfurt (DE) • Schiphol (NL) • Madrid (ES) • Charles de Gaulle (FR)
Sea	Helsinki (FI) • Piraeus (EL) • Genoa (IT)
Land (road)	Kipoi (EL) • Udvar (HU) • Vaalimaa (FI)
Land (train)	Iași (RO)
Outcome	the pilot confirms that it is feasible to enrol fingerprints at all types of borders in various set-ups. However, in practice, enrolling four fingerprints is faster than enrolling eight or ten, although a higher number of fingerprints will deliver better accuracy for subsequent use. The quality of the fingerprints enrolled is generally fit for purpose. Enrolling fingerprints in controlled conditions is seen as the biometric identifier that is the least intrusive to travellers, according to both travellers' and border guards' feedback.

Main findings

Success/quality

- The quality of fingerprint enrolment cannot be directly linked to the number of fingerprints enrolled.
- There are currently no certification standards for contactless scanners.
- When the success rate was below 30 %, this was mainly due to set-up and technical constraints.
- Identification accuracy can reach around 99.3 % based on performance predictions provided by a number of vendors and with a database containing four FPs each from 100 million records. When performing a verification of a known traveller, performance is known to be a fraction less than 100 %⁽⁵⁾.

4 In addition, a comparison of the results according to different biometric identifiers has been made with great caution due to the following factors:

- verification could only be tested for facial image and not for fingerprints and iris;
- only the vendors' quality thresholds could be used for FI and iris;
- kiosks were implemented only in limited operational settings; and
- iris is the newest biometric type and mostly unknown to border guards, whereas FP and FI are already used (FP for verification against the VIS; and FI at ABC gates).

5 Data on single-finger verification transactions is available from the on-going Fingerprint Verification Competition run by the University of Bologna (<https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx>).

Duration













- The added duration of the border-control process is directly linked to the number of fingerprints enrolled and the desired quality: enrolling four FPs had the least impact⁽⁶⁾ on time and is considered to have a relatively limited impact on the border-crossing process, with the vast majority of cases being performed in under 30 seconds on average. At air borders, average durations ranged from 17 seconds for 4 FPs to 60 seconds for 10 FPs. At sea, duration ranged from an average of 20 (4 FPs) to 46 seconds (10 FPs), and at land borders from 21 (4 FPs) to 49 seconds (10 FPs).
- In a nutshell, enrolling eight fingerprints took roughly twice as long as enrolling four (≈+126%), while enrolling ten fingerprints took almost three times longer (+185%).

Technology⁽⁷⁾

- The technology used to acquire four fingerprints was assessed as mature at all locations. A specific set-up might still be required at certain locations. In general, enrolling FPs in outdoor and moving conditions can sometimes raise issues (e.g. extreme temperature conditions, direct UV light on the optical lens).
- It is important that the system provides real-time feedback to both the traveller and the border guards during the enrolment process.

Experience

- Fingerprints are the type of biometric tested which seem to be the most favoured by travellers and border guards.
- Enrolling eight or ten fingerprints is perceived to be substantially more time-consuming.

4 FPs	   	8 FPs	   	10 FPs	   
Success/quality	● ● ● ●	Success/quality	● ● ● ●	Success/quality	● ● ● N/A
Duration	● ● ● ●	Duration	● ● ● ●	Duration	● ● ● N/A
Technology	● ● ● ●	Technology	● ● ● ●	Technology	● ● ● N/A
Experience	● ● ● ●	Experience	● ● ● ●	Experience	● ● ● N/A

Key			
Success/quality	● ≥ 75 %	● ≥ 50 % - < 75 %	● < 50 %
Duration	● < 30 s	● ≥ 30 s - < 60 s	● ≥ 60 s
Technology	● Mature	● Medium maturity	● Low maturity
Experience	● ≥ 65 %	● ≥ 35 % - < 65 %	● < 35 %

6 Based on the conclusions outlined in the European Commission's 2014 Technical Study.

7 Technology is assessed as 'mature' if it is already widely available on the market and in working condition, and is not highly impacted by environmental conditions. Medium maturity means being available on the market but sensitive to environmental conditions. Immature means that the equipment available on the market is not fit for purpose, has shown too many deficiencies and/or is too heavily impacted by the environment and therefore cannot be deployed at this type of border.

Facial-image (FI) enrolment and verification

Table 2 Summary of locations per type of border where facial-image enrolment and verification were tested.

Enrolling live facial image (FI) (TC4): capturing FI from eMRTD (TC6), verifying FI captured from eMRTD against live facial image (TC7) – at 10 BCPs	
Air	Madrid (ES) • Charles de Gaulle (FR) • Arlanda (SE)
Sea	Helsinki (FI) • Piraeus (EL) • Cherbourg (FR) • Genoa (IT)
Land (road)	Vaalimaa (FI) • Sculeni (RO)
Land (train)	Iași (RO)
Outcome	the pilot confirms that enrolling a facial image, capturing the image from the eMRTD chip and performing the verification are technically feasible at all types of borders in terms of success rate, quality, duration and experience.

Main findings

Success/quality

- Live facial images can be acquired using a standard off-the-shelf (web) camera, which can produce a high image quality for verifying travellers' identity. Very high success rates can be obtained, with verification accuracy reaching 93 %.
- Facial image as the unique biometric identifier cannot be used for identification purposes with large-scale databases.

Duration⁽⁸⁾

- The duration of the process was generally deemed acceptable except at border crossings on moving trains, where acquiring a live image was affected by changing conditions due to the movement of the train. In general, chip-image capture never lasted more than 3.5 seconds on average at air, sea and road borders; live image capture took 5.5 seconds on average; and verification was always done in less than 1 second at all types of borders.

Technology⁽⁹⁾

- To ensure that the live facial image captured is of a high quality and to guarantee subsequent high verification success rates, backlighting and reduced lighting should be avoided.
- The technology needed is widely available on the market today.

Facial Image					Key
Success/quality					 ≥ 75 %  ≥ 50 % - < 75 %  < 50 %
Duration					 < 15 s  > 15 s - < 30 s  ≥ 30 s
Technology					 Mature  Medium maturity  Low maturity
Experience					 ≥ 65 %  ≥ 35 % - < 65 %  < 35 %

8 For comparison purposes, the thresholds set for assessing FI duration were adapted in order to reflect the difference in processes of enrolling FP and iris. Indeed, for FI the assessment was made on the whole facial image process (i.e. enrolment of biometrics, capture of chip and verification) which performed extremely fast.

9 Ibid.

- Capturing the image from the chip can be done using equipment which is already available at most borders.
- The camera must be user-friendly and suitable for local environmental conditions at the BCP.
- An auto-adjustable camera is an advantage as it ensures image quality by adapting to travellers' height and position.

Experience

- Taking a facial image is very common at borders where ABC gates are in use, which could explain the positive feedback left by travellers.
- Feedback from border guards and travellers was positive; automatic verification increased the border guards' confidence in the correctness of their decisions.

Iris enrolment

Table 3 Summary of locations per type of border where iris enrolment was tested.

Iris pattern enrolment (TC5) – 5 BCPs, at 2 of which the test was combined with FI	
Air	Lisbon (PT)
Sea	Cherbourg (FR)
Land (road)	Sculeni (RO) • Kipoi (EL)
Land (train)	Iași (RO)
Outcome	the pilot confirms the feasibility of using the iris as a biometric identifier within the context of a future EES system at all types of borders, and validates it as a possible complementary biometric identifier along with a facial image and/or fingerprints for registered travellers. Facial image and iris appeared to be a more effective combination than iris and fingerprints.

Main findings

Success/quality

- High success rates for enrolment were achieved at a set quality threshold.

Duration⁽¹⁰⁾




- Using fixed equipment for enrolment added only limited time, while the use of mobile equipment was more time-consuming. Indeed, at sea and road borders where fixed equipment was deployed, enrolment never took longer than 4 seconds on average. This duration increased by up to 20 seconds on average with mobile equipment.

Technology⁽¹¹⁾

- The technology required currently exists and is available in terms of both fixed and mobile solutions.
- Fixed devices are easy to use, and capturing irises at a distance (usually around 1 m) worked in under five seconds in 78% of cases.

¹⁰ For comparison purposes, thresholds set for assessing the duration of iris enrolment are the same as for fingerprints.

¹¹ Ibid.

Iris	   
Success/quality	● ● ● ●
Duration	● ● ● ●
Technology	● ● ● ●
Experience	● ● ● ●

Key			
Success/quality	● ≥ 75 %	● ≥ 50 % - < 75 %	● < 50 %
Duration	● < 30 s	● > 30 s - < 60 s	● ≥ 60 s
Technology	● Mature	● Medium maturity	● Low maturity
Experience	● ≥ 65 %	● ≥ 35 % - < 65 %	● < 35 %

- Enrolling an iris pattern in outdoor conditions or on moving trains is more problematic due to time and space constraints. It took about 26 seconds on average.
- Hot weather conditions and bright or dim light conditions impacted the functioning of the mobile equipment.
- Elderly people were reported to have difficulties in enrolling their irises, as well as people with almond-shaped eyes with epicanthic folds (majority of Asian travellers).
- Iris enrolment was assessed as being no more prone to spoofing than any other biometric identifier.

Experience

- Feedback from border guards and travellers was generally positive.
- Based on border guards' feedback, capturing irises seems to require fairly little training and instructions.

ABC gates



Table 4 Summary of locations per type of border where ABC exit of TCNs was tested.

ABC gates for exit checks for TCNs (TC9) – at 7 BCPs	
Air	Charles de Gaulle (FR) • Schiphol (NL) • Lisbon (PT) • Frankfurt (DE)
Sea	Helsinki (FI)
Land (road)	Narva (EE)
Land (train)	Gare du Nord (FR)
Outcome	the pilot confirms that using ABC gates at exit for TCNs and performing bearer verification on the basis of the facial image are technically feasible.

Main findings

Success/quality

- ABC gates performed as well for TCNs as they currently do for EU citizens.

ABC gates	   
Success/quality	● ● ● ●
Duration	● ● ● ●
Technology	● ● ● ●
Experience	● ● ● ●

Key			
Success/quality	● ≥ 75 %	● ≥ 50 % - < 75 %	● < 50 %
Duration	● Lower than baseline	● ≥ baseline - ≤ 125 % of baseline	● > 125 % of baseline
Technology	● Mature	● Medium maturity	● Low maturity
Experience	● ≥ 65 %	● ≥ 35 % - < 65 %	● < 35 %

Duration

- The time taken to cross the border was assessed as comparable with manual control times. Average durations for the whole process ranged from 14 to 41 seconds on average.
- Passive authentication took less than 6 seconds.

Technology⁽¹²⁾

- The main environmental constraint identified was lighting, which impacts live facial-image capture and subsequently verification.
- The technology is already in place and operational at several borders across the Schengen Area.
- While the BCP environment may need to be adapted in some cases, the two primary remedies (removing or adding light) can be implemented easily.
- In terms of security, authenticating the travel document automatically was seen as having a positive impact on border guards' confidence in the decisions they make at the border.

Experience

- In general, feedback from travellers was very positive.
- Border guards highlighted that ergonomics and a user-friendly, uniform interface are essential for ensuring traveller acceptance and usability.

Kiosk

Table 5 Feasibility assessment of kiosk per type of border where the use of kiosks was tested.





Use of self-service kiosks (TC10) – at 3 BCPs, pre-border checks at land borders (TC11) – at 1 BCP	
Air	Lisbon (PT) • Madrid (ES)
Sea	Helsinki (FI)
Land (road)	Sillamäe (EE)
Land (train)	N/A
Outcome	<p>the pilot confirms that using kiosks at entry for capturing data from travel documents (eMRTD) and enrolling/verifying four or eight FPs and FI are technically feasible in controlled environments.</p> <p>Land borders seem less suited to kiosk deployment at entry lanes due to constraints in available space (i.e. waiting area).</p> <p>However, the number of participants in the kiosk test case at land borders remained too low to draw meaningful conclusions. There was no kiosk test case at a train station or on a moving train.</p>

Main findings

Success/quality

- In general, kiosks are able to capture data from the travel document and enrol fingerprints at a similar quality to that achieved with manual booths.

¹² Ibid.

Kiosk	   
Success/quality	● ● ● N/A
Duration	● ● N/A N/A
Technology	● ● ● N/A
Experience	● ● ● N/A

Key			
Success/quality	● > 70 % completion of the process without errors	● ≥ 50 % - < 75 % completion	● < 50 % completion
Duration	● +/- 20 % difference with manual booth	● 20-50 % difference	● > 50 % difference
Technology	● Adapted and working	● Some constraints	● Not adapted
Experience	● ≥ 65 %	● ≥ 35 % - < 65 %	● < 35 %

Duration

- Less time is spent at the manual booth when tasks are performed at the kiosk, i.e. there was a reduction of up to 35 seconds (including capturing four fingerprints).

Technology⁽¹³⁾

- Unfavourable light conditions can impact the quality of the live facial-image capture.
- The technology needed to assemble a kiosk exists today. Some further refinement in terms of their user interface would be an improvement.
- The impact of extreme weather conditions could not be assessed, since kiosks were always installed in indoor environments.
- Human supervision is required to strengthen security, primarily to prevent unauthorised persons being enrolled.
- Automatic height adjustment resulted in good facial-image verification (often superior to manual booths).

Experience

- Feedback from travellers and border guards was generally positive.
- According to border guards, travellers almost always need guidance, when using these systems for the first time.
- A human interface and ergonomics are essential for guaranteeing traveller acceptance and usability.

13 Ibid.

Key findings from desk research

In addition to operational testing, desk research was conducted to address some further issues covered by the Terms of Reference of this pilot, in particular:

- potential fall-back scenarios in the event that the EES is unavailable or unreachable, and describing related procedures, architecture and consequences;
- VIS border checks while using the travel document number (instead of the visa-sticker number);
- web services for travellers and carriers; and
- equipment costs.

The table below summarises the key findings for each of the four topics.

Desk-research topic	Key findings (the following measures should be considered)
Fall-back scenario	<ul style="list-style-type: none"> • High-level availability (similar to the level of SIS II, i.e. 99.99 % per month) should be developed at central level. • Member States should aim to achieve the same high level of availability. • If the EES is temporarily unavailable, solutions for local electronic buffering and later synchronisation with the central system should be developed and implemented. • Manual (correction) procedures should be developed in case an entry or exit record is missing from the EES.
VIS border check using travel document number	<ul style="list-style-type: none"> • Searching the VIS by using the passport document number simplifies the border-control process and makes it easier for visa holders to use automated solutions (i.e. self-service kiosks and ABC gates). • Several options for consulting VIS based on the travel document number (instead of the visa sticker number) were assessed and considered feasible from a technical perspective. The technically preferred option is to use the alphanumeric search engine.
Web service for travellers and carriers	<ul style="list-style-type: none"> • For travellers to be able to consult the system, the proposed option would be to use data from the passport and provide a simple but discrete OK/NOK answer. • A credential-based system is proposed for carriers, whereby using travellers' passport data as an input, a simple OK/NOK answer is provided if a single day of stay remains. The option to introduce a proof-of-check mechanism was also assessed in order for the carriers to confirm that they performed the check.
Equipment costs	<ul style="list-style-type: none"> • The estimated average acquisition prices⁽¹⁴⁾ for biometric devices have been provided in the report. However, the final costs will depend on the choice of biometric identifiers made.

