TSP services, standards and risk analysis

Trusted e-ID infrastructures and services in EU

Brussels, September, 24th 2013

Contents

- Context
- Survey
- Services
- Standards
- Risk Analysis
- Recommendations summary
- Pending issues

Context

- Proposal for a **new Regulation** on eID and Trust Services for electronic transactions.
- **Current Directive** 1999/93/EC on a Community framework for e-signatures.
- Provisions regarding the **security requirements** applicable to TSPs.
- ENISA works on 2013 on a series of studies:
  - The security aspects of trust service providers issuing electronic certificates.
  - **Security and interoperability aspects specific to the new trust services foreseen in the proposed Regulation.**

Survey

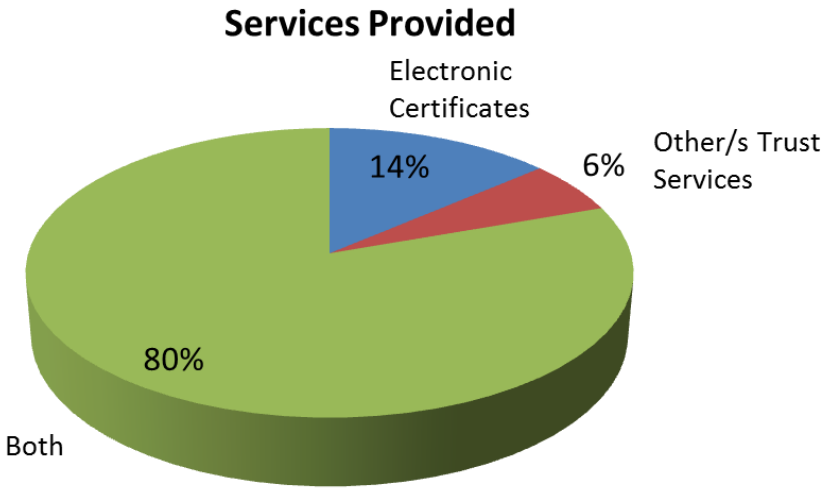
- Participants: EU TSPs
- Scope: **services** they offer, **security** practices, **standards** used, **interoperability** issues and **type of risks** related with their operation.
- The study is focused on the **services** whose provisions will be regulated in the new Regulation:
  - Electronic Time Stamps (TS)
  - Electronically signed documents storage or management (eDoc)
  - Electronic delivery services (eDeliv)
  - Validation of electronic signatures (eVal)
  - Long time preservation of electronic signatures (LTP)

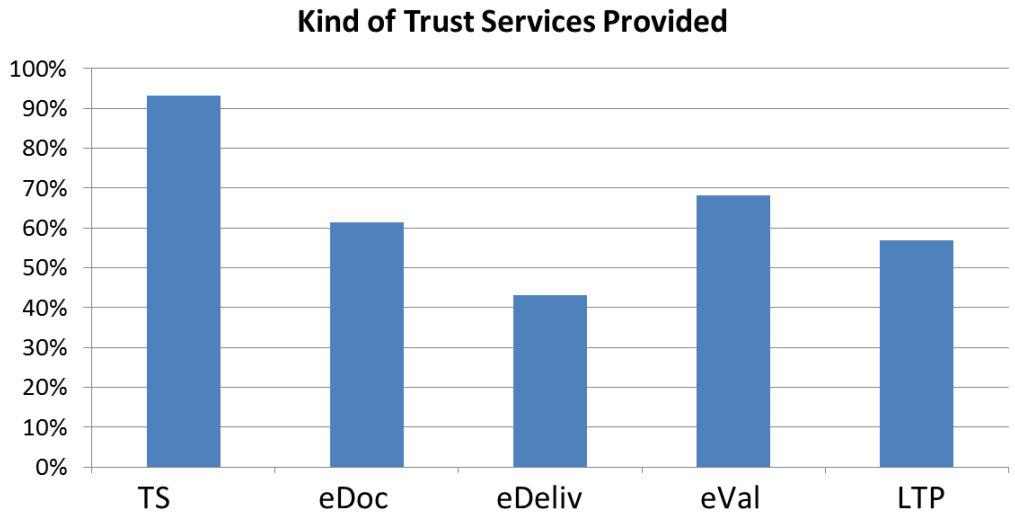
Survey

- The universe of the survey is **51 TSPs** corresponding to 20 EU Member States.
- Invitations were made mainly through **national regulators of certification service providers** and the **trust services lists** they produce.

Services: Type of service provided

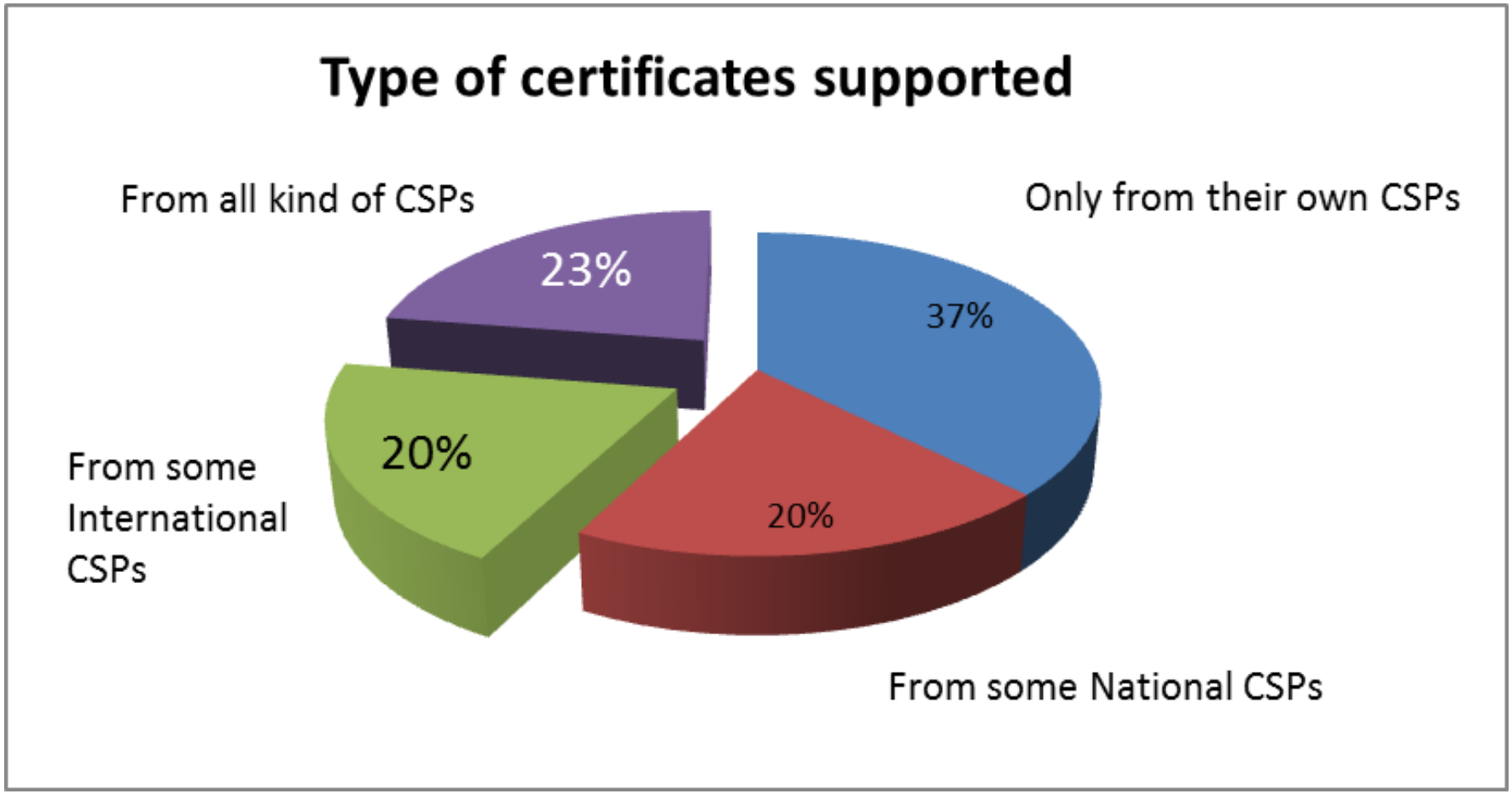
- Almost all provide certificates as well as other services.
- They are already used to implement certification schemas.
- 67% of TSPs offer services to both Public and private sector.





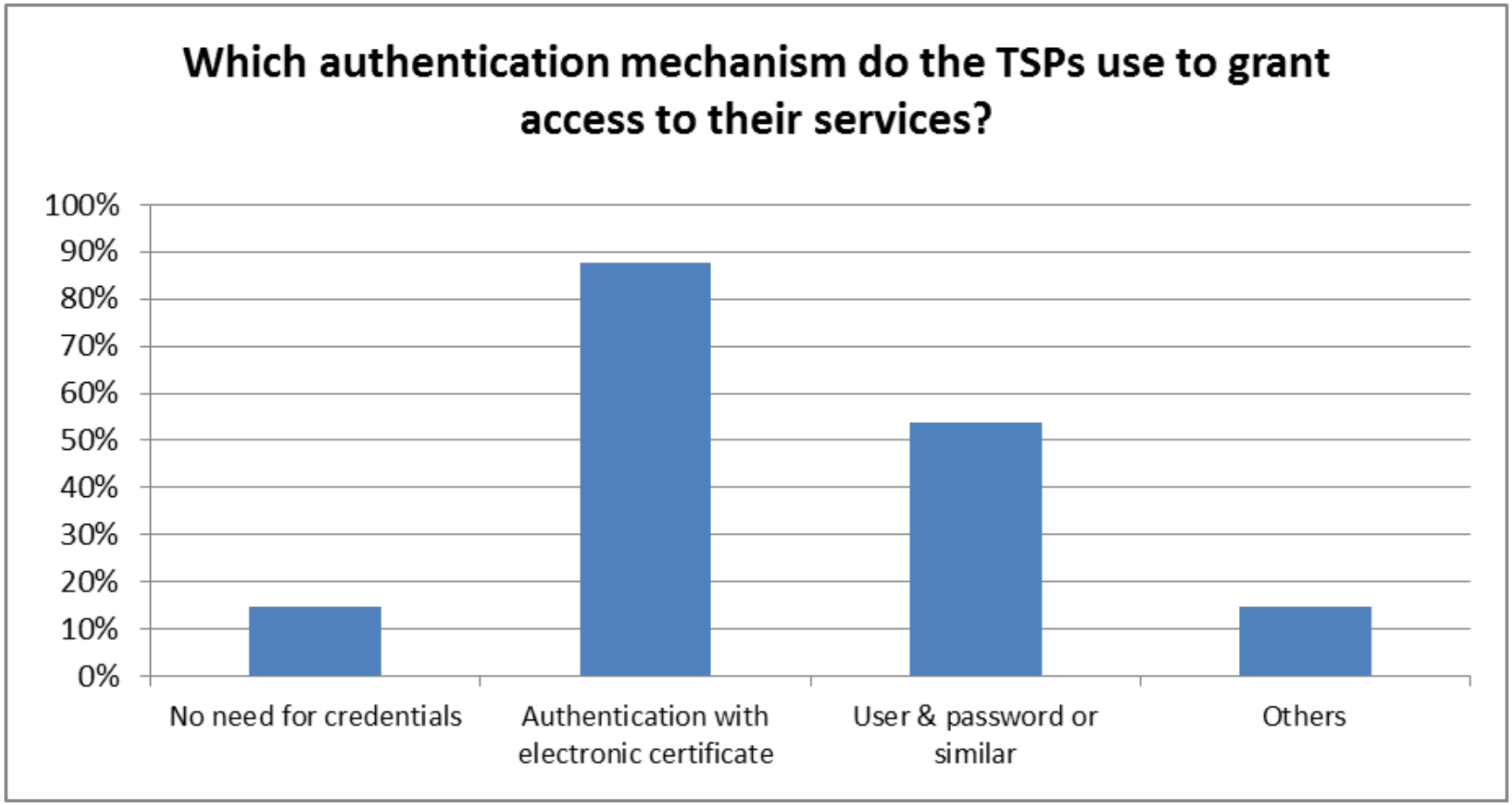
REC: CSP Certification schemas could be extended to other TSP services to have harmonised criteria of QoS and SLA guidelines.

Services: Scope of certificates



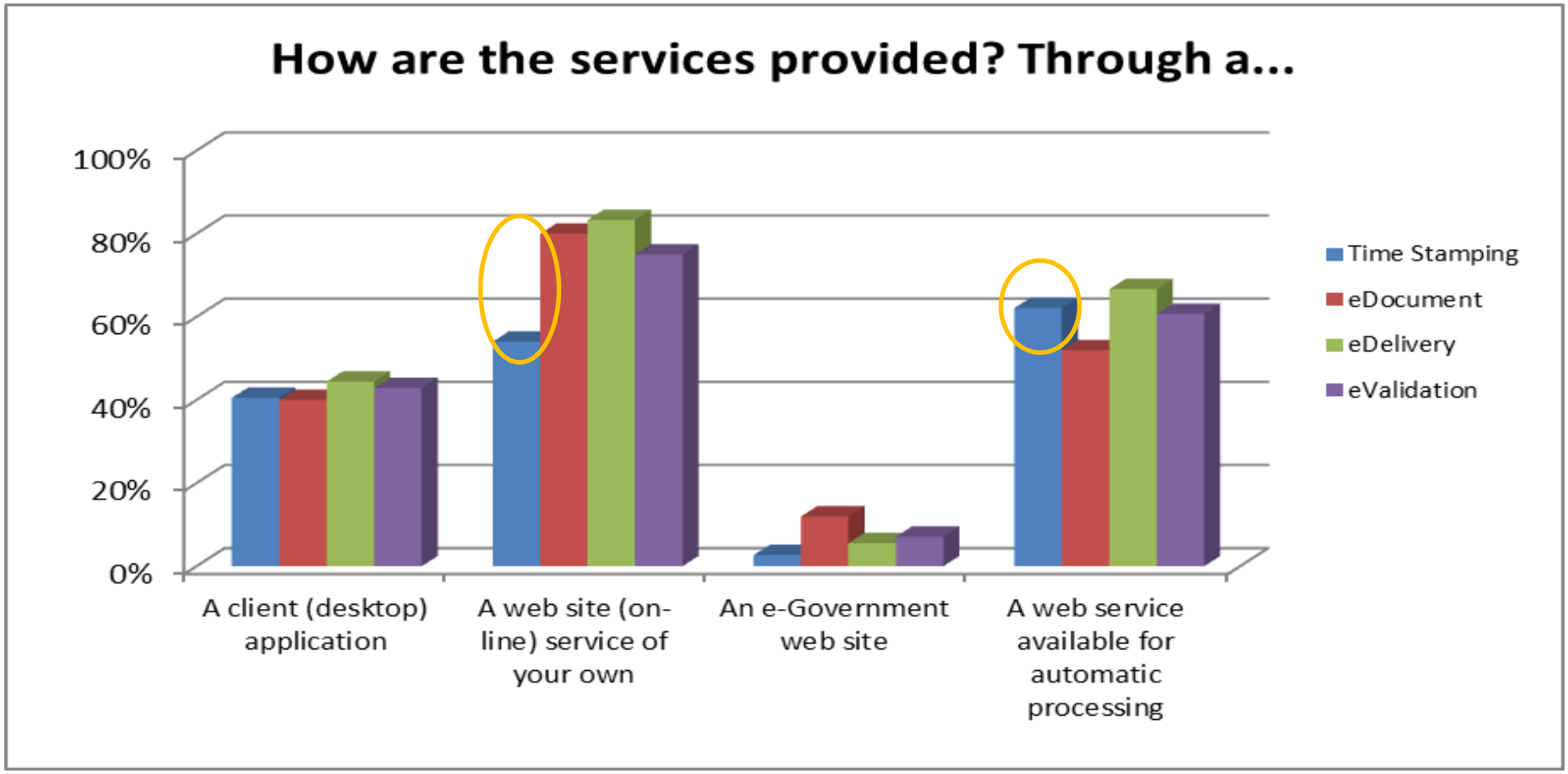
REC: Cross-border interoperability has to be promoted.

Services: Authentication mechanisms



REC. The strength of the authentication mechanism should be proportional to the criticality of the accessed services.

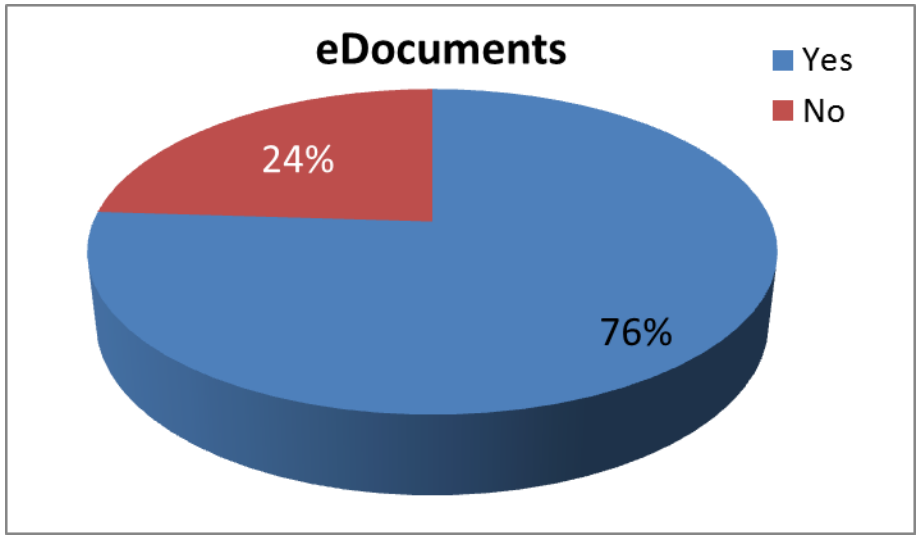
Services: Platforms used

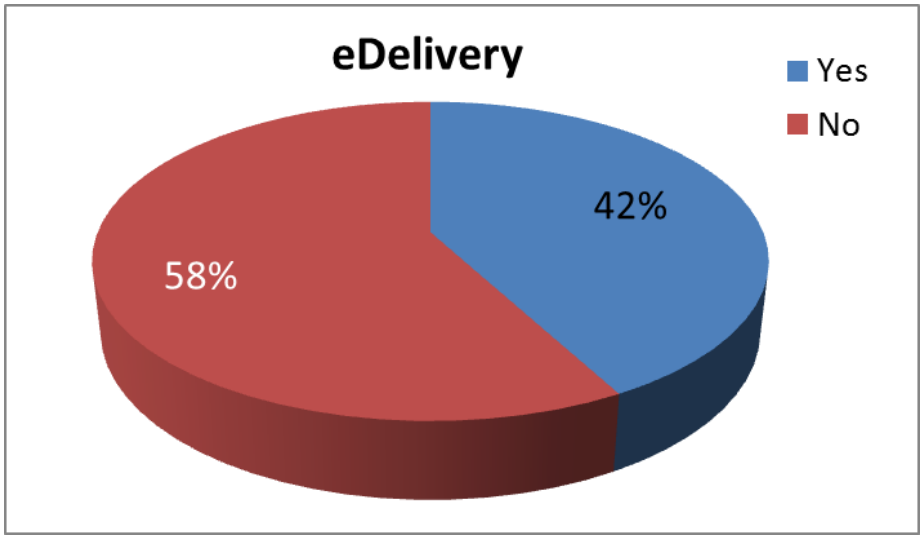


REC. Promote the implementation of clients to be executed in the customer computer with web-service access to TSP (https unsafe)

Services: Documents storage in the TSP's servers

The difference can be explained because of the nature of the services.

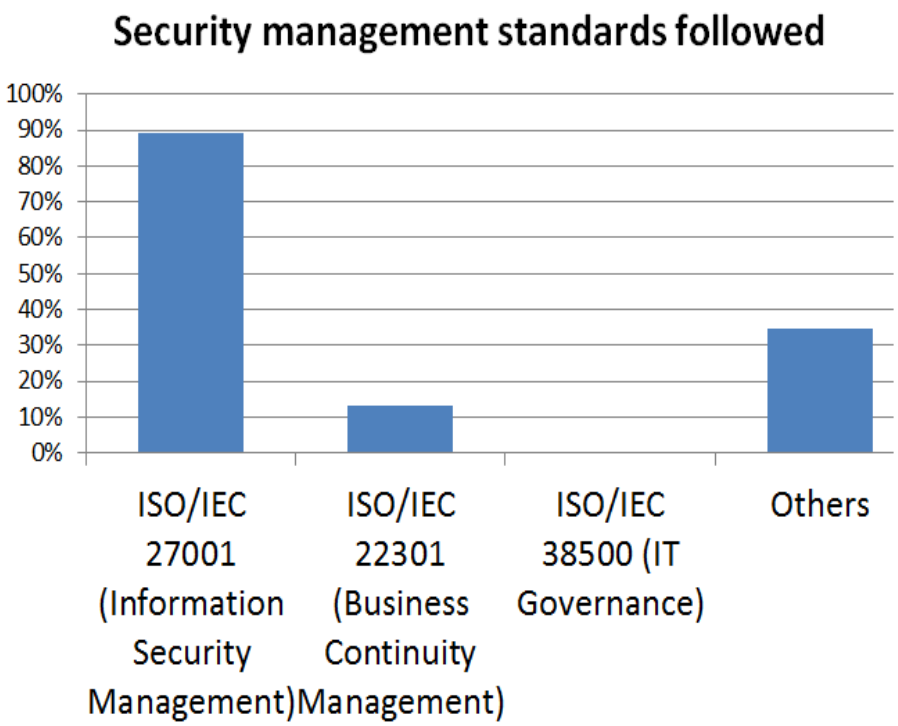


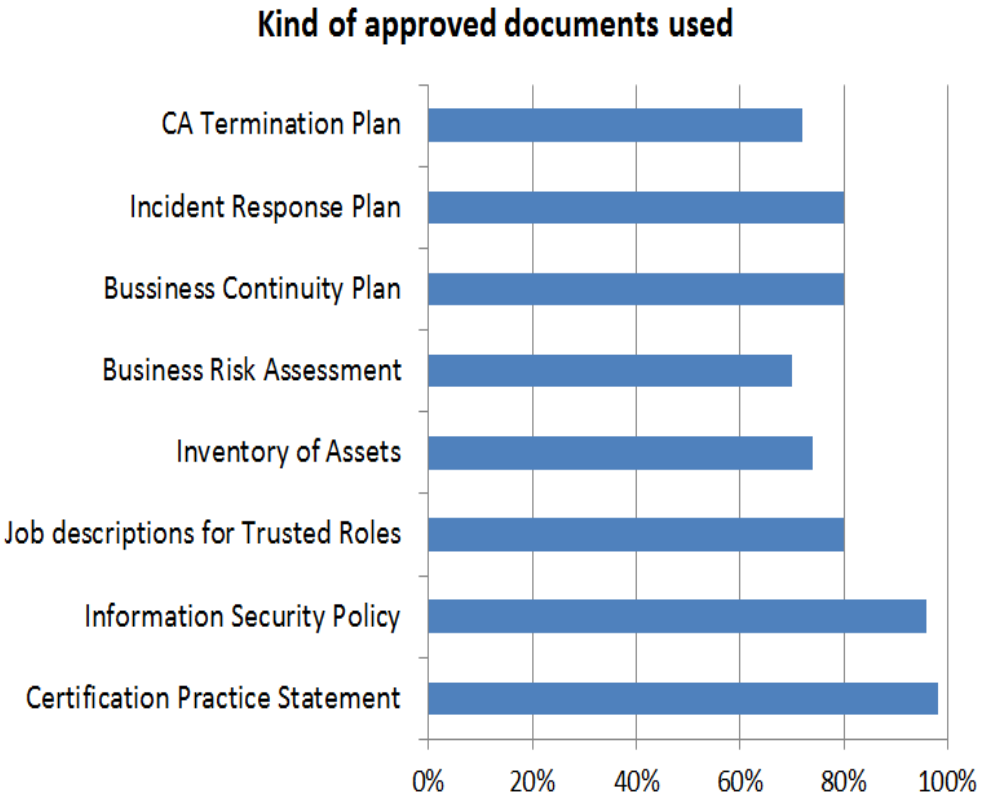


REC. The impact of this practice in the adequate security mechanisms to be adopted recommends to define different profiles of the service provision in each case.

Standards: Security Management standards

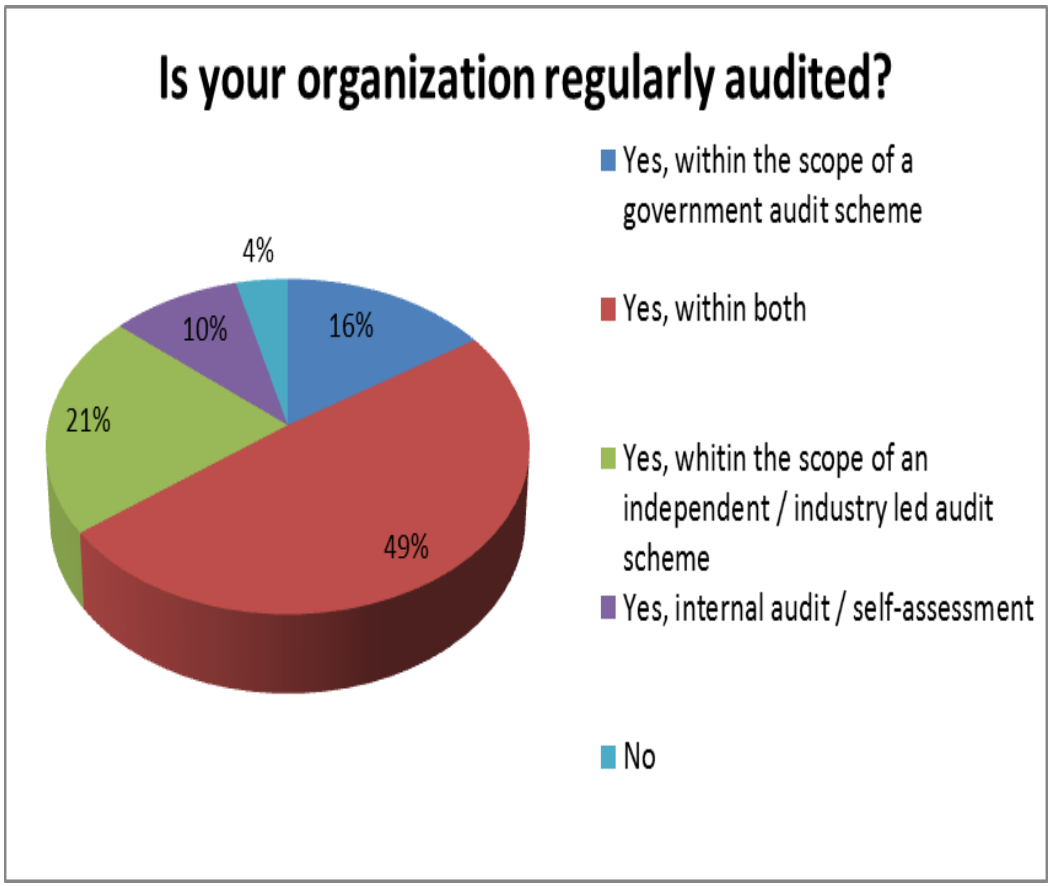
BCM: Low use of the ISO standard, although 80% have BCP documents.

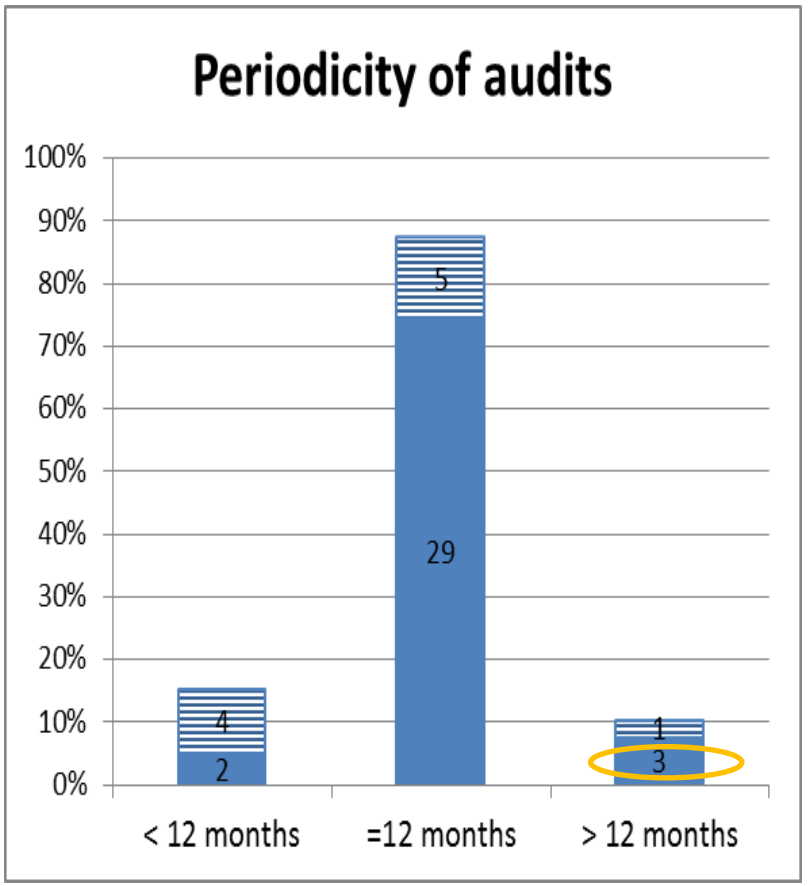




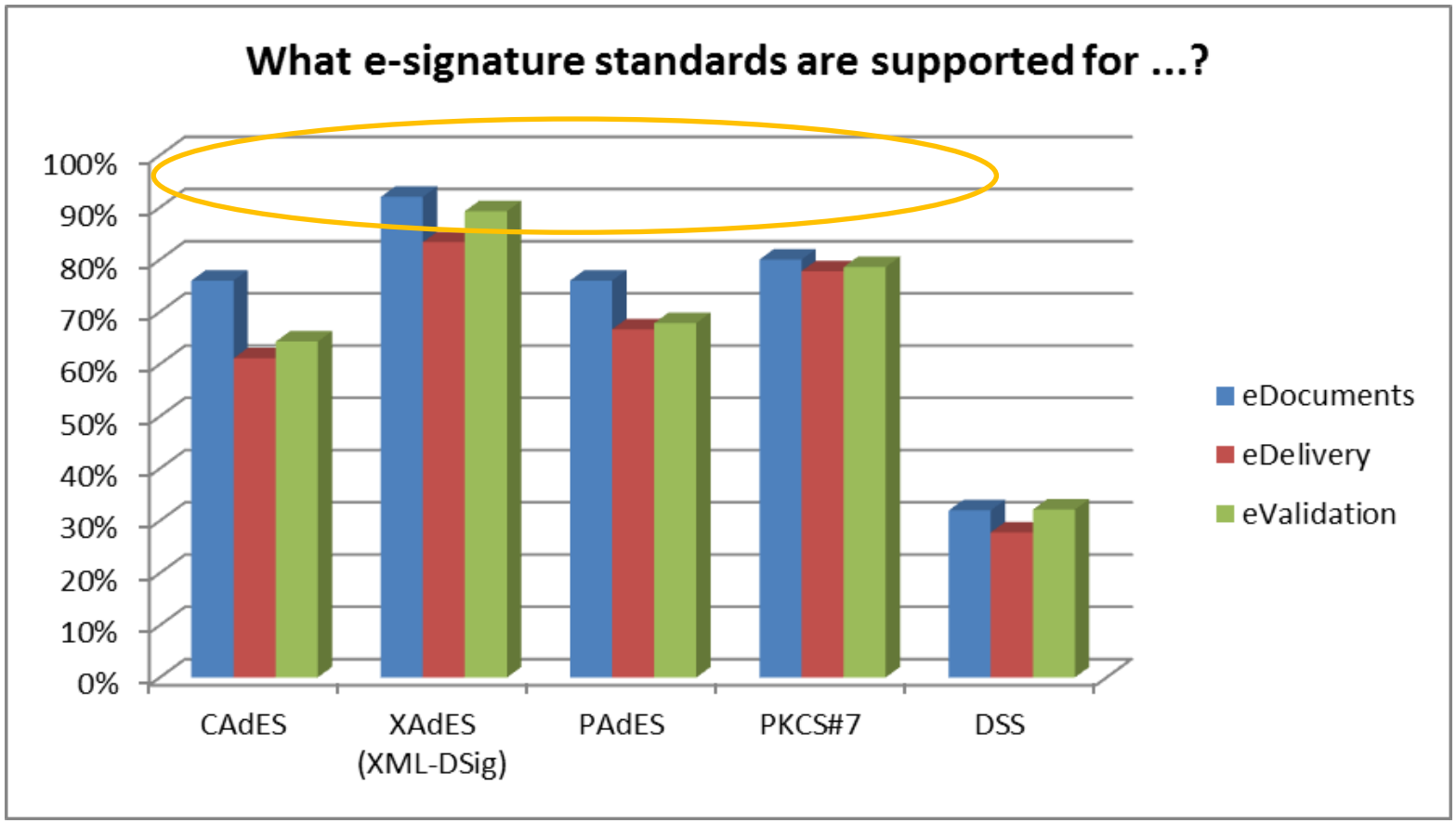
REC. BCM standards should be promoted to address the 'unavailability of the services' type of risk.

Standards: Audits





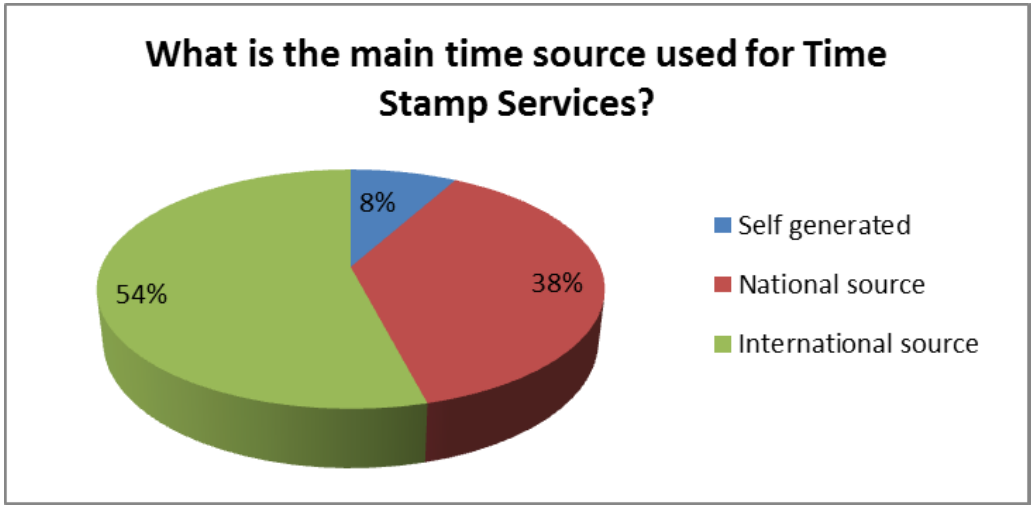
Standards: e-Signature standards

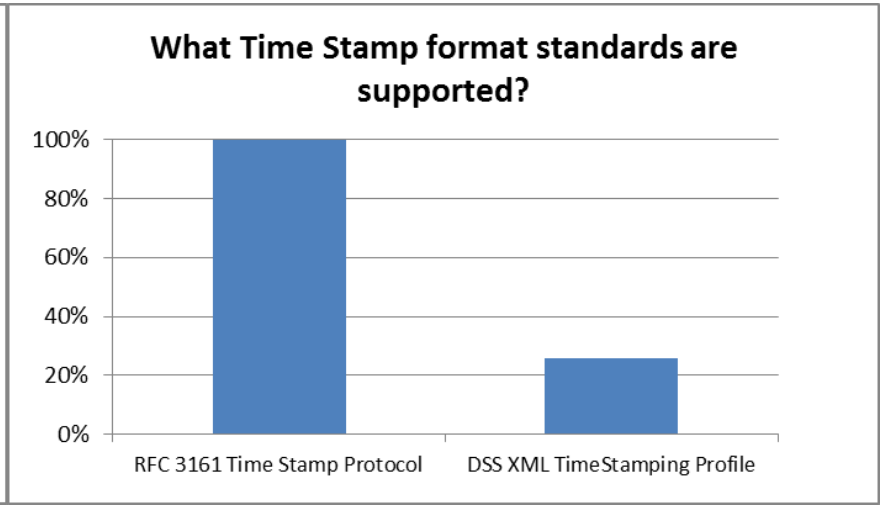


REC. Achieve full interoperability, reaching the 100% of acceptance of standards.

Standards: Time Stamping services

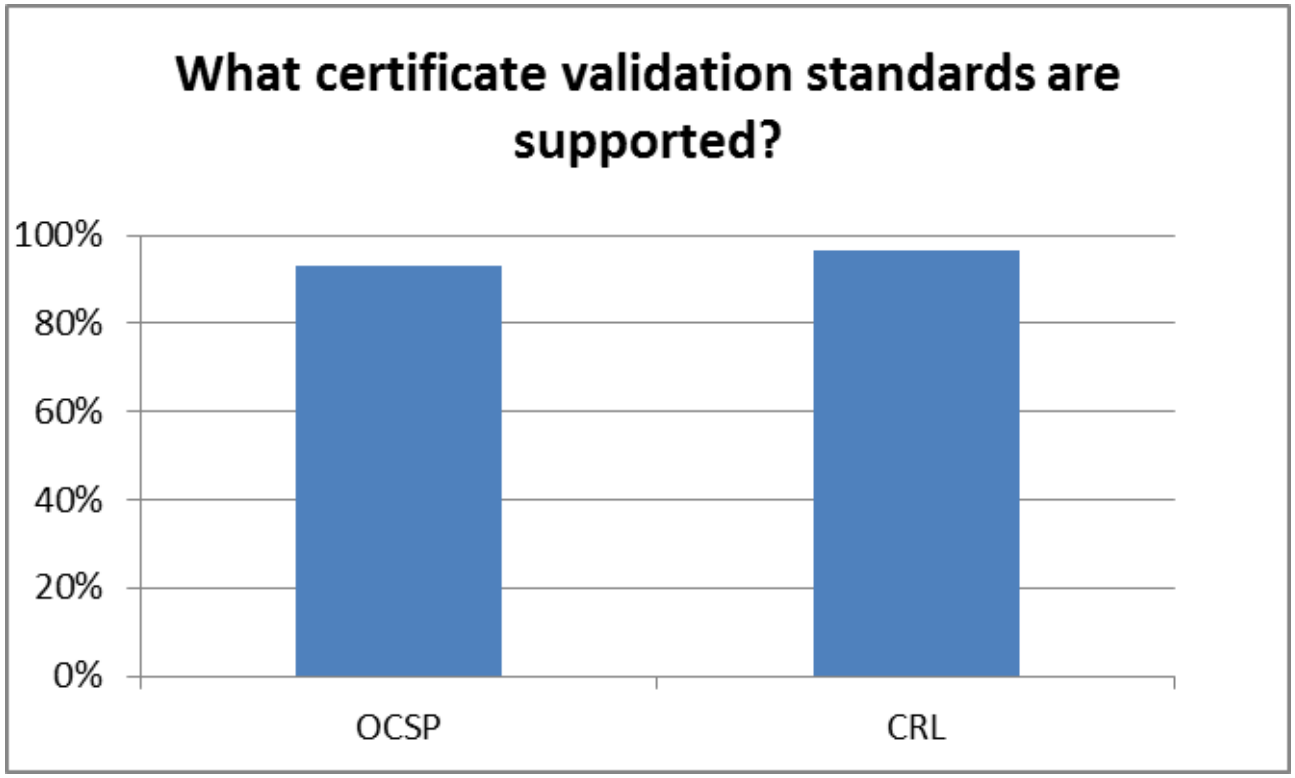
This is the service most offered in the survey (93%).





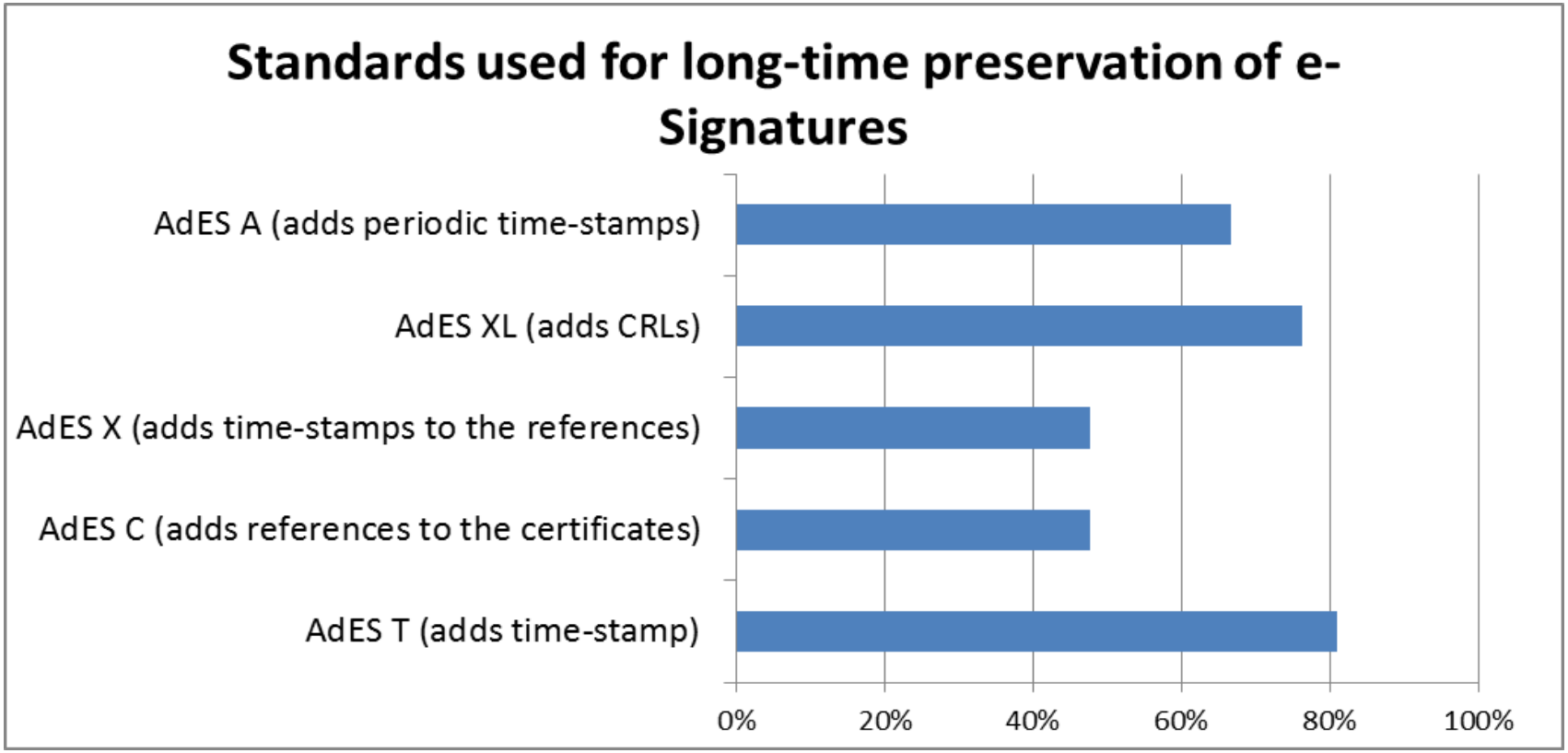
REC. Although self-generated main time source is low used, it should be taken into consideration in the specification of the quality of a Time Stamping service.

Standards: Validation services



Standards: Long Time Preservation services

Adding CRL/certificates is preferred more than only references



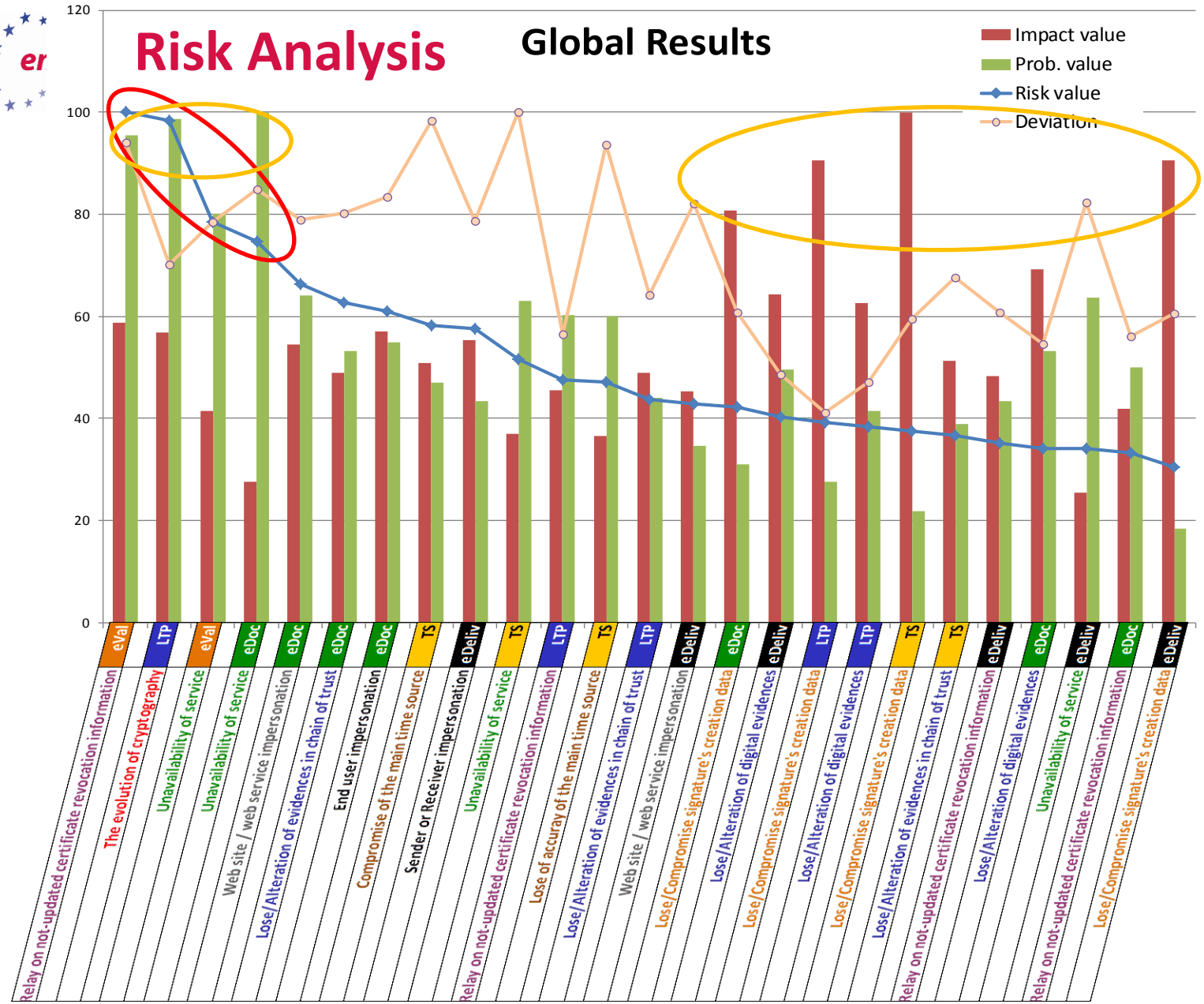
REC. The dispersion of standards used implies that best practices must be defined.

Risk Analysis

- Probability, Impact and Risk Values have been normalised to 100% for uniformity.
- 100% means the worst, but in most cases has been reported as 3/5, i.e. medium probability or impact.
- The aim is to identify areas where actions need to be taken, because they are weakest of the scenario.
- Deviation of responses indicates:
  - Confidence of the result.
  - Need to harmonise views.
  - Need of guidelines implementation.

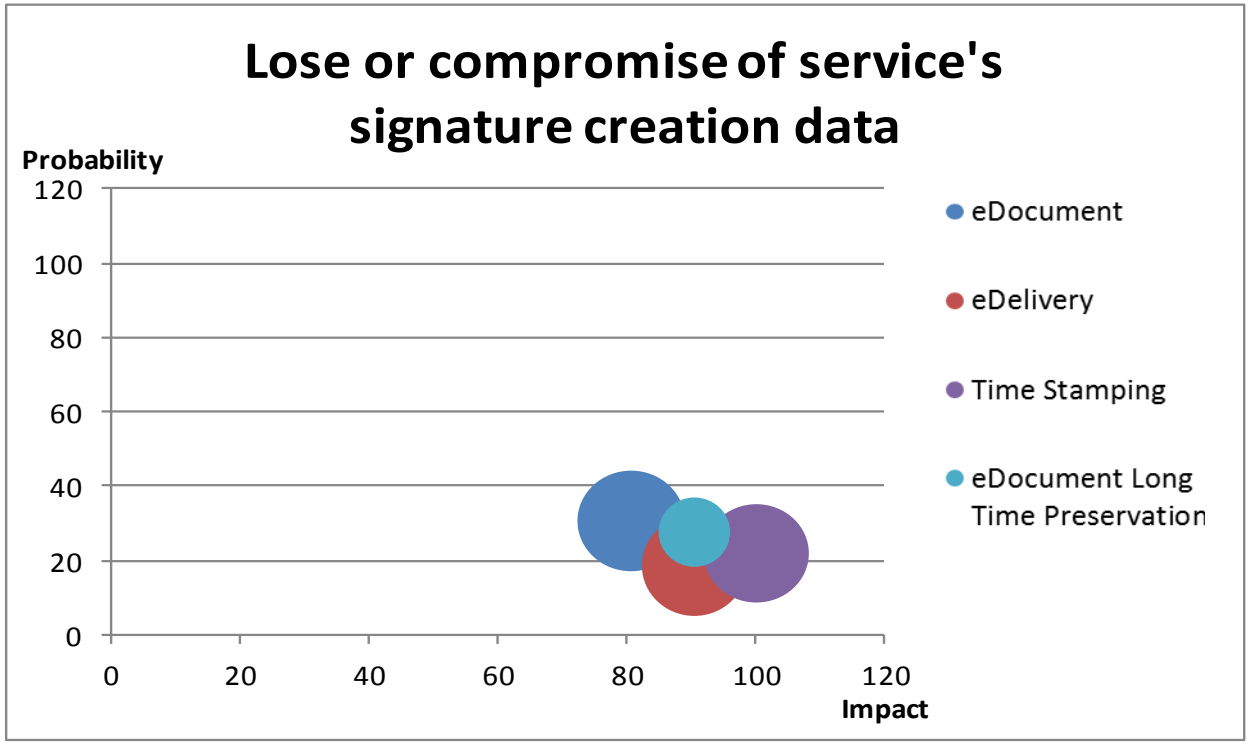
Risk Analysis

Global Results



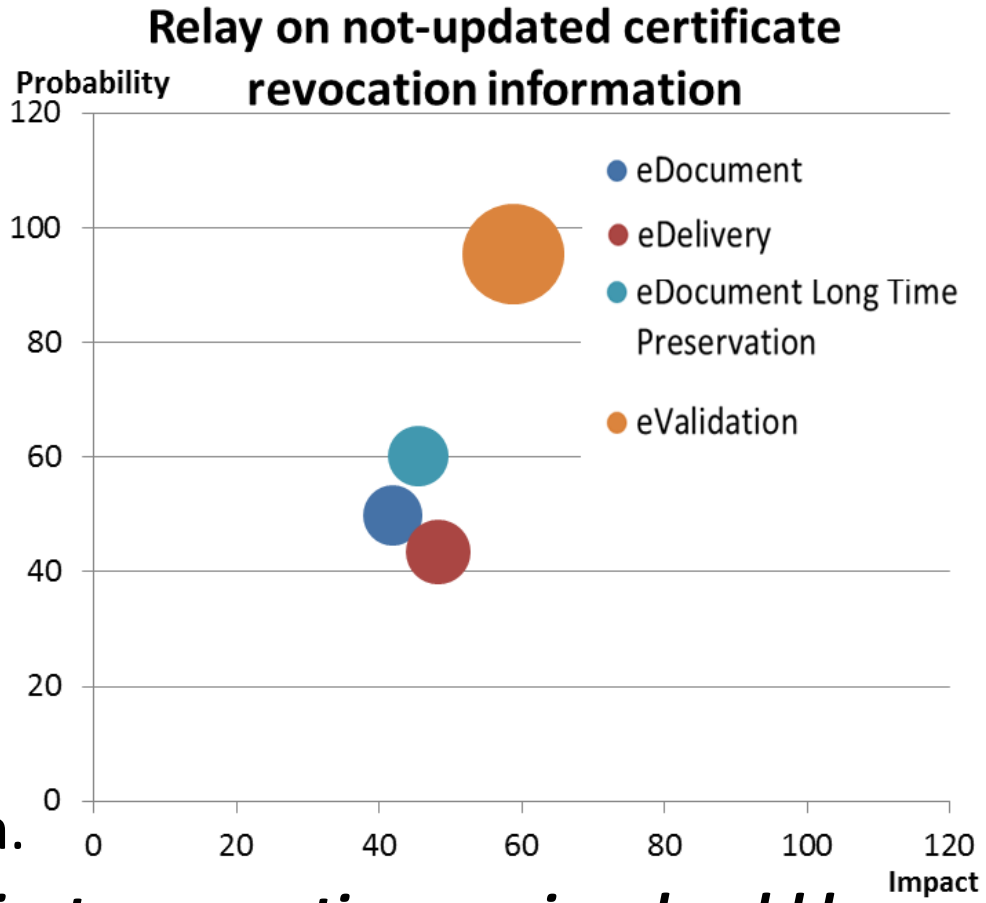
Risk Analysis

- **Lose or compromise of service's signature creation data**: high impact, but low probability and risk.
  - Adequate measures to prevent it are taken.



Risk Analysis

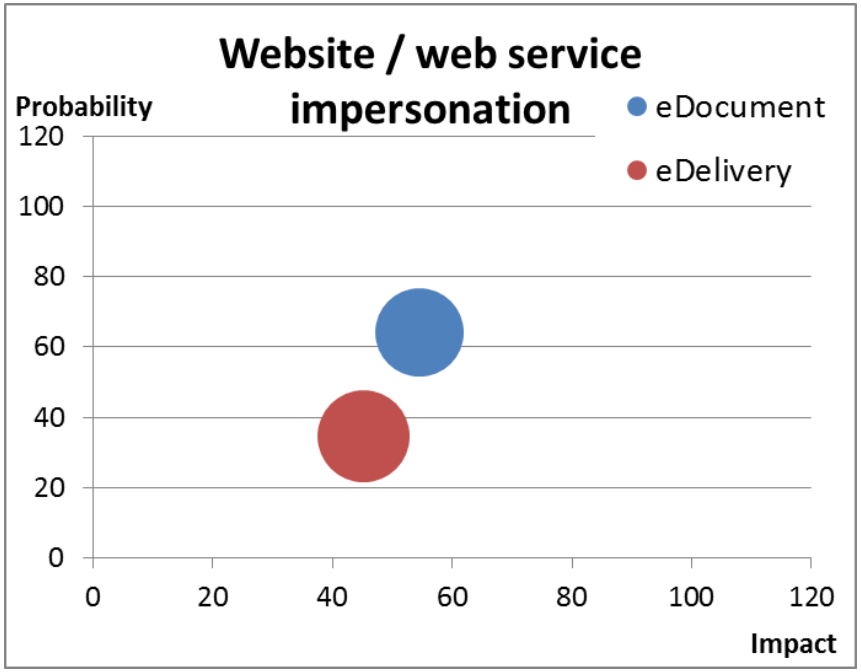
- **Relay on not-updated certificate revocation information** in **eValidation**: high risk and probability
  - Measures are taken: services through CRLs and OCSP, but they still don't rely on the quality of the information.

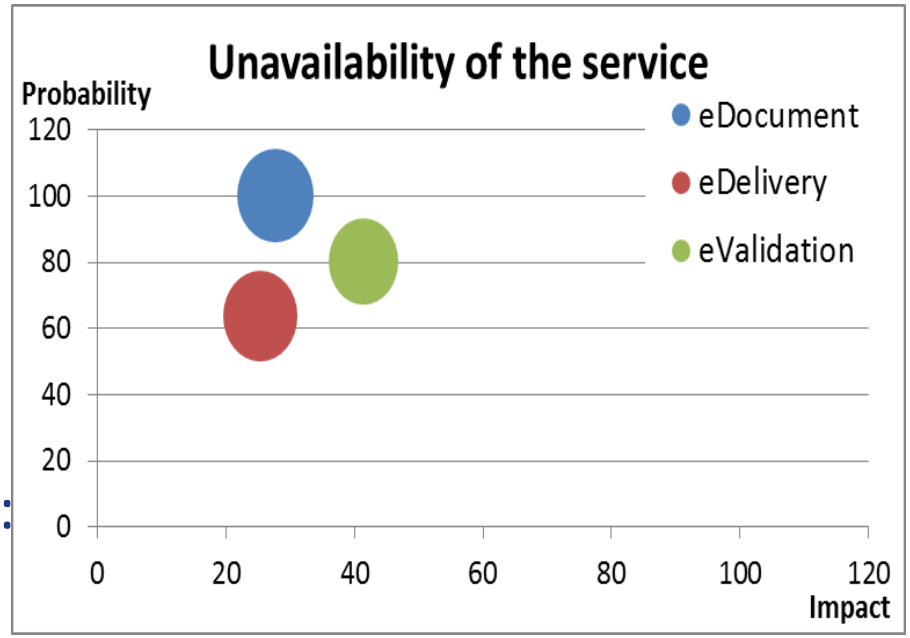


  - ***REC. Quality of the certificate revocation service should be guaranteed, to allow eVal. services to trust more on them.***
  - In LTP & eDeliv. Probability of this Risk is much lower, because these services are offered to customers close to the service provider, using credentials issued by close TSP.

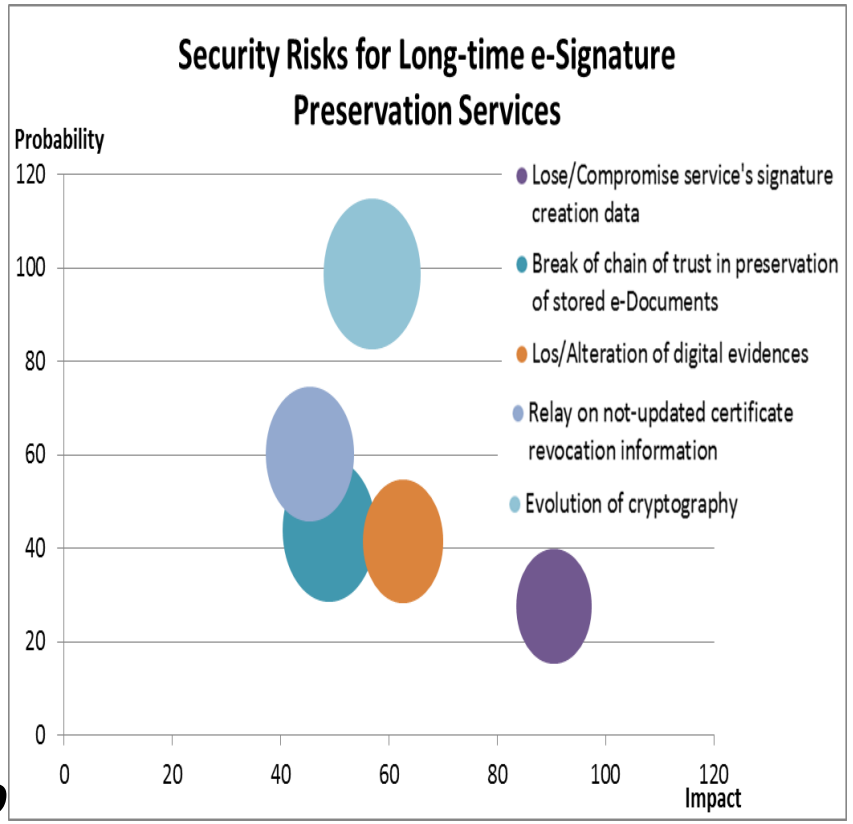
Risk Analysis

- **Web site / web service impersonation** for **eDocuments**: high probabil. /high impact:
  - User training and awareness about the risk.
  - Use of strong credentials in client and server.
  - Promoting the implementation of clients to be executed in the customer computer with web-service access to TSP.
- **Unavailability of the service** has also high risk, due to high probabil.:
  - Cloud hosting service providers.





Risk Analysis



- **Evolution of cryptography** in **Long Time Preservation**: high risk and probability
  - It is out of control: Difficult to anticipate the evolution of algorithms.
  - ***REC: The use of two algorithms will help, because breaking two algorithms at the same time is less probable.***
- **Electronic Time Stamp**
  - Compromise of the main time source & Unavailability of the main time source have large dispersion of values.
  - ***REC. Promote the use of internationally trusted time sources and define best practices to standardize the QoS through SLAs.***

Recommendations summary

- **Cross-border interoperability of credentials** has to be promoted.
- The **strength of the authentication mechanism** should be proportional to the criticality of the accessed services, both in client and server.
- CSP **Certification schemas** could be extended to **other TSP services** to have harmonised criteria of QoS and SLA guidelines.
- Promote the use of **internationally trusted main time sources** and define best practices to standardize the QoS through SLAs. Although self-generated main time source is low used, it should be taken into consideration in the specification of the quality of a Time Stamping service.
- Focus on user **training and awareness** to prevent 'Web site / web service impersonation' for **eDocuments**.

Pending issues

- In relation with the **platform used**, promote the implementation of **clients to be executed in the customer** computer with **web-service access to TSP** (https unsafe).
- The impact of **storing eDocs** in the adequate **security mechanisms** to be adopted recommends to **define different profiles of the service provision** in each case.
- **BCM standards** should be promoted to address 'unavailability of the services' type of risk / Use **Cloud hosting service** providers to prevent unavailability.

Pending issues

- Achieve **full interoperability**, reaching the 100% of acceptance of **eSignature standards**.
- The dispersion of standards used in **LTP services** implies that best practices about standards adopted must be defined.
- Quality of the certificate revocation service should be guaranteed, to allow **e-Validation services** to trust more on them.
- The use of **two PKI/Hash algorithms** will help to prevent cryptanalysis , because breaking two algorithms at same time is less probable.

Thank you

Follow ENISA: