Council of the European Union

Brussels, 26 April 2016
(OR. en)

7675/16
ADD 3

Interinstitutional File:
2016/0106 (COD)

FRONT 165
VISA 91
CODEC 391
COMIX 268

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	7 April 2016
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2016) 115 final part 1/3
Subject:	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) 2016/399 as regards the use of the Entry/Exit System (EES)

Delegations will find attached document SWD(2016) 115 final part 1/3.

Encl.: SWD(2016) 115 final part 1/3

EUROPEAN
COMMISSION

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. 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 nationals[2] travelling to the Schengen area[3], (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 Code[5] 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's[6] 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 Members 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 writing[10].

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 2015[11].

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 efficnent 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 unchanged[12], and so do several other features of the original proposals. This Impact Assessment is building on the 2013 Impact Assessments[13] 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 Code[14] 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 country[15].

Unless stated otherwise, wherever this Impact Assessment speaks about third country nationals it refers to people that enter for a short stay[16].

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 borders[17] 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 Study[18] 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 States[19].

On 15 December 2015, the Commission proposed an amendment to the Schengen Borders Code[20] 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 period[21]. 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 nationals[22]. 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 complement 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 document[23].

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 State[24]. 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 million[25]. 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 validaty 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 economics[26]. International criminal organisations are developing their activities across borders[27]. 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 States[30] 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 Reseach Unit. "Non-immigrant Overstays: Brief Synthesis of the Issue – January 22, 2014 on https://fas.org/sgp/crs/homesec/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 Mexico[32].

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 2012[33], 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 nationalities[34].

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 citziens and permanent residents). On average 7% of arriving passengers in the US use the trusted traveller lanes[35].

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 (Netherland) 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 countries[36] 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 systems[37] 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 image [38]of the applicant. The enrolment of these biometric identifiers in VIS prevents visa fraud and allows identity verification at borders, as well as identification[39].

- Adoption of the Commission proposal for a touring visa[40] will resolve the unsatisfactory patchwork of bilateral agreements[41].

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 Policy[42]. 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 management[43].

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 budget[44] 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 Migration[45] 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 2009[47].

In October 2011 the Commission further developed this idea in a Communication on the implementation options for the EES and RTP[48]. 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 Migration[49] and the European Agenda on Security[50]. 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 intiative, 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 arrivd 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 Rights[51] 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 costs[53] 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 Study[54], 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 System[55] (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 years[58]. 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 risk[59] 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 iris[62] 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 that[63]:

- 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 equipment[64] 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 fingerprints[66];

- Finally, iris was perceived by travellers as more intrusive than any other biometric[67].

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 control[68] 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 exceeded[69].

In the case of an overstayer, 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 Eurodac[70] and the actual use[71] 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 years[72].

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 granted[73].

(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 Convention[74]. 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 EU[75], the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society[76]. 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 management[77], 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

[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

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 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* principles[78]:

- 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 Convention[79], 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 overstay[80].

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 "Analyis 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 the 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 limitation[81] and the data minimisation[82] (*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 years[83] 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

[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

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 choice for this option was furthermore based on a study[84] 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

[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

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 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.

<table>
<tr><th></th><th></th><th>Option (a)
Ten fingerprints</th><th>Option (b)
Fingerprints and facial image combined</th><th>Option (c)
Facial image only</th></tr>
<tr><td rowspan="5">Objectives</td><td>Better border management and facilitation</td><td>-√√√</td><td>+√√√√</td><td>+√√√</td></tr>
<tr><td>Overstayers: identifying at the border</td><td colspan="3">All three options fully meet the objective.</td></tr>
<tr><td>Idem: inland identification.</td><td colspan="2">+√√√√</td><td>+√√√</td></tr>
<tr><td>Use as criminal intelligence tool</td><td colspan="3">All three options fully meet the objective</td></tr>
<tr><td>Use as criminal identification tool</td><td>+√√√</td><td>From +√√ to +√√√ depending on number of FP's</td><td>+√√</td></tr>
<tr><td rowspan="2">Impact on</td><td>Duration of border crossing</td><td>-√√√√ at first enrolment to 0/-√ at repeat visit</td><td>From -√ to -√√√ at first enrolment depending on number of FP's; 0/-√ at repeat visit</td><td>-√ at first enrolment; 0 at repeat visits</td></tr>
<tr><td>Travel experience of third country nationals</td><td>-√√√√ at first enrolment to -√ at repeat visit</td><td>From -√ to -√√√ at first enrolment depending on number of FP's; 0 at repeat visit</td><td>-√/0 at first enrolment; 0 at repeat visits</td></tr>
</table>

	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 (≈+126%), while enrolling ten fingerprints took almost three times longer (+185%)*[85]".