¹⁴ Installation and maintenance costs have not been included in the analysis.

Survey conducted by the FRA – key findings

There are a number of fundamental-rights implications related to the use of identification and verification technology in the context of border control. A small-scale survey conducted by the FRA looked into third-country-national travellers' attitudes and opinions regarding the use of biometrics at BCPs and various associated fundamental-rights aspects (e.g. the right to dignity, the right to respect for private and family life and the right to protection of personal data). Travellers' perception is believed to be an arguably subjective yet highly relevant element that needs to be taken into account when assessing the compliance of certain measures with fundamental rights (in addition to legal analysis).

The results show that the majority of respondents do not perceive that the use of biometrics at borders might compromise their right to dignity. There is also a tendency not to perceive the provision of fingerprints and facial image at borders as compromising the right to privacy. This is however not the case for iris-scan, which is considered the most intrusive option.

However, travellers expressed concerns with regard to the reliability of the system in the future. The majority of respondents believed that they would not be able to cross the border if the system malfunctioned. Similar concerns emerged in relation to the right to rectify the data, whereby half of the respondents believed that if there was a mistake in the data, it would be difficult to correct.

Conclusion

The pilot confirms the feasibility (in terms of accuracy, effectiveness and impact) of deploying biometric identifiers at Schengen external borders. Depending on the choice of biometric identifiers, the use of biometrics adds relatively little duration to the border-crossing process. Desk research proves that this time can be saved if some processes are better streamlined (e.g. by searching the VIS using the passport number).

The deployment of accelerators such as ABC gates and kiosks could further decrease border-crossing times. It was observed that the technology set-up and integration, as well travellers' interaction with it, influences the results much more than the type of border.

In addition, border guards felt that training was needed to prepare them for new equipment and processes. These key observations and considerations should now be put together and analysed further in developing successful combinations of biometrics for the future of Schengen borders.

The final report of the pilot was submitted to the European Commission as planned. The results of the pilot are representative and conclusive given the broad support provided by the Member States for the pilot, the number of the executed test cases for all types of borders and the amount of statistical evidences collected. The results of this unique project, conducted over a year, will contribute to the work on the modified legal proposal for Smart Borders.



Publications Office

ISBN 978-92-95208-00-1
doi:10.2857/598631
Catalogue n°: EL-04-15-806-EN-N

1. Fundamental Rights Agency Survey results

FRA survey in the framework of the eu-LISA pilot on smart borders – travellers' views on and experiences of smart borders

Main findings

This Annex presents the views of travellers on a number of fundamental rights aspects related to the use of biometrics in the context of border control. The results are based on a small-scale survey conducted with 1,234 randomly selected third-country nationals. The interviews for the survey were conducted between July and October 2015 at seven different border crossing points among those selected for the Smart Borders Pilot entrusted to eu-LISA by the European Commission.

The results show that most respondents are comfortable with providing biometrics when crossing borders, with the exception of iris-scan. Most respondents do not feel that biometrics compromises their right to dignity. Except for iris-scan, there is a tendency among respondents to perceive biometric data provision as not being intrusive on their privacy. Trust in the reliability of biometric technologies is also high; however, up to one third of the respondents were less positive.

A key result is what happens when something goes wrong and the system does not function as expected. Here, more than half of the respondents believe that they would not be able or do not know if they will be able to cross the border in case the technology does not work properly. Similar concerns emerged in relation to the right to correct wrong data. Half of the respondents believe that in case of an error in their personal data, the latter could not be easily corrected.

This finding resonates with the concerns expressed by the European Data Protection Supervisor (EDPS) and other organisations on the negative consequences that mistakes in the system and in the automated processing of personal data can have on an individual. For example, when the system fails to recognize an individual or if the extension of a visa is not included in the database, a person might be denied entry into an EU Member State or, in the worst case, run the risk of being apprehended and detained. The person affected may face difficulties to prove that he/she really is the person he/she claims to be. In the case of third-country nationals travelling to the EU, this vulnerability might be compounded by language problems.

Many problems could occur, for example data errors, but also fraud and forgery of biometric data and incorrect or not up to date personal data included in the IT system. The most likely implication of incorrect data in the Entry Exit system concern the risks of persons mistakenly flagged as over-stayers and the use that police, immigration or other officials may make of such information.

The results of the survey show that third-country national travellers take data protection seriously and more than 80% consider it important to be informed on the purpose of collecting and processing their personal data.

There is a widely held view that automated systems could cause less discrimination – for example on the basis of race or ethnicity – compared to checks carried out in person by border guards. This might be based on the assumption that machines entail a lower risk of discriminatory profiling compared to checks by border guards. However, it should be noted that automated systems could be programmed to identify individuals using sensitive data, such as race, ethnicity or health. Measures to avoid discriminatory profiling are, therefore, required.

Most respondents believe that only adults (i.e. 18 years of age onwards) should be allowed to go through biometric checks. Hence, there is a difference between the views of the respondents and the current age limits for fingerprinting set in the EES proposal, according to which fingerprints should be provided from 12 years onwards.

Finally, respondents were asked whether they are afraid that the technology to collect their biometrics might be harmful to their health. The survey result show that more than half of the respondents either believe that biometric technologies could harm their health or show uncertainty on this issue. Travellers would benefit from receiving objective and scientific information on the health consequences of the use of biometric data.

1.1. Background

In the context of the Smart Borders second phase of the 'Proof of Concept' also referred as "Pilot" which was entrusted to eu-LISA by the European Commission, the European Union Agency for Fundamental Rights (FRA) complemented eu-LISA's tests by conducting a survey of travellers on fundamental rights-related issues linked to the use of biometrics during border checks.

Biometric identifiers can be biological properties, physiological characteristics, living traits or repeatable actions that are both unique to that individual and are measurable¹ such as fingerprints, iris-scan (referred to 'iris pattern' in the report) and facial image.

Modern identification and verification technologies entail both risks and benefits for fundamental rights that have not yet been fully explored. In the context of the Smart Borders proposal, the European Data Protection Supervisor, the Article 29 Working Party and representatives of civil society have expressed concerns over the necessity and proportionality of the Commission proposal to create a new large-scale centralised system for processing fingerprints and personal information of third-country nationals crossing the Schengen borders.

¹ Article 29 Working Party (2012), [Opinion on biometrics](#), WP 193, Brussels, 27 April 2012.

Data protection and privacy related issues have so far been at the forefront of discussion in this field. Other fundamental rights, such as the right to dignity and non-discrimination, may also be at stake. In parallel to FRA's survey in the context of the eu-LISA Pilot on Smart Borders, FRA is currently conducting a project on "Biometric data in large EU IT-systems in the areas of borders, visa and asylum – fundamental rights implications". The project will identify the positive as well as negative fundamental rights implications of processing biometric data in the following already existing large-scale IT-systems: Eurodac², the Schengen Information System (SIS II)³ and the Visa Information System (VIS).⁴

The objective of FRA's small-scale survey is to explore third-country national travellers' attitudes about the use of biometrics at border crossing points (BCPs) in relation to selected fundamental rights issues. The results intend to provide information to policy makers about the attitudes they can expect to encounter from travellers when introducing Smart Borders technologies.

Travellers' attitudes are an important element when assessing how new measures will be received. They can help authorities to forecast possible reactions and address existing fears or concerns. At the same time, travellers' perceptions are only one element to take into account when assessing fundamental rights compliance of certain measures. Violations of fundamental rights may occur regardless of whether the individual consents or not to a certain treatment, particularly in light of limited rights awareness.

1.2. Methodology and sample

1.2.1. Scope

The survey was conducted in seven border crossing points in six Schengen Member States, all covered by the eu-LISA Pilot and aimed at interviewing a similar number of travellers in each BCP. The seven BCPs were selected to cover a variety of different types of borders (road, train, seaports and airports) and to allow for a balanced geographical distribution between Member States and travellers. As illustrated in Figure 1 interviews were conducted in the following BCPs:

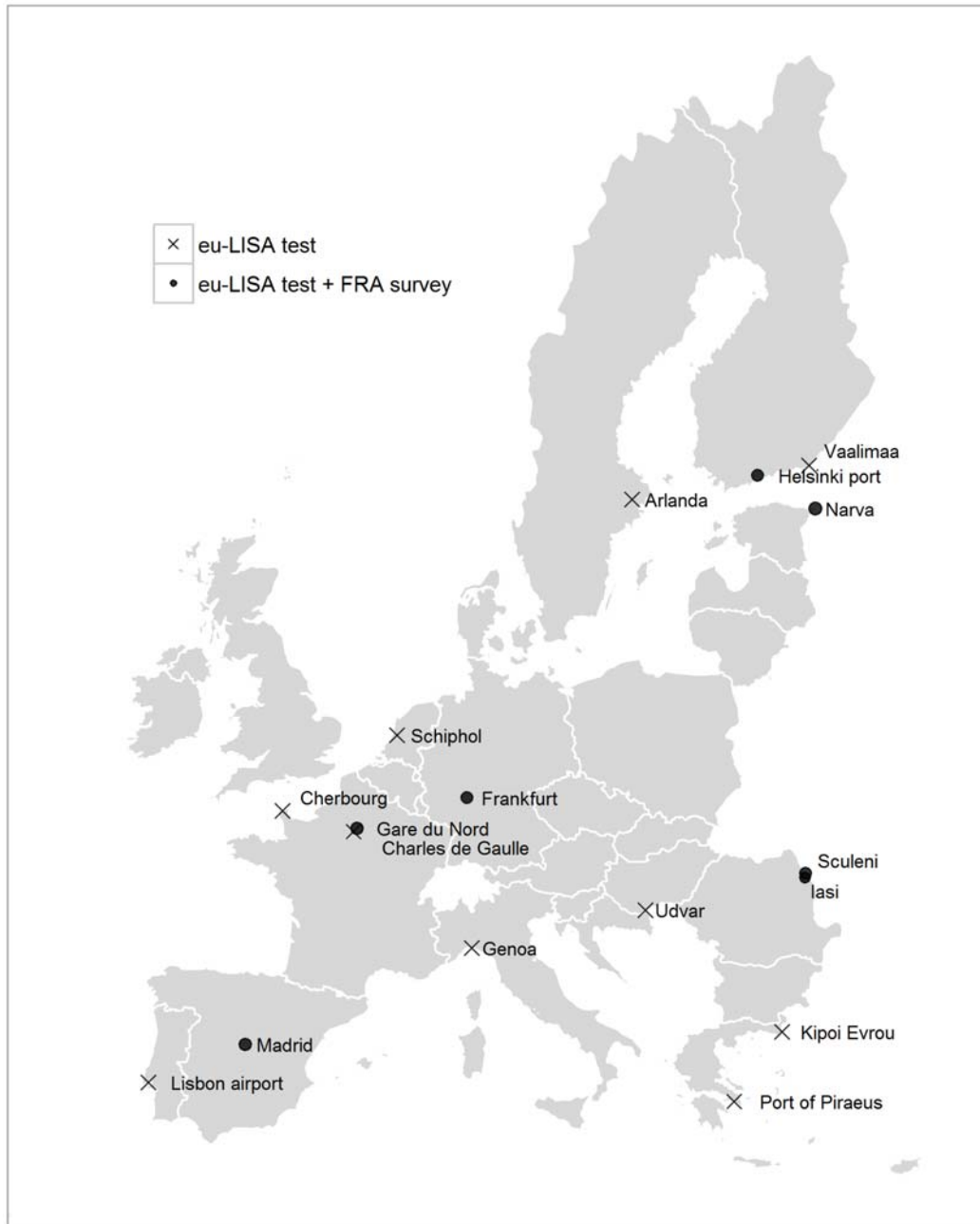
- three airports: Charles de Gaulle (Paris), Frankfurt (Germany) and Madrid (Spain)
- one harbour: Helsinki (Finland)
- three land border crossing points: the road BCP in Sculeni (Romania); the road BCP in Narva (Estonia) and the train BCP in Iași (Romania)

² European Commission, Identification of asylum applicants, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/identification-of-applicants/index_en.htm

³ European Commission, Schengen information system, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm

⁴ European Commission, Visa information system, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm

Figure 1: Overview of border crossing points covered by the FRA survey within the eu-LISA Pilot on smart borders⁵



1.2.2. Target group

The target group included non –EU citizens (i.e. third-country nationals and stateless persons) crossing an external border of the Schengen Area.⁶ This was the same target group of the eu-LISA Pilot, except for Narva, where the eu-LISA pilot targeted only people holding an alien’s passport issued by Estonia (stateless persons residing permanently in Estonia). As few people belonging to this group were travelling in Narva when the survey was conducted, it was decided to include all third-country nationals, in line with the eligible population of the other BCPs surveyed. All respondents were aged 18 years or older.

⁵ The background of the maps presented in Figure 1 and Figure 2 are based on shapefiles made available through Eurostat, © EuroGeographics for the administrative boundaries, available at: <http://ec.europa.eu/eurostat/web/gisco/geodata/reference-data/administrative-units-statistical-units>.

⁶ Citizens of a country that is a member of the European Free Trade Association (EFTA) have not been included in the sample.

1.2.3. Sample selection

The sampling approach aimed to deliver a representative sample of the target group in the BCPs covered. The following strategies were followed to randomly select travellers, screen for their eligibility and conduct the interview at airports, ports and land BCPs, respectively.

At airports interviews were conducted at the departure area, at boarding gates of flights travelling outside the EU. Boarding gates were considered the best place to approach respondents because travellers reach boarding gates some 30-60 minutes before flight departure and, having completed all departure procedures, have time and are more likely to be willing to take part in the survey.

A two stage sampling was carried out at gates. Boarding gates with departing flights to destinations outside the EU were selected randomly. At each gate, passengers were approached through systematic sampling, with every third traveller selected. No more than 30 persons were interviewed at each gate in order to guarantee heterogeneity of the sample in terms of destinations and nationality of travellers.

Only at Frankfurt airport, where access to boarding gates was not possible due to the airport's security measures, interviews were conducted at the check-in area and in the waiting hall prior to security. Travellers checking in for flights departing to destinations outside the EU were selected and approached in a systematic way (i.e. every third traveller resting in sitting areas next to check-in counters) and only eligible travellers were interviewed.

The fieldwork took place at Madrid airport between 14 and 16 July 2015; at Paris airport between 7 and 9 August 2015 and at Frankfurt airport between 25 and 27 August 2015 and from 21 to 22 October 2015.

At Helsinki sea port (Finland), interviews were conducted with people travelling on ferries arriving from or travelling to St. Petersburg (Russia) between 18 and 20 July 2015. Two ferries a day were surveyed (disembarking in the morning, boarding in the afternoon). Travellers arriving were approached in the waiting area, just before border check procedures and on the ferry itself. Travellers departing were approached after border check procedures. As in airports, every third traveller was selected.

