The Standards People

BIS Seminar on Standardization in the usage of Digital Signature

ETSI standards for trust services and digital signatures

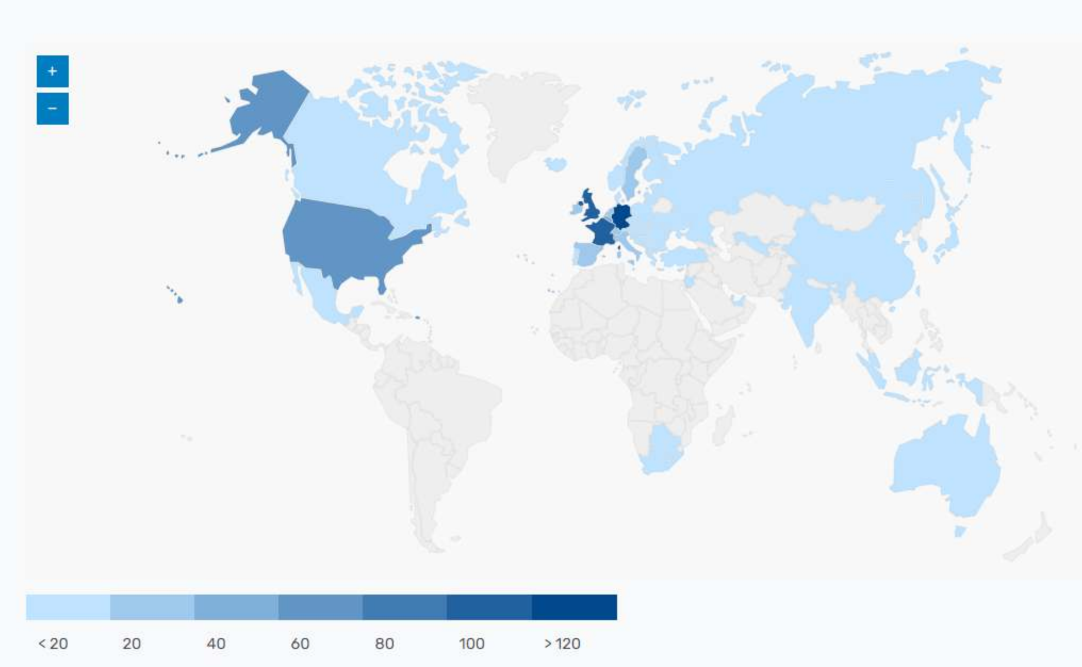
Presented by Mr. Dinesh Chand Sharma
Director – Standards & Public Policy (EU Project SESEI)
on behalf of
Mr. Nick Pope, Chair ETSI TC ESI
with help from
Mr. Vijay Kumar, CTO eMudra

16.06.2023

Agenda

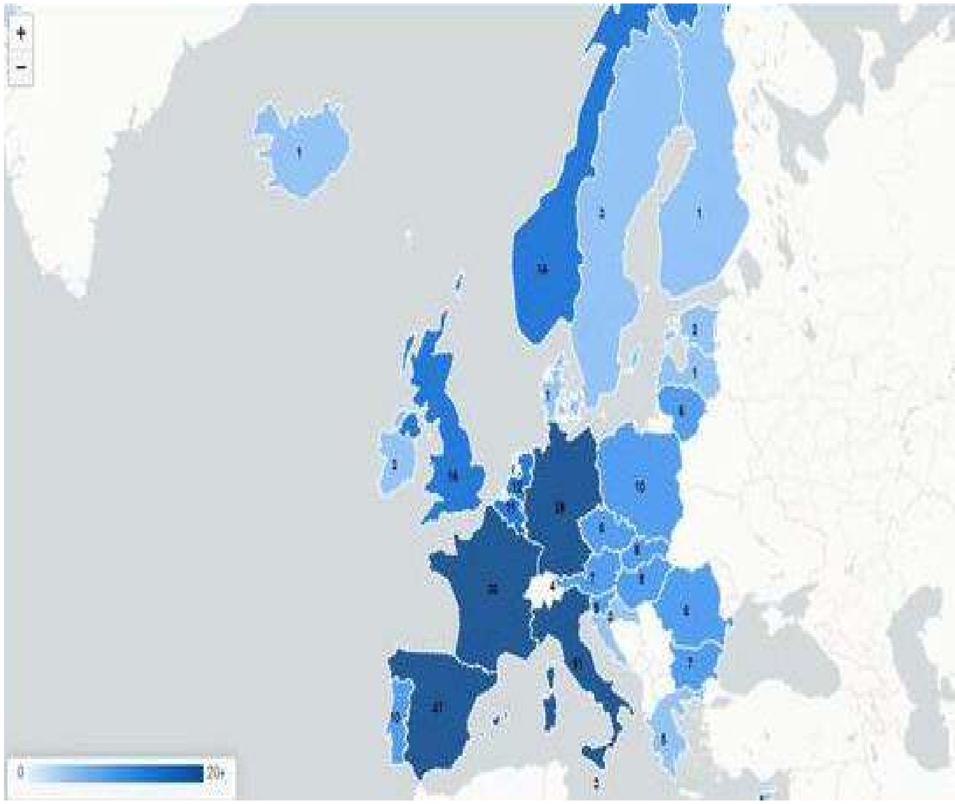
1) Overview of ETSI standards for Digital Signatures and Trust Services
2) ISO Signature Format Standards & ETSI AdES Standards
3) Study by SSD10 & Recommendations

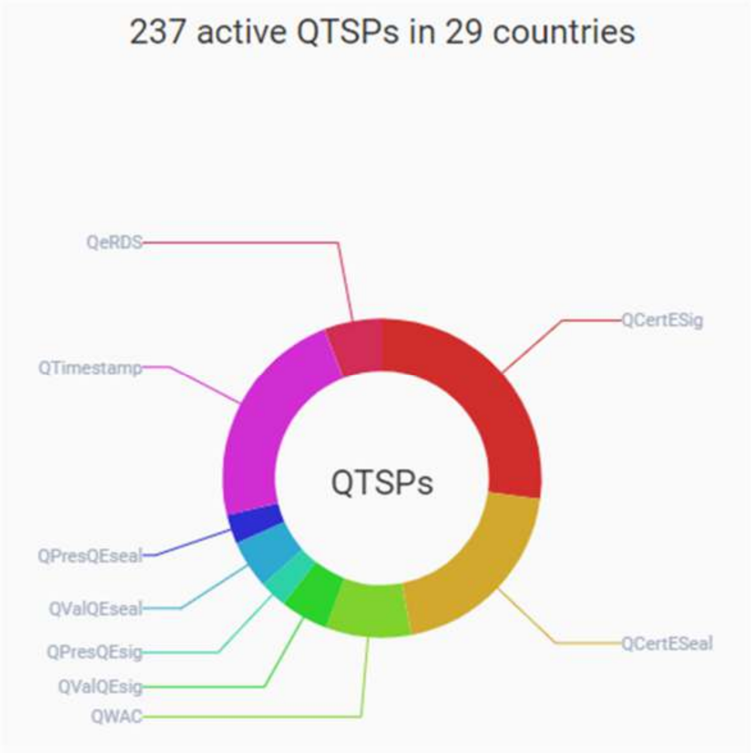
ETSI a Global Standardisation Body Based in the EU



- More than 900 member organizations worldwide,
- Drawn from over 60 countries and five continents
- Recognised by EU as provider of European Norms

Qualified trust service providers (TSPs)





https://eidas.ec.europa.eu/efda/tl-browser/#/screen/statistics

ETSI support for EU Regulation on qualified trust Services

- EU Regulation 910/2014 on eID and Trust services (eIDAS)
  - Governmental supervision scheme for providers of trust services

eIDAS Trust Services:

- Electronic signature: personal identity linked to data via certificate
- Electronic seal: organisation identity linked to data via certificate
- Website authentication: identity linked to website via certificate
- Registered e-delivery / e-mail: trusted service provider proof delivery etc.
- Time-stamping: Trusted time linked to data via time-stamp

EU Qualified & Globally applicable standards

Global
Best Practices
+ eIDAS
Specific
Requirements

EU Qualified: EU eIDAS Regulation 910/2014 on electronic identification and trust services for electronic transactions defines specific requirements on practices which give legal assumption.

These are met by specific options within ETSI standards

Global
Best Practices

(e.g. ISO,
CA / Browser Forum)

ETSI Standards: Build on globally accepted best practices and can be applied to different contexts

ETSI & CEN Standards supporting eIDAS – the overall picture

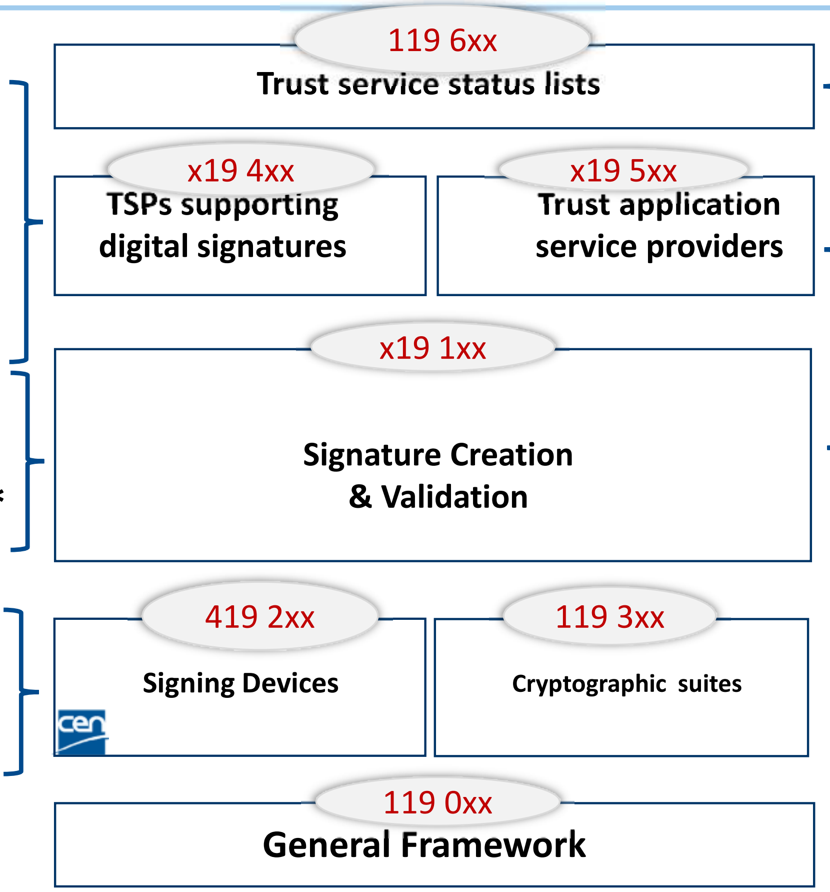
Trust services:

- TSP Audit ✓
- Issuing certificates ✓*
- Time Stamping ✓
- Signature creation services ✓
- Signature validation services ✓
- Identity proofing ✓*
- Open Banking ✓
- Support for NIS 2 (new)
- Attribute Attestations (new)

- AdES creation & validation
  - Part 1: procedures ✓*
  - Part 2: signature validation report ✓*

CC Protection Profiles

- QSCD - Smart Cards ✓
- HSM used as QSCD ✓
- HSM used by TSPs ✓
- Remote QSCD ✓



119 6xx
Trust service status lists

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

x19 1xx
Signature Creation & Validation

419 2xx
Signing Devices

119 3xx
Cryptographic suites

119 0xx
General Framework

Trusted list ✓
Using & interpreting trusted list ✓
Validation policy using trusted list ✓

Trust services for:

- Registered eDelivery / eMail ✓*
- Long term preservation ✓

Interop tests

Formats + Interop test:

- XAdES (XML) ✓*
- CAdES (CMS) ✓*
- PAdES (PDF) ✓
- ASiC (containers) ✓
- JAdES (JSON ✓
- CB-AdES (CBOR) (new)

- Signature suites ✓
  - Hash
  - Asymmetric crypto
  - Key generation
  - Lifetime
- Schema for algorithm catalogues (new) ✓

- Standards framework ✓ *
- Common definitions ✓
- Guides ✓

✓	Completed
	Update in progress
*	New
(new)	

International Alignment

- Best practices and audit scheme recognised by CA/Browser guidelines
- Input to ISO DIS 27099 standard on “Information Technology — Public key infrastructure (PKI) — Practices and policy framework”
- ISO Alignment with ETSI advanced electronic signature (AdES) Digital Signature Formats (see later)
- Regional / sector partnerships:
  - PKI Consortium (International PKI Service providers)
  - ASIA PKI,
  - Arab ICT organisation,
  - Japan Network Security Association
  - Safe Identity (international healthcare security consortium)
  - CA/Browser forum (Web server certificates)
- TR 103 684 Study Report on Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services

ISO & ETSI Digital Signature Formats

ETSI Digital Signature Format Standards

- Adapts existing digital signature format to meet legal requirements including long term validity using time-stamping
- First developed based on IETF Cryptographic Message Syntax RFC 3652 (now 5652) in developing ETSI TS 101 733 in December 2000
- Since then, updated and applied to other signature formats:
  - ETSI EN 319 122-1: CMS (Cryptographic Message Syntax) Advanced Electronic Signatures (CAdES) digital signatures (IETF 5652 CMS based)
  - ETSI EN 319 132-1: XML Advanced Electronic Signature (XAdES) based on W3C XML Signature
  - ETSI EN 319 142-1 : PDF Advanced Electronic Signatures (PAdES) based ISO 32000-1 PDF
  - ETSI EN 319 162-1 : Associated Signature Containers (ASiC) (Signatures in ZIP package)
  - ETSI TS 119 182-1 : JSON Advanced signatures (JAdES) based on IETF RFC JSON Web Signatures

ETSI AdES Maintenance Updates

Last major update in 2016 and 2021

Further updates to CAdES under approval process in 2023

ISO Standards Relating to ETSI Standards

Following ISO standards have aspects which overlap with ETSI standards as indicated below. Conformance to the ETSI standard does not necessarily imply conformance to the listed ISO/ITU standard but they are taken into account by ETSI.

TSI ESI standard	ISO / ITU-T standard	Title / Topic
TSP issuing certificates policy requirements and conformity assessment (e.g. EN 319 401, EN 319 411-1 & 2, EN 319 412-x, EN 319 403)	**ISO/IEC 27099:2022**	**PKI - Practices and Policy framework**
	ISO/IEC TR 14516:2002 / ITU-T X.842:2000	**Guidelines for the use and management of trusted third party services**
	ISO/IEC 15945:2002 / ITU-T X.843	**Specification of TTP services to support the application of digital signatures**
TS 119 461	**ISO/IEC TS 29003:2018**	**Identity proofing**
	ISO 21188: 2018	**PKI for financial services — Practices and policy framework**
	ISO 15782-1	**Certificate management for financial services — Part 1: Public key certificates**
	ISO 17090-1:2013	**Health Informatics - Part 1: overview of certificate services**
	ISO 17090-2:2015	**Health Informatics - Part 2: Certificate profile**
	ISO 17090-3:2008	**Health Informatics - Part 3: Policy Management of CA**
	ISO 17090-4:2014	**Health Informatics - Part 4: Digital Signatures for healthcare documents**
	ISO 17090-5: 2017	**Health Informatics - Part 5: Authentication using Healthcare PKI credentials**
	ISO/IEC 9594-8, ITU-T X.509	**The Directory: Public-key and attribute certificate frameworks**
PAdES	**ISO 32000-1:2008**	**Portable document format — Part 1: PDF 1.7**
		Portable document format — Part 2: PDF 2.0
	ISO 32000-2:2017	
CAdES	**ISO 14533-1 (upd. in progress)**	**Long term signature profiles — Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)**
XAdES	**ISO 14533-2 (upd. in progress)**	**Long term signature profiles — Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)**
ASiC	**ISO/IEC 21320-1:2015**	**Document Container File — Part 1: Core**

Modalities for Signing In India

	DSC in USB Token	eSign (v2) - Aadhaar	eSign (v3) - CA KYC
Certificate Type	Individual / Organization Individual	Individuals	Individual / Organization Individual
Enrolment	Online | Paperless | Video	Not Required. Aadhaar.	Online | Paperless | Video
Integration	Client system integration	Online integration (Gateway)	Online integration (Gateway)
Dependency	Desktop OS and crypto token is required	Hardware independent	Hardware independent
Auth / Password	Local Auth. Max 10 failed attempts, certificate reissuance.	Aadhaar OTP Authentication. (needs Mobile seeding)	2FA Online Auth With password reset options
Key Loss	Reissuance if token gets lost.	Not Applicable	Not Applicable
Hardware cost	Yes	No	No
OS Support	Limited OS support by token vendors		
Troubleshooting	Driver and other troubleshooting required	High availability of service	High availability of service
Timestamping and LTV	Signing time from user system	Supported	Supported
Bulk signing	Based on client system configuration	1 documents/transaction	5 documents/transaction
Sign using mobile	No	Yes	Yes
Userbase	10 million+	100 million+	3 million+

Modalities for Signing In India

Use Case	Digital Signature	Adoption
GST Return Signing	JSON data signing	30-40 Lacs / Mandatory
Income Tax Return Signing	Document Hash / Text data signatures	Large use case
MCA Return Signing	PDF Signature	Large / Mandatory
Tax Letters (IT/GST) / Aadhaar	PDF Signature	Less Signers, More Docs
Tendering Portals	Document Hash / Text data signatures	Mandatory
UIDAI (AUA/KUA/etc)	XML Signatures (xml-dsig)	High Volume
Banking Transactions	XML / Text data signatures	More Transactions
G2B / G2C	PDF Signatures	Increasing
B2B / B2C	PDF Signatures	Increasing
Emails	SMIME CMS Signatures	Low adoption

Reference study carried out by SSD 10

- Key RFC Works: RFC 5126 (CMS Digital Signatures)

- Key ISO Works:
  - ISO 27099 (PKI Policy & Practices)
  - ISO 21188 (PKI for Financial Services)
  - ISO 9594-8 (PKI digital signatures and certificates)
  - ISO 32000-1 / ISO 32000-2 (PDF Digital Signatures)

- ETSI - Electronic Signatures & Infrastructure (ESI) group
  - Trust Service Status Lists (119 6xx): List of CA / TSPs
  - CA/TSP for Digital Signatures (x19 4xx): Issuance of Certificates, Time Stamping, Signature Creation Services, Signature Validation Services
  - Application Service Providers (x19 5xx): E-Delivery / Emails, Long Term Preservation
  - Signature Creation & validation (x19 1xx): AdES Creation & validation, Formats for XML (XAdES), PDF (PAdES), CMS (CAdES), JSON* (JAdES), Asssociated Signature Containers (ASiC)
  - Signing Devices / CC Protection Profiles (419 2xx): QSCD (Smart Cards / USB Crypto Tokens), QSCD - HSM for CA/TSPs, QSCD - HSM for Signing, QSCD for Remote / Online Signing
  - Cryptographic Suites (119 3xx): Hashes, Asymmetric Cryptography, Key Generation, Lifetimes
  - General Frameworks (119 0xx): Standards Framework, Common Definition, Guides

Comparison between ISO and ETSI

Standard	Purpose	Derived from
ISO 14533-1: 2014	Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)	ETSI TS 101 733 / ETSI EN 319 122
ISO 14533-2: 2012	Processes, data elements and documents in commerce, industry and administration- Long term signature profiles-Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)	ETSI TS 101 903 / ETSI EN 319 132
ISO 14533-3: 2017	Processes, data elements and documents in commerce, industry and administration- Long term signature profiles-Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)	ETSI EN 319 142 / ISO 32000-2
ISO 14533-4: 2019	Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part 4: Attributes pointing to (external) proof of existence objects used in long term signature formats (PoEAttributes)	Majorly derived from above.
ISO/IEC 20248: 2018	Information Technology- Automatic identification and data capture techniques- Data structures- Digital signature meta structure	This is a barcode / RFID representation ISO/IEC 9594-8 will be base reference.

Comparison between ISO and ETSI – Gap Analysis

CA/TSP for Digital Signatures (x19 4xx)

- Signature Creation Services
- Signature Validation Services

Application Service Providers (x19 5xx)

- Long Term Preservation

Signature Creation & validation (x19 1xx)

- JSON* (JAdES), Asssociated Signature Containers (ASiC)

Cryptographic Suites (119 3xx)

- Hashes
- Asymmetric Cryptography
- Key Generation
- Lifetimes

Adoption of following list of standards

#	Type	Standard	Description
1	ISO	ISO 27099	PKI Policy & Practices
2	ISO	ISO 21188	PKI for Financial Services
3	ISO	ISO 9594-8	PKI digital signatures and certificates
4	ISO	ISO 14533-1: 2014	Digital Signature Profiles (Long Term): CAdES
5	ISO	ISO 14533-2: 2012	Digital Signature Profiles (Long Term): XAdES
6	ISO	ISO 14533-3: 2017	Digital Signature Profiles (Long Term): PAdES
7	ISO	ISO 14533-4: 2019	Digital Signature Profiles (Long Term): Attributes pointing to (external) proof of existence objects
8	ISO	ISO/IEC 20248: 2018	Digital Signature in barcode and/or RFID tag data
9	ETSI	x19 4xx	Digital Signatures: Issuance, Creation and Validation
10	ETSI	x19 5xx	Application Providers, Secure Email and Long-Term Preservation
11	ETSI	x19 1xx	Advanced Electronic Signatures for PDF, XML, CMS, JSON*, etc
12	ETSI	419 2xx	Signature Devices and Protection Profiles
13	ETSI	119 3xx	Cryptographic Suites and Algorithms
14	ETSI	119 0xx	General Framework and standards
15	ETSI	119 6xx	Trust Services list, status, and providers

Further information

ETSI standards: available for free download: http://www.etsi.org/standards-search

- Information on Signatures and Trust Services standards :
  https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

- News list on Signatures and trust services:
  https://list.etsi.org/scripts/wa.exe?SUBED1=e-signatures_news&A=1

- Online training on signature and trust service standards:
  https://www.etsi.org/events/1926-webinar-etsi-standards-for-trust-services-and-digital-signatures

- ENISA Study: Towards global acceptance of eIDAS audits
  https://www.enisa.europa.eu/publications/towards-global-acceptance-of-eidas-audits
  https://esignature.ec.europa.eu/efda/home/#/screen/home

Save the date!!!

BIS is organizing a training workshop on **ETSI standards on digital signatures and trust services** covering in detail:

- Signature formats, Signature creation and Validation procedures,
    - Best practices for signature creation and validation,
- Upcoming EU new regulation on trust services and eID and initiatives for cross recognition of digital signatures

- Date: 21st Sept 2023
- Time: 13:30 – 16:30 IST (10:00 to 13:00 CEST)
- Venue: Lal C Verman Hall, Manak Bhavan, BIS, New Delhi
- Mode: Hybrid

thank you!

Dinesh Chand Sharma
(Seconded European Standardization Expert in India)
Director – Standardization & Public Policy
SESEI C/O EBTC, DLTA Complex, Gate No 3, 1st Floor, 1,
Africa Avenue, New Delhi 110029
Mobile: +91 9810079461, **Tel:** +91 11 3352 1525,
dinesh.chand.sharma@sesei.eu
www.sesei.eu ⇔ www.sesei.in