Trusted e-ID Infrastructures and services in EU

TSP services, standards and risk analysis report

Report, December 2013

European Union Agency for Network and Information Security

www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

This report has been produced by ENISA (Prof. Manel Medina and Clara Galán) in collaboration with Atos Consulting (Alejandro Elices and M. Elena Martínez B.), and with the support of EC DG Connect "eIDAS Legislation Task Force" and the ISPC of the JRC.

Acknowledgements

The participants in the survey that have authorized to mention their contribution to this report are:

AC Camerfirma SA
AGETIC
AS Sertifitserimiskeskus
BANCO DE ESPAÑA
Borica - Bankservice AD
British Telecom PLC
Bundesnetzagentur
Commfides Norge AS
Consejo General de la Abogacía Española
DATEV eG
DGP
DHIMYOTIS
DigiSign SA
DigitalSign - Certificadora Digital, SA
Disig, a.s.
D-TRUST GmbH
EAD Trust, European Agency of Digital Trust
e-commerce monitoring gmbh
EDICOM (INTERCAMBIO ELECTR. DE DATOS Y COM. SL)
ESG de electronische signatuur B.V.
FÁBRICA NACIONAL DE MONEDA Y TIMBRE - REAL CASA DE LA MONEDA
FIRMAPROFESIONAL
Halcom d.d.
HSCIC
InfoNotary Plc.
Information Services Plc.
Izenpe
MINHAP
Ministerio de Defensa
Ministry of the interior
Multicert S.A.
Narodny bezpecnostny urad
National Security Authority
OpenCA Labs
Population Register Centre
Post.Trust
První certifikační autorita
QuoVadis Trustlink B.V.
Science and Technology Facilities Council
Sertifitseerimiskeskus
Spektar JSC
SSC
Viafirma S.L

Contact

For contacting the authors please use sta@enisa.europa.eu.

For media enquires about this paper, please use press@enisa.europa.eu**.**

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-076-5 doi: 10.2824/27048

Executive summary

ENISA has conducted a survey about the security mechanisms used by TSPs (Trust Service Providers) in Europe, and their interoperability, under the scope of the proposed new Regulation on electronic identification and trust services for electronic transactions in the internal market[1], which will supersede the current Directive 1999/93/EC on a Community framework for electronic signatures.

The target of the survey is 51 TSPs corresponding to 20 EU Member States and its focus has been the services whose provision will be regulated in the new Regulation:

- Validation of electronic signatures (eValidation)
- Long time preservation of electronic signatures
- Electronic Time Stamp
- Electronic documents admissibility (eDocument)
- Electronic delivery services (eDelivery)

The survey has addressed several issues of the services that are been offered: security practices, imlemented standards and risk analysis. Out of all the conclusions and recommendations, these ones have been considered the most relevant[2]:

- REC.1/R: Most of the TSPs participating in the survey have already adhered to national **CSP (Certificates Service Providers) certification schemas**. It is recommended to **extend** these schemas **to other Trust services** to have harmonized criteria of QoS (Quality of Service) assessment and SLA (Service Level Agreement) guidelines.
- REC.2/R: Promote **Trusted Marks assessed** against eIDAS requirements that would be recognised **across borders**.
- REC.3/R: **Cross-border interoperability of credentials** has to be promoted, mainly **e-singature**.
- REC.7/P: **Full adoption of e-signature format standards** by TSPs should be reached in order to be capable to validate any of them.
- REC.6/R: Specific BCM (**Business Continuity Management) standards** should be adopted in the provision of trusted services.
- REC.8/P: The use of **internationally trusted main time sources** and the definition of best practices to standardize the QoS through SLAs **must be promoted**.
- REC.12/P: Focus on user **training and consciousness** of threats to prevent 'Web site / service impersonation' threat has to be targetted.
- Other recommendations intend to reduce the **<u>higher reported risks</u>**:
  - REC.11/P **Relay on qualifiedqualified certificate revocation information** (mainly in eValidation services)
  - REC.10/P **Use 2 hash algorithms** to prevent **Evolution of cryptography** (mainly in Long Time Preservation services)
  - REC.6/R **Prevent Unavailability of service** through BCM (mainly in eValidation services)

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:en:PDF

[2] See full list in Section 6. The letter following the recommendation number indicates the category of stakeholder with higher responsibility on its implementation: Trust Service Providers (P), the Regulators/Supervisors (R) or the Customers of TSP (C).

- REC.4/P Promote **end-to-end encryption** to prevent **Web site / service impersonation** (in several services)

The document is divided in 3 different sections: Services, Standards, and Risks. Each section is structured in 2 parts: The first one shows the general results for all the services, and the second one the specific results for each of the offered services.

Table of Contents

Executive summary iv

1 Introduction 1

1.1 Background information 2
1.1.1 Motivation 2
1.1.2 Legal and policy background 2

1.2 State of the art 3
1.2.1 Relevant activities in EU: 3
1.2.2 EU funded Large Scale Pilots 3
1.2.3 Other EU funded projects 4
1.2.4 CIP PSP 5
1.2.5 Relevant communities 6
1.2.6 Activities outside the EU 6
1.2.7 Non-EU projects 7

2 Methodology 8

2.1 Questionnaire 8

3 Trust Services 11

3.1 General results 11
3.1.1 Electronic certificates versus other trust services 11
3.1.2 Which Other trust services? 11
3.1.3 Certificates scope 12
3.1.4 Sectors where the services are addressed 13
3.1.5 Authentication mechanisms 14
3.1.6 How is the service provided? 15
3.1.7 Storage of Documents 16

4 Standards 17

4.1 General results 17
4.1.1 Security Management Standards 17
4.1.2 Audits 18
4.1.3 Documents 19

4.2 e-Signature Standards 20

4.3 Electronic time stamp services 21
4.3.1 Main time source 21
4.3.2 Time stamp format standards 21

4.4 Validation services 22

4.5 Long Time Preservation standards 22

5 Risk Analysis 24

5.1 Overview of the risks 27
5.1.1 Web site / web service impersonation 28
5.1.2 Unavailability of the service 29
5.1.3 Lose or alteration of evidences in chain of trust 30
5.1.4 Lose or alteration of digital evidences 31
5.1.5 Lose or compromise of service’s signature creation data 32
5.1.6 Relay on non-updated certificate revocation information 33

5.2 Overview of the services 34
5.2.1 Electronic Time Stamp services 34
5.2.2 eDocument services 35
5.2.3 eDelivery services 36
5.2.4 Validation services 37
5.2.5 Long Time Preservation services 38

6 Conclusions and Recommendations 39

6.1 Services scope 39

6.2 Standards implemented 40

6.3 Risk Analysis 41

6.4 Summary of Recommendations 42

7 Annex I: Acronyms 44

8 Annex II: Launch of the Survey on Trust Services in the EU 46

1 Introduction

The European Commission presented in June 2012 a proposal for a new Regulation on electronic identification and trust services for electronic transactions in the internal market[3], which will supersede the current Directive 1999/93/EC on a Community framework for electronic signatures. Art. 15 of the proposed Regulation establishes certain provisions regarding the security requirements applicable to trust service providers.

In order to facilitate the implementation of this provision, as well as to generally support trust service providers (TSP) in the introduction of security best practices, the European Union Agency for Network and Information Security (ENISA) is working in 2013 on a series of studies on the security aspects of trust service providers issuing electronic certificates, as well as on the security and interoperability aspects specific to the new trust services foreseen in the proposed Regulation.

The definition of "trust service" in the EU Regulation is quite wide, since it theorically covers all combinations of the services applied over the objects shown in the Table 1 below.

TRUST SERVICES		**eService**				
		Creation	Verification	Validation	Handling	Preservation
Objects	eSignature	🟩	🟩	🟩	🟩	🟩
	eSeal	🟩	🟩	🟩	🟩	🟩
	eTimeStamp	🟩	🟩	🟩	🟩	🟩
	eDocument	🟩	🟩	🟩	🟩	🟩
	eDelivery	🟩	🟩	🟩	🟩	🟩
	WebSite	🟩	🟩	🟩	🟩	🟩
	eCertificate	🟩	🟩	🟩	🟩	🟩

Table 1: Trust services as defined in the EU Regulation

ENISA has conducted a survey about the security mechanisms used by TSPs in Europe, and their interoperability. This survey was addressed to every current TSP that is offering, or intending to offer in the future, any of the services identified in the proposed Regulation. In order to simplify the combinations of services over objects, only those services most frequently referenced in eGovernment applications have been included in the survey:

- Electronic certificates, including e-Signature ones (summarized in other ENISA reports[4])
- Electronic time stamps (creation and handling)
- Electronically signed documents storage or management (creation, handling or preservation)
- Electronic delivery of eDocuments services (handling, preservation)
- Validation of electronic signatures (documents, certificates, seals, websites)
- Longtime preservation of electronic signatures (documents, time stamps)

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:en:PDF
[4] http://www.enisa.europa.eu/activities/identity-and-trust/trust-services

1.1 Background information

1.1.1 Motivation

In its Work Programme 2013 ENISA has divided its work into Work Packages; this project is related in particular with its Work Package 1.2. The purpose of this work package is to identify the risks and threats trust services European infrastructure is exposed to. Such risks/threats can emerge both from the technologies and services themselves (like bad design, improper coding, etc.) and from their improper usage. Besides the risks and threats, wherever possible the opportunities should also be identified, as this is key to taking advantage of new models for security controls and new usages of existing controls.

1.1.2 Legal and policy background

Herein follow some relevant legal initiatives relevant to this project:

- On 4 June 2012, the European Commission published a new draft EU regulation on "electronic identification and trust services for electronic transactions in the internal market"[5] that is meant to extend the existing e-Signatures Directive to include new services such as e-time-stamping or e-seals that would guarantee the origin and the integrity of an electronic document. The proposed Regulation will ensure people and businesses can use their own national electronic identification schemes (e-IDs) to access public services in other EU countries where e-IDs are available. In order to analyse the impact of the implementation of this new Regulation, the Commission made two studies:
    - Study to support the implementation of a pan-European framework on electronic identification and trust services for electronic transactions in the internal market (SMART 2012/0001)[6].
    - Impact assessment[7] of the new regulation
- Proposal for a Directive of the European Parliament and of the Council on the accessibility of public sector bodies' websites[8]
- European eGovernment Action Plan 2011-2015[9]. The European Commission aims to support the provision of a new generation of eGovernment services for businesses and citizens. The Action Plan identifies four political priorities based on the Malmö Declaration[10], agreed on 18 November 2009.

[5] http://www.edri.org/edrigram/number10.11/ec-proposal-electronic-identity
http://eur-lex.europa.eu/Notice.do?checktexts=checkbox&checktexte=checkbox&val=679649%3Acs&pos=1&page=1&lang=en&pgs=10&nbl=1&list=679649%3Acs%2C&hwords=&action=GO&visu=%23texte

[6] http://ec.europa.eu/information_society/newsroom/cf/dae/itemdetail.cfm?item_id=8363

[7] http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

[8] http://ec.europa.eu/information_society/newsroom/cf/dae/itemdetail.cfm?item_id=9125

[9] https://ec.europa.eu/digital-agenda/en/european-egovernment-action-plan-2011-2015

[10] http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf

- Communication from the Commission to the EU Parliament, the Council, the EU Economic and Social Committee and the Committee of the Regions "Towards interoperability for European public services"[11]

1.2 State of the art

The aim of this section is to summarise the information collected during the desktop research phase of the project, showing the projects that provide or use trust services. In the context of the project it has been used to select some stakeholders to contribute, validate and/or disseminate the results of the analysis made of the status of the TSPs security in EU, and to identify some relevant regulatory actions. It is provided just for information purpose.

1.2.1 Relevant activities in EU:

World e-ID Congress[12] has become in eight years a key event gathering over 350 e-ID programs managers, government officials and technology experts around world's major e-ID projects, policies trends and latest innovations.

The Commission launched a study on collaborative production in eGovernment (SMART 2010/0075)[13]. As part of this collaborative activities, the Commmission has developed **Open e-Prior**[14], open source version of e-Prior software, for e-Procurement services in the Public sector, freely available for the EU public administrations.

1.2.2 EU funded Large Scale Pilots

The Build/Connect/Grow[15] EU magazine identifies the following Large Scale Pilots[16]:

- Secure Identity Across Borders Linked (**STORK II**[17]). STORK simplifies bureaucratic hurdles and administrative delays to provide citizens and the business community with easy but secure access to their benefits and administrative records no matter where they are in Europe. Within this overarching framework, there are pilots dedicated to:
    - Cross-border authentication for electronic services;
    - Providing safer internet chat for children and adolescents;
    - Facilitating mobility for university students seeking to study abroad within Europe;
    - Developing cross-border mechanisms for secure online delivery of documents; and
    - Assisting people formalize a cross-border change-of-address.

[11] COM(2010) 744 final: http://www.epractice.eu/files/Towards%20interoperability%20for%20European%20public%20services%20-%20Commission%20Communication.pdf
[12] http://www.worlde-idcongress.com/call-for-papers-2013
[13] http://ec.europa.eu/information_society/newsroom/cf/dae/itemdetail.cfm?item_id=9141
[14] http://joinup.ec.europa.eu/software/openeprior/forum/all
http://www.youtube.com/watch?v=VHGI7re4Q_k
http://www.peppol.eu/news/news_repository/open-e-prior-release
[15] http://www.buildconnectgrow.net/en/build?load=build/infographics-build
[16] http://ec.europa.eu/digital-agenda/en/egovernment
[17] https://www.eid-stork.eu/

- **SPOCS** [18] (Simple Procedures Online for Cross-Border Services) has made significant achievements, from establishing 'Document Equivalence' between national administrations to enhancing 'semantic interoperability' (making different countries understand each other and work together digitally). Furthermore, they highlighted areas requiring improvement, notably in terms of abolishing legal barriers and addressing public misconceptions of the security of electronic information transfers.
- Despite the completion of the Pan-European Public Procurement Online (**PEPPOL**[19]) project in August 2012, a number of public and private members of the PEPPOL community committed themselves to further drive adoption of standardised eProcurement solutions – encompassing eAttestations, eCatalogues, eOrders, eInvoices and eSignature validation and an open document exchange network – with the creation of OpenPEPPOL. OpenPEPPOL is a non-profit international association of public and private PEPPOL community members.
- **e-CODEX**[20] "e-Justice Communication via Online Data Exchange" Cooperating with other LSPs in the fields of eDelivery, ePayments, eDocuments, eID and eSignatures, e-CODEX will demonstrate how the building blocks for cross-border interoperability can be implemented in numerous domains, including e-Justice. Two pilots are developed under this project:
  - The European Arrest Warrant (EAW) requires a national executing judicial authority to recognise requests for the surrender of a person made by the judicial authority of another Member State (the issuing judicial authority) for the purposes of prosecution.
  - Mutual Recognition of Financial Penalties. Previously, many offences – ranging from simple road traffic offences to organised crime – went unpunished due to their transnational nature. With this pilot, financial penalties imposed against an offender in a foreign country can follow them to their home country, with their domestic authorities being tasked to collect the penalty. The pilot is currently being developed for three EU Member States – France, Germany and the Netherlands.
- Smart Open Services for European Patients (**epSOS**[21]) ensures those European travellers are well cared for. It provides standards for the exchange of medical information, thereby leading to informed health care and a safe continuity of treatment.

1.2.3 Other EU funded projects

EU security projects funded by the FP7[22] include the following, which are quite closely related to trusted eIDAS and e-Government:

- **ABC4Trust**[23] Attribute-based Credentials for Trust
- **FutureID --** Shaping the Future of Electronic Identity
- **Primelife**[24] Privacy and Identity Management in Europe for Life
- **PICOS**[25] Privacy and identity management for community services

[18] http://www.eu-spocs.eu/
[19] http://www.peppol.eu/
[20] http://www.e-codex.eu/
[21] http://www.epsos.eu/
[22] http://cordis.europa.eu/fp7/ict/security/projects_en.html#TSI
[23] https://abc4trust.eu/
[24] http://www.primelife.eu/
[25] http://www.picos-project.eu/

- **GINI-SA**[26] Global Identity Networking of Individuals - Support Action
- **SWIFT**[27] Secure widespread identities for federated Telecommunications
- **OPTET**[28] OPerational Trustworthiness Enabling Technologies
- TURBINE[29] Trusted revocable biometric identities
- **CUMULUS**[30] Certification infrastrUcture for MUlti-Layer cloUd Services
- **BEST**[31]
- **SIGNEO**[32]
- **SABRINA**[33]

From the previous Framework Programme we can mention the following initiatives:

- **BRITE** Business Register Interoperability Throughout Europe
- **EEPOCH**[34] eEurope Smart Card Charter proof of concept and holistic solution
- **PRIME** Privacy and Identity Management for Europe
- **FIDIS** Future of Identity in the Information Society

Another interesting programme was the IDABC[35] where two relevant studies were produced, one on eID, and another (PEGS[36]) on e-Signature recognition in e-Government.

1.2.4 CIP PSP

There is an initiative to build a Thematic Network for European eID (**SSEDIC**[37])

The objective of this network is to provide a platform for all the stakeholders of eID (electronic identity) to work together and collaborate to prepare the agenda for a proposed Single European Digital Identity Community as envisaged by the Digital Agenda (DAE) in its Key Action 16

They have launched a survey on the use of eID of different kind and also to retrieve the opinion of the citizens about the use of eSignature and Privacy: http://ivox.socratos.net/l.0/1d3aDfnkc4k6rSj7at4tmNXMVVy3uy

It's also worth to mention the CIP project:

SEMIRAMIS[38] Secure Management of Information across multiple Stakeholders

[26] http://cordis.europa.eu/fetch?CALLER=ICT_UNIFIEDSRCH&ACTION=D&DOC=3598&CAT=PROJ&QUERY=012566805427:fddf:67bd9cf8&RCN=95534

[27] http://www.ist-swift.org/content/view/23/32/

[28] http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=13272191

[29] http://www.turbine-project.eu/

[30] http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=13156501

[31] http://www.besthw.eu/

[32] http://www.bitoceans.com/

[33] http://www.sabrina.uni-karlsruhe.de/

[34] http://www.eepoch.netl

[35] http://ec.europa.eu/idabc/en/document/6484.html

[36] http://ec.europa.eu/idabc/en/document/6485.html

[37] http://www.eid-ssedic.eu/

[38] http://ec.europa.eu/information_society/apps/projects/facts heetlindex.cfm?project_ref-250453

1.2.5 Relevant communities

There are several communities identified in the JOINUP[39] portal funded by the Commission. Here are some of the most relevant to this project:

- The National Interoperability Framework Observatory (NIFO[40]), one of the projects from the EC's ISA program (Interoperability Solutions for European Public Administrations), is intended to provide assistance
- This group is for developer and integrators who are integrating peppol[41]. The idea is to share knowledge, exchange ideas and general discussion on E-invoice system.
- IDABC[42]
- Greek eGovernment Interoperability Framework, eGIF[43]

1.2.6 Activities outside the EU

NSTIC[44]: National Strategy for Trusted Identities in Cyberspace. Five U.S. organizations will pilot identity solutions that increase confidence in online transactions, prevent identity theft, and provide individuals with more control over how they share their personal information:

- The Cross Sector Digital Identity Initiative (CSDII) lead by the American Association of Motor Vehicle Administrators (AAMVA) will implement a secure online identity ecosystem that will lead to safer transactions by enhancing privacy and reducing the risk of fraud in online commerce.
- The Criterion pilot will allow consumers to selectively share shopping and other preferences and information to both reduce fraud and enhance the user experience.
- The Daon pilot will demonstrate how senior citizens and all consumers can benefit from a digitally connected, consumer friendly Identity Ecosystem. The pilot will employ user-friendly identity solutions that leverage smart mobile devices.
- The Resilient pilot seeks to demonstrate that sensitive health and education transactions on the Internet can earn patient and parent trust by using a Trust Network built around privacy-enhancing encryption technology to provide secure, multifactor, on-demand identity proofing and authentication across multiple sectors.
- UCAID, known publicly as Internet2, intends to build a consistent and robust privacy infrastructure through common attributes; user-effective privacy managers; anonymous credentials; and Internet2's InCommon Identity Federation service; and to encourage the use of multifactor authentication and other technologies.

NSTIC also Launched in August 2012, the Identity Ecosystem Steering Group (IDESG), which includes volunteer companies, organizations and individuals dedicated to promoting the creation of standards and policies that will accelerate the development and adoption of the Identity Ecosystem.

[39] https://joinup.ec.europa.eu/community/all
[40] https://joinup.ec.europa.eu/community/nifo/home
[41] https://joinup.ec.europa.eu/community/pid/home
[42] https://joinup.ec.europa.eu/community/idabc/home
[43] https://joinup.ec.europa.eu/community/greek-egif/home
[44] http://www.nist.gov/nstic/pilot-projects.html

1.2.7 Non-EU projects

To finish, it is worth to mention some projects from outside EU that are relevant to eIDAS and TSP:

Non-profit-organizations/initiatives:

- **Central Authentication Service Project**
- **Identity Commons**
- **Kantara Initiative**
- **Open Identity Exchange**
- **eID working group**
- **OpenID**

Open Source projects/initiatives:

- **OAuth**
- **OAuth 2.0**
- **OpenSocial**
- **Portable Contacts**
- **Information Cards**
- **The Pamela Project**
- **simpleSAMLphp**
- **Shibboleth**
- **OSIS**

2 Methodology

This report collects the results of the survey launched by ENISA about the current security practices implemented by the newly regulated trust services in the EU, whilst other reports of ENISA[45] have analysed the results of the eSignature and e-Seal related services, including the certificates that enable them and their application to e-Documents or Web-Sites.

This report describes the answers of the TSPs to that survey and the conclusions regarding the different issues related to the new trust services they provide, the security and interoperability mechanisms they implement, and the assessment of the different risks they face.

The survey was launched mainly to the relevant TSPs accredited in the Trust-Service Status List (TSL[46]) published by the Supervising authorities, as well as some private contacts of the authors of this report. Amongst those, relevant representatives of the most relevant ones from each MS were contacted directly by the authors, in order to guarantee that they would contribute to the survey.

The survey obtained 67 answers, of which 51 were considered valid, since several answers were merged as they referred to different services from the same TSP, and some others were from providers outside the EU. Finally, only the replies which included complete and consistent information were taken into consideration. The main background information about the participants is:

- The TSPs are from the following countries: Austria, Bulgaria, Czech Republic, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Lithuania, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and United Kingdom.
- 93% of the TSPs participating in the survey are also Qualified Certificate Service Providers (CSP). This may be because most of the TSPs invited to participate in the survey were contacted via TSL and the national supervising authorities, that in most of the cases reported that only have official records of the qualified CSP. So, since invitations were made mainly through national regulators of certification service providers and the trust services lists they elaborate, and since till now only the CSP TSP are regulated, TSPs not providing CSP are not in those TSL and the national regulators neither keep records of them, since their services are not regulated.

2.1 Questionnaire

ASIC-S	Simple Associated Signature Container, published by ETSI as TS 102 918
BCM	Business Continuity Management
CA	Certification Authority
CAdES	CMS Advanced Electronic Signatures , published by ETSI as TS 101 733
CEN	European Committee for Standardization

[45] http://www.enisa.europa.eu/activities/identity-and-trust/trust-services

[46] https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers, standard format published by ETSI as TS 102 231

CEN BII	CEN Workshop on 'Business Interoperability Interfaces"
CRL	Certificate Revocation List, see “RFC 5280”
DG	Directorate General
DPA	Data Protection Authority
DSS	OASIS Digital Signature Services
EC	European Commission
e-CODEX	e-Justice Communication via Online Data Exchange
eID	Electronic Identification
eGov	e-Government
eIDAS	electronic Identification and Authentication Service
ENISA	European Union Agency for Network and Information Security
epSOS	Smart Open Services for European Patients
eSign	electronic Signature
ETSI	European Telecommunications Standards Institute
ETSI TS	ETSI Technical Specification
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Standards Organisation
IT	Information Technology
LSP	Large Scale Pilots
MS	Member State
NCP	National Contact Point
NIS	Network and Information Security
NRA	National Regulator Authorities
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol, see “RFC 2560”
PAdES	PDF Advanced Electronic Signature, published by ETSI as TS 102 778
PEPPOL	Pan-European Public Procurement Online
PKI	Public Key Infrastructure
PoC	Point of Contact
QoS	Quality of Service
REC	Recommendation
SAML	Security Assertion Markup Language
SHA	Secure Hash Algorithm.
SLA	Service Level Agreement
SML	Service Metadata Locator
SMPs	Service Metadata Publishers
SP	Service Provider
STORK	Secure *IdenTity* AcroSs BoRders LinKed project
TS	Trusted Service
TSL	Trust-Service Status List, published by ETSI as TS 102 231

TSP	Trust Service Provider
TTP	Trusted Third Party
URL	Uniform Resource Locator
USB	Universal Serial Bus
USD	United States Dollar
XAdES	XML Advanced Electronic Signature, published by ETSI as 101 903
XKMS	XML Key Management Specification
XML	eXtended Markup Language

Annex II: Launch of the Survey, reproduces the list of questions made to the participants in the survey.

3 Trust Services

This section reflects the results about the type of services delivered and the way they are offered by the providers.

3.1 General results

3.1.1 Electronic certificates versus other trust services

Figure 1 represents the level of implementation of the trust services (others than electronic certificates) which will be regulated in the future.

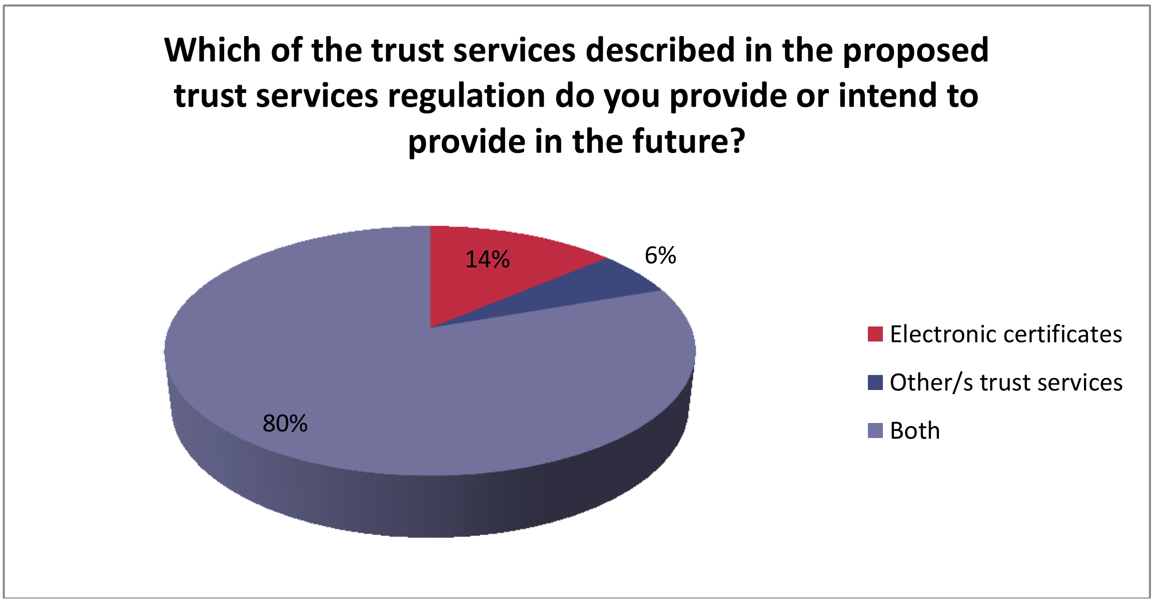


Figure 1: Trust services provided

The results show that only 6% of TSPs participating in the survey are providing **only** other trust services than electronic certificates. So the vast majority of TSPs are already complying with current regulation, and the number of qualified TSPs in the market will not grow excessively with new regulation.

3.1.2 Which Other trust services?

Figure 2 represents the percentage of implementation for the rest of trust services considered.

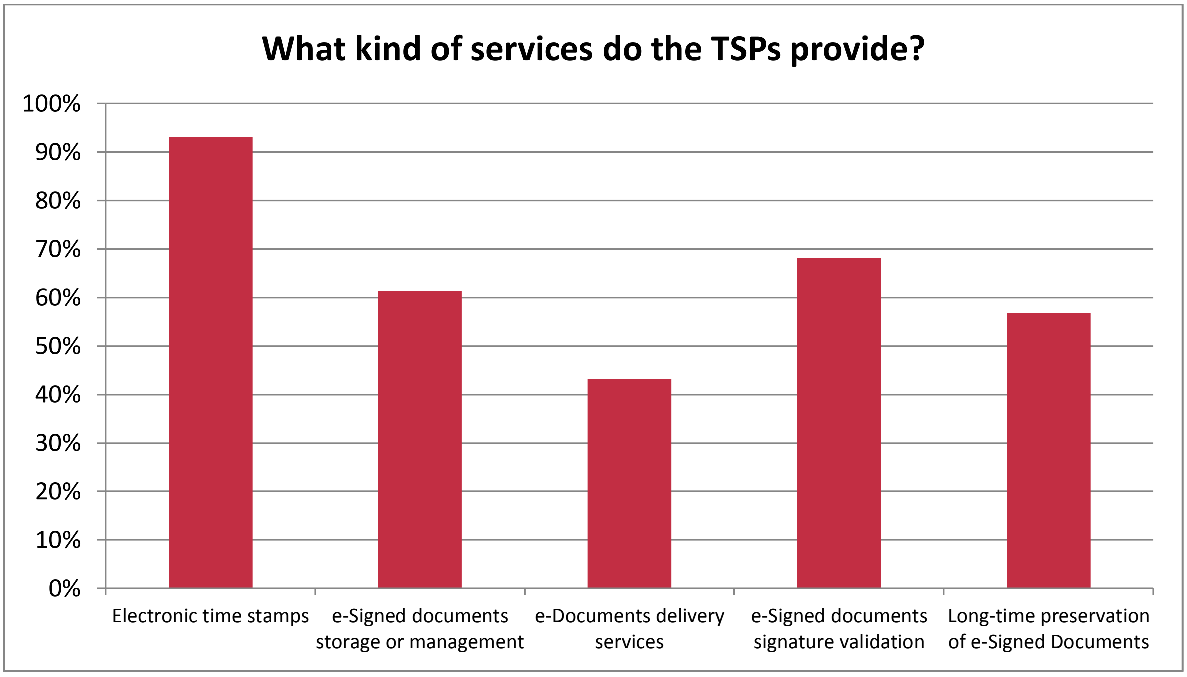


Figure 2: Trust services provided

More than 90% of all the TSPs participating in the survey reported that they provide '*Electronic time stamps services*', whilst '*e-Documents delivery services*' was the least spread service offered (less than 50%). The other services are between 60% and 70%.

3.1.3 Certificates scope

Figure 3 represents the span of supported certificates: '*Only own CSP support*', '*National CSPs support*', '*Partial international support*', '*Total international support*'.

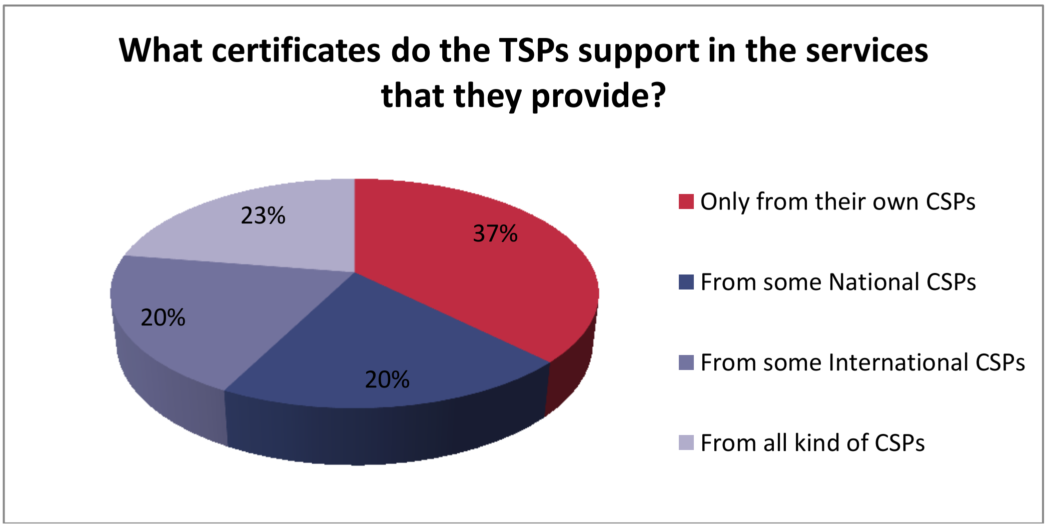


Figure 3: Span of supported certificatescertificates

37% of the TSPs support certificates only from their own CSP, but it is maybe worst to notice that 57% only accept certificates issued in the same country. The conclusion is that the segmentation of the EU market is very high, as shown in the graphic, and that cross-border interoperability has to be promoted.

3.1.4 Sectors where the services are addressed

Figure 4 represents the type of target customers for trust services. It shows that most of the TSP participating in the survey provide services to several categories of customers.

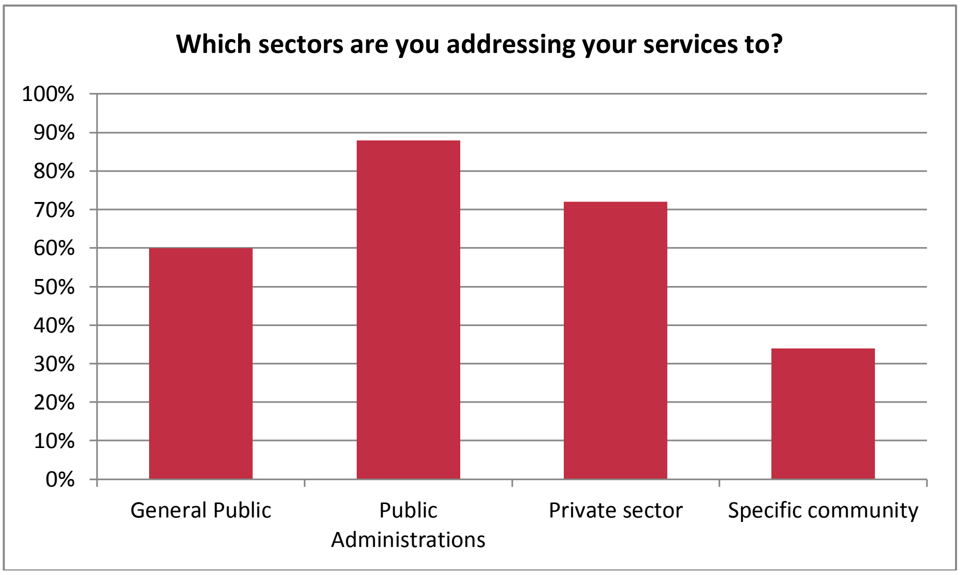


Figure 4: type of target customers for trust services

Figure 5 and Figure 6 detail the results of the participants that have selected one of the following categories of customers:

- **General Public**
- **Specific Communities**
- **Public Administrations versus Private Sector**

1- Figure 5 shows the Results Focused on General Public:

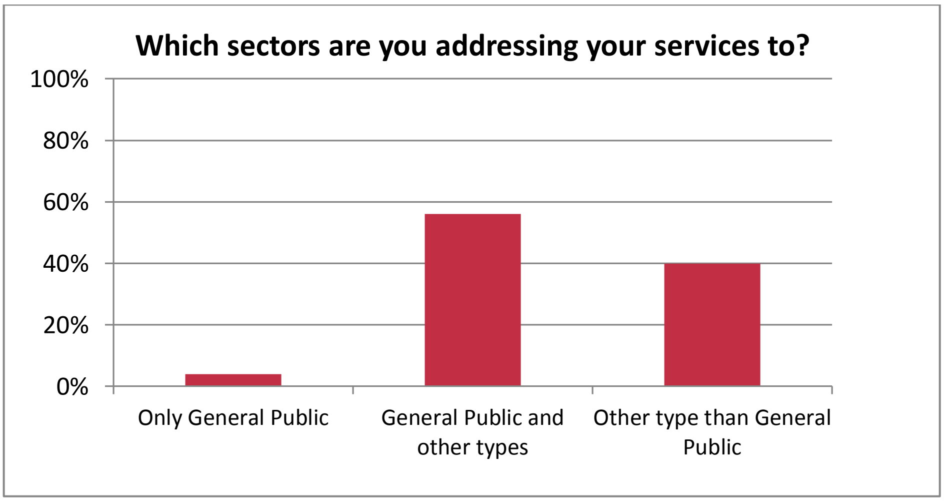


Figure 5: Sectors where services are addressed: General Public view

Amongst those that indicated that they offer the service to General Publice, the provision for '*Only General Public*' is residual. Although 40% of TSPs don't provide their services specifically to General Public, the combination of '*General Public and other types*' represents more than 50% of the results.