At land borders the sampling units included pedestrians, cars and buses, as relevant. Systematic sampling was applied by selecting every third pedestrian and every third car. Within each car, one person was selected, unless there were four or five people travelling in the car, in which case two questionnaires could be completed for the same vehicle (provided the selected persons were eligible). All buses were approached and every third person within each bus was selected.

Interviews were conducted in different areas. In Narva (Estonia), the sampling units included pedestrians, buses and cars. Cars were selected in two different locations: close to the BCP, where cars are queueing for border checks and in the car waiting area 3 km away from the BCP. Interviews with people travelling by bus were conducted in a special waiting area for bus passengers while the bus was being inspected by customs officers. Pedestrians entering as well as leaving the Schengen Area were approached and interviewed. Border guards advised the interviewers not to approach trucks due to low flows and because the average waiting time for trucks at the waiting area was too short to complete the questionnaire.

In Sculeni (Romania), the sampling units were cars, which were systematically selected in the same way as in Narva. Pedestrians were very few; trucks were also very few and difficult to approach.

In Iași (Romania), interviews were conducted on trains connecting Romania and Moldova in both directions, including local trains connecting Iași-Ungheni (in both directions) and trains connecting Chisinau and Bucharest.

The fieldwork was conducted in Narva between 11 and 13 August 2015 and in Iași and Sculeni between 20 and 24 August 2015.

1.2.4. Questionnaire

The questionnaire was designed by FRA and covers attitudes towards potential fundamental rights issues related to collecting, storing and processing biometric data in the context of border crossing. Besides the general attitudes towards the provision of biometric data for border crossing, the questions reflect issues related to the following Articles of the Charter of Fundamental Rights of the European Union:

- Dignity (Article 1): interviewees were asked whether they thought it was humiliating to give their biometrics, have their passport checked by a border guard (with no biometrics involved) or any kind of border check in general
- Respect for private and family life (Article 7): interviewees were asked if they believe that giving their biometrics when crossing the border is intrusive or not to their privacy
- Right to protection of personal data (Article 8), including
 - the right to information on the purpose for collecting the data and on its processing: interviewees were asked whether they believe it is important to be informed on why their biometric identifiers are collected and used;
 - the right to access and rectify the data: interviewees were asked whether they believe that their personal data could be easily corrected in case of mistakes; interviewees were also asked if they trust that only legally authorised people access the data and if they have problems with the police accessing their data.
- Non-discrimination (Article 21): interviewees were asked whether they believed that automated systems would cause more or less discrimination compared to checks done by border guards.

Additional questions on previous experience with providing biometrics and information on general attitudes to technology were asked to help contextualise and interpret the results.

Comments on the questionnaire were provided by eu-LISA.

The English questionnaire was translated into seven languages, including four languages of EU Member States where the survey was conducted (Spanish, French, Romanian and German) plus a selection of languages widely spoken by third-country nationals travelling through the BCPs surveyed (Russian, Chinese and Arabic).

Fieldwork

The fieldwork was carried out by Eticas Research & Consulting from July 14 2015 until 22 October 2015. A team of four interviewers was deployed to carry out the fieldwork. In addition to English, each interviewer was fluent in at least two languages among the following: Spanish, French, Chinese, Russian and Arabic. The interviewers were trained prior to fieldwork in a one day training attended by FRA and eu-LISA.

Interviews were conducted with interviewees completing the questionnaire themselves, using both tablet devices and on paper. Interviews were self-administered. Interviewers were always available for questions and clarifications.

1.2.5. Descriptive statistics of the sample

In total 1,234 interviews were conducted⁷ ranging from 72 at Iași BCP up to 249 in Frankfurt, with an average of 176 interviews per BCP. In all BCPs, but one, at least 150 interviews were carried out. In Iași only 72 were conducted due to the small number of eligible respondents at the time of the survey.⁸

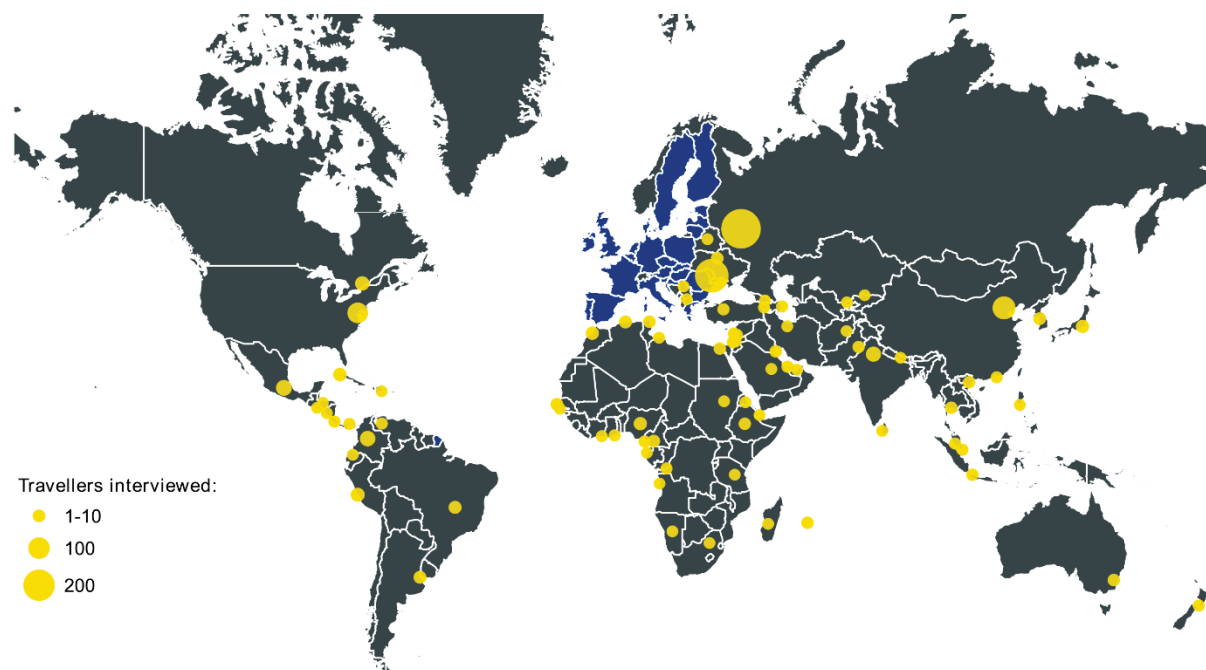
The respondents are citizens from over 80 different countries. The distribution of countries of citizenship of respondents is shown in Figure 2. The majority of respondents are citizens of a European country⁹ (42.1 % of

⁷ Initially a minimum of 150 interviews per BCP was planned. This requirement could not be reached due to lower traffic and very low response rates at the BCP in Iași, where only 72 interviews were conducted. In order to reach a bigger overall sample, an additional fieldwork phase was carried out at Frankfurt airport.

⁸ Most of the travellers on the trains surveyed were either Moldovan residents with double nationality, Moldovan and Romanian (and thus non-eligible) or did not want to take part to the survey.

the sample), followed by Asia (22.9 percent), Latin America or the Caribbean (13.2 percent), Africa (9.8 percent), Northern America (9.6 percent) and Oceania (0.9 percent). 1.5 percent of respondents were either 'stateless' persons in Estonia or the exact citizenship could not be established. Most respondents were Russian citizens (282 respondents or 22.9% of the sample) followed by Moldovans (223 or 18.1%), Chinese (114 or 9.2%) and US citizens (91 or 7.4%).

Figure 2: Distribution of countries of citizenship of respondents in the survey¹⁰, average of the seven BCPs surveyed



Source: FRA survey on smart borders, 2015

The citizenship of travellers differs across BCPs. Table 1 provides an overview of the citizenship of travellers interviewed per BCP. In Sculeni and Iași almost all travellers were Moldovan citizens and in Narva almost all were Russian citizens. Travellers in Helsinki, arriving by ferry, were mainly Russians and Chinese. In Frankfurt airport 51.8 percent of the sample were citizens from an Asian country (mainly China and India). In Madrid airport the majority of respondents originated from Latin America and the Caribbean (most travellers from Mexico, Colombia, Cuba and Peru, but also from other countries). At Charles de Gaulle the majority came from Asia (36.2%), but also from Africa (26.0%) and Northern America (22,4%).

Table 1: Percentage distribution of region of citizenship of respondents per border crossing point¹¹

BCP	Charles de Gaulle	Frankfurt	Helsinki	Iași	Madrid	Narva	Sculeni
Africa	26.0	13.7	0.0	0.0	18.8	0.0	0.0
Asia	36.2	51.8	37.7	2.8	9.9	0.5	0.0
Europe*	3.1	2.8	53.7	91.7	7.3	88.1	100.0

⁹ 'Europe' does not include citizens of any EU or EFTA country. Russia is counted as a European country according to the regional composition defined by the United Nations.

¹⁰ Background of the map is based on shapefiles made available through Eurostat, © EuroGeographics for the administrative boundaries, available at: <http://ec.europa.eu/eurostat/web/gisco/geodata/reference-data/administrative-units-statistical-units>.

¹¹ The allocation of countries to regions is based on composition by the United Nations, available here: <http://unstats.un.org/unsd/methods/m49/m49regin.htm> (last revision: October 2013).

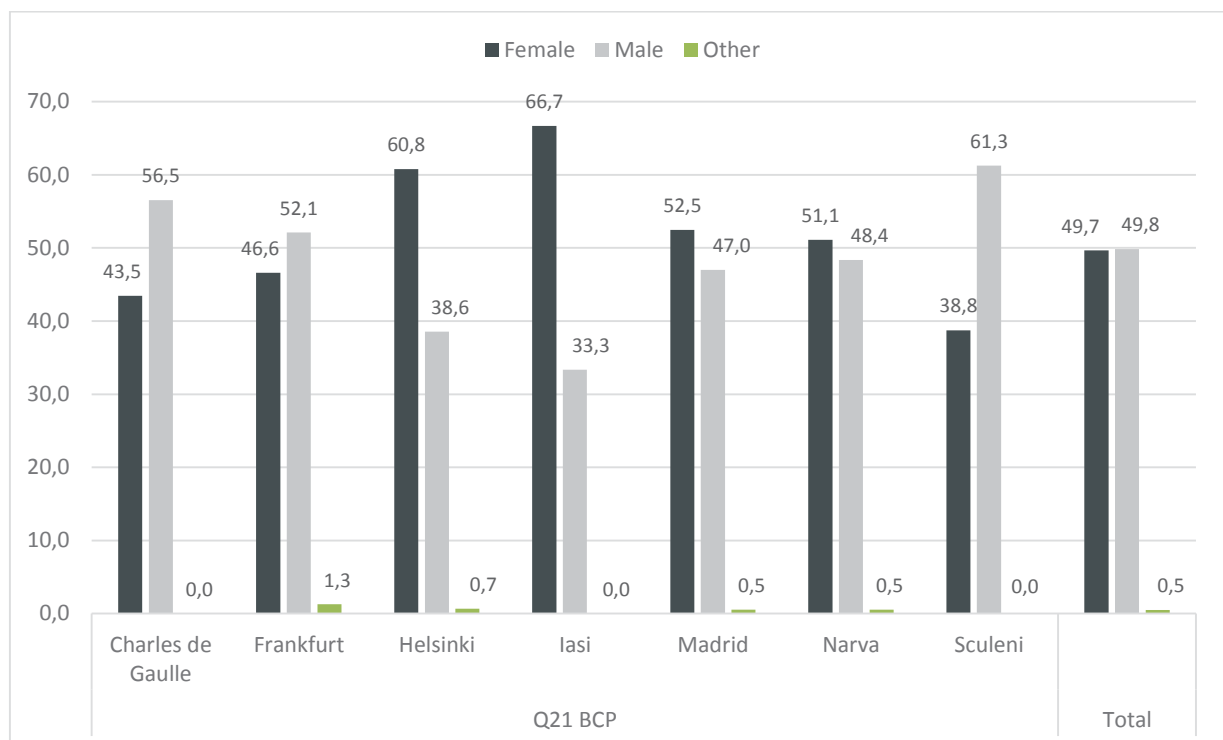
Latin America and the Caribbean	11.7	17.7	4.3	0.0	45.3	1.0	0.0
Northern America	22.4	12.9	1.9	2.8	16.7	2.5	0.0
Oceania	0.0	0.8	2.5	2.8	1.6	0.0	0.0
Unknown or stateless**	0.5	0.4	0.0	0.0	0.5	7.9	0.0
Total	100	100	100	100	100	100	100

* 'Europe' does not include citizens of any EU or EFTA country. Russia is counted as a European country according to the regional composition defined by the United Nations. ** Respondents who declared that they were third-country nationals, but exact citizenship could not be established, and stateless persons.

Source: FRA survey on smart borders, 2015

The gender distribution of the sample is balanced with 47.2 percent women and 47.4 percent men. Six respondents (0.5%) chose 'other' gender and for the remaining 4.9 percent the information could not be collected (because the respondent did not fill in the field). For 4.1 percent of the sample the gender of the respondent was guessed by the interviewer. At the BCP for Charles de Gaulle, Frankfurt and Sculeni more men were interviewed and at Helsinki and Iași considerably more women were interviewed.

Figure 3: Gender distribution across BCPs in the sample (%)

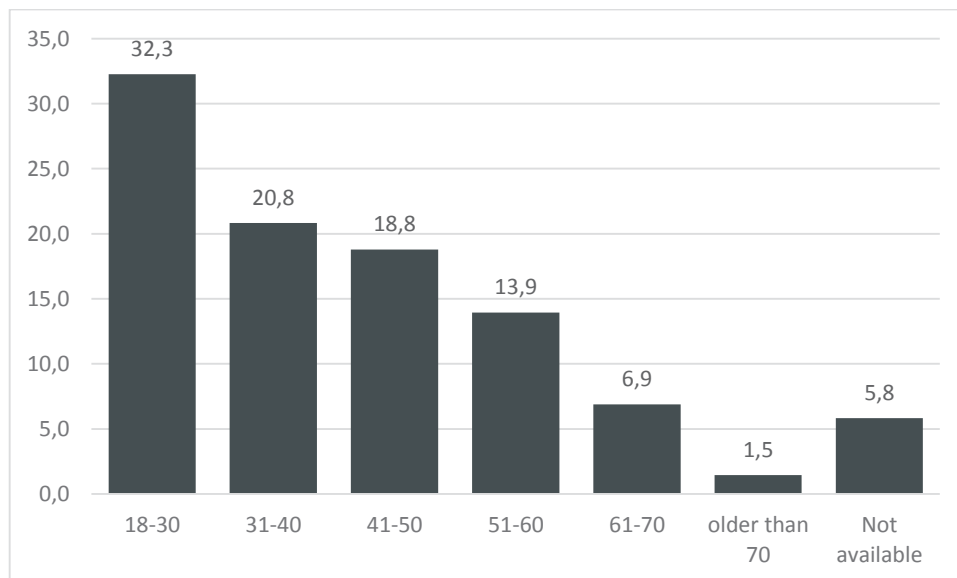


Note: cases with missing information excluded. Category 'other' not included in the graph. N = 1,174

Source: FRA survey on smart borders, 2015

The sample consists of more 'younger' persons. 32.3 percent of the sample are aged between 18 and 30. 20.8 and 18.8 percent of the sample belong to the age groups 31 to 40 and 41 to 50, respectively. 13.9 percent were between 51 and 60 years of age and 8.4 percent were older than 60.

Figure 4: Age distribution in the sample, average of the seven BCPs surveyed (%)



Source: FRA survey on smart borders, 2015

1.3. Results

1.3.1. Acceptability of technology

Acceptability of technology refers to the general agreement by the public with the use of biological characteristics for biometric systems.¹²

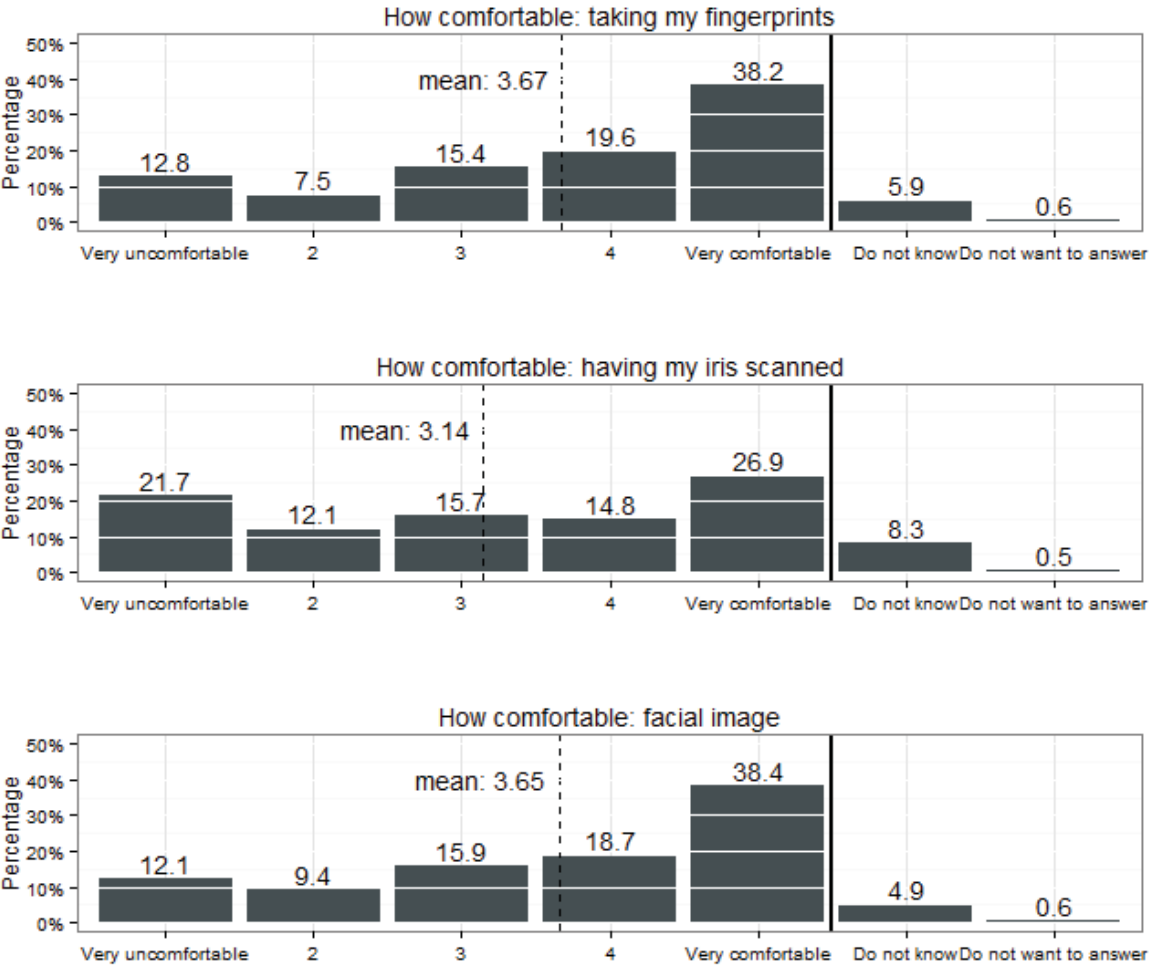
Respondents were asked whether they feel comfortable with the use of the following biometric identifiers when crossing the border: fingerprints, iris-scan and facial image. Generally, third-country nationals travelling to the EU tend to feel comfortable with providing biometric data when crossing the border. For all three types of biometric identifiers (fingerprints, iris-scan and facial image) most respondents feel very comfortable. However, there are important differences: people feel more comfortable with providing fingerprints or facial image when crossing the border compared to having their iris scanned, a tendency which remains true across all BCPs, across all regions of citizenship of travellers, gender and age groups.¹³ Figure 5 presents an overview of how comfortable respondents are with the provision each of the three biometric identifiers when crossing the border.

Approximately 1 in 10 travellers feels very uncomfortable with providing fingerprints or facial image (12.8 and 12.1 percent) when crossing the border, while 38.2 and 38.4 percent respectively feel 'very comfortable'. The percentage of travellers feeling very uncomfortable is considerably higher for iris-scan: 21.7 percent chose this answer. With 26.9 percent there is also a lower percentage of travellers feeling very comfortable with having their iris scanned when crossing the border.

¹² E. Kindt (2013), *Privacy and Data Protection Issues of Biometric Applications*, p.33.

¹³ Further analysis per BCPs, per region of citizenship of travellers, gender and age groups is not reported and can be made available, upon request.

Figure 5: How comfortable are travellers with providing biometrics (fingerprints, iris-scan and facial image, respectively) when crossing the border, average of the seven BCPs surveyed (%) The dashed vertical line gives the average/mean of the values chosen on the 1-5 scale.

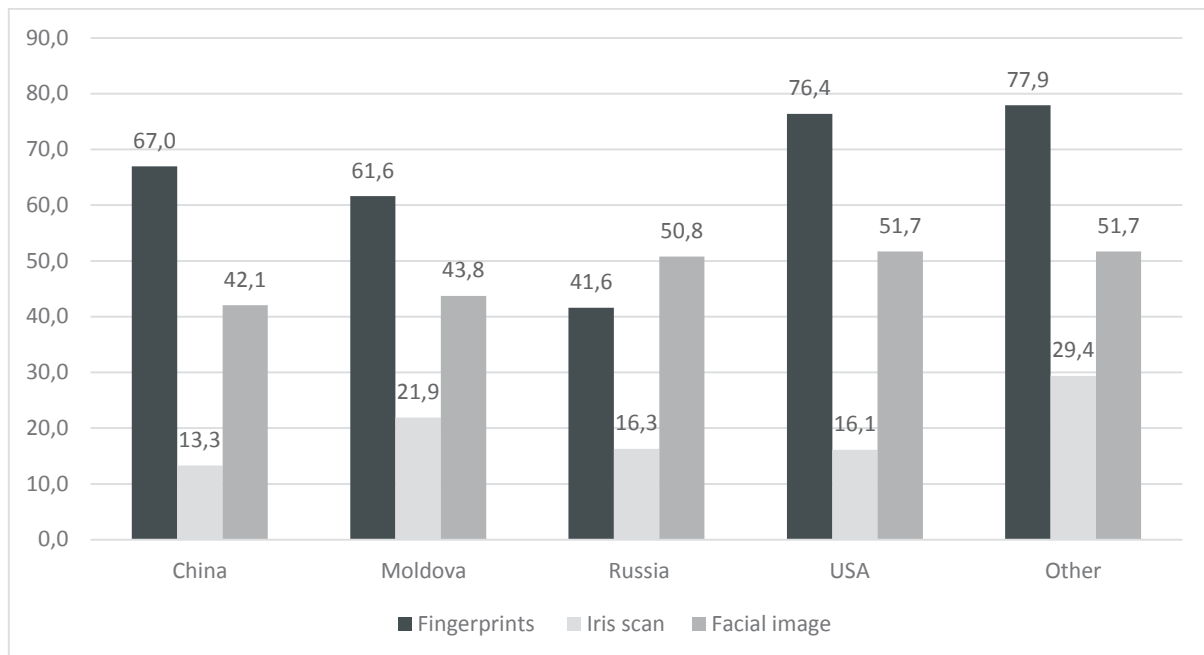


Source: FRA survey on smart borders, 2015. Question: How comfortable are you with the use of the following biometric identifiers when crossing the border? Fingerprints, iris-scan, facial image. N: 1,233, 1,228 and 1,227, respectively.

Having previously provided biometrics has an influence on how comfortable people are with this technology being used in the context of border control.¹⁴ 65.5 percent of respondents have provided their fingerprints previously. Compared to fingerprints, fewer travellers had a previous experience of iris-scan (22.5 percent) or facial image (50.4 percent). Figure 6 presents respondents' previous experience with providing biometric details by citizenship of respondents (four main countries of citizenship considered). Wider differences among respondents of different nationality can be observed in relation to past experience with provision of fingerprints, compared to iris-scan and facial image. As an illustration, 76 percent of US citizens had previously provided their fingerprints compared to only 42 percent of Russians. However, a similar share of US citizens and Russians have let their iris be scanned and provided their facial image.

¹⁴ According to the VIS regulation, visa applicants are under the obligation to provide fingerprints when applying for a visa at consulates and embassies of EU Member States.

Figure 6. Past experience with providing biometric details by citizenship, average of the seven BCPs surveyed (in %)



Source: FRA survey on smart borders, 2015. Question: have you ever given your biometric details in the past? Fingerprints, iris-scan, facial image. N = 1,148, 1,101 and 1,113, respectively.

For each of the three biometric identifiers, previous experience leads to higher acceptability. As an illustration, while 40.7 percent of travellers who had given their fingerprints in the past feel very comfortable, only 33.9 percent of travellers without any experiences feel very comfortable.

In addition, persons who tend to be more in favour of the use of new technologies in general, also feel more comfortable with providing their biometrics when crossing the border. Most travellers interviewed indicated to be in favour of new technologies in general. On a five-point scale, where 1 means 'in favour of new technologies' and 5 'against new technologies', 42.4 percent selected the value 1 and 19.5 percent the value 2. Only 5.5 percent selected the value 5, meaning that only a small group of travellers is against new technologies.

Looking at fingerprints specifically, how comfortable people feel with this biometric identifier when crossing the border depends on several factors. The difference can be explained to some extent by the citizenship and gender of travellers. Russian citizens feel on average slightly more comfortable than other nationalities with providing fingerprints when crossing the border (average value of 3.9 compared to the overall average of 3.7). Comparing the mean score by gender, we find that women feel slightly more comfortable than men. Persons aged 51 or older tend to select more often that they feel very comfortable with providing fingerprints. However, no clear patterns were found with respect to age of respondents and how comfortable they feel with the provision of fingerprints when crossing the border.

Table 3 summarises the results of a logistic regression analysis that estimates the influence of each of several factors on the likelihood of travellers feeling comfortable with the provision of fingerprints when crossing the border (feeling comfortable means having selected either 4 or 5 on the 5-point-scale, where 1 means very uncomfortable). The estimates in the tables provide an estimate to what extent the likelihood changes. Although the estimates cannot be directly interpreted³⁵, as a general rule, a positive estimate means that this factor increases the likelihood of feeling comfortable and a negative estimate decreases the likelihood. The

³⁵ In a logistic regression model the likelihood needs to be transformed for an efficient estimation.

results confirm some of the above reported differences in a multivariate context. Having provided fingerprints previously increases the likelihood of feeling comfortable with the provision of fingerprints in the context of border control, even when controlling for other factors such as citizenship, gender, age and views on technologies. Compared to the group of Russian citizens, all other groups of citizens are less likely to feel comfortable with providing fingerprints, holding other factors constant. This lower likelihood is not statistically significant for the group of US citizens and has a very low level of significance for Chinese and 'other' citizens (as compared to Russians). Being less in favour of new technologies decreases the likelihood of feeling comfortable with fingerprints considerably. The results show that for a Russian male citizen aged 18 to 30, who has already given fingerprints and is in favour of new technologies, there is an estimated likelihood of 78 percent that he feels comfortable with giving fingerprints when crossing the border. For a person with the same characteristics but who has never given fingerprints, the estimated likelihood decreases to 70 percent. If the latter person would be against the use of new technologies, the estimated likelihood decreases to 31 percent.

Table 3: Logistic regression on the likelihood of reporting that the person feels comfortable with the provision of fingerprints when crossing the border (i.e. has selected either 4 or 5 on the five points scale compared to all other results)

		Estimate (standard error)
Intercept (result when all variables take the value 0)		1.24 (0.25)***
Experience with fingerprints		0.42 (0.16)**
Citizenship	Russia	Reference
	China	-0.54 (0.28)*
	Moldova	-0.61 (0.22)**
	Other	-0.46 (0.19)*
	USA	-0.41 (0.28)
Gender	Man	Reference
	Woman	0.22 (0.14)
Age	18-30	Reference
	31-40	-0.20 (0.18)
	41-50	0.05 (0.19)
	51 or older	0.19 (0.18)
In favour of or against new technologies (measured on a five-point scale 1 = in favour and 5 = against new technologies)		-0.41 (0.06)***

Source: FRA survey on smart borders, 2015. Notes: Number of observations = 1,004. Significance levels: *** < 0.001, ** < 0.01, * < 0.05. A logistic regression model estimates the influence of a number of independent variables on the likelihood of an event occurring. For this the likelihood of the event is transformed to create a linear relationship (into the 'logit'). The 'estimates' provide the average value by which the dependent variable changes if the independent variable changes by 1. Since the dependent variable is transformed into the logit, the estimates are not straightforwardly interpreted. Generally, the detailed influence on the likelihoods can be determined, when transforming the estimated coefficients, which has been done in the text for some

examples. A statistically significant positive value of the estimates means that the observed group has a higher likelihood compared to the reference group. A negative value of the estimates indicates a lower likelihood.

In sum, there is the tendency to feel comfortable with providing biometrics when crossing the border among third-country nationals travelling at the selected BCPs. This tendency is lower for iris-scan and this remains true across all BCPs, across all regions of citizenship of travellers, gender and age groups.

1.3.2. Private (and family) life

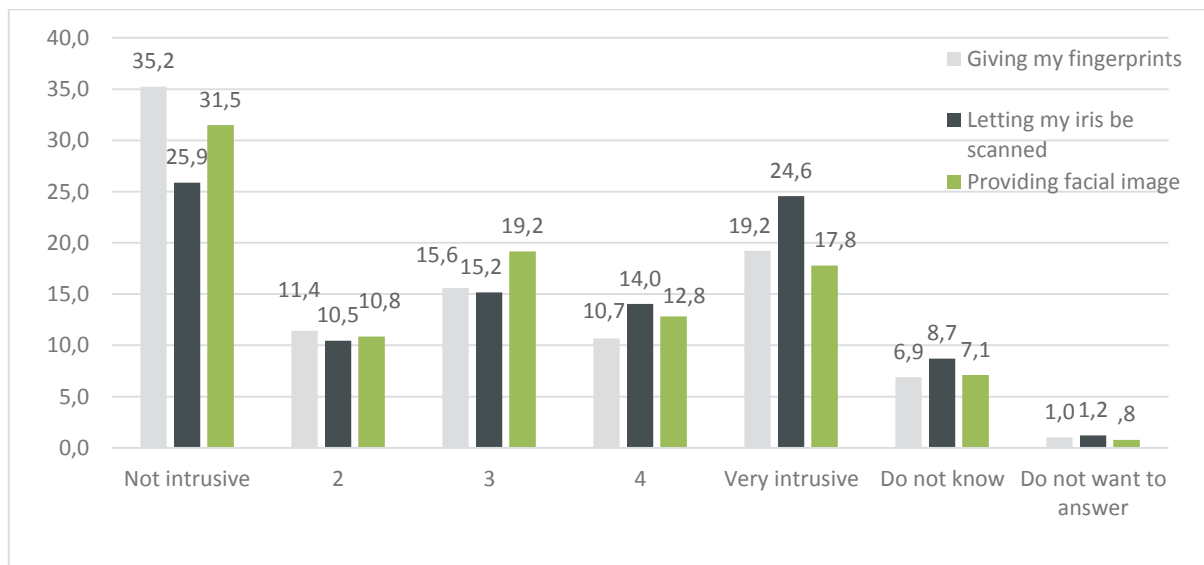
Case law by the European Court of Human Rights (ECtHR) and the Court of Justice of the EU (CJEU) recalls that the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 of the European Convention on Human Rights (ECHR).¹⁶ The routine storage of data on individuals relating to their entry to and exit from the territory of European Union Member States may affect directly the traveller and indirectly the family. For example, family life could be affected in the context of family reunification process where a member of the family is refused entry because of a previous record in the system indicating that the person has overstayed his/her visa. Article 7 of the Charter of Fundamental Rights and Article 8 of the ECHR protect the right to respect for private and family life. Such rights can be limited but restrictions must be in conformity with the general requirements of Article 52 (1) of the Charter of Fundamental Rights. This means that limitations must be provided for by law, must meet genuine objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others, respect the essence of the right, and be proportionate. The European Data Protection Supervisor listed several aspects to be taken into account to assess the degree of interference, such as, the nature of the data, the scale of data collection, the further use and possible change of purpose as well as transfer of data to third countries.¹⁷

Respondents were asked whether they believe that giving their biometrics when crossing the border is intrusive or not to their private life. The results are presented in Figure 7. 46.6% and 42.3%, believe that providing fingerprints and facial image respectively is not intrusive to their privacy (i.e. selected options 1 or 2 on the five points scale). Still, there is a relevant share of persons - approximately 30 percent, depending on the biometric identifier - who think that the provision of the respective information is intrusive or very intrusive (i.e. selected options 4 or 5 on the five points scale). Attitudes towards iris-scan are different, with a higher percentage (36.4%) believing that having their iris scanned is intrusive or very intrusive to their privacy (i.e. selected options 4 or 5 on the five points scale). In general, having previously provided fingerprints and being more in favour of new technologies is correlated with the perception that providing biometric data is not intrusive to one's privacy (no considerable differences could be found according to age and gender of respondents).

¹⁶ See, for example, ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987, para. 48; *Amann v. Switzerland* [GC], No. 27798/95, 16 February 2000, para. 65; CJEU, Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen and Bundesanstalt für Landwirtschaft und Ernährung*, 9 November 2010, paras. 52 and 59.

¹⁷ EDPS, Opinion on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP), 18 July 2013.

Figure 7: Perception of intrusiveness of collection of providing biometric data (in %)



Source: FRA survey on smart borders, 2015. Question: Do you believe that giving your biometrics when crossing the border is intrusive or not to your privacy? N: 1,192, 1,148 and 1,153, respectively.

In sum, with the exception of iris-scan, there is a tendency among respondents to perceive the provision of biometric data to be not intrusive on their privacy. However, a large share, approximately 30 percent, perceived providing fingerprints and facial pattern as intrusive or very intrusive. As with any other limitation to a right enshrined in the Charter of Fundamental Rights, the collection and processing of biometric data has to respect the requirements of Article 52 (1) of the Charter, else it would not be justified.

1.3.2.1. Dignity

The concept of dignity forms a cornerstone in the EU Charter of Fundamental Rights. The first five articles fall under the title 'Dignity', bringing together various rights that are especially closely related to dignity, for instance the right to integrity of the person (Article 4(1)). Article 6 of the Schengen Borders Code as amended in 2013 requires that "border guards shall, in the performance of their duties, fully respect human dignity, in particular in cases involving vulnerable persons".¹⁸ This raises the question on how far Member States can go in enforcing the collection of biometric data when – due for example to medical reasons (an injured hand), or damaged fingerprints due to manual work – factual difficulties emerge, an issue which needs to be addressed in a manner which does not interfere disproportionately with the right to physical and mental integrity of the person.

In the questionnaire, violation of human dignity has been operationalised as 'humiliating behaviour'. In human rights law there is an intimate connection between the notion of human dignity and the notion of humiliation, and humiliation can be explained in terms of (violation of) human dignity. For example, when assessing if a certain action constitutes degrading treatment, the ECtHR examines whether the treatment suffered humiliates or debases an individual, showing a lack of respect for, or diminishing, his or her human dignity, or arouses feelings of fear, anguish or inferiority capable of breaking an individual's moral and physical resistance.¹⁹

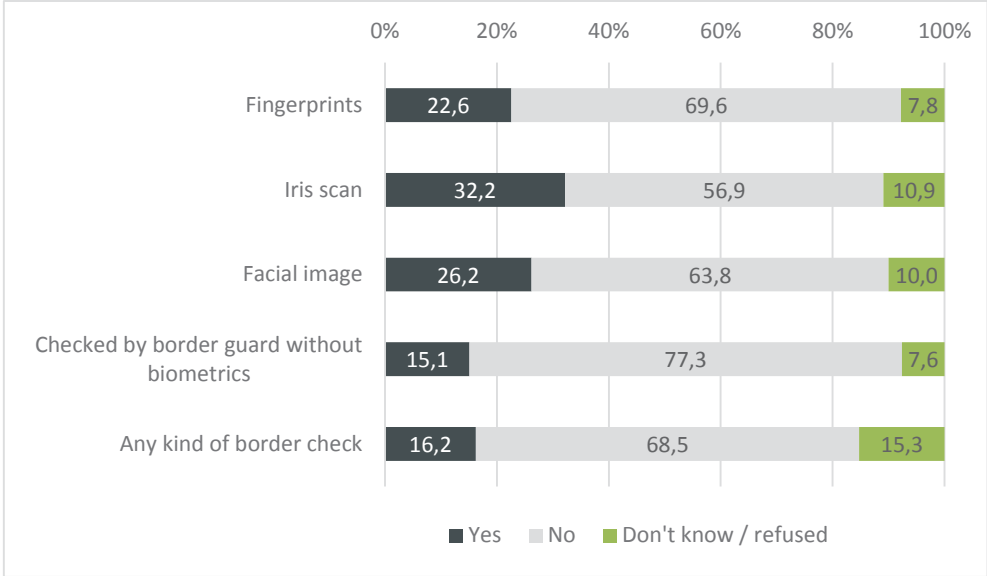
Respondents were asked whether they believed that the following situations might be humiliating: to give their biometrics (fingerprints, iris-scan and facial image, respectively), to have their passport checked by a

¹⁸ The Schengen Borders Code (Regulation (EC) No. 562/2006 amended by Regulation (EU) No 610/2013), Article 6.1.

¹⁹ See, for example, ECtHR, *M.S.S. v. Belgium and Greece*, No. 30696/09, 21 January 2011. para. 220, and *Pretty v. the United Kingdom*, no. 2346/02, 29 April 2002, para. 52.

border guard (with no biometrics involved) or any kind of border check in general. The results are presented in Figure 8. The majority of respondents find these situations not humiliating. Almost one third (32.2%) believe that letting their iris be scanned might be humiliating, one in four (26.2%) finds that providing facial image might be humiliating and slightly more than a fifth (22.6%) that providing fingerprints might be humiliating. Again, iris-scan is the biometric identifier which is more negatively perceived among the three considered. The least humiliating situation is having a 'passport checked by a border guard with no biometrics involved' (only 15.1% find it humiliating). Thus, more respondents think that providing biometrics might be humiliating compared with those who think that a check conducted by a border guard might be humiliating.

Figure 8: Assessment on situations that might be humiliating, average of the seven BCPs surveyed (in %)



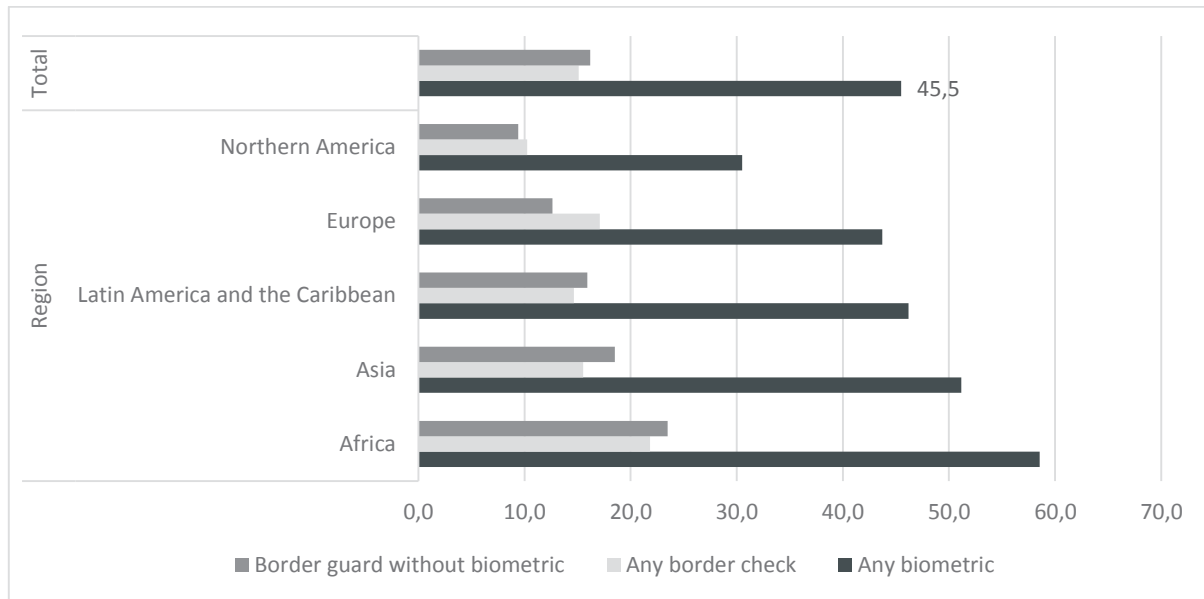
Source: FRA survey on smart borders, 2015. Question: Please tell us which of the following situations might be humiliating or not. N = 1,141 fingerprints, 1,134 iris-scan, 1,131 facial image, 1.140 border guard, 1.127 any border check.

There are differences in the extent to which persons find border checks humiliating by region of citizenship of the travellers. Figure 9 reports the percentage of travellers who perceive the following situations to be humiliating: the provision of any biometric identifier (i.e. respondents who reported the provision of at least one of the three biometric identifiers as humiliating), a border check conducted by a border guard or any kind of border check. Overall, 45.5 percent of respondents consider at least one of the three ways of providing biometric data potentially humiliating. This percentage is much higher for citizens of an African country, where 59 percent find at least one way of providing biometric data potentially humiliating. Among citizens of an Asian country there is also a slightly higher percentage seeing the provision of biometric data as humiliating. On the other end, North Americans are less likely to see any of the ways of providing biometric data as humiliating (30.5%). There is also a higher percentage of Africans who think that having their passport checked by a border guard without biometrics involved (23.5%) or 'any kind of border check in general' (21.9%) might be humiliating.

This result could be interpreted as a higher perception among African people of being discriminated against at border checks, which is confirmed by the findings of FRA's EU-MIDIS survey where African people report higher rates of perceived discrimination compared with most other groups of immigrants in the EU.²⁰

²⁰ FRA (2009), EU-MIDIS. European Union Minorities and Discrimination Survey. Main Results Report.

Figure 9: Travellers who think that the provision of at least one of the three biometric identifiers or other border checks might be humiliating by region of citizenship, average of the seven BCPs surveyed (%)



Source: FRA survey on smart borders, 2015. Question: Please tell us which of the following situations might be humiliating or not. Notes: persons with citizenship from Oceania and unknown citizenship excluded due to low numbers of observations (below 30)

In sum, although the majority of all respondents do not feel that providing biometrics in the context of border control might be humiliating, more respondents find providing biometrics more humiliating compared to a check conducted by a border guard. More research would be needed to understand the reasons for this finding. The EU legislator might consider addressing travellers concerns by increasing the fundamental rights safeguards related to the protection of dignity in the EES proposal, including the handling of situations where there are objective obstacles for travellers to provide biometrics.

1.3.3. Accuracy of the data

The accuracy of the biometric data depends on the quality of fingerprints – both when taking fingerprints and reading these for comparison – and on the accuracy of other personal data included in the database. The quality of fingerprints and the accuracy of information in the databases may impact on the fundamental rights of the person. Human and technical factors influence fingerprints' quality. For example, when the system fails to recognise an individual (also called 'false negative'), the person may risk to be denied entry into an EU Member State. The person affected may face difficulties to prove that he/she really is the person he/she claims to be. In the case of third-country nationals travelling to the EU, this vulnerability might be compounded by language problems.

Biometric and other personal data included in the database should be correct and up to date. If the data stored is outdated this may lead the authorities to take a wrong decision affecting the person concerned. For example, if the extension of a visa is not included in the EES database, a person may be wrongfully considered as having overstayed the visa, which in turn could lead to apprehension, detention or denial of entry into an EU Member State. No evidence is available on the prevalence of incorrect data included in any of the three EU IT-systems currently in use in the areas of borders, visa and asylum (i.e. VIS, Eurodac and SIS II).²¹

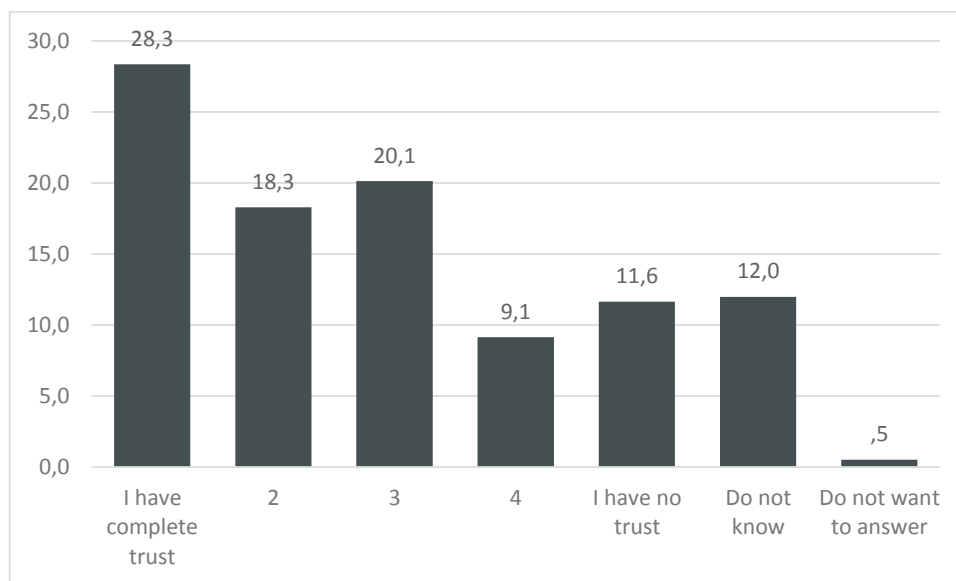
²¹ This issue is addressed in FRA ongoing project "Biometric data in large EU IT-systems in the areas of borders, visa and asylum – fundamental rights implications".

The European Data Protection Supervisor (EDPS) has underlined the importance of accuracy of the data in light of the risk of severe negative consequences for the person concerned. For example, Article 9 of the EES proposal in particular deserves specific attention as it provides that, in order to facilitate the calculation of stay, the system will automatically calculate which entry records do not have exit data immediately following the date of expiry of the authorised length of stay and inform competent authorities. This raises questions about how to avoid mistakes caused by an automated decision which could fail to register exits due to various reasons (dual status of the third-country national - e.g. person with a EU as well as a non-EU nationality using different passports when crossing the border, extended stay due to force majeure or humanitarian reasons, or technical problems with the system).²² There is a need to find solutions which would not make it excessively difficult for a traveller to provide evidence that he/she did not overstay without justified grounds.

Travellers were asked whether they trust biometric technologies to always properly identify who they are. The results are presented in Figure 10.

More respondents (46.6%) have trust (i.e. selected options 1 and 2 of the five points scale) that biometric technologies will always properly identify who they are, compared to those who tend to have no trust (20.8% selected options 4 and 5 of the five points scale). 12 percent do not know what to answer and 20.1 percent chose the middle value, which could be interpreted as lack of knowledge on the reliability of the data. There is higher trust among those who previously provided biometric data. Russians show the highest level of trust as compared to other groups of citizenship. There are no marked differences according to gender and age with respect to the level of trust in the reliability of biometric technologies.

Figure 10: Trust in reliability of biometric technologies, average of the seven BCPs surveyed (%)



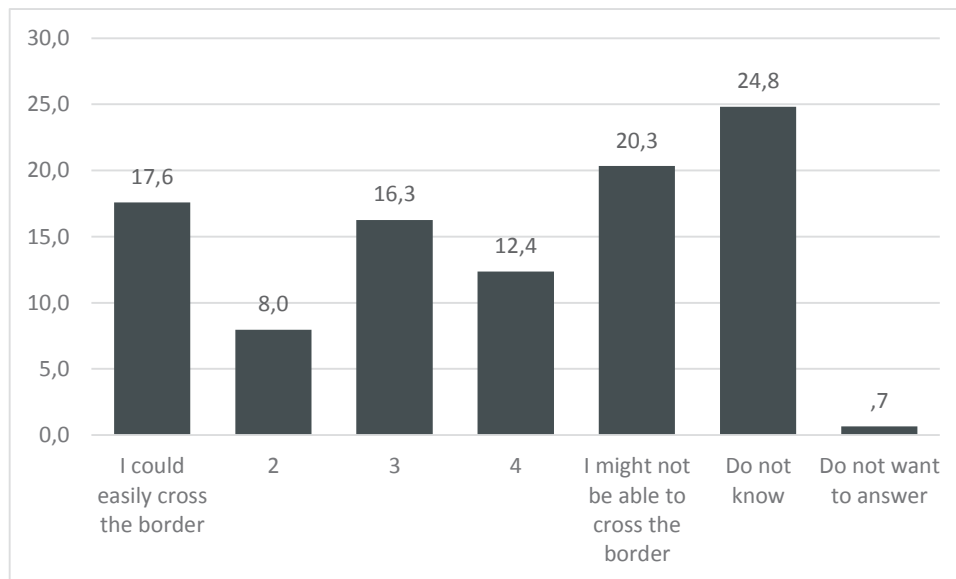
Source: FRA survey on smart borders, 2015. Question: Do you trust biometric technologies to always properly identify who you are? N = 1,203

In sum, although close to half of the respondents trust that biometric technologies will always properly identify who they are, there is a great amount of uncertainty about how well biometric systems work to properly identify people. In order to increase trust in biometric technologies, objective information on the reliability and accuracy of biometric systems could be provided to third-country nationals travelling to the EU and communicated through adequate means.

²² EDPS, Opinion of 26 March 2008 on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation No 2252/2004, OJ C 200, 6.8.2008, p. 2.

Respondents were also asked what they think would happen in case the technology does not work properly. The results are presented in Figure 11. Respondents had to indicate to what extent they believe they would be able to cross the border in those cases. Most respondents (24.8%), almost one in four, declare not to know if they would be able to cross the border. One fifth (20.3%) believe they might not be able to cross the border and 17.6% believe they could easily cross the border if the technology does not work properly. There are more people (32.7%) who believe they might not be able to cross the border in case of problems with technology (options 4 and 5 of the five points scale), compared to those (25.6%) who believe they will be able to cross the border (options 1 and 2 of the five points scale).

Figure 11: Ability to cross the border In case technology does not work properly, average of the seven BCPs surveyed (%)



Source: FRA survey on smart borders, 2015. Question: In case the technology does not work properly, to what extent do you believe you would be able to cross the border? N = 1,205

The fact that most respondents either believe that they will not be able (i.e. selected options 4 or 5 of the five points scale) or do not know if they will be able to cross the border in case the technology does not work properly is an important finding. It resonates with the concerns expressed by the EDPS on the negative consequences that mistakes in the system and in the automated processing of personal data can have on the individual.

An important implication of potential incorrect data in EES concern the risks of persons mistakenly flagged as over-stayers and the use that police, immigration or other officials may make of such information. Specific measures could, therefore, be introduced in the EES to deal with situations where the data stored in the system are – for various reasons – not up to date without negative consequences for the travellers. In addition, police or immigration officers should have a clear duty to verify the accuracy of the lists of over-stayers produced by the IT-system before they take action, initiating for example, a return procedure.

1.3.4. Data protection

The use of biometric technologies and of IT systems in the context of border control affect the right to data protection. The right to data protection is guaranteed in Article 8 of the Charter of Fundamental Rights. It forms part of the rights protected under Article 8 of the ECHR. According to the Charter, a person's data can only be processed fairly, for specified purposes, on the basis of the consent of the person concerned or some other legitimate basis laid down by law, and everyone has the right to access to data which have been

collected concerning him or her, and has the right to have it rectified. The right to correct wrong data relates directly to the right to an effective remedy, which is enshrined in Article 47 of the EU Charter of Fundamental Rights. The possibility to correct the data is particularly crucial. If data connected to the biometric identifier is inaccurate or outdated, this may lead the authorities to take a wrong decision affecting this and other fundamental rights of the person concerned. Secondary EU law, such as the Data Protection Directive 95/46/EC, the forthcoming data protection reform package or the EES proposal further specify the right to the protection of personal data. Further, general security measures aimed at protecting the biometric information need to be taken to protect the right to data protection.

Respondents were asked a number of questions relating to data protection, including questions on access to data by authorised persons and by law enforcement authorities and on the rights of the individuals, such as on the provision of information on the purpose of collecting biometrics and on the right to access and rectify one's own personal data.

1.3.4.1. *Right to information*

Article 33 of the EES proposal clarifies the information that should be provided by Member States to persons whose data are recorded in the EES.²³ The information to be provided include, inter alia, the identity of the controller of the data, the purposes for which the data will be processed, the categories of recipients of the data; the data retention period and the existence of the right of access to one's own data, the right to rectify inaccurate or unlawfully processed data including information on the procedures for exercising those rights and contact details of supervisory data protection authorities. This information should be provided in writing.

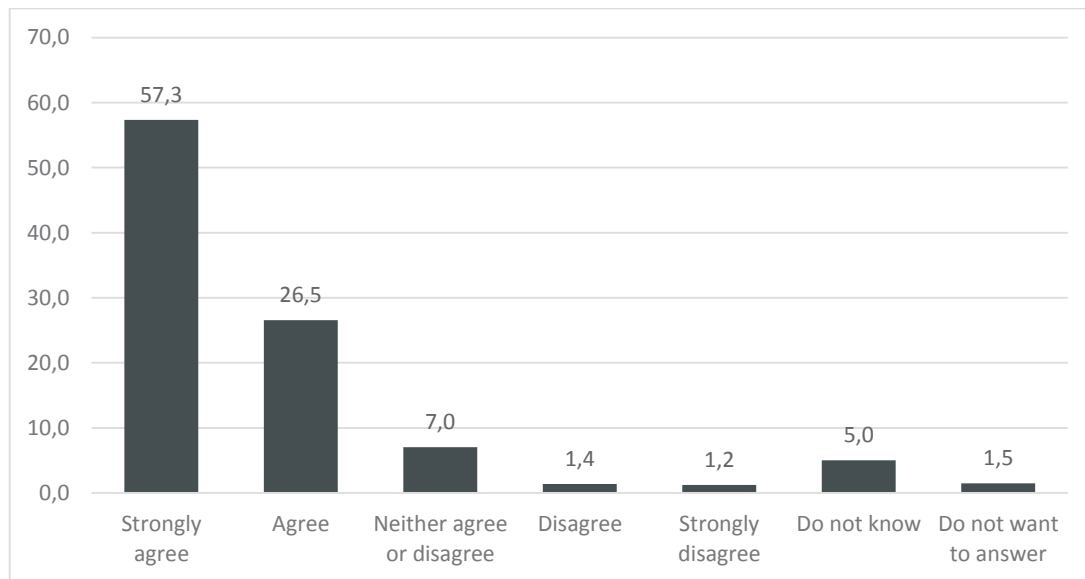
The EDPS suggested to include an obligation to provide additional information to the travellers, especially in relation to overstay, for example, information on the fact that overstay will lead to the publication of the individual's personal data on a list of over-stayers which will be sent to recipients of this list.²⁴

Respondents were asked whether they considered it important to be informed about why their biometric identifiers are collected and used. The results are presented in Figure 12. 83.9 percent of the respondents strongly agree, or agree, that it is important to be informed on why their biometric identifiers are collected and used. This shows a wide consensus.

Figure 12: Agreement to the importance of being informed on why biometric identifiers are collected and used, average of the seven BCPs surveyed (%)

²³ Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union, COM(2013) 95 final, Article 33.

²⁴ EDPS Opinion, p.13



Source: FRA survey on smart borders, 2015. Question: Please say to what extent you agree or disagree with each of the following statements. It is important that I am informed on why my biometric identifiers are collected and used. N = 1,153

The legal obligation to provide information on the data recorded in the EES is further underlined by a strong interest of respondents to receive information on the purpose of collecting and processing their personal data. As recommended by the EDPS, the EES proposal could specify that such information be provided "in an intelligible form, using clear and plain language, adapted to the data subject" as it is foreseen in Article 11.1 of the proposed Data Protection Regulation. Translations of this information should be available for third-country nationals not understanding the language of the responsible Member State.²⁵

1.3.4.2. *Right to access and rectify the data*

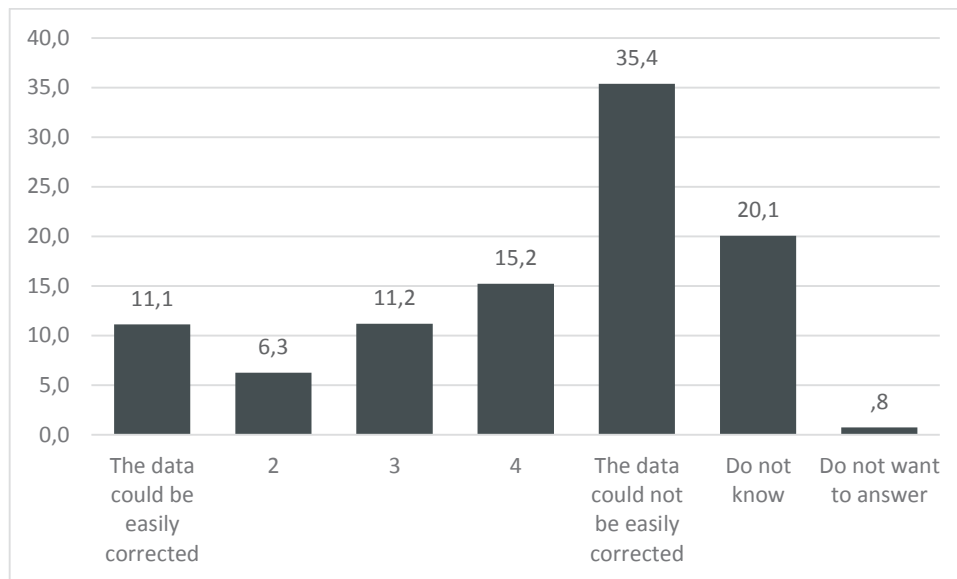
According to Article 8 of the Charter of Fundamental Rights "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified". This is reflected in Article 34 of the EES²⁶ proposal which provides a framework for the rights of information, access and rectification of third-country nationals' personal data. According to article 34 (2) any person may request that data relating to him or her which is inaccurate be corrected and that data recorded unlawfully should be deleted. The correction and deletion shall be carried out without delay by the Member State that is responsible, in accordance with its laws, regulations and procedures.

Respondents were asked whether – in case of an error in their personal data when crossing the border – they believe that their personal data could be easily corrected. The results are presented in Figure 13. Half of the respondents (50.6%) believe that their data could not be easily corrected (options 4 and 5 of the 5 points scale). Only 17.4 percent believe that the data could be easily corrected (options 1 and 2 of the 5 points scale). One in five respondents does not know what to answer (20.1%).

²⁵ Ibid., p.14

²⁶ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing an Entry/Exit System (EES) to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union, COM(2013) 95 final, Article 34.

Figure 13: Opinions on possibility to correct the data in case of an error in the personal data, average of the seven BCPs surveyed (%)



Source: FRA survey on smart borders, 2015. Question: In case there is an error in your personal data when crossing the border, for example your biometrics do not match with your name, do you think that your personal data could be easily corrected? N = 1,196

As reported by the EDPS, the rights of the data subject are key to data protection. Ensuring the effectiveness of the rights of the data subject is particularly important in the area of freedom, security and justice, where, on the one hand, the exceptions and limitations imposed by law have a larger scope of application, and, on the other hand, the erroneous processing of personal data may have serious direct consequences on the data subject.²⁷

Most respondents are concerned that their right to have wrong personal data corrected would not be easily safeguarded. This could be based on travellers' unfamiliarity with their rights and access to remedies, as well as a lack of trust in the effectiveness of these mechanisms. Third-country nationals travelling to an EU Member State need to be better informed about the right to access and to rectify personal data and the existence of remedies and available support in case of difficulties.

1.3.4.3. Access to data by authorised persons

Unauthorised access to personal data constitutes a violation of the right to protection of personal data and as the case may be the right to private life. Technical security measures including logging practices can limit the risk that people who are not authorised to access the database do so or that authorised persons access the data for a non-authorised purpose, such as a private one.

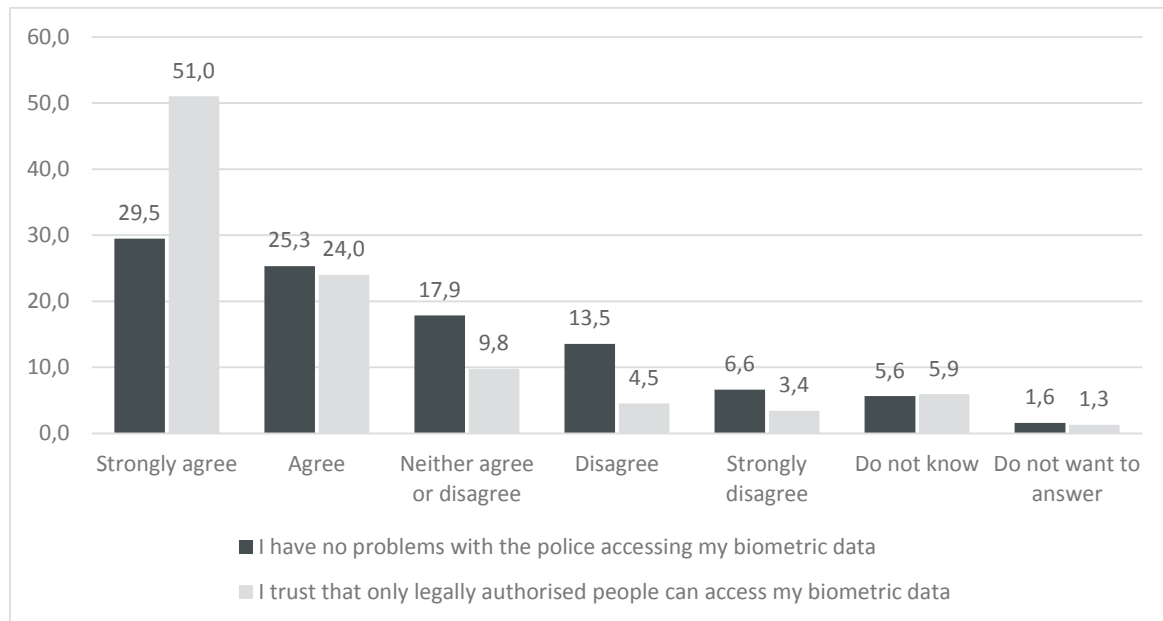
According to Article 7 of the EES proposal, each Member State must designate the competent authorities, including border, visa and immigration authorities, the duly authorised staff of which has access to enter, amend, delete or consult data in the EES. According to Article 40, the authorised staff of Member States, of eu-LISA and of Frontex has access to the specific personal data listed in Article 40, for the purposes of reporting and statistics without allowing individual identification.

Respondents were asked whether they trust that only legally authorised people will access their data. The majority of travellers trust that only legally authorised people can access biometric data. As shown in Figure

²⁷ SIS II Supervision Coordination group, Report on the exercise of the rights of the data subject in the Schengen Information System (SIS), October 2014, p. 2.

14, approximately three quarters of respondents strongly agree or agree with this statement and only 7.9 percent disagree or strongly disagree.

Figure 14: Views on access to data, average of the seven BCPs surveyed (%)



Source: FRA survey on smart borders, 2015. Question: Please say to what extent you agree or disagree with each of the following statements: 1. I have no problems with the police accessing my biometric data, 2. I trust that only legally authorised people can access my biometric data. N = 1,137 and 1,145.

In order to make sure that only authorised persons access personal data included in the EES database, adequate security measures should be in place. The number of persons having authorised access could also be limited to what is absolutely necessary for the purpose to be attained. For example the data controller (eu-LISA or the respective authority at national level) may only produce anonymised statistics for relevant stakeholder instead of giving those who need the statistics direct access to the personal data.

1.3.4.4. Access to data for law enforcement purposes

According to the EES proposal, after two years of its functioning an evaluation of the system should take place. The European Commission should also evaluate the possible access to the system for law enforcement purposes. On the basis of this evaluation, as well as the evaluation of the experience of access for such purposes into the VIS, the Regulation could be amended to define the conditions for access by law enforcement authorities.²⁸

Access by law enforcement authorities to the EES would fit in the general trend to grant law enforcement authorities access to several large-scale information and identification systems.

A number of Member States have, however, expressed their preference for including the access by law enforcement authorities directly into the proposal, particularly for the purpose of combating cross-border crime and terrorism, as an ancillary objective from the very start of operation of the EES.²⁹

²⁸ Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union, COM(2013) 95 final 2013/0057 (COD), p.6

²⁹ Council of the European Union, Access for law enforcement purposes to the EES, Brussels, 16 July 2015, available at <http://data.consilium.europa.eu/doc/document/ST-10732-2015-INIT/en/pdf>.

This initiated a discussion on the legal challenges of such extension of the purpose of the instrument – as well as on additional fundamental rights issues – particularly bearing in mind the principles of necessity and proportionality which shall be observed; the CJEU emphasised in the Digital Rights Ireland judgment that a measure of indiscriminate, blanket nature violates the Charter.³⁰ Other potential issues relate to discrimination, presumption of innocence and potential stigmatisation of third-country nationals given that the availability of their data for law enforcement purposes would necessarily affect the detection rate and statistics of criminal activity compared to EU nationals.

Respondents to FRA's survey were asked whether they have no problems with the police accessing their personal data. The results are reported in Figure 14. More than half of the respondents do not have any problems with the police accessing their biometric data (54.8 percent agree or strongly agree with this statement). However, access by law enforcement authorities to EES is an issue for a relevant part of the population, with approximately one in five (20.1%) who either disagree or strongly disagree with the statement.

While the majority of the respondents express no concerns over the measure, it needs to be taken into account that the question could only be phrased very generally and could not refer to the actual extent of, and fundamental rights safeguards relating to, possible law enforcement access. Regardless of the indicative information provided by this survey, it will be the obligation of the EU legislator to ensure full compliance with fundamental rights and take into account standards set by relevant CJEU and ECtHR judgements, as well as experience with systems where law enforcement access is currently permitted.³¹

1.3.5. Automated border control systems

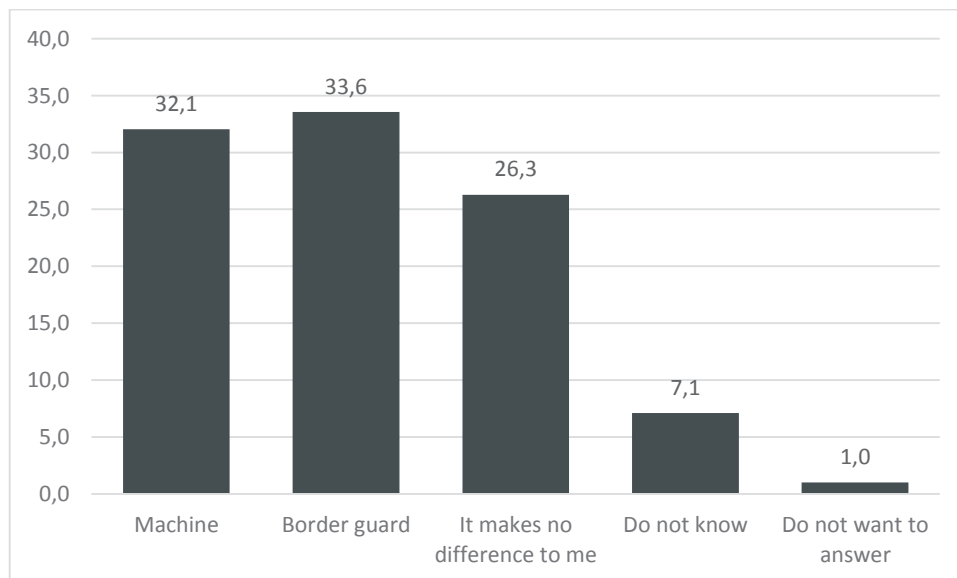
Border controls are changing and there is increasing reliance on automated border controls (ABC) including relevant technologies. Increasingly in the EU, biometric data are being used in conjunction with ABC. The ABC gate compares the biometric data (in most cases, facial image) from the passenger's travel document with the real-life equivalent. It also verifies the validity and reliability of the travel document. If the scoring is high enough, the passenger is let through the gate.³² In addition, an ABC gate could also carry out checks against the authorities' databases. These systems are considered to match the high security in verification of a traveller's identity with increased efficiency and speed in conducting border control. Respondents were asked if they were to choose, whether they would go to a machine or a border guard. Results are presented in Figure 15. Approximately one third of the respondents reported they would go to a machine and another third reported they would go to a border guard. For one in every four respondents, it makes no difference.

³⁰ CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014.

³¹ ECtHR, *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000; ECtHR, *M.K. v. France*, No. 19522/09, 18 April 2013; ECtHR, *Liberty and Others v. the United Kingdom*, No. 58243/00, 1 July 2008; ECtHR, *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008; CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014.

³² See project [ABC4EU](#).

Figure 15: Travellers' preference between machine or border guard, average of the seven BCPs surveyed (%)



Source: FRA survey on smart borders, 2015. Question: Border controls are changing and there is increasing reliance on automated systems (with no border guards involved). If you could choose, would you go to a machine or to a border guard to have your documents checked at the border? N = 1,195

There are no marked differences in the results by age or gender, where men tend to prefer machines slightly more often than women. However, there are clear differences with respect to region of citizenship. Citizens of an African country, Latin America, the Caribbean and North America prefer border guards over machines. While citizens of Asian countries do not have specific preferences, travellers who are European citizens prefer machines over border guards. The latter is mainly due to Moldovan citizens strong preference for machines over board guards, since Russian citizens appear to be indifferent in their choice regarding machine or border guard.

1.3.6. Discrimination

Article 6 of the Schengen Borders Code requires that "border check controls have to be carried out in a way which does not discriminate against a person on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation".³³ This provision must be read in light of Article 21 of the Charter of Fundamental Rights which extends the prohibition of discrimination to other grounds.

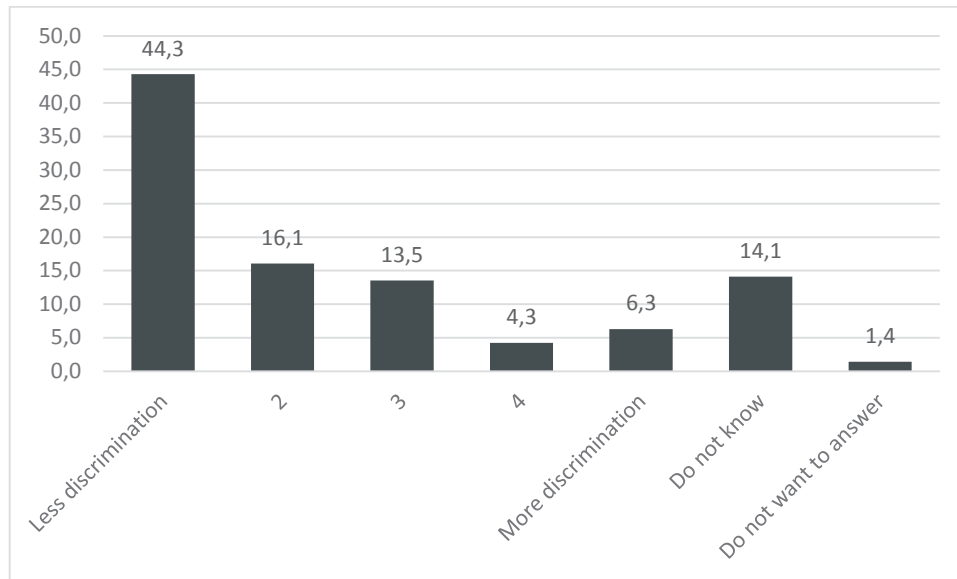
It could be argued that automated systems cause less discrimination than border guards because of the absence of human judgement selecting passengers for further checks.

The results of the survey confirm this view. Respondents were asked whether they believe that automated systems could cause more or less discrimination compared to checks done by border guards. The results are presented in Figure 16. The majority believe that automated system could cause less discrimination. Overall, 60.4% believe it could cause less discrimination (options 1 and 2 of the 5 points scale) and only one in ten (10.6%) believe that an automated system could cause more discrimination (options 4 and 5 of the 5 points scale). 13.6% do not know what to answer.

Particularly, citizens of a European country, most notably Moldovans, think that the use of machines would lead to less discrimination.

³³ The Schengen Borders Code (Regulation (EC) No. 562/2006 amended by Regulation (EU) No. 1051/2013), Article 6.1

Figure 16: Travellers opinion on the extent to which automated system cause more or less discrimination, average of the seven BCPs surveyed (%)



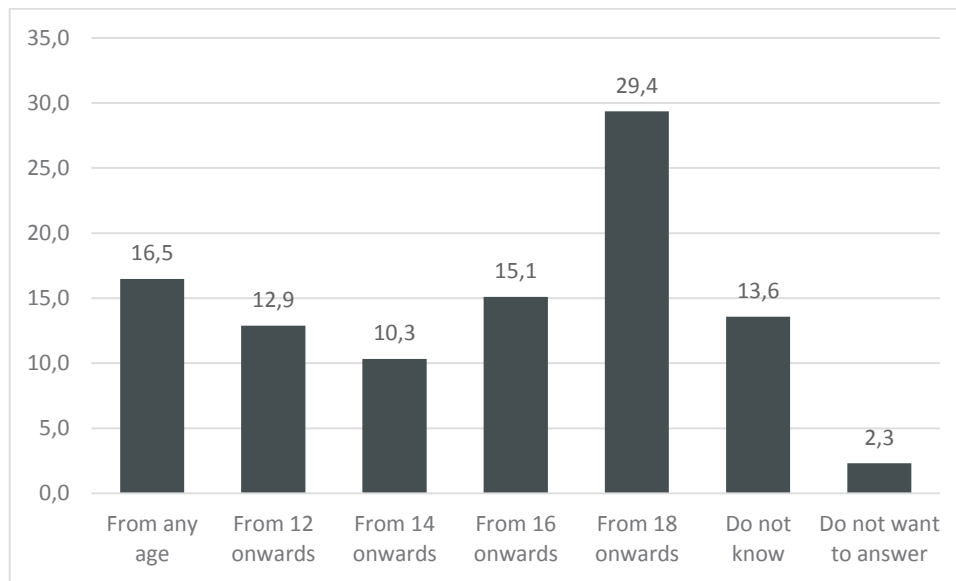
Source: FRA survey on smart borders, 2015. Figure: Do you think that automated systems could cause more or less discrimination compared to checks done by border guards? By discrimination we mean when somebody is treated unfavourably compared to others because of their skin colour, age, sex, sexual orientation, disability, ethnic origin, religion or religious beliefs. N = 1,176

There is a widely held view that automated systems could cause less discrimination compared to checks carried out in person by border guards. This might be based on the assumption that machines entail a lower risk of discriminatory profiling compared to checks by border guards. However, it should be noted that automated systems could be programmed to identify individuals using sensitive data, such as race, ethnicity or health. Measures to avoid discriminatory profiling are, therefore, required.

1.3.7. Children

The EES proposal envisages the processing of fingerprints of children from the age of 12. In the survey, FRA asked from what age respondents think that children should be allowed to go through biometric checks. The results are presented in Figure 17. Most respondents (29.4%) think that only adults (from 18 years onward) should go through biometric checks, followed by those who think that biometric checks should be done at any age (16.5%) and those who would recommend them from 16 years onwards (15.1%).

Figure 17: age at which biometric checks of children should be allowed, average of the seven BCPs surveyed (%)



Source: FRA survey on smart borders, 2015. Question: In some countries children already go through biometric checks. From what age do you think they should be allowed? N = 1,172

In sum, although most respondents believe fingerprints should be taken from 18 years of age onwards, there are different views on at which age children should be allowed to provide biometric checks. Less than one third of the respondents believe children should be allowed to provide fingerprints from 12 year onwards (i.e. selected the option 'from any age' or 'from 12 onwards'), the current age limits for fingerprinting set in the EES proposal. Based on these results and on the previously discussed negative fundamental rights implications on the individual in case of mistakes in the data, more reference to the specific situation of children (but also of other vulnerable groups such as older people and persons with disability) could be made in the EES proposal. Not only the methods for collecting fingerprints, but also those for providing information about fingerprinting should be carried out in an age-appropriate manner. Moreover, long data retention periods, even if allowed by law, may cause a particular hardship to children. The child had most likely no role in the decision to travel. Therefore, retaining a child's data in EES may disproportionately impact on any future decisions by the state concerning the child in question.

It should be noted that including children in the EES dataset might also have positive fundamental rights implications. If SIS II was to be optimised for tracing missing children, for instance by including all missing children in the database on a routine basis, an alert could appear in EES when a missing child is checked against the database.

1.3.8. Other issues

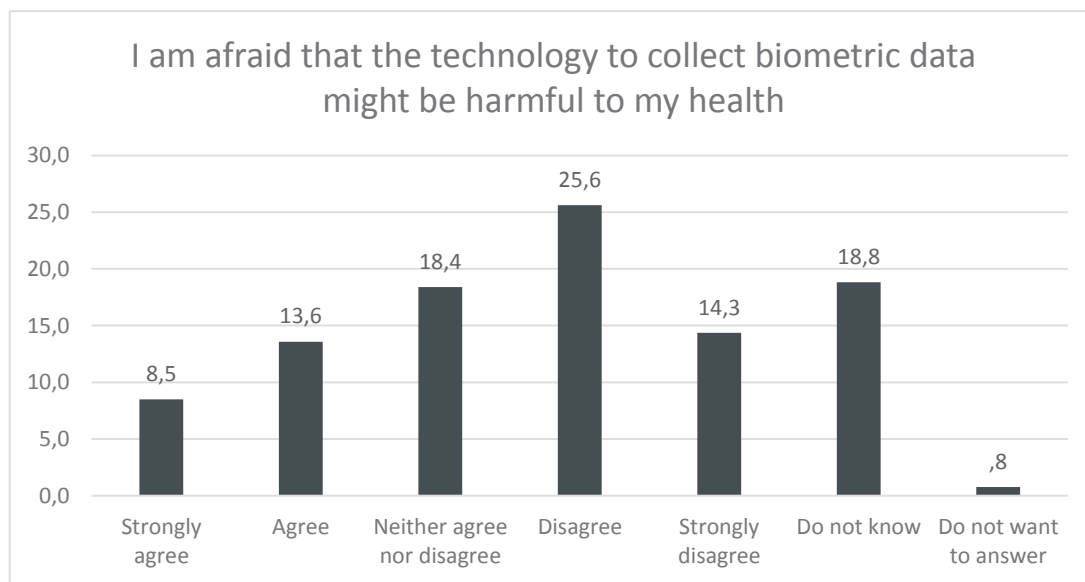
Finally, respondents were asked whether they are afraid that the technology to collect their biometrics might be harmful to their health. The results are reported in Figure 18. 39.9 percent of the respondents either disagree or strongly disagree with this statement. 22.1 percent believe biometric technologies could harm their health (agree or strongly agree). A large share of travellers, almost one in five, does not know if technologies to collect biometric data would be harmful to their health (18.8 percent). 18.4 percent neither agree nor disagree with the statement.

In sum, despite the tendency to feel safe, more than half of the respondents either believe that biometric technologies could harm their health or show uncertainty on this issue. Objective and scientific information should be provided to travellers on the health consequences of the use of biometric data.

Respondents were also asked if the collection of biometric data is important to secure borders, one of the objectives mentioned for the establishment of an entry/exit system (EES).³⁴ The majority agree with the statement (67%). Only 8.7 percent believe that the use of biometric technologies is not important to secure EU borders (i.e. either disagrees or strongly disagree with the statement).

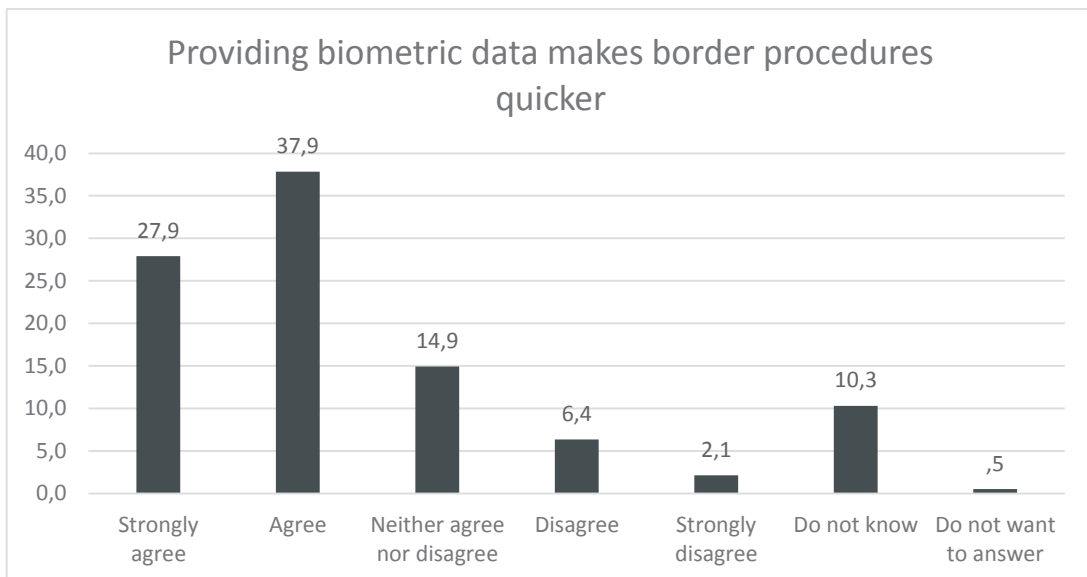
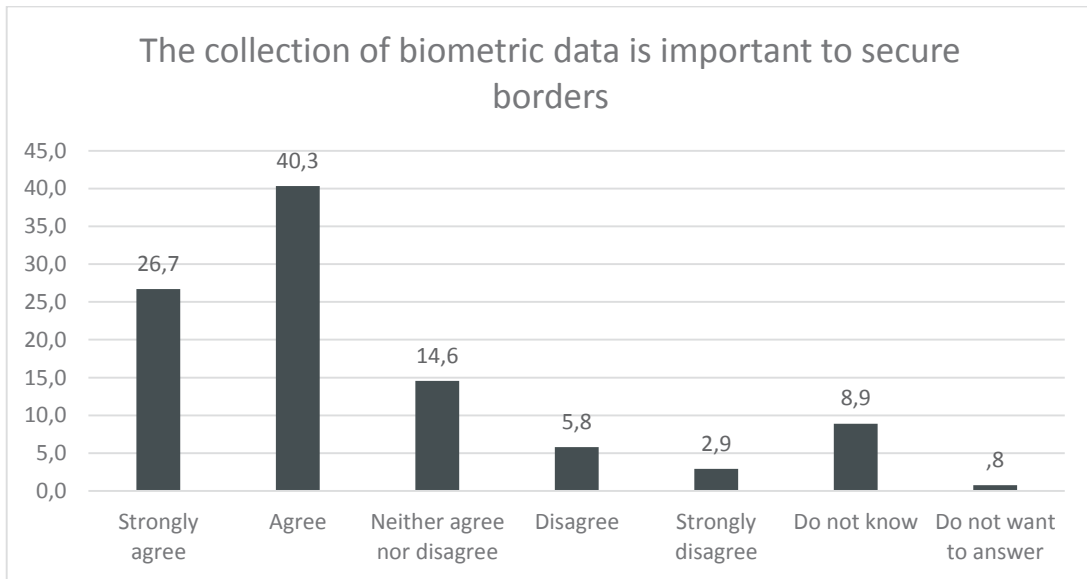
One of the aims of the Smart Border proposal is to speed up border crossing.³⁵ Respondents were finally asked whether they believe that providing biometric data makes the border procedure quicker. Two thirds of the respondents either strongly agree or agree with the statement. 8.5 percent disagree or strongly disagree. About one quarter of respondents said either that they neither agree nor disagree or that they do not know whether or not to believe the collection of biometric data at the border increases the speed of border checks.

Figure 18: Opinions on biometric data regarding speed, security and health (in %)



³⁴ See the Commission Communication of 13 February 2008 preparing the next steps in border management in the European Union COM (2008) 69 final and the accompanying Impact Assessment SEC(2008) 153 'An open and secure Europe serving and protecting the citizens', Official Journal of the European Union of 4.5.2010, C 115/1.

³⁵ See eu-LISA, Smart Borders Roadmap of the Testing Phase, Version 5.0, 28 February 2015.



Source: FRA survey on smart borders, 2015. N = 1,164, 1,168 and 1,165, respectively.

1.4. Conclusions

There are a number of fundamental rights implications related to modern identification and verification technologies in the context of border control. Third-country national travellers' views on these implications can inform the legislator and policy makers on specific areas of concern and how the population targeted by these measures will perceive the Entry Exit System, once in place. At the same time, travellers' perceptions are only one element that needs to be taken into account when assessing fundamental rights compliance with certain measures. Violations of fundamental rights may occur regardless of whether the individual consents or not to a certain treatment, particularly in light of limited rights awareness.

The results show that most respondents are comfortable with providing biometrics when crossing borders, with the exception of iris-scan. Most respondents do not feel that biometrics compromises their right to dignity. Except for iris-scan, there is a tendency among respondents to perceive biometric data provision as not being intrusive on their privacy. However, about 30% believe that biometrics represent an interference with their private life and between 22% and 32%, depending on the biometric identifier, feel that the provision of biometric data is potentially humiliating. In addition, more respondents think that providing biometrics might be humiliating compared to those who think that a check conducted by a border guard might be humiliating. Travellers' concerns could be addressed by increasing the fundamental rights safeguards related to the protection of dignity in the EES proposal, for instance by complementing specific provisions with an obligation to act in full respect of the human dignity of the third-country national.

The results of the survey show that trust in the reliability of biometric technologies is quite high. This reflects the consensus among experts that identifies biometrics as the most accurate means to determine a person's identity.

A key finding of the survey relates to what happens when something goes wrong and the system does not function as expected. Here, more than half of the respondents believe that they will not be able (or do not know if they will be able) to cross the border in case the technology does not work properly. Similar concerns emerged in relation to the right to rectify the data, a key to data protection. Half of the respondents believe that in case of a mistake in the data, it would be difficult to correct this.

This finding resonates with the concerns expressed by the EDPS and other organisations on the negative consequences that mistakes in the system and in the automated processing of personal data can have on an individual. For example, when the system fails to recognise an authentic individual (also called 'false negative'), the person might be denied entry into an EU Member State or, in the worst case, run the risk of being apprehended and detained. The person affected may face difficulties to prove that he/she really is the person he/she claims to be. In the case of third-country nationals travelling to the EU, this vulnerability might be compounded by language problems.

There are many ways mistakes could occur, for example errors such as false negatives, but also fraud and forgery of biometric data and incorrect or not up to date personal data included in the database. The most likely implication of incorrect data in EES concern the risks of persons mistakenly flagged as over-stayers and the use that police, immigration or other officials may make with such information. Specific measures could be, therefore, introduced in the EES to deal with situations where the data stored in the system are – for various reasons – not up to date without negative consequences for the travellers. In addition, police or immigration officers should have a clear duty to verify the accuracy of the lists of over-stayers produced by the IT-system before they take action, initiating for example, a return procedure.

The results of the survey show that third-country national travellers take data protection seriously and more than 80% consider it important to be informed on the purpose of collecting and processing their personal data. The legal duty to provide information on the data recorded in the EES could be further strengthened by

specifying in the proposal that information should be provided in a way that takes into account the needs of specific groups (for example, child-friendly language for children and 'easy to read' for persons with disabilities). Translations of this information should be made available for third-country nationals not understanding the language of the responsible Member State.

There is a widely held view that automated systems could cause less discrimination – for example on the basis of race or ethnicity – compared to checks carried out in person by border guards. This might be based on the assumption that machines entail a lower risk of discriminatory profiling compared to checks by border guards. However, it should be noted that automated systems could be programmed to identify individuals using sensitive data, such as race, ethnicity or health. Measures to avoid discriminatory profiling are, therefore, required.

Less than one third of the respondents agree with the current age limits for fingerprinting set in the EES proposal, according to which fingerprints should be provided from 12 years onwards. Most respondents would exclude children (i.e. minors) from the obligation to provide fingerprints. Based on these results and on the serious negative fundamental rights implications on the individual in case of mistakes in the data, more efforts should be made to protect the fundamental rights of children.

Finally, respondents were asked whether they are afraid that the technology to collect their biometrics might be harmful to their health. The survey result show that despite the tendency to feel their health is not at risk, two thirds of respondents either believe that biometric technologies could harm their health or show great uncertainty on this issue. Objective and scientific information should be provided to travellers on the health consequences of the use of biometric data.