Trusted e-ID Infrastructures and services in EU

Recommendations for Trusted Provision of e-Government services

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 unit H4 and the ISPC of the JRC.

Contact

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

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

Acknowledgements

This report has been possible thanks to the contributions of the participants in the large scale projects: EPSOS, PEPPOL (Jon Ølnes and Lefteris Leontaridis) and e-CODEX, that kindly answered the questionnaire prepared by ENISA and the contractor of this project Atos Consulting.

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.

ISBN 978-92-9204-075-8 doi: 10.2824/26540

Executive summary

Under the scope of the 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, ENISA has conducted a study about the security mechanisms and interoperability issues specific to the new regulated trust services. The aim of this report is to complement the report that summarises the results of the survey, also published by ENISA: "TSP services, standards and risk analysis report"[2], making more specific recommendations to e-Government service providers, encouraging them to use Trusted Third Party service providers to implement the trust services required to give citizens the expected level of confidence and trustwotthines on the services.

This document collects the experience of some of the Large Scale Pilots[3] (LSP) funded by the European Commission, that implement trust services defined in the proposed new Regulation (in particular epSOS, e-CODEX and PEPPOL), as cases studies to analyse the current practices and identify gaps and improvement opportunities. Then, the recommendations collected in the Trust Service Providers (TSP) overview report published by ENISA[4] have been adapted for the provision of e-Government Services, which include issues for security practices and risk management.

The following categories of recommendations have been considered the most relevant ones, to assist in defining and establishing the basis to offer trustworthy e-Gov. services to EU citizens[5]:

- **REC.6**.R: Specific BCM (Business Continuity Management) standards should be adopted in the provision of trusted services (by TSPs) and required by the e-Government customers.
- **REC.5**.R, **eGov_R1:** There is a need to define standard qualified profiles and best practices for trusted services, in order to clarify the definition of the services (SLA) and to standardize the QoS to be required by e-Government from TSPs.
- **REC.2**.R: Promote **Trusted Marks assessed** against eIDAS requirements that would be recognised **across borders**. Independent Trust Services should be integrated in e-Gov. services, with European scope, complying both with European eIDAS Regulation and national supervision. Assessment of qualified trust Services schemas should be extended to other TSPs regulated in the future[6], and mutual assistance system between supervisory bodies in the Member States should be set up.
- Based on the criticality of the e-Gov. services, always assess three aspects:
  - **REC.3**.R: the strength of the authentication mechanisms to be used, giving priority to e-signature
  - **REC.4**.P: the need for end-to-end encryption and
  - **eGov_R8 (TSP_R4):** the need for audit trails to collect and preserve electronic evidences.

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

[2] http://www.enisa.europa.eu/publications#c2=publicationDate&reversed=on&c5=all&c0=10&b_start=0

[3] http://ec.europa.eu/digital-agenda/en/egovernment

[4] The "TSP services, standards and risk analysis report" will be published in ENISA's website: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables .

[5] See full list in Section 3. 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 eGovernment SP (G).

[6] Once the draft Regulation on electronic identification and trust services will be approved by the European Parlaimant.

Table of Contents

Executive summary iii

1 Introduction 1

1.1 Motivation 2

2 Study Cases 3

2.1 epSOS 3

2.2 e-CODEX 4

2.3 PEPPOL 5

3 Recommendations 8

3.1 General recommendations to e-Government service providers 8

3.2 General recommendations to Member States Regulators 9

3.3 Specific Recommendations for Trust Service Providers 9

3.4 Summary of Recommendations 10

4 Annex I: Abbreviations 12

1 Introduction

The European Commission presented in July 2012 a proposal for a new Regulation on electronic identification and trust services for electronic transactions in the internal market[7], 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 on 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.

One of the actions taken on those studies was a survey conducted by ENISA to Trust Service Providers [8] (TSP).

Another action was the brief analysis of some Large Scale Pilots operating in Europe, focusing on the use of:

- Electronic certificates, including e-Signature ones (summarized in other ENISA reports[9])
- Electronic time stamps (creation and handling)
- ElectronicDocuments[10] 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)

The definition of “trust service” in the EU Regulation is quite wider, since teorically 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

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

[8] The “TSP services, standards and risk analysis report” will be published in ENISA’s website: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables.

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

[10] An eDocument should be considered as any kind of data digitally signed using advanced electronic signature (with or without an electronic signature creation device)

1.1 Motivation

This document is intended to provide a summary of the recommendations for the implementation of TSP provided in the ENISA's "TSP services, standards and risk analysis report"[11] for the particular case of e-Government portals. This document identifies recommendations for Trusted Provision of eGovernment services based in the experience of the LSPs and the recommendations extracted from the survey and fully described in that ENISA's report.

Some services already provided in the market are identified by the object they are applied, like Time Stamping or eCertificate provision, whilst others are advertised with the name of the service they provide, like eValidation or Preservation. Others like "Creation" of eSignatures or eSeals over eDocuments may be hidden in other services, like submission of documents to a public administration portal. In order to simplify the combinations, only those services most frequently referenced in eGovernment applications have been included in the analysis.

[11] Published in: http://www.enisa.europa.eu/activities/identity-and-trust/trust-services/reports

2 Study Cases

This section summarises the description of the scenarios built for the provision of e-Gov. services by the members of the LSPs funded by the EC, which are themost relevant for this analysis.

This summary reflects the way each LSP implement the TSPs that are needed to build trust amongst the users of the LSP, either integrated in the platform of the project, or provided by a third party, which in some cases is also partner of the project, providing the service in a commercial basis to the members of the LSP in the same conditions as they provide the TS to other customers.

2.1 epSOS

The Smart Open Services for European Patients (epSOS[12]) project architecture is based on National Contact Points usually embedded to a competent authority of the country. Health organizations in each participating nation will be connected to the epSOS network through the National Contact Point.

epSOS is implemented only by selected end users (or PoC) of the Participating Member States (MS).

Those PoC delegate the following processes to the National Contact Point (NCP) of each country:

- User authentication (requestor or provider of a document),
- possibility for electronic signature of documents by its provider,
- requirements about those signatures,
- the user authorization to sending personal data out of the country,
- etc.

There have been established bilateral agreements between each pair of countries to accept the application of the technologies used in each MS, because:

- There are different requirements of the competent authority in each country about, e.g. the use of electronic signature technologies, like: recognised hash algorithms, advanced vs qualified electronic signature.
- epSOS is a health service and healthcare is excluded from the EU Directive 2006/123/EC[13].provisions about services in the internal market, which makes epSOS unable to mandate the use of advanced electronic signature (that EU Commission Decision 2009/767/EC[14] establishes).

There are two software solutions for the NCP: the fully Open Source OpenNCP toolkit and the "NCP in-a-box", both based on Open Source components and the closed source backbone from one Vendor. Both are mandated to support the application of electronic signatures. epSOS adopts SHA-2 hashed certificates. Since only few CAs offer SHA-2 certificates for servers, most of epSOS Countries have adopted certificates generated by the Czech CA "1st Certification Authority".

[12] http://www.epsos.eu/

[13] The Directive 2006/123/CE establishes the requirement to simplify the relation with the administration in order to facilitate the dissemination of services in the internal market. Healthcare services are out of this requirement.

[14] The Commission Decision 2009/767EC describes the security requirements for procedures according to Art. 8 Services Directive 2006/123/EC. In particular, Art. 1 establishes the possibility to require advanced electronic signature.

epSOS specifications require the use of TSPs included in any Trusted List. However not all the epSOS Countries are in the condition to fulfill the requirement: termporary relaxation has been approved by the epSOS Steering Board.

epSOS organizations are expected to comply with ISO/IEC 27000 or equivalent and the epSOS specific security safeguards. The National Contact Point is responsible for auditing its implementations and service providers. They are not expected to comply with BCM standards.

The following main services have been implemented:

- **e-Delivery:** 4 types of messages are Exchanged between the countries (medical information, e-prescription or e-dispensation, interchange consent, healthcare encounter report). eDelivery is provided as **a document requesting –delivering system.** Both the authentication data in the requests of information and the delivered package are signed electronically. Signatures are made/validated in the National Contact Point.
- **e-Document:** There is no requirement of including signatures of the exchanged documents itself. The epSOS organizations are free of doing it, and in that case the e-documents will be stored in the National infrastructures, not in the epSOS network.
- **Long-Time Preservation and Time-Stamping:** these services are used for Audit Trail events in the accesses to patient's data.
    - Audit trails are always electronically signed. They are stored for 10 years.
    - Future re-signs are anticipated and have been extended for fitting one or more electronic signature formats.
    - Audit trails are time stamped. In general, the time stamp in performed internally by a web service on the National Contact Point (without any external TSA) and it is of its responsibility. There is no requirement about using a National or International main time source.
    - Legally, the Audit Trails are compiled, stored and managed under the sole responsibility of the member state operating the system accordance with local law.
- **Validations Services:** epSOS performs certificates validations over OCSP, CRL and even with manual certificate validation services in some cases. epSOS doesn't use any *e-signed document* validation services.

2.2 e-CODEX

e-CODEX[15] "e-Justice Communication via Online Data Exchange" network is composed of National Gateways, one in each country adhere to the pilot. National Systems are then connected to the National Gateway. National Systems are outside the control of e-CODEX.

End-user authentication and end-user signing documents relay on the National System, not in any e-CODEX component.

e-CODEX National Systems delivering trusted documents **have to be characterized as an advanced electronic signature system**. It seems that this LSP adheres to the Commission Decision 2009/767/EC[16] and EU Directive 2006/123/EC[17].

[15] http://www.e-codex.eu/

[16] The Commission Decision 2009/767EC describes the security requirements for procedures according to Art. 8 Services Directive 2006/123/EC. In particular, Art. 1 establishes the possibility to require advanced electronic signature.

[17] The Directive 2006/123/CE establishes the requirement to simplify the relation with the administration in order to facilitate the dissemination of services in the internal market.

Within the e-CODEX gateways DG Market's DSS Tool (a java based open source software module that can be used to create, extend and validate XAdES, PAdES ans CAdES eSignatures) is used for signature validation. The validation is done in the country of origin before sending an e-document.

Internally, the e-CODEX gateways use X.509 certificates but without any external CSP to provide them.

The e-CODEX National Systems can use their own tools, TSPs, or certificates providers. So e-CODEX doesn't have any special requirement.

No time stamp service is used in this LSP.

The e-CODEX Sender National Gateway and the e-CODEX Receiver National Gateway have the following tasks to develop:

- The Sender Gateway has to be able to verify e-document's signature (from its own country) when receiving them from the e-CODEX National System, and then generate a validation report (the "Trust OK" token). The processed validation report is transported together with the e-document and a signed Token; thereby the sending country gives an assessment of the signature based on his national requirements. These documents are transported within an ASIC-S container signed by the e-CODEX gateway.
- The Receiver Gateway must validate the signed ASIC-S container and Token received from the Sender Gateway against a predefined e-CODEX Keystore. If the integrity of all documents is confirmed, the documents can be passed on to the e-CODEX National System. The Trust OK token is then accepted as evidence of validity of original signature of eDocument without further validation.

There are ETSI Rem (Registered Electronic Mail, ETSI TS 102 640) evidences of all the processes, signed with advanced electronic signature and stored in e-CODEX platform for as long needed to fulfill national requirements.

As a summary these are the trust services implemented in e-CODEX:

- **e-Document**: The end user signing documents service is delegated to National Systems.
- **e-Delivery:** This service is implemented by the National Gateways inside the e-CODEX systems to guarantee the integrity in the transmission.
- **e-Validation:** Verification of end user e-documents and internal messages is done by the National Gateways.
- **Time Stamping**: Not implemented
- **Long Time Preservation**: Not implemented

2.3 PEPPOL

Pan-European Public Procurement Online (**PEPPOL**[18]) project is composed by a Transport Infrastructure (coordinated by OpenPEPPOL Authority) to which Peppol Access Points/Peppol Authorities are engaged. There could be more than one Access Point per country. Service Providers typically represent an eProcurement community and are engaged to an Access Point. Users access an eProcurement community via the Service Providers or via the end-user IT systems, when they have implemented Peppol natively.

In PEPPOL, the Transport Infrastructure is used to exchange standardised, structured (XML) eProcurement documents but the Transport Infrastructure can be used also for other purposes in

[18] http://www.peppol.eu/

other contexts than eProcurement. There is an extensive use of the PEPPOL Transport Infrastructure and the standardised documents in some countries, with a continuously growing number of countries connected and using the service.

The Transport Infrastructure includes one Service Metadata Locator (SML) and several Service Metadata Publishers (SMPs) for discovery and routing of messages between the Access Points of the Transport Infrastructure.

There is no requirement for the Access Points to be characterized as an advanced electronic signature system neither as a qualified electronic signature system.

Access Points are operated subject to agreements between the Access Point Service Provider and a Peppol Authority, which regulates some basis business rules (such as the obligation of Access Points about not to charge each other for inter-communications between them, the publication of end-user capacity via the SML/SMP system to receive certain types of documents (in order to facilitate discovery and routing) and the obligation to support PEPPOL document formats). When there is no Peppol Authority in the country, the agreement is signed directly with OpenPeppol.

There are also agreements between a Peppol Authority and OpenPeppol. OpenPEPPOL is a non-profit international association of public and private PEPPOL community members.

The Peppol infrastructure has its own internal PKI provided by Verisign. When an Access Point is allowed to connect to the infrastructure, the Access Point obtains a certificate from this PKI. Posession of such a certificate proves that the Access Point is authorized. There are Certificates to sign and encrypt messages between Access Points. Certificate validity is checked by OCSP provided by the internal PKI, and by CRLs for continuity purposes. Protection of messages when delivered from the sender to an Access Point and from an Access Point to the receiver is out of scope.

No time stamp service and no long time preservation service are used in this LSP.

There are transactions logs kept by Service Providers but the specifications do not impose explicit requirements, so such policies are left to the Service Providers and are part of their commercial policies. There is no requirement to be digitally signed nor time stamped.

End-user authentication and end-user signing documents is outside the control of Peppol. It is delegated to Service Providers or end-user IT systems (when applied). The authentication mechanism used is also out of Peppol scope.

PEPPOL (and OpenPEPPOL) however provides a validation infrastructure for the recipient of a signed document. This service is completely independent from the Transport Infrastructure and can be integrated in the recipients' end system, or in any other system as wished. The usual mode of operation is that the receiver uses a validation service for certificate validation, while other signature processing is done locally. A profile of the XKMS protocol is used for this interface. The response attests not only to the validity of the certificate but also to its quality and legal status (e.g. qualified). The validation infrastructure covers all issuers of qualified certificates in the EU, a substantial number of non-qualified certificates, and qualified certificates from a number of non-EU countries such as from Eastern Europe.

A further interface to the validation infrastructure is specified as a profile of OASIS DSS but this interface was not tested by PEPPOL. Using this interface, an entire signed document is sent to the validation infrastructure, which attest to both validity of signatures and signature quality and legal status (e.g. qualified).

As a summary these are the trust services implemented in PEPPOL:

- **e-Document**: eProcurement documents are standardised by the CEN BII workshop based on the results of PEPPOL. These are today mainly XML documents for post-award procurement, like catalogue, order, order confirmation and invoice, intended for automated transfer between the IT-systems of the involved actors over the PEPPOL Transport Infrastructure. There is no requirement to sign the documents.
- **e-Delivery:** Secure and reliable (receipt confirmation etc.) document transfer between the Access Points of the PEPPOL Transport Infrastructure.
- **eValidation:** Validation infrastructure (certificate validation using an XKMS-based interface) for end user e-signed documents. Validation and quality assessment of certificates from all relevant certificate issuers in the EU and some non-EU countries is provided. There is also a validation infrastructure for the transport infrastructure associated to the internal PKI.
- **Time Stamping**: Not implemented
- **Long Time Preservation**: Not implemented

3 Recommendations

This section emphasizes the recommendations made in the TSP Report of ENISA, that are applicable to eGovernment services and it includes some new ones identified from the analysis of LSPs experiences collected in the survey. In some cases the recommendation will be applicable as it was stated there, and in others it will include some implementation guidelines, specific for the eGovernement environment.

The following recommendations are aimed to offer trustworthiness to the provision of any eGovernment service. They have been grouped according to the role of the actor that should be responsible of implementing them, with the aim to facilitate their idenfication and adoption by the corresponding agent. The recommendations are numbered using a prefix and a sequence number. The prefix may be:

- **TSP_Rx**, when the recommendation is also given in the TSP overview report of ENISA. In this case, the sequential number “Rx” corresponds to the number “x” given in that report.
- **eGov_Rn (TSP_Rx)**, when the recommendation “n” is specific of this report. Those specific recommendations (**eGov_Rn**) express a particularisation of the “original” recommendation (**TSP_Rx**) given in the ENISA’s TSP report.

3.1 General recommendations to e-Government service providers

- **TSP_R4:** 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.
- **TSP_R5:** It’s recommended the definition of the adequate service’s profiles based on best practices that comply with expected QoS.
  - **eGov_R1 (TSP_R5):** It is recommended the selection of TSPs based on standardized profiles, to obtain standard QoS through SLAs (e.g. for time stamp services, the synchronization time with main time source or the service recovery time).
- **TSP_R6:** Bussiness Continuity Management standards applied to the service as a whole (as could be ISO/IEC 22301) should be promoted. It could be possible also the use of non-especific standards as ETSI 101 456 or EN 319 411-2 because they include business continuity requirements.
- **TSP_R8:** It’s recommended the promotion of the use of national or internationally trusted time sources, taking it into consideration for the specification of a qualified service.
  - **eGov_R3 (TSP_R8):** It is recommended the use of independent time stamp services when there is any requirement about the moment any transaction or operation is made. Time stamp service should be provided by an organization independent from the originator of the transaction or the recipient of the transaction in order to provide guarantees of its authenticity and integrity.
- **TSP_R11:** It is recommended guaranteeing the quality of the certificate revocation service to allow the eValidation service trusts more on them.
  - **eGov_R2 (TSP_R11):** It’s recommended to analyze which common requirements on revocation service QoS are needed prior to the selection of TSPs, once the eGovernment service has identified the risk it is going to assume. (e.g., the time passed between the users notify the revocation and the revocation itself is effective).
- **TSP_R12:** 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.

3.2 General recommendations to Member States Regulators

- **TSP_R2:** It should be promoted the use of widely recognised Trusted Marks based on conformity assessment of qualified TSPs against eIDAS requirements that would be recognised across borders. 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[19], e.g. cross-border or mutual recognition of accreditation schemas or independent auditing body. **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.
    - **eGov_R4 (TSP_R2):** Trust Services should be developed with European scope, complying with European Regulation, which should be promoted. This practice would solve all interoperability and security issues in a common and trusted way. e-Gov. service providers should accept and prioritise TSPs audited by a recognised independent body confirming that TSPs fulfil the obligations laid down in the Regulation[20].

3.3 Specific Recommendations for Trust Service Providers

Recommendations for e-Document[21] services (creation, handling or preservation)

- **TSP_R9**: best practices must be defined to harmonise the quality and functionality of the Long Time Preservation service (**QoS & SLA**).
- **TSP_R10:** It is recommended the use of **two hash algorithms** in Long Time Preservation services to protect the integrity of the e-Signatures; breaking both algorithms at the same time is less probable.
- **TSP_R11:** It is recommended guaranteeing the quality of the certificate revocation service to allow the eValidation service trusts more on them.
    - **eGov_R6 (TSP_R11)**: It is recommended to obtain all the needed information and/or evidences to allow the validation of eDocuments from signing time, and keep it with the document.

Recommendations for e-Validation services

- **TPS_R3:** Supervisors should **promote a wider use of e-Signature** as authentication mechanism to access TSP services, **barriers for cross-border interoperability** of e-Signature & eIDAS certificateshave to be removed. And e-Government SP should accept them, under this assumption:
    - **eGov_R5 (TSP_R3):** It's recommended never to accept any eDocument whose origin has not been previously authenticated.
    - **eGov_R7 (TSP_R3):** Integrate tools to allow cross-border acceptance of e-Signature Certificates. This could be accomplished in different ways:
        - With a **unique access point** (generally supported by an **external Certificate Validation TSP**) accepting all kinds of certificates.
        - With several **access points distributed in the member states**, for user authentication and e-signature validation. It's easier for national contact points to know how to validate and understand every one of its own citizen's profiles and attributes (power of attorney or warrant, liability, etc.).

[19] As recommended in the whereas 34 of the new Regulation.

[20] Art. 16 of draft EU Regulation on electronic identification and trust services.

[21] An eDocument should be considered as any kind of data digitally signed using advanced electronic signature (with or without an electronic signature creation device)

  - Promoting the automatic processing of **Trusted Lists**, to allow interchange of information about accredited service providers, extended to all kinds of Regulated TSPs.
- **TSP_R7:** Full adoption of e-signature standards by TSPs should be reached, to achieve full interoperability.

Recommendations for e-Delivery services

- **TSP_R5:** It's recommended the definition of the adequate service's profiles based on best practices that comply with expected QoS.
  - **eGov_R8 (TSP_R5):** It is recommended to implement audit trails of the transactions, specially when reception is a critical point. For high quality services, which depend on their criticality, it is recommended to electronically sign and time stamp the trails, to preserve the evidence and guarantee their non-repudiation though a TTP (Trusted Third Party TSP).

3.4 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 eGovernment SP (G). In some cases the (G) column has been marked with (V), meaning that the eGovSP is encouraged to Validate that the TSP is providing the service following the recommendation.

RECOMMENDATION	TSP	Reg/ Stndr	eGov SP
[**REC.2**.P/R/G] 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 bord.	X	**R**	↓
eGov_R4 (TSP_R2): Trust Services should be developed with European scope, complying with European Regulation, which should be promoted.	X	**R**	X
[**REC.3**.R/G] Supervisors should **promote a wider use of e-Signature** as authentication mechanism to access TSPs, **barriers for cross-border interoperability** of e-Signature & eIDAS certificateshave to be removed.		**R**	↓↓
eGov_R5 (TSP_R3): It's recommended never to accept any eDocument whose origin has not been previously authenticated			R
eGov_R7 (TSP_R3): Improve the support of a wider scope of international e-signature certificates.			**R**
[**REC.4**.P/R/G] 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

RECOMMENDATION	TSP	Reg/ Stndr	eGov SP
[**REC.5**.P/R] It's recommended the definition of the adequate **service's profiles** based on best practices that comply with expected QoS.	X	**R**	↓↓
eGov_R1 (TSP_R5): It is recommended the selection of TSPs based on standardized profiles, to obtain standard QoS through SLAs (i.e. for time stamp services, the synchronization time with main time source or the service recovery time)			**R**
eGov_R8 (TSP_R5): It is recommended to implement audit trails of the transactions, specially when reception is a critical point. For high quality services, which depend on their criticality, it is recommended to electronically sign and time stamp the trails, to ensure their moment and their non-repudiation from a TTP.			**R**
[**REC.6**.P/R/G] **BCM standards** (ISO 22301) applied to the service as a whole should be promoted, as well as non-specific ones, including BCM controls.	X	**R**	V
[**REC.7**.P/G] **Full adoption of e-signature** standards should be reached, to achieve full interoperability.	**R**		X
[**REC.8**.P/G] recommended the promotion of the use of national or internationally **trusted time sources**, taking it into consideration for the specification of a qualified service.	**R**		↓
eGov_R3 (TSP_R8): It is recommended the use of **independent time stamp services** when there is any requirement about the moment any transaction or operation is made.			**R**
[**REC.9**.P/R/G] 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/G] It is recommended the use of **two hash algorithms** in Long Time Preservation services to protect the integrity of the e-Signatures; breaking both algorithms at the same time is less probable.	**R**		V
[**REC**.11.P/G] It is recommended guaranteeing the quality of the certificate **revocation service** to allow the eValidation service trusts more on them.	**R**		↓
eGov_R2 (TSP_R11): It's recommended to analyze which common requirements on revocation service QoS are needed prior to the selection of TSPs, once the eGovernment service has identified the risk it is going to assume (i.e, the time passed between the users notify the revocation and the revocation itself is effective).			**R**
eGov_R6 (TSP_R11): It is recommended to obtain all the needed information and/or evidences to allow the validation of eDocuments from signing time, and keep it with the document.			**R**
[**REC.12**.G] There should be a focus on user **training and consciousness** of threats to prevent web site / web service **impersonation**.	**R**		X

Table 2: Summary of recommendations with Stakeholder category relevance.

4 Annex I: Abbreviations

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
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

Catalogue Number: TP-01-13-8

ISBN 978-92-9204-075-8

9 789292 040758

doi: 10.2824/26540

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

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