2- Figure 6 shows the Results of TSPs providing service only to Public Administrations and Private Sector (i.e. excluding 'only General Public').

The bars in the Figure 6 also indicate the percentage of TSPs that are offering services to 'specific communities' within the category. This happens in 3/4 of the TSP offering service only to Private sector, 1/5 of the providers of only Public Administration and 3/8 of those that provide service to both sectors:

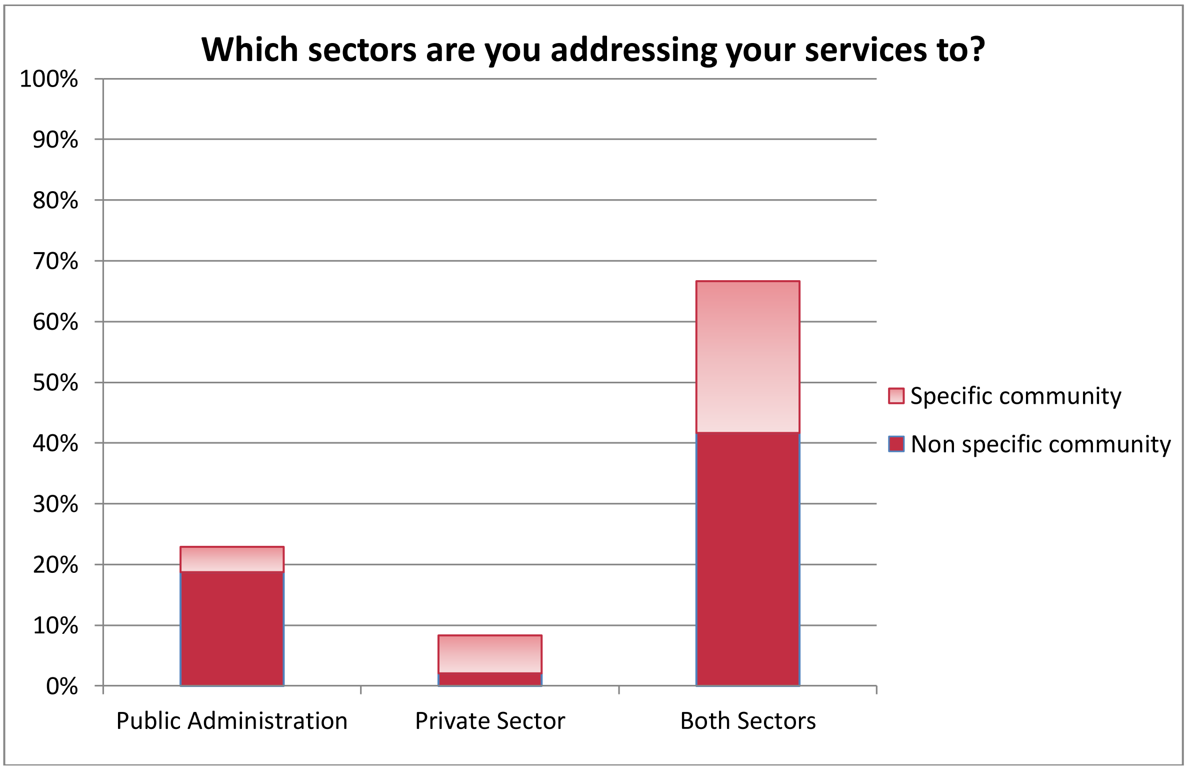


Figure 6: Sectors where services are addressed: specific communities

3.1.5 Authentication mechanisms

Figure 7 shows the different authentication mechanisms used by TSPs to grant customers access to their different services.

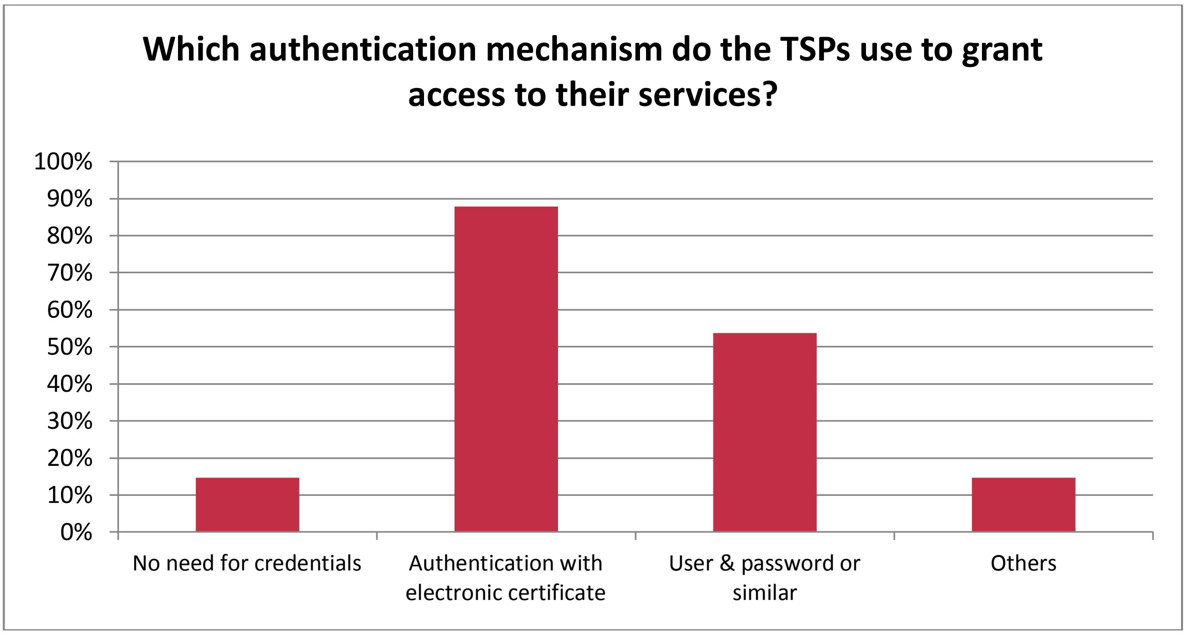


Figure 7: Authentication mechanism implemented by TSPs

Despite of the fact that 88% of the participants indicated that they use eID certificates to authenticate their customers, most of them also allow authentication using other mechanisms. Amongst those that answered ‘*No need for credentials*’, 5/6 stated that they also use ‘*Electronic certificates*’ and ‘*User/password*’. There was only one TSP that only answered ‘*No need of credentials*’ (and no other mechanism). This was a provider of Certificates and Time Stamp services, where user authentication is not usually needed. The remaining TSPs use different authentications mechanisms based on the criticality of the offered service.

In the option ‘*Other mechanisms*’, the providers answered the following mechanisms:

- OTP based in EMV-CAP (1 answer)
- PostIdent - German identification process (1 answer)
- X-Road (1 answer)
- IP address authentication or IP whitelisting (3 answers)
- Federated identity (Shibboleth) (1 answer)
- Moonshot (1 answer)

3.1.6 How is the service provided?

Figure 8 shows the platform offered by the TSPs to provide their services to final users.

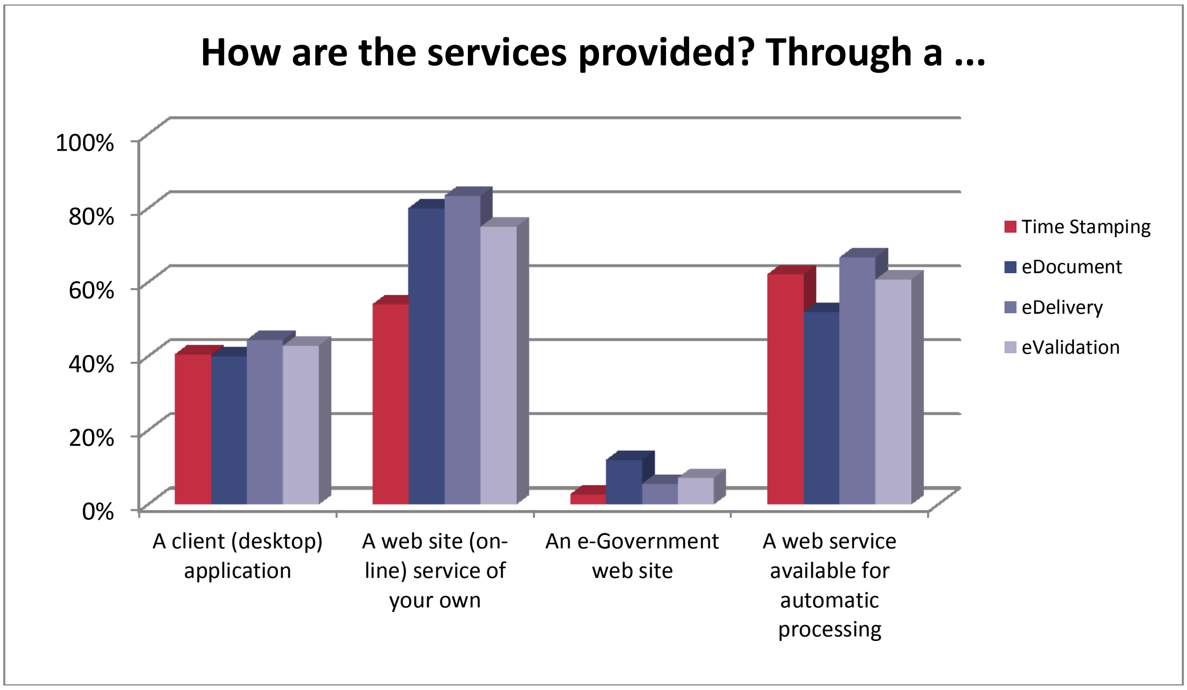


Figure 8: Service provision platform of TSPs

The '*Government web site'* is rarely used regardless of the type of service (less than 10%). '*On-line TSP web site'* is the most common answer for all services (between 70 and 80%), except for Time Stamp, for which the preferred option is '*Web service available for automatic processing'*.

The graphic also indicates that there are TSPs that use several channels to provide the service.

For security reasons it is recommended to promote the use of web services, to force secure communication channel with parameters agreed with the TSP in a way transparent to the user.

3.1.7 Storage of Documents

Graphics in Figure 9 indicate whether providers store the documents or not. This information is compared between the eDocuments signature management and the eDelivering services.

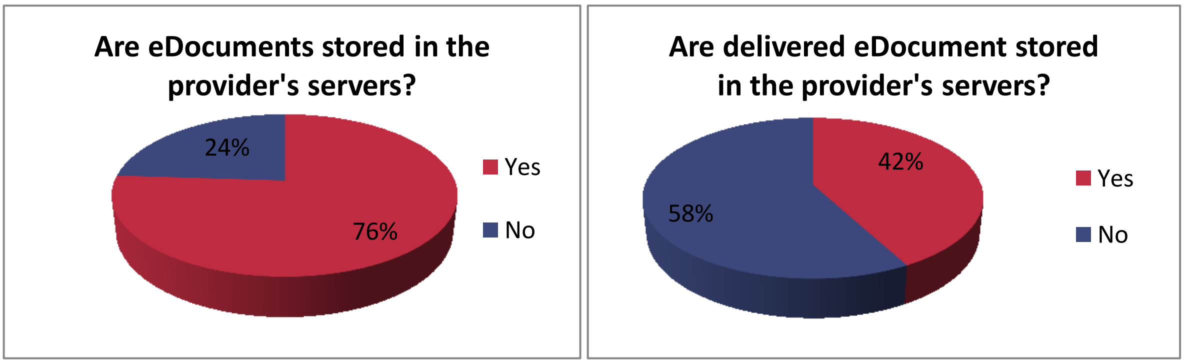


Figure 9: Storage of documents practice.

The results show that most of eDocuments trust providers store the documents (76%), while for eDelivery this percentage drops to 42%. This difference can be explained by the nature of the services.

4 Standards

This section reflects the results about the type of standards and schemas that the TSPs adhere or are compliant to.

4.1 General results

4.1.1 Security Management Standards

Figure 10 indicates the main security management standards followed by the TSPs.

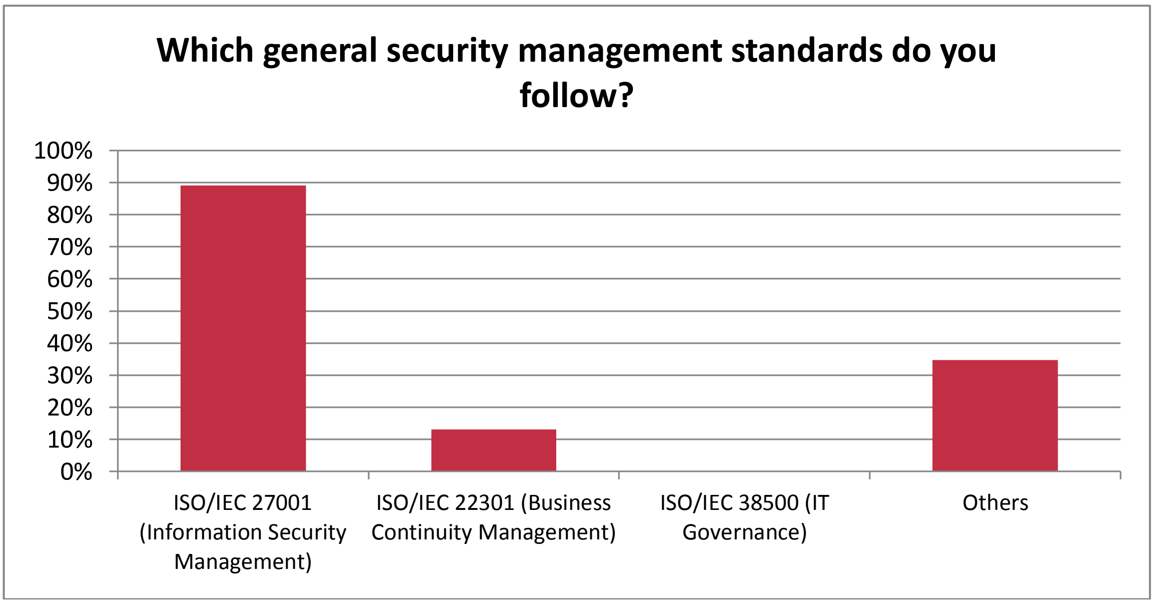


Figure 10: Information Systems Security management standards adopted/assessed

The results indicate that about 90% of the TSPs that answered this question follow the '*ISO/IEC 27001*' standard. Only 5 TSPs don't use it, either because they have local standards for that purpose (as those developed by the German Federal Office for Information Security BSI) or because the TSPs are neither a CSP nor a Qualified TSP, so they don't need to comply with ISO/IEC 27001.

Few TSPs have adopted other relevant standards:

- It's remarkable that the de-facto market standard 'ISO/IEC 38500 for IT Governance' is not implemented at all, probably because it's not a security standard and it's not required in the certification schemas.
- It's also worth mentioning the low adoption of ISO/IEC 22301: Business Continuity Management. Since one of the most relevant risks identified by the participants in the survey is the unavailability of the service, and the most relevant incidents in the sector have been related with service interruptions, specific standards to guarantee the continuity management should be promoted.

TSPs that have indicated 'Others standards' have named the following (although not all of them are specific to IS Security Management Standards):

- ETSI TS 102 042 (1)
- BSI Grundschutz (1)
- Ministry of Defense Information Security Policy (1)
- ISO 20000 (2)
- ETSI 101 456 (4)
- Webtrust (3)
- ISO/IEC 12207 (1)

- IGTF (2)
- ISO/IEC TR 13335 (1)
- ISO/TR 13569 (1)
- ISAE3402 (1)

4.1.2 Audits

Figure 11 reflect the type of security audits the organizations perform, as well as their frequency.

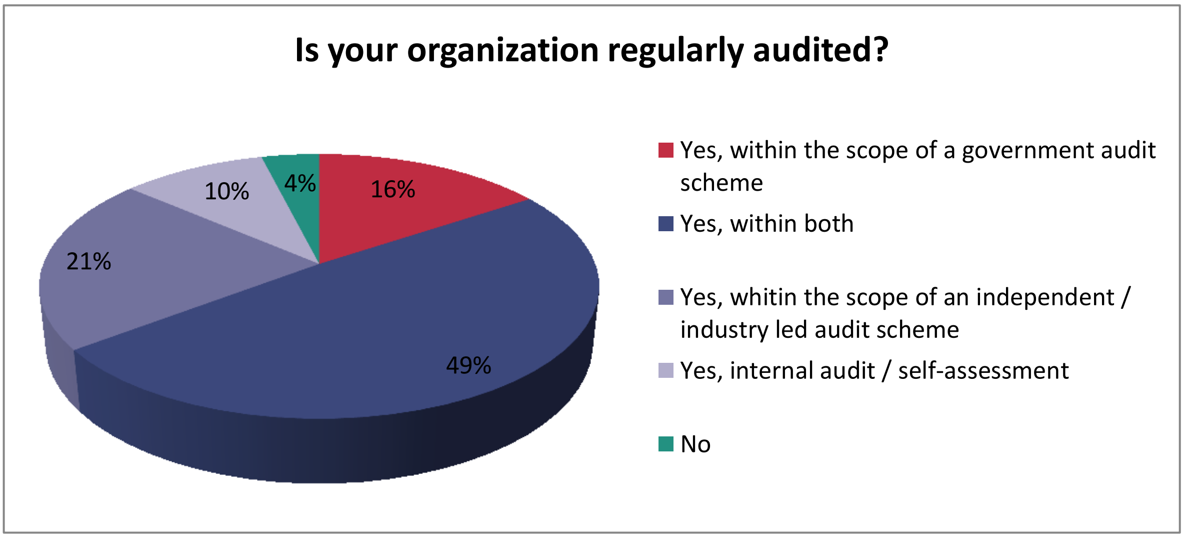


Figure 11: Auditing policy

16% of the TSPs stated that they are audited ‘*within the scope of a government audit scheme*’, similarly to those that acknowledged that they audited ‘*within the scope of an independent / industry led audit scheme*’, with a 21% ratio. Moreover, 49% informed that they are audited ‘*within both scopes*’.

96% of providers are regularly audited. Half of them are both audited ‘within the scope of an independent / industry led audit scheme’ and ‘within the scope a government audit scheme’. Only 4% of the surveyed TSPs indicated that they are not audited. This can come as a result of not offering qualified services.

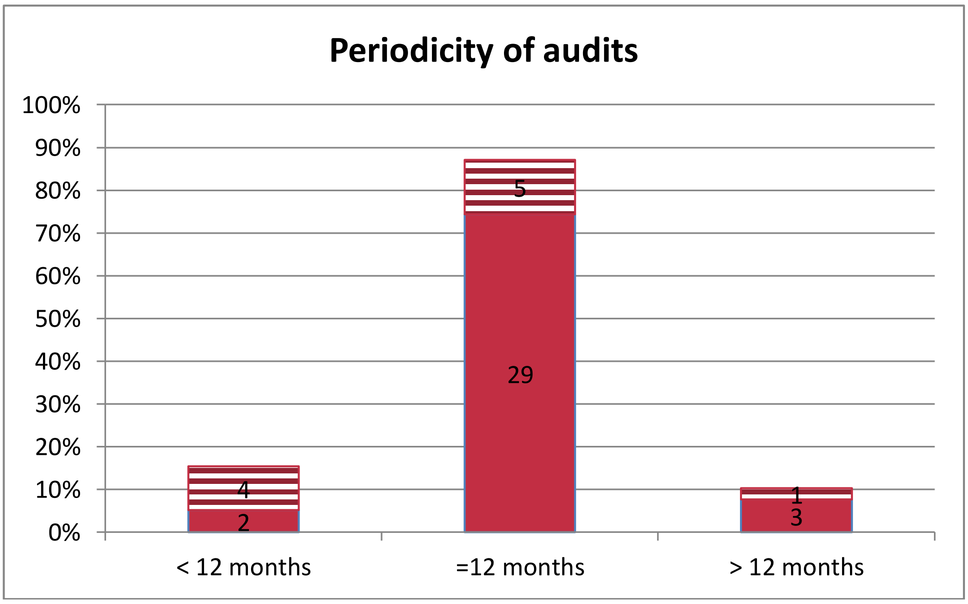


Figure 12: Auditing frequency

Regarding audits' frequency(see Figure 12), almost 90% of the TSPs perform '*annual audits*' and 13% of those TSPs said they complement them with other ones: 4 TSPs monthly or every 6 months. Only 3 TSPs answered that its frequency was higher than one year; 1 TSP informed of a biannual audit. Annual audits should reach the 100%.

4.1.3 Documents

Figure 13 shows the answers about the existence of security, risk and continuity policies, statements, and plans in the surveyed organizations.

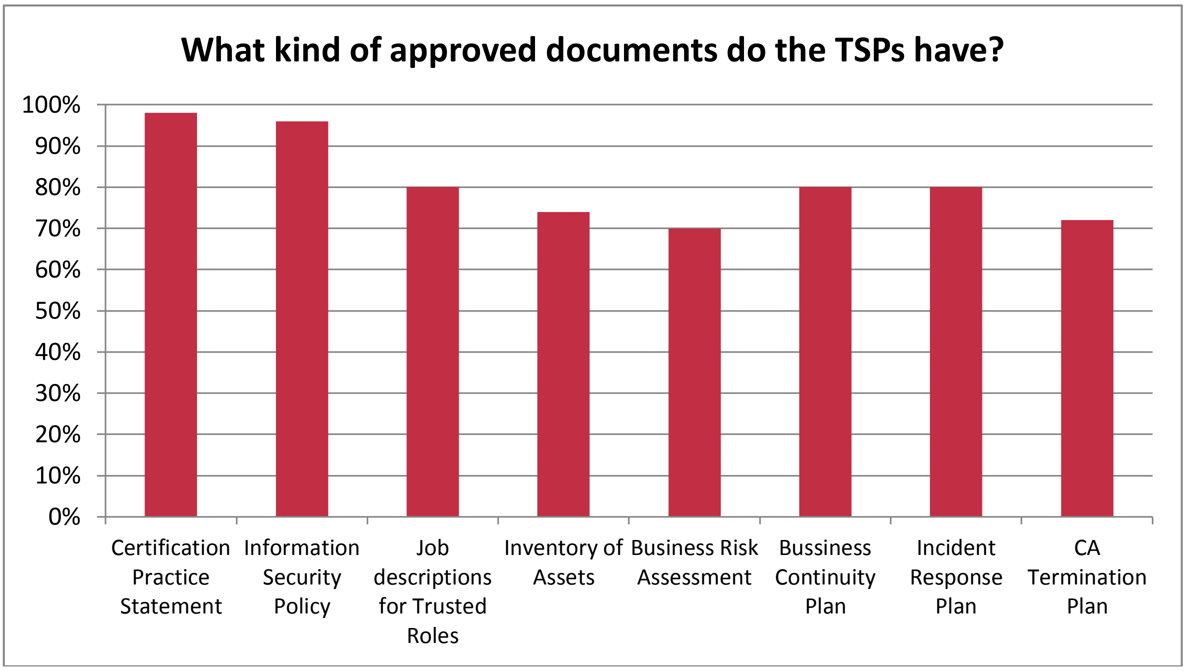


Figure 13: Security policy Documents approved

Almost every TSP (96-98%) implements '*Certification Practice Statement*' and '*Information Security Policy*' types. Regarding approved documents, all TSPs providing electronic certificates have the *'Certificate Practice Statement'* document implemented. However, the documentation regarding continuity of services *('Business Risk Assessment', 'Business Continuity Plans'*, *'Incident Response Plans'*) is not fully implemented (about 80%), although it should be.

In the case of 'Certificate Practice Statement', 3 TSPs inform that they offer different services than electronic certificates, but there has been only 1 TSP stating that it doesn't have a Certificate Practice Statement, probably because a document describing the use of internal certificates exists.

It is interesting to notice that almost 20%-30% of TSPs do not have '*Business Risk Assessments*' (BRA) nor '*Business Continuity Plans*' (BCP), neither '*Incident Response Plan*' (IRP), which could be explained through the consideration of BRA, BCP and IRP as a part of their Information Security Policy.

Our recommendation regarding continuity of services is that all the documents related with it must be implemented: '*Business Risk Assessment*', '*Business Continuity Plan*' and also '*Incident Response Plan*' and '*CA Termination Plan*' (this last one if applicable).

4.2 e-Signature Standards

Figure 14 displays the comparison of the different e-signature standards supported in the services analysed.

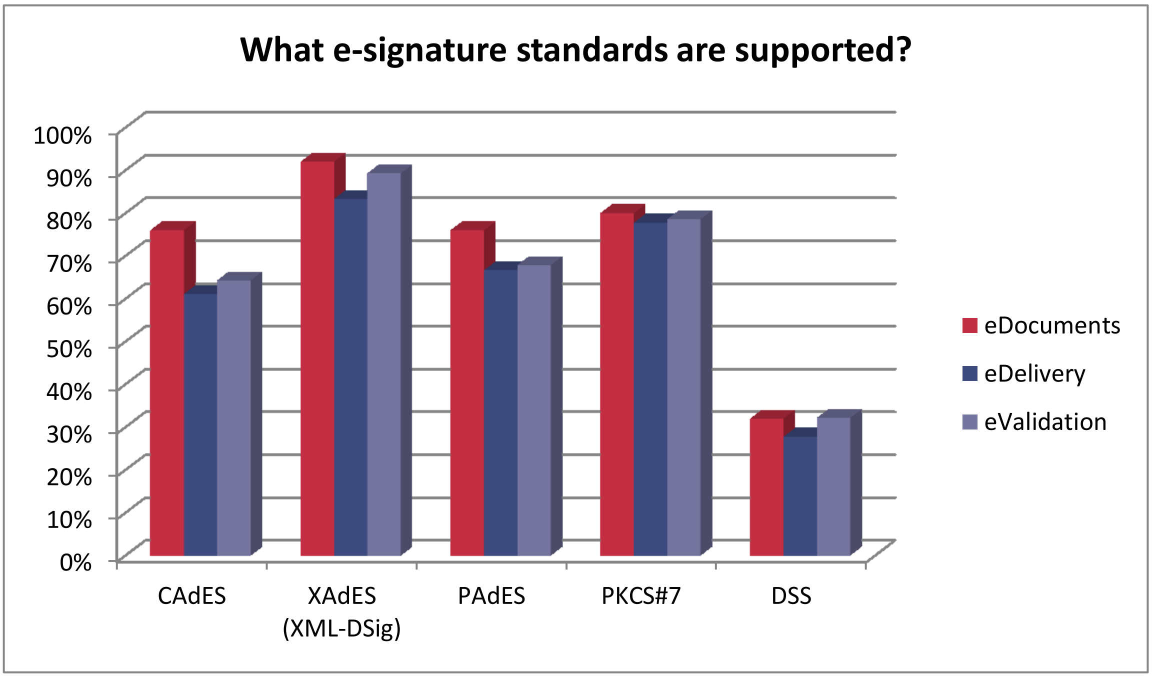


Figure 14: e-signature standards are supported

‘*XAdES*‘ is the most supported standard in all services: between 80-90%.

All services have the same series of standards supported with a similar ratio of coverage: ‘*XAdES*’ being the most supported one with 80-90% ratios, followed by ‘*PKCS#7*’, ‘*PAdES*’ and ‘*CAdES*’ with a similar percentage, and finally ‘*DSS*’ with the least support with 25-30%.

Regardless of the standard, the eDocuments service shows the highest level of support, followed by the eValidation and the eDelivery service. In order to improve interoperability, all TSPs should be able to accpet any e-signature standard.

4.3 Electronic time stamp services

4.3.1 Main time source

Thechart in Figure 15 shows the main time source used by the TSP for delivering the service, with a expected low rate for the Self-generated" time source.

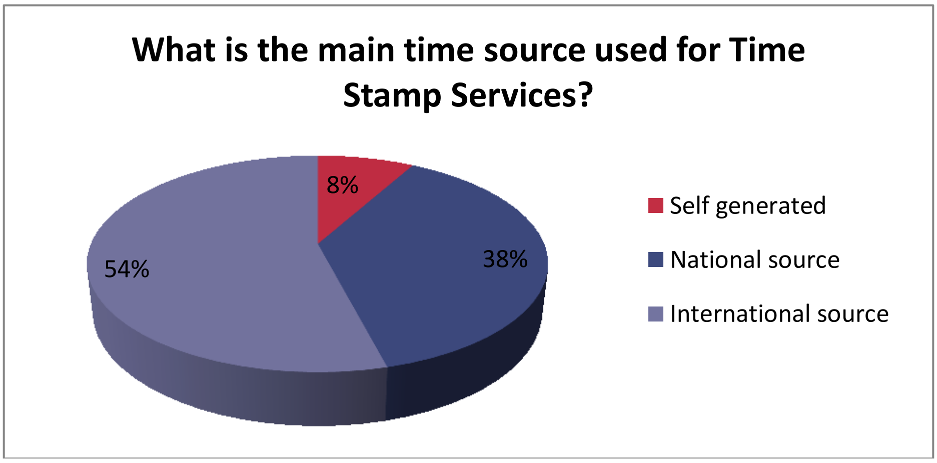


Figure 15: Main time source used for Time Stamp Services

4.3.2 Time stamp format standards

As for the Time Stamp format standards supported by the TSP (See Figure 16) for delivering the service, all of them support the '*RFC3161 Time Stamp Protocol*', whilst only 25% of TSPs support the '*DSS XML Time Stamp profile*'.

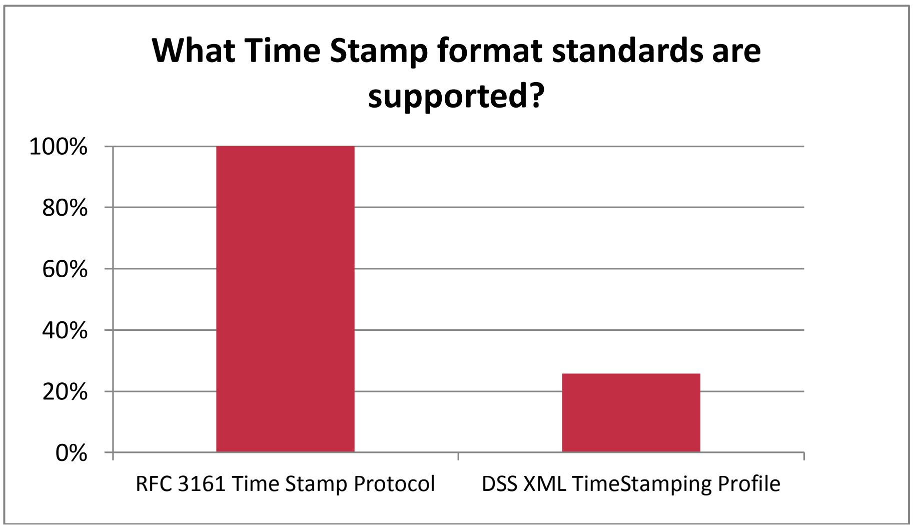


Figure 16: Time Stamp format standards supported

4.4 Validation services

Almost all TSPs support the '*OCSP*' and '*CRL*' protocols as certificate validation standards (See Figure 17), so interoperability is guaranteed in more than 90% of the cases, but it would be good to work towards the achievement of the 100%, through the adoption of both standards by all providers.

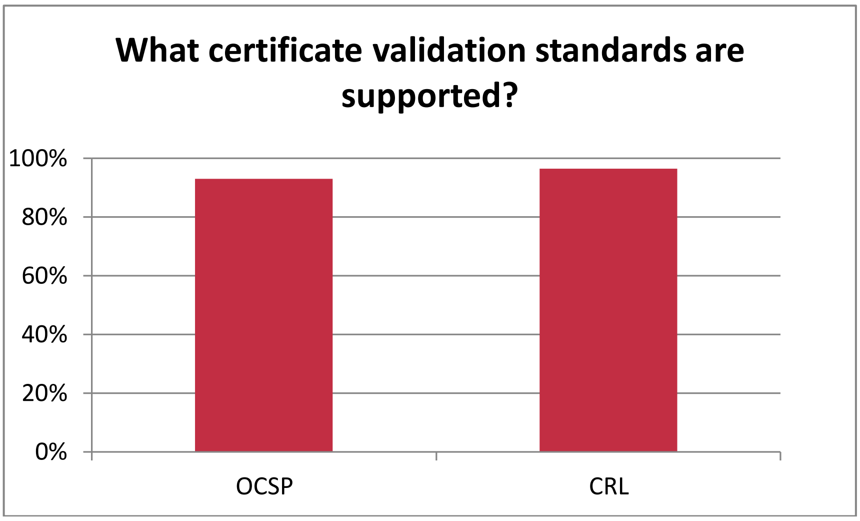


Figure 17: Certificate Validation standards supported

4.5 Long Time Preservation standards

Thegraphic in Figure 18 explains long term preservation standards. There is a dispersion of the standards used:

80% of the TSPs use '*AdES T*' standard which adds a time stamp, probably used for digital evidences storage purposes.

75% of the TSPs use '*AdES XL*' standard which adds CRLs and certificates, probably to allow future validations.

65% of the TSPs use '*AdES A*' standard which implies re-signing processes, probably for long time preservation of e-documents purposes.

The least used standards are 'AdES C' (which adds references to certificates and/or CRLs) and 'AdES X' (which adds time stamps to the references of 'AdES C'). It is remarkable, as AdES C is the format that adds the lightest information overhead. Nevertheless, with the risk 'Relay on not-update certificate revocation information' for Long Time Preservation Services deemed as almost negligible, it is just natural that AdES XL is the most widely used for this particular type of service.

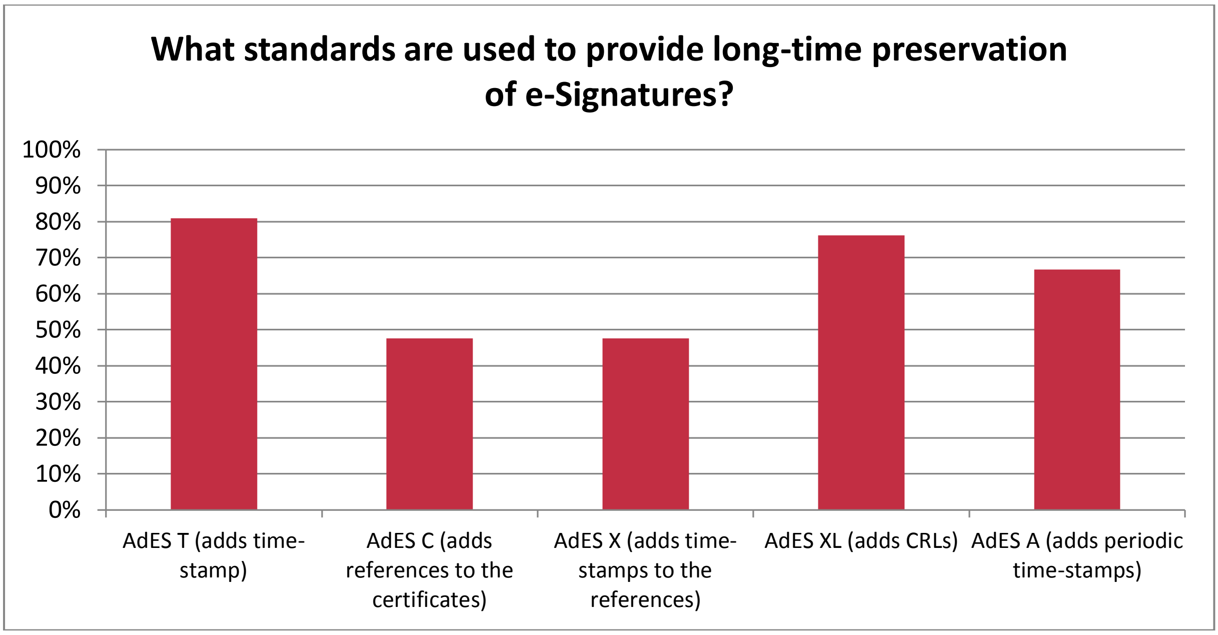


Figure 18: Long-Time Preservation e-singature standards implemented

5 Risk Analysis

This section reflects the results about the type of risks that can compromise the services according to the experience of the TSPs. The analysis has been made for the 'type of risk' point of view in section 5.1; and looking inside 'each service' in section 5.2.