  The results of the Smart Borders Pilot[86] 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*

[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."

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 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

[87] Smart Borders Pilot Final report volume 1, Eu-LISA, November 2015, section 2.2.5.2 - page 44
[88] See annex 15 - Fundamental Rights Agency survey – section 1.3.1
[89] See annex 15 – Fundamental Rights Agency survey – section 1.3.3

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 posts[91].

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 border[92], the impact 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.

<table>
<tr><th></th><th></th><th>Option (a)
2013 proposal.
registration in consular post/airport before travelling</th><th>Option (b)
on-line registration only after at least one visit to Schengen</th><th>Option (c)
use of accelerators</th></tr>
<tr><td rowspan="5">Objectives</td><td>Better border management and facilitation</td><td colspan="3">All three options achieve the objective of facilitation and focusing controls better.</td></tr>
<tr><td>Reducing the number of overstayers</td><td colspan="3">The choice of option on facilitation has no impact on achieving this objective</td></tr>
<tr><td>Use as criminal intelligence tool</td><td colspan="3" rowspan="2">The choice of option on facilitation has no impact on achieving this objective</td></tr>
<tr><td>Use as criminal identification tool</td></tr>
<tr><td rowspan="2">Impact on</td><td>Duration of border crossing</td><td colspan="2">+√ for all travellers
+√√ for registered travellers</td><td>+√√ for all travellers</td></tr>
<tr><td>Border guard's workload</td><td colspan="2">+√√</td><td>+√√√</td></tr>
</table>

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

	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

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 subscribers[95]. 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].

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

[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 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 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 system[97]: 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 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**
O 1	Better border management and	0	-√√	+√√√

[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.

		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
	facilitation			
	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	+√	+√	+√√√
	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.

[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.

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 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.

[99] Cost Report of the Technical Study, section 4.3.3

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 after an evaluation two years after start of operation	**Option (b) from the start**	**Option (c) no law 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 period[100], 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.

[100] Cost Report of the Technical Study, section 4.1.4

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).

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.

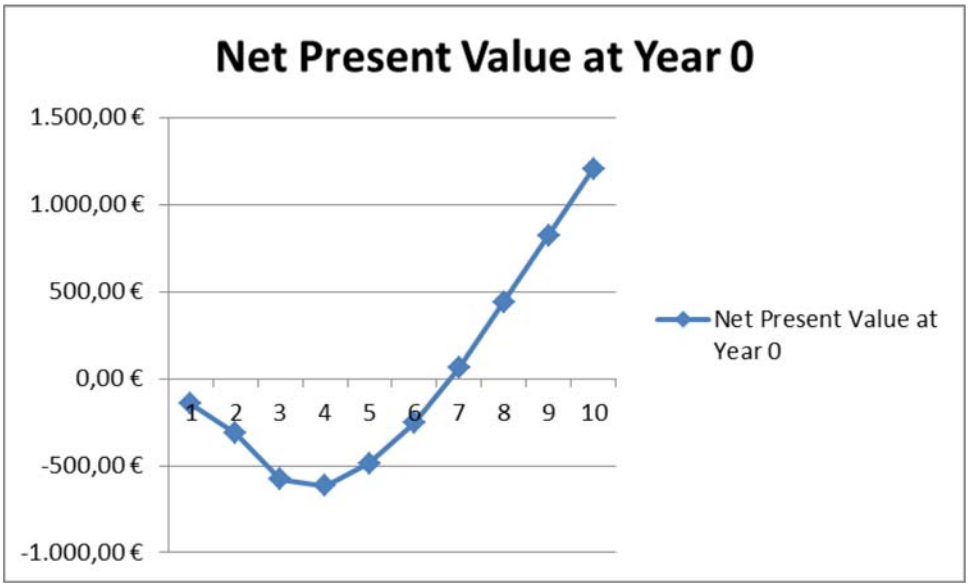

Chart showing the Net Present Value (in million €) after 1, 2, ..N years

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