EUROPEAN MULTI-STAKEHOLDER PLATFORM (MSP) ON ICT STANDARDISATION

Alain Wahl
OBJECTIVES OF THIS PRESENTATION

• Understand the role of the European MSP on ICT Standardisation
• Understand the objective of the Rolling Plan for ICT Standardisation
• Awareness of standard activities in different ICT fields
• Understand the benefits of using ICT standards
• Understand the European legislation and standardisation activities related to electronic identification and trust services including e-signatures
• Promote use and implementation of ICT standards in your company
• Encourage your participation in the standardisation process
European Multi-Stakeholder Platform on ICT Standardisation

Rolling Plan for ICT Standardisation

- Societal challenges
  - eHealth
- Innovation for the Digital Single Market
  - e-Invoicing; Card, Internet and Mobile Payments
- Sustainable growth
  - Smart Grids and Smart Metering
  - Smart Cities / Technologies and Services for a Smart and Efficient Energy Use
- Key enablers and security
  - Cloud computing; Internet of Things; Network and Information Security
  - Electronic identification and trust services including e-signatures
European Multi-Stakeholder Platform on ICT Standardisation

Rolling Plan for ICT Standardisation

• Societal challenges
  o eHealth
• Innovation for the Digital Single Market
  o e-Invoicing; Card, Internet and Mobile Payments
• Sustainable growth
  o Smart Grids and Smart Metering
  o Smart Cities / Technologies and Services for a Smart and Efficient Energy Use
• Key enablers and security
  o Cloud computing; Internet of Things; Network and Information Security
  o Electronic identification and trust services including e-signatures
OBJECTIVES

- Increase interoperability
- Promote the use of standards and specifications
- Industry preference/need for global standards
- Ensure availability of required standards and specifications for public authorities
- Provides public authorities with the certainty that with the use of the specs their “public interest” expectations are met
- Recognized specifications are not European Standards
- Specifications suitable for referencing, use remains voluntary, made available (recommended) for use in policies and legislation
ORGANISATION

European Multi-Stakeholder Platform on ICT Standardisation

- 4 meetings per year; first meeting March 2012
- Possibility to create sub-groups
- Experts and observers may be invited

Rolling Plan for ICT Standardisation

- Current version of the Rolling Plan for ICT Standardisation from 2015
- To be updated at least once a year by the Commission, in collaboration with the MSP
MSP ON ICT STANDARDISATION
Rolling Plan for ICT Standardisation

STAKEHOLDERS

- European Institutions
- Administrations of Member States (~50% of the Platform members)
- European and international ICT standardisation bodies active in Europe: CEN, CENELEC, ETSI, ISO, IEC, ITU, …
- Citizens, experts
- Industry, businesses, SME
- Non-Governmental Organisations
- Persons or organisations with any legitimate interest
- Invitations to MS to nominate participants
MSP ON ICT STANDARDSATION
Rolling Plan for ICT Standardisation

TASKS

European Multi-Stakeholder Platform on ICT Standardisation

• Advise the European Commission on ICT standards work program
• Identify future ICT standardisation needs from policies and legislation
• Advise the European Commission on possible ICT standardisation mandates
• Inform Commission on progress in ICT standardisation activities
• Any other issue concerning support for ICT interoperability

Rolling Plan for ICT Standardisation

• Defines the most important standardisation initiatives and actions supporting EU policies
• As the 2010-2013 ICT standardisation work program, its predecessor, the Rolling plan is a Commission document, written in collaboration with & advised by the MSP
MSP ON ICT STANDARDISATION
Rolling Plan for ICT Standardisation

THE STRATEGIC ROLE OF ICT STANDARDISATION IN THE CONTEXT OF EU POLICY MAKING

• Identifies EU policy priorities where ICT standards should be considered as part of policy making (mostly from the EC)
• Rolling plan identifies areas for action at the standardisation landscape
• Make sure state-of-the-art technologies get implemented
• European standards developed by CEN, CENELEC and ETSI
• Standards developed by global industry-driven ICT fora and consortia
• Standards used in support of industrial or innovation policy
• Standards play a role in EU Research and Innovation
• Standards take an important role in government internal policies and public procurement
Rolling Plan for ICT Standardisation

PROMOTING THE IMPLEMENTATION OF STANDARDS

The use of standardisation in support of policy making
• Create awareness of importance of standards

Public procurement
• Identifies available standards in areas with policy relevance
• Diminish lock-in

Research and Innovation
• Source of new standards
• Standardisation awareness in R&I

Testing and quality improvement in standards
• Ensure that there are products implementing the standards
• To enable interoperability in a multi-vendor environment
Rolling Plan for ICT Standardisation

SUMMARY

European Multi-Stakeholder Platform on ICT Standardisation

Rolling Plan for ICT Standardisation

- Societal challenges
  - eHealth
- Innovation for the Digital Single Market
  - e-Invoicing; Card, Internet and Mobile Payments
- Sustainable growth
  - Smart Grids and Smart Metering
  - Smart Cities / Technologies and Services for a Smart and Efficient Energy Use
- Key enablers and security
  - Cloud computing; Internet of Things; Network and Information Security
  - Electronic identification and trust services including e-signatures
MSP ON ICT STANDARDSATION
Rolling Plan for ICT Standardisation

SUMMARY

European Multi-Stakeholder Platform on ICT Standardisation

Rolling Plan for ICT Standardisation

- Societal challenges
  - eHealth
- Innovation for the Digital Single Market
  - e-Invoicing; Card, Internet and Mobile Payments
- Sustainable growth
  - Smart Grids and Smart Metering
  - Smart Cities / Technologies and Services for a Smart and Efficient Energy Use
- Key enablers and security
  - Cloud computing; Internet of Things; Network and Information Security
  - Electronic identification and trust services including e-signatures
EU POLICY AREAS

Societal challenges

- eHealth
- Active and Healthy Ageing
- Accessibility of ICT products and services and Web Accessibility
- e-Skills and e-Learning
- Emergency communications
- eCall
Rolling Plan for ICT Standardisation

E-HEALTH

- ICT applied to health and healthcare systems can increase their efficiency
- Lack of interoperability between eHealth systems
- Related ongoing standardisation and research activities
  - CEN – Technical Committee 251 – Health Informatics: providing a focal point for standards in this domain, in close collaboration with ISO C215
  - ETSI – develops DECT ULE, a low power wireless technology providing optimal radio coverage in indoor scenarios for reliable audio and data services suitable for many eHealth applications, e.g. health monitoring, emergency alarms for vulnerable people and remote medical monitoring
    ETSI Project (EP) eHealth provides a focus point in ETSI on issues such as mHealth and telemedicine. Development of standards to facilitate telemedicine and the “Internet Clinic”
  - EMA – pharmaco-vigilance database in order to use it for ePrescriptions
SUMMARY

European Multi-Stakeholder Platform on ICT Standardisation

Rolling Plan for ICT Standardisation

- Societal challenges
  - eHealth
- Innovation for the Digital Single Market
  - e-Invoicing; Card, Internet and Mobile Payments
- Sustainable growth
  - Smart Grids and Smart Metering
  - Smart Cities / Technologies and Services for a Smart and Efficient Energy Use
- Key enablers and security
  - Cloud computing; Internet of Things; Network and Information Security
  - Electronic identification and trust services including e-signatures
MSP ON ICT STANDARDDISATION
Rolling Plan for ICT Standardisation

INNOVATION FOR THE DIGITAL SINGLE MARKET

- e-Procurement – Pre and Post award
- e-Invoicing
- Card, Internet and Mobile Payments
- eXtensible Business Reporting Language (XBRL)
- Online Dispute Resolution (ODR)
E-INVOICING

- Invoice, transmitted and received in a structured electronic data
- Automatic and electronic processing
- Increased efficiency, faster payments, reduced environmental impact
- EDI (Electronic Data Interchange): earliest form of e-invoicing, still used
- New e-invoicing standards, based on different versions of XML
- Vast number of e-invoicing standards (many proprietary standards), data formats exist across EU
- Related ongoing standardisation and research activities
  - CEN Project Committees: CEN/PC 434 and CEN/PC 440
  - UN/CEFACT Cross-Industry Invoice
  - ISO Adoption of Universal Business Language (UBL) Version 2.1 is ongoing
CARD, INTERNET AND MOBILE PAYMENTS

- Payments involving mobile phone, gain importance
- Mobile connected devices exceed the number of people on earth
- Based on card payments, credit transfer, direct debits or pre-funded cards and accounts
- Absence of shared standards, standardisation gaps, lack of interoperability
- Related ongoing standardisation and research activities
  - Industry organisations: European Payment Council, Global Platform (Near Field Communication, NFC)
  - ETSI: Smart Secure Platform (SSP)
  - ITU-T: Recommendations on secure mobile payments and mobile banking solutions
  - W3C: Forum for Web Payments technical discussions
  - ISO TC68/SC7/WG10: Mobile payments WG
  - EPASOrg and EPC: protocols for card payment in Eurozone
MSP ON ICT STANDAR DISATION
Rolling Plan for ICT Standardisation

SUMMARY

European Multi-Stakeholder Platform on ICT Standardisation

Rolling Plan for ICT Standardisation

• Societal challenges
  o eHealth
• Innovation for the Digital Single Market
  o e-Invoicing; Card, Internet and Mobile Payments
• Sustainable growth
  o Smart Grids and Smart Metering
  o Smart Cities / Technologies and Services for a Smart and Efficient Energy Use
• Key enablers and security
  o Cloud computing; Internet of Things; Network and Information Security
  o Electronic identification and trust services including e-signatures
MSP ON ICT STANDARDISATION
Rolling Plan for ICT Standardisation

SUSTAINABLE GROWTH

- Smart Grids and Smart Metering
- Smart Cities / Technologies and Services for a Smart and Efficient Energy Use
- ICT Environmental Impact
- European Electronic Toll Service (EETS)
- Intelligent Transport Systems (ITS)
- Advanced Manufacturing
SMART GRIDS AND SMART METERING

- EU ambition: develop a low-carbon economy
- Upgraded electricity network, backbone of power system
- Two-way digital communication between supplier and consumer
- Intelligent metering and monitoring systems, remote operation of meters
- Related ongoing standardisation and research activities
  - ESOs: EC mandate 490 (Smart grids technologies) completed in 2015
    Smart Meters Coordination Group (SM-CG)
    Electro-mobility work program, standards for the charging of electric vehicles
  - IEC: Committee on Smart Energy
  - IEEE, ITU-T, OASIS, IETF are also active in this field
SMART CITIES / TECHNOLOGIES AND SERVICES FOR A SMART AND EFFICIENT ENERGY USE

- Construction sector: highest energy consumer in the EU (~40%)
- Controlling the efficient consumption of energy at buildings
- Related ongoing standardisation and research activities
  - SEMANCO is developing a Semantic Energy Information Framework to model the energy-related knowledge planners
  - eeSemantics (stakeholders group launched by DG CONNECT): active in the area of Building Energy Management Systems
  - “Stimulating industrial innovation in the construction sector through smart use of ICT” project of DG GROW
  - ISO, IEC: TC 268 “Sustainable development in communities”
SUMMARY

European Multi-Stakeholder Platform on ICT Standardisation

Rolling Plan for ICT Standardisation

- Societal challenges
  - eHealth
- Innovation for the Digital Single Market
  - e-Invoicing; Card, Internet and Mobile Payments
- Sustainable growth
  - Smart Grids and Smart Metering
  - Smart Cities / Technologies and Services for a Smart and Efficient Energy Use
- Key enablers and security
  - Cloud computing; Internet of Things; Network and Information Security
  - Electronic identification and trust services including e-signatures
KEY ENABLERS AND SECURITY

- Cloud computing
- Public Sector Information, Open Data and Big Data
- eGovernment
  - DCAT Application profile for data portals in Europe
  - Exchange of metadata on re-usable interoperability assets (eGovernment)
  - Core Concepts to facilitate the development of interoperable solutions
KEY ENABLERS AND SECURITY

- Electronic identification and trust services including e-signatures
- Radio Frequency Identification (RFID)
- Internet of Things
- Network and Information Security
- ePrivacy
- E-Infrastructures for Research Data and Computer-Intensive Science
- Broadband Infrastructure Mapping
- Preservation of digital cinema
MSP ON ICT STANDARDISATION
Rolling Plan for ICT Standardisation

CLOUD COMPUTING

• Establish a coherent framework for Cloud Computing
• Related ongoing standardisation and research activities
  o ETSI Cloud Standards Coordination (see http://csc.etsi.org)
  o Cloud Standards Customer Council (see www.cloud-council.org)
  o Distributed Management Task Force (see www.dmtf.org/standards/cloud)
  o ETSI – TC CLOUD (see www.etsi.org/technologies-clusters/technologies/grid-and-cloud-computing)
  o ISO/IEC – JTC 1/SC 38
  o …
INTERNET OF THINGS

- Dynamic global network infrastructure
- Physical and virtual "things" have identities, physical attributes and virtual personalities
- Connect these “things” to data networks
- Related ongoing standardisation and research activities
  - Internet of Things Research in Europe Cluster (IERC) that are dealing with aspects of the standardisation in IoT
  - Future Internet PPP (FI-PPP) deals with some issues connected to the standardisation of the IoT
  - Focus group in ISO/IEC JTC 1
  - ...

Rolling Plan for ICT Standardisation
NETWORK AND INFORMATION SECURITY

- Network and Information Security Public-Private Platform has been implemented by the Commission with representation of all stakeholders

- Related ongoing standardisation and research activities
  - CEN, CENELEC and ETSI have set up a Cyber Security Coordination Group. The CSCG and the NIS Public-Private Platform will regularly update the MSP on stakeholder requirements and advise the MSP.
  - OASIS hosts the PKCS 11 standardisation project for cryptographic tokens controlling authentication information (see www.oasis-open.org/committees/pkcs11) and the Key Management Interoperability Protocol (KMIP) (see www.oasis-open.org/committees/kmip)
  - IEEE has standardization activities in the network and information security space, including in the encryption, fixed and removable storage
MSP ON ICT STANDARDISATION
Rolling Plan for ICT Standardisation

ELECTRONIC IDENTIFICATION AND TRUST SERVICES INCLUDING E-SIGNATURES


• Related ongoing standardisation and research activities
  o ETSI: Trusted Lists (ETSI TS 119 612) and signature formats (CAdES, CAdES profile, ASiC, and ASiC profile)
  o e-SENS (Electronic Simple European Networked Services): eID, eDocuments, eDelivery, and eSignature etc. for a pan-European digital platform for cross-sector, interoperable eGovernment services
  o STORK: eID Interoperability Platform

  ...
MSP ON ICT STANDARDISATION
Rolling Plan for ICT Standardisation

EIDAS REGULATION (EU) NO 910/2014

Objective

• Strengthen EU Single Market by boosting TRUST and CONVENIENCE in secure and seamless cross-border electronic transactions
MSP ON ICT STANDARDSATION
Rolling Plan for ICT Standardisation

EIDAS REGULATION (EU) NO 910/2014

• Mutual recognition of e-identification means

• Electronic trust services
  o Electronic signatures
  o Electronic seals
  o Time stamping
  o Electronic registered delivery service
  o Website authentication.

• Electronic documents
EIDAS REGULATION (EU) NO 910/2014

- Provides legal certainty and fosters the usage of eID means for on-line access (not regulated at EU level before)
- Addresses all the stages of a generic e-transaction, from the authentication of a web site to preservation
- Provides the legal framework for a comprehensive “toolbox” of mechanisms and services to boost trust and confidence in electronic transactions
- Takes a risk management perspective, not based on normative rules but on principles:
  - Transparency and accountability: well-defined minimal obligations for TSPs and liability
  - Trustworthiness of the services together with security requirements for TSPs
  - Light-touch reactive monitoring for TSPs vs. full-fledged supervision for QTSPs
  - Technological neutrality: avoiding requirements which could only be met by a specific technology
  - Market rules and building on standardisation
- Provides one set of rules directly applicable across all EU MS (regulation, 1 DA and 28 IA)
EIDAS REGULATION (EU) NO 910/2014

Mandatory recognition of electronic identification

Voluntary notification of eID schemes

"Cooperation and interoperability" mechanism

Assurance Levels: "high" and "substantial" (and "low")

Interoperability framework

Access to authentication capabilities: free of charge for public sector bodies & according to national rules for private sector relying parties
MSP ON ICT STANDARDISATION
Rolling Plan for ICT Standardisation

EIDAS REGULATION (EU) NO 910/2014

Trust services

Horizontal principles: Liability; Supervision; International aspects; Security requirements; data protection; Qualified services; Prior authorisation; trusted lists; EU trust mark

- Electronic signatures, including validation and preservation services
- Electronic seals, including validation and preservation services
- Time stamping
- Electronic registered delivery service
- Website authentication
EIDAS REGULATION (EU) NO 910/2014

E-Transactions workflow – Submitting a tax declaration

**Website authentication:** check if the website you enter is really linked to the tax authority.

**eID:** identify (or authenticate) yourself using, for instance, an eID means

**Creation of the tax declaration**

**E-registered delivery:** Tax authority sends acknowledgement of receipt

**Time stamp:** Proof of submission of the tax declaration in due time

**E-signature/ e-seal:** Signing or Sealing the tax declaration

**Preservation:** storage of the tax declaration and acknowledgment of receipt
MSP ON ICT STANDARDISATION
Rolling Plan for ICT Standardisation

EIDAS REGULATION (EU) NO 910/2014

Timeline of implementation

- **2014**: Entry into force of the Regulation
- **2015**: Voluntary recognition eIDs
- **2016**: Date of application of rules for trust services
- **2017**: Mandatory recognition of eIDs
- **2018**:
- **2019**:

---

**ILNAS**
Scope

- Specifies general policy requirements relating to trust service providers (TSPs)
  - Issuance of public key certificates
  - Provision of registration services
  - Time-stamping services
  - Long term preservation services
  - E-delivery services
  - Signature validation services
  - Other type of trust service provider

- Defines policy requirements on the operation and management practices of TSPs.

- Does not specify how the requirements can be assessed by an independent party
  - See ETSI EN 319 403 Requirements for conformity assessment bodies assessing TSPs
The following references documents are not necessary for the application of the standard but they assist the user with regard to a particular subject area:

- Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- CA/Browser Forum – Guidelines for the issuance and management of extended validation certificates
References

- The following references documents are not necessary for the application of the standard but they assist the user with regard to a particular subject area:
  - ETSI EN 319 403 – Electronic signatures and Infrastructures – Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers
  - CA/Browser Forum – Network and certificate system security requirements
  - ETSI TS 119 112 – Electronic Signatures and Infrastructures – cryptographic suites
  - ETSI EN 319 411-1 Policy and Security Requirements for Trust Service Providers issuing certificates – Part 1 : General requirements
  - ETSI EN 301 549 – Accessibility requirements suitable for public procurement of ICT products and services in Europe
Definitions

- Relying party: natural or legal person that relies upon an electronic identification of trust service
- Subscriber: legal or natural person bound by agreement with a trust service provider to nay subscriber obligation
- Trust service: electronic service which enhances trust and confidence in electronic transactions
- Trust service policy: set of rules that indicates the applicability of a trust service to a particular community and/or class of application with common security requirements
- Trust service practice statement: statement of the practices that a TSP employs in providing a trust service
- Trust service provider: entity which provides one or more trust services
MSP ON ICT STANDARDISATION
Rolling Plan for ICT Standardisation

DRAFT ETSI EN 319 401 V2.0.0 (2015-06)
GENERAL POLICY REQUIREMENTS FOR TSP

Abbreviations

- CA  Certification authority
- IP  Internet Protocol
- IT  Information technology
- TSP Trust Service Provider
- UTC Coordinated Universal Time
Risk Assessment

- The TSP shall carry out a risk assessment to
  - Identify
  - Analyse
  - Evaluate
  - Treat

- Trust service risks taking into account business and technical issues

- See ISO/IEC 27005:2011
Trust Service Practice (TSP) statement

- Shall have a statement of the practices and procedures used to address all the requirements identified for the applicable TSP policy
- Shall identify the obligations of all external organisations supporting the TSP services
- Shall make available to subscribers and relying parties its practice statement
- Shall have a management body with overall responsibility for the TSP practices
- Shall define a review process for the practices
- Shall notify notice of practice changes
- Shall state in its practices the provisions made for termination of service
Terms and Conditions

- The trust service policy being applied
- Any limitations on the use of the service and the subscriber’s obligations
- Information for parties relying on the trust service
- The period of time during which TSP event logs are retained
- Limitations of liability
- The applicable legal system
- Procedures for complaints and dispute settlement and the TSP contact information
- Whether the TSP’s trust service has been assessed to be conformant with trust service policy
Information security policy

• Documented, implemented and maintained

• Shall retain overall responsibility for conformance with the procedures within its security policy

• Shall be reviewed at planned intervals or if significant changes occur

• A TSP’s management security policy shall be documented, implemented and maintained including security controls and operating procedures for TSP facilities

See ISO/IEC 27002:2013 clause 5.1.1 for guidance
Internal organization

• Reliability
  o Trust service practices shall be non-discriminatory
  o The TSP shall make its services accessible to all applicants
  o The TSP shall maintain sufficient financial resources and obtain appropriate liability insurance in accordance with national law
  o The TSP shall have financial stability and resources required to operate in conformity with its policy
  o The TSP shall have policies and procedures for the resolution of complaints and disputes
  o The TSP shall have a documented agreement and contractual relationship in place

• Segregation of duties
  o Duties and responsibilities shall be segregated to reduce misuse of the TSP assets
Human resources

- Necessary expertise, reliability, experience and qualifications
- Should be able to fulfil the requirement of “expert knowledge, experience and qualifications”
- Appropriate disciplinary sanctions shall be applied when violating TSP policies or procedures
- Security roles and responsibilities shall be documented in job descriptions
- TSP personnel shall have job descriptions defined from the roles they fulfil
- Procedures in line with information security management procedures
- Managerial personnel shall possess experience or training with the trust service that is provided
- Shall be free from conflict of interest that might prejudice the impartiality of the TSP operations
Asset management

- General requirements
  - The TSP shall ensure an appropriate level of protection of its assets
  - The TSP shall maintain an inventory of all information assets and shall assign a classification consistent with the risk assessment

- Media handling
  - All media shall be handled securely in accordance with the requirements of the information classification scheme
Access control

- Controls (e.g. firewalls) shall protect the TSP’s internal network domains from unauthorized access

- The TSP shall administer user access of operators, administrators and system auditors

- Access to information and application system functions shall be restricted in accordance with the access control policy

- TSP personnel shall be identified and authenticated before using critical applications related to service

- TSP personnel shall be accountable for their activities

- Sensitive data shall be protected against being revealed through re-used storage objects being accessible to unauthorized users
Cryptographic controls

• Appropriate security controls shall be in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle

Physical and environmental security

• Physical access to components of the TSP’s system whose security is critical to the provision of its trust services shall be limited to authorized individuals

• Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities

• Controls shall be implemented to avoid compromise or theft of information and information processing facilities

• Critical components shall be located in a protected security perimeter
Operation security

• An analysis of security requirements shall be carried out at the design and requirements stage of any system development project.

• Change control procedures shall be applied for releases, modifications of any operational software.

• The integrity of TSP systems and information shall be securely handled to protect media from damage, theft, any unauthorized access and obsolescence.

• Media management procedures shall protect against obsolescence and deterioration of media.

• Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services.

• Shall specify and apply procedures for ensuring security patches are applied within a reasonable time after they come available.
Network security

- Shall segment systems into networks or zones based on risk assessment
- Restrict access and communications between zones to those necessary for the operation
- Maintain any elements of their critical systems (e.g. Root CA systems) in a secured zone
- Dedicated network for administration of IT systems that is separated from the operational network
- Test platform and production platform shall be separated from other environments
- Communication between trustworthy systems shall only be established through trusted channels
- External network connection to the internet shall be redundant to ensure availability of services
- Perform regular vulnerability scan on public and private IP addresses and a penetration test
Incident management

- Monitoring activities should take account of the sensitivity of information
- Abnormal system activities that indicate a potential security violation, shall be reported
- The TSP IT systems shall monitor events (Availability and utilization of needed services, …)
- Respond quickly to incidents and to limit the impact of breaches of security
- The TSP shall establish procedures to notify the appropriate parties
- TSP shall also notify the natural or legal person of the breach of security or loss of integrity
- Audit logs shall be monitored or reviewed regularly to identify evidence of malicious activity
- The TSP shall remediate within a reasonable period after the discovery of a critical vulnerability
Collection of evidence

- Confidentiality and integrity of records shall be maintained.
- Records concerning the operation of services shall be completely and confidentially archived.
- Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.
- The precise time of significant TSP environmental, key management and clock synchronization events shall be recorded.
- Records concerning services shall be held for a period of time after the expiration of the validity of the signing keys or any trust service token as appropriate for providing necessary legal evidence.
- Events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.
Business continuity management

• In the event of a disaster, including compromise of the private signing key or trust service credentials, operations shall be restored as soon as possible

• TSP shall define and maintain a continuity plan to enact in case of a disaster
  
  o Other disaster situations include failure of critical components of a TSP trustworthy system, including hardware and software
  
  o See clause 17 of ISO/IEC 27002:2013 [i.3] for guidance
TSP termination and termination plans

- The TSP shall have an up-to-date termination plan
- Inform the following of the termination: all subscribers and other interested entities
- Terminate authorization of all subcontractors to act on behalf of the TSP
- Transfer obligations to a reliable party for maintaining information necessary to provide evidence
- TSP private keys, including backup copies, shall be destroyed, or withdrawn from use
- Have an arrangement to cover the costs to fulfil these minimum requirements
- State in its practices the provisions made for termination of service
- Shall maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period
Compliance

• Shall provide evidence on how it meets the applicable legal requirements

• Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities. Applicable standards such as ETSI EN 301 549 should be taken into account

• Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
European Multi-Stakeholder Platform on ICT Standardisation

Rolling Plan for ICT Standardisation

- Societal challenges
  - eHealth
- Innovation for the Digital Single Market
  - e-Invoicing; Card, Internet and Mobile Payments
- Sustainable growth
  - Smart Grids and Smart Metering
  - Smart Cities / Technologies and Services for a Smart and Efficient Energy Use
- Key enablers and security
  - Cloud computing; Internet of Things; Network and Information Security
  - Electronic identification and trust services including e-signatures
THANK YOU
For your interest

For more information:

ILNAS – Département de la confiance numérique
1, Avenue du Swing
L-4367 Belvaux

(+352) 247 743 50
(+352) 247 943 50

www.portail-qualite.lu
alain.wahl@ilnas.etat.lu