COUNCIL OF THE EUROPEAN UNION

Brussels, 7 June 2012

10977/12
ADD 2

Interinstitutional File: 2012/0146 (COD)

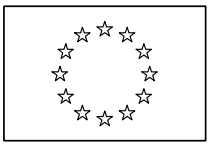
TELECOM 122
MI 411
DATAPROTECT 73
CODEC 1576

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	5 June 2012
to:	Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.:	SWD(2012) 135 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a regulation of the Europena Prliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

Delegations will find attached Commission document SWD(2012) 135 final.

Encl.: SWD(2012) 135 final



EUROPEAN COMMISSION

Brussels, 4.6.2012
SWD(2012) 135 final

COMMISSION STAFF WORKING PAPER

IMPACT ASSESSMENT

Accompanying the proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on

electronic identification and trust services for electronic transactions in the internal market

{COM(2012) 238 final}
{SWD(2012) 136 final}

TABLE OF CONTENTS

COMMISSION STAFF WORKING PAPER

IMPACT ASSESSMENT

Accompanying the proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on

electronic identification and trust services for electronic transactions in the internal market

List of Annexes

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

Proposal for a
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on electronic identification and trust services for electronic transactions in the internal market

PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

Identification

Lead DG: Information Society and Media Directorate-General

Agenda Planning: 2012/INFSO/002

1. INTRODUCTION

This report assesses the impact of policy options for a European legal framework for cross-border recognition and interoperability of electronic Identification, Authentication, Signature and electronic related trust services (referred to as 'elAS services'). The objective is to enable secure and seamless electronic interactions between businesses, citizens and public authorities, thereby increasing the effectiveness of public and private online services and electronic commerce in the EU, thus creating trust in electronic transactions in the internal market.

This initiative is a step further to the development of a digital single market from which citizens, businesses and public authorities could fully benefit and for the fostering of a European citizenship, which are both essential to improve the functioning of the internal market in the digital age. The framework builds on the revision of Directive 1999/93/EC on a *community framework for electronic signatures* ("e-signature Directive").

This report analyses alternative policy scenarios by assessing how they would help to overcome current obstacles to eIAS. The impact of these options on consumers/citizens, the private sector and public administrations will be considered.

This document does not pre-judge the final form of any decision to be taken by the European Commission.

1.1. Electronic identification, authentication and signatures - key elements for electronic interactions and the Digital Single Market

Easy to use and reliable eIAS can create **user convenience and trust and confidence**, thereby facilitating a **full 'European citizenship' in the digital single market and favouring electronic business transactions.**

At the same time, a well regulated and operational Digital Single Market is an incentive for the accelerated development of online services, at national and cross-border level, which in turn will favour the development of the knowledge economy, generating potential favourable impacts on economic growth and the creation of jobs.

Nonetheless, still existing barriers to the cross-border access of online services need to be eliminated to fully reap these economic and social benefits of the Digital Single Market. **In order to be productive enablers, rather than barriers to cross border services, electronic identification, authentication and signatures need to be mutually recognised and accepted throughout the EU.**

E-identification, e-authentication and e-signatures are the electronic equivalent of personal identification, validation of personal identification and integrity of documents and handwritten signatures respectively. In simple terms, they perform the same functions in an electronic environment as in the paper world: a person provides his/her name (identification) and proves (e.g. by showing a passport or identity card) the correctness of the data provided (authentication). Currently only an e-signature has been formally defined at the European level, as *"data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication"*[1].

Collectively, eIAS services serve as a basic 'trust ecosystem', that allows participants in the digital society to communicate and engage in transactions with the necessary confidence in electronic claims, in particular when a high degree of certainty and security is required. **As such, eIAS services are crucial to citizens, businesses and public administrations in enabling the transition from a largely physical and paper based society to a European citizenship in the digital world, where reliable, trustworthy and seamless alternatives are available.**

1.2. Policy context of electronic identification, authentication and signatures

The Single Market Act (SMA)[2] stresses the need for boosting confidence in electronic transactions and restates the objective "to make secure, seamless electronic interaction possible between businesses, citizens and public authorities, thereby increasing the effectiveness of public services and procurement, service provision and electronic commerce (including the cross-border dimension)".

The Digital Agenda for Europe[3] (DAE) identifies existing barriers to Europe's digital development and proposes legislation on e-signatures (Key Action 3) and the mutual recognition of e-identification and authentication (Key Action 16), establishing a clear legal framework eliminating fragmentation and the lack of interoperability, enhancing digital citizenship and preventing cybercrime.

[1] Article 2 of e-signature Directive

[2] COM(2011) 206 final of 13.4.2011

[3] COM(2010) 245 of 19.05.2010

The Roadmap for Stability and Growth[4] underlines the key role of the future common legal basis for mutual recognition and acceptance of eIAS across borders for the development of the digital economy.

1.3. External expertise and consultation of interested parties

The Commission has collected feedback from Member States, the European Parliament and stakeholders during discussions, workshops and conferences. The Commission launched a number of studies in relation to eIAS (see Annex 3) and assessed available literature published by third parties.

A wide **online public consultation** on eIAS was launched from 18.2.2011 to 15.4.2011 with a view to provide input for policymakers on how eIAS can contribute to delivering the European Digital Single Market[5]. The on-line questionnaire was accessible through the "Your Voice" website. The consultation was complemented by a "SME Test Panel" to identify the specific views and needs of SMEs[6].

1.4. Commission inter-service consultation and Impact Assessment Board process

To support the preparation and drafting of this impact assessment, a Commission inter-service steering group was established. Given the overarching nature of the subject, all Commission Services were invited to participate. The group met three times.

On 2 March 2012, the Impact Assessment Board (IAB) asked DG INFSO to submit a revised version of the report. Following the IAB examination and in line with the Board's comments and recommendations, the following modifications were made to the report: (a) the final impact assessment report provides now an structured presentation of the problems; (b) the policy options are presented more clearly; (c) the report provides a narrower analysis of impacts and comparison of the options; (d) the views of stakeholders are clearer distinguished and monitoring and evaluation arrangements defined. In line with the suggestions of the Board, the report respects the recommended presentation standards set out in the IA guidelines and refrains from advance conclusions on the preferred option.

2. IDENTIFICATION AND ASSESSMENT (DEFINITION) OF THE PROBLEM

This chapter identifies and describes the problems at stake.

2.1. Introduction

Increasing mobility and flexibility of citizens and businesses within the internal market together with the technological transition to digital economies and administrations show the need for secure and trustworthy cross-border online services that are accessible without creating new electronic barriers. The examples below should illustrate the **main difficulties citizens and businesses encounter today when it comes to the cross-border use of eIAS services**.

Examples

- Elisa, a Belgian student, wants to enrol in a university in Italy. She logs in to the university website and discovers that she cannot use her Belgian electronic identification when she is asked to identify herself. The reason is simple: her Belgium eID is neither recognised nor

[4] COM(2011)669, 12.10.2011

[5] See http://ec.europa.eu/information_society/policy/e-signature/eu_legislation/revision/pub_cons

[6] See http://ec.europa.eu/information_society/policy/e-signature/eu_legislation/revision.

accepted in Italy. Elisa then has to buy a train ticket to Italy and to queue up to do the necessary paperwork in person which involves an unnecessary waste of time and money.

- A SME based in Hungary wants to participate electronically to a public call for tenders launched by the Portuguese administration but because of specific national requirements and interoperability problems the electronic signature is denied. As a result, it will need to submit a bid on paper, which implies additional administrative burdens and costs for the company (printing of multiple copies and sending them by courier) and, hence, impair its competitiveness compared to Portuguese competitors.

- An international company based in France wants to sign contracts electronically with a counterpart based in Latvia. This is technically possible, but the legal requirements for trust services such as electronic seals, electronic documents, time stamping, etc. differ. The French multinational company will need to perform a very expensive exercise to assess whether it is legally possible to use electronic documents and processes.

- An notice of default must be delivered from Estonia to Germany. The Estonian sender would like to use an electronic document, but is this legally valid under Estonian and German law? He will need to examine the applicable laws in both countries, and in case of ambiguities will likely opt for paper mail.

In the sections below, we will identify the specific problems concerning the secure and seamless cross-border use of electronic identification, authentication and signatures encountered by the different stakeholders, describe possible solutions and explain the consequences of the lack of a common European framework regulating eIAS.

2.2. Lack of a common framework for electronic interactions and main problems

eIAS services are pre-requisites for a wide range of electronic interactions such as e-banking, e-government or e-health services. A regulatory framework has been set up at EU level for electronic signatures, but there is no specific framework for mutual recognition and acceptance of elD and e-authentication, or for related trust services such as the time stamping, long-term preservation of e-signatures or registered document delivery services.

PROBLEM 1: FRAGMENTATION OF THE MARKET

a) e-signatures

With respect to **e-signatures** the CROBIES[7] Study has demonstrated that the European **harmonisation brought about by the e-signatures Directive** is imperfect and incomplete, resulting in market fragmentation. The major problems identified are:

(1) Divergent national implementations due to different interpretations by MS of the current Directive[8] leading to cross-border interoperability problems and thus to a segmented EU landscape and distortions in the internal market[9];

(2) A *de facto* usage of the "public sector clause" of the Directive[10] to justify additional requirements for the use of electronic signatures in the public sector. As a result, the

---

7 Study on Cross-Border Interoperability of e-signatures, see http://ec.europa.eu/information_society/policy/e-signature/crobies_study/index_en.htm

8 An interesting example of divergent implementations is illustrated by the introduction of new categories of signature in the different national regulatory frameworks, such as the "universal electronic signature" in Bulgaria, the "secure e-signature" in Lithuania and Poland, the RGS differentiation of "middle, standard or strengthened e-signature" in France or the "guaranteed electronic signature" in Slovakia. While a purely terminological issue, one might see how the introduction of new categories of signatures on a national basis holds a risk of creating market confusion. Indeed, as noted in the IDABC study on the Study on the Mutual Recognition of eSignatures (2009) and pointed out in a position paper delivered by Chambersign in Octor 2010, the lack of a common terminology on the one hand confuses end-users and complicates the communication strategy of CSPs that have to customise their services; on the other, it is often unreasonably complex and costly to determine whether a foreign signature meets the requirement of the national framework.

9 As a basic foundation of the Directive, internal market rules have been implemented via article 4 . CSPs are thus largely governed by a country-of-origin rule. This ensures, on the one hand that they do not need to comply with 27 materially different sets of rules if they choose to operate in all 27 MS, but on the other, it provides for a segmented EU landscape.

10 Article 3.7 of the e-signature Directive allows Member States to impose additional requirements to the ones laid down in the Directive under certain conditions such as "such requirement may not constitute an obstacle to cross border services for citizens". Although not formally notified to the European Commission, a significant number of Member States apply this clause. They use (voluntary) accreditation schemes to determine the accessibility of an e-signature in an e-government application or their legal framework contains requirements that cannot be met by foreign solutions. Being excluded from such application hinders significantly the penetration of a market because the signature is not considered as universally usable.

Commission is unable to undertake actions when eSignatures barriers are created or maintained by the Member States in the public sector, as they can be justified on the basis of the public sector clause. Thus, interoperability challenges within the EU public sector can remain, contrary to the goals of the Directive[11];

(3) Outdated standards leading to a highly complex EU standardisation framework. Standards are no longer in line with current market expectations, e.g. the use of mobile phones[12] or highly secure remote signing technologies[13] are increasingly popular in the European e-signature market, but they are not clearly addressed by the European framework[14]:

(4) Trust in e-signatures depends to some extent on national supervision[15]. The Directive is vague on supervision obligations, leading to a lack of trust as the effectiveness of supervision regimes is unclear, and creating market distortions for service providers who need to meet different standards depending on their country of establishment[16].

b) Electronic identification

The usage of electronic identification is most often limited to the access of national online services and interactions, i.e. an eID issued in one MS cannot be used to access online services in a different Member State. The reasons are of technical and legal nature:

(1) Member States use different technological solutions for personal identification which lead to interoperability problems when it comes to cross-border interaction.

(2) There is no framework of reference for determining the reliability of the entity that issued the eID, the legal certainty on the cross-border use of eIDs and a clear liability for the correctness of the ID when it is used as electronic representation of a person.

---

11 The Study on Electronic Signatures as Obstacle for Cross-Border e-procurement in Europe - Lessons from the PROCURE-project (2009) has for example highlighted that certain MS, in clear violation of the public sector clause of the Directive, have enacted at least three additional requirements which constitute an obstacle for cross-border e-procurement, i.e. conflicting requirements regarding the type of electronic signatures allowed; the requirements for accreditation and the requirement for unequivocal identification of the signatory in form of unique national specific person identifiers.

12 When signing calculations are done on a server (vs done in the SIM card of the mobile phone).

13 E.g. through Hardware Security Modules (HSM).

14 E-signatures require a minimum common technical framework to ensure their operation (for "qualified" signatures). This technical framework is provided through a fairly high level set of requirements in its four annexes. The Directive also incorporates a trust infrastructure to support certification service providers through the concepts of supervision, conformity determinations and accreditation. The Annexes do not provide – on purpose - guidance for specific implementation or assessment activities, as they are too generic for that aim but additional guidance were provided through two Commission Decisions 2000/709/EC and 2003/511/EC. However, Commission Decision 2003/511/EC only references three specific standards on signature hardware out of a set of 30 e-signature standards. The fact that the Directive can only create a presumption of compliance with the requirements of Annex II(f) and Annex III of Directive 1999/93/EC via this Decision, and not with other requirements, makes it impossible to provide a formal value to the other standards. Furthermore, the standards referred to in Decision 2003/511/EC – namely CEN CWA 14169 and CWA 14167 - are obsolete and do not unambiguously apply to some new e-signature creation scenarios. For instance, the use of mobile telephones is increasingly popular in the signature market or the usage of "hardware security modules" for mass signatures.
NB. CEN is currently working on these two standards and plans to deliver updated and upgraded versions by mid 2012. Decision 2003/511/EC is therefore expected to be updated in 2013 still within the scope of Directive 1999/93/EC comitology.

15 Art. 3.3 of the e-signature directive, "*Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification service-providers which are established on its territory and issue qualified certificates to the public*". Article 2.13 of the directive: *" 'voluntary accreditation' means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification- service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.* "

16 As a pragmatic example: an analysis of Member State supervision practices shows that the frequency with wich service providers are audited by the supervisory bodies varies widely. 17 Member States are known to organise periodic audits to re-assess compliance with the Directive and national transposing acts. Of these, 11 organise annual audits (DK, EE, LV, LT, LU, HU, NL, PL, PT, SK, UK). The 6 other Member States organise them every 1.5 years (IT), 2 years (AT, MT), 3 years (BE, ES), or 4 years (CY). Of the 10 Member States without known periodic audits, there is either no data available, or a regimen of audits only in cases of incidents or suspicion of non-compliance. Thus, in practice the supervision regime results in an uneven playing field, both with respect to trustworthiness (some providers are audited annually, some not at all), and with respect to costs, as audits will incur expenses for the service provider

The consequences are discrimination of non nationals and their exclusion to the access to online services. Evidence of the effect of electronic barriers is provided in the context of the implementation of the Services Directive[17]. According to Article 8 of the Services Directive, Member States are obliged to enable service providers who want to establish or exercise a business in another Member States to complete certain administrative procedures through Points of Single Contact, i.e. websites which act as one-stop-shops for this purpose. This implies that Member States need to provide online services that allow service providers to electronically interact with public authorities. In cross border scenarios, this is highly complicated due to the missing link of mutual recognition and acceptance of electronic means of identification (including specifically official eIDs) throughout the EU. Exchanging electronically signed documents will be equally difficult due to a lack of interoperability.

Example

An Austrian citizen moving to Portugal wants to change his address. The website of the local community where he wants to live asks him to insert the eID card into his card reader. The Austrian citizen however has no Portuguese eID card but an Austrian mobile-ID, and the Portuguese commune cannot recognise, accept or validate the Austrian mobile-ID. The Austrian citizen will have to go to the city hall in person to change the address.

c) Related trust services

With respect to **related trust services**, the lack of a common European framework has led to:

(3) The adoption of national rules for some of these services in some Member States[18] resulting in potential internal market barriers);

(4) high costs for those service providers who want to offer their services in other Member States due to the fact that they need to ensure technical compliance with the rules of the country of destination and obtain guarantees with respect to trustworthiness of foreign eIAS tools.

European companies providing **related trust services** are unable to offer their services in other Member States without incurring in extra costs. Today, conditions are clearly not favourable for dedicated suppliers of eServices and products in the eIAS market[19].

Example

The Austrian eSignature Ordinance[20] specifies requirements for qualified time stamping services, including technical parameters and algorithms which must be used. In contrast, the Romanian Decision no.896 of 2 October 2008[21] has its own and different set of standards and norms for time stamping. If time stamping service providers from other Member States want to ensure the validity of their services for clients in Austria and Romania, they will have to satisfy contradictory requirements. This is a clear market barrier for this related trust service.

PROBLEM 2: LACK OF TRUST AND CONFIDENCE

One of the current barriers impeding European citizens to benefit from the same kind of services in the digital world as in the physical world is the **lack of trust and confidence in**

---

17 Directive 2006/123/EC of 12 December 2006 on services in the internal market

18 The ongoing IAS. Study on an electronic identification, authentication and signature policy (IAS) - IAS in the European policy context, 28 September 2011, highlighted at least ten Member States who had adopted national laws in relation to one or more ancillary services; see www.iasproject.eu/attachments/File/deliverables/IAS_Deliverable_D1_%28version_3_28_sept2011%29.pdf, p. 61 and following.

19 Indeed, trust service providers for example currently do not even try to perform activities outside of their country of establishment in significant numbers.

20 See http://www.signatur.rtr.at/en/legal/sigv.html

21 See www.glin.gov/download.action?fulltextId=196944&documentId=215798&glinID=215798 for the full version in Romanian

electronic systems[22]**, the tools provided and the legal framework**, e.g. a feeling of absent legal safeguards in comparison to physical interactions.

The SME Test Panel replies on e-signature and eID shows that only 11% of SMEs use e-signatures in the context of cross-border transactions. The **lack of common trust enhancing rules** for eIAS was clearly mentioned as a barrier to the cross border use[23]. This is also confirmed by the public consultation[24].

For **e-signature**, the requirements that aim to ensure an adequate security level for e-Signature services provided for in Directive 99/93/EC are somehow weakened, as detailed by the "CROBIES" study[25]. For example, as already mentioned under problem 1, **national supervision requirements are qualitatively very different** from MS to MS, ranging from a simple notification letter of the certification service provider to the supervisory body to full and periodically recurring audits. This makes it very complex for relying parties to assess how effectively a service provider is supervised.

For **eID and related trust services**, the lack of a common European legal framework does not enable citizens, businesses and administrations to feel secure when interacting online in cross border scenarios.

In particular for eID and in the context of eGovernment, a major concern is a '**trust tension**'[26] between the need to collect data on individuals as the basis for providing services, such as electronic health records and voter registration, and fears of data surveillance or the inappropriate secondary use of personal information in computer databases. eGovernment raises indeed particular trust concerns as a number of public services require the handling of personal data in digital forms[27]. It is therefore of the utmost importance that access to personal data is highly secured with advanced authentication and identification procedures for end users to feel confident.

2.3. The drivers behind the identified problems

The main drivers behind the two identified problems are the following:

Driver 1: Insufficient scope of the current legal framework

The current framework on e-Signatures covers only one of the eIAS-components which are necessary for the ecosystem of certification services. Hence, **legal uncertainty leading to a lack of trust (problem 2) and new market distortions (problem 1) will inevitably arise, in particular for the mutual recognition and acceptance of eIDs and related trust services**.

The narrow scope of the eSignature Directive results in a patchwork of different national rules for electronic identification, authentication and related trust services leading to distortions of the internal market[28]: although an related trust service provider is allowed to provide services

---

22 As recurrently indicated by surveys (ex. Eurobarometer 250, 2009; Eurostat household survey 2010, IDC ICT security market study, 2008).

23 36% out of 57% indicated that they could be incentivised to use an e-Signature abroad if it was less burdensome or clear rules about the validity of e-Signature were in place, in particular in the cross-border context (See answers to questions 15 and 16 of SME Test Panel)

24 The lack of trust in cross border applications of e-signatures and ancillary trusted services was also confirmed by 28% of respondents to the public consultation

25 Also confirmed by the Action Plan on eSignatures and eID, 2008

26 Guerra et al 2003

27 A Legal and Institutional Analysis of Barriers to eGovernment, Modinis Study, 2007

28

a) Austria, as one of the leading EU Member States in this area, has implemented legislation regulating not only e-signatures, but also electronic identification, through the 2004 eGovernment Act. - E-Government-Gesetz.

in other Member States, it cannot provide guarantees with respect to the legal value of its services. Worse yet, national legislation may be contradictory between countries, meaning that a service provider would at the very least need to modify its service offering on a per country basis. De facto, this is a significant disruption of the eIAS market in Europe. Legal certainty offered by a single Member State is not sufficient for the take up of the digital economy. The functioning of the Digital Single Market will depend from the capability to enable the cross-border use of eIAS.

Example

The Italian Decree of 11 February 2005, nr. 6810[29] establishes rules for electronic registered mail, including references to mandatory technical requirements. Service providers offering electronic registered mail services in other countries would need to satisfy these requirements in order to be legally considered as equivalent to registered mail in Italy. Most likely, service providers in France would not meet this bar, even if they comply with their own legal requirements under Article 1369-8 of the French Civil Code and the executive Decree of 2 February 2011 (n° 2011-144)[30].

Driver 2: Lack of coordination between eSignature and eID developments

National eIAS infrastructures and systems were developed in isolation without coordination at European level[31]. On the one hand, the result of these different approaches is the **absence of cross-border interoperability** of technical solutions which creates **barriers to the operational achievement of electronic transactions (problem 1)**. On the other, **the lack of mutual recognition and acceptance** is one of the main reasons why **both users and providers of online services are sceptical about the deployment of eIAS** (problem 2).

With regard to **eSignatures**, the existing Directive foresees mutual recognition rules of qualified certificates. However, due to the aforementioned problem in the Directive (diverging national implementations of eSignature systems, Member States often dismissing foreign signatures in public sector applications), mutual recognition and acceptance of eSignatures remains problematic in practice.

---

b) Belgium adopted a generic legal framework for certain trust services in 2007, including electronic registered mail, time stamping and electronic archiving. Despite a recent update for the rules on electronic registered mail in 2010 (integrated into the general e-signatures Act), executive rules were never fixed, and the law remains largely inoperative at present. However, new legislation in this area is planned for the near future. - Wet van 15 mei 2007 tot vaststelling van een juridisch kader voor sommige verleners van vertrouwensdiensten/ Loi du 15 mai 2007 fixant un cadre juridique pour certains prestataires de services de confiance

c) The Czech Republic has implemented rules for time stamping in its e-signatures Act of 2000. - Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

d) Estonia, as another technology leader in the EU, has a legal framework that supports (and indeed requires) time stamping, digital stamps, and official e-mails.- Digitaalallkirja seadus, RT I 2000, 26, 150.

e) Similarly, Finland has adopted an Act on strong electronic identification and electronic signatures. - Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista, 7.8.2009/617.

f) Germany likewise introduced the notion of qualified time stamping in its e-signatures Act. - Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) vom 16.5.2001 (BGBl. I S. 876).

g) Italian law contains rules on electronic registered mail. - Through the Codice dell'Amministrazione Digitale (the current version is Decreto Legislativo 30 dicembre 2010, n. 235); Roberta Falciai and Laura Liberati, 'The Italian certified e-mail system', *Digital Evidence and Electronic Signature Law Review, 3 (2006) 50 – 54.*

h) The Slovakian e-signatures Act contains specific rules for time stamping. - Zákon č.215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov –The Slovakian Act ('as amended' or 'v znení neskorších predpisov') was consolidated in 2009 (§9 of this Act still explicitly refers to time stamping (Časová pečiatka – time stamping)), see http://www.zbierka.sk/zz/predpisy/default.aspx?PredpisID=208862&FileName=zz2009-00076-0208862&Rocnik=2009.

i) The Slovenian e-signatures Act recognises the concept of a time stamp as being comparable to advanced e-signatures, with the same rules applying mutatis mutandis; - Zakon o elektronskem poslovanju in elektronskem podpisu.

j) Finally, the Spanish Act on Electronic Citizen Access to Public Services recognises e-signatures, e-seals (company signatures), and time stamping. - Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

NB. This listing is not exhaustive.

29 See http://www.digitpa.gov.it/sites/default/files/normativa/DPR_11-feb-2005_n.68.pdf

30 See http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023513151&categorieLien=id

31 Notwithstanding some coordinating effect of the "European E-Signature Standardisation Initiative" (EESSI, www.ictsb.org/Working_Groups/EESSI) and via the *Forum of European Supervision Authorities* (FESA, www.fesa.eu).

With regard to **electronic identification**, what is missing today is the possibility of citizens and businesses to use their "official eIDs"[32] throughout the EU when they need to interact electronically with public administrations of other Member States in cases they e.g. want to move, travel, study, work or do business abroad. The lack of commonly agreed legal provisions allowing for mutual recognition and acceptance of each others' "official eIDs" makes it **currently almost impossible for citizens and businesses to access cross-border online services of other Member States when they need to identify themselves electronically**. They are cut out of these services due to the fact that almost no MS foresees the use of other MS' "official eID" in their online processes or their mutual recognition and acceptance[33].

Besides this cross-border dimension, there is also a "cross-sector" dimension: eIDs can be issued by private or public sector parties, and/or their use may be specific to a sector, such as social security, e-payment or eHealth. In both cases, the absence of a general framework for eID recognition and acceptance makes it hard to use an eID outside of its context, mainly because of liability and data protection challenges.

With respect to liability, the primary issue is that eIDs are made available under a set of guarantees and warranties that are appropriate for the use in a specific context. Bank issued eIDs will have liability limitations (e.g. a 'liability cap' limiting the liability of the issuer to an amount of 5.000 EUR) which are appropriate for use in banking applications. However, these may be insufficient for cross-sector us: a liability cap of 5.000 EUR might be inappropriate for a public procurement application in which bids with a value of millions of EUR could be submitted. With respect to data protection, the challenge relates to ensuring that personal data is not made needlessly available to third parties. An eHealth card may e.g. contain health information, or information on the social insurance scheme of the holder. It would not be appropriate for this information to be made available to any recipient that does not require it (e.g. when using the card in an e-tax application). Therefore, clear rules are needed to determine which data can be share in cross-sector applications, and to what extent.

Example

A study[34] showed the **important role of the private sector** in some Member States, noting that "13 out of 32 surveyed countries are deploying government supported eID cards, including however a group of six countries relying on eID cards issued by private operators with a public sector mandate (Austria, Iceland, Liechtenstein, Luxembourg, the Netherlands and Sweden); in the seven others eID cards are issued by public bodies (Belgium, Estonia, Finland, Italy, Lithuania, Portugal and Spain)." The same study also examined **sector specific** eIDs, identifying eHealth and social security eID cards in 6 countries (Belgium, Croatia, Denmark, France, Italy and Poland); and noting that **identification numbers were subject to legal usage restrictions in 20 out of 32 examined countries to minimise privacy risks**.

---

32 eID issued by or on behalf of a Member State.

33 Example: The Large Scale Pilot STORK shows how citizenship in the Digital Single Market could work (www.eid-stork.eu).
STORK implements a European wide eID interoperability platform that enables citizens, businesses and civil servants to use their national electronic identities in any participating Member State for certain public eGovernment services. The pilot-micro-environment served as "playing ground" to settle the challenges of a future EU-wide eID-infrastructure as envisaged in the Connecting Europe Facility proposal by the Commission.
The following real time use cases show the wide range of beneficiaries of "official eIDs" and secure authentication:
"Safer Chat" enables children and young people to build a platform for a safer online environment. The key to enter the room is the age of the chat user provided through "official eID". No further identity data are needed. Exactly one of the problems the online gambling sector faces today (see chapter 5).
Foreign students get access with their "official eIDs" to any online administrative service offered by universities through the "Student Mobility" pilot. Beneficiaries of this pilot are in particular Erasmus students which represent a population of around 230.000 per year.
The "change of address pilot" addresses the situation of moving to another country. The communication is made via the use of the "official eID".
"ECAS integration" is piloted by the Member States together with the Commission which operates the ECAS system. It enables the secure login of national experts to the CIRCA-network through the use of "official eIDs".
The few examples gives a flavour of the variety of application areas and beneficiaries - public as well as private - which could profit from the use of "official eIDs" and authentication

34 eID Interoperability for PEGS study, 2009, see http://ec.europa.eu/idabc/servlets/Doc2ba1.pdf?id=32521

Both the cross-border and cross-sector dimensions share the same general challenge, i.e. allowing electronic information to be used outside of its original context (with that original context being either a specific country, or a specific sector, or both (a sector within a country).

EU-wide mutual recognition and acceptance of electronic identification and authentication is vital to **ensure the scalability and sustainability of eIAS** which depends on the volume of cross-border services accessible without barriers and discrimination.

Driver 3: Lack of understanding of security guarantees

The e-signatures Directive recognised that legal certainty can only be attached to electronic signatures that offer high security guarantees, and are thus sufficiently protected against forgery or fraud. To this end, the Directive introduced a category of e-signatures referred to as 'advanced signatures', which, under the current state of the art, require the use of cryptographic algorithms. If the processes and devices used to create such advanced e-signatures meet clear security requirements[35], then the Directive guarantees to these e-signatures the same legal effect as handwritten signatures. This highly secure type of e-signature is commonly referred to as a 'qualified e-signature'.

It is of course not possible to eliminate all security risks:

- a person might give his or her smartcard and signature PIN to a third party. This is like giving a signed blank check to somebody or to sign a blank page.
- similarly, the use of highly secure devices such as smart cards does not guarantee that there is no virus on the PC of the signatory that could try to corrupt the signing process. A virus could sign changed or additional documents after the signatory enters his or her PIN-code, in addition to (or instead of) the document the signatory wanted to sign.
- In much the same way, corrupted or badly designed signing software might not display faithfully what is to be signed to the signatory.

To date, **there is no report that any qualified e-signature was ever forged**. Furthermore, some manufacturers offer today fully autonomous external devices (e.g. in the form of USB-drives) that can perform all the computing operations required to create a qualified signature, without dependence on additional software including to ensure a proper display of the data to be signed on the PC screen. Thus, security guarantees are still continuously improving.

> What the above highlights, is that high and harmonised security requirements are essential to create trustworthy solutions (problem 2). This is particularly relevant for the access to services where sensitive personal data are involved, such as eJustice, eGovernment and eHealth.
>
> **The lack of secure electronic identification and authentication systems** is perceived by users of online services as an important or very important barrier[36]. The traditional userID / password systems used for accessing online services are often not sufficient for public administrations, since they need to establish exactly who is asking for a specific service and whether it is indeed the person he claims to be, in order to deliver the requested service.

---

[35] Specifically, the advanced signatures must be based on qualified signature certificates (which have stringent procedural and technical requirements behind them), and must be created using a secure signature creation device, such as highly secured smart cards. With this combination of tools, qualified e-signatures offer a very high degree of protection against forgery and fraud.

[36] Confirmed by 64% of project survey participants in the context of the Modinis study (cf footnote 38)

To overcome the **difficulty of identifying a person in an unambiguous manner**, Member States have progressively introduced "official eIDs" in recent years, which in many countries are embedded on ID cards (e.g. BE, EE, DE, PT, ES); in others they are designed as citizen cards or mobile-ID used simply to access public online services (e.g. AT)[37]. Yet, the **lack of a harmonised legal framework means that the security and reliability of "official eIDs" cannot be objectively determined across borders.** This creates cross-border barriers thereby leading to a **lack of trust** (problem 2) and a **fragmented market** (problem 1).

Another main concern with regard to **electronic identification and authentication** is related to the potential of online theft and fraud[38]. Secure eIDs can help reduce this risk, by combining state of the art cryptography with common security practices such as private PIN-codes or passwords. Inversely, badly secured eIDs can increase the risk of identity theft by making it easier for criminals to obtain false or compromised eIDs.

Example

National eID cards commonly base their security policies on the best practices pioneered by the financial sector to reduce fraud risks. The Belgian national eID card has a limited duration of five years (shorter than the paper card which it replaced), operates using a PIN-code only known by the citizen, and can be revoked if a card is stolen or lost. Like a bank card, the card blocks itself automatically after three unsuccessful usage attempts. Revocations are published online (https://www.checkdoc.be/CheckDoc/), and revoked cards cannot be successfully used for electronic identification or electronic signatures. An online card-stop website and phone number are available to citizens and the police to immediately block lost or stolen cards (https://www.docstop.be/DocStop/).

Currently, the EU has no common practices that would help citizens, businesses and administrations make the distinction between secure and insecure eIDs. As they can only trust eIDs that they know in detail, this leads to fragmentation (problem 1) and lack of trust (problem 2).

Driver 4: Lack of awareness and user adoption

The complexity behind the technologies used in online transactions and the key role played by trusted third parties result in an environment where it is difficult to assess trust (problem 2). Particularly **end users (citizens and SMEs)** who generally do not have sufficient expertise must be able to rely on rules which establish clear rights and responsibilities of all stakeholders (online service providers, end users and governance bodies such as supervisory authorities).

Concerning the market demand for trust enablers (eIAS services) and related trust services, the public consultation demonstrated that different stakeholder groups (users, policy makers, industry, businesses) are not fully aware of the added value of eIAS[39] to secure online transactions. The SME Panel showed a similar result[40], which becomes less significant as soon as the use of electronic applications in general is assessed[41].

---

37 The problem of unambiguous identification of a person is solved by the official eID which links certain person data (e.g. name, date of birth) to a person identifier assigned to a person (e.g tax number derived from the tax register, number derived from the population register or residence register). This mechanism makes it possible to distinguish clearly each single individual from one another. Especially in cases of common family names (e.g. John Smith) it is important for the administration to establish to which John Smith.
The 2 basic conditions to get the official eID are the following:
- the person presents him/herself physically to the authority which issues the official eID (or the entity which does it on behalf or the responsibility of the authority);
- the authority checks and verifies the identity document demonstrated by the person.

38 Considered an important or very important barrier by 62% of survey participants in the context of the Modinis study (op. cit.)

39 Respondents that do not use eIAS indicated as major reasons of their reluctance the absence need (32%) followed by complexity (15%) and costs (14%).

40 16% of SMEs indicated that they do not need electronic signatures for their business.

41 Although in most of these application areas electronic solutions are deployed to ensure at least a minimum level of security for online transaction, the direct demand for more reliable eIAS mechanisms is less apparent. The fact that online payments are used by a significant number of SMEs (roughly two thirds of them) may be explained by the fact that e-payment transactions are

2.4. Who is affected and to what extent?

The following players of the eIAS market are the main stakeholders affected by the problems identified:

On the supply side, **eIAS service or solution providers** mainly suffer from the fragmented market (diverging national rules and standards) which leads to barriers to enter other European markets and hamper the deployment of cross-border/cross-sector services.

On the demand side, the lack of trust:

- prevents **the public sector** from moving towards modernisation, cost effectiveness and re-organisation in view to delivering faster high quality services with less resource consumption (i.e. reduction of administrative burden);

- limits the market for **the private sector**, i.e. the European providers of such services, as the legal value of their services may vary from MS to MS;

- reduces confidence and ease of use for **end users** who lose the potential benefits that eIAS offer (especially in cross border scenarios)**.**

For an extended overview of the difficulties encountered by each of the stakeholders and the interest in the revision of the framework, please refer to Annex 7

2.5. Baseline scenario - how would the problem evolve, all things being equal?

Technological advances are likely to increasingly threaten Internet security jeopardising the trust and confidence of users in electronic systems, tools and legal framework.

Example

The UK National Fraud Authority estimates that in the UK alone, identity fraud is estimated to cost victims around £1.9 billion a year (approx €2.3 billion), or some €36 per capita. As noted in the report, "if the costs of responding to and dealing with identity fraud are taken into consideration, it is estimated that the real cost of identity fraud is at least £2.7 billion a year"[42], or €3.2 billion in total or some €52 per capita. Extrapolated across the EU and assuming equal prevalence and cost, this would amount to an estimated total cost over €26 billion.

The extent and seriousness of the problems identified under section 2.2 are therefore also expected to increase. Without further regulatory intervention, it is anticipated that under the baseline scenario the problems in the current situation would evolve as follows:

Fragmentation, interoperability problems not solved

Member States are likely to continue to implement and enforce the eSignatures Directive in a diverging manner, including by regulating other services than eSignatures as shown in the examples above, leading to interoperability challenges and market fragmentation. As further EU integration and globalisation is expected to result in an increase in the numbers of businesses operating in more than one Member State and of citizens performing electronic transactions beyond national borders, this will become an increasingly greater burden to the mobility of citizens and businesses.

Legal certainty not ensured

The problems driven by the lack of mutual recognition of electronic signatures and by the absence of a legal framework regulating eID and related trust services would impede the legal

carried out in a closed environment, namely the system operated by the bank. Other services show significantly lower numbers, as they inherently require interaction with third parties outside of such a controlled environment.

[42] See www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/annual-fraud-indicator/annual-fraud-indicator-2011?view=Binary

recognition of a range of cross-border interactions. If no common legal framework exists, cross border scenarios would be avoided due to reasonable doubts over the legal value of key services in other Member States.

The components required to ensure a legally-proof (irrefutable in front of the Court) interaction like, e.g. the time (time stamping) or the identification and authentication of participants (eID) would still be missing. Without certainty on the legal validity of transactions, take-up of the use of electronic interactions would not increase.

Users' needs not fully satisfied

Technological developments are a key factor in increasing the demand for services by improving user friendliness. An emerging signature model which is likely to become very popular is the "*remote signature*" where the cryptographic operations are executed on a secure server (called HSM or Hardware Security Module) of a service provider instead of the equipment of the signatory – but still under the control of the signatory. This includes mobile eSignatures (when signing is not performed on the SIM card of the smart phones or tablets) and mass signature for instance of invoices or contract of a phone company. Remote signature is excluded by the current framework.

Leading European (policy) initiatives not fully leveraged

Recent European policy initiatives which have endeavoured to eliminate interoperability challenges and cross border recognition and acceptance issues related to certain types of electronic interactions will be handicapped by the lack of an appropriate cross-sector legislative framework.

Examples

1. The Services Directive

As noted above, Member States are obliged to implement Points of Single Contact which must be accessible to service providers across the EU. In reality, cross-border electronic interactions are in most cases currently not possible since the existing eIDs are only accepted in the country in which they are issued. Similar challenges are encountered with respect to e-signatures (where the legal framework for mutual recognition only covers a small category of e-signatures[43]), and for the communication of e-documents (which is often impossible if e-documents are not accepted).

Considering the wide range of service categories covered by the Services Directive and that the fact that the services sector represents around 70% of GDP and employment in the EU, the potential savings missed due to an insufficient legal framework are significant.

2. Roll-out of services building on the results of large scale pilot projects

Several large scale pilots (LSPs) have been put in place at the EU level in recent years to support the development of interoperable and trustworthy means of electronic communication (including SPOCS, supporting the implementation of the Services Directive; STORK, supporting the development and use of interoperable eIDs; PEPPOL, supporting the development and use of interoperable eProcurement solutions; epSOS, supporting the development and use of interoperable eHealth solutions; eCodex, supporting the development and use of interoperable eJustice solutions.)

Each of these LSPs represents a multi-million euro investment from participating Member States and the European Union. These investments have yielded a significant number of useful and functioning components to support the use of eIAS services (e.g. e-signature validation services, eID/eAuthentication components, quality assurance policies, secure document storage and exchange facilities, etc.). The participation of Member States in these initiatives shows that there is a clear interest in using the results in operational public eGovernment services. However, the policy framework (including legislation) to do so is currently missing at the European level. This means that the outputs of these LSPs have no formal status: there are mere project deliverables. As a result, the investments made in the LSPs cannot be effectively monetized.

By way of example: the STORK pilot represents an investment of €20 million, 50% of which was funded by the European Commission[44]. It has piloted working and successful eID interoperability solutions, allowing citizens from one Member State to use their eIDs in applications managed by other Member States. However, as there is no legal framework covering eIDs (regulating the responsibilities and liabilities of service providers and the rights of end users such as businesses and citizens), project results cannot be taken up outside of this pilot context,

[43] Specifically, only mutual recognition of e-signatures based on qualified certificates is required by Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the points of single contact under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

[44] See https://www.eid-stork.eu/index.php?option=com_content&task=view&id=55&Itemid=76#stork_faq_6

impeding the monetization of the €20 million investment.

International coordination opportunities missed

Maintaining the current electronic signature framework would impede achieving the globalisation of digital transactions. In this regard, a broad common understanding on the need for e-signature recognition at international level was raised during " Stakeholder Workshop Digital Agenda for Europe: electronic identification, authentication and signatures in the European digital single market" held the 10th of March 2011 in Brussels[45].

Moreover, UNCITRAL[46] underlined that international mutual recognition could be eased if Article 9.3[47] of the *United Nations Convention on the Use of Electronic Communications in International Contracts* was reflected in EU legislation.

More specifically, other regions of the world are currently developing their own eIAS policies and proposals, including the US National Strategy for Trusted Identities in Cyberspace[48]. In the absence of a common EU policy on topics such as eID, the EU would not be able to initiate meaningful discussions with the USA or other key trade partners on common approaches. Member States could only engage in bilateral or multilateral discussions. Solutions would be developed purely at the national level, in isolation of international needs, trends or standards, thus limiting the appeal of European eIAS products and services on international markets.

Conclusion

The baseline scenario suggests that the existing problems of market fragmentation and lack of confidence would remain or worsen, and that their negative economic impact would become more significant: investments cannot be optimally monetised, efficient electronic processes cannot replace paper alternatives, and cross border trade is hampered. This would harm the development of the Digital Single Market, and in extension, of a European Citizenship.

2.6. EU added value and right to act

2.6.1. Treaty basis

Legal basis

[45] See http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision/ws_3_2011/index_en.htm
[46] United Nations Commission on International Trade Law
[47] Article 9.3.: Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:
(a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and
(b) The method used is either:
(i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
(ii) Proven in fact to have fulfilled the functions described in subparagraph *(a)* above, by itself or together with further evidence.
[48] See http://www.nist.gov/nstic/identity-ecosystem.html

The legal basis for the legislative proposal is Article 114 TFEU[49]. Indeed, the legislative proposal intends to remove existing barriers to the functioning of the internal market by promoting the approximation of Member States legislation, in particular the mutual recognition and acceptance of electronic identification, authentication, signatures and related trust services across-borders when needed for the access and completion of electronic procedures or transactions. This objective pursued cannot be achieved by less restrictive means than the legislative proposal. The general division of responsibilities between the Union and the MS with regard to monitoring and reporting as established under the e-signature Directive are not affected by the proposed changes compared to the current situation.

It should also be noted that the electronic signatures Directive 1999/93/EC was already based on article 114 (ex article 95*: "Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof*[50]*"*).

The legal basis of Directive 1999/93/EC is also adequate for related trust services, as they build on e-signatures and other eIAS components, and share the same challenges and complexities.

Identity management as such in relation to official eIDs falls under the subsidiarity of Member States. The scope of the proposal is the mutual recognition and acceptance of certain official eIDs (as notified by the Member States at their own choice and discretion), and not harmonisation of national eID-systems and infrastructures; the latter would likely not be permissible under the legal basis of Art. 114. What the new regulatory framework would provide for is the "free movement" of official eIDs used at national level including their use in each Member States regardless of where they are issued.

Finally, it is important to stress that the proposal (like Directive 1999/93/EC) would not make the use of any eIAS service obligatory for citizens, businesses or administrations. The goal of the proposal is solely to ensure that they have the possibility of using eIAS services when they want to, including in cross-border or cross-context situations.

2.6.2. Subsidiarity

In order for EU action to be justified, the subsidiarity principle must be respected:

a) Transnational nature of the problem (necessity test)

The transnational nature of eIAS is an important element in determining whether EU action is necessary. Domestic action alone would not suffice for the fulfilment of the objectives and the achievement of the targets set out in the *Europe 2020 Strategy*[51]. Conversely, experience has shown that national measures have de facto created barriers to the EU-wide

---

[49] Article 144 TFEU, §1: "*Save where otherwise provided in the Treaties, the following provisions shall apply for the achievement of the objectives set out in Article 26. The European Parliament and the Council shall … adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market."*

Article 26 TFEU: *"1. The Union shall adopt measures with the aim of establishing or ensuring the functioning of the internal market, in accordance with the relevant provisions of the Treaties. 2. The internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties. 3. …"*

[50] Article 47(2) addressed the taking-up and pursuit of activities as self-employed persons and laws governing the professions with respect to training and conditions of access for natural persons. Article 55 referred to the right of establishment of service providers.

[51] See Communication from the Commission: Europe 2020 – A strategy for smart, sustainable and inclusive growth, COM (2010) 2020 of 3rd March 2010.

interoperability of e-signatures, and that they are currently having the same effect for eID, eAuthentication and related trust services. It is therefore necessary that the EU creates the enabling framework for addressing cross-border interoperability.

Improvements to the supervision schemes, which would now also encompass related trust services in addition to eSignatures, also require EU level coordination.

b) Effectiveness test (added value)

Action at EU level would produce clear benefits compared with action at the level of Member States. The objectives outlined below are currently not being achieved by voluntary coordination among Member States, nor are they reasonably likely to be addressed by coordination in the future, due to the risk of duplication of efforts, setting different standards, transnational characteristics of the spill-overs generated by ICT, and the administrative complexity of establishing such coordination through bilateral and multilateral agreements.

In addition, overcoming the identified problems, such as an absence of legal certainty related to a lack of mutual recognition of national provisions due among others to a heteroclite interpretation of the legal texts and a lack of interoperability of the systems set up at national level due to non-adapted technical standards, requires the co-ordination across all EU27 MS which can be carried out more effectively at the EU level, thereby ensuring interoperability and EU-wide usability. EU action will ensure that gaps and weaknesses are clearly identified and concrete action is taken to address the issues at stake.

Due to eIAS inherent non-territoriality nature, action at EU level would be adequate and proportionate to implement the Digital Single Market. Regulatory measures taken at Member States level cannot be expected to achieve the same outcome.

3. DEFINITION OF THE POLICY OBJECTIVES

In accordance with the Impact Assessment Guidelines[52], when defining objectives, a distinction is made between general, specific and operational objectives.

Three **general objectives** have been identified: ensuring the development of a digital single market; stimulating and strengthening competition in the single market; enhancing user-friendliness (citizens and businesses). These objectives are in line with strategic EU policies such as the *EU 2020 Strategy*, the *Digital Agenda for Europe*, the *Single Market Act* and the *Roadmap for Stability and Growth*.

The general objectives identified are the following:
1. The development of a Digital Single Market
2. Stimulating and strengthening sustainable competition in the Digital Single Market
3. To promote the interest of consumers and to ensure high level of consumer protection for all EU citizens and businesses.

The **specific objectives** express the desired outcomes specifically related to the eIAS market (the '*what'*) of putting in place the operational objectives (or '*measures'*). Particular attention was given to presenting both the envisaged *economic* objectives (e.g. Specific objective 1) as well as *social* objectives[53] (e.g. Specific objective 5).

[52] See European Commission Impact Assessment Guidelines of 15 January 2009, SEC (2009)92.
[53] Relates to social/digital inclusion, the protection of consumers, etc.

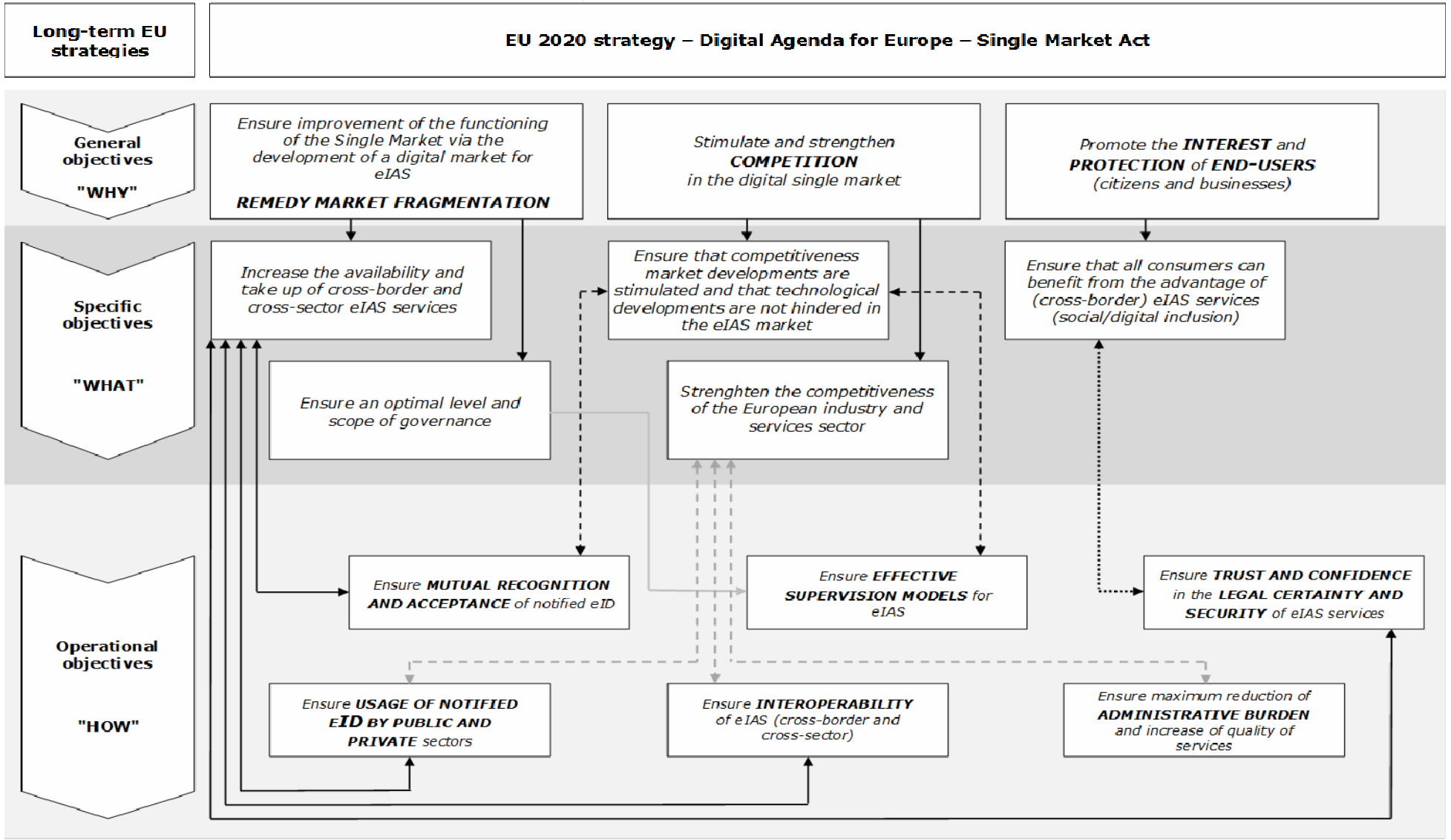
The specific objectives identified are the following:

1. Increase the availability of cross-border and cross-sector eIAS services and stimulate the take up of cross-border electronic transactions in all sectors (public and private);
2. Ensure an optimal level and scope of governance;
3. Ensure that competitive market developments are stimulated and that technological developments are not hindered in the eIAS market;
4. Strengthen the competitiveness of the European industry and services sector;
5. Ensure that all consumers can benefit from the advantages of (cross-border) eIAS services.

Finally, the operational objectives are directly derived from the problem and problem drivers identified in sections 2.2 and 2.3. (cf. intervention logic under 3.1), and point out 'how' appropriate policy option can help solving the problems.

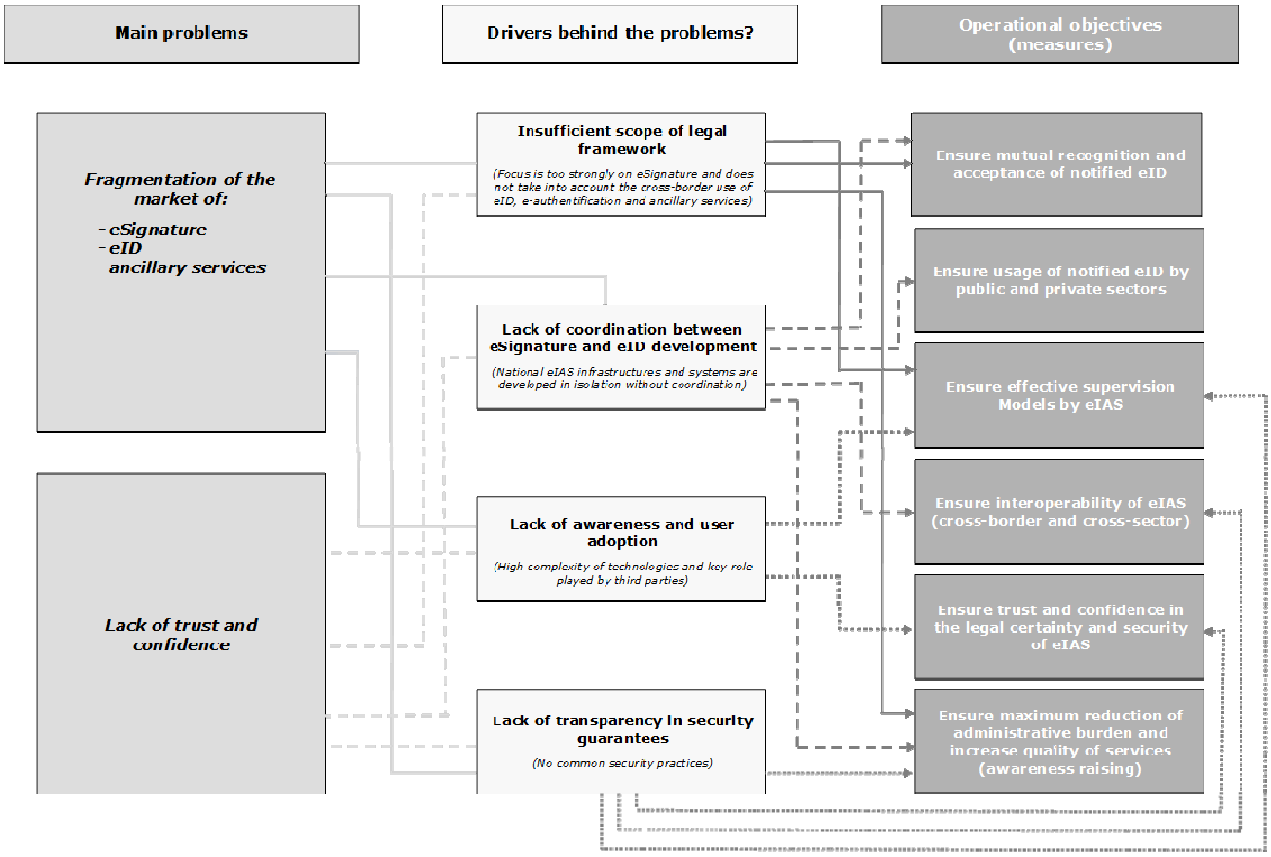
The operational objectives identified are the following:
1. Ensure mutual recognition and acceptance of notified eIDs
2. Ensure usage of notified eID by public and private sectors
3. Ensure effective supervision models by eIAS
4. Ensure interoperability of eIAS (cross-border and cross-sector)
5. Ensure trust and confidence in the legal certainty and security of eIAS
6. Ensure maximum reduction of administrative burden and increase quality of services. (awareness raising)

3.1 Overview of general, specific and operational measures


Long-term EU strategies
EU 2020 strategy – Digital Agenda for Europe – Single Market Act
General objectives "WHY"
Ensure improvement of the functioning of the Single Market via the development of a digital market for eIAS
REMEDY MARKET FRAGMENTATION
Stimulate and strengthen COMPETITION in the digital single market
Promote the INTEREST and PROTECTION of END-USERS (citizens and businesses)
Specific objectives "WHAT"
Increase the availability and take up of cross-border and cross-sector eIAS services
Ensure that competitiveness market developments are stimulated and that technological developments are not hindered in the eIAS market
Ensure that all consumers can benefit from the advantage of (cross-border) eIAS services (social/digital inclusion)
Ensure an optimal level and scope of governance
Strenghten the competitiveness of the European industry and services sector
Operational objectives "HOW"
Ensure MUTUAL RECOGNITION AND ACCEPTANCE of notified eID
Ensure EFFECTIVE SUPERVISION MODELS for eIAS
Ensure TRUST AND CONFIDENCE in the LEGAL CERTAINTY AND SECURITY of eIAS services
Ensure USAGE OF NOTIFIED eID BY PUBLIC AND PRIVATE sectors
Ensure INTEROPERABILITY of eIAS (cross-border and cross-sector)
Ensure maximum reduction of ADMINISTRATIVE BURDEN and increase of quality of services

3.2 Intervention logic

The intervention logic linking the main problems and the *operational* measures is illustrated in the next figure:



4. POLICY OPTIONS

In order to solve the problems and meet the objectives set out in the previous sections, three different sets of options are considered, respectively addressing the scope of the envisaged framework, the legal instruments and the supervision organisation.

4.1. Options for the Scope of the Framework

Option 0: Repeal of the e-signature Directive and no regulatory activities with respect to eID or related trust services

This policy option implies the cessation of all EU activities in the field of electronic signatures including those already started. It would thus lead to repealing Directive 1999/93/EC and its two related Decisions 2000/709/EC and 2003/511/EC. Any directives referring to Directive 1999/93/EC would need to be amended. Only national legal frameworks would remain and would be free to evolve based solely on the preferences of national legislators.

This option also implies that no legislation would be adopted on eID, e-authentication and related trust services.

Option 1 No policy change

This option corresponds to the baseline scenario developed in section 2.5 above. It implies retaining the e-signatures Directive as it stands. It should be noted that one of its weaknesses (outdated references to technical standards) could be addressed by revising Decision 2003/511/EC.

Option 2 - Enhancing legal certainty, boosting coordination of national supervision and ensuring mutual recognition and acceptance of eIDs

This option consists of expanding the scope of the e-signature Directive by including new provisions for the cross border recognition and acceptance of certain eIDs. The provisions of the current Directive in relation to electronic signatures would be revised in order to solve its current weaknesses.

Within this policy option, the primary change in scope is thus the mutual recognition and acceptance of 'notified' eIDs, i.e. official eIDs which the Member States consider suitable for cross-border use[54]. These should benefit from general recognition and acceptance, both in a cross-border and cross-sector context. Practically, this would imply that EU-wide use of notified eIDs would become possible in any online interaction where reliable identification is needed, irrespective of the location of the end user or service provider. Through the cross-sector approach, the private sector could also benefit from notified eIDs, in the same way as they can currently rely on paper official identity documents in offline contexts, instead of being required to develop their own eID-solutions.

It should be noted that the concept of a notified eID is not limited to public sector issued eIDs: Member States could also notify eIDs issued by the private sector that they recognise to be used for their own public sector services. This approach is necessary to ensure that the strategy is applicable and useful to all Member States, as not all Member States all Member States have eIDs issued by the public sector. The outcome would thus be an eID scheme that is conducive to supporting any eID policy choices made by a Member State at national level.

Example: the Netherlands have not yet introduced an official electronic identity card. In the meantime, citizens can use a scheme based on usernames, passwords and SMS confirmations to identify themselves. This scheme is called **DigiD**[55], and is managed by the public sector. Businesses can identify themselves electronically using solutions offered by the private sector, which have to observe the rules established by the government in a scheme called **eHerkenning**[56]. Thus, the Netherlands is an example of a country that uses a mixed private-public sector model, for which a cross-sector approach would be important to achieve cross border interoperability.

Option 2 would also require that data protection provisions are integrated into the proposal, to ensure that eID providers are not able to track the behaviour of eID holders. This is particularly relevant when cross-context usage is considered: private sector eID issuers should not be able to track when their customers use eGovernment applications, nor is it desirable that public administrations can track eID use in private sector services as a matter of course. Existing experiences at the Member State level can be leveraged to achieve this result, and the proposal will be aligned with the currently ongoing revision of the Data Protection Directive (including specifically with respect to privacy-by-design rules[57]).

Example: the **Austrian Citizen Card** is known for its high level of data protection. The unique identification number of each citizen (the so-called sourcePIN or *Stammzahl*) is cryptographically hidden from service providers. They can only see identification numbers which are derived from this sourcePIN on a sector per sector basis. As a result, they cannot link citizen behaviour between different sectors.

---

54 More formally: a "notified" eID is an official eID scheme notified by a given Member State to the Commission, specifically to ensure that they can benefit from cross-border recognition by other Member States.

55 See http://www.digid.nl/

56 See http://www.eherkenning.nl/eRecognition

57 See the current proposal for a General Data Protection Regulation, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, notably Article 23

Option 3 – Expansion to incorporate certain related trust services

This option expands option 2 by including further related trust services and credentials in the scope of the legislative framework.

Essential related features to be added in the legislation would be: − Time stamping, i.e. the application of a trustworthy time reference to electronic data, so that its existence at a given point in time can be determined with certainty. − Electronic seals, i.e., the equivalent to the signature of a legal person[58]; in practical terms, this can be thought of as the electronic equivalent of stamps or seals on paper documents, which are tied to a legal entity rather than to a natural person. − Long-term preservation of information, i.e., to ensure the legal validity of electronic signature over extended periods of time, ensuring that e-signatures can be validated irrespective of future technological evolutions. − certified e-document delivery, i.e., the reliable and verifiable electronic delivery of data; this can be thought of as the electronic equivalent to traditional registered mail.[59] − admissibility of electronic documents, i.e. ensuring that paper documents can be converted into electronic equivalents without losing their legal validity; this can be thought of as an electronic equivalent to the paper certified copy (*copie conforme*). − Website authentication, i.e. an obligation for legal person's website to include trusted information (e.g. a certificate) allowing the user to verify the authenticity of the website and the existence of the legal person.