Table 2: Quantitative and qualitative risk values and parameters relative values. Shows on the leftmost columns the average absolute Risk value and the typical deviation of the Risk calculated for each of the responses. This absolute Risk value is the result of applying a weight to the qualitative probability[47] and impact[48] values selected in the answers, and multiplying them. In a traditional qualitative risk analysis, those values should be considered as euros of expected loss due to probability of successful threat with the expected impact, but since each organisation should have their own probability and most important impact estimations in their particular environment, the numbers are provided just for comparing the results of one risk with others.

The Deviation has been calculated using the Standard Deviation of the values obtained. In the worst cases the highest values of the deviation, compared with the risk, show that some answers indicated relatively low risk and others very high risk. The conclusion of this large deviation of values is that the environments set up to provide the services are very different, and for this reason the values of the Risk for those vulnerabilities should be analysed with care. On the contrary, when the standard deviation is low, we should feel confident that most of the participants agreed on the estimation of that Risk.

To consolidate the responses given to each type of risk for each service, different calculations have been made, but toto simplify the results, all the values have been translated / normalized to scales from 0 to 100, being 100 the worst case[49].

Four parameters have been analysed, the lowest values are marked in green, showing that they are well protected, and the highest in Red, highlighting that they need improvement:

- Impact: It is calculated as the average of all individual impact responses and normalized to 0-100.
- Probability: It is calculated as the average of all individual probability responses and normalized to 0-100.
- Risk: It is calculated as the average of all the individual risks calculated from the values provided by the participants in the survey and normalized to 0-100. Each individual risk value was previously calculated as the product of the individual impact and the individual probability
- Standard Deviation: Statistical parameter alculated of the Risk values extracted from the answers of each participant in the survey for every type of risk and service. In general, the higher Standard deviations (highlighted in orange) corresponds to the higher risk, and those to the higher probability values.

[47] % ranging from very unlikely (1 every 30 years) to Frequent (3 times/year)

[48] ranging from very low (2K€) to very high (300K€)

[49] From the survey, all the risks have been in general been rated with Medium values (100% only means the worst between all of them). Normalization to 100 provides the spread of the results allowing an easier comparison of results and the identification of areas of improvement. .

Quantitative			Qualitative			
Deviat.	Risk value	Type of Risk	Risk value	Impact value	Prob. value	Deviation
25533	22924	Relay on not-updated certificate revocation information / **eVal.**	100	59	95	94
18709	22546	The evolution of cryptography / **LTP**	98	57	99	70
16732	18015	Unavailability of service / **eVal.**	79	41	80	78
17166	17098	Unavailability of service / **eDoc.**	75	28	100	85
14219	15212	Web site / web service impersonation / **eDoc.**	66	54	64	79
13647	14373	Lose or alteration of evidences in chain of trust / **eDoc.**	63	49	53	80
13831	14005	End user impersonation / **eDoc.**	61	57	55	83
15551	13348	Compromise of the main time source / **TS**	58	51	47	98
12270	13189	Sender or Receiver impersonation / **eDel.**	58	55	43	79
13975	11810	Unavailability of the main time source / **TS**	52	37	63	100
7280	10889	Relay on not-updated certificate revocation information / **LTP**	47	45	60	57
11994	10820	Lose of accuracy of the main time source / **TS**	47	37	60	94
7610	10025	Lose or alteration of evidences in chain of trust / **LTP**	44	49	44	64
9545	9812	Web site / web service impersonation / **eDel.**	43	45	35	82
6959	9681	Lose or compromise of service's signature creation data / **eDoc.**	42	81	31	61
5299	9231	Lose or alteration of digital evidences / **eDel.**	40	64	50	49
4388	8995	Lose or compromise of service's signature creation data / **LTP**	39	90	28	41
4907	8806	Lose or alteration of digital evidences / **LTP**	38	63	41	47
6044	8598	Lose or compromise of service's signature creation data / **TS**	38	100	22	59
6723	8413	Lose or alteration of evidences in chain of trust / **TS**	37	51	39	68
5804	8077	Relay on not-updated certificate revocation information / **eDel.**	35	48	43	61
5060	7828	Lose or alteration of digital evidences / **eDoc.**	34	69	53	55
7634	7824	Unavailability of service / **eDel.**	34	25	64	82
5055	7612	Relay on not-updated certificate revocation information / **eDoc.**	33	42	50	56
4984	6964	Lose or compromise of service's signature creation data / **eDel.**	30	91	18	60

Table 2: Quantitative and qualitative risk values and parameters relative values.

Figure 19 shows the general results obtained (ordered by Risk Value).

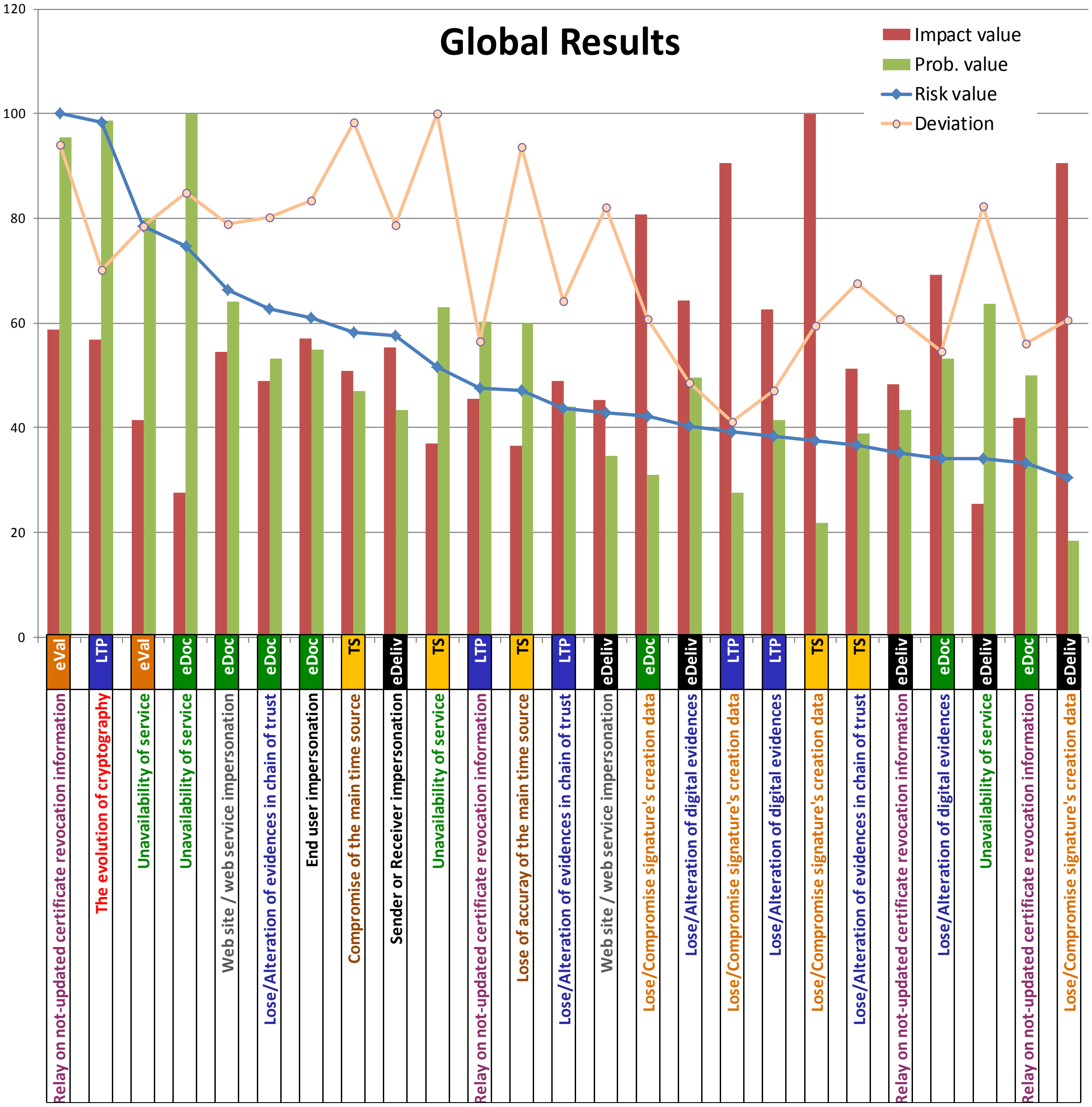


Figure 19: Qualitative risk and parameters values. The TSP is encoded in the shadowing colour of the boxes, and the threats of the same kind are encoded with the same font colour[50].

The graphic clearly shows that the risk values are largely affected by the threat probability assigned to them, with impact having a much lower correlation with the Risk. Regarding the relevance of

[50] This makes easier the comparison of results for the same service or type of threat, e.g. black shadow cells of eDelivery service or green font for "Unavailability of the service" threat.

Probability, Impact or both on the overall Risk associated to one threat or service, we can highlight the following cases:

- There are **three risks** cases which show a **higher** overall **value** compared to the rest:
  - 'The evolution of **cryptography'** which is specific for **Long Time Preservation** services. This risk is out of TSP's control because it is difficult to anticipate the evolution of the cryptographic algorithms.
  - 'The relay on not-updated **certificate revocation information**' in **eValidation** services. TSPs seem to have taken measures to minimize it because of the simultaneous use of OCSP and CRLs, but they still don't rely on the quality of the information, probably because it is produced out of their control.

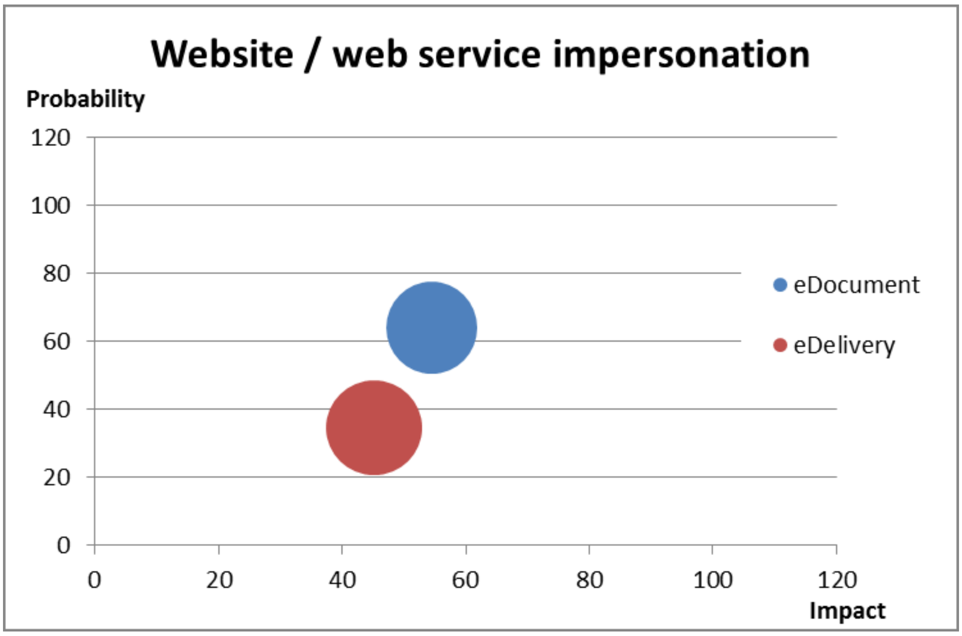
    This same risk has a significantly lower rate in the rest of services as Long Time Preservation or eDelivery, probably because these services are offered to customers close to the service provider, using credentials issued by them.
  - 'Web site / web service **impersonation**' (see section 5.1.1 below) for **eDocument related services** has also a high risk value because the combination of high impact and high probability.
- Other cases may be highilighted due to **large Impact** values:
  - The 4 cases with the **highest impact** (and also with the **lowest probabilities** values) correspond with the type of risk 'l**ose or compromise of service's signature creation data**' for the services eDocument, eDelivery, Time Stamping and Long Time Preservation. The highest impact is the expected answer because of the sensitivity of the data. The lowest probability shows that security measures have already been implemented.
  - The **lowest values for Impact** correspond to types of risk related to the '**main time source' in Time Stamp** and the type of risk of '**unavailability of service**' in eDocument and in **eDelivery** services.
- Other cases may be highilighted due to **large probability** values:
  - Two of the top 4 in **highest probabilities** are related to '**unavailability of service**' in **eDocument** services and in **eValidation** services**. Business continuity** management has to be promoted for this kind of providers (even if a cloud service provider is used).
  - '**Unavailability of service**' has a **high probability and a low impact** score in the 3 main services assessed. It is obvious that these services are more concerned with confidentiality and integrity than with availability.
- It is also worth to mention the cases with **higher deviation** values in the **Time Stamp** service: in the risks 'Compromise of the main time source' and 'Unavailability of the main time source' of the Time Stamp Services. This may be due to the **lack of uniformity** on the way those **services are provided**, and then, the differences on the quality of the tools used and the security mechanisms set in place, are the reasons of those deviations.

5.1 Overview of the risks

This section will analyse those risks that apply to 2 or more services in order to compare them.

A single graphic will be used to represent the values obtained for both Probability and Impact, taking into account the deviation or dispersion of the answers (represented as the size of the bubbles: the larger the dispersion, the bigger the bubble size, indicating that the range of values of risk resulting from the answers is high). In the table below each graphic, the associated risk values are also shown and highlighted in **Red** or **Green** if they are one of the highest or lowest risk values identified in the general Table 2 above, and the higher deviations values are highlighted in **Orange**.

5.1.1 Web site / web service impersonation



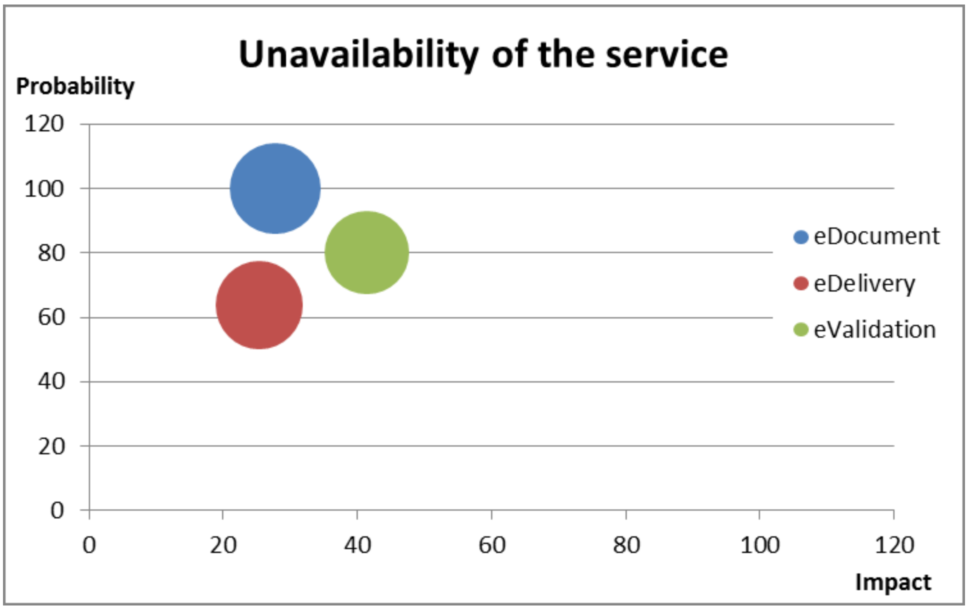
Web site / web service impersonation	eDocument	eDelivery
Risk Value	66	43
Impact Value	54	45
Probab. Value	64	35
Deviation value	79	82

Table 3: Web site / web service impersonation Risk

Table 3 shows that '*Web site / web service impersonation*' in eDocument Services rated a little bit higher in Probability and Impact than for eDelivery Services. The impact for eDocument service is higher because in some implementations of that service, the impersonation may lead with a higher probably to document content disclosure.

There is no correspondence with the fact of storing or not the managed eDocuments.

5.1.2 Unavailability of the service



Unavailability of service	eDocument	eDelivery	eValidation
Risk Value	**75**	**34**	**79**
Impact Value	**28**	**25**	41
Probab. Value	**100**	64	**80**
Deviation Value	85	82	78

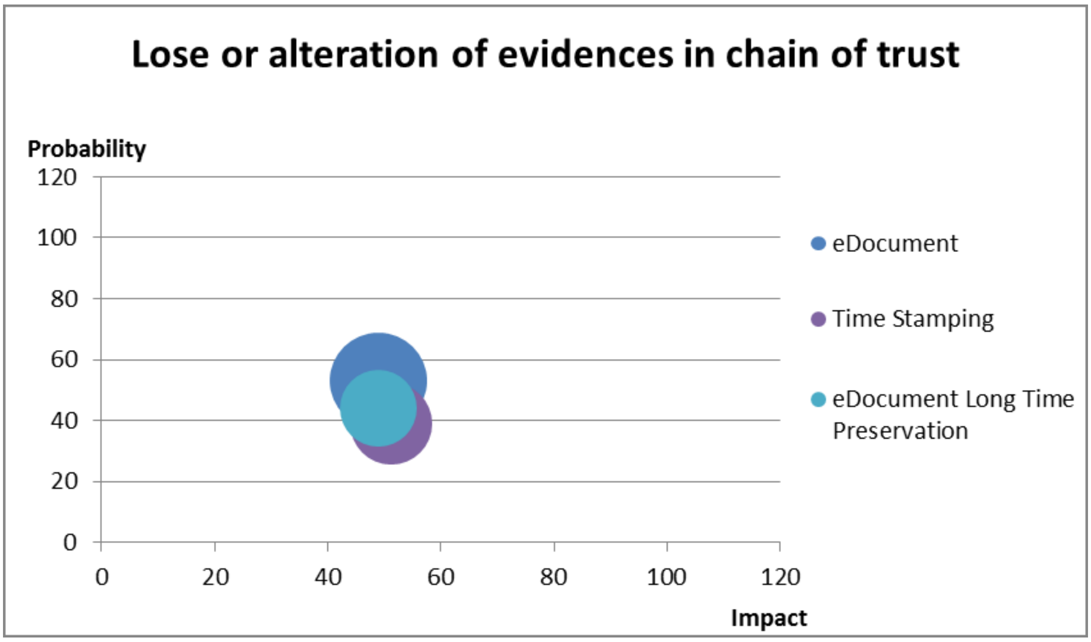
Table 4: Unavailability of service Risk

Table 4 shows that '*Unavailability of the service*' is a risk with the **high probability** of occurrence (in eDocument service) and **low impact** (especially in eDocument and eDelivery services).

The **low impact** perhaps is due to the fact that a denial of this kind of services doesn't imply any disclosure of documents; the relatively **high probability** may be a consequence of the limited application of business continuity plans; and the **high deviation** may be a result of the different types of implementations.

Risk value in eDelivery is significantly lower than risk value in eDocument and eValidation services.

5.1.3 Lose or alteration of evidences in chain of trust

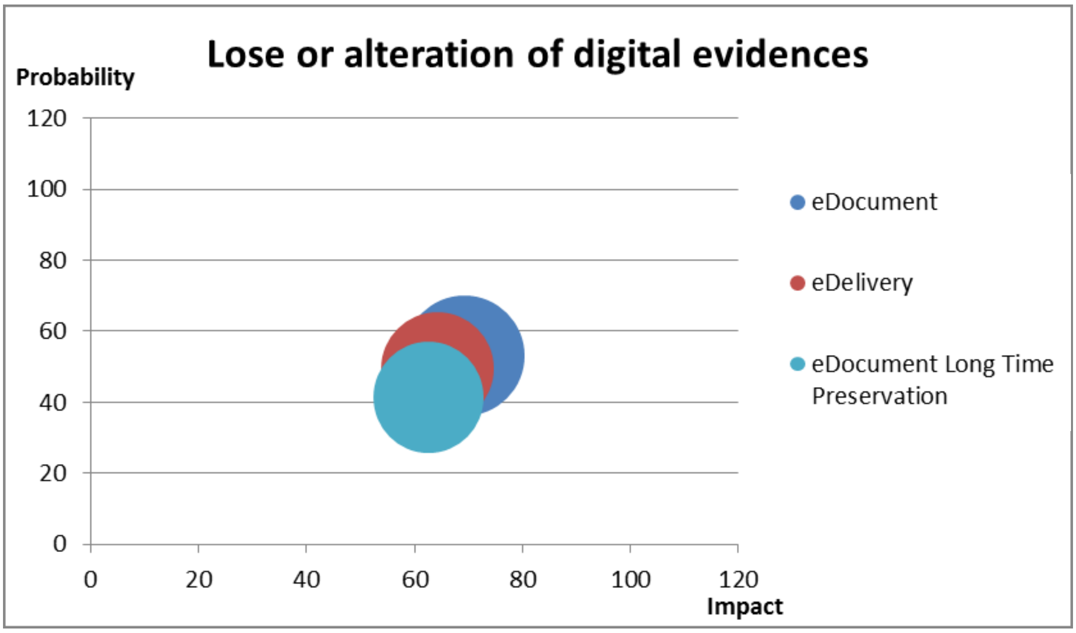


Lose or alteration of evidences in chain of trust	TimeStamp	eDocument	Long Time Preserv.
Risk Value	**37**	63	44
Impact Value	51	49	49
Probab. Value	39	53	44
Deviation Value	68	80	64

Table 5: Lose or alteration of evidences in chain of trust Risk

Table 5 shows that Risk values and parameters reported by the participants are almost the same for the different impacted services. The deviation value is relatively high for the e-Document related services, compared with the others, but this is due to the different kind of services provided under this category, and one of the reasons of recommending the definition of standard QoS profiles.

5.1.4 Lose or alteration of digital evidences

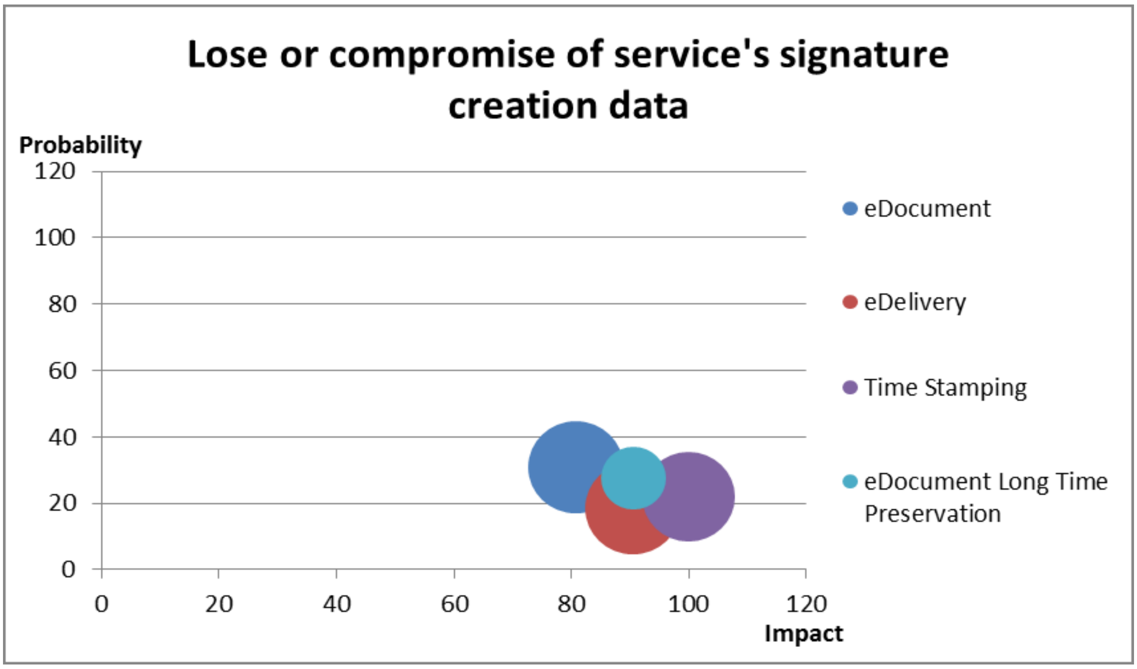


Lose or alteration of digital evidences	eDocument	eDelivery	Long Time Preserv.
Risk Value	34	40	38
Impact Value	69	64	63
Probab. Value	53	50	41
Deviation Value	55	49	47

Table 6: Lose or alteration of digital evidences Risk

Table 6 shows that Risk values and parameters reported by the participants are almost the same for the different impacted services.

5.1.5 Lose or compromise of service’s signature creation data

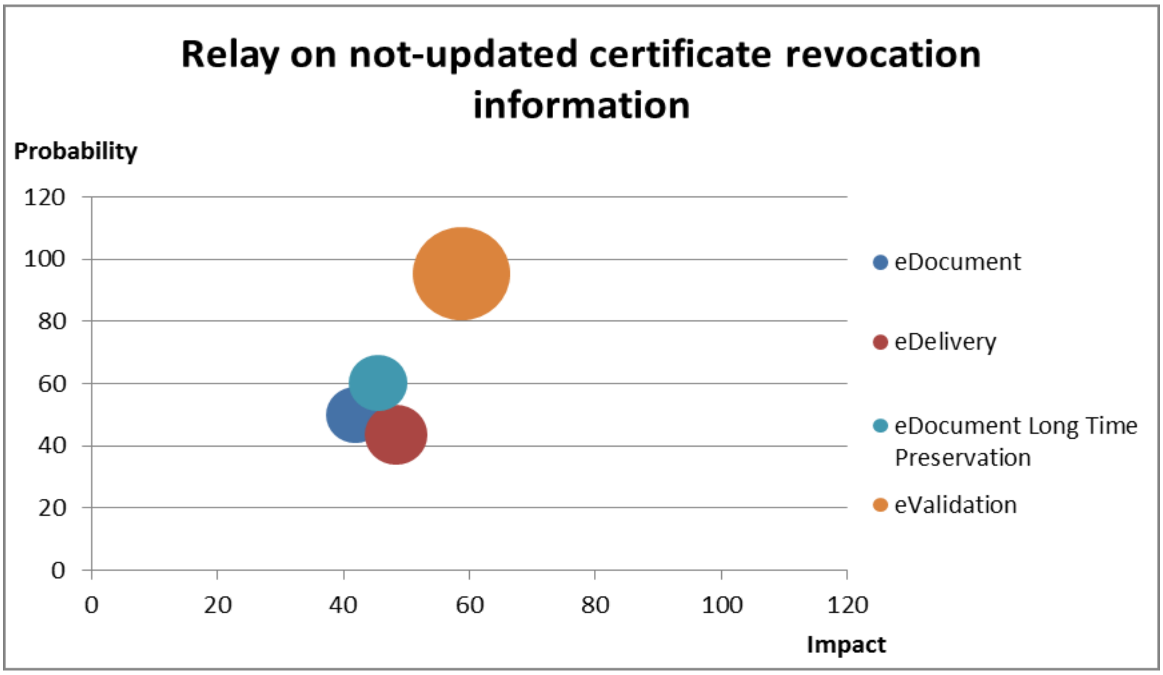


Lose or compromise of service’s signature creation data	TimeStamp	eDocument	eDelivery	Long Time Preserv.
Risk Value	38	42	**30**	39
Impact Value	**100**	**81**	**91**	**90**
Probab. Value	**22**	**31**	**18**	**28**
Deviation Value	59	61	60	41

Table 7: Lose or compromise of service’s signature creation data

Table 7 shows that ‘*Lose or compromise of service’s signature creation data*’ has been **unanimously** rated as the most striking risk for all the services (impact), but also as the most unlikely risk (because there are well established and known standards for its implementation, and they are frequently in place). Globally considered, the risk values are not very high.

5.1.6 Relay on non-updated certificate revocation information



Relay on not-updated certificate revocation information	eDocument	eDelivery	eValidation	Long Time Preserv.
Risk Value	33	35	100	47
Impact Value	42	48	59	45
Probab. Value	50	43	95	60
Deviation Value	56	61	94	57

Table 8: Relay on not-updated certificate revocation information Risk

Table 8 shows that this risk for eValidation Services has been rated as the highest one, and also with high probability. In the 2 extreme cases analyzed where they rated frequent or likely for this risk, they didn't rated so high for the rest of the risks. So these cases must be taken into account.

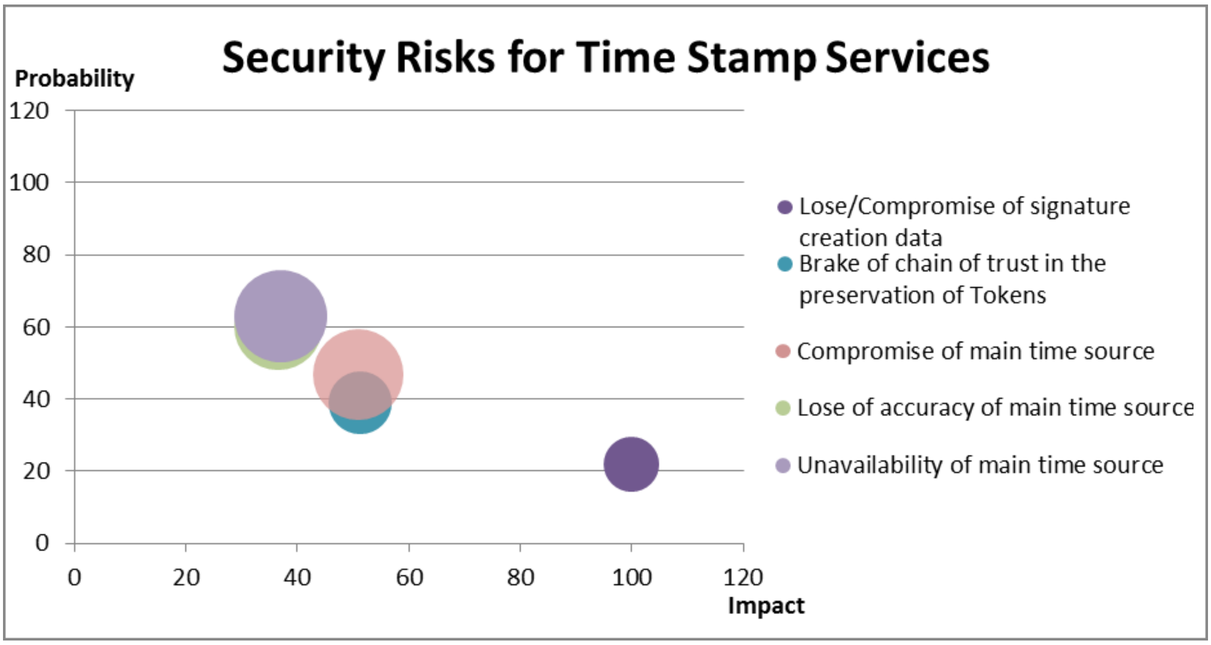
The TSPs seem to have been taken measures to minimize it: Almost all of them offer validation services through CRLs and OCSP simultaneously. So this is not the cause of high rate.

5.2 Overview of the services

This section will analyse the type of risks identified in each Service.

A graphic will be used to represent the values obtained for both Probability and Impact, taking into account the deviation or dispersion of the answers (represented as the size of the bubbles: the larger the dispersion, the bigger the size). In the table below the associated risk values are also shown and highlighted in **Red** or **Green** if they correspond to one of the highest or lowest risk values identified previously.

5.2.1 Electronic Time Stamp services



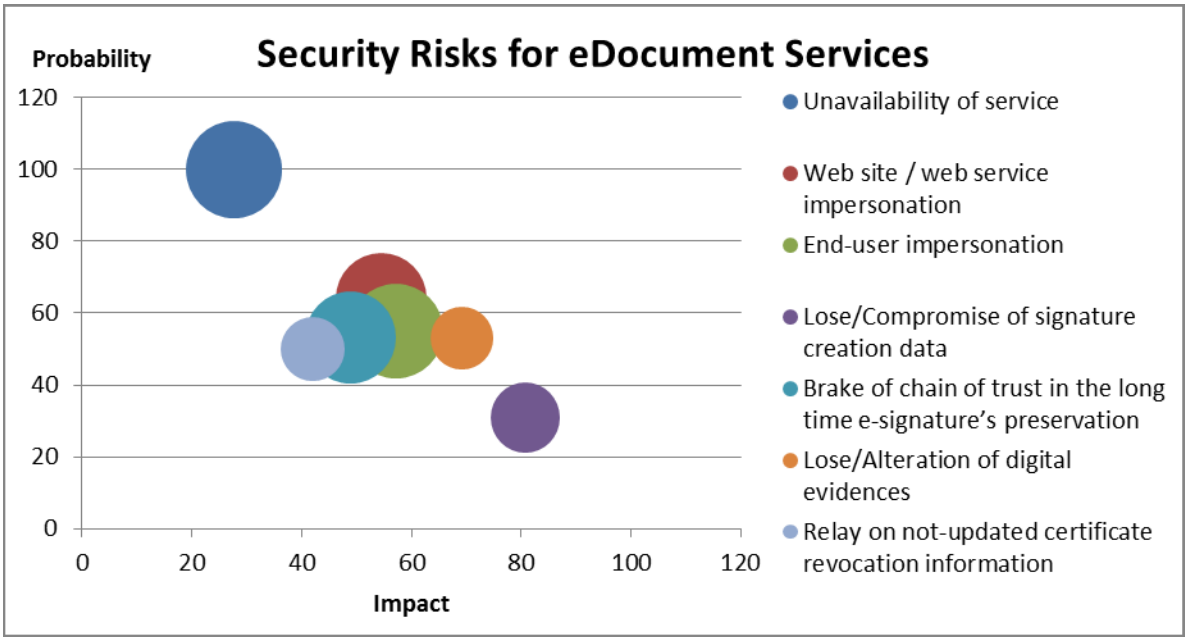
Type of Risk	Risk Value	Impact Value	Probab. Value	Deviat. Value
● Lose or compromise of service's signature creation data	38	100	22	59
● Lose or alteration of evidences in chain of trust	37	51	39	68
● Compromise of the main time source	58	51	47	98
● Lose of accuracy of the main time source	47	37	60	94
● Unavailability of the main time source	52	37	63	100

Table 9: Electronic Time Stamp services Risks

Table 9 shows that the large deviation of responses observed for the three risks related to the main time source are consequence of the different tools (different use of time sources) used by the TSPs and the security of their implementation.

Although the risks '*Lose of accuracy of the main time source*' and '*Unavailability of the main time source*" don't show a great impact, they have been rated as the most likely ones for 'time stamp services'.

5.2.2 eDocument services



Type of Risk	Risk Value	Impact Value	Probab. Value	Deviat. Value
● Unavailability of service	75	28	100	85
● Web site / web service impersonation	66	54	64	79
● End user impersonation	61	57	55	83
● Lose or compromise of service's signature creation data	42	81	31	61
● Lose or alteration of evidences in chain of trust	63	49	53	80
● Lose or alteration of digital evidences	34	69	53	55
● Relay on not-updated certificate revocation information	33	42	50	56

Table 10: e-Document Services Risks

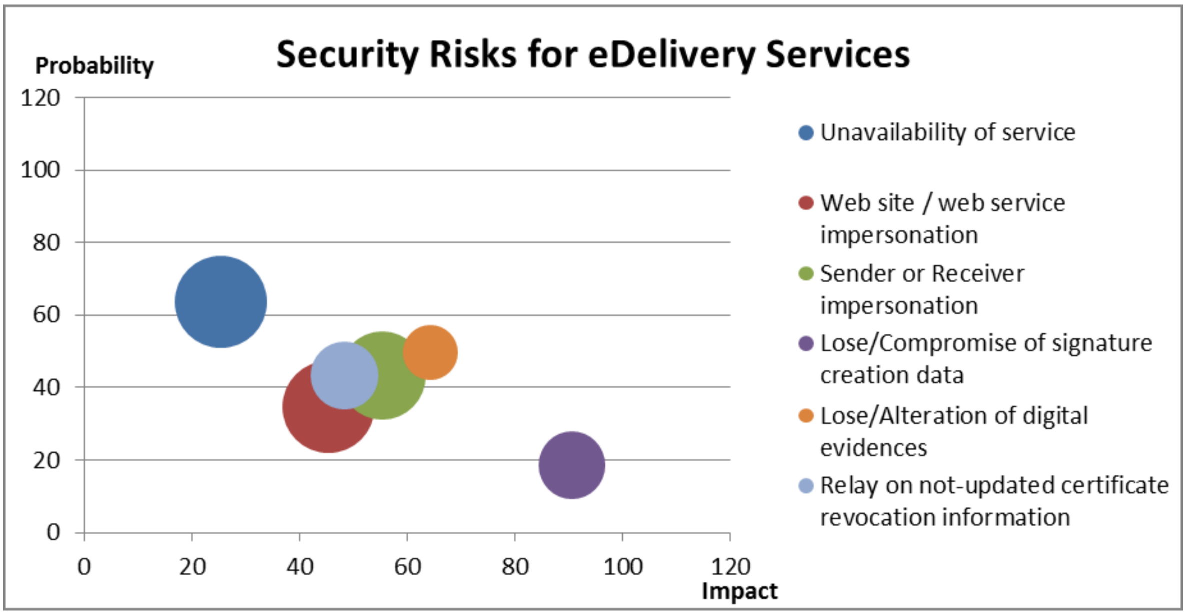
Table 10 shows that *'Unavailability of service'* has a **high probability** but also a high deviation. Nevertheless there is only one peak response for probability.

The highest risk responses are those of service providers that deliver the service only through a web, or that haven't audited it at all. In general the differences may be consequence of the different type of implementations.

None of them are following ISO27001 as a security management standard.

'Lose or alteration of digital evidences' and *'Relay on not-updated certificate revocation information'* have two of the lowest risk values overall.

5.2.3 eDelivery services



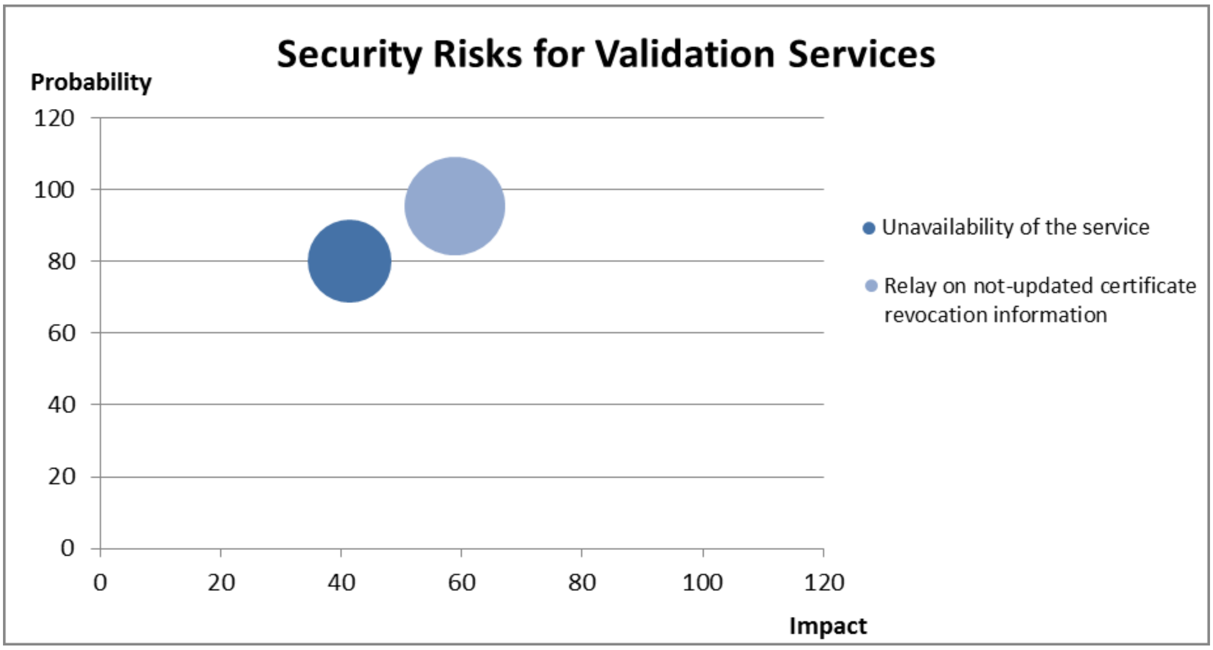
Type of Risk	Risk Value	Impact Value	Probab. Value	Deviat. Value
● Unavailability of service	34	25	64	82
● Web site / web service impersonation	43	45	35	82
● Sender or Receiver impersonation	58	55	43	79
● Lose or compromise of service's signature creation data	30	91	18	60
● Lose or alteration of digital evidences	40	64	50	49
● Relay on not-updated certificate revocation information	35	48	43	61

Table 11: e-Delivery Services Risks

Table 11 shows that '*Lose or compromise of service's signature creation data*' has been unanimously rated as the most striking risk but with a low probability.

The high deviation of values for some Risks is due to the different types of implementation of the service, since only some of them store the e-documents they deliver. It may also be a consequence of the different kinds of customers, as this service is provided to users that don't belong to the organization of the service provider.

5.2.4 Validation services

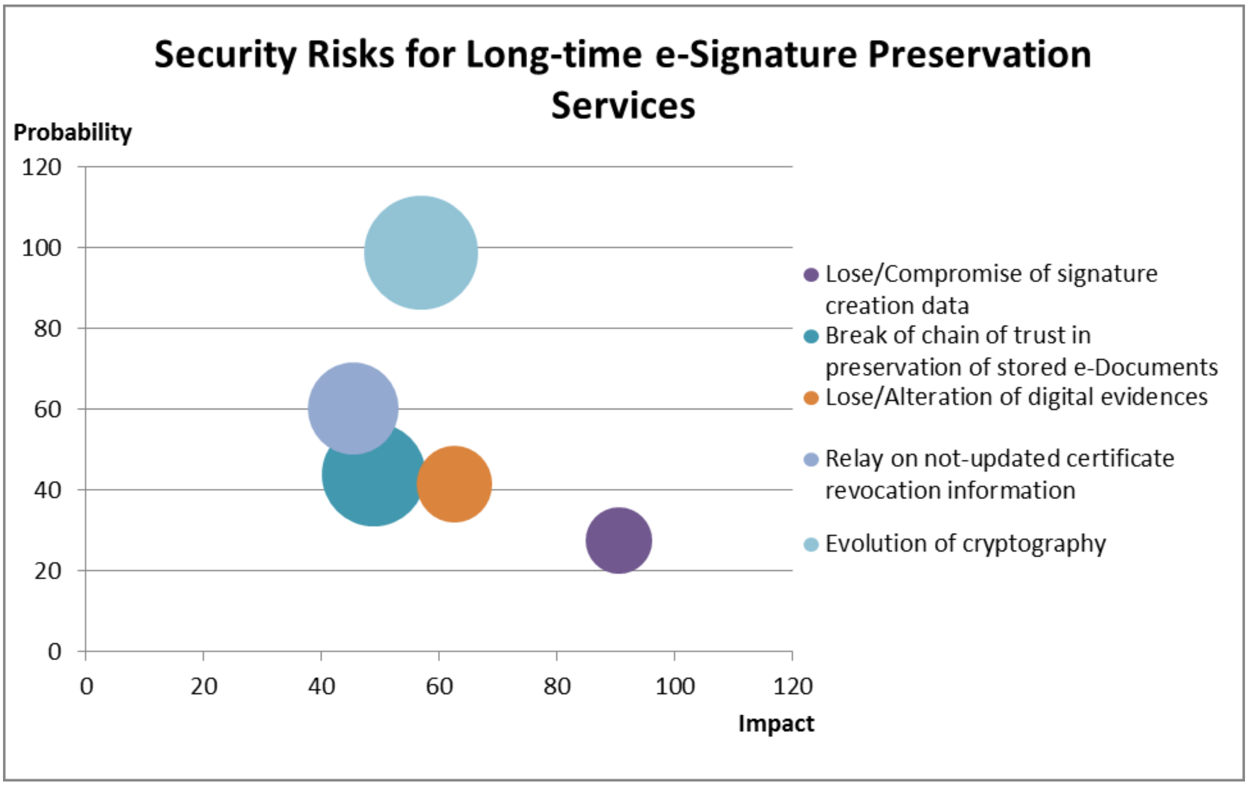


Type of Risk	Risk Value	Impact Value	Probab. Value	Deviat. Value
● Unavailability of service	**79**	41	**80**	78
● Relay on not-updated certificate revocation information	**100**	59	**95**	**94**

Table 12

Table 12 shows that both risks are considered as some of the most probable risks to materialise, with a high risk value also in the global overview. The dispersion of values given in the responses and the high probability show that there are no consolidated implementation guidelines and that this service needs guiding instructions and standardization work.

5.2.5 Long Time Preservation services



Type of Risk	Risk Value	Impact Value	Probab. Value	Deviat. Value
● Lose or compromise of service's signature creation data	39	90	28	41
● Lose or alteration of evidences in chain of trust	44	49	44	64
● Lose or alteration of digital evidences	38	63	41	47
● Relay on not-updated certificate revocation information	47	45	60	57
● The evolution of cryptography	98	57	99	70

Table 13: Long Time Preservation Services Risks

Table 13 shows that '*The evolution of cryptography*' has one of the **highest risk values (98)**. This is mainly due to a very **high probability** value (97). This type of risk is only evaluated in this service, so it cannot be compared with other services in the survey.

It is the risk out of control of any TSP, because it is complicated to anticipate what can happen in the future with the algorithms that are been used today.

Table 13 also shows that *'Lose or compromise of service's signature creation data'* has a high impact value and a low probability value.

6 Conclusions and Recommendations

The following section shows all the relevant conclusions extracted from the survey and the recommendations associated to them when apply. Recommendations have been numerated and categorized by the addressee of the recommendation: the Trust Service Providers (P), the Regulators/Supervisors/Standardising bodies (R) or the Customers of TSP (C).

6.1 Services scope

The vast majority of providers offer both *'electronic certificates'* and *'other trust services',* so they are already using CPS Certification schemas, so it is

[REC.1.R] recommended extending CSP Certification schemas to other Trust services and to the whole EU to have harmonised security audits[51] criteria of QoS and SLA guidelines.

Many TSP complain about the administrative barriers to be recognised and operate in different Member States, what in many cases deals not only in lack of interoperability, but also in difficulties to reach a critical mass of customers to make the services sustainable, without having to invest too much following regular audits on several national accreditation schemas. To overcome this problem the EU eIDAS Regulation proposes that a mutual assistance system between supervisory bodies in the Member States should be set up[52], e.g. cross-border or mutual recognition of accreditation schemas or independent auditing body. This could be facilitated through the following recommendation:

[REC.2. **P/R/C*]* It should be promoted the use of widely recognised Trust Marks based on** conformity assessment of qualified TSPs against eIDAS requirements that would be recognised across borders**.**

The scope of certificates supported by the TSPs in the trust services they provide is not very large (up to 37% support only their own CSPs; and up to 43% do not support international CSPs). Since e-signature is one of the strongest authentication mechanisms, and the eID associated to that e-signature can be recognised cross border in EU, following the eIDAS regulation, its use to grant access to TSPs has to be promoted. As the segmentation of the market is very high, to improve the current situation, so

[REC.3. R/C] Supervisors should promote a wider use of e-Signature as authentication mechanism to access TSPs, barriers for cross-border interoperability of e-Signature & eIDAS certificates have to be removed.

About the sectors the services are addressed to, some conclusions can be drawn:

- The provision for 'only general public' is residual. Almost all TSPs are providers of Public Administrations, Private sector or both.
- If we focus on Public vs. Private, most of them provide services to both sectors.
- Less than 50% TSPs address their services to specific communities.

[51] As stated in Art. 14.1 of eIDAS Regulation, making reference to Articles 15, 16 and 17.
[52] As recommended in the whereas 34 of the new Regulation.

Regarding the authentication mechanisms to grant access to their services, although almost all of them provide them with electronic certificates, there is a variety of mechanisms used. So the strength of the authentication mechanisms used should be proportional to the criticality of the accessed services.

The Trust Services are usually provided by an 'on-line TSP web site' (almost 80% of the TSPs), followed by a 'web services available for automatic processing' (almost 60% of the TSPs), and 'a client application' (roughly 40% of the TSPs). Although an on-line web site service is the most preferred platform, it is worth to recommend the use of clients based on SAML web services end-to-end encrypted communication to handle the communication. This approach will allow also the use of end to end encryption between client and server in a way transparent to the user, avoiding changes on the configuration that may have a negative impact on the security of the data being transferred.

[REC.4.P/R/C] Promote the implementation of client desktop applications to be executed in the customer computer using web-service access to TSP with end-to-end encryption in the communication between them.

Finally, for the 'eDocuments' supporting services, the percentage of providers storing documents is higher (76%) than for the 'eDelivering' service (42%), due to the nature of the service. The storing or not storing of documents impacts directly in their security, so the description of the service whould include those kind of details, and the security measures in place to prevent the threats to which the service is vulnerable, based on the way it's provided. In order to facilitate the customers, e-government and others, to recognise some standard service quality and levels it's recommended to:

[REC.5.P/R] Define adequate service profiles based on best practices that comply with users' expected QoS and allow comparison.

6.2 Standards implemented

Nearly 90% of the participants indicated that they follow ISO/IEC 27001, but a very low percentage has adopted others. It is worth mentioning the lack of implementation of IT Security Governance standards and that only 12% of TSPs implemented the Bussiness Continuity Management (BCM) standard ISO/IEC 22301, which has proven to be related with one of the most relevant risks of the trust service providers.

In order to address risks related with the unavailability of the services specific BCM standards, as ISO/IEC 22301 should be promoted, but keeping in mind the suitability of the use of non-specific international standards as ETSI 101 456 or EN 319 411-2 which include BCM controls on their requirements, so it could also be acceptable the use of TSP especific standards including BCM controls.

[REC.6.P/R/C] The implementation of Bussiness Continuity Management standards applied to the service as a whole should be promoted. TSP specific standards, including BCM controls could also be acceptable.

The most supported e-signature standard is 'XAdES' (80-90%) and the least supported one is DSS (25-30%). In the middle range are 'PKCS#7', 'PAdES' and 'CAdES' with similar high end percentages. Although almost all the e-signature standards are highly supported, in order to be capable to validate any of them,

[REC.7.P/C] full adoption of e-signature standards by TSPs should be reached, to achieve full interoperability.

Regarding Time Stamp services, there is a low percentage of TSP that use of a 'self-generated' time source, which could facilitate internal threats, being the international source the most adopted one. Nevertheless, it is still worth to:

[REC.8.P/C] It's recommended to promote the use of national or internationally trusted time sources, taking such policy into consideration for the specification of a qualified service.

As for Validation services, almost all TSPs support the 'OCSP' and 'CRL' protocols.

Finally, regarding Long Time Preservation of e-Signatures standards, the dispersion of standards used is high, which implies that

[REC.9.P/R/C] best practices must be defined to harmonise the quality and functionality of the Long Time Preservation service (QoS & SLA).

6.3 Risk Analysis

We can summarise the Risk Analysis made in section 1 above, highlighting some issues and the corresponding recommendations to minimise them:

- There are three risks cases which show a higher overall value compared to the rest:
  - 'The evolution of cryptography' which is specific for Long Time Preservation services. This risk is out of TSP's control because it is difficult to anticipate the evolution of the cryptographic algorithms. To try to mitigate this risk

    [REC.10.P/C] the use of two hash algorithms in Long Time Preservation services is recommended to protect the integrity of the e-Signatures; breaking both algorithms at the same time is less probable.
  - 'The relay on not-updated certificate revocation information' in eValidation services. TSPs seem to have taken measures to minimize it because of the simultaneous use of OCSP and CRLs, but they still don't rely on the quality of the information, probably because it is produced out of their control. It is

    [REC.11. P/C] recommended to guarantee the quality of the certificate revocation service to allow the eValidation service trusts more on them.

    This same risk has a significantly lower rate in the rest of services as Long Time Preservation or eDelivery, probably because these services are offered to customers close to the service provider, using credentials issued by them.
  - 'Web site / web service impersonation' (see section 5.1.1 above) for eDocument services has also a high risk value because the combination of high impact and high probability. To mitigate this type of risk, it is proposed a *combination of recommendations*:

    [REC.12. P/C] There should be a focus on user training and consciousness of threats to prevent web site / web service impersonation.

    For example, using messages remembering users about security best practices in storing credentials.

    And one already mentioned:

    [REC.4.P/R/C] Promote the implementation of client desktop applications to be executed in the customer computer using web-service access to TSP with end to end encryption in the communication between them..

- About deviation values:
  - The large deviation of responses in the risks ‘Compromise of the main time source’ and ‘Unavailability of the main time source’ of the Time Stamp Services. This may be due to the lack of uniformity on the way those services are provided, and then, the differences on the quality of the tools used and the security mechanisms set in place, are the reasons of those deviations. Two already mentioned recommendations may solve this problem:
  - ***[REC.8.P/C] it’s recommended to promote the use of national or international trusted time sources, taking such policy into consideration for the specification of a qualified service.***

    and
  - ***[REC.9.P/R/C] best practices must be defined to harmonise the quality and functionality of the Long Time Preservation service (QoS & SLA).***

6.4 Summary of Recommendations

This section summarizes the actors to which the recommendations are more relevant (X), the table also indicates which of the actors will have more responsibility (R) on the adoption or imposition of the recommendation: the Trust Service Providers (P), the Regulators (R) and the of TSP (C). In some cases the Cusomer column has been marked with (V), meaning that the customer is encouraged just to Validate that the TSP is providing the service following the recommendation.

RECOMMENDATION	TSP	Reg/ Stndr	Customer
[REC.1.R] It is recommended **extending CSP Certification schemas** to other TSP services and to the whole EU to have harmonised security audits criteria of QoS and SLA guidelines.		**R**	
[REC.2. P/R/C*]* It should be promoted the and use of **widely recognised Trust Marks**based on conformity assessment of qualified TSPs against eIDAS requirements that would be recognised across borders.	X	**R**	V
[REC.3.R/C] Supervisors should **promote a wider use of e-Signature** as authentication mechanism to access TSPs, **barriers for cross-border interoperability** of e-Signature & eIDAS certificates have to be removed.		**R**	V
[REC.4.P/R/C] Promote the implementation of **client desktop** applications to be executed in the customer computer with web-service access to TSP with end to end encryption in the communication between them.	**R**	X	X
[REC.5.P/R] Define adequate **service profiles** based on best practices that comply with users' expected QoS.	X	**R**	V
[REC.6.P/R/C] **BCM standards** (ISO 22301) applied to the service as a whole should be promoted. TSPspecific standards including BCM controls could also be acceptable.	X	**R**	V
[REC.7.P/C] **Full adoption of e-signature** standards by TSPs should be reached, to achieve full interoperability.	**R**		X
[REC.8.P/C] Use of national or internationally **trusted time sources**, taking such policy into consideration for the specification of a qualified service.	**R**		V
[REC.9.P/R/C] best practices must be defined to harmonise the quality and functionality of the Long Time Preservation service (**QoS & SLA**).	X	**R**	V
[REC.10.P/C] Use of **two hash algorithms** in LTP services is recommended to protect the integrity of the e-Signatures.	**R**		V
[REC.11.P/C] To guarantee the quality of the certificate **revocation service** to allow the eValidation service trusts more on them.	**R**		V
[REC.12.P/C] There should be a focus on user **training and consciousness** of threats to prevent web site / web service **impersonation**.	**R**		X

Table 14: Summary of recommendations with Stakeholder category relevance.

7 Annex I: Acronyms

ASIC-S	Simple Associated Signature Container, published by ETSI as TS 102 918
BCM	Business Continuity Management
CA	Certification Authority
CAdES	CMS Advanced Electronic Signatures , published by ETSI as TS 101 733
CEN	European Committee for Standardization
CEN BII	CEN Workshop on 'Business Interoperability Interfaces"
CRL	Certificate Revocation List, see “RFC 5280”
DG	Directorate General
DPA	Data Protection Authority
DSS	OASIS Digital Signature Services
EC	European Commission
e-CODEX	e-Justice Communication via Online Data Exchange
eID	Electronic Identification
eGov	e-Government
eIDAS	electronic Identification and Authentication Service
ENISA	European Union Agency for Network and Information Security
epSOS	Smart Open Services for European Patients
eSign	electronic Signature
ETSI	European Telecommunications Standards Institute
ETSI TS	ETSI Technical Specification
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Standards Organisation
IT	Information Technology
LSP	Large Scale Pilots
MS	Member State
NCP	National Contact Point
NIS	Network and Information Security
NRA	National Regulator Authorities
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol, see “RFC 2560”
PAdES	PDF Advanced Electronic Signature, published by ETSI as TS 102 778
PEPPOL	Pan-European Public Procurement Online
PKI	Public Key Infrastructure
PoC	Point of Contact
QoS	Quality of Service
REC	Recommendation
SAML	Security Assertion Markup Language
SHA	Secure Hash Algorithm.
SLA	Service Level Agreement

SML	Service Metadata Locator
SMPs	Service Metadata Publishers
SP	Service Provider
STORK	Secure *IdenTity* AcroSs BoRders LinKed project
TS	Trusted Service
TSL	Trust-Service Status List, published by ETSI as TS 102 231
TSP	Trust Service Provider
TTP	Trusted Third Party
URL	Uniform Resource Locator
USB	Universal Serial Bus
USD	United States Dollar
XAdES	XML Advanced Electronic Signature, published by ETSI as 101 903
XKMS	XML Key Management Specification
XML	eXtended Markup Language

8 Annex II: Launch of the Survey on Trust Services in the EU

The following survey is intended for Trust Service Providers (TSPs) in the EU. The survey explores security mechanisms used by TSPs, and their interoperability. The results will be incorporated as part of a future ENISA report.

The results will be collected anonymously. However, if you wish so, your organization name may appear in the acknowledgements section in the final report.

Your contact data are optional and will only be used for future ENISA communications *.

Please note that questions with a red mark are mandatory questions. Completing the questionnaire should take you between 10 and 30 minutes (this will depend on the number of trust services your organization provides).

Should you have any doubts or need for any further assistance, please don't hesitate to contact us at: sta@enisa.europa.eu

Thanks in advance for your cooperation.

*** All personal data shall be processed in accordance with Community Regulation (EC) No 45/2001 of the European Parliament and of the Council (OJ L8 of 12.01.2001, p1) on the protection of individuals with regard to the processing of personal data by the Community Institutions and bodies and on the free movement of such data, accessible here [Link].**

General Information

Organization Name:

Country where you are operating *:

Contact Person:

Contact E-mail:

Contact Telephone:

Would you like your organization to appear in the acknowledgements of the final reports?

YES/NO

Which of the trust services described in the proposed trust services Regulation do you provide or intend to provide in the future? *

Please, include both qualified and non-qualified services. For the future, please make an estimation (about 3 to 5 years). See here the proposed Trust Service Regulation [link]

Electronic certificates (For electronic signatures, seals, web site authentication, etc.)

Other trust services (Time-Stamping,e-Signed Documents,e-Documents Delivery, Certificate or e-Signed Document Validation,Long-time preservation)

Which general security management standards do you follow?

ISO/IEC 27001 (Information Security Management)

ISO/IEC 22301 (Business Continuity Management)

ISO/IEC 38500 (IT Governance)

Others

To which sectors do you address your services?

General Public

Public Administrations

Private sector

Specific community

Is your organization regularly audited?

Yes, within the scope of a government audit scheme

Yes, whitin the scope of an independent / industry led audit scheme

Yes, within both

Yes, internal audit / self-assessment

No

In case you answered yes, please specify the periodicity of audits (in months):

Do you have an approved document for:

Certification Practice Statement

Information Security Policy

Job descriptions for Trusted Roles

Inventory of Assets

Business Risk Assessment

Bussiness Continuity Plan

Incident Response Plan

CA Termination Plan

Questions for Certification Services Providers

What type of electronic certificates do you provide?

Electronic certificates for individuals

Electronic certificates for legal entities

Website authentication certificates

Others (Please specify):

Do you provide qualified certificates (in accordance with Directive 1993/99) ?

Yes, only qualified certificates

Yes, both qualified and non qualified certificates

No, only non qualified certificates

Which standards / technical specifications do you follow for the security of the certification lifecycle management?

ETSI TS 101 456 Policy Requirements for Certification Authorities issuing qualified certificates

ETSI TS 101 042 Policy Requirements for Certification Authorities issuing public key certificates

RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

CWA 14167 Security requirements for trustworthy systems managing certificates for electronic signatures

Others (Please specify):

Which media/s do you use to store the subjects' private key?

Smart card (Cryptographic device)

Soft token (Memory device)

Software

Others (Please specify):

Are the cryptographic devices that you use certified against any certification scheme?

Question	FIPS certified	CC (EAL) certified	Other certification	No certification
The Hardware Security Modules (HSMs)				
The subjects' devices (where cryptographic operations are performed)				

If you choose other certification scheme, please specify:

Which public key cryptographic algorithm do you use?

	RSA-1024	RSA-2048	RSA-4096	ECC-256	Other
For the Root CAs					
For the subjects' keys					

If you chose other, please specify:

Which hash algorithm do you use?

	SHA-1	SHA-256	SHA-384	RIPEMD-160	Other
For the Root CAs					
For the subjects' keys					

If you chose other, please specify:

Which types of attacks do you think are most likely to affect a certification service provider?

Please rate from 1 (less probable) to 4 (most probable)

	1	2	3	4

Logical attacks				
Cryptographic attacks				
Physical attacks				
Insider attacks				

Below you can find a list of common security risks for certification service providers. Please rate in terms of your perceived:

Impact for the organization

	Very low	Low	Medium	High	Very high
Compromise of the Certificate Authority					
Compromise of a Registration Authority					
Compromise of a Subject's Certificate					
Compromise of the Revocation Services					
Compromise of the Cryptographic Algorithms					
Impersonation					
Repudiation Claim by Certificate Subject					
Accidental Loss of Availability of the Certification Services					
Personal Data Breach					

Probability of occurrence

	Very unlikely	Unlikely	Possible	Likely	Frequent
Compromise of the Certificate Authority					
Compromise of a Registration Authority					
Compromise of a Subject's Certificate					
Compromise of the Revocation Services					

Compromise of the Cryptographic Algorithms					
Impersonation					
Repudiation Claim by Certificate Subject					
Accidental Loss of Availability of the Certification Services					
Personal Data Breach					

If you believe there are other critical risks for certification service providers not included in the list, please add them here:

What is the maximum latency you guarantee for including the revocation of a certificate in your certificate database after such revocation has taken effect?

< 5min

< 15min

< 1h

< 5h

< 1day

Other, please specify:

General Questions for other trust services (e.g. e-sign documents, long time preservation, signature validation)

Which other trust services do you provide or intend to provide in the future?

Electronic time stamps

e-Signed documents storage or management

e-Documents delivery services

e-Signed documents signature validation

Long-time preservation of e-Signed Documents

What certificates do you support?

Support certificates only of your own / associated CSP

Support certificates of several CSPs in your country

Support certificates of any CSP of your country

Support certificates of CSPs of some EU Countries

Support certificates of any CSP of any EU Country

What e-signature standards are supported?

CAdES

XAdES (XML-DSig)

PAdES

PKCS#7

DSS

Other

Which authentication mechanism do you use to grant access to your services?

No need for credentials

User & password or similar

Authentication with electronic certificate

Other

Time-Stamping

How is the Time-Stamping service provided? (select all that apply)

Through a client (desktop) application

Through a web site (on-line) service of your own

Through a e-Government web site

Through a web service available for automatic processing (e.g. e-invoicing)

What is the main time source?

Self generated

National source

International source

What TimeStamping format standards are supported? (select all that apply)

RFC 3161 Time Stamp Protocol

DSS XML TimeStamping Profile

Below you can find a list of common security risks for TimeStamping service providers. Please rate them according to your perception (if there are different possible threats in one risk, rate the worst case):

Impact for the organization

	Very low	Low	Medium	High	Very high
Compromise of the TSA's signature creation data (private key)					
Lose of evidence in chain of trust in the preservation of Tokens					
Compromise of the main time source					
Lose of accuracy of the main time source					

Unavailability of the main time source					

Probability of occurrence

	Very unlikely	Unlikely	Possible	Likely	Frequent
Compromise of the TSA's signature creation data (private key)					
Lose of evidence in chain of trust in the preservation of Tokens					
Compromise of the main time source					
Lose of accuracy of the main time source					
Unavailability of the main time source					

If you believe there are other critical risks for TimeStamping service providers not included in the list, please add them here:

e-Signed Documents storage or management

How the eDocument management or storage service is provided? (select all that apply)

Through a client (desktop) application,

Through a web site (on-line) service of your own,

Through a e-Government web site

Through a web service available for automatic processing (e.g. e-invoicing)

Are the managed documents kept stored in the servers?

Yes

No

Below you can find a list of common security risks for e-signed Documents service providers. Please rate them according to your perception (if there are different possible threats in one risk, rate the worst case):

Impact for the organization

	Very low	Low	Medium	High	Very high
End-user impersonation (the TSP does a false end-user authentication)					
Web site / web service impersonation (the user signed-in in a false TSP web)					
Unavailability of service (e.g. Discontinuation of the activity,					

interoperability problems due to change of protocols or versions, change on the service provision conditions)					
Lose of evidence in chain of trust in the long time e-signature's preservation (e.g. letting signature expire)					
Lose or alteration of digital evidences (e.g. signed records/acknowledgement of receipt, OCSP responses)					
Relay on not-updated certificate revocation information					
Lose or compromise of service's signature creation data (private key)					

Probability of occurrence

	Very unlikely	Unlikely	Possible	Likely	Frequent
End-user impersonation (the TSP does a false end-user authentication)					
Web site / web service impersonation (the user signed-in in a false TSP web)					
Unavailability of service (e.g. Discontinuation of the activity, interoperability problems due to change of protocols or versions, change on the service provision conditions)					
Lose of evidence in chain of trust in the long time e-signature's preservation (e.g. letting signature expire)					
Lose or alteration of digital evidences (e.g. signed records/acknowledgement of receipt, OCSP responses)					
Relay on not-updated certificate revocation information					
Lose or compromise of service's signature creation data (private key)					

If you believe there are other critical risks for e-signed Document service providers not included in the list, please add them here:

e-Documents Delivery services

How the eDocument delivery service is provided? (select all that apply)

Through a client (desktop) application

Through a web site (on-line) service of your own

Through a e-Government web site

Through a web service available for automatic processing (e.g. e-invoicing),

The managed documents are stored in the servers

What e-signature standards are supported?

CAdES

XAdES (XML-DSig)

PAdES

PKCS#7

DSS

Below you can find a list of common security risks for e-Documents Delivery service providers. Please rate them according to your perception (if there are different possible threats in one risk, rate the worst case):

Impact for the organization

	Very low	Low	Medium	High	Very high
Sender or Receiver impersonation (the TSP does a false sender or receiver authentication)					
Web site / web service impersonation (the receiver or the sender uses a false TSP web, or the receiver receives a fake notification)					
Unavailability of service (e.g. Discontinuation of the activity, interoperability problems due to change of protocols or versions, change on the service provision conditions)					
Lose or alteration of digital evidences (e.g. signed records/acknowledgement of receipt, OCSP responses)					
Relay on not-updated certificate					

revocation information					
Lose or compromise of service's signature creation data (private key)					

Probability of occurrence

	Very unlikely	Unlikely	Possible	Likely	Frequent
Sender or Receiver impersonation (the TSP does a false sender or receiver authentication)					
Web site / web service impersonation (the receiver or the sender uses a false TSP web, or the receiver receives a fake notification)					
Unavailability of service (e.g. Discontinuation of the activity, interoperability problems due to change of protocols or versions, change on the service provision conditions)					
Lose or alteration of digital evidences (e.g. signed records/acknowledgement of receipt, OCSP responses)					
Relay on not-updated certificate revocation information					
Lose or compromise of service's signature creation data (private key)					

If you believe there are other critical risks for e-Documents Delivery service providers not included in the list, please add them here:

Certificate or e-Signed Document Validation Service

How is the Validation service provided ? (Select all that apply)

Through a client (desktop) application

Through a web site (on-line) service of your own

Through an e-Government web site

Through a web service available for automatic processing

What certificate validation standards are supported?

OCSP

CRL

What e-signature standards are supported?

CAdES

XAdES (XML-DSig)

PAdES

PKCS#7

DSS

Below you can find a list of common security risks for Validation service providers. Please rate them according to your perception (if there are different possible threats in one risk, rate the worst case):

Impact for the organization

	Very low	Low	Medium	High	Very high
Unavailability of the service (e.g. discontinuation of activity, interoperability problems that causes some users cannot use the service, change on the service provision conditions)					
Relay on not-updated certificate revocation information ((e.g. lack of availability of the revocation information or lack of connectivity with the provider))					

Probability of occurrence

	Very unlikely	Unlikely	Possible	Likely	Frequent
Unavailability of the service (e.g. discontinuation of activity, interoperability problems that causes some users cannot use the service, change on the service provision conditions)					
Relay on not-updated certificate revocation information ((e.g. lack of availability of the revocation information or lack of connectivity with the provider))					

If you believe there are other critical risks for Certificate or Validation service providers not included in the list, please add them here:

Long-time preservation of e-Signed Documents

What kind of information is added to the sign in order to long-time preservation? Select the standards used for doing it:

AdES T (adds time-stamp)

AdES C (adds references to the certificates)

AdES X (adds time-stamps to the references)

AdES XL (adds CRLs)

AdES A (adds periodic time-stamps)

Below you can find a list of common security risks for Long-time preservation service providers. Please rate them according to your perception (if there are different possible threats in one risk, rate the worst case):

Impact for the organization

	Very low	Low	Medium	High	Very high
Break of chain of trust in the preservation of stored data/e-Document's (e.g. Not launching the re-signing process on due time)					
Lose or alteration of digital evidences (e.g. signed records/acknowledgement of receipt, OCSP responses)					
Relay on not-updated certificate revocation information					
The evolution of cryptography (e.g. security threats that break signatures, making weak the algorithms or shorter the key length)					
Lose or compromise of Service's signature creation data (private key)					

Probability of occurrence

	Very unlikely	Unlikely	Possible	Likely	Frequent
Break of chain of trust in the preservation of stored data/e-Document's (e.g. Not launching the re-signing process on due time)					
Lose or alteration of digital evidences					

(e.g. signed records/acknowledgement of receipt, OCSP responses)					
Relay on not-updated certificate revocation information					
The evolution of cryptography (e.g. security threats that break signatures, making weak the algorithms or shorter the key length)					
Lose or compromise of Service's signature creation data (private key)					

If you believe there are other critical risks for Long-time preservation service providers not included in the list, please add them here:

Catalogue Number: TP-04-13

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN 978-92-9204-076-5

9 789292 040765

doi: 10.2824/27048

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu