Welcome to the World of Standards

ETSI World Class Standards

cen

ENISA Trust Services Forum – 30TH JUNE 2015

Standardisation development status

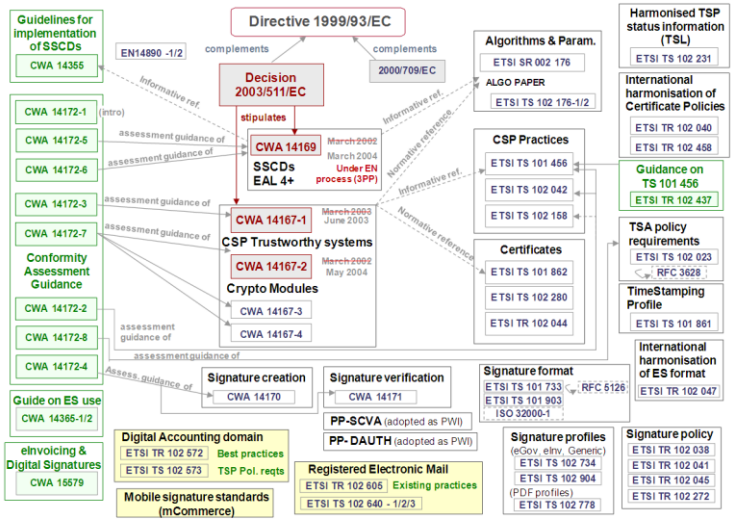
Presented by Sylvie Lacroix

Agenda

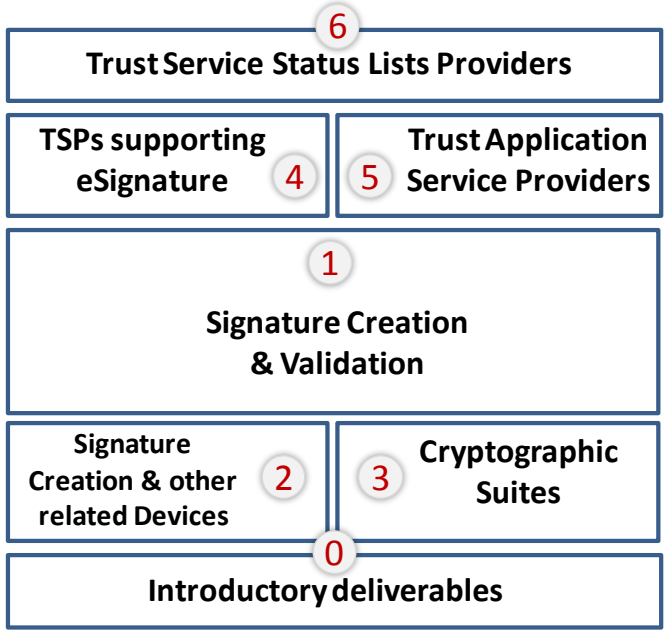
- Introduction
- Key points & new items in each standardisation area
  0. Framework
  1. Signature creation and validation
  2. Signature creation & other related devices
  3. Cryptographic suites
  4. TSPs supporting digital signatures
  5. Trust application service providers
  6. Trust service status list providers
- Testing conformance & interoperability
- Challenges and next steps, alignment with eIDAS Regulation

M/460 Phase 1 – Output summary

- **Objectives:**
  - Inventory
  - Rationalised structure
  - Gap Analysis
  - Work Programme
  - Quick fixes



Rationalised structure:



Consistent numbering (x19 000 series):

DD L19 xxx-z

- Functional Area & Sub-Area
- Document type

Guidance
Policy & Security Requirements
Technical Specifications
Conformity Assessment
Testing Conformance & Interoperability

Framework for digital signature stds

6 **Trust service status lists providers**

List of TSP services approved (supervised) by National Bodies (e.g. Trusted lists)

- TSP issuing certificates
- Time Stamping Auth^{ies}
- Signing services
- Validation services

TSPs supporting digital signature 4

5 **Trust application service providers**

- eDelivery / Reg^{ed} email
- Long term preservation

- Rules & procedures
- Signature creation / validation protection profiles

1 **Signature Creation & Validation**

- XAdES
- CAdES
- PAdES
- AdES in mobile env^{mt}
- ASiC (containers)

CC Protection Profiles

- Smart Cards
- HSM's
- Signing Services

Signature creation & other related devices 2

3 **Cryptographic suites**

- Key generation
- Hash functions
- Signature algorithms
- Parameters, …

0 **Introductory deliverables**

Aera 0 - Framework documents

- **Phase 1 resulted in Rationalized Framework** (SR 001 604)
- **Phase 2 work in progress**
  - Updating framework presentation document (TR 119 000 as update of SR 001 604/ just approved)
  - Study on The framework for standardisation of signatures: Extended structure including electronic identification and authentication (TR 419 010 – wait for EC's inputs on LoA)
  - Study on The framework for standardisation of signatures: Standards for AdES in mobile environments (SR 019 020 – final draft September)
  - Guidelines for SMEs & citizens (TR 419 030 & TR 419 040)
  - Document centralising definitions and abbreviations (TR 119 001 - under publication)

Quite all the documents in this area are new!

						Introductory documents of the framework for signature standardisation	Replaces	Expected publication
						Sub-areas		
						Guidance		
TR	1	19	0	0	0	The framework for standardisation of signatures: overview	SR 001604 v1.1.1	published
TR	4	19	0	1	0	The framework for standardisation of signatures: Extended structure including electronic identification and authentication	(new)	Feb. 2016 (hand over to CEN)
SR	0	19	0	2	0	The framework for standardisation of signatures: Standards for AdES in mobile environments	(new)	Nov. 2015
TR	4	19	0	3	0	The framework for standardisation of signatures: Best practices for SMEs	CWA 14365	Dec. 2015
TR	4	19	0	4	0	The framework for standardisation of signatures: Guidelines for citizens	CWA 14365	Dec. 2015
SR	0	19	0	5	0	Rationalised framework of standards for electronic registered delivery applying electronic signatures	(new)	published
						Policies		
TR	1	19	0	0	1	The framework for standardisation of signatures: Definitions and abbreviations	(new)	published

Aera 1 - Signature Creation & Validation

- **Phase 1 Quick fixes**
- **Phase 2 work in progress**
  - Business driven guidance for creation & validation of dig. sig. (new - TR 119 100)
  - Policy reqmnts for creation & validation of dig. sig. (new - TS 119 101/draft Sep. 2015)
  - Protection Profiles for signature creation & validation applications (new - EN 419 111)
  - C/X/PAdES & ASiC formats (baseline & extended/additional signatures/containers)
    - Revisions and migration to ENs (EN 319 122/132/142/162 – under EN Approval)
  - Procedures for creation and validation of digital signatures
    - New - EN 319 102-1 (TB approved)
  - Signature policies
    - New - TS 119 172-1 (TB approved)
  - Conformity assessment for SCA / SVA
    - New - EN 419 103
  - Testing conformance & interoperability
    - Signature formats - TS 119 1x4

Signature Creation and Validation						
				Sub-areas		
				Guidance		
TR	1	19	1	0	0	Business driven guidance for implementing digital signature creation and validation
				Policy & Security Requirements		
TS	1	19	1	0	1	Policy and security requirements for signature creation applications and signature validation
EN	4	19	1	1	1	Protection profiles for signature creation and validation application
				Technical Specifications		
EN	3	19	1	0	2	Procedures for creation and validation of AdES digital signatures
EN	3	19	1	2	2	CAdES digital signatures
EN	3	19	1	3	2	XAdES digital signatures
EN	3	19	1	4	2	PAdES digital signatures
TS	1	19	1	5	2	Architecture for AdES in mobile environments
EN	3	19	1	6	2	Associated Signature Containers (ASiC)
TS	1	19	1	7	2	Signature policies
				Conformity Assessment		
TS	4	19	1	0	3	Conformity assessment for signature creation & validation (applications & procedures)
				Testing Conformance & Interoperability		
TS	1	19	1	2	4	CAdES Testing conformance & interoperability
TS	1	19	1	3	4	XAdES Testing conformance & interoperability
TS	1	19	1	4	4	PAdES Testing conformance & interoperability
TS	1	19	1	5	4	Testing conformance & interoperability of AdES in mobile environments
TS	1	19	1	6	4	ASiC Testing conformance & interoperability

Area 2 - Sig. & other related devices

- **Phase 1 resulted in a work plan including new topics and revision and maintenance of existing documents**
  - Protection Profiles for SSCD (Phase 1), EN 419 211
- **Phase 2 work in progress**
  - Business driven guidance (TR 419 200)
  - Protection Profiles
    - Time Stamping (new - EN 419 231)
    - Move to EN (PP crypto module EN 419 221 & 419 261, Security requirements for server signing EN 419 241)
    - Evaluation & Certification (PP DAUTH EN 419 251)
  - Application Interfaces for SSCDs EN 419 212

							Signature creation and other related devices	Replaces	Expected publication
							Sub-areas		
							Guidance		
TR	4	19	2	0	0		Business driven guidance for signature creation and other related devices	(new)	February 2016
							Policy & Security Requirements		
EN	4	19	2	1	1		Protection profiles for secure signature creation device - Part 1: Overview - Part 2: Device with key generation - Part 3: Device with key import - Part 4: Extension for device with key generation and trusted communication with certificate generation application - Part 5: Extension for device with key generation and trusted communication with signature creation application - Part 6: Extension for device with key import and trusted communication with signature creation application	- (new part) - prTS 14169-2 - prTS 14169-3 - prTS 14169-4 - prEN 14169-5 - (new part)	published
EN	4	19	2	2	1		Protection Profiles for TSP cryptographic modules - Part 1: Overview - Part 2: Cryptographic Module for CSP signing operations with backup – Protection Profile (CMCSOB-PP) - Part 3: Cryptographic module for CSP key generation services – Protection Profile (CMCKG-PP) - Part 4: Cryptographic module for CSP signing operations without backup – Protection Profile (CMCSOPP) - Part 5: Cryptographic module for trust services	- (new part) - prTS 14167-2 - prTS 14167-3 - prTS 14167-4 - (new part)	By end 2015 By end 2015 By end 2015 By end 2015 In 2016
EN	4	19	2	3	1		Protection profile for trustworthy systems supporting time stamping	(new)	In 2016
EN	4	19	2	4	1		Security requirements for trustworthy systems supporting server signing - Part 1: Security requirements - Part 2: Protection profile for trustworthy signature creation module (PP-TSCM) - Part 3: Protection profile for signature activation data management and signature activation protocol (PPSAD+SAP)	CWA 14167-5	- TS published (EN: 2015) - NWI in 2015 - NWI in 2015
EN	4	19	2	5	1		Security requirements for device for authentication - Part 1: Protection profile for core functionality - Part 2: Protection profile for extension for trusted channel to certificate generation application - Part 3: Additional functionality for security targets	EN 16248 (PP-DAUTH)	published
EN	4	19	2	6	1		Security requirements for trustworthy systems managing certificates for electronic signatures	prTS 14167-1	published
							Technical Specifications		
EN	4	19	2	1	2		Application interfaces for secure elements used as qualified electronic signature (seal-) creation devices - Part 1: Introduction - Part 2: Basic services - Part 3: Device authentication - Part 4: Privacy specific protocols - Part 5: Trusted eServices	EN 14890	By end 2015
							Conformity Assessment		
							no requirement identified		
							Testing Conformance & Interoperability		
-	-	-	-	-	-		*no requirement identified*		

Area 3 - Cryptographic suites

Main activities

- TR 119 300 published in 05/2015
- TS 119 312 published in 11/2014
- Maintenance & monitoring : collaboration ETSI - ENISA

						Cryptographic suites	Replaces	Expected publication
						Sub-areas		
						Guidance		
TR	1	19	3	0	0	Business guidance on cryptographic suites	(new)	published
						Technical Specifications		
TS	1	19	3	1	2	Cryptographic suites	TS 102 176-	published
						Testing Conformance & Interoperability		
-		-	-	-	-	*no requirement identified*		

Area 4 - TSPs supporting signatures

Main activities

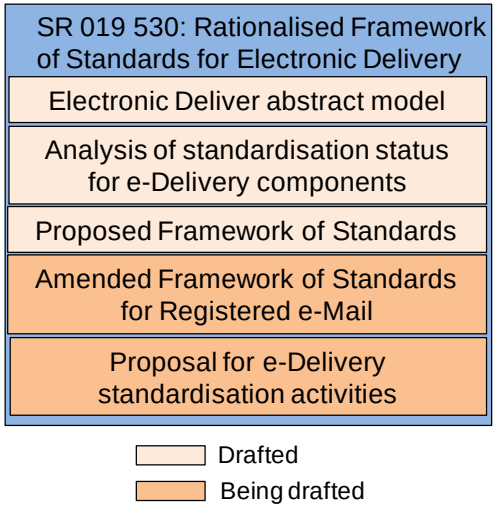
- Business Guidance (TR 119 400)
- TSP Conformity Assessment
  - Draft EN 319 403 (in EN vote)
- TSP Policy requirements (in EN approval)
  - Revised EN 319 401: General reqmts
  - Revised EN 319 411-x TSPs issuing certificates
  - New draft EN 319 421 Time-stamping
- Certificate and time-stamp profiles (in EN approval)
  - Draft EN 319 412-1 to -5 Certificates (natural, legal, web, qualified)
  - Draft EN 319 422 Time-stamping
- Phase 3
  - EN 319 431-432: Signature Generation Service Providers - Profiles
  - EN 319 441-442: Signature Validation Service Providers - Profiles

TSPs supporting digital signatures and related services						
					Sub-areas	
					Guidance	
TR	1	19	4	0	0	Business driven guidance for TSPs supporting digital signatures
					Policy & Security Requirements	
EN	3	19	4	0	1	General Policy Requirements for Trust Service Providers
EN	3	19	4	1	1	Policy & Security Requirements for TSPs Issuing Certificates
EN	3	19	4	2	1	Policy & security requirements for trust service providers issuing time-stamps
EN	3	19	4	3	1	Policy & security requirements for TSPs providing signature generation services
EN	3	19	4	4	1	Policy & security requirements for TSPs providing signature validation services
					Technical Specifications	
EN	3	19	4	1	2	Certificate Profiles - Part 1: Overview and common data structures - Part 2: Certificate profile for certificates issued to natural persons - Part 3: Certificate profile for certificates issued to legal persons - Part 4: Certifcate profile for web site certificates issued to organisations - Part 5: QCStatements
EN	3	19	4	2	2	Time-stamping protocol and time-stamp profiles
EN	3	19	4	3	2	Protocols and profiles for signature generation services
EN	3	19	4	4	2	Protocols and profiles for signature validation services
					Conformity Assessment	
EN	3	19	4	0	3	Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers
					Testing Conformance & Interoperability	
-	-	-	-	-	-	*no requirement identified for such a document*

Area 5 – Trust applic° service providers

Main activities

- **Business Guidance** (TR 119 500)
- **Study on e-Delivery standardisation needs** (SR 019 050 published 06/2015)
  - Addressing e-Delivery services as defined in Regulation proposal
  - Identify standards required to be produced
  - Define scope and purported contents
  - Raise recommendations
- **Phase 3:**
  - Study on Preservation Services followed by actual standardization
  - e-Registered delivery services – policy requirements & profiles (EN 319 521/522)
  - Registered Electronic Mail (REM) Services – policy requirements & profiles (EN 319 531/532)



Trust Application Service Providers							
					Sub-areas		
					Guidance		
TR	1	19	5	0	0	Business Driven Guidance for Trust Application Service Providers
SR	0	19	5	3	0	Study on standardisation requirements for e-Delivery services applying e-Signatures
					Policy & Security Requirements		
EN	3	19	5	1	1	Policy & Security Requirements for Preservation Service Providers
EN	3	19	5	2	1	Policy & Security Requirements for e-Registered Delivery Service Providers
EN	3	19	5	3	1	Policy & Security Requirements for Registered Electronic Mail (REM) Service Providers
					Technical Specifications		
EN	3	19	5	1	2	Technical specifications for preservation services
EN	3	19	5	2	2	Technical specifications for e-Registered delivery services
EN	3	19	5	3	2	Technical specifications for Registered Electronic Mail services
					Conformity Assessment		
EN	3	19	5	1	3	Conformity Assessment - Requirements for conformity assessment bodies assessing Preservation Service Providers and the trust services they provide
EN	3	19	5	2	3	Conformity Assessment - Requirements for conformity assessment bodies assessing e-Registered Delivery Service Providers and the trust services they provide
EN	3	19	5	3	3	Conformity Assessment - Requirements for conformity assessment bodies assessing Registered Electronic Mail Service Providers and the trust services they provide
					Testing Conformance & Interoperability		
TS	1	19	5	0	4	General requirements for Testing Conformance & Interoperability of TASP services
TS	1	19	5	1	4	Testing Conformance & Interoperability of Preservation Services
TS	1	19	5	2	4	Testing Conformance & Interoperability of e-Registered Delivery Services
TS	1	19	5	3	4	Testing Conformance & Interoperability of Registered Electronic Mail Services - Part 1: Test suites for testing interoperability of REM services using same format and

Area 6 - TSLs & Trusted Lists

- Phase 2
  - **Published Business driven guidance** (TR 119 600 may 2015)
  - **Testing conformance & interoperability** (TS 119 614)
- **Trusted Lists** (TS 119 612)
  - V1.1.1 published June 2013
  - Referenced by CD 2013/662/EU
  - Allow non-EU countries and International organisations to set-up TL's in order to facilitate (mutual) recognition of "approved" trust services
  - V2.1.1 to be published & referenced by eIDAS Art.22.5 implementing act
  - Tools available:
    - TLManager (EC – Joinup)
    - TL Conformance Tester (ETSI / UPC)

Trust Service Status Lists Providers							
					Sub-areas		
					Guidance		
TR	1	19	6	0	0	Business guidance for trust service status lists providers	
					Policy & Security Requirements		
TS	1	19	6	1	1	Policy & security requirements for trusted lists providers	
					Technical Specifications		
TS	1	19	6	1	2	Trusted lists	
					Conformity Assessment		
-	-	-	-	-		*no requirement identified for such a document - relying on TS 119 403 / EN 319 403*	
					Testing Conformance & Interoperability		
TS	1	19	6	1	4	Testing conformance & interoperability of trusted lists: - Part 1: Test suites for testing interoperability of XML representation of trusted lists. - Part 2: Specifications for testing conformance of XML representation of trusted lists	

Testing Conformance & Interoperability

Testing Conformance & Interoperability

- Generate a Special Report detailing activities related to testing interoperability and conformity to be run during the implementation and deployment of the Rationalised Framework of Electronic Signatures (RF henceforth).
- Production of a set of Technical Specifications defining test suites for testing interoperability and conformity against core standards of the RF.
- Design and implement a set of conformity testing tools.

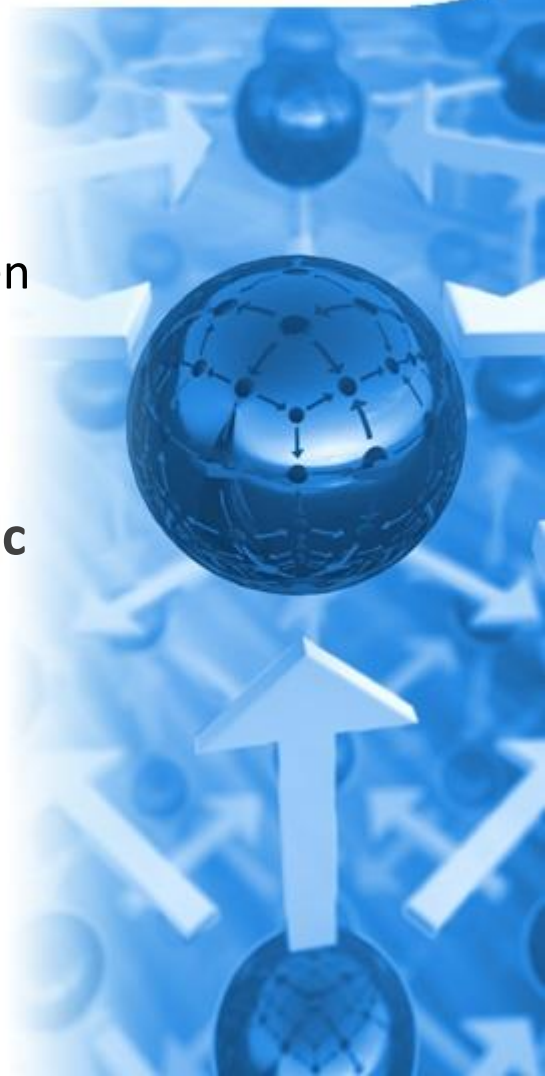
Testing interoperability & conformance Plans.

- Published Special Report SR 003 186 formalizing plans for:
  - Organization, definition and conduction of test events in the next one and a half years.
  - Scheduling of Technical Specifications and the software tools production will mainly depend on the plans formalized for the test events.
- Schedule available from
  - ETSI Publications Download Area:
    http://pda.etsi.org/pda/queryform.asp
- PAdES Plugtests May 2015
- CAdES Plugtests 11 June - 10 July 2015
- XAdES Plugtests planned for October 2015

Challenges and next steps

Challenges

- **Mapping to eIDAS legal requirements**
  - Mandatory (3 dated or 2 not) vs non mandatory acts
  - Acts for which the EC is empowered to define the technical requirements and specifications that when met will grant presumption of compliance vs acts for which the EC may/shall establish reference numbers of standards but is not empowered to determinate directly their content. **Non automatic referencing – principles established by EC**
    - ENISA's assistance:
      - Standards assessment: Eligibility for enabling eIDAS compliance
      - Study on TSPs' standards
    - IAS2 study



Mapping with eIDAS

- **Mandatory acts (coming soon):**
  - eSig/eSeal formats Art 27.5/37.5 IA to point to current version C/P/XAdES – ASiC baseline profiles TS 103 17x
  - Trusted list Art 22.5 IA: to rely on TS 119 612 – v2.1.1
  - QSCD
    - list of standards for the security assessment of information technology products
    - establishment of specific criteria to be met by the designated bodies
  - (trust mark)

Mapping with eIDAS

- **Supervision TSP – layered model**
  - Trusted list Art 22.5 IA: relies on TS 119 612 – v2.1.1 (end – point of the process)
  - legal framework: EA (CAB accreditation: EC 765/2008). Rely on:
    - L1: ISO 17065 (hook to ISO 27006 & 17021), for accrediting CAB competencies (to assess products, services)
    - L2: ETSI EN 319 403, reqs for CABs for assessments of QTS(P)s
    - L3: TSP audit criteria (control objective list for eIDAS conformity),
    - L4: (not mandatory): policy and requirements to achieve L3: e.g. ETSI 319 4x1 series
      - requires fine tuning for the REG (e.g. cert. status info kept “beyond” expiry … in technical terms)

Mapping with eIDAS

- **QSCD – on going**
  - Complex because
    - 3 IAs and 1 DA to be harmonised, not all mandatory
    - Scope of QSCD mandatory certification is limited to the “heart” of the device

PPs and other technical standards mapped/aligned with the certification process related standards

Mapping with eIDAS

- **Other implementing acts**
  - may wait that industry self-regulate
  - E.g. standards for AdES (art 27.4) relies on:
    - Technical specs of SCD, certificates (e.g. level low, high), long term preservation features.
    - Standards for establishing LoA of above components (e.g TSP practices certified as “high”)

Numerous standards exist. Combination complex… IA Needed?

Mapping with eIDAS

- **Non in acts**
  - TPS offering signature services and/or handling SCD for the users
  - if QES, QTSP needs audit.

No IA for signature creation or (Q)SCD handled by TSP, but “connected” IAs for AdES / QSCD… and of course, standards.

Next steps

- **Not all standards ready by 01/07/2016 but …**
  - Most are ready or on the point to
  - Timeline is aligned with EC for mandatory and dated IAs
  - The referencing principles will anyway need fine-tuning of the standards with regard to the selected outcome based TSP's audit criteria
  - E.g. eDelivery (no standard yet) is broader than REM (standard exists). Preferable to be established under the light of ENISA's studies, industry behavior in the framework of the Regulation.

Website & Stakeholders mailing list

- www.e-signatures-standards.eu

- Stakeholders mailing list:
  - Subscription via above website

    (via "Subscribe to the newsletter").
    - To get news.
    - To receive drafts.
    - To be notified of commenting periods.
    - Etc.

Useful links

- e-Signature Standards Portal: http://www.e-signatures-standards.eu
- STF web pages
  - STF 457: http://portal.etsi.org/STFs/STF_HomePages/STF457/STF457.asp
  - STF 458: http://portal.etsi.org/STFs/STF_HomePages/STF458/STF458.asp
  - STF 459: http://portal.etsi.org/STFs/STF_HomePages/STF459/STF459.asp
- ETSI Publications Download Area: http://pda.etsi.org/pda/queryform.asp
- ETSI Electronic Signatures Portal: http://xades-portal.etsi.org/pub/index.shtml
- Standardisation mandate m460 to CEN and ETSI on electronic signatures https://ec.europa.eu/digital-agenda/en/news/standardisation-aspects-esignatures
- Study on Cross-Border Interoperability of eSignature (CROBIES) - (2008-2010): https://ec.europa.eu/digital-agenda/en/news/crobies-study-cross-border-interoperability-esignatures-2010
- European Commission page on EU Member States Trusted Lists: https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers
- Revision aspects of European electronic signature Directive 1999/93/EC & Draft proposal for a Regulation "on electronic identification and trusted services for electronic transactions in the internal market": https://ec.europa.eu/digital-agenda/en/trust-services
- Studies on an electronic identification, authentication and signature policy (2011-2012, 2013): http://iasproject.eu/home.html