4.2. Options for the Legal Instrument of the Framework

Option A: One comprehensive legal instrument vs Option B: Two separate legislative instruments

In the context of these sub-options, two alternatives are considered for the legal instrument that could implement the options for the scope of the framework.

The legislation would either consist of one single comprehensive measure covering electronic identification, authentication and signatures; or of two instruments, namely an Act on electronic identification and authentication and an Act for the revision of the eSignature Directive.

Option C: Directive vs Option D: Regulation

In the context of these sub-options, the legislation(s) would either consist of a Directive or of a Regulation.

4.3. Options for the Level of Supervision of e-Trust services

Option i): Maintaining national supervision schemes ("basic variant")

This option envisages maintaining the current national based supervision schemes, but with stronger harmonisation through high level common essential requirements, including e.g. regular audits of supervised service providers. These essential requirements should ensure that all national supervision schemes attain a quality level that fully ensures security and legal certainty.

Option ii): Establishing a EU-based supervision system ("advanced variant")

This option envisages the establishment of a EU-based supervision system. The goal would be to ensure that differences between national supervision approaches are either further reduced or eliminated entirely, depending on the preferred sub-option under this scenario.

---

[58] The important feature of some documents issued by an organisation is their authenticity, i.e. that the document was genuinely produced by the organisation (ex. a certificate). Authenticity can be proven by an electronic stamp which is to a certain extent.

[59] Once a document has been created and signed (ex. a contract, a notification of a judge), there are no means to send it in another country using a electronic service equivalent to registered mail.

The first and conceptually simplest sub-option under this scenario would be to eliminate entirely the existing national supervision schemes, and replace them with a single European supervision scheme and body. In this sub-option, either a new European body would have to be created to perform this supervisory function, or an existing European body would be given this duty.

A second sub-option is to establish a federated supervision system involving an EU-based supervisory body (again, either as a new body or as an additional mandate for an existing body) while maintaining the national supervisory schemes and bodies.

Under this federated system, the exact responsibilities of the European body might include:

- Interpretation of minimum requirements to be followed by national supervisory bodies;
- Supervision of trust service providers established in a Member State, if that Member State has chosen to delegate its supervision competences to the European supervisory body[60];
- Supervision of trust service providers established outside of the EU that also wish to be supervised in Europe on a voluntary basis;
- Possibly supervision of remaining national supervisory bodies.

5. ASSESSMENT OF THE POLICY OPTIONS

In the following sections, the policy options will be assessed and compared to the baseline scenario (i.e. Option 1: Status Quo).

5.1. Scope of the Framework

The sections below present the *effectiveness*[61] and *coherence*[62] of the different options for the scope of the framework. For the assessment of the *efficiency*[63] of these options, we refer both to the indications of possible the cost(s) incurred and cost savings made by the different parties involved as well as to the comparison of the costs of governance (cf. section 0) and costs of managing the supervision (cf. section 5.3.3).

5.1.1. Assessment of Option 0: 'No EU Policy'

Economic, social, environmental impacts and administrative burden of option 0

Member States would be free to modify substantially their internal legislation, going from maintaining their current transposition law, to properly cancelling it, and having also the opportunity to simply adapt it to their own needs. Bilateral or multilateral agreements would likely be reached between some Member States with a common view of the topic or with common economic objectives. An integrated approach set up amongst all 27 Member States, even if theoretically possible, seems to be an unlikely option.

If Member States collectively decide to cancel their own internal law, then this would lead to a legal no man's land with absolute market freedom. However, in the absence of a legal framework, there would also be absolute uncertainty as to the legal validity of any such service.

[60] This could be economically advantageous and pragmatic for Member States with no or only a very limited number of trust service providers to be supervised, or who have difficulties in ensuring the availability of competent staff for their national supervisory body.

[61] '*'Effectiveness'* indicates the extent to which options achieve the objectives of the proposal.

[62] 'Coherence' indicates the extent to which options are coherent with the overarching objectives of EU policy, and the extent to which they are likely to limit trade-offs across the economic, social, and environmental domain.

[63] 'Efficiency' indicates the extent to which objectives can be achieved for a given level of resources/at least cost ("cost-effectiveness")

Economically, the risk related to investing in eIAS services would remain high and payback periods long and uncertain. Most probably, all investments made at EU, Member States, and private sector level would be, proportionally to the attitude of Member States, lost.

Example: a number of Member States have invested in electronic identification cards that allow also the creation of qualified electronic signatures, to ensure that the resulting signatures would be legally equivalent to hand written signatures across the EU (including e.g. Austria, Belgium, Estonia, Spain, Italy). In the absence of European harmonisation on this point, this guaranteed legal effect would disappear, and the millions of Euros invested by each of these Member States in order to achieve this effect would be to some extent wasted.
Example: several Member States have implemented Points of Single Contact that rely on the legal framework of the e-signatures Directive and the Commission Decisions to achieve at least a small degree of cross border interoperability (e.g. Cyprus, Greece, Spain, Liechtenstein and Lithuania). If this legal framework disappears, then these Member States would have to develop entirely new solutions, and their existing developments would be largely wasted.

Socially, there is a risk to see high and low level jobs disappear. Indeed, if the electronic signature was no more effective at cross-border level, the risk of collapsing companies would be very high due to the fact that the market would be more fragmented and that only the national market would be easily accessible for companies. In this regard, the customer potential would be hugely reduced. Environmentally, the potential benefits raised by the use of electronic interactions – mainly represented by the reduction of the amount of paper used – could be nullified.

The only aspects that would benefit from this option would be the decreasing of the administrative burden at Member States level brought by the cancellation of the supervision model, and ensuring complete freedom for market developments. This option would thus give optimal room for the development and uptake of voluntary industry initiatives and standards, such as e.g. OpenID[64] and the Kantara Initiative[65]. However, it should be noted that these initiatives are by themselves not sufficient to resolve the identified problems of market fragmentation and especially the lack of trust, as they do not have any regulatory backing to establish rights and obligations for services providers and end users.

Finally, cancelling all activities at EU level in the area of electronic signatures would have, on the one hand, an impact on other EU policies. Indeed, EU policies on e-invoicing, e-procurement or VAT are strongly related to the efficiency of cross-border electronic signature.

Example: the Public Procurement Directives 2004/17/EC and 2004/18/EC allow Member States to require qualified electronic signatures for the submission of offers. As shown in the 2010 Evaluation of the 2004 Action Plan for Electronic Public Procurement[66], 6 Member States make the use of such signatures mandatory. In total, 13 Member States require the use of at least advanced electronic signatures as regulated by the Directives. The elimination of European rules could threaten all investments made in this policy area, which are based to some extent on the concepts introduced by the Directive.

On the other hand, it would also have a negative impact on potential alignment with third countries. A fragmented legislation implies the practical impossibility to reach an agreement at international level to create a global safe environment for electronic transactions based on electronic signatures.

Effectiveness of Option 0

Based on the assessment of the economic, social and environmental impacts, the following conclusions are obtained regarding each of the specific objectives (cf. detailed assessment presented in Annex 10):

SPECIFIC OBJECTIVE 1: Option 0 would first of all not increase the availability and take-up of cross-border and cross-sector eIAS services. The inability to increase the availability and

64 See http://openid.net/
65 See http://kantarainitiative.org/
66 See http://ec.europa.eu/internal_market/consultations/docs/2010/e-procurement/evaluation-report_en.pdf

take-up of cross-border and cross-sector eIAS services would not allow for a strong reduction of barriers. Depending on the efforts made by MS to enable e.g. the dematerialisation of administrative formalities, improvement of the local situation could be obtained (as is the case in the Baseline scenario), but this would not solve the problems related to cross-border transactions.

SPECIFIC OBJECTIVE 2: Option 0 would not ensure an optimal level and scope of governance. Without an EU Policy, it would first of all be very difficult to increase legal certainty, trust and security of electronic transactions. The repealing of Directive 1999/93/EC on e-signatures would furthermore take away the only driver available today for enhancing harmonisation at the EU level and make it possible for MS to create even more legal and technical barriers than those still remaining today.

SPECIFIC OBJECTIVE 3: Option 0 would not stimulate market developments and could hinder technological developments in the eIAS market by eliminating any drive for alignment. While the absence of any EU rules could avoid the risk of steering the market into a certain direction, this benefit is likely offset by the risk of Member States adopting their own rules (i.e. rather than one set of rules, service providers might be governed by 27 separate sets of rules). Furthermore, without an EU Policy, the eIAS market would remain fragmented.

SPECIFIC OBJECTIVE 4: Option 0 would contribute even less to the strengthening of the competitiveness of the European industry and services sectors. First of all, the EU industry and services sector would not be able to build business models on their strong eIAS products and services. Repealing the Directive 1999/93/EC would furthermore disrupt the current process of working towards the enabling of cross-border electronic services. It can be expected that, without support at the EU level, MS will not continue this process on a voluntary basis, or at least that they would be less efficient in doing so. MS would meanwhile focus on or limit their efforts to national eIAS services. The trust landscape created as such would not be very attractive to investments by foreign eIAS operators. and in the longer run, if eServices would become clearly less developed in the EU compared to other regions, this could decrease the attractiveness of the EU for many other sectors.

SPECIFIC OBJECTIVE 5: Option 0 cannot ensure that all end-users can benefit from the advantage of (cross-border) eIAS services. Without an EU policy, MS will not have many incentives to create an EU trust landscape that allows participation to the digital single market by all social groups. (cf. Regional development).

Coherence of Option 0

Finally, it can be concluded that Option 0 is not coherent at all with the overarching objectives of EU policy (cf. EU 2020 Strategy, DAE, Single Market Act and the Roadmap to Stability and Growth) as presented in section 3.

5.1.2. Assessment of Option 1: 'Status quo' (No Policy change)

Economic, social, environmental impacts and administrative burden of option 1

Economically, there is a high risk of low return on investments in eIAS infrastructure, products and services since new sectors are difficult to access and take-up rates have remained low. Opportunities created by the European Large Scale Pilots (LSPs) cannot be grasped as the required framework for doing so is lacking.

Moreover, until today, the unavailability of an appropriate framework has had a negative impact on the availability of cross-border electronic services. As such, it is difficult to estimate the cross-border saving potentials based on real life examples. However, the order of

magnitude of the relative savings already estimated or observed at the national level provide a good proxy for possible cross-border savings[67].

In this regard, it should be noted that:

According to the recent communication on a coherent framework for building trust in the Digital Single Market for e-commerce and online services the potential of the Digital Single Market is enormous and would benefit all the territories and economic sectors of the European Union. In the G8 countries, South Korea and Sweden, the internet economy has brought about 21% of the growth in GDP in the last five years. It also generates 2.6 jobs for every job cut and at times accounts for 25% of net employment creation. Online services are by nature cross-border and can speed up European integration and the creation of the Single Market.'

According to the communication on a coherent framework for building trust in the Digital Single Market for e-commerce and online services 'The Digital Single Market is far from achieving its full potential; the cost of failure to complete it is expected to be at least 4.1% of GDP between now and 2020, i.e. EUR 500 billion or EUR 1000 per citizen.

In the Single Market Act , it was recently reiterated that 'The development of digital technology is one of the main levers for boosting growth and employment in the EU in various respects: the information and communications technology industry (whose added value to the European economy was approximately EUR 600 billion in 2007), an increasing number of Europeans who use the Internet on a regular basis or even daily (65% and 53% respectively in 2010), a broadband market which was a world-leader in 2010 , a market for public-sector information estimated at EUR 27 billion , to name just a few.'

The availability of cross-border IAS services could be strongly beneficial to the development of intra-EU market access and trade. In 2009, intra-EU trade in goods represented 37% of GDP (EUR 4 320 billion) and intra-EU trade in services 10.5% of GDP (EUR 1 233 billion). Despite this relatively large figure, only a relatively modest 9% of EU citizens carried out purchases from suppliers in other Member States in that same year. Thus, a significant margin of growth for cross border electronic trade still exists.

The above-mentioned figures underline the importance of developing all required building blocks, incl. an appropriate cross-sector framework for secure, trustworthy and easy-to-use electronic interactions, so that the Digital Single Market can develop to its full potential.
Some concrete examples

1. eProcurement has been commonly recognised as one of the high-impact services to be provided by European governments, with a significant savings potential. Government purchases in the European Union account for an estimated 19% of GDP, or €2,200B annually. Currently, less than 5% of total procurement budgets are awarded electronically, and only 1.6% of contracts are supplied by an entity in another Member State.

It is estimated that a hypothetical reduction of average public procurement budgets of 1% due to the implementation of eProcurement would already amount to a saving of 3.92 billion EUR for EU advertised public procurements, and of 21.6 billion EUR for all EU public procurements together. As a cost saving of 5% is commonly quoted as a realistic outcome of implementing eProcurement, savings of 100 billion EUR for universal adoption would be possible[68]. Given the importance of IAS as a current blocking factor in eProcurement, this already shows the vast economic potential of establishing a coherent trust framework for eID, e-signatures, time stamping, long term archiving, electronic registered mail, and other services which are crucial to ensure the reliability and validity of eProcurements.

2.The French electronic health card Sesam-Vitale shows an impressive example of the cost and time reductions of electronic interactions compared to paper interactions[69] in the national context. Taking into account that 190 million European Health Insurance Cards (EHIC) were issued by 2009, and that some 3 to 4% of EU citizens are using their card in case of health care services used abroad, electronic interactions could potentially replace at least some 5.7 million tedious manual cross-border reimbursements if systems would be interoperable. If similar solutions could be implemented in other Member States with similar results, the economic impact could be very substantial.

3. Not all benefits can be expressed in terms of monetary gain. Estonia became an early adopter of eVoting via the Internet (rather than via dedicated eVoting booths) in 2005, leveraging its national eID scheme. While cautioning that this approach would certainly not be more cost effective initially, due to high set-up costs and low scale of deployment (with around 1 million eligible Estonian voters), the use of eVoting was seen as a potential way of increasing voter turnout and participation[70]. Based on available statistics[71], the number of eVoters out of the eligible voters in the population has increased from 3.4% in 2007 to 15.4% in 2011. In terms of actual voters (rather than all eligible voters), eVoter participation rose from 5.5% in 2007 to 24.3% in 2011. Total participation in voting (including electronic and traditional voting) rose from 61.9% in 2007 to 63.7% in 2011. Obviously, this does not prove conclusively that eVoting is solely or even partially responsible for this modest increase in voter turnout, but the increased adoption of eVoting shows the appeal of this option to voters. Furthermore, it is worth noting that eVotes cast by Estonian citizens in foreign countries represented 3.9% of all eVotes in 2011, with votes being cast from a total of 105 different countries. This last figure is a concrete example of digital citizenship being enabled through reliable IAS infrastructure that will become increasingly important as citizen mobility in the EU continues to grow.

[67] Indeed, all the different categories of cost savings will be more or less the same, independent of whether the interaction is national or cross-border. Moreover, it could be argued that cost savings will likely be more significant for cross-border interactions, given the greater administrative cost for cross border interactions (e.g. cost of sending paper bids by regular mail, or the need to provided formal translations of certain documents).

[68] Study on the evaluation of the Action Plan for the implementation of the legal framework for electronic procurement - Analysis, assessment and recommendations report; http://ec.europa.eu/internal_market/consultations/docs/2010/e-procurement/siemens-study_en.pdf

[69] According to the data of the organisation, "average cost for an electronic claim is of 0.27€ against 1.74€ for a paper claim processing. Moreover, time to refund insured citizens for medical expenses has been dramatically reduced. Nowadays, the whole reimbursement procedure of patients or health professionals (in case of direct payment by the health insurance) lasts 5 days maximum whereas up to 5 weeks were needed with the paper based manual procedure". Source: Sesam-Vitale.

[70] See E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world, Ülle Madise and Tarvi Martens, http://www.e-voting.cc/static/evoting/files/madise_martens_estonia2005_13-26.pdf

[71] Published on http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics

Socially, the hindering of market and technological developments are finally hindering the growth of employment in the ICT market (employment of mainly highly skilled workers).

Administratively and environmentally, there would be not much room for reducing the administrative burden by using eIAS, the possibilities would remain limited to some specific (national) closed environments. As a direct consequence, the possibility of reducing the amount of paper used would remain very limited.

Effectiveness of Option 1

(cf. detailed assessment presented in Annex 10):

SPECIFIC OBJECTIVE 1: the current framework is not optimally stimulating market dynamics. If the current EU policy is not changed, the EU economy would not be able to benefit much from an increased impact of ICT investments in eIAS services on overall productivity and competitiveness, especially not for cross-border transactions. In extension, the lack of availability of eIAS and/or a lack of trust and confidence in (cross-border) electronic transactions does not allow reaping the benefits related to the wide availability of broadband connections which could allow exercising many professions from a distance, incl. in rural areas.

SPECIFIC OBJECTIVE 2: The current regulatory approach is also not ensuring an optimal level and scope of governance. The current Directive is not providing sufficient legal certainty, trust and security of electronic transactions throughout the EU. It also cannot be excluded that MS could continue to use the public service clause[72], leading to interoperability challenges for which no clear legal recourse is available. Moreover, the differences in national supervision will continue to lead to fragmentation of the market and lack of trust. The EU Framework is currently largely limited to e-signatures reducing the possible economies of scale and scope for suppliers of eIAS products and services. Finally, since electronic identification and authentication is currently not included in the EU framework, the risk of fraud and ID theft can vary between MS and cannot be reduced by EU-measures.

SPECIFIC OBJECTIVE 3: The current framework does not allow the development of competitive markets and technological developments are hindered. Indeed, the potential offered by innovative services is jeopardised due to market fragmentation.

SPECIFIC OBJECTIVE 4: The baseline scenario is not helping to strengthen the competitiveness of the European industry and services sector. Full electronic processing of transactions is currently often (technically) not possible (e.g. due to interoperability problems at the EU level) and the development of on-line services is furthermore hampered by legal uncertainty and trust issues which are not sufficiently dealt with by the current EU Framework. Development of online services is therefore mostly limited to local applications. In extension, there is currently little incentive for companies from outside the EU or from other MS to invest in the development of eIAS products and services that can be used in a particular MS. Moreover, as for option 0, in the longer run, if eServices would become clearly less developed in the EU compared to other regions, this could decrease the attractiveness of the EU for many different sectors.

SPECIFIC OBJECTIVE 5: Option 1 does not ensure that consumers can benefit from the advantage of (cross-border) eIAS services. The lack of a sufficient level of trust and security of eIAS infrastructures, products and services as well as the lack of interoperability make eIAS unnecessarily complicated (e.g. because of the need of different devices, the unavailability of notified eID, ...) placing social groups that have less developed eSkills at risk. Secondly, the faltering development of (cross-sector and cross-border) on-line services

[72] Cf. note 57

has a negative impact on the accessibility of services (e.g. eHealth, eGovernment) for people living in rural areas and could thus negatively affect regional development.

Coherence of Option 1:

Option 1 is not coherent with the overarching objectives of EU policy (cf. EU2020 Strategy, DAE, Single Market Act and the Roadmap to Stability and Growth) as presented in 1.2.

5.1.3. Assessment of Option 2: 'Enhancing legal certainty, boosting coordination of national supervision and ensuring mutual recognition and acceptance of eIDs'

Economic, social, environmental impacts and administrative burden of option 2

Economically, many types of electronic transactions become more efficient with an eID system. These systems enable individuals to authenticate when using online services and create legally-binding electronic signatures when concluding a contract on-line or registering for a service.

Estonia has issued approximately 1.2 million eID smartcards. Since inception, cardholders in Estonia have used their eID to create more than 52 million electronic signatures and authenticate more than 88 million electronic transactions. The government has not placed any restrictions on the use of the eID in the private sector and the authentication mechanism is available to any outside developer. Currently, applications exist for using the eID to authorise online bank transactions, to sign contracts and tax declarations, to authenticate to wireless networks, to access government databases, and for automated building access.[73]

The risk of exclusion from the digital economy for SMEs (and even more for micro-enterprises) is unlikely to increase. While there is an initial set-up cost for SMEs (or other end users), this cost is dwarfed by the economic benefits of reduction of administrative burden through trustworthy economic communications.

Through the Estonian e-Business portal, a simple limited liability company can be set up entirely electronically. This type of business is particularly suitable for SMEs. The entire process can currently be completed online in18 minutes[74]. Creating a company via the internet requires an Estonian ID card, or alternatively ID cards from Belgium, Portugal, Lithuania, and Finland. A legal framework for eID recognition could boost the scope of this project to other Member States, as Estonia would be able to trust eIDs from other Member States without assessing them on a case-by-case basis. Obviously, the monetary gain compared to a tradition paper process (which would require travel to Estonia to physically appear before the competent officials) is enormous. Similar gains can be made in other policy areas: in eProcurement, the cost of preparing and submitting a paper bid is orders of magnitude higher than the cost of preparing and submitting an electronic bid. The cost of sending a paper bid via courier in cross border procurements alone can easily cost between 50-100 EUR per offer. Compared to an eID cost of e.g. 17,50 EUR per card in Belgium[75], or 10 EUR in Estonia[76], and generic USB card readers costing around 20 EUR[77], costs are easily recuperated. This is even more so when other use cases are factored in, such as e.g. annual submission of company balance sheets. In Estonia, this process was streamlined from a paper process that took 3 months and involved countless person hours for printing, sending, scanning and manually inputting data into a register, to an electronic process called e-Annual Report that takes 20 minutes from the final preparation to inclusion into a register. The time saving (and thus cost saving) is clear, if usable eIDs are available.

In order to have access from eIAS services, internet access is absolutely required. In this regard, other policies can be used (ex. Universal services directive, Connecting Europe Facility (CEF)) to deploy internet in remote places. From a social point of view, Option 2 would make it much easier to exercise a profession or develop an (e-)business in rural areas, since many administrative formalities and business could be done from a distance. This could bring about a positive effect on employment. A priori, this would involve mainly highly skilled workers.

Regional development is hard to predict. While certain Member States certainly have a more advanced eIAS infrastructure in

[73] http://www.itif.org/files/2011-e-id-report.pdf
[74] See http://estonia.eu/about-estonia/economy-a-it/e-estonia.html
[75] See http://www.brussels.be/artdet.cfm?id=4827&
[76] See http://www.itapa.sk/data/att/1965_subor_sk.pdf
[77] See http://porvoo9.gov.si/pdf/THU_11c_1415_Country_update_Estonia.pdf

place at this time than others, there are some indications that advanced services already exist in all Member States. As a small indicator, it can be noted that the national trust lists containing supervised (and in some Member States accredited) service providers show that currently more than 100 companies are providing qualified certificates to the public, spanning 24 out of 27 Member States. From those 24, commercial offers (i.e. not focused exclusively on the public sector) for the issuance of qualified certificates are available in 20 Member States. Thus, even when focusing exclusively on this small group of relatively technologically advanced service providers, there is a relatively even spread across the Member States. Regional development would thus likely not be harmed by a policy focus on advanced eIAS tools.

The increased availability of eIAS will also fully enable their potential to reduce the administrative burden, as shown by the examples above in relation to balance sheet submission. By consequence, Option 2 would allow making paperless a significant number of transactions that currently require a 'physical' identification, authentication or signature. Government receives many of the benefits from increased efficiency, for example by eliminating duplicate data entry, and reducing the costs associated with unnecessary paperwork including printing costs, storage, transportation and disposal.

Security added value brought by eID provisions:
Finally, Option 2 can improve the security of online transactions and help prevent fraud and identity theft. eIDs can make it more secure for users to login to information systems by enabling multi-factor authentication. An example of multi-factor authentication is requiring the user both to know a PIN and have an eID token to login to a website (i.e., the same security system as when using a bank-card). Since users must remember multiple usernames/passwords today, they often choose an easier-to-remember password or re-use the same password for different services. As Option 2 would instead allow users to use a single reliable eID in multiple contexts (i.e. cross border and cross sector), then the need for multiple passwords disappears and bad security habits can be reduced.[78]

Obligations for the different stakeholders

This option will mainly impact *governments* (which would need to modify national supervision schemes and to notify "official" eIDs), *the service providers* themselves (which would need to seek supervision if they wish to benefit from cross border market recognition), and *solution providers* (which would need to comply with common European standards if they wish to benefit from European level interoperability).

In particular, the new system of notified eIDs implies that Member States:
- who want their official eIDs mutually recognised and accepted at EU level would need to notify these to the Commission. The Commission would set up a list of notified eIDs which would be published (Delegated Act).
- will be liable for the notified eID: this liability will be limited to the unambiguous link between the identification data attributed to a person via the eID (e.g. person data such as name, date of birth and person identifier such as tax number in Italy, or the residence register in Austria). This ensures that each individual can be uniquely identified, even if some attributes are shared (e.g. multiple John Smiths, who may even share the same date of birth or city of residence). Member State liability would not extend to the entire transaction in which an eID is used (e.g. the validity of an eProcurement offer), but only to the exact identification of the person.
- Need to provide an authentication possibility in order to check and verify that an eID is still valid (e.g. that it was not revoked after the theft of an eID card). They would also be responsible (and liable) for the correctness of this authentication process. .

Note that this does not imply an obligation for Member States to change their eID-systems and infrastructures. However, *if* they wish to notify official eIDs (which is their own choice), then they will need to meet the European regulatory requirements, including by providing the required interfaces to their systems. The costs needed to put in place the required interfaces and infrastructures would be nonetheless limited as many countries – the 14 MS that have participated in the LSP STORK (AT, BE, EE, FR, DE, IT, LU, NL, PT, SL, ES, SE, UK and SK) – have already an interface and infrastructure, developed within STORK, which allows for the cross-border interoperability of eIDs. Assuming a MS has its own eID and the infrastructure associated with it, then it is a question of implementing these common STORK components. This is a relatively cheap activity, compared to the now sunk cost of the development of these components , and an estimate in the region of 100k should be largely sufficient. Should a MS not have its own eID in place, , then Option 2 will make it more attractive for them to adopt an eID: the existing interoperability components would still be available for their use, meaning that the potential use of an eID is much greater, and that no unnecessary costs would be incurred to create any new interoperability solutions. The major challenges relate more to organisational and governance problems. A sustainable governance is possible in the context of the proposed CEF and the planned digital service infrastructure for electronic identification and authentication.

[78] http://www.itif.org/files/2011-e-id-report.pdf

It should be noted that for *end users* of these products and services (which can include citizens, businesses (including SMEs and administrations) no new obligations/responsibilities are contemplated under any of the options of the proposal. While their range of choices and options increases, they would not be compelled to undertake new actions. Specifically, it is not envisaged to make the use or acceptance of eIAS or related trust services mandatory (notwithstanding the fact that use/acceptance may already be mandatory under separate and independent frameworks, such as within the context of the Services Directive, or national obligations to file certain tax declarations electronically). Moreover, as with the eSignatures Directive, national laws regulating the contractual area will not be modified by the new legal framework.

A special attention must be paid to the SMEs case:
Following an on-going study carried out by Formit and studying the usage of e-signatures in 6 different countries (Spain, Italy, Luxembourg, Finland, Romania and Germany), the current usage of e-signatures depend first, on the size of the enterprise and second on the sector of activities. This conclusion confirms Eurostat figures showing that the use of eSignatures is higher in large enterprises than in SMEs. However, analysing these figures, we can notice that the growth is proportionally higher for SMEs:

- Large: 2009: 44% - 2010: 48%
- Medium: 2009 36% - 2010: 40%
- Small: 2009: 23% - 2010: 26%

Nonetheless, if one of the objectives is to further raise SMEs' awareness on using use eSignatures and related trust services, the impacts of the initiative will be the same for all categories of enterprises. Indeed, the requirements of the new Regulation would have to be fulfilled by MS, from one hand, and CSPs from the other.

However, if businesses wish to use eIDs and electronic signatures, they will incur costs for certificates and software: the price of certificates is very heterogeneous and depends on three main parameters (Member State sponsorship, quality of the certificate and validity periods). The important variability in prices and price structure makes it very difficult to give a scale of prices. As the aforementioned examples of Estonia and Belgium show, government sponsored eIDs can be provided relatively cheaply (approx. 20 EUR). The annual price for a qualified signature certificate issued by commercial service providers (absent of government sponsorship varies between EUR 25 and 299, and between EUR 10 and 150 for a non qualified one.

Effectiveness of option 2

(cf. detailed assessment presented in Annex 11):

SPECIFIC OBJECTIVE 1: Option 2 would improve the availability and take-up of cross-border and cross-sector eIAS services. eIAS products and services would gain appeal, which in turn would positively impact the return on investments made in eIAS infrastructure, products and services. New services would be created, and new markets and new investments can be unlocked, thus stimulating innovation.

Highly innovative companies presently exist, offering some of the services which are currently not covered by harmonized legislation, such as time stamping services offered by Universign in France[79], electronic registered mail offered by UnifiedPost in Belgium[80], or electronic archiving offered by Unizeto in Poland[81]. However, these companies cannot offer their clients clear guarantees on the legal value of their services across Europe in the absence of common rules. By introducing such rules, their market potential would expand to the whole internal market, benefiting the availability of services in countries where no similar providers exist yet, and opening the market for new opportunities.

SPECIFIC OBJECTIVE 2: a better level and scope of governance would also be achieved to a large extent under Option 2. Indeed, a harmonised regulatory approach at EU-level that would also cover eIDs (unlike under Option 1) would enhance legal certainty, trust and security of

[79] See https://www.universign.eu/
[80] See http://www.unifiedpost.com/en/solutions/de-aangetekende-zending.html
[81] See http://www.unizeto.eu/unizeto/uni,offer_edocument.xml

electronic transactions and reduce the fragmentation of the market for eIDs, since cross-border interoperability would be improved by allowing references to a clear, flexible and reality-proof set of common technical standards. Furthermore, since notified and mutually recognised eIDs could also be used for applications in private sectors, these latter could profit from the large scale roll-out of (notified/official) eIDs (which took already place over the last few years) for accessing a large number of potential clients.

SPECIFIC OBJECTIVE 3: The technology neutral EU Regulation for e-signature and eID as proposed under Option 2 would stimulate competitive market developments and ensure that technological developments in the eIAS market are not hindered. Option 2 will allow that easy-to-use and trustworthy eIAS products and services become more easily available, also in remote regions and/or MS for which currently not much eIAS services were developed.

SPECIFIC OBJECTIVE 4: Through the development of eIAS services, Option 2 would in the end strengthen the competitiveness of the European industry and service sector. First of all, by using eIAS the European industry and services sector could innovate some steps of their internal and external processes. The development of on-line services could be positively impacted since the concept of "notified eID" would allow that the private sector could benefit from the important roll-out of eID already realised by many MS. Furthermore, the mutual recognition and acceptance of these eID would stimulate the development of on-line services, especially at the cross-border level, for both the public and private sector. Option 2 would remedy the current market fragmentation, creating an important harmonised outlet market for eIAS which could also attract investments from outside the EU. The possibility for MS to implement the Services Directive without compromising on security or trustworthiness would furthermore decrease the administrative barriers for setting up a business in any EU MS.

