The Standards People

eIDAS and Electronic signature standards

7th Annual DIGITAL TRUST & PAPERLESS CONFERENCE - Prague, Czech Republic

22 May 2019

Agenda

- Importance of technical standards besides the laws and regulations
- The role of ETSI in enabling the eIDAS regulation
- ETSI standards and their evolvement
  - CA policy requirements
  - TSA policy requirements
  - Electronic Registered Delivery and Registered Electronic Mail (REM) services
  - Long-term (signature) preservation
  - Support for PSD2 use of qualified certificates
  - Signature formats
  - Signature validation
  - Algorithms

Agenda

- Remote signing/sealing
  - CEN & ETSI standards scope
  - Other standards
  - Certification process challenges
- What's coming next
  - Using Trusted Lists
  - Audit Update
  - Machine processable signature policies
  - Proposed new work item on identity proofing
  - Global acceptance of trust services

Importance of technical standards

- Standards provide people and organizations with a basis for mutual understanding and set the state of the art in fields of application
- Standards play an important role in the economy, by:
  - facilitating business interaction
  - enabling companies to comply with relevant laws and regulations
  - speeding up the introduction of innovative products to market
  - providing interoperability between new and existing products, services and processes
- Standards moreover disseminate knowledge in industries where products and processes supplied by various providers shall interact with one another

ETSI role in enabling eIDAS regulation

ETSI ESI is the committee dealing with digital signatures (signatures format, certificates), trust service providers and ancillary services (Registered email, Registered e-delivery, Time-Stamping, Long-term data preservation)

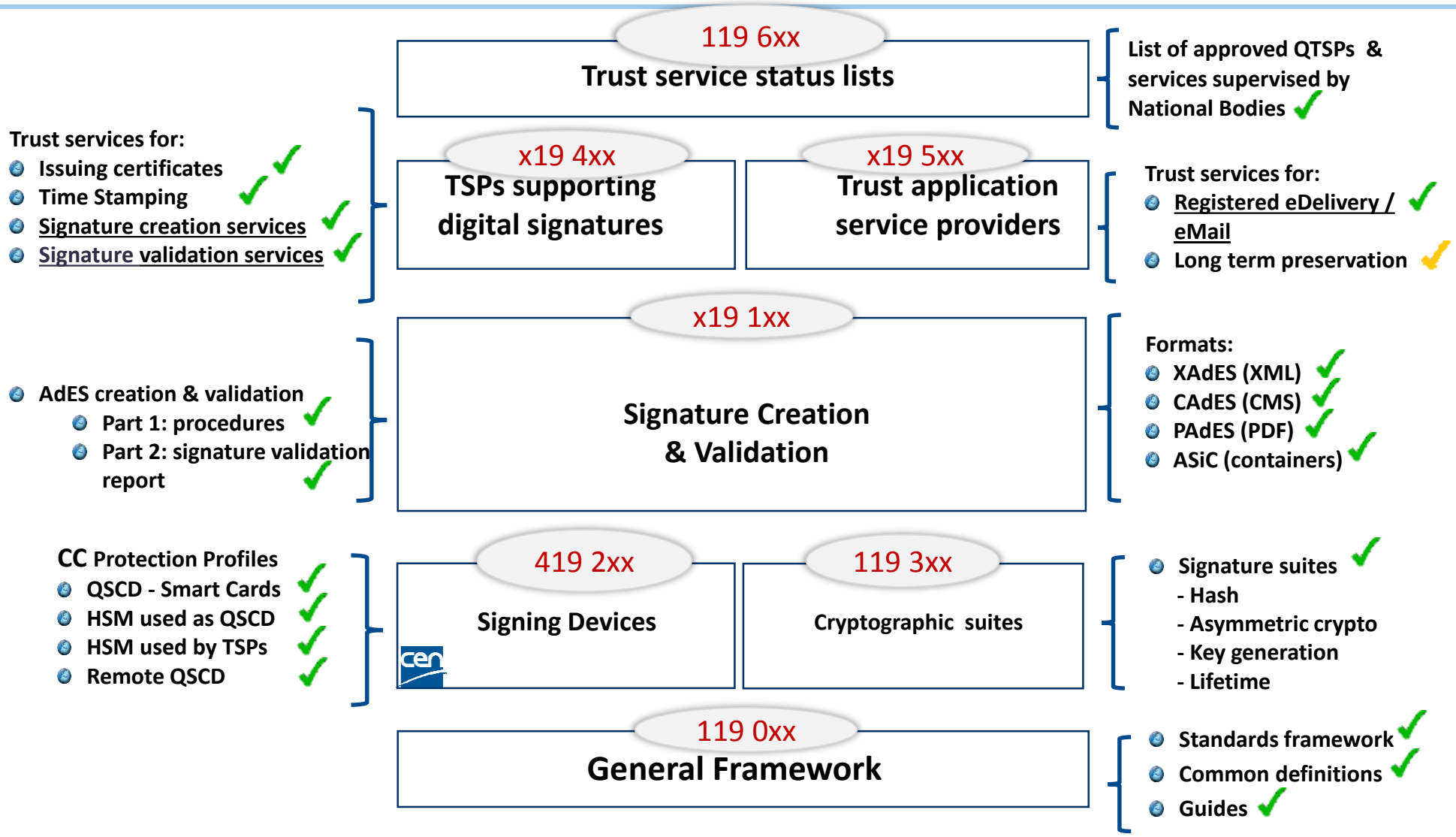
ESI activity covers signature creation and verification based on CAdES (CMS digital signatures), XAdES (XML digital Signatures), PAdES (PDF digital Signatures), and ASiC (Associated Signature Container).

ESI deals with cryptographic suites recommendations, trust service providers supporting signatures (e.g. certification authorities, time-stamping authorities) and/or providing remote signature creation or validation services, trust application providers (e.g. registered e-delivery providers, Registered Emails (REM) providers, information preservation providers), and Trust-service Status List (TSL).

In order to prove interoperability of implementations and enhance standards robustness, ETSI is running regular CAdES/XAdES/PAdES/ASiC Plugtests™ events.

ETSI also organizes Plugtests™ events on signature validation.

eIDAS Standards Framework: Published Standards



Standards framework complete – excepting preservation which is draft

Remote Signing & CEN Standards

Remote Signing & CEN Standards for Trustworthy Systems

CEN standards for remote signing systems:

- EN 419 241-1: General System Requirements - published
- EN 419 241-2: Protection Profile for QSCD for Server Signing - published
- EN 419 221-5: Cryptographic Module - published

Authentication can be delegated to an Identity Provider outside QSCD

Other CEN Documents recently published

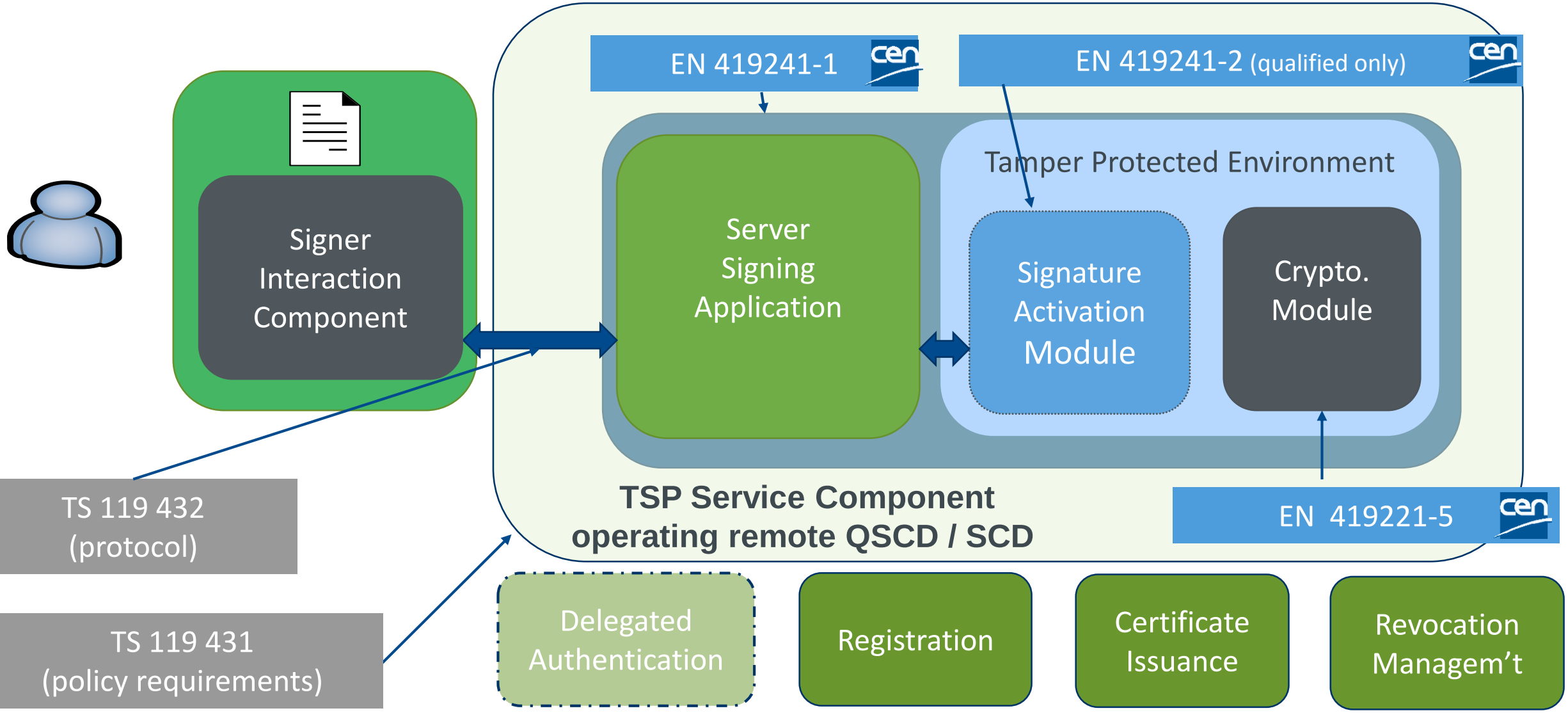
- CEN TS 419 221-6: Conditions for use of EN 419 221-5 (HSM-PP)as qualified electronic signature or seal creation device
- CEN TR 419 210: Applicability of CEN Standards to Qualified Electronic Seal

ETSI Signature Creation Protocols & TSP Component Policy Requirements

Standards published:

- TS 119 431-1: Policy and Security Requirements for TSP Service Components Operating a Remote QSCD / SCD
- TS 119 431-2: Policy and Security Requirements for TSP Service Components Supporting AdES Digital Signature Creation
- TS 119 432: Protocols for Remote Digital Signature Creation

Scope of Remote Signing Standards



Remote Signature Creation and eIDAS regulation

- eIDAS does not recognise Remote Signature Creation as an independent qualified Trust Service

- Remote Signature Creation provided as a component added to other qualified trust services
  - Certificate issuance
  - Time-stamping
  - Signature validation

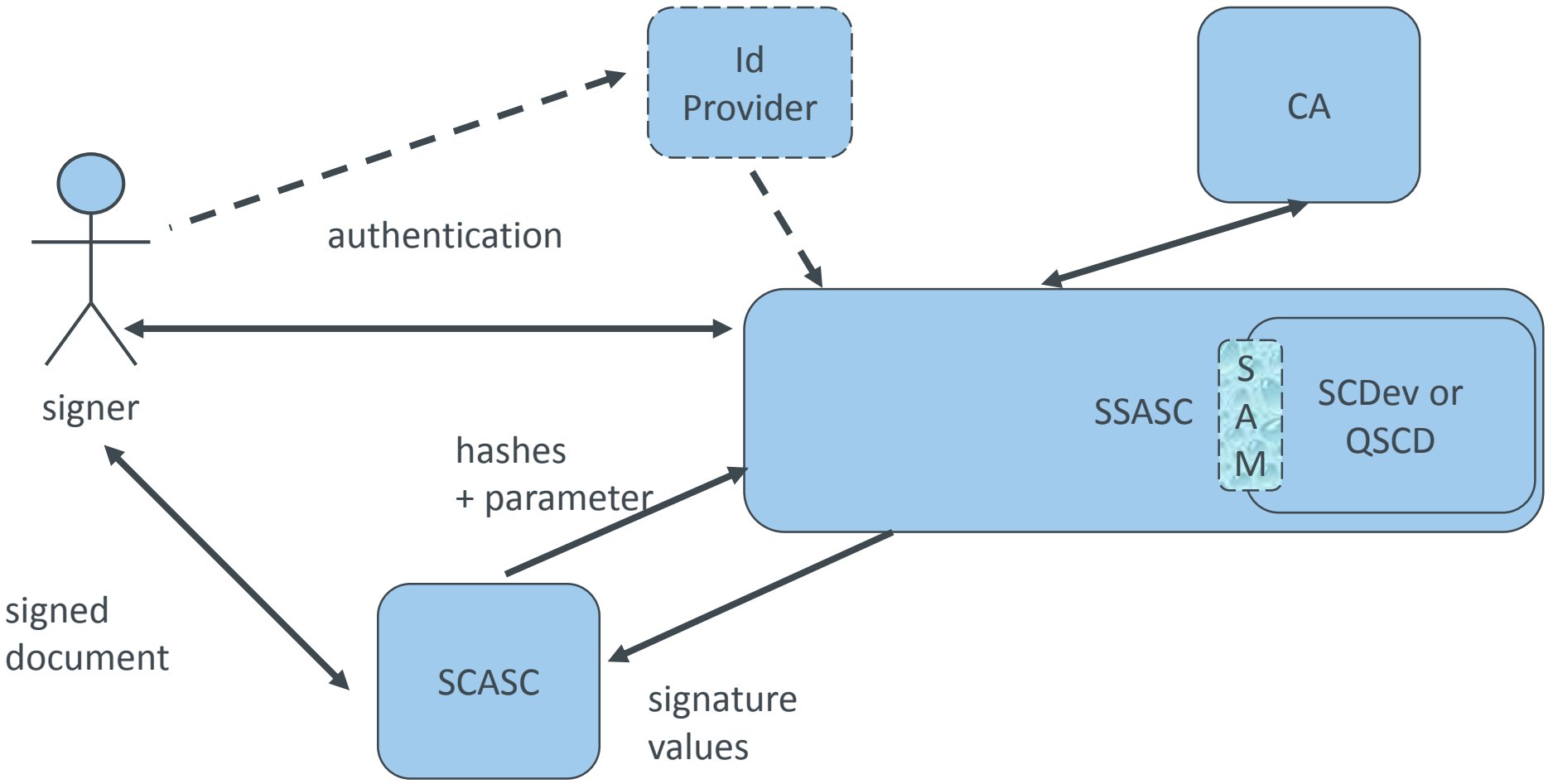
TS 119 431-1

Policy and security requirements for trust service providers; TSP service components operating a remote QSCD / SCDev

- Based on ETSI EN 319 401 (General Policy Requirements for Trust Service Providers)
- References to some requirements of ETSI EN 319 411-1 (Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements)
- References to many requirements of CEN EN 419 241-1 (Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements)

TSP providing Remote Signature Creation shall ensure that all policy requirements are met

Architecture (example)



Different trust service policies

Policies defined in the document