SPECIFIC OBJECTIVE 5: The regulatory approach of Option 2 would finally also help ensure that all consumers can benefit from the advantage of (cross-border) eIAS services. Making eIAS a mass product would furthermore avoid that costs of implementation create a barrier to this participation. Finally, the cross-border and cross-sector use of notified eIDs could strongly reduce the complexity of eIAS (e.g. multiple devices, passwords, etc.), and remedy the main obstacles related to eIAS currently impeding the access to (on-line) services in rural areas. This view was also expressed in an expert survey organized between August and October 2011 by the SSEDIC Network[82]. Based on replies from 211 experts (comprising representatives of the IT & Telecoms sector, as well as public sector representatives, consultants and academics/researchers), 88.6% of respondents agreed that "there should be a clear common legal framework for the use of eIDs at the European and even international level", and 77.1% of respondents agreed that "digital identities should be subject to EU regulation"[83]. Thus, this position has clear support among stakeholders.

Coherence of Option 2:

Option 2 is to a very large extent contribution to the achievement of the overarching objectives of EU policy (cf. EU2020 Strategy, DAE, Single Market Act and the Roadmap to Stability and Growth) as presented in 1.2.

5.1.4. Assessment of Option 3: Expansion to incorporate certain related trust services

Option 3 further expands the legal framework for trust services to include certain related trustservices: time stamping, electronic seals, long-term preservation of information, certified e-document delivery, admissibility of electronic documents and website authentication.

[82] Scoping the Single European Digital Identity Community; see http://www.eid-ssedic.eu/

[83] See http://www.eid-ssedic.eu/images/stories/pdf/SSEDIC%20GA%20part%202_V1.1.pdf, slide 48

Indeed, a strong interconnection between e-signature, eID and related trust services is required in order to create a trusted environment. The implementation of provisions on related trust services would have a positive impact on the legal recognition of a range of cross-border interactions. Indeed, in order to ensure the legal validity of certain electronic interactions in cross border scenarios (as at national level), the e-signatures that might be used are not the only relevant component.

These other components include the time and the duration of the interaction, its content, the channel of communication, and the participants themselves. Without certainty on the legal validity of all these components in case of conflict, businesses and citizens would remain reluctant to use the digital interactions as their natural way of interaction.

The Public Consultation also addressed this issue, asking respondents to indicate for which trust building services and credentials legal or regulatory measures should be considered at EU-level in order to ensure their cross-border use. This resulted in the following overview:

64,57% of respondents asked for provisions on certified electronic documents, 52.39% on time stamping, 51.67% on electronic seals, 46.65% on certified delivery of email, 45.69% on long term archiving and only 6,22% felt that no further services required any regulation (see table in annex 7). This shows a very wide support among stakeholders for the notion that greater efficiencies in the underlying processes could be achieved through a broader policy approach.

Each of these related trust services has multiple possible use cases, and will have advantages and drawbacks that might not be shared with other related trust services. Therefore, in the section below, we will first briefly examine each related trust service separately, before assessing the option as a whole.

Selected individual related trust services

1. Qualified **time stamps** and **time stamping services** are required to introduce a non disputable time stamp on a signed document which serves as a proof that it existed at a point-in-time and that it has not changed since then. *Example of use case: somebody has submitted by e-mail at 23:55, his application to a competition with a deadline at midnight but the e-mail was delayed for some technical reason. With a time stamp, the e-mail delay would have no consequence.* So far at least AT, CZ, DE, EE, ES, FR, GR, HU, IT, LV, LT, LU, PL, PT, RO, SK, SL and ES have integrated or are considering to integrate time stamping in their national legislation. Given the high number of MS integrating this service in their national legislation, a common EU framework regulating time-stamping will undoubtedly contribute to a successful and interoperable cross-border use of electronic signatures.

2. *Qualified information preservation services through signing. This s*ervice makes use of electronic signatures and time-stamping to maintain the authenticity and integrity of documents when stored over long periods[84]. *Example of use case: electronic university degrees have to be kept for decades and are regularly submitted to third parties during the course of the career of their owner.* Already/about to be in AT, BE, CZ, DE, EE, FI, FR, HU, IT, RO and SK legislation. The wide application of this service in the MS also calls for the need of a EU framework in order to ensure interoperability across MS.

3. **Qualified electronic seal which is equivalent to the e-signature of a legal person.** *Example of use case: using a qualified e-seal, a company could issue millions of authentic invoices matching EU legal requirements; without e-seals, a responsible person of the company should sign each invoice separately to reach the same level of legal certainty.* Already or about to be implemented in AT, CZ, DE, EE, ES, IT, LV and PL legislation.

4 Qualified **certified e-document delivery** service which is the electronic equivalent to registered mail at EU level. *Currently, the legal effect of the "registration" stops at the border of the Member State of origin of an e-mail unless the Member State of destination recognises the registered nature of the email via a bilateral agreement.* Already implemented in BE, DE, DK, FI, FR and IT legislation.

5 **Recognition and acceptance of e-documents**: to establish the conditions of equivalence of a native electronic document with a paper document and the equivalence of a scanned document with its paper original. This is the *sine qua non* condition for paper less business to take-up (indeed, businesses need legal certainty that their electronic documents will be recognised by third parties like paper documents). Already or about to be implemented in AT, BE, EE, ES and PL legislation. *For instance, AT has introduced the concept of official signature, which provides for legal equivalence to official attestations and supports the validation of print-outs.* Again, different regimes may lead to Member State A not recognising an e-document legally valid in Member State B.

6 **Website authentication:** an obligation for legal person's website to include trusted information (e.g. a certificate) allowing the user to verify the authenticity of the website and the existence of the legal person. Users will benefit from website authentication because they will be sure that the information they get from the website is genuine or that they will carry out a transaction with the real organisation. Organisations will equally benefit from the assurance that no hacker can to set-up a fake website that could ruin the organisation's reputation or rob their transactions with their users. *Website authentication is becoming fairly common: when the address of a website becomes green in the browser, it means that the website is authenticated with a certificate. However, the conditions of issuance of website certificate depend on the commercial practices of producers of mainstream web browsers: i.e. the level of guarantee is unknown to the user. Furthermore, not all EU organisations are securing (yet) their website with this kind of mechanism.*

All services would be subject to supervision if they are offered at a high security (qualified) level, to ensure their cross border validity.

[84] Some signed documents need to be kept for decades. A recent e-signature is almost impossible to forge today but will be easily forged in ten years. Therefore, a "qualified" service provider (i.e. matching given reliability requirements) will put an

Economic, social, environmental impacts and administrative burden of Option 3

Economically and socially speaking, the creation of new (cross-border) activities related to the related trust services would bring competition at the EU level, leading to lower prices in the medium term. These new service developments would imply high-level job creation but could also provoke low level job losses, specifically in sectors with high usage of paper-based services today. It is however impossible to assess whether the job creation due to a successful technological sector development (e.g. certified delivery email) will perfectly balance the loss because of the cessation of paper-based activities (e.g. a specific branch of the postal sector). However, increasing economic efficiency through modernization generally has a beneficial impact on jobs and economic growth, with a McKinsey report showing that e.g. in France, the Internet economy *"generates 2.6 jobs for every job cut and at times accounts for 25% of net employment creation"*[85].

Employment and regional development could be beneficially impacted by a broader eIAS framework. The number of citizens working in another Member State was reported to stand at 5.8 million citizens in 2009, equivalent to 2.5% of the EU working population[86]. This shows the societal importance of facilitating access to electronic cross border services, especially in the light of cross border eVoting, and cross border access to eJustice and eHealth. These are practical issues that European citizens working in a different Member State than their home country must be able to resolve efficiently in order to go towards a European Citizenship in the Digital Single Market.

Administratively and environmentally speaking, the completion of the scope of the current electronic signature framework will lead to a safe and legally-proof contractual area allowing stakeholders to interact completely in a digital way. This would lead to a simplification of administrative procedures (in B2B, B2G, B2C and G2C interactions) as well as to a massive reduction of paper-based processes. Indeed, the replacement of paper-based interactions by electronic interactions allows for savings to be realised at many different levels such as postage, printing costs, processing time, ease of reuse of information, reduced error rates in data processing, transportation costs, archiving costs, etc.

A study from the Finnish University of Jyväskylä showed that fully electronic invoicing dropped costs from 8,60 EUR per invoice to 1,89 EUR per invoice (-78%)[87]. According to a CapGemini study funded by the Commission, savings of 70 to 75% were realistic, and cost savings through generalised European e-invoicing for B2B transactions alone could amount to 40 billion EUR per year[88]. To achieve these results, however, full management of the e-invoicing lifecycle is necessary. This includes components such as time stamping, e-document delivery and e-archiving, which are related trust services and currently not yet a part of the European policy framework.

The results of the SME Panel quoted above corroborate this to a certain extent, with surprisingly high self-reported take-up numbers for e-invoicing (28%) and especially electronic archiving (35%). Thus, market interest in these services clearly exists, even when (as in the case of electronic archiving) no clear legal framework for these services has been implemented. An expanded legal framework (as contemplated by Option 3) would only expand this appeal.

Effectiveness of Option 3 (cf. detailed assessment presented in Annex 11):

---

electronically authenticated document in an "electronic envelope" and seal it electronically with state-of-the-art technology. Some years later, the service provider will put the previous envelope in a new one that it will seal again, and so on, to always be a step ahead of hackers. This service (which may not cost more than a few cents) will ensure the legal validity of e-signatures through time. NB. The storage means and place of the "envelope" is not relevant: it can be with the customer, the preservation service or any other third party.

[85] This has applied to France since 2000. "The impact of the Internet on the French Economy", McKinsey. March 2011

[86] Eurostat

[87] See http://www.ebrc.fi/kuvat/215-229.pdf

[88]

The detailed assessment of the economic, social and environment impacts of Option 3: *"Expansion to incorporate certain related trust services"* indicates that there are significant benefits to be gained from a broader EU policy covering at least certain related trust services.

SPECIFIC OBJECTIVE 1: Option 3 is significantly more effective than option 2 in increasing the availability and take-up of cross-border and cross-sector eIAS services by completing the ecosystem for trust services remaining incomplete under option 2 in the absence of other fundamental building blocks.

SPECIFIC OBJECTIVE 2: The assessment shows that market fragmentation already exists for some related trust services, such as eSeals, time stamping and certified eDocument delivery, as a result of some Member States being more proactive in establishing national legal frameworks for such rules. In the absence of harmonising provisions at the European level, the European internal market would thus be distorted.

SPECIFIC OBJECTIVE 3 & 4: Moreover, certain gains expected from the legal framework for trust services (such as improved accessibility of services, increased efficiencies, stimulating innovation) depend on a scope of regulation that goes beyond e-signatures and eID. Excluding related trust services would lead to situations where e.g. documents could be signed electronically, but not exchanged reliably (i.e. in a way that could be shown in court to be legally effective) nor archived over a longer period of time. Paper would remain crucial for such processes, thus reducing the potential beneficial impact of European policy intervention, and discouraging the investment in innovative services.

SPECIFIC OBJECTIVE 5: Option 3 is more effective in ensuring that all end-users can benefit from the advantage of (cross-border) trust services, specifically by ensuring that related trust services can be used in cross border scenarios as well.

Coherence of Option 3:

Option 3 is fully contributing to the achievement of the overarching objectives of EU policy (cf. EU2020 Strategy, DAE, Single Market Act and the Roadmap to Stability and Growth) as presented in 1.2.

Expected Impacts of the different options

Advantages of options				
	Option 0 **No Action**	**Option 1** **No Policy change**	**Option 2** **Revision of eSignature Directive and Mutual recognition and acceptance of eID**	**Option 3** **expanding to related trust services**
Economic impact	Free "budget area" for Member States that could be open for other kind of expenses.	Stand-still situation means no further expenses for Member States and CSPs.	Investments made in large scale pilot projects would bring full benefits & increase competition in the national market by a "de jure" and "de facto" possibility for foreign companies to enter it. This leads to an important increase of economic development at the EU level.	Creation of new cross-border sector of activities
Social impact			High level-Job creation	Creation of high-level jobs to implement and run the systems
Environmental Impact			No need for travelling and filling in paper documents thanks to the opportunity given to identify online. Reduction of paper based relationships thanks to the possibility to identify your	Completion of the process of giving up paper based relationships by ensuring the time, value of the document and validity through time of the agreement. Further

			recipient and the possibility to agree on the terms of your agreement with an electronic signature.	increase in possibilities for saving paper.
Administrative burden	For those Member States that would still align themselves to the directive or for those who decide to stop their national legislation on eSignature - decrease of administrative burden directly related to the implementation of eIAS regulation.	No additional administrative burden at national level as the situation stays at it is.	Simplification of the procedure when interacting with stakeholders established in a different MS and with authorities established in the same MS. Decrease of administrative burden in the medium-turn as a direct consequence of the eIAS framework.	Further decrease of administrative burden at national level in the mid and long-rum, enabled by the usage of eIAS,including related trust services.
Disadvantages of options				
Economic impact	Investments in the establishment of the current infrastructures would be lost. This impacts MS but even more the CSPs that would be put in a situation of total legal uncertainty.	High risk to see the eIAS services being reduced to a "lost budget area" for Member States spending money for the administration of a non-functioning sector.	The need to create the interfaces and infra-structures needed for the cross-border inter-operability of eIDs will have a budgetary impact for Member States	The need to create the interfaces and infra-structures needed for the cross-border inter-operability of eIDs will create have a budgetary costs impact for Member States
Social impact	Jobs losses both at private and public level. Missed opportunities of having access to services from rural areas	Missed opportunities of opening up new markets and thus creating new jobs, the high risk of failure in the development of eIAS services would lead to job losses	Possibility of low-level jobs losses	Possibility of low-level jobs losses (specifically in sectors covered by "paper services" like certified delivery mail)
Environmental Impact	Missed opportunity for moving towards paperless transactions and thus a cleaner environment	Missed opportunity for moving towards paperless transactions and thus a cleaner environment		
Administrative burden	For the MS that stop their eIAS legislation: missed opportunity to streamline processes		The need to maintain the interfaces and infrastructures for the cross-border interoperability of eIDs will create administrative burdens for MS.	As the bodies needed for the administration of the eID and eSignature sector would be mutatis mutandis the same that the one needed for related trust services, not much additional increase of the administrative burden is expected compared to Option 3.

Cost of governance

The cost of governance relates to the costs incurred by the public authorities that are charged with the development and maintenance of the regulatory approach for eIAS. Depending on the option chosen, these global costs can significantly differ. Also, the distribution of the cost of governance between the EU level and the MS can be impacted depending on the option chosen, as shown in the table below.

	Option 0 No EU Policy	Option 1 Status Quo (No policy change)	Option 2 EU Regulation for eSignature and eID	Option 3 EU Regulation for eSignature, eID and expansion to ancillary trusted services
Cost of Governance				
At the EU level				
Development of regulatory framework for eIAS	N/A	The framework was already previously developed.	An expanded framework would need to be developed	A comprehensive framework for eIAS and ancillary trusted services would need to be developed
	No cost	**No - Low cost**	**Medium cost**	**High costs**
Maintenance of regulatory framework for eIAS	N/A			
	No cost	**Medium cost**	**Medium cost**	**Medium cost**
Impact on other EU Policies	A large number of EU Policies that currently refer to the existing Directive 199/93/EC will need to be amended.	Some synergies could be realised, but these are limited (e.g. the Services Directive cannot be implemented)	More synergies could be realised.	Synergies could be realised.
	Medium cost	**Low cost**	**No - Low costs**	**No - Low costs**
At the national level				
Development of regulatory framework	Each MS will need to develop its own regulatory approach for all eIAS, incl. ancillary trusted services; MS cannot benefit for support at the EU level (e.g. including also not for the development of standards, minimum requirements, ...)	Each MS will need to develop its own regulatory approach for the services other than eSignatures	Each MS will need to develop its own regulatory approach for the other services than eSignatures and eID	Each MS will be able to rely on an EU framework for all eIAS and ancillary trusted services
	High cost	**Medium - High cost**	**Medium cost**	**Low cost**
Maintenance of regulatory framework	Provided the very evolutive nature of the eIAS market, the regulatory framework will (esp. Standards) will need regular revision. Without any EU policy for any eIAS, it can be expected that there will also be very limited support to MS when maintaining their regulatory framework.	MS need to assist to EU working groups regarding the development of requirement, standards, etc. For eSignatures. For the other services, they need to keep up-to-date their skills, standards, ... theirselves.	MS need to assist to EU working groups regarding the development of requirement, standards, etc. for eSignatures and eID. For the other services, they need to keep up-to-date their skills, standards, ... theirselves.	MS need to assist to EU working groups regarding the development of requirement, standards, etc. for all eIAS and ancillary trusted services. They can however heavily rely on the support of the EU.
	High cost	**Medium cost**	**Medium - Low cost**	**Low cost**

5.2. Legal instrument of the Framework

5.2.1. Option A. One instruments vs Option B. two instruments

Providing a comprehensive framework within **one instrument (Option A)** would contribute to ensure the consistency of the legislations regulating the different elements of eIAS products and services. Indeed, electronic signatures and electronic identification are inseparable when analysing the requirements needed to ensure legal certainty, trust and security in electronic transactions. In this regard, common provisions and principles are needed in order to create a safe digital environment.

Following this reasoning, using **two separate instruments (Option B)** could introduce slight differences in the legal provisions adopted for both electronic signatures and electronic identification – and more important, in the orientation of the initiatives. These differences could lead to hamper the take up of eIAS products and services and, in extension, the use of electronic interactions.

5.2.2. Option C. Directive vs Option D Regulation

The Commission plans to table a proposal with the aim to harmonise the national transposition laws on electronic signature and create a secure legal framework for the mutual recognition of notified eIDs and related trust services.

In this regard, adopting **a Directive (Option C)** has shown its limits since 1999. Indeed, the freedom given to MS when transposing a Directive (in terms of interpretation and of implementation of the systems) contributed to the current problems of mutual recognition of services and products and of cross-border interoperability. Moreover, the delays inherent to a Directive's implementation period would not allow the expendiency matching the needs of other EU legislation like the Services, Public Procurement or VAT (e-invoices) Directives.

Delays may also jeopardise the efforts and investments made in large scale pilots by Member States and the Commission to provide EU-wide electronic services.

Meanwhile, **a Regulation (Option D)** provides immediate applicability and stronger harmonisation. Indeed, the objective of the Commission is to present an immediate solution to current problems and develop a long-term-use instrument. In this respect, the direct applicability of a Regulation will contribute to solving problems of harmonisation, and will avoid the interpretational issues that have plagued the e-Signatures Directive since its adoption, thus better fitting the purpose of the proposed legislation than a Directive. Furthermore, a Regulation would be capable of providing quick relief for the challenges currently encountered by leading European and national eIAS initiatives.

5.3. Level of supervision of e-Trust services

5.3.1. Option i: Maintaining national supervision scheme

Under this option, the new legislation will maintain the current national based supervision scheme and impose on Member States the responsibility to supervise the activities of service providers by following minimum essential requirements. In particular, MS should ensure that service providers fulfil the obligations provided for in the new legislation in order to manage the risks posed to security of the provided electronic services. The new legislation would thus strengthen the national supervision of trust service providers by:

- defining the specific tasks of the supervisory body;
- setting clear rules concerning notification of security breaches;
- specifying essential rules for supervising service providers (e.g. regular audits);
- verifying compliance with requirements for qualified electronic service providers (e.g. ensuring financial resources for their activities);
- ensuring mutual assistance between Member States supervisory bodies to facilitate the cross-border supervision of trust service providers;
- establishing a system of peer review by Member States of their respective supervision schemes to reinforce mutual trust.

Moreover, the current supervision system, only applicable to electronic signatures, will be extended to the full set of related trust services in order to ensure an adequate level of security for all of the aspects of a transaction.

It is assumed that the homogeneity of supervision that would result from common essential supervision requirements of eIAS services and related trust services would increase trust, facilitate fraud detection and foster the development of measures to prevent identity theft.

The harmonised approach at EU-level for both e-signature and related trust services, improving effective supervision would enhance legal certainty, trust and security of electronic transactions, leading to convince more social groups (e.g. through an effective communication strategy) to participate to the digital single market.

5.3.2. Option ii: Establishing an EU-based supervision system ('advanced variant')

Under this option, the framework adds an EU-based supervision system for the trust service providers covered by the relevant regulatory instrument.

As noted in the detailed descriptions in Annex 14, two sub-options exist: under the first one, a European supervision would *replace* national supervision schemes, under the second sub-

option, an European supervision exists as a *complement* to national supervision schemes[89]. Option ii can furthermore be implemented based on a *centralised* model, in which a single body at a single location is established, or on a *decentralised* model is chosen in which some tasks of the European body are delegated to local organisations.

In general, it can be assumed that adding an EU-level to the supervision of the eIAS market would be **beneficial for the credibility** of the supervision mechanism. Depending on the variant chosen, the market would know that the consistent application of supervision requirements is monitored by a European body or would be aware that supervision will be entrusted to an adequately staffed and funded body, either locally or at the EU level.

As such, it would **further increase the effectiveness of Options 2 and 3** of which the basic variants have a harmonised national supervision model (based on a list of minimum requirements). Indeed, a credible supervisory system could contribute strongly to the building of trust and confidence, which is crucial for the development of the eIAS market.

The most effective option would appear to be federated EU supervision (retaining national supervision bodies) with delegation power for Member States, closely followed by decentralised EU supervision (eliminating national supervision bodies). Only a purely centralised supervision approach compares negatively to the current system.
The cost effectiveness of a European supervisory body could be further bolstered by foreseeing other responsibilities. Mainly, such a body could be designated as an EU point of contact for international discussions on trust services, thus working towards achieving international interoperability, an area in which the current e-signatures Directive has proven ineffective. At a more operational level, the body could also be put in charge of the supervision of trust service providers established outside of the EU that also wish to be supervised in Europe on a voluntary basis, in order to benefit from the same status and certainties as their European counterparts. These additional possibilities however would create equal advantages in any one of the sub-options, and thus do not factor into their internal comparison.

Nonetheless, in spite of the advantages related to EU supervision, it should be noted that it should be noted that MS during consultations have expressed **serious reservations** about the need for - and value added of - EU supervision, whilst several raised subsidiarity concerns. The experience has shown that supervision can be conducted by MS although common requirements with tangible guidelines and the exchange of best practices is required to ensure trustworthiness and interoperability.

5.3.3. Comparison of costs (cost-efficiency) of managing the supervision schemes

National supervision schemes

While no exact data is available on current national supervision costs, certain trends can be derived from an informal questionnaire sent to Member States during the impact assessment.
The total operational costs for running a supervision scheme seem to range between €100.000 and €200.000 for an average sized MS. Estimates from larger MS are either unavailable or ambiguous as they do not indicate total operating costs. Costs for service providers to get supervised vary quite substantially, due to the role of private sector independent auditors conducting the actual audits and charging these separately. Based on the available data, a cost

[89] A specific task that could be envisaged for the EU supervisory body could be an 'optional supervisor of any European trust service provider'. However, this does not appear to be a viable or desirable option, as it creates a clear risk of 'forum shopping' and competition between national and European supervision bodies: a service provider who is negatively assessed by a national body might be tempted to turn to the European body as a de facto body of appeal. This situation would undermine the authority and competence of national bodies and install uncertainty.

for service providers of €25-30.000 per year seems normal if private auditing is required, and €3-5000 per year if the supervisory body conducts the audits itself. After investigation, between 1 and 10 CSPs are located in a Member State, which leads to a maximum total cost of €300.000 (for countries as Germany or Italy if the supervision is delegated to a private company.)
Expanding the scope of the supervision scheme under option 2 would obviously increase costs somewhat, but there would be possibilities to re-use and pool resources.In term of costs, supervising two types of services is therefore not twice as expensive as supervising one. Some Member States already supervise time-stamping service providers, and their costs do not appear to be significantly higher than other Member States. As a limited but interesting data point, one Member State indicated that the supervision for qualified eSignatures costs €4500. According to its response: "If the CSP provides only qualified time-stamping services, the fee of the initial supervision audit as well as the annual fee for regular supervision amount to €1500", i.e. the cost of initial registration is only 30% and the costs of annual audits are 50%."
Even assuming that national supervision costs would double under option 3 in comparison with the current supervision model (only related to e-Signatures) **i.e. an additional €150.000 EU average per Member State**, the total additional cost of the new supervision scheme compared to the status quo would be around 27x€150k, **or approx. €4M**.

EU Based supervision schemes

In order to establish an EU based supervision scheme, the EU would have to set up a new agency. The European Network and Information Security Agency (ENISA) is, from our point of view, representative of the size of the agency which would be needed in order to properly carry out the supervision of the CSPs in the 27 Member States. The budget allocated to ENISA for 2012 is **€8.5M**. Even doubling our estimation of costs at the national level, the establishment of an EU based supervision scheme would be more expensive.
The table below gives an overview of the costs related to supervision under the different scenarios developed above:

	Basic variant for Option 2 and 3 : Harmonised supervision at the national level (list of minimum requirements)	Advanced variant: EU supervisory body while cancelling national supervision		Advanced variant: : EU supervisory body while maintaining national supervision
		Centralised model (one single body at a single location)	Decentralised model (some tasks of the European body are delegated to local organisations)	Federated model
Cost of managing the Supervision				
At the EU level				
Cost of setting up and running the supervisory body	N/A	Need to establish a new European level body or to charge an existing body with supervisory tasks	Need to establish a new European level body or to charge an existing body with supervisory tasks	Need to establish a new European level body or to charge an existing body with supervisory tasks. This EU body could also take up the supervision responsabilities of MS (at the demand of these MS) where no or few trust service providers need to be supervised
	No cost	**High cost**	**High cost**	**Medium cost**
Travelling costs for EU body	N/A	Since the agents need to supervise service providers established across the EU and local audits are sometimes needed, the centralised approach could lead to very high travelling costs (also the producers could incur high travelling costs when they need to present theirselves at the supervisory body).	Travelling by the EU agents would be limited since a network of national points of presence would be set up (by means of private contractors) for tasks that require physical presence.	Travelling by the EU agents would be limited since the existing network of national supervisory bodies would be used for tasks that require physical presence.
	No cost	**Medium to High cost**	**Low cost**	**Low cost**
Cost of contracting private companies (by the EU body)	N/A	N/A	In each MS, private companies would be contracted for executing local audits. The remuneration of the companies would be variable (in function of the number of audits done) and would not imply fixed cost engagements.	N/A
	No cost	**No cost**	**Low to Medium cost**	**Low cost**
Total at European level	**0 million EUR/ year (for all EU 27)**	**Approximately 8.5 million EUR (cf. budget for ENISA as a proxy)**	**Maximum 8.5 million EUR (cf. budget for ENISA as a proxy)**	**Maximum 8.5 million EUR (cf. budget for ENISA as a proxy)**
At the national level				
Cost of setting up and running the supervisory body	Each MS needs to set-up and run its own supervisory body, so there are 27 bodies in total. These are all separately organised, staffed and funded.	Cancellation of the national supervisory bodies	N/A	Each MS (except those who delegate their supervisory responsabilities to the EU level) needs to set-up and run its own supervisory body, so there are 27 bodies in total. These are all separately organised, staffed and funded.
	Medium cost	**No cost**	**No cost**	**Medium cost**
Travelling costs for national bodies	Travelling costs for e.g. local audits are limited since distances are limited	N/A	N/A	Travelling costs for e.g. local audits are limited since distances are limited
	Low cost	**No cost**	**No cost**	**Low cost**
Total at national level	**Approximately 4 million EUR/ year (for all EU 27)**	**0 million EUR/ year (for all EU 27)**	**0 million EUR/ year (for all EU 27)**	**Approximately 4 million EUR/ year (for all EU 27)**

There are clear indications of possible improvement in the credibility and effectiveness by establishing an EU based supervision system. However, given the strong reservations in accepting EU intervention, it is concluded that supervision should be maintained at the national level.

6. COMPARISON OF THE OPTIONS

The table below[90] presents an overview of the scores per operational objective and per policy option. Please note that the reasoning behind the scores is presented in detail in Annex 10. The detailed determination of the expected impacts per policy option was executed through a data analysis exercise which consisted of desk research, discussions with experts as well as internal brainstorming. These impacts were furthermore cross-checked with the contributions to the public consultation of the Commission[91] and elements related to the assessment by the different stakeholders were added.

[90] The assessment of all of the impacts under each of the options was done by analysing the magnitude of the expected impact, as well as the likelihood that the impact will actually occur as a result of the proposed policy option.
The notation used to express the magnitude (compared to the baseline scenario) is the following:
- - - very negative impact
- - negative impact
- slightly negative impact
0 no impact
+ slightly positive impact
+ + positive impact
+ + + very positive impact

[91] See Annex 4.

The table below presents the aggregated outcome of this assessment work and allows for an easy comparison of the way in which each option contributes to all of the specific objectives and thus the general objectives as presented in Chapter 3.

Options	**0**	**1**	**2**	**3**
Objectives	**Repeal of the existing Directive (No EU Policy)**	**Baseline option (No Policy change)**	**EU framework for e-signature and eID (with supervision at national level)**	**EU framework for e-signature and eID and related trust services (with supervision at national level)**
EFFECTIVENESS				
Overall objective				
Harmonised general trust framework for electronic transactions as a building block for the Digital Single Market,	--	0	++	+++
Operational objectives				
Ensure usage of notified eID by public and private sectors	0	0	++	++
Ensure effective supervision model for eIAS	--	0	++	++
Ensure mutual recognition and acceptance of notified eIDs	0	0	++	++
Ensure interoperability of eIAS (cross-border and cross-sector)	--	0	++	++
Ensure maximum reduction of administrative burden and increase of quality of services (awareness raising)	-	0	++	+++
Ensure trust and confidence in the legal certainty and security of eIAS services	-	0	++	+++
COHERENCE				
Coherence with the overarching objectives of EU policy (cf. EU 2020 Strategy, DAE, Single Market Act and the Roadmap to Stability and Growth)	---	--	++	+++
EFFICIENCY				
Global cost-efficiency for achieving the objectives	--- N/A (Objectives are not achieved)	--- N/A (Objectives are not achieved)	++ Additional cost of governance ad implementation cost required. No fundamental difference at the level of supervision costs compared to Baseline scenario	++ Additional cost of governance ad implementation cost required. No fundamental difference at the level of supervision costs compared to Baseline scenario

Concerning the ***Scope of the Framework***, the detailed assessment of Option 0 indicates that in general, without an EU Policy, the operational and thus specific and general objectives

cannot be reached. Also, the baseline scenario would not allow meeting any of the objectives mainly because the scope of the current Directive 1999/93/EC is limited to e-signatures only. Option 2, adding provisions on mutual recognition of notified eIDs, would significantly contribute to achieve each of the objectives identified above and results in various positive economic, social and environmental impacts. However, possibilities would remain limited if there is no access to harmonised related trust services for which legal certainty and technical security is ensured. The conclusion that emerges consistently from the section above is that related trust services are essential in order to provide the trust and legal certainty needed to ensure that citizens and businesses can rely on interactions in the electronic world as they do in the physical environment. Thus, a comparison of these different policy options suggests that **Option 3** is the most suitable to meet the objectives of the initiative.

The choice of the ***legal instrument*** is fundamental in view of ensuring that the initiative will create a more efficient framework for electronic interactions. In this context, one single legal framework (**Legal instrument - Option A**) seems to be the most efficient and effective instrument to attain the general objective of the initiative. Moreover, a Regulation seems to be more appropriate than a Directive. Indeed, the objective being to bring forward immediate solutions to current problems and develop a long-term-use instrument. In this respect, the direct applicability of a Regulation will better fit to solve the existing issues. **(Legal Instrument – Option D)**

Concerning the adequate ***level of supervision*** to be adopted, in terms of effectiveness, efficiency and coherence, both national systems and EU based scheme are equivalent. However, the potential reluctance of Member States and the risk to hurt the principle of subsidiarity, suggest to go for the improvement of the current national supervision model (**option i "Maintaining national supervision scheme"**)

7. MONITORING AND EVALUATION

The Commission is the guardian of the Treaty and therefore will monitor how Member States have implemented the changes in the electronic signature Framework and the necessary measures on electronic identification and related trust services. Where needed, the Commission services will offer assistance to Member States for the implementation of the legislative changes in the form of workshops with all the Member States or bilateral meetings at the request of any of them. When necessary, the Commission will pursue the procedure set out in Article 258 of the Treaty in case any Member State fails to respect its duties concerning the implementation and application of Union Law.

The Commission will be monitoring the application of the legislative framework

Progress indicators to monitor the application of the legislative framework:

1. Existence of eIAS suppliers that have activities in multiple EU member states:
2. Usage of eIAS services by eService providers in other sectors than the “traditional closed niche sectors”;
3. Degree to which devices become interoperational (e.g. eCard readers) between sectors, countries;
4. Usage of eIAS by all categories of population (cf. via ‘Household survey’-type questionnaires);
5. Follow-up of reasons why consumers remain reluctant to use eIAS (cf. via ‘Household survey’-type questionnaires);
6. Extent to which eIAS are used by end-users for national transactions and international (cross-border) transactions;
7. Degree of harmonisation across members states when regulating eIAS (incl. related trust services).
8. Official eIDs notified to the Commission
9. Services accessible with notified eIDs in the public sector (eGovernment, eHealth, eJustice, eProcurement)
10. Services accessible with notified eIDs provided by central, regional, local authorities
11. Services accessible with notified eIDs provided by Points of Single Contact
12. Electronic delivery systems accessible with notified eIDs

13. Services accessible with notified eIDs in the private sector (online banking, eCommerce, eGambling, login to websites, safer internet services e.g. chatrooms for children)

Moreover, the new legislative framework will request Member States to provide the European Commission with statistics based on their supervision activities.

The Commission will be mainly responsible for collecting the data presented above mostly through desk research, online surveys, conferences, workshops, etc. External contacts for more specific data collection may be required, as well as cooperation with. Nonetheless, the data collection related to the monitoring of the legislative framework are not likely to result in significant additional costs.

The evaluation of the impact of the application of the new Framework could take place four years after the entry into force of the legislative measure in the form of a Commission report to the Council and the European Parliament. Indeed, the period of two years left for evaluation of the current electronic signature Directive proved to be too short to obtain informative quantitative figures measuring the impact of the Directive in all the areas concerned. In order to measure efficiently the impacts mentioned above, 4 year-period seems also appropriate as it is necessary to take into account the possible progressive modification of behaviour of the different stakeholders and the possible development of new technological instruments over time.

ENISA could be involved to evaluate security issues that may arise in the Framework operation.

ANNEX 1 – LIST OF ACRONYMS AND GLOSSARY

CAGR	Compound annual growth rate
CIP	Critical Infrastructure Protection
CSP	Certification Service Provider
CEF	Connecting Europe Facilities
CEN	European Standards Committee
DAE	Digital Agenda for Europe
DSM	Digital Single Market
EEA	Economic European Area
eID	Electronic identification
eIAS	Electronic identification, authentication and signature
EHIC	European Health Insurance Cards
ETSI	European Telecommunications Standards Institute
EU	European Union
HSM	Hardware security module
ICT	Information and Communication Technologies
IETF	Internet Engineering Task Force
LSP	Large Scale Pilot project
MS	Member State of the European Union
PIN	Personal identification number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
SMA	Single Market Act
SME	Small and Medium Enterprise
TSPs	Trust Service Providers
TTP	Trusted Third Party
UNCITRAL	United Nations Commission on International Trade Law

GLOSSARY

Advanced Electronic Signature	"advanced electronic signature" means an electronic signature which meets the following requirements: • it is uniquely linked to the signatory; • it is capable of identifying the signatory; • it is created using signature means that the signatory can with high level of confidence maintain under his sole control; • it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. (art. 2.2, Directive 1999/93/EC)
Authentication	Electronic process that allows the validation of the electronic identification of a natural or legal person; or of the origin and integrity of an electronic document;
Certified e-document delivery	Service that makes it possible to transmit data by electronic means and provides evidence relating to the handling of the data, including proof of sending or receiving the data, and which protects transferred data against the risk of loss, theft, damage or any unauthorised alterations;
Connecting Europe Facility	EU proposal aiming at maximising the potential for growth through the realisation of synergies between transport, energy and telecommunications policies and their implementation, thus enhancing the efficiency of the Union's intervention.
Conversion of paper to eDocuments	Ensuring that paper documents can be converted into electronic equivalents without losing their legal validity; this can be thought of as an electronic equivalent to the paper certified copy (*copie conforme*).
Digital Agenda for Europe	EU initiative aiming at delivering sustainable economic and social benefits from a digital single market based on fast and ultra-fast internet and interoperable applications.
Digitalisation	The process of converting information in analogue form into digital form.
Digital Signature	Mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit
eCODEX	An e-justice project to improve the cross-border access of citizens and businesses to legal means in Europe as well as to improve the interoperability between legal authorities within the EU.

Electronic Transactions	Dealings between people and organisations (such as finding out a piece of information, filling out a form, or making a payment) that take place using electronic networks.
epSOS	An European electronic Health (eHealth) interoperability project co-funded by the European Commission and the partners. It focuses on improving medical treatment of citizens while abroad by providing health professionals with the necessary patient data.
eSeals	Data in electronic form which are attached to or logically associated with other electronic data to ensure the origin and the integrity of the associated data;
e-Signature / electronic signature	data in electronic form which are attached to or logically associated with other electronic data and which are used by the signatory to sign
e-Signature product	Hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures
e-Signature Technology Providers	Producers of hardware and software for example electronic components (microchips, smartcards, tokens), and firmware/software products
e-Signature Solutions Integrators	Companies that assemble what provided by technology providers to create solutions for e-Signature scenario.
Europe 2020 Strategy	Europe 2020 is the EU's growth strategy for the coming decade in order to become, in a changing world, a smart, sustainable and inclusive economy which should help the EU and the Member States deliver high levels of employment, productivity and social cohesion. It implies a set of five ambitious objectives - on employment, innovation, education, social inclusion and climate/energy - to be reached by 2020. Each Member State has adopted its own national targets in each of these areas. Concrete actions at EU and national levels underpin the strategy.
Interaction	A two-way exchange of information.
Long-term preservation of e-signatures	To ensure the legal validity of electronic signature over extended periods of time, ensuring that e-signatures can be validated irrespective of future technological evolutions.
PEPPOL	Pan-European Public Procurement OnLine project, which aims at expanding market connectivity and interoperability between eProcurement communities. PEPPOL enables access to its standards-based IT transport infrastructure through access points, and provides services for eProcurement with standardised electronic document formats

Public Key	The publicly-known key associated with a given person's use of a public-key cryptographic system.
Public Key Infrastructure (PKI)	PKI is a set of hardware, software, organisation, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority
Private Key	The private (secret) key associated with a given person's public key for a public-key cryptographic system.
Qualified Certificate	Attestation which links validation data respectively to a natural or a legal person and confirms those data of that person, used to support trust services, issued by a qualified trust service provider and meet the requirements laid down in Annex I of Directive 99/93/EC;
Qualified Electronic Signature	Electronic signature which meets the following requirements: - it is uniquely linked to the signatory; - it is capable of identifying the signatory; - it is created using electronic signature creation data that the signatory can with high level of confidence use under his sole control; and - it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable; and has been created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signature;
Secure Signature Creation Device	Configured software or hardware used to implement the signature-verification-data
SPOCS	SPOCS (Simple Procedures Online for Cross- Border Services) is a large-scale pilot project launched in May 2009. SPOCS aims to build the next generation of online portals (Point of Single Contact or PSC), which every European country now has in place, in the context of the Service Directive
STORK	A competitiveness and innovation framework programme, co-funded by EU. It aims at implementing an EU wide interoperable system for recognition of eID and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State. It will also pilot transborder eGovernment identity services and learn from practice on how to roll out such services, and to experience what benefits and challenges an EU wide interoperability system for recognition of eID will bring.

SWOT Analysis	SWOT analysis is a strategic planning method used to evaluate the Strengths, Weaknesses, Opportunities, and Threats involved in a project or in a business venture. It involves specifying the objective of the business venture or project and identifying the internal and external factors that are favorable and unfavorable to achieve that objective. • Strengths: characteristics of the business, or project that give it an advantage over others • Weaknesses: are characteristics that place the project at a disadvantage relative to others • Opportunities: external chances to improve performance (e.g. make greater profits) in the environment • Threats: external elements in the environment that could cause trouble for the business or project
Time stamping	Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time
Token	When used in the context of authentication, a (usually) physical device necessary for user identification.
Trust services	Any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery and electronic certificates, including certificates for electronic signature, for electronic seals and for website authentication

Adapted from Modinis sudy

ANNEX 2 – INFORMATION SOURCES: LIST OF STUDIES, WORKSHOPS AND LITERATURE IN RELATION TO EIAS

Communications from the Commission

(1) Communication COM(2010)245 of 19.5.10 - A Digital Agenda for Europe.

(2) Communication COM(2011)206 of the 13.04.11 - Single Market Act

(3) Communication COM(2006)120 of 15.3.06 - Report from the Commission to the European Parliament and the Council on the operation of Directive 1999/93/EC on a Community framework for electronic signatures.

(4) Communication COM(2008)798 of 28.11.08 on an Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market.

(5) Communication on a "Proposal for a European Parliament and Council Directive on a common framework for electronic signatures", COM(1998)297 of 13.5.1998.

(6) Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: "Ensuring security and trust in electronic communication. Towards a European framework for digital signatures and encryption". COM(1997)503 of 8.10.1997.

(7) Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions "A coherent framework to build trust in the Digital single market for e-commerce and online services". COM(2011) 942 final

(8) Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: "Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century". COM(2012) 9 final

(9) Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: "A strategy for e-procurement". COM(2012) 179 final

(10) Communication on a "Proposal for a Directive of the European Parliament and of the Council on public procurement" COM(2011) 896 final

(12) Communication from the Commission "A roadmap to stability and growth" COM(2011) 669 final

(13) Communication from the Commission "Europe 2020 A strategy for smart, sustainable and inclusive growth" COM(2010) 2020 Final

European Legislation

(1) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

(2) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

(3) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

(4) Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts

(5) Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors

REFERENCES & STUDIES

Main related studies ordered by the Commission or related bodies

(1) Study on an electronic identification, authentication and signature policy (IAS study), 2012, INFSO, http://ec.europa.eu/information_society/policy/esignature/ias_crobies_studies/index_en.htm

(2) Study on the supply side of the market for e-signature, 2012, INFSO. (not yet published)

(3) Two Impact Assessment support studies on eID mutual recognition and on eSignatures to support the impact assessment, 2012, INFSO

(4) Online public consultation on electronic identification, authentication and signature, 2011, INFSO, http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision/pub_cons/index_en.htm

(5) "SME panel" survey on eSignatures and eID to identify business needs, 2011, ENTR/INFSO

(6) European Parliament report on electronic signatures, www.europarl.europa.eu/activities/committees/studies/download.do?language=en&file=41711 , 2011, EP

(7) Pan-European survey of practices, attitudes and preferences as regards personal identity data management, 2011, IPTS for INFSO

(8) Special Eurobarometer 359 - Attitudes on Data Protection and Electronic Identity in the European Union, 2011, INFSO / JUST / JRC

(9) Study on cross-border interoperability of e-signatures (CROBIES study). 2010, INFSO

(10) The state of the Electronic Identity market: technologies, infrastructure, services and policies, 2010, JRC/IPTS

(11) Feasibility study of a European federated e-signature validation service, 2010, DIGIT IDABC

(12) Several ENISA reports and position paper on eID and authentication – see www.enisa.europa.eu/publications

(13) Household survey 2010, http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-050/EN/KS-QA-10-050-EN.PDF , Eurostat

(14) Enterprise survey 2010, http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-049/EN/KS-QA-10-049-EN.PDF , 2010, Eurostat

(15) Study on eID interoperability for Pan European eGovernment Services, 2009, DIGIT IDABC

(16) Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive, 2009, MARKT

(17) Studies on the set-up of an Electronic Signature Service Infrastructure (ESSI) for the European Commission, 2009, DIGIT

(18) Study on mutual recognition of e-signatures for eGovernment applications, 2009, DIGIT IDABC 2009

(19) Flash Eurobarometer #250, Confidence in the Information Society, 2009, INFSO

(20) Study on the EU ICT Security Market, IDC, 2009, http://ec.europa.eu/information_society/policy/nis/strategy/activities/data_ict_market

(21) Study on the standardisation aspects of e-signature, 2007, INFSO

(22) The legal and market aspects of electronic signatures, 2003, INFSO Standardisation mandate m460 in the field of information and communication technologies applied to electronic signatures, 22.12.09.

(23) European Parliament resolutions "Completing the internal market for e-commerce", 21.9.10, P7_TA(2010)0320.

(24) European Parliament resolution "Internet governance: the next steps", 15.6.10, P7_TA(2010)0208.

(25) Report on a new Digital Agenda for Europe: 2015.eu, 25.3.10, European Parliament, Committee on Industry, Research and Energy, P7_TA(2010)0133.

(26) PORVOO reports, in particular "Regulating a European eID: a preliminary study on regulatory framework for entity authentication and a pan European Electronic ID ", Thomas Myhr, 31.1.2005, porvoo9.gov.si/Thomas_Myhr_report.pdf

(27) Eurostat Survey on ICT usage and e-commerce in enterprises, http://www.imamidejo.si/resources/files/ICT_usage_in_ent._2010.pdf

(28) United Nations Convention on the Use of Electronic Communications in International Contracts, http://ec.europa.eu/information_society/policy/esignature/docs/workshop_10_03/02_luca_castellani_uncitral.pdf

DISCUSSIONS, WORKSHOPS, CONFERENCES

Major events from which feedback could be collected on issues related to the e-signature Directive and issues related to eID.

Only the events that occurred after the publication of Action Plan on e-signature and e-identification COM(2008)798, 28.11.2008 are reported. Indeed the implantation of the action plan indicated that eIAS issues cannot be fully resolved within the existing legal framework of the e-signature Directive.

A number of bilateral meetings with stakeholders including Member States are not indicated.

Circumstance	Parties	Date	Place
Commission workshop with MS on eSignatures	All+MS	25.1.12	Brussels
Tallinn-Going Local 2011	MS	25.11.11	Tallinn, EE
CEN and ETSI Workshop on mandate m460 on e-signature standardisation	All	21.11.11	Paris, FR
Ministerial eGovernment Conference - Rountable on eID	MS	17-18.11.11	Poznan, PL
Digital Agenda taskforce of BUSINESSEUROPE	Industry	17.11.11	Brussels
Polish Presidency and Commission workshop with MS on eSignatures	All+MS	9-10.11.11	Warsaw, PL
Polish Presidency's conference on eSignatures	MS	9.11.11	Warsaw, PL
FESA meeting	MS	8.11.11	Warsaw, PL
eID & ePassport Conference	All	24-25.10.11	Istanbul, TR
Prague-Going Local 2011	MS	6.10.11	Prague, CZ
"IAS study" workshop	All+MS	3.10.11	Brussels
Small Business Act follow-up meeting with stakeholders	SMEs	28.9.11	Brussels
European Multi-Stakeholder Forum on E-invoicing	All+MS	13.9.11	Brussels

Circumstance	Parties	Date	Place
SPOCS – ETSI meeting	ESO	8.9.11	Den Haag, NL
Digital Agenda Assembly workshop on "What next for e-Identity and e-Signatures?"	All+MS	16.6.11	Brussels
European Parliament, IMCO, presentation of its report on e-signature entitled "Digital Internal Market"	EP	15.6.11	Brussels
eGovernment High Level Group inaugural meeting	MS	7.6.11	Brussels
11th eSignature Conference (EFPE)	All	6.6.11	Międzyzdroje, PL
Meeting of the Banking Technology Committee of the World Savings Banks Institute / European Savings Banks Group	Industry	19.5.2011	Brussels
General assembly of European Land Registry Association	Stakeh.	17.5.11	Brussels
FESA meeting	MS	5-6.4.11	Stockholm, SE
Stakeholder workshop on electronic identification, authentication and signature	All+MS	10.3.11	Brussels
General assembly of ChamberSign	Industry	10.2.11	Brussels
6th ETSI Security Workshop	All	19-20.1.11	Sophia Antipolis, FR
BE Presidency conference: "Lift-off towards Open Government 2010"	All+MS	15-16.12.10	Brussels
AFNOR conference: Sécurite des systèmes d'information: la normalisation, un atout?	All	26.11.10	Paris, FR
eID & ePassport Conference	All	19-20.10.10	Athens, GR
FESA meeting	MS	18.10.10	Mainz, DE
Expert meeting on identity theft and identity management	MS	4.10.10	Brussels
9th eSignature Conference (EFPE)	All	4.7.10	Międzyzdroje, PL
General assembly of Eurosmart	Industry	30.4.10	Brussels
FESA meeting	MS	13.4.10	Warsaw, PL
5th ETSI Security Workshop	All	20-21.1.10	Sophia Antipolis, FR
Commission workshop with MS on eSignatures	All+MS	25.1.12	Brussels
Tallinn-Going Local 2011	MS	25.11.11	Tallinn, EE
CEN and ETSI Workshop on mandate m460 on e-signature standardisation	All	21.11.11	Paris, FR
Ministerial eGovernment Conference - Rountable on eID	MS	17-18.11.11	Poznan, PL
Digital Agenda taskforce of BUSINESSEUROPE	Industry	17.11.11	Brussels
Polish Presidency and Commission workshop with MS on eSignatures	All+MS	9-10.11.11	Warsaw, PL
Polish Presidency's conference on eSignatures	MS	9.11.11	Warsaw, PL
FESA meeting	MS	8.11.11	Warsaw, PL
eID & ePassport Conference	All	24-25.10.11	Istanbul, TR
Meeting of the Banking Technology Committee of the World Savings Banks Institute / European Savings Banks Group	Industry	13.1.2010	Brussels
SE Presidency: 5th Ministerial eGovernment Conference	All+MS	19-20.11.09	Malmö, SE
National eID conference	All	22.10.09	Lisbon, PT
RSA Conference	All	21.10.09	London, UK
FESA meeting	MS	7.10.09	Reykjavik, IS
18th meeting of the working group on electronic public procurement	MS	22.9.09	Brussels
FESA meeting	MS	28.4.09	Belgrade, SRB
CZ Presidency high-level conference on eID and public registers	All+MS	7.4.09	Hradec Králové, CZ
Open e-ID Solutions 2009	All	4.2.09	Oslo, NO
Meeting of the working group on electronic public procurement	MS	12.12.08	Brussels
Services Directive comitology: numerous expert meetings to prepare CD 2009/767/EC and 2011/130/EU	MS	2008-2011	Brussels

Circumstance	Parties	Date	Place
IDABC eID interoperability expert group (numerous meetings)	MS	2008-2009	Brussels
IDABC eSignature interoperability expert group (several meetings)	MS	2008-2009	Brussels
ISA working group on trusted information exchange (several meetings)	MS	2010-2011	Brussels
STORK several meetings with consortium partners	All	2008-2011	Brussels

Key: All = All kinds of stakeholders

ANNEX 3: POLICY CONTEXT OF ELECTRONIC SIGNATURE AND ELECTRONIC IDENTIFICATION

The policy context of e-signatures

The Directive[92] on a Community framework for electronic signatures was adopted to establish a legal framework for e-signatures, to ensure the mutual recognition of signature certificates, to remove barriers to the free circulation of e-signature products.

Since 1999, the Commission has undertaken several actions that have complemented the Directive to implement the **EU E-signature framework:**

- Directive 1999/93/EC, its two decisions 2000/709/EC and 2003/511/EC, and also the decisions which formally relates to the Services Directive but *de facto* complement the e-signature framework, namely 2009/767/EC as amended by 2010/425/EU and 2011/130/EU.

- The standards referred to by the legal framework and the CEN and ETSI e-signature standards in general,

- Implementations under the European Commission responsibility such as the EU "trusted list" , Research and innovation, and deployment addressed via the funding of projects by the EU R&D Framework Programme and the Competitiveness & Innovation Framework Programme.

In 2006[93], the Commission reported on the operation of the Directive and acknowledged problems with the mutual recognition and cross-border interoperability of e-signatures. Divergent solutions adopted in the Member States have created *de facto* barriers to the EU-wide interoperability of e-signatures.

As a follow-up, the Commission adopted in 2008 an Action Plan on e-signature and e-identification[94] to remove interoperability obstacles. Some improvements could be achieved as a consequence of the Action Plan (e.g., the so-called "Trusted List" of providers of qualified signature certificates but adopted in the formal context of the Services Directive 2006/123/EC). However, no more barriers can be removed with the current regulatory framework of Directive 1999/93/EC because the Direciteve does not permit to adopt implementing measures needed to remove barriers or to address information society evolutions.

More recently, the implementation of the Services Directive has provided a new impetus for extending the European legal framework surrounding the e-signature directive, including through a 2009 Commission Decision[95] that required each Member State to establish, maintain and publish a "Trusted List" containing information related to the certification services providers (CSPs) issuing qualified certificates who are supervised/accredited by Member States, and the 2011 Decision establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities[96].

[92]Directive 1999/93/EC on a Community framework for electronic signatures
[93] Report on the operation of e-Signatures Directive COM(2006)120 final
[94] COM(2008)798 of 28.11.2008
[95] COM(2009)767 of 16.10.2009
[96] C(2011)1081 of 25.02.2011

With relation to standards, European standardization organisations CEN, CENELEC and ETSI were granted with a standardization mandate in December 2009[97] with the objective to update the existing European eSignature standardisation deliverables in order to create a rationalised framework. The rationalised framework for electronic signature standardization has been proposed providing a coherent basis for selection of standard appropriate to business needs. An inventory of existing standardisation at the International, European and national/sector level is also available.[98]

The policy context of eID

The action plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market identified "Electronic Identity Management" as a key element for the delivery of any e-services ensuring that no unauthorised use is made of the identity of persons and personal data and the validity of identity claims. One of the actions envisaged by the Commission was to determine after the delivery of the results of the Large Scale Pilot on eID (STORK) scheduled for end of 2011 if and what additional actions might be required to enable an effective EU wide usage of e-ID. The legislative proposal on cross-border mutual recognition and acceptance of electronic identification and authentication is one of these actions.

The crucial importance of secure, trustworthy and easy to use seamless online services for a strong and well-functioning European Digital Single Market is stressed in the Digital Agenda for Europe. Following these goals, the Commission announced to take action to ensure mutual recognition of e-identification and e-authentication with the aim to eliminate fragmented digital markets, lack of interoperability and to prevent the increase of cybercrime.

The need to strengthen confidence in electronic transactions as necessary condition for the development of a Digital Single Market from which citizens, businesses and public authorities can fully benefit is reiterated in the Single Market Act (SMA) where one of its 12 key actions envisages legislation ensuring the mutual recognition of electronic identification and authentication across the EU.

In its European eGovernment Action Plan 2011-2015[99], the Commission proposes in one of its actions a legislative measure on mutual recognition of electronic identification and authentication across the EU with the objective to enhance eGovernment services in Europe in general and to create the pre-conditions for the EU-wide use of national electronic identity solutions in particular. Concretely, the action will support the Member States to "apply and roll out the eID solutions, based on the results of STORK and other eID-related projects" as foreseen in the action plan for the period 2012-2014. In addition, they will contribute to create the necessary conditions for the setting up of digital service infrastructures for which the Commission proposes an amount of € 2 billion in the context of the Connecting Europe Facility[100] as well as the Guidelines for trans-European telecommunication networks[101], both of which embedded in the overall proposal for a Multiannual Financial Framework 2014-2020.

---

[97] http://ec.europa.eu/information_society/policy/esignature/docs/standardisation/mandate/m460_en.pdf
[98] http://www.e-signatures-standards.eu/reference-documentation/rationalised-framework-on-electronic-signature/rationalised-framework-for-electronic-signature-final-version-02-2012
[99] COM(2010)743 of 15.12.2011
[100] COM(2011)669 of 19.10.2011
[101] COM(2011)657 of 19.10.2011

The Council recognises explicitly in its Conclusions on the European eGovernment Action plan 2011-2015 the proposal of the Commission of a legislation "to ensure mutual recognition of e-identification and e-authentication across the EU" [102]. Member States also committed themselves to "deploy and roll-out cross-border eGovernment services based on and building on results delivered by the large scale pilots" one of which succeeded to solving the cross-border interoperability problems of "official eIDs" .

Finally, the vital role of a future common legal basis for mutual recognition and acceptance of electronic identification and authentication across borders for the virtual cycle of the digital economy was underlined in the Roadmap for Stability and Growth by getting assigned fast track priority for 2012. Electronic identification (eID) and authentication of entities (natural and legal persons) are pre-requisites for electronic interaction and online transactions: Identification enables to establish whether the person is indeed the one he/she claims to be; through authentication the claimed identity can be verified.

The European Council confirmed in its conclusions of October 2011 that "particular attention should be paid to facilitating secure electronic identification and authentication" in order to promote a fully integrated Digital Single Market by 2015.

[102] Council Conclusions on the European eGovernment Action Plan 2011-2015, 3093rd Transport, Telecommunicaions and Energy Council, 27 May 2011

ANNEX 4 – PUBLIC CONSULTATION ON ELECTRONIC IDENTIFICATION, AUTHENTICATION AND SIGNATURES IN THE EUROPEAN DIGITAL SINGLE MARKET

Introduction on the goals and scope of the consultation

On 18 February 2011, the European Commission launched a public consultation in the context of the Digital Agenda for Europe, regarding electronic identification, authentication and signatures. The purpose of this consultation was to seek stakeholder input for policymakers on how electronic identification, authentication and signatures can contribute to deliver the European digital single market.

The consultation closed on 15 April 2011, and generated **434** contributions[103] from **37** countries and from a wide range of actors, including Member States, EU and national organisations, regional and local authorities, business and professional federations, individual companies, and NGOs. Roughly half of the submissions originated from these organisations, with the other half of the respondents being from individual citizens.

This document summarises the main findings of the consultation. More details, including the complete set of contributions, can be found on the consultation's website[104].

Main findings on electronic identification, authentication and signatures usages

The overall usage of electronic identification, authentication and signatures tools by the respondents is reported to be relatively high (around 80 %), with responses showing no significant difference between organisations and individuals. electronic identification, authentication and signatures tools are mainly used for securing transactions and guaranteeing the integrity of electronic documents. Over 80% of respondents consider eGovernment and eBanking as the major application areas, emphasizing the importance of ensuring integrity and security in these domains.

e-signatures tailored to face the challenges of the digital single market

When examining how the respondents perceived the impact and role of e-signatures on the Digital Single Market, almost 80% of respondents estimated that take-up was low, characterising it as marginal or moderate. The most frequently indicated causes for this relatively low success rate were (1) the limited number of services requiring e-signatures; (2) insufficient user friendliness; (3) cross-border interoperability issues.

As the main interoperability challenges to be fixed by future initiatives, respondents refer to the heterogeneous approach to security requirements in different Member States, unclear terminology (both in the e-signatures Directive and in national implementations), and insufficient harmonisation of profiles of qualified certificates. These criticisms relate to areas in which the Directive has seemingly left a margin of appreciation or where its language is too ambiguous, resulting in diverging implementations that have caused market disruptions.

Generally, respondents suggested that future regulations could improve interoperability by eliminating ambiguities and reducing national divergences. In particular, **87%** of respondents replied that EU legislation should also address **related trust services** like certified e-documents, time stamping, mandates, e-seals, certified document delivery or archiving,

[103] Most contributions were made via the Commission's online consultation tool (IPM — Interactive Policy Making), and several others were sent in as separate submissions.

[104] Contributions can be accessed online at:
http://ec.europa.eu/information_society/policy/e-signature/eu_legislation/revision/pub_cons/index_en.htm

whereas only **5%** entirely opposed new regulatory initiatives. Finally, **61%** favoured the introduction of **eConsent** as a building block in EU e-signature legislation.

From a technical point of view, when analysing the options for addressing e-signature challenges, opinions are less clear. **32%** of respondents are in favour of a creating a central EU signature validation service, **21%** are in favour of a national governmental signature validation service, and **17%** would prefer to have this services managed by the private sector. Similarly, **50%** of respondents believe that a common European e-signature **security classification scheme** would be useful, while **22%** replied that the complexity would outweigh any advantages and **11%** are against.

Other topics found more universal support, such as supporting **mobile devices as IAS tools** (favoured by **82%** of the respondents), and maintaining or keeping the EU's high **"qualified" signatures** security, as expressed by **66%** of respondents (as opposed to the **16%** who would prefer relaxed requirements).

Principles for future e-identification and authentication legislation and policy

The consultation gauged opinion on the perceived need for legislative measures to address e-identification and e-authentication in particular, including the fundamental principles of such legislation, expected effects on the Digital Single Market, potential benefits for users, cross-sector interoperability and any lessons learned.

A large majority of **65%** of respondents favoured EU legislation for electronic identification, whereas only **23%** was against. Key areas to be covered by such legislation according to the respondents are notably data protection and privacy (78%), transparency (65%), and liability of the eID provider (59%). Affordability and cross-sector usability were considered important by 39%. Identity federation saw significantly more support (44%) than a centralised approach (23%). Respondents thus clearly favoured an open, trustworthy and interoperable eID environment.

Looking at the expected impact of legislative measures addressing mutual recognition and acceptance of eID across borders on the Digital Single Market, the main expected effects were an improvement of legal certainty (62,2%), a reduction of administrative burdens (60,8%), and the increase of cross-border mobility (59,1%). Economically, respondents expect that increased economies of scale (49%) will have a strong positive impact as eIDs would become useful of an increased number of applications.

Finally, respondents frequently stressed the importance of international standardization, if possible supported through international agreements to use the same standards in international transactions. IAS services are seen as an inherently international phenomenon, and European initiatives should be attuned to this reality.

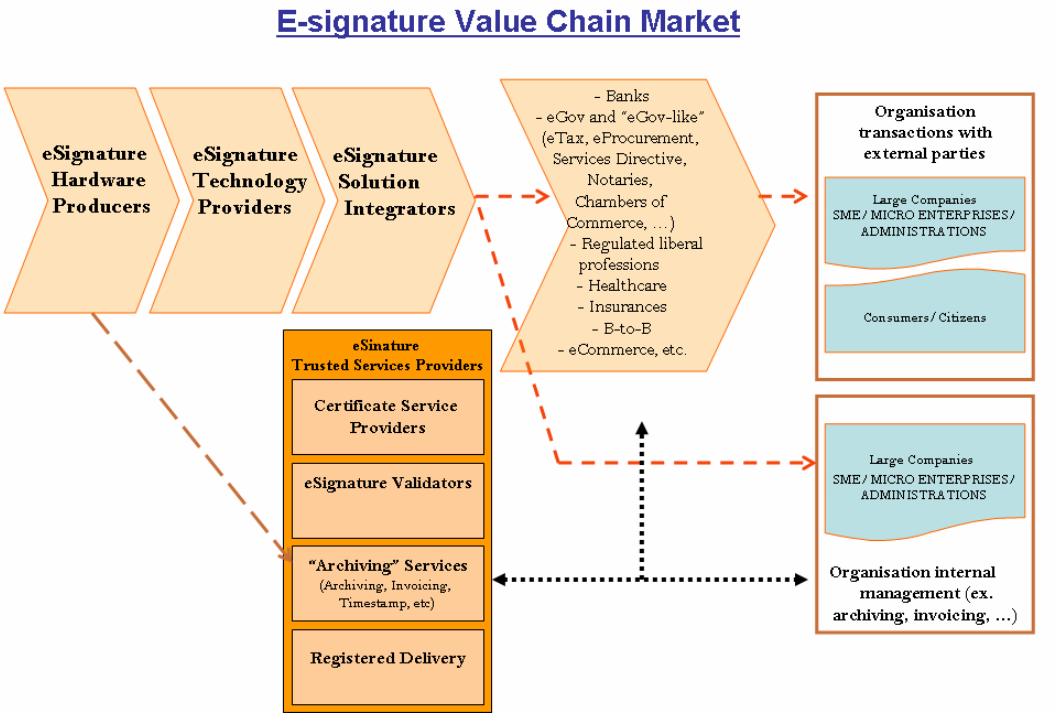
ANNEX 5 – THE SME TEST

(1) Consultation with SMEs representatives	Consultation with SMEs took place throughout the following process: • Public consultation which ended on 15.04.2011 – this gave the opportunity to SMEs to respond. • The initiative was discussed during the SBA Follow-up meeting with stakeholders (SMEs European Associations) on 28.09.2011. The discussion focused on the current EU e-Signature framework and the future steps and initiatives to improve the legislative framework. • The SME Panel was available on the Internet and ran from 04.10.2011 to 22.12.2011. 1251 answers from SMEs across Member States were received. • SMEs were also consulted through regular bilateral meetings with specific companies. **Feedback from SMEs:** SMEs associations gave a positive feedback. They consider the e-Signature could offer many valuable advantages for enterprises with regards to efficiency, costs and time reduction in their commercial relations. The revision of the e-signature Directive is one of their priorities and they believe that this improvement could bring growth and create jobs for SMEs.
(2) Preliminary assessment of businesses likely to be affected	See Annex 7
(3) Measurement of the impact on SMEs	There is no specific analysis of the distribution of the potential costs and benefits of the policy options over the businesses' size. Indeed, most of the proposals under the selected option would imply benefits for businesses but not affect them directly (except electronic seals for which impacts identified for SMEs were compared with those of large enterprises).
(4) Assess alternative options and mitigating measures	At the end of the impact assessment, the selected option shows that the initiative might result in a reduction of the administrative burden and have a very positive economic impact on the stakeholders in general, including SMEs. Consequently, there is no element showing the need for SME specific measures in order to ensure compliance with the proportionality principle.

ANNEX 6 – E-SIGNATURE MARKET SEGMENTATION AND TRENDS

Through a **value chain analysis** of the e-signature market we can identify a full range of actors involved in the sector from hardware providers, technology providers, solutions integrators, etc, to the end-user or final consumer, citizens, SMEs, Large Companies, and Administrations.

Figure 1



E-signature market failures

The absence of "massive usage" of electronic signatures by citizens, consumers or companies in Europe as well as the low take up of its market since the adoption of Directive 99/93/EC 12 years ago does not imply one single explanation.

According to EUROSTAT data[105], an increasing usage of e-signature by EU enterprises is a considerable augmentation of the demand of digital signature products and services. The use of e-Signature by enterprises results increasing by around 5% per year between 2007 and 2010, depending on the market and the EU country, to reach a current average of 29% (in 2010) of enterprises making use of digital signatures for their computerised activities. Nonetheless, it should be noticed that in some countries the use of e-Signature is widespread, like in Spain, where this indicator reaches 14% in microenterprises with 1 to 9 employees, which is a tiny percentage if compared to the levels of SMEs - between 10 and 249 employees (52%), and large companies (over 250 employees) using e-Signature (88%) in 2010.

In order ensure that adequate measures will be taken with regards to needs and expectations of SMEs, the European Commission, through the Enterprise Europe Network, consulted from October to December 2011, European SMEs on the impact of the e-ID and the e-Signature in

[105] EUROSTAT. Survey on ICT usage and e-commerce in enterprises

their business. According to the majority of respondents 62,1% of the European SMEs use e-Signature.

However, few individuals seek to obtain signature products or services and this lack of potential customers discourages companies from investing in signature products and applications leading to low commercial usage for electronic signature.

Social grounds explain the low take-up of e-signature products and services. Firstly, e-signature is not perceived as a "easy to use product" and private users do not believe that using e-signature would enhance his or her job performance or life. Secondly, a lack of communication on and knowledge of e-signature industry, products, benefits, etc. is hindering its usage by a major part of the society.

Electronic signature market adjustments

Despite a satisfying average use of e-signature in Europe by companies, the e-signature market needs to be adjusted.

Firstly, costs to quit e-signature industry are high because of the high level of investment required to enter and participate in the market, meaning that existing firms will fight hard to survive because they cannot easily transfer their resources elsewhere. Many “niche” solutions exist in specific sectors (such as financial services, insurance, telecom) but there are interoperability barriers often “embedded” within the solution.

Secondly, markets are mainly national and the incumbent champions often based on natural monopolies. The barriers to enter these markets are very strong considering for example that the e-signatures Directive imposes more than thirty different requirements on qualified electronic signatures. In addition, several countries put additional detailed requirements on the CSP leading to the creation of barriers for the establishment of foreign CSPs. This situation may lead to unfair competition and, in extension, acts as a trade obstacle within the internal market.

Thirdly, the natural market demand for Qualified Certificates and related services is very low. Within the scope of the Directive, very few applications are in use today , mainly limited to e-government and e-banking which are the largest application area in Europe for electronic signatures.

Low take-up of electronic signature products and services

The public consultation (see annex 4), enquired how respondents judged the take-up of electronic signatures in Europe. **Almost 80% of respondents in total estimated that take-up was marginal or moderate, whereas only 15% described it as high or very high.** Enquiring after the main reasons for this relatively modest take-up rate, respondents primarily noted the limited number of services requiring e-signature, lack of user-friendliness, and interoperability challenges. Costs and lack of legal certainty were smaller negative factors.

When analysing the reasons for such a slow take up of the e-signature, the **first reason** is that signing a document or an email is not handy (lack of user-friendly signature solutions). To install a certificate on the computer is uneasy and most applications used for private purpose badly integrate e-signature functionalities. Free webmail services (such as hotmail, yahoo or gmail) do not allow signing emails.

The Second reason is that service providers have little incentive to develop multi-application electronic signature and prefer to offer solutions for their own services, for instance, solutions developed by the banking sector. This slows down the process of developing interoperable solutions. The lack of applications, such as comprehensive solutions for electronic archives, might also prevent the development of a multi-purpose e-signature, which requires reaching a critical mass of users and usage.

The third reason is an element that explains the lack of interoperability. The Directive does not grant enough legal certainty with respect to the use of electronic signatures and related services. Many businesses in Europe claim that they are willing to use an e-Signature abroad but having difficulties or at least uncertainties about the validity of their e-Signature across border.

Despite of the market imperfections, new usage scenarios like signature creation through mobile devices, remote signatures, mass signing and server signing are the new trends of the esignature market that could make it grow. The increasing convergence of mobile telecommunications and the Internet as well as the growing number of added value services for mobile devices will result in a strong market demand for secured transactions on the Internet. CSPs could target millions of potential customers thanks to the high market penetration of smart mobile phones.

Strengths and weaknesses of the electronic signature market

Electronic Signature Market	
Strengths	**Weaknesses**
1. Technology has not changed in the last decade 2. Demand is a constantly and progressively growing. 3. Large investments on the e-signature sector already done by companies, Public administration, etc. 4. Extended government support in most MS as a means to reduce administrative burden (i.e. e-signature directive 1999/93/EC: Market access and internal market provisions) 5. Massive use in some sectors (home banking, healthcare, etc) 6. Supply side competitive and diversified 7. Many tangible and intangible benefits for users and SMEs (facilitate the business transactions and save time, money etc) 8. E-signature products and services are environmentally friendly (i.e. e-archiving, e-invoicing)	1. The market is fragmented (There are lots of small to medium size companies and where even the big players have stiff competition) 2. Strong barriers to entry through economies of scale. 3. The market is "protected" by European legislation and Member States national legislation. Artificial demand 4. Numerous requirements on qualified electronic signatures. Complex product 5. Few user-friendly signature solutions 6. Limited EU cross-border interoperability 7. Insufficient legal certainty of e-Signature implementations 8. Small potential Return on investments for companies by implement e-signature solutions. 9. Little marketing of product and services. Lack of user's awareness. 10. No perceived cost savings for companies especially for SMEs and private users,. 11. Limited number of services requiring e-signatures. 12. E-signature standardisation framework = lacks business orientation

Market failures and legislative failures

Electronic Signature Market failures and legislative failures	
Market Failures	**Legislative Failures**
The market is fragmented (There are a lots of small to mid size companies and where even the big players have stiff	Legal uncertainties due to the large variety of approaches to e-signatures

competition)	
The market is geographical, working in silos	Mutual recognition and cross-border interoperability of e-signatures
Strong barriers to entry through lack of economies of scale.	Mutual recognition and cross-border interoperability of e-signatures. Member States transpose through their own lawmaking processes the provision of a Directive
Strong barriers to entry (several countries put additional detailed and unnecessary requirements on the CSP)	Member States transpose through their own lawmaking processes the provision of a Directive
Few e-signature applications are in use today and they are almost completely limited to e-government.	Standardisation. The technical framework is outdated and does not clearly link to legal requirements.
The market is "protected" by European legislation and Member States national legislation. Artificial demand	Member States transpose through their own lawmaking processes the provision of a Directive
Few private customers seek to obtain signature products or services	Unclear supervision leading to lack of confidence
Lack of e-signature standardisation framework = lacking business orientation	Standardisation. The technical framework is outdated and does not clearly link to legal requirements.

Status of electronic signature in EU (2010)

Country	Providers of qualified signature certificates[106]	Status of providers (public/private)[107]	Number of issued qualified certificates[108]	SSCD certification[109], [110]	Validation services[111]
Austria	1	1 private company	120.000	DB	MOA – SP (public)
Belgium	1	1 private-public company	10.000.000	SD	No
Bulgaria	5	5 private companies[112]	Unknown	DB[113]	No
Cyprus	0	-	0	No specific rules	No

106 Source: AT, BE, CZ, DE, HU, IT, PL, SK, SE, IC, NO: Forum of European Supervisory Authorities for Electronic Signatures (FESA); rest: CROBIES: Cross-Border Interoperability of e-signatures, Work Package 2 "Trusted Lists", Annex 1 – Observations on the current Trusted Lists in Member States [data as of July 2009] AND also Trusted Lists of Certification Service Providers, http://ec.europa.eu/information_society/policy/e-signature/eu_legislation/trusted_lists.

107 Names of the services providers found on different websites of supervision authorities and in IDABC Study on Mutual Recognition of e-signatures: update of Country Profiles: Analysis & assessment report (in particular country profiles – data as of summer 2009) http://ec.europa.eu/idabc/en/document/6485. For the purpose of this table, Chambers of Commerce and Professional Associations are assimilated to public companies.

108 Source: Forum of European Supervisory Authorities for Electronic Signatures (FESA) – spring 2010.

109 **Key**: **SSCD**, Secure Signature Creation Device; **DB** = Determination of conformity by a Designated Body (art. 3.4 of Directive 1999/93/EC); **SD**: self-declaration; **VAS**: voluntary certification scheme.

110 Source CROBIES, Work Package 4, Framework for Interoperable Secure Signature Creation Devices AND also IDABC study – same as footnote http://ec.europa.eu/idabc/en/document/6485 unless stated otherwise - see footnotes 106 and 107.

111 Source: IDABC Study on Mutual Recognition of e-signatures: update of Country Profiles; page 7 http://ec.europa.eu/idabc/servlets/Doc?id=32436 [data from 2009] except Estonia.

112 Source: Communications Regulation Commission; http://www.crc.bg/files/_en/registar-es-en.pdf

113 In accordance to art. 36 of the Law for the Electronic Document and Electronic Signature

Country	Providers of qualified signature certificates[106]	Status of providers (public/private)[107]	Number of issued qualified certificates[108]	SSCD certification[109], [110]	Validation services[111]
Czech Republic	3	2 private and 1 public company[114]	193.000	Only formal verification[115]	No
Denmark	0	-	0	SD	No
Estonia	1	1 private company	1.000.000	DB	DigiDoc[116]
Finland	1	1 State entity	275.200[117]	DB[118] "authorisation"	No
France	2	2 public companies	Unknown	DB[119]	No
Germany	12	2 private, 10 public companies	320.000	DB	VPS (public)
Greece	3	1 private, 2 public companies	Unknown	SD or VAS[120]	No
Hungary	5	3 private, 1 public company, 1 State entity	11.866	DB[121]	No
Ireland	3	2 private, 1 public company	Unknown	SD or VAS[122]	No
Italy	16	11 private, 3 public companies, 2 State entities	3.200.000	Accredited CSP: DB; Supervised CSP: SD[123]	No
Latvia	1	1 public company	25.000[124]	SD or VAS[125]	No
Lithuania	3	1 public, 1 private company, 1 State entity	Unknown	SD or VAS	No
Luxembourg	1	1 public-private company	Unknown	SD and obligatory notification[126]	No
Malta	0	-	0	SD or VAS[127]	No
Netherlands	5	4 private companies, 1 State entity	20.000	Registration compulsory	No
Poland	5	4 private, 1 public company	256.000	DB[128]	e-Notarius (private)
Portugal	5	5 State entities	Unknown	Registration compulsory [129]	No
Romania	3	3 private companies	Unknown	SD and obligatory notification [130]	No
Slovakia	5	5 private companies	90.000	VAS or DB[131]	No

114 http://www.mvcr.cz/mvcren/article/scope-of-activities-egovernment-electronic-signature.aspx?q=Y2hudW09Mw%3d%3d

115 According to the Section 6 of the Act on Electronic Signature; http://www.mvcr.cz/mvcren/article/scope-of-activities-egovernment-electronic-signature.aspx?q=Y2hudW09Mg%3d%3d

116 https://digidoccheck.sk.ee

117 www.vaestorekisterikeskus.fi/vrk/fineid/files.nsf/files/5F7890ACBE4B162AC2257700001C8E56/$file/Country_Update_from_Finland.pdf

118 http://www.ficora.fi/en/index/saadokset/maaraykset/laatuvarmennetoiminta.html

119 Décret relatif à la signature électronique, art. 7; www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=vig

120 www.eett.gr/opencms/opencms/EETT_EN/Electronic_Communications/DigitalSignatures/InfoConformityAssess.html

121 http://users.skynet.be/fa283208/pdf/INFSO-CROBIES-DFC-WP4-SEALED-29032010_v1.pdf

122 Electronic Commerce Act, section 29 http://www.ispai.ie/legal/ie/1999-ecomm-act.pdf

123 http://www.cnipa.gov.it/site/it-IT/Attivit%c3%a0/Firma_digitale/

124 http://ec.europa.eu/idabc/servlets/Doc?id=32284

125 Electronic Documents Act http://www.dvi.gov.lv/eng/legislation/edl/

126 Loi sur commerce électronique, art. 29 http://www.ilnas.public.lu/fr/legislation/confiance-numerique/loi-cadre-relative-commerce-electronique/loi-14aout2000.pdf

127 http://www.mca.org.mt/infocentre/openarticle.asp?id=185&pref=22

128 http://www.mg.gov.pl/English/ECONOMY/Internal+Trade+Regulation/ Law on electronic signature, art. 10 http://isap.sejm.gov.pl/DetailsServlet?id=WDU20011301450

129 http://www.gns.gov.pt/gns/pt/ce/

130 Law on electronic signature, art. 13 http://www.anrcti.ro/Portals/57ad7180-c5e7-49f5-b282-c6475cdb7ee7/LEGE_455_2001.pdf

131 Law on electronic signature, article 13 http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/legislativa/1-3/215_2006en.pdf

Country	Providers of qualified signature certificates[106]	Status of providers (public/private)[107]	Number of issued qualified certificates[108]	SSCD certification[109], [110]	Validation services[111]
Slovenia	5	4 private companies, 1 State entity	Unknown	SD or VAS; registration required to use e-signature within public administration[132]	No
Spain	12	5 private, 2 public companies, 5 State entities	Unknown	SD[133]	@firma (public)
Sweden	1	1 private company	50	SD[134]	No
UK	1	I private company	1	DB[135]	No

The table above shows estimates of certificates volumes in the different countries. The following observations can be made:

- A large number of Qualified Certificates have been issued by accredited CSPs in Italy. The main application area for these certificates is for access to company registration information (InfoCamere).
- In Belgium and Estonia the large volume is a result of large-scale deployment of electronic ID cards.
- In Germany quite a large number of Qualified Certificates have been issued and are regularly used in various e-government applications.
- In Slovenia a substantial number of Qualified Certificates have been issued mainly for corporate e-banking purposes and for e-government.
- The differences in certificates from accredited versus supervised CSPs are mainly a reflection of the different governments promoting/mandating accredited CSPs.

132 Law on e-signatures, art. 18 and next; http://www.uradni-list.si/1/objava.jsp?urlid=200498&stevilka=4284

133 http://www.mityc.es/dgdsi/es-ES/Servicios/FirmaElectronica/Paginas/Prestadores.aspx

134 http://www.pts.se/en-gb/Industry/Internet/Electronic-signatures/

135 http://www.tscheme.org/directory/index.html

ANNEX 7 – TABLE REPRESENTING THE DIFFICULTIES ENCOUNTERED BY EACH OF THE STAKEHOLDERS AND THE INTEREST IN THE REVISION OF THE FRAMEWORK

SUPPLY SIDE	
eService/device producers	***How are they affected by the unavailability of an appropriate cross-sector framework for secure, trustworthy and easy-to-use electronic transactions in the Single Market?***

	- Different regulatory approaches in different Member States result in a f**ragmented market** for eService/device producers in the EU. Different legislations create, for producers, a **barrier to enter** other European markets and hamper the deployment of cross-border services
	- Some exceptions set apart (banking applications and tax declaration eServices), the volumes of demand for IAS is quite limited generating important limitations on
	  o Service economies of scale
	  o Investment recovery (technology and organisation)
	  o New entrants to the market (barriers to entry)
	- There are significant barriers to exit and investments are service-specific
	- IAS

	What are their specific interests regarding the revision of the current EU legislation about e-signature?
	- A harmonised legislation for all EU Member States imposing similar standards (legal and technical) which would allow them to develop electronic services and devices usable in all EU countries and by all sectors. As such, they would have access to one **European market** for their services and products instead of national markets. - An **improved alignment between legislation and standards**, to support the development of new or more advanced IAS technologies required by the market, such as mobile signatures (through mobile devices) and server signing through HSMs. - A legislation that goes **beyond e-signatures**, to allow them to develop and promote e.g. also eID tools as part of a rationalised device offering.

DEMAND SIDE	
ESERVICE PROVIDERS	
PUBLIC SECTOR	
Governments and administrations	***How are they affected by the unavailability of an appropriate cross-sector framework for secure, trustworthy and easy-to-use electronic transactions in the Single Market?***
	- The definite trend to sophistication of online services is a crucial ingredient to **modernisation, cost effectiveness and re-organisation of public administrations** with the objective to deliver faster high quality with less resource consumption (i.e. **reduction of administrative burdens**), the logic consequence is migration to electronic services and transactions which do not stop at national borders especially[136]. These cross-border transactions are currently hampered by a lack of an appropriate EU framework.

[136] A good indicator for the importance of cross-border cooperation between public authorities in the EU is the fact that 5,737 national competent authorities were registered in the IMI (Internal Market Information) system at

	- By way of an example: not all European contracting authorities have adopted **eProcurement** and the existing systems are very difficult to access by contractors located in other Member States [137]; these authorities are currently missing the opportunity to receive better and cheaper offers for their procurement from contractors across Europe. This could be remedied by an appropriate framework for IAS services at the EU level. Similar challenges present themselves for other public services, e.g. in the implementation of the **Services Directive** (requiring the establishment of electronic points of single contact, i.e. service portals that can be used by service providers throughout the EU), or in the development of cross-border **eJustice** and **eHealth** systems, which require highly reliable identification and authentication of the relevant professionals.
	What are their specific interests regarding the revision of the current EU legislation about e-signature?
	- A EU framework including **mutual recognition and the acceptance** of "(official) eIDs" as a common way to access public online services in another Member State, and an improved (more effective) recognition and acceptance of e-signatures. This is expected to lead to an increase in the use of these services by citizens and companies allowing for a reduction of administrative burdens, an improvement of the quality of services provided by the administration, a more efficient usage of the budget dedicated to public procurement, etc. - A general EU framework for IAS that is sufficiently comprehensive to **support the different e-Government solutions** that have been developed in the past years as large scale pilots (e.g. STORK, PEPPOL, SPOCS, eCodex, and epSOS) and should be channelled into long term sustainable digital service infrastructures as proposed by the Connecting Europe Facility[138]. Member States (and the Commission) have invested millions in these projects, which cannot be brought to a fully operational stage without a common legal/policy framework that would support some of the outputs of these projects (such as the STORK Quality Authentication Assurance framework, which allows the classification of official eIDs issued in the Member States on the basis of their reliability assurances).
PRIVATE SECTOR	
With existing specific systems for electronic transactions ***(e.g. banking sector, e-Commerce, liberal professions, etc.)***	***How are they affected by the unavailability of an appropriate cross-sector framework for secure, trustworthy and easy-to-use electronic transactions in the Single Market?***
	- The fact that (official) eIDs cannot be currently used by the private sector for electronic interactions makes them more **complex and not very user-friendly**. Indeed, customers need **multiple devices** and/or remind **several different usernames and passwords** for each interaction with each individual company. - The lack of trust from consumers due to the unavailability of an appropriate framework ensuring secure, trustworthy and easy-to-use electronic transactions can **hinder the take-up of electronic transactions** across the EU (e.g. in sector of e-Commerce). This slows down the boost that could be given to the economic activity / recovery in the EU; - The **insufficient legal certainty** surrounding both electronic interactions and the existing tools for online transactions does not allow companies to easily verify the reliability of information received from a customer (e.g. that the person is actually who he/she claims to be, that he/she actually has the age he/she pretend, the

the end of 2010 (cf. Single Market Act, Annex 2). IMI is a secure online application that allows national, regional and local authorities to communicate quickly and easily with their counterparts abroad. IMI is accessible via the internet without the need to install any additional software, http://ec.europa.eu/internal_market/imi-net).

[137] Currently, less than 5% of total procurement budgets are awarded electronically, and only 1.6% of contracts are supplied by an entity in another Member State. It is estimated that if eProcurement is adopted by all European contracting authorities, annual savings could exceed €50B.

[138] Short explanation of CEF

	validity of official documents, etc.) - The **lack of a general approach to trust services** (IAS services and related trust services in general) limits the market for European providers of such services, as the legal value of their services is questionable and may vary from Member State to Member State. If they wish to offer their services in other Member States, they will have to first identify which requirements (if any) exist for their services, and conduct compliance audits. The lack of a common European framework causes a large cost of market entry, which in turn discourages investments into new and innovative trust services.
	What are their specific interests regarding the revision of the current EU legislation about e-signature?
	- A framework for electronic transactions ensuring more **legal certainty** and leading to an **increase in trust and ease of use** for users. This new framework is expected to increase the number of e-Services users leading to different benefits for the private sector (e.g. **reduction of administrative burden, improvement of quality of services provided, innovative services, additional cross-border economic activity, increased growth** for e-Commerce, etc.) - A **more streamlined and harmonised approach for trust services in general,** which lowers their operating costs by limiting or eliminating national regulatory divergences, and thus opening up a European Digital Single Market.
private sectors without specific systems for electronic transactions	***How are they affected by the unavailability of an appropriate cross-sector framework for secure, trustworthy and easy-to-use electronic transactions in the Single Market?***
	- The fact that (official) eIDs can currently not be used for electronic interactions between private sector service providers and their customers makes their **customers less interested** in eServices since they need to have several devices and/or remind several different usernames and passwords; - The lack of true interoperability between European service providers means that there is **limited competition in IAS markets, which raises the cost for end users**. - **Closed "niche" solutions** have been developed for specific industries such as e-banking, e-payment or e-health, but there is a barrier to using such solutions in other eServices (it is not interoperable) as they are often "embedded" within the solution. Development of new products and services for specific sectors separately is costly and not efficient; - The **insufficient legal certainty** surrounding both electronic interactions and the existing tools provided to interact online does not allow the exchange of electronic documents between two companies located in different Member States with the same guarantees that exist in the physical world (e.g. contracts, registered mail, etc.);
	What are their specific interests regarding the revision of the current EU legislation about e-signature?
	- A framework for electronic transactions leading to **increased legal certainty** allowing them to engage in electronic transactions (e.g. communicating signed contracts) with the same ease of use and legal value as physical documents; - A framework leading to **full interoperability of e-products and services across sector and Member States** allowing them to use applications already developed for other sectors for their own business. This would allow e.g. the re-use of eID cards or private sector issued eIDs (bank cards, mobile phones, etc) in any other type of application.
END USERS	
Citizens/Consumers	***How are they affected by the unavailability of an appropriate cross-sector framework for secure, trustworthy and easy-to-use electronic transactions in the Single Market?***
	- The fact that different legislations are applicable across Member States makes citizens **not very confident and trusting** when travelling to another Member

	State or shopping cross-border on the Internet, because their rights, and the way of exercising them, can vary significantly depending on the applicable national legislation; - Citizens **cannot use their "official eIDs" they obtained in their own Member State throughout the EU** in order to benefit fully from the Digital Single Market when they want to move, travel, study, work or do business abroad. They are currently not able to access cross-border online services of other Member States when they need to identify themselves electronically due to the fact that almost no Member States foresee or support the use of other Member States' official eIDs; - It is currently **not possible to use "official eID" for cross-border electronic interactions with the private sector.** This results in citizens receiving multiple devices, usernames and passwords, which reduces the appeal of these eServices and encourages bad security practices as end users are likely to re-use the same passwords;
	What are their specific interests regarding the revision of the current EU legislation about e-signature?
	- A legislation **solving the problem of the lack of interoperability of their "eID" between Member States** (e.g. allowing them to fulfil administrative formalities from abroad); - A legislation guaranteeing **secure and trustworthy cross-border electronic transactions** and allowing them to benefit fully and uniformly from their rights across the EU; - A legislation leading to **user-friendly, easy-to-use and uniform e-products and Services** for end users.
Business (including SMEs)	***How are they affected by the unavailability of an appropriate cross-sector framework for secure, trustworthy and easy-to-use electronic transactions in the Single Market?***
	- Businesses **cannot use any eIDs given by their own Member State** throughout the EU in order to benefit fully from the Digital Single Market when they want to move or do business abroad[139]. They are currently not able to access cross-border online services of other Member States when they need to identify themselves electronically due to the fact that almost no Member States foresee or support the use of other Member States eID for businesses; - The lack of a common framework for all IAS services (including eID) results in **limited accessibility of crucial e-Services**. By way of example, **e-Procurement** is not adopted by all European contracting authorities. This can lead companies to miss business opportunities. Moreover, enterprises willing to participate in procurements in other Member States can be discouraged by the more complicated procedures and higher administrative costs. The fact that electronic procedures may be available to national tenderers but not to foreign ones also **distorts competition**, as this raises the cost of participation for foreign tenderers. - The **lack of a common framework for other trusted services** also impedes the use of more advanced trust services, such as electronic registered mail or e-archiving. Companies therefore miss out on the opportunity of using such services in a legally reliable manner, needlessly increasing their cost of operation.
	What are their specific interests regarding the revision of the current EU legislation about e-signature?

[139] A concrete example is the following: The implementation of the "Services Directive" allowing companies willing to provide their services in another EU Member State to fulfil the required administrative formalities remotely is still not possible due to the fact that they are not able to use their "official eID" in other Member States because of the missing link of mutual recognition and acceptance of "official eIDs" throughout the EU.

	- A legislation **solving the problem of the lack of interoperability of eIDs between Member States** (e.g. improving e-Procurement availability and accessibility across the EU); - A legislation guaranteeing **secure and trustworthy cross-border electronic transactions and** allowing them to benefit fully and uniformly from their rights across the EU; - A legislation leading to **user-friendly, easy-to-use and uniform e-products and Services** for end users.
Governments and administrations	***How are they affected by the unavailability of an appropriate cross-sector framework for secure, trustworthy and easy-to-use electronic transactions in the Single Market?***
	- The lack of a common framework for all IAS services means that governments and administrations as end users **cannot easily support eIDs and e-signature solutions offered by third parties, especially in other Member States**. Migration to electronic services and transactions therefore cannot be completed: foreign citizens and businesses often cannot benefit from electronic public sector services provided to them. This is a barrier to the Digital Single Market. It also creates unnecessary costs, as (less efficient) paper systems are the only solution that can currently be offered to foreign users. - This also implies that it is **difficult for public administrations to fully comply with their legal obligations under various European legislations**. Both the implementation of **e-Procurement** platforms and the **creation of points of single contact under the Services Directive** require that public administrations provide certain electronic services to citizens and businesses, including in other Member States. The development of such services is difficult or impossible, at least while Member States require secure and advanced methods of eID and e-signatures to use such systems.
	What are their specific interests regarding the revision of the current EU legislation about e-signature?
	- As end users of IAS services, their interests are the same as in their role of eService providers: they are interested in an EU framework including **mutual recognition and the acceptance** of "(official) eIDs" as a common way to access public online services in another Member State, and an improved (more effective) recognition and acceptance of e-signatures. Similarly, any solution should allow them to support the different e-Government solutions that have been developed in the past years as large scale pilots (e.g. STORK, PEPPOL, SPOCS, eCodex, and epSOS).

ANNEX 8 – DETAILED ASSESSMENT OF IMPACTS – RELATED TRUST SERVICES – EU SUPERVISION LEVEL

I. Detailed assessment of impacts

The following section presents a comprehensive outline of the main economic, social and environmental impacts that could result from the implementation of option 2, 3 or 4.

1. Economic impacts

Macro-economy

How significant could the economic impact of a European Digital Single Market be? The answer to this question is based on model scenarios using estimates of the productivity impact of increased use of digital technologies and services in Europe.

Scenarios and how they relate to the Digital Single Market

The scenarios can be used to quantify the possible impact of an accelerated diffusion of digital technologies and services in Europe. This acceleration can be formulated as the difference between the "base case" (assuming "business-as-usual" and a continuation of the current trend) and a "best case" (assuming an acceleration of the use of digital technologies and services),

Three scenarios for Pan European Framework for Identification, Authentication and Signature impact of the digital economy

In a study for the European Commission (DG Information Society and Media), entitled "The Impact of Broadband on Growth and Productivity" the consultants MICUS (2009) has developed a model of the macro economic impact of broadband that can be transposed to the Pan European Framework on Identification, Authentication, and Signature.

The study by MICUS (2009) works with two key scenarios:

"Best case": The speed of adoption of online services increases to that of advanced knowledge societies (Belgium, Denmark, Finland, Luxembourg, Netherlands and Sweden). The adoption rate in these countries was on average 4.1 percent during 2004-2006. The advanced knowledge societies are also better at taking advantage of online services. Therefore, the best case scenario has both a higher adoption rate and a greater effect on GDP.

"Base case": The speed of adoption of online services continues at the speed during the period 2004-2006.

The study also operates with a "worst case". This is less relevant for our purpose, but for the sake of completeness, it is assumed that the speed of adoption of online services drops to that of countries with less developed broadband (Bulgaria, Greece, Latvia, Poland, Romania and Slovakia). The adoption rate in these countries was on average 1.8 percent during 2004-2006 with a corresponding lower ability to take advantage of online services. Therefore, the worst case scenario has both a lower adoption rate and a lower effect on GDP[140].

[140] Source Micus (2009)

The model and scenarios are useful for our purpose, because they allow for a quantification of the effects linked to an increased use of online services, improved digital infrastructure, and improved e-skills.
Better regulation of the digital economy and harmonisation of the regulation across European borders can create a framework which stimulates competition and innovation and thereby accelerates the creation of new digital technology and services. This is precisely what is needed to make the difference between "business-as-usual" (i.e. the base case) and the accelerated diffusion of the digital economy (i.e. the best case).
The recent study prepared for the European Commission in the digital economy, see Micus (2009), focuses on two factors, namely "digital infrastructure" and "digital readiness" as the main policy drivers for economic impact. It is the impact of these two factors which are specifically analysed in their study. The Pan European Framework for Identification, Authentication and Signature is focusing on a third factor - "digital content & services" - and stresses the impact of a well-functioning market, providing incentives for innovation in the services layer which requires harmonisation and a large unified market in order to achieve the required scale and scope.
We claim that the "best case" scenario will not stand a chance of materialising without the third factor, which aims at stimulating content provision and innovation in the service layer of the digital economy. The policy instruments required to foster this third factor are regulatory harmonisation, large scale markets and a focus on innovation. These are exactly the ingredients brought about by the Pan European Framework for Identification, Authentication and Signature.
The digital single market stimulates the development and take-up of online services, encourages online trade, has a population with high e-skills, and it encourages investment in digital infrastructure. It is hard to predict to what extent the Pan European Framework for Identification, Authentication and Signature will affect the take-up of online services and how it will influence e-skills. We argue that the impetus provided by the Pan European Framework for Identification, Authentication and Signature will make a significant contribution to the possible acceleration of the use of electronic interactions.

Impact on GDP in Scenarios
The digital economy is a major source of growth and innovation. The analysis of the GDP impact of these scenarios shows that the digital economy can contribute with up to a 12 percent increase in EU27 GDP between 2010 and 2020 (corresponding to an increase in the annual growth rate of +1.09 percent).
1. Best Case: Over a ten year period from 2010 to 2020, the cumulative impact of a best case acceleration of the digital economy on EU27's GDP is in the order of 12 percent higher GDP in 2020, cf. Micus (2009).
2. Base Case: Uptake of digital technologies are already increasing at a rapid speed, so even without any further acceleration the digital economy will continue to add to GDP. A continuation of the current trend, as in a "base case" scenario, will add 8 percent to EU27 GDP over a ten year period, cf. Micus (2009). An 8 percent increase of EU27 GDP is large, and it corresponds roughly to the size of Spain's GDP.
3. Net impact of acceleration (= best case – base case): The net impact of a best case acceleration of the digital economy on EU27's GDP is estimated to be in the order of 4 percent over a ten year period. This is calculated as the difference between the "best case" (+12 percent) and the "base case" (+ 8 percent).

Micro-Economy

Today's economic impact of e-signature

Today, digital service infrastructure can generate large economic impacts. A 2010 KPMG study estimated that the cadastre's online access and digital certifications provision was saving Spanish tax-payers at least €157M a year (against cadastral budget of €118M for the same year). Another cost-benefit-analysis conducted by RSO and Cap Gemini showed the Cadastre's electronic office was saving the tax payer about €7,758M[141].

For businesses, the cost savings that organisations realise by replacing paper-based processes with fully digital ones incorporating e-signatures can be very significant - Forrester estimates up to 75% of the amount previously spent pushing paper around. Firms implementing e-signatures save considerable amounts of money on materials (chiefly paper and copy supplies) and personnel (to generate, send, receive, process, and store all that paper). But cycle time is also a key component: the value of this advantage increases exponentially with the number of signers or the number of stages of a multistep signing process involved in

[141] Pricing of Public Sector Information Study, Deloitte, July 2011

completing the execution of a contract. Moreover, the likelihood of customers signing and returning a document within minutes of receipt is far higher when the process does not involve copying, and returning paper. Financial services firms and insurance companies report average contract cycle times falling from one or two weeks to a matter of days - or hours.

2. Positive externalities

Positive externalities are benefits that do not accrue to only a single economic actor, but spill over to society as a whole – thus making the social returns to capital investment higher than initial outlays[142]. The following main categories of positive externalities of common European action in the area of eIAS would emerge both at regional / MS level:

a. The Innovation Diffusion Externality. New and more innovative services emerge that would benefit a growing number of users, thus ultimately improving the overall quality of life. From the infrastructure side, penetration rates correlate positively with the "e-Readiness", or the capacity of consumers, businesses and governments to reap the full benefits of the Information Society[143].

Single sign on solutions, secure e-delivery and e-safes are not only essential key enablers of electronic interaction but also new and innovative online services. They are already available in EU27, although with a different degree of frequency (75% eIDs and single sign on, 47% secure e-delivery, 38% electronic safes. More than half of the countries having in place e-Safes use also single sign on and e-Delivery. Official eIDs are used by all of them as access key. The table below demonstrates their interdependencies[144].

b. The Economic Efficiency Externality. Transaction costs are reduced; which makes it easier to conduct online business and attract foreign investments to certain locations[145]. Electronic signature is already supporting a wide and increasing number of dedicated business, government and leisure applications and services. Bringing electronic signature to new areas means expanding the market for e-Commerce: more consumers would be able to purchase on-line, including across border, thus enlarging the market base, and to access public services on-line.

142 Deloitte report "background support study to the DAE"

143 A positive correlation is evident with the "2009 e-Readiness Rankings" compiled by The Economist's Intelligence Unit (EIU)

144 9th eGovernment Benchmarking Report, December 2010

145 In October 2008, the IMI, together with the National Irish Bank, published the results of its tenth survey of multinational companies located in Ireland. Compared to three years ago, the strategic importance of broadband availability moved up twelve positions in the ranking from 18th to 6th.

Similar effects can be achieved with the cross border and cross sector use of electronic identification. Emerging sectors such as the e

Gambling industry which expects a growth from €8.3B to €12,5B in 2012[146] could profit from the possibility of minimal data disclosure made possible by the use of official eIDs (e.g. only the age of a person needs to be provided without the need to disclose other person data). Looking to the potential market figures from Germany gives an idea of the potential scale. The brutto amount per gambler increased between 2005 and 2009 on average 361% from €8,3M to €29M. The betting amount totalled to €477 million in 2009 leading to a gross earning of around 6%[147].

With the growth of the online gambling market regulation on standards became stricter. Full identification of gamblers is required in order allow them to play, for pay out or when account funds reach certain levels. Identification allows the protection of minors and vulnerable people but prevents also potential fraudsters and money launderers from accessing online gambling. Today's offline identification means makes it difficult for operators to face the challenges of online identification without compromising ease of use for customers. The challenges rise with the increasing number of cross

border gamblers of different nationalities. Official eIDs would correspond to the different requirements of the online gambling market by making secure and unequivocal identification possible. They would also allow for minimal data disclosure and the verification of the identity claims of gamblers. The proposed Framework for electronic identification, authentication and signature enabling the mutual recognition and acceptance of official eIDs represent to the online gambling market a powerful trans national alternative to current solutions.

Another important sector which could benefit from mutual recognition and acceptance of official eIDs across border is the e

Health sector. According to a study carried out in Italy[148], overall savings from the introduction of Information and Communication Technologies in the health sector (online physicians, electronic prescriptions and sick leave certificates, digital health records, online booking of health services through online payments and medical reports, telemedicine) are estimated at around 11,7% of National Health Service (NHS) expenditures (i.e. €12,4 billion). Savings due to the introduction of online prescriptions should account for around 1,84% (almost € 2 billion). Territorial trials allow the conclusion that the introduction of online prescriptions could follow a 8

10% reduction of pharmaceutical and specialist healthcare expenditure (i.e. from €1,2 billion to €1,5 billion) currently originated by different causes such as misuse, material errors, wrong use of prescriptions, misalignment among registry offices or verification of exemptions.

c. Network Externality. The more users that benefit from the Pan European Framework for Identification, Authentication and Signature, the more visible and effective the above impacts are. Technological progress e.g. in remote care, which directly lowers health care costs, postpones or eliminates the need for institutionalised care, and makes it possible to increase workforce participation from home. As an example, the Scottish West Lothian council independent living programme has succeeded in ensuring that elderly couples with severe impairments can stay in their own homes. They have thus saved the public budget £84,000 on an annual basis.

The public consultation (see Annex 4) showed that stakeholders expect an impact of legislative measures addressing mutual recognition and acceptance of eID across borders. The main expected effects (with positive reply rates of more than 50%) were higher legal certainty (62,2%), reduction of administrative burden (60,8%), and the increase of cross-border mobility (59,1%). Economically, a positive impact is expected through the increase of economies of scale (49%).

3. Sector specific impacts of electronic identification and authentication

3.1. e-Procurement

---

146 Gamgling Capital, Arpil 2012

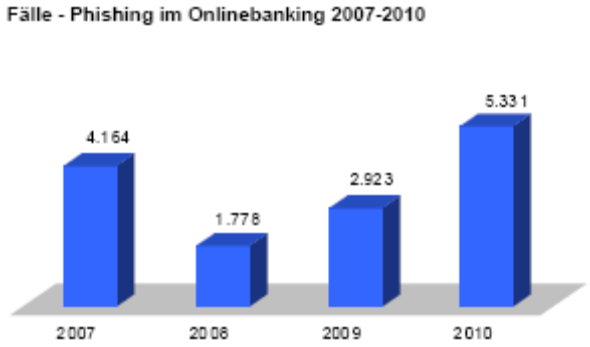
147 Gluckspielmarkt Deutschland 2015, Situation und Prognose des Gluckspielmarktes in Deutschland, Goldmedia, Berlin, 2010

148 Confindustria Servizi innovativi e tecnologici, ICT Project in the field of Health, 2010

On average, foreign suppliers in the e-Procurement sector are still limited to approximately 5% of total registered suppliers, signalling the relative weakness of the single market integration in public procurement[149]. A few small countries appear to be more open: Ireland (with 25% of foreign suppliers) and Cyprus, Estonia, Malta (with more than 10%). These economies use the national e-Procurement platform also to ease the access of suppliers from elsewhere in Europe, for the convenience of their public buyers. Another group of platforms (in Austria, France, Portugal, United Kingdom) declares a presence of foreign suppliers between 4 and 6% of the total registered suppliers and the other countries are around 1 to 2%. The public sector market has always been difficult for non domestic suppliers and the transparency and standardization of electronic procurement processes is a way around legal and practical barriers. Even if these numbers are still low, they represent a first step towards a greater opening of the internal market.
In the field of e-Procurement potential savings are the driver of implementing new systems and procedures. From the Scottish example we can learn about audited savings of almost £800 million over a 4-year period. Sweden has reported a reduction on prices between 10% and 30% as well as efficiency improvements in the procurement process of 20% going up to 30% when the entire tender is processed online. In Portugal there is a much shorter time to process tenders accompanied with a greater level of transparency. PECAP the Plataforma Electrònica de Contractació de les Administracions Públiques in Spain documents savings between 15 and 45% on overall prices of energy and telecom services for the local administrations. Similarly the Basque Country Regional Government has announced overall savings of 20% on purchase prices due to the increase in competition made possible by the electronic channel. Although the opportunities offered by e-Procurement are not yet fully reaped some of the national examples show the potential of further growth. eIAS with its different use cases (e.g. secure identification of bidders access to online platforms) could bring further benefits. Official eIDs have the advantage that they are already issued and used in the Member States with the connected authentication system in place allowing for verification and validation of identity claims. E-Procurement could profit from these already existing solutions and their EU-wide use enabled by the proposed action on mutual recognition and acceptance of official eIDs throughout the Union.

3.2. Identity theft

Official eIDs and authentication can also help to reduce fraud and identity theft in the internet. The growing number of threats demonstrate that action is needed. Compared to 2009, Germany registered an increase of 19% of cybercrime in 2010 (FN: Bundeslagebericht "Cybercrime 2010", Bundeskriminalamt, 2011, www.bka.de). The damage caused by internet crime grew from €39,6 million to €61,5 million in 2010. According to estimates the volume of cases not officially reported may be higher than 50%. A significant increase of phishing attacks (more than 82% compared to 2009) were reported totalling to 5.300 cases were criminals tried to get access to bank accounts via online banking .



Source: Cybercrime 2010, Federal Status Report, Federal Criminal Police Office, Germany

Secure electronic identification through the use of national eIDs could become attractive to all business sectors involved in or offering online business such as the credit card sector or online shops. Stolen credit card would become more difficult as national eIDs in combination with their related authentication systems are technologically much less easy to crack than currently used identification systems based on e.g. userdID and password.

149 9th eGovernment Benchmarking Report, December 2010

The use of eIDs issued in the Member States to securely access public online services could create significant added value for all those sectors where a higher security level of electronic identification is needed. One of these could be the environmental sector, in particular the new EU Emission Trading Scheme managing allowances with assets of around €110 billion. In January 2011 the Commission had to suspend transactions due to phishing attacks in the Member States which lead to the theft of emission certificates of a value of €28 million. The losses reported in Germany amounted to around 3 € million with 200.000 to 250.000 stolen certificates.

3.3. Large Scale Pilot STORK

The EU co funded Large Scale Pilot STORK offers an EU wide cross-border authentication platform for electronic services**.** The pilot enables European citizens to access services in participating countries in a secure way, by using their national eIDs. The process allows the individual the control of its ID data and the STORK infrastructure provides a high level of trust, security, privacy and data protection. STORK is implemented by a consortium of 32 partners, including 17 EU Member and Associated States, a number of companies and organisations from the private, academic and civil society sectors. As EU wide systems cannot be built without the support of industry and the interest of future users, the project has also created various communities of interest (Member States Reference Group, Industry Group) involving these stakeholders.

The different pilots running already real time show the wide range of use cases for official eIDs and secure authentication. "Safer Chat" demonstrates that official eIDs can be used by children and young people by building a platform for a safer online environment. The key to enter the room is the age of the chat user provided by the official eID. No further identity data are needed – one of the characteristics of official eIDs which would add value to the online gambling sector as described above. The pilot "Student Mobility" enables foreign students to get access to any online administrative service offered by a particular University using their national eID for identification purposes. It is used for the registration of Erasmus students which represent a population of 230.000 per year. The implementation of the pilot by the partner lead to spill over effects as universities involved integrated the official eID in their own environment for the whole range of online services in use. Other spill overs can be expected as the interest of other universities for take-over is very high. "Electronic Delivery" is piloting the mechanisms developed for secure cross-border delivery online. From the 9th Benchmarking eGovernment Report we already know that the electronic delivery is available in 47% of EU+27. The change of address pilot has shown also interesting spill over effects in the case of Portugal where the change of address is connected to another cascade of online services available to the citizens reporting the change of address. When communicating the change of address the foreign citizens can also opt to automatically communicate the change of addresses to e.g. the water supply company, electricity supply company, etc. "ECAS integration" is piloted by the Member States together with the Commission which operates numerous electronic services that require user authentication. Work is carried out in close cooperation between the STORK Member States supporting the pilot, the Directorate General Informatics (DIGIT), and the Commission's application owners. In practice, the pilot enables Member States experts to access the CIRCA network with their national eID.

What STORK and the future roll out of STORK enabled services is missing is an EU wide legislation for mutual recognition and acceptance. Currently, STORK and its pilots are based on agreements between partners to overcome the lack of common legal EU provisions for official eIDs. The proposed framework would provide these and with them the necessary conditions for the long term sustainability of STORK and all other projects and applications using the STORK platform.

4. Social impacts

The development of an eIAS Framework will also have significant employment effects. The Framework is expected to foster competitiveness and innovation. This will lead to greater employment in the EU and to a shift in employment structure towards more high-skilled jobs. This does not imply that the low skilled labour will become unemployed, but that their job-content increases because they move to sectors with higher productivity. However, it must be acknowledged that there are transition costs related to the inevitable transformation away from 'old' industries.

To give a concrete example of job creation in the area of new technology, the improvement of digital infrastructure alone will have important stimulating effects on the economy. Katz et al (2009) estimate that fulfilling the German National Broadband Strategy, where 75 percent of the population has access to 50 Mbps by 2014, will generate around 300,000 jobs from network construction alone. In the current business cycle situation of the EU, this is potentially a welcome stimulus to a construction industry which is more or less idle in some areas.
However, the dynamic employment effects of moving towards the eIAS Framework will generate even more jobs in the longer run. Using the MICUS model, we estimate an employment increase in the EU, including an increase in the adoption of online services from 3 percent to 4 percent per year. This is perhaps a conservative estimate, because Katz et al (2009) estimate that in Germany alone the improvement of digital infrastructure will trigger innovation and growth leading to an additional 427,000 jobs over the period 2015-2020.

Further social (and environmental) impacts can affect depopulated rural areas through the development of tele-working, eCommerce or smart metering. In rural areas the value added from people going online to profit from e.g. eGovernment, education and culture, eInclusion and eHealth services is even higher than in urban areas.

5. Environmental impacts

Organisations are moving away from the traditional time consuming paper processes and searching for new innovative technology to improve efficiency. E-signatures can significantly benefit organisations by eliminating the last of the paper in the business cycle. The ability to instantly sign and seal documents and transactions electronically results in much shorter process cycle times, accelerated customer service and drastic cost savings. Digital signatures provide enhanced convenience for both the consumer and the organisation, while significantly reducing application processing time.

A Deutsche Bank Research from 2008 analysed the use of automated data exchange for sending or receiving e-invoices by enterprises in the Member States and the EFTA countries. Indeed, this process can significantly have an impact on the environment by hugely reducing the amount of paper used by companies.
The top countries are Estonia (39%), followed by Norway (32%) and Italy (29%); while Sweden is beyond the average (18%) and Hungary is the bottom one (5%).

Italy expects immediate annual savings for the National Health Service from the abolition of paper flows of almost €600 million[150]. In 2008, prescriptions almost totalled €550M[151]. Following the abolition of printing costs and costs related to the delivery of forms to physicians, as well as costs derived from prescription printing, forwarding and filing a total saving accounting for almost €600 Mio per year could be obtained (with savings for each prescription between 1 and 1,5 euro)[152]. Savings for dependent workers accounting for almost €70 million would result from the abolition of the obligation to send sick leave certificates by certified mail letter to both the competent health administration and the employer. The cost of certified mail letters is €2,80 each, and sick leave certificates issued for private sector employees are almost €12 million a year, for a total of 24 million certified mail letters sent every year. The use of eIAS would be at the basis of most of these online applications thus contributing to the paperless office and its positive impact for the environment.

"Tax-online" figures from Austria show a continuous growth of paperless tax declarations since around the last decade, with an increase from 10% in 2002 to 48% in 2010[153]. The multi-channel access to the applications (2,6 mio users and 8,1 mio applications per year, 6,5 mio of which tax declarations) includes the use of the citizen card for electronic identification and authentication with smart cards since 2004 and mobile phone since December 2009.

6. Administrative burden

150 "Tavola della Sanita Elettronica": e-Health Standing Bureau (TSE) is an institutional platform where stakeholders consult each others with a view to harmonizing measures and elaborating a framework of shared technical rules.

151 Source: Federfarma

152 Confindustria Servizi Innovativi e Tecnologici, Data gathered from elaborations by Confindustria on the basis of the study entitled "Best Demonstrated Practice eHealth Impact", commissioned by the European Commission to Booz Allen Hamilton (2005)

153 Erich Waldecker, Entlastung der Verwaltung, Wirtschaft und BürgerInnen durch nachhaltige E-Government Projekte der Finanzverwaltung, e-Government Konferenz 2011, Salzburg, 8-9 June 2011

A major advantage of the eIAS framework is its ability to greatly reduce administrative burden by speeding administration and reducing compliance costs (for example, by reducing paper and mailing costs).

In this regard, Estonian's regulation has to be pointed out as a reference model. Most management of business with the government can be executed either by e-mail or through different portals. Simpler proceedings can be performed by way of summary procedures, but more complex transactions requiring legal certainty must be confirmed either with personal or notary's e-signature.

The development of e-services in Estonia has been facilitated by the comprehensive digital deployment of the Estonian ID card and broad availability of the Internet. Portugal has a similar aim and other countries are also moving in the same direction. Most Estonians know that they can communicate with the government without leaving home and confirm transactions by e-signature, if necessary.

Foreigners willing to do business in Estonia usually establish a company in the country but since November 2008, the Company Registration Portal[154] also recognises Portuguese, Finland, Belgium and Lithuania eIDs, allowing them to set up a company in Estonia through the Internet.

Similarly to the Estonian Company Registration Portal, the Portuguese business portal allows, in addition to the establishment of a company, submitting annual reports and amending registry details of a company.

Electronic proceeding considerably reduces administrative burden and facilitates the life of businessmen. For instance in 2008, 40% of companies were established and 20% of annual reports were submitted through the Estonian Company Registration Portal and the percentages have doubled every year.

154 https://ettevotjaportaal.rik.ee/index.py?chlang=eng

II. Related Trust Services

1. Electronic seals

The current e-signature Directive only covers e-signatures for natural persons and not for legal persons. The objective of electronic stamps or seals is to fill this gap by providing the same kind of instrument to legal entities in transposing mutatis/mutandis the rules of the currently used electronic signature to legal persons. The important feature of some documents issued by an entity is their authenticity. The fact that the document was indeed issued by the entity (e.g. insurance certificate, authorisation) can be proven by an electronic seal.

Estonia and Spain have already introduced this service in their national legislation.

The Estonian case In addition to electronic signatures, Estonian legislation covers the use of electronic seals (digital stamps in Estonian legislation). Electronic seals are technically equal to electronic signatures but have a legally different significance, since they can be performed without the direct consent of a physical person and consequently allowing for automated stamping. Certificates for electronic sealing can be issued to both legal and natural persons, by a certification service provider. It is expected that the public sector will find a number of new applications for the use of electronic sealing and therefore increase the market in this area. In Estonia, electronic seals are technically similar to electronic signatures.
Analysis Conceptually, regulating e-seals in the way provided by the Estonian regulation would recognise the specificities of the digital world towards the real one. Indeed, if in the real world a legal entity needs a legal representative, as a natural person, to give its agreement on a transaction, it is because the legal entity has no physical presence. In practice, currently a company proceeds through a physical person to agree on a transaction. This is also the case in the digital world. This means that at least one member of the company needs to possess its own electronic signature certificate. This certificate is supposed to be its own one and, in principle, cannot be shared. However, in practice, the certificates are shared in order to allow other company's members to act on behalf of the company. Obviously, electronic seal will not settle the problem of a magic wand: to be effective, an internal control system must be implemented within the companies in order to provide an efficient tool giving to the company, and its counterpart, the certainty that the right person(s) engaged the company.

(a) 2. Time stamping

Digital time stamp serves as a proof that the contents of the document existed at a point-in-time and that the contents have not changed since that time. The procedures maintain complete privacy of the documents themselves. The result is simple, secure, independent and portable proof of electronic record integrity.

52.4% of the respondents to the public consultation (see Annex 4) pointed out the need to regulate time stamping at EU level. The reason lies into the fact that relying parties mainly need to assess whether an e-signature was valid at the time it was created.

So far, at least 8 member states, i.e. Austria, Czech Republic, Germany, Italy, Romania, Slovakia, Slovenia and Spain have already have integrated time stamping in their legislation.

There is another related trust service which is built on time stamping: electronic registered delivery. In the absence of the basic tool, the derivative service cannot be created either.

In the absence of harmonising provisions at the European level, new internal market barriers will develop. A “qualified time stamping service” in Member State A may have no legal value in Member State B, either because Member State B has no legal framework for this type of service, or

because the legal framework is different. In practical terms, the time stamping service provider has no way of learning about possible issues other than to seek legal advice on a country by country basis, in order to discover whether its service has any value outside of its national borders, and what changes might be necessary to satisfy national legal requirements. This would appear to be a textbook example of the type of barrier that the European internal market should aim to avoid.

(b) 3. Admissibility of electronic documents

A paper document is a written or printed paper that bears the original, official, or legal form of something and can be used to furnish decisive evidence or information. By extension, an electronic document would be considered as proof to the same extent as a written document on paper format, provided that the document is retained in such conditions which guarantee the integrity of the document.

The objective in adding legal provisions on "electronic documents" in the future legal framework would be to provide a legal equivalence between physical and electronic documents subject to define security measures in order to facilitate the uptake of electronic documents.

The first obvious use case for electronic signatures is to authentically copy the handwritten signatures and hence the consent or commitment and aim of the signer may be that the electronic signature is meant and recognised as equivalent to a handwritten signature with a legal binding of the signer to the signed data.

Besides such an expected legal effect and scope of the signature, different natures or types of commitments may be associated to the signed data with or without the expression of a desired legal effect. This can range from positive or negative assertions or even mixing them to express more complex natures of the consent of signer to a signed data or document.

Typical use cases include the signing of an electronic document in different application contexts in whatever type of electronically processed communication or transaction (e.g. e-Business, e-Banking, e-Government, e-Procurement, e-VAT, e-Guichet, e-Procedures, e-Health, e-Justice, etc).

In this regard, an interesting legislation is the French Act of 13 March 2000 which contains multiple provisions relating to the law of evidence. It amends the French Civil Code: article 1316-1 allows an electronic document as proof to the same extent as a written document on paper format, provided that the document is retained in such conditions which guarantee the integrity of the document. Article 1348 specifies what constitutes an authentic copy.
An example of the utility of electronic documents at administration level is provided by the Austrian's eGovernment Act establishing rules for a specific category of signatures for civil servants (the Amtssignatur, §19) and for the authenticity of printouts of electronic documents. The so-called “official signatures” have been defined in the eGovernment Act (§18). Official signatures are indicated by an attribute in the certificate to facilitate recognition of the fact that a document originates from an authority. The official signature is represented in the electronic version of the document by an image which the authority has published on the Internet. Furthermore, the public authority is required to provide information on how to validate the signature. Finally, the eGovernment Act specifies that eDocuments signed with an official signature have equal legal value to official attestations (öffentlichen Urkunde) (§19). The print-out of the document itself must indicate a website where it can be electronically validated.

The official signature is an interesting concept, especially in combination with the electronic document validity and validation information obligations (i.e. their legal equivalence to official attestations and the support for validation of print-outs, which facilitates the transition between paper and electronic documents).

Finally, the eIAS Framework should be wide enough to cover all kind of documents (music, photos,…)

(c) 4. Long term preservation of e-signatures

The objective would be to ensure the legal validity of electronic signature through time despite and technology evolutions. In this respect, ensuring legal and technical ways of authentication of electronic signature and of certification authorities are of paramount importance in order to provide legal certainty.

The complex areas of archiving and long-term validation of electronically signed documents are often perceived as obstacles for the use of electronic signatures.

By analysing the existing models, we can determine the different elements which could be taken into account to regulate at national level in order to ensure validity of an electronic signature over time and technological evolutions.
1. Establish the equivalence between electronic documents and paper documents;
2. In order to meet the provisions on national prescription delays and to establish with absolute certainty the starting point of a transaction, ensure the harmonisation of time stamping's legislations. As harmonise the prescription delays seems out of the scope of EU attributions, a mandatory rule fixing the delay of conservation of the document in case of cross-border transaction seems appropriate. This delay should be the longer one provided by national laws applicable to the transaction;
3. Determine standards to guarantee the integrity of the document during the whole process;
4. Establish a "central national archiving office" in charge of taking care of the archiving of documents when required by law, or when asked by citizens and organisations (as well private than public);
5. Establish a term for the storage of documents depending of the duration of the prescription but also the duration of the contract. For example in France, for a contract, the duration of prescription is 10 years but the duration of a leasehold is 99 years.

(d) 5. Certified e-document delivery

This service would permit to certify the sending and delivery of a message (for example, an e-document).

Once a document has been created and signed (e.g. a contract, a notification of a judge), there are no means to send it to another country using an electronic service equivalent to registered mail. Provisions at EU level would be useful.

Adding "certified e-document delivery" provisions in the future legal framework would provide a legal equivalence between certified delivery by post and certified delivery by email subject to defined security measures. (if complemented by national law)

Unlike the common ‘read receipt’, a registered delivery e-mail helps protecting businesses and citizens with legally verifiable proof that a sent email was delivered, and legally verifiable proof of the content sent and received.

Belgium, Germany, France and Italy have already, or about to be, integrated in their national legislation the concept of registered delivery email.

In Belgium, the definition of electronic registered mail was introduced in the Act of 13.12.2010 (withdrawn due to procedural error). This new legislation intended to modify the act governing the organisation of postal services in Belgium and introduced legal constraints for the electronic registered mail in the Act of 9.7. 2001. "Electronic registered mail" is defined as "any service of electronic data transfer that includes a lump sum guarantee against the risk of loss, theft or damage of the data, in which the sender, possibly at his request, receives proof of sending and/or of delivery to the addressee. Electronic registered mail was considered to meet the requirements of registered mail, unless further regulatory requirements applied. In the absence of such requirements, electronic registered mail would be usable in all cases where traditional registered mail is legally required.

In France, the Decree of 2.2. 2011 (n° 2011-144) sets out the requirements with regard to the identification of the third party responsible for mailing (its legal status and contact details must be detailed), sending registered mail by electronic means (identification of both sender and recipient, with or without acknowledgment of receipt,

warranty for loss, theft or deterioration, etc.). The decree also provides for specific procedures and timeframes for the recipient to accept or refuse the registered e-mail.
Another country which has successfully implemented the registered delivery email in its national law is Italy. Electronic registered e-mail ("posta elettronica certificata") is defined in the Italian Code of Digital Administration as *"the communication system able to certify the sending and delivery of an e-mail"*. What is interesting about the Italian usage of this trusted service is that it appears to be the preferred means of communications between (i) different branches of the public administration, and (ii) the public administration and the citizens and companies, provided that the citizen/company obtained an electronic registered e-mail address and that this address has been registered in specific dedicated databases. It should also be noted that companies are obliged to have an electronic registered e-mail address as well as members of liberal professions enrolled in a registry, such as lawyers, accountants, etc. Citizens are not obliged to have an electronic registered e-mail address but they may get one (and in this case they may use it only to communicate with the public authorities). Public administrations as well shall have an electronic registered e-mail address that shall be published in the Internet site of the public authority concerned. Applications and declarations submitted to the public authorities through electronic registered e-mail are legally valid and accepted provided that the authentication tokens have been issued through the previous identification of the holder and that the system administrator certifies this.

6. Website Authentication

Authentication is part of verifying a website's ownership to establish trust. Before Web visitors provide username and password, payment information or other personal data, they need to know that they can trust the requested website. Improving access to business information and making it available for citizens in their own language could create a safer and more transparent "online" environment. **A company logo or brand name is not enough** because they can be easily faked:

First, some companies provide some sort of identification on their web-sites (such as legal name, legal form, registration number, address, contact information…) but the credibility of such self-declared credentials is questionable.

Second, some phishing sites are copy sites and make them look as close to the original as possible (everything from the logo placement, to the fake ads, etc) but the legal entity behind this web site is not the same as it is claimed.

The idea of secure authentication of the web company/owner has come up as an instrument to building up confidence.

What is Website Authentication?

The question to be answered is the following: " How to ensure that a Web site is indeed the website of the organisation **X** and how can users be sure that the organisation **X** legally exists?"

Website Authentication aims to make official company information easily accessible directly on the company's website, allow to display a "mark" from with the user will get a set of data to identify the owner of the website (i.e. Company name and code, address and contact details, legal form and current status, type of business activities, date of registration and registration authority, share capital and date of the latest annual accounts, etc).

"Authentication thought the Extended Validation (EV) Secure Sockets Layer (SSL) Certificate"

The Extended Validation (EV) SSL Certificate standard is intended to provide an improved level of authentication of entities that request digital certificates for securing transactions on their websites. An SSL provider (Certificate Authority) verifies an organization's right to use a domain name and

other required identification information. SSL Certificates are uniquely issued to a specific domain and Web server.

First a secure or encrypted website address using SLL certificates will begin with HTTPS rather than HTTP. Physically consumers will see a lock icon in the Address bar. Secure connections use certificates to identify the website and to encrypt the connection so that it will be more difficult for a hacker to view.

A fully-authenticated EV SSL certificate, contain information about the domain name and the legal name of the business or organization. It will also contain the geographical location information for the city, state, and country where the business is registered to do business.

Consumers can double-click the gold padlock icon from the Internet browser and it will display the information embedded within the SSL certificate of the site you are visiting. On the General tab it can see that the SSL certificate is issued to a specific domain name. The issuer of the certificate is also included. All SSL certificates will have this basic information: domain, validity period, and issuer.

Authentication thought the Extended Validation (EV) Secure Sockets Layer (SSL) Certificate seems to be a good way to ensure that a Web site is indeed the Web site of a specific organisation. However, there are some elements that do not solve the problem.

First, the EV certificate is issued for a certain period of validation, for instances, one year.155 The certificate do not guarantee that the information about the company – owner has been adequately updated.

As well, sometimes a company's website is independent of its stores, and the owner it might have different name than in the real world. The name of the owner display in the certificate could be different.

Finally, many consumers still do not understand the difference between a secure green address bar and a regular white bar, or the meaning of a lock icon in the Address bar. Consumers have not yet fully caught on to how EV certificates work, and not all older browsers support EV in terms of green bars and company names being displayed. These larger retailers may not see a large enough benefit to change their ways.

What are the benefits of identifying organization's Web sites for citizens and Member States?

The provision of information on Internet of legal persons is the responsibility of the market and business. Despite the efforts made by the private sector, products and technologies solutions in the market are not fully contributing to reassure consumers and citizens.

The identification systems of web sites' company owners that can be found on the Market should be improved with higher security requirements to reinforce the authenticity of information.

However, the Commission and Members States may play a role in ensuring such information in order to promote their neutrality and reliability:

- Website Authentication will provide the Web users with proof of identity of the organisation owning or operating the Web Site. It will cover the need to make web pages more transparent by ensuring that the consumer always knows the identity and contact details of the supplier.

[155] D&B's indicates what follows: A new business opens every minute, A business files bankruptcy every 8 minutes, A business closes every 3 minutes, A suit, lien or judgment is filed against a company every 14 seconds, a chief executive office changes every minute, A company name changes every 2 minutes. http://www.dnbmdd.com/mddi/record_updates.aspx

- Website Authentication will provide assurance that the holder of the identification tool is a real and legitimate company, with a physical presence at an identifiable location. The origin of the mark (the company registered authorities, chamber of commerce, etc) would bring trust.
- Website Authentication will ensure that a web page really belongs to the legal person and will avoid phishing through fake web page and potentially increase e-commerce by providing a trusted way to secure transactions.
- Website Authentication would be very useful for businesses to enable them to communicate to current and potential customers that "it is reputable", the confidentiality of their business, and the elements you would have in any possible legal action.
- SSL Certificates providers will be supervised in a transparent and neutral manner.
- At this stage, it is hard to define specific clauses for website authentication.

III. EU-based supervision system of e-trust services

Establishing a EU supervision body while cancelling national supervision

Under this sub-option, the national supervision system would be cancelled, and supervision tasks allocated to an EU level supervision body. National supervisory bodies that currently exist in all Member States (as required by the e-signatures Directive) would thus be abolished, or at least no longer perform any supervisory tasks.

The impact of this sub-option partially depends on whether a centralised model is followed, in which a single body at a single location is established, or whether a decentralised model is chosen in which some tasks of the European body are delegated to local organisations.

Centralised model

At the national level, the economic impact would be positive, as the cancellation of the national supervisory tasks would reduce costs to the national budget. This economic benefit would be partially offset by the need to either establish a new European level body, or to charge an existing body with supervisory tasks, which inevitably requires funding. A single centralised body can be expected to be more economically efficient, as it does not require 27 different bodies to be separately organised, staffed and funded, which inevitably implies administrative overheads that could be reduced by a single centralised body.

Impact on employment would thus likely be negative, as a single European body would need less staff than 27 national bodies. The social impact would also depend in part on the existing structure adopted by each Member States: if the supervisory body is part of an established public administration, public officials would likely be relocated to other services in their administration. Per contra, if the supervision has been delegated to an external partner or if a specific body has been created, the social impact of this option would be negative.

The global expected economic benefit (lower operational costs) relates solely to the cost of organisation of supervision. A centralised body in a single location would be economically inefficient in other ways. Specifically, the need to effectively supervise service providers across the EU means that (a) those service providers will need to show that they satisfy the supervision criteria to a body that might be geographically remote to them; and (b) that agents of the supervisory body would have to supervise service providers established across the EU, which might be very inefficient in cases where local audits are needed. On both counts, geographic distance will render supervision either expensive due to travel needs, or ineffective due to the impossibility of local visits. Either way, a strictly centralised model is likely not optimally efficient and cost effective.

Decentralised model

Under this option, the European body would decentralise some its activities, notably those requiring a physical presence, typically by delegating these tasks to private sector bodies at the national level. This option could have a positive economic impact: permanent tasks would be organised at the European level, so that Member States could free up their national budgets. Local auditing tasks could be contracted to private sector service providers via framework contracts, thus ensuring that costs are only ensured when audits are actually needed and performed. This would create a new sector of auditing activities within private national economies, giving support to the IT sector and developing a new proximity policy in the field of eIAS products and services. Moreover, the

negative social impact of the centralised model (due to the elimination of jobs in existing supervisory bodies) would be reduced, and could even be reversed.

Furthermore, the efficiency issue of the centralised model would be resolved, as trust service providers would still be audited by local companies, eliminating the challenges created by geographic remoteness. Perhaps most importantly, the credibility of the supervision system would be improved significantly compared to the current situation, as the single European body would apply the same norms, standards and practices across the EU. This would resolve the current problem of diverging supervisory practices.

This sub-option has an environmental impact by reducing needs to travel to Member States.

Globally, this would result in the following overview, scored against the status quo of strictly national supervision:

EU supervision model **Impact**	**Centralised**	**Decentralised**
Economic impact	+++	+
Social Impact	-	+
Environmental impact	--	0
Administrative burden	+	-
Credibility/effectiveness of supervision	++	+++
Score	**3**	**4**

A decentralised EU supervision model is thus clearly preferable to a strictly centralised EU supervision, and also outperforms the existing national supervision approach. The centralised approach does not appear to be superior to the current national supervision approach.

Establishing a EU supervision body while maintaining national supervision

Under this sub-option, a federated supervision system would be established involving an EU-based supervision body (again, either as a new body or as an additional mandate for an existing body), while maintaining the national supervisory bodies. Essential requirements for national supervision would still be developed and applied at the national level. The supervisory bodies would thus play the same role as it plays today. The EU level body would primarily be responsible for ensuring the consistent application of these minimum criteria.

Other tasks could also be envisaged for the European supervisory body, including as an optional supervisor of any European trust service provider. However, this does not appear to be a viable or desirable option, as it creates a clear risk of non-desirable competition between national and European supervision bodies: a service provider who is negatively assessed by a national body

might be tempted to turn to the European body as a de facto body of appeal. This situation would undermine the authority and competence of national bodies and install uncertainty.

An alternative model would be to allow Member States on a voluntary basis to delegate their supervision responsibilities to the European supervisory body. This would have the disadvantage for the EU body of greater responsibilities and thus greater economic costs than a mere coordination role, but would create significant benefits for Member States in which the operation of a credible supervisory body (including the need to ensure sufficient funding and availability of skilled experts) would be economically undesirable or impractical. This would thus be a beneficial option to Member States in which few or no trust service providers are to be supervised (i.e. Member States for whom the cost would otherwise be entirely wasted).

Both variants of this model would be beneficial for the credibility of the supervision mechanism: in the first variant (no delegation powers) the market would know that common minimum criteria are applied and monitored by a European body; and in the second (delegation right for the Member States) the market would be aware that supervision will be entrusted to an adequately staffed and funded body, either locally or at the EU level.

It should be noted that the impacts of the delegation suboption are hard to quantify, as it depends largely on the number of Member States that would opt on a voluntary basis to delegate their supervisory tasks. This issue might be politically sensitive in a number of Member States.

EU supervision model **Impact**	**Federated EU supervision – national supervision in all countries**	**Federated EU supervision – delegation power for Member States**
Economic impact	-	+
Social Impact	-	+
Environmental impact	0	0
Administrative burden	+	+
Credibility/effectiveness of supervision	+	++
Score	**0**	**5**

ANNEX 9 – IMPACT ASSESSMENT MATRIX

The matrix presents the determination of the expected impacts per policy option.

The assessment of the impacts under each of the options was done by analysing the *magnitude* of the expected impact, as well as the *likelihood* that the impact will actually occur as a result of the proposed policy option.

The notation used to express the magnitude of an impact in comparison with to baseline scenario is the following:

- - -	very negative impact	- 3
- -	negative impact	- 2
-	slightly negative impact	- 1
0	no impact	0
+	slightly positive impact	+ 1
+ +	positive impact	+ 2
+ + +	very positive impact	+ 3

The likelihood will be expressed as follows:

1	low likelihood	1
2	medium likelihood	2
3	high likelihood	3

The magnitude of the impact is weighed by to likelihood. The value given for the likelihood is an absolute score, i.e. not relative to the score of the baseline scenario.

Impacts	Option 0 No EU Policy				Option 1 Status Quo (No policy change)				Option 2 EU Regulation for eSignature and eID with supervision at national level				Option 3 EU Regulation for eSignature, eID and expansion to ancillary trusted services			
Specific objective 1: Increase the availability and take-up of cross-border and cross-sector eIAS services																
Economic impacts																
	Magnitude (compared to baseline)		**Likelihood**		**Magnitude**		**Likelihood**		**Magnitude (compared to baseline)**		**Likelihood**		**Magnitude (compared to baseline)**		**Likelihood**	
Risk of no or too low return on investments previously made in eIAS infrastrure, products and services	Without a EU Policy, it is not expected that many MS would collaborate on a voluntary basis, allowing eIAS supplies to find a larger outlet and to decrease payback times for investments. Investments made at EU, Member States, and private sector level based on the existing framework could be fullly lost, depending on the attitude of Member States after repealing the current Directive. In any case, EU-level services building on the results of Large scale pilots (LSPs) would not be roll-out.	-	Medium	2	Markets for eIAS products and services remain hard to access due to a lack of common rules, reducing possible return on investment. Take-up rates remain in general low (except in specific closed environments such as the banking sector) which causes very long investment payback periods. Services building on the results of Large scale pilots (LSPs) cannot be rolled out.	0	High	3	eIAS products and services gain appeal, increasing the return on investment on eIAS infrastructure, products and services.	++	Medium	2	eIAS products and services gain appeal, as ancillary services increase their overall usability to citizens, businesses and administrations. New investments in ancillary services are also likely to be triggered, further increasing the benefits.	+++	High	3
Increased impact of ICT investments on overall productivity and the competitiveness of the EU economy	Without common EU policies, Member States would be free to develop their own rules. This could lead to market fragmentation, thus harming the internal market and growth potential of European trust service providers.	0	Medium	2	Potential of eIAS is currently not fully exploited, especially not for cross-border transactions. Private investments remain insufficient in many regions; this cannot be remedied by investments made in other MS since other standards and rules apply. Services building on the results of Large scale pilots (LSPs) cannot be roll-out.	0	High	3	eIAS will become available for all sectors, all kind of companies, while eliminating cross-border barriers; new markets and new investments can be unlocked, thus stimulating innovation.	++	Medium	2	Ancillary services can generate significant benefits for productivity and competitiveness of the EU economy. New markets can be unlocked, new services can be developed, and existing inefficiencies can be reduced or eliminated.	+++	Medium	2
Reduction of the administrative burden (cost and time savings on e.g. printing, sending, receiving and storing of documents) for trust service providers and end users	With nationally diverging rules, Member States would need to adopt their own policies to reduce administrative burdens. Such policies would likely engender little to no benefits for trust service providers and end users in other Member States, and could in fact create barriers in the internal market.	0	Medium	2	Except for local applications in MS that have developed their own specific framework, there is not much room for reducing the administrative burden by using eIAS. Especially at the cross-border level and in the private sector (again, except in some specific closed environments), there are only limited ad hoc possibilities.	0	High	3	eIAS will become available for all sectors, all kind of companies and to the same extent for establishments located in different MS, so its potential could be fully exploited.	++	Medium	2	Ancillary services aim to increase the usability of trust services, and to ensure that an optimal number of paper based services can be replaced by more efficient trustworthy electronic alternatives. Significant reduction of administrative burden (including particularly printing, sending, receiving and storing of documents) can be expected.	+++	Medium	2
Social impacts																
Reduce barriers to move between areas (by allowing efficient EU-wide teleworking, eCommerce,...)	Without an EU policy, it is not expected that the current situation would significantly change. There could be some improvement, following local initiatives taken by MS (it is assumed that MS will continu to develop national eIAS), but these would not increase the availability of and trust en confidence in cross-border transactions.	0	Low	1	The wide availability for broadband connections currently allows exercising many professions from a distance, incl. in rural areas. However, a lack of availability of eIAS and/or a lack of trust and confidence in (cross-border) electronic transactions could still impede people to move away too far from (administrative) centers.	0	Medium	2	The EU Framework suggested under Option 2 would make it much easier to exercise a profession in rural areas, since many administrative formalities can be done from a distance. Also, since eServices (incl. eCommerce) would become more secure and trustworthy, more eCommerce activities could move to / set-up in rural areas.	++	Medium	2	Expansion of the legal framework to ancillary services would make it much easier to exercise a profession in rural areas. The positive effect would be stronger than for Option 2, since certain ancillary services (e.g. certified eDocument delivery and long term archiving) would especially favour rural areas where traditional alternatives might be less accessible..	+++	Medium	2

Impacts	Option 0 No EU Policy				Option 1 Status Quo (No policy change)				Option 2 EU Regulation for eSignature and eID with supervision at national level				Option 3 EU Regulation for eSignature, eID and expansion to ancillary trusted services			
Specific objective 1: Increase the availability and take-up of cross-border and cross-sector eIAS services (continued)																
Environmental impacts																
Reduced amount of paper used	Idem as under Option 1, assuming that MS would continu developping national initiatives of other trust services than eSignature.	0	Low	1	The possibility of reducing the amount of paper used is currently strongly reduced by the lack of an EU framework that transcends eSignatures. Indeed, some individual MS (continue) develop(ing) national frameworks for eIAS incl. ancillary services, but these frameworks differ between MS. As such, even if dematerialisation could be realised at the national level (e.g. by using electronic registered mail, time stamping, eArchiving), the lack of legal certainty and recognition at EU level is negatively impacting a large-scale shift to a paper-less administration.	0	Medium	2	An appropriate framework for eIAS that is harmonised at the EU level, would allow making paperless a significant number of transactions that require currently a 'physical' identification, authentication or signature. However, since ancillary services (e.g. electronic seals, time-stamps, certified e-document delivery, ...) would not be included in the harmonisation, multiple opportunities for further reducing paper would still be missed.	++	Medium	2	An comprehensive framework for eIAS and ancillary services could have a strong impact on paperless business and administration. An optimal number of opportunities for reducing paper can be leveraged.	+++	Medium	2
Total score Specific Objective 1			***- 2***				***0***				***+ 20***				***+ 33***	
Specific objective 2: Ensure an optimal level and scope of governance																
Economic impacts																
	Magnitude (compared to baseline)		**Likelihood**		**Magnitude**		**Likelihood**		**Magnitude (compared to baseline)**		**Likelihood**		**Magnitude (compared to baseline)**		**Likelihood**	
Increased legal certainty, trust and security of electronic transactions	This option is not expected to increase end user trust since no requirements are imposed or even suggested for the supervision of trust service provider. Possibly, bilateral or multilateral agreements between some MS for the mutual recognition of eID could improve the legal certainty of electronic transactions between these countries, but this would most probably remain very fragmented.	0	High	3	The current Directive is not providing legal certainty, trust and security of electronic transactions throughout the EU. Member states could continue to use the public service clause, leading to interoperability challenges for which no clear legal recourse is available.	0	High	3	A harmonised regulatory approach at EU-level, including effective supervision will enhance legal certainty, trust and security of electronic transactions. However, under this option, ancillary services would not be affected, which limits the beneficial impact.	++	High	3	A harmonised regulatory approach at EU-level, including effective supervision will enhance legal certainty, trust and security of electronic transactions.	+++	High	3
Reduced fragmentation of the market	This option allows the MS to define or maintain their own rules which could significantly differ from one MS to another and therefore lead to maintaining or increasing current legal and technical barriers. Cross-border interoperability is not expected to improve and could even become worse leading to an even more fragmented market.	-	Medium	2	Existing ambiguities will persist, leading to a segmented EU landscape and distortions in the internal market. Moreover, the differences in how market supervision is organised in each country will continue to be important and will lead to further fragmentation and distortions of the market.	0	High	3	Under Option 2, cross-border interoperability will be improved by establishing a clear, flexible and reality-proof set of harmonised technical standards. Furthermore, mutual recognition and acceptance of notified eID will further remove the current barrier to the single market for eIAS, leading to increased competition between suppliers of eIAS in the EU since they would all operate under the same (single) market conditions.	++	High	3	Under Option 3, cross-border interoperability will be improved by establishing a clear, flexible and reality-proof set of harmonised technical standards. Furthermore, mutual recognition and acceptance of all eIAS and the covered ancillary services would reduce market fragmentation, leading to increased competition between suppliers since they would all operate under the same (single) market conditions.	+++	High	3

Impacts	Option 0 No EU Policy				Option 1 Status Quo (No policy change)				Option 2 EU Regulation for eSignature and eID with supervision at national level				Option 3 EU Regulation for eSignature, eID and expansion to ancillary trusted services			
Specific objective 2: Ensure an optimal level and scope of governance (continued)																
Economic impacts (continued)																
Increased economies of scale and scope	Without a policy at the EU level, legal barriers due to non-harmonised legislation at the EU level are not expected to decrease compared to the current situation. As under Option 1, this would negatively impact economies of scale and scope.	-	Medium	2	The EU Framework is currently largely limited to eSignatures (scope); there are no "notified eIDs" available to both the public and private sector and there is no mutual recognition or acceptance of "notified eID". These elements strongly reduce the economies of scale and scope for suppliers of eIAS products and services.	0	High	3	Option 2 will remedy the market fragmentation for eIAS, as such the outlet for eIAS suppliers and the providers of trust services increases significantly, allowing for important economies of scale. Furthermore, since notified and mutually recognised eID could also be used for applications in private sectors, these latter could profit from the large scale role-out of (notified/official) eIDs (which took already place over the last few years) for accessing a large number of potential clients.	++	High	3	Option 3 will remedy the market fragmentation for eIAS and ancillary services; as such the outlet for eIAS suppliers and the providers of trust services increases significantly, allowing for important economies of scale. As with Option 2, these services would be available to all end users, including citizens, businesses and public administrations, thus realising an optimal potential.	+++	High	3
Socio-economic impacts																
Reduced risk of fraud and identity theft	Idem as under Option 1	0	Medium	2	Since eID products and services are currently not included in the EU framework, the risk of fraud and ID theft can vary between MS and cannot be reduced by EU-measures.	0	Medium	2	The harmonisation of the framework, including harmonised supervision of eIAS services allow for better detection of fraud and the development of measures to prevent identity theft.	++	Medium	2	Small gains can be expected compared to Option 2 due to the added possibilities offered by some ancillary services (attribute provision and time stamping, notably, which would respectively reduce exposure of personal data and increase the reliability of logs/audit trails).	++	Medium	2
Total score Specific Objective 2			***-4***				***0***				***+ 22***				***+ 31***	
Specific objective 3: Ensure that competitive market developments are stimulated and that technological developments are not hindered in the eIAS market																
	Magnitude (compared to baseline)		**Likelihood**		**Magnitude**		**Likelihood**		**Magnitude (compared to baseline)**		**Likelihood**		**Magnitude (compared to baseline)**		**Likelihood**	
Economic impacts																
Increased incentive for innovation	Idem as under option 1. While the absence of any EU rules would also avoid the risk of steering the market into a certain direction, this benefit is likely offset by the risk of Member States adopting their own rules (i.e. rather than one set of rules, service providers might be governed by 27 separate sets of rules)	-	Medium	2	The potential offered by innovative services is jeopardised due to market fragmentation.	0	High	3	Since the new framework would be technologically neutral and provide access to a larger outlet, there would be more incentives for developping innovative services. Innovative development for ancillary services would however still largely remain hampered by a lack of harmonisation at the EU level	+	Medium	2	Since the new framework would be technologically neutral and provide access to a larger outlet, there would be more incentives for developping innovative services. Under option 3, ancillary services would benefit from this effect as well.	++	Medium	2
Reduced risk that some regions can not benefit from private investments	Idem as under Option 1.	0	Medium	2	Since the current framework is leading to market fragmentation, there is no competition in the eIAS market at the EU level and regions with few local suppliers cannot benefit from eIAS services developed abroad.	0	Medium	2	Remedying the market fragmentation will allow easy to use and trustworthy eIAS products and services to become more easily available, also in remote regions and/or MS for which currently not much eIAS services were developed.	++	High	3	Remedying the market fragmentation will allow easy to use and trustworthy eIAS products and services to become more easily available, also in remote regions and/or MS for which currently not much eIAS services were developed.	++	High	3

Impacts	Option 0 No EU Policy			Option 1 Status Quo (No policy change)			Option 2 EU Regulation for eSignature and eID with supervision at national level				Option 3 EU Regulation for eSignature, eID and expansion to ancillary trusted services		
Specific objective 3: Ensure that competitive market developments are stimulated and that technological developments are not hindered in the eIAS market (continued)													
	Magnitude (compared to baseline)		**Likelihood**	**Magnitude**		**Likelihood**	**Magnitude (compared to baseline)**			**Likelihood**	**Magnitude (compared to baseline)**		**Likelihood**
Social impacts													
Increased employment of highly skilled workers	Idem as under Option 1.	0	Medium 2	Since the current framework is leading to market fragmentation and is not stimulating innovation, competitive and technological market developments are hindered. This has a negative impact on the employment of highly skilled workers.	0	Medium 2	A harmonised framework at the EU level could bring about the growth of existing and the creation of new businesses in the eIAS market, with a positive effect on employment. A priori, this would involve mainly highly skilled workers.	++	Medium	**2**	Same effect as Option 2, only somewhat stronger, due to the wider range of services affected by the Regulation.	++	Medium **2**
Total score Specific Objective 3			***- 2***			***0***			***+ 12***				***+ 14***
Specific objective 4: Strenghten the competitiveness of the European industry and services sector													
	Magnitude (compared to baseline)		**Likelihood**	**Magnitude**		**Likelihood**	**Magnitude (compared to baseline)**			**Likelihood**	**Magnitude (compared to baseline)**		**Likelihood**
Economic impacts													
Increased innovation in the EU industry and services sectors	Idem as under option 1. While the absence of any EU rules would also avoid the risk of steering the market into a certain direction, this benefit is likely offset by the risk of Member States adopting their own rules (i.e. rather than one set of rules, service providers might be governed by 27 separate sets of rules)	-	Medium 2	The unavailability of easy-to-use and trustworthy cross-border eIAS services is hindering the EU industry and services sector in innovating their internal and external processes (e.g. by making them more paperless).	0	Medium 2	By using eIAS, the European industry and services sector could innovate some steps of their internal and external processes. However, possibility would remain limited if there is no access to harmonised ancillary eServices for which legal certainty and technical security is ensured	+	Low	1	By using eIAS, the European industry and services sector could innovate on key steps of their internal and external processes. By including ancillary services, EU services could get an optimal boost.	++	Medium 2
Increased development of (public & private) on-line services, incl. at the cross border level	Without any support and coordination at EU level, Member States have greater difficulties in investing efficiently into cross-border interoperable solutions.	-	Medium 2	Full electronic processing of transactions is currently often (technically) not possible (e.g. due to interoperability problems at the EU level). The development of on-line services is furthermore hampered by legal uncertainty and trust issues which are not sufficiently dealt with by the current EU Framework. Development of on-line services is therefore mostly limited to local applications, e.g. for market players which only/mainly have a national footprint and that have access to official eIDs (e.g. national public authorities).	0	High 3	The development of the concept of "notified eID" will allow that the private sector can benefit from the important roll-out of eID already realised by many MS. Furthermore, the mutual recognition and acceptance of these eID will stimulate the development in on-line services, especially at the cross-border level, for both the public and private sector.	++	Medium	2	Same effect as Option 2, only somewhat stronger, due to the wider range of services affected by the Regulation.	++	Medium 2

Impacts	Option 0 No EU Policy			Option 1 Status Quo (No policy change)			Option 2 EU Regulation for eSignature and eID with supervision at national level			Option 3 EU Regulation for eSignature, eID and expansion to ancillary trusted services		
Specific objective 4: Strenghten the competitiveness of the European industry and services sector (continued)												
	Magnitude (compared to baseline)		Likelihood	Magnitude		Likelihood	Magnitude (compared to baseline)		Likelihood	Magnitude (compared to baseline)		Likelihood
Economic impacts (continued)												
Increased attractiveness for foreign investments	Idem as under Option 1.	0	High 3	There is currently litte incentive for companies from outside the EU or from other MS to invest in the development of eIAS products and services that can be used in a particular MS. Furthermore, the fact that the Services Directive cannot be implemented within the current framework makes it very unlikely that a company from one MS will soon be able to set up an activity in another MS via an electronic process; the cumbersome current paper based process is not encouraging investments in other MS. Moreover, in the longer run, if eServices would become clearly less developed in the EU compared to other regions, this could decrease the attractiveness of the EU for many diffferent sectors.	0	High 3	Option 2 will remedy the current market fragmentation, creating an important harmonised outlet market for eIAS which could also attract investments from outside the EU. The possibility for MS to implement the Services Directive would furthermore decrease the administrative barrier for setting up a business in any EU MS. Finally, the availability of eIAS without including ancillary services is not expecting to significantly reduce the risk that the EU would become less attractive if it is not developping eServices as well as global pioneer regions.	++	Medium 2	Option 3 would provide the EU with a very comprehensive framework for trust services, and provide a strong basis for European service providers to develop and market their services internationally. Inversely, the existence of European rules might make market entry harder for non-European service providers.	++	Medium 2
Total score Specific Objective 4			***-4***			***0***			***+ 9***			***+ 12***

Impacts	Option 0 No EU Policy			Option 1 Status Quo (No policy change)			Option 2 EU Regulation for eSignature and eID with supervision at national level				Option 3 EU Regulation for eSignature, eID and expansion to ancillary trusted services			
Specific objective 5: Ensure that all consumers can benefit from the advantage of (cross-border) eIAS services														
	Magnitude (compared to baseline)		Likelihood	Magnitude		Likelihood	Magnitude (compared to baseline)		Likelihood		Magnitude (compared to baseline)		Likelihood	
Socio-economic impacts														
Social inclusion/ eInclusion: Increased participation to the digital single market across different social groups	Idem as under Option 1. The situation will remain unchanged since it is expected that the individual MS will not have much incentives to create an EU trust landscape that allows participation to the digital single market by all social groups.	0	High	3	Take-up of (cross-border) on-line services (with the exception of some closed environments) is currently hampered by a lack of a sufficient level of trust and security of eIAS infrastructures, products and services as well as interoperability issues. These latter make eIAS unneccessarily complicated (e.g. because of the need of different devices, the unavailability of notified eID, etc.). Also, not all social groups have developed the required skills in order to feel at ease when using eIAS.	0	High	3	A harmonised regulatory approach at EU-level, including effective supervision will enhance legal certainty, trust and security of electronic transactions, leading to convince more social groups (e.g. through an effective communication strategy) to participate to the digital single market. Making eIAS a mass product would furthermore avoid that cost of implementation create a barrier to participate to the digital single market. Finally, the cross-border and cross-sector use of notified eID could strongly reduce the complexity of eIAS (e.g. multiple devices, passwords, etc.)	+	Medium	2	As option 2, but expansion of the legal framework to ancillary services would make IAS and ancillary services more easily available, which would benefit eInclusion further.	+	Medium	2
Regional development: Increased access to different services for people living in rural areas	Idem as under Option 1.	0	Medium	2	A faltering development of (cross-sector and cross-border) on-line services has a negative impact on the accessibility of services (e.g. eHealth, eGovernment,..) living in rural areas. Today, solely national services are becoming more and more available on-line, but these are mostly restricted to specific sectors (e.g. public sector, banking sector, ...).	0	Medium	2	Option 2 would allow to remedy the main obstacles related to eIAS that currently impede the access to (on-line) services in rural areas.	++	Medium	2	Expansion of the legal framework to ancillary services would make it much easier to access services from rural areas. The positive effect would be stronger than for Option 2, since certain ancillary services (e.g. certified eDocument delivery and long term archiving) would especially favour rural areas where traditional alternatives might be less accessible..	+++	Medium	2
Total score Specific Objective 5		*0*			*0*			*+6*				*+8*		
Grand Total		*- 12*			*0*			*+69*				*+98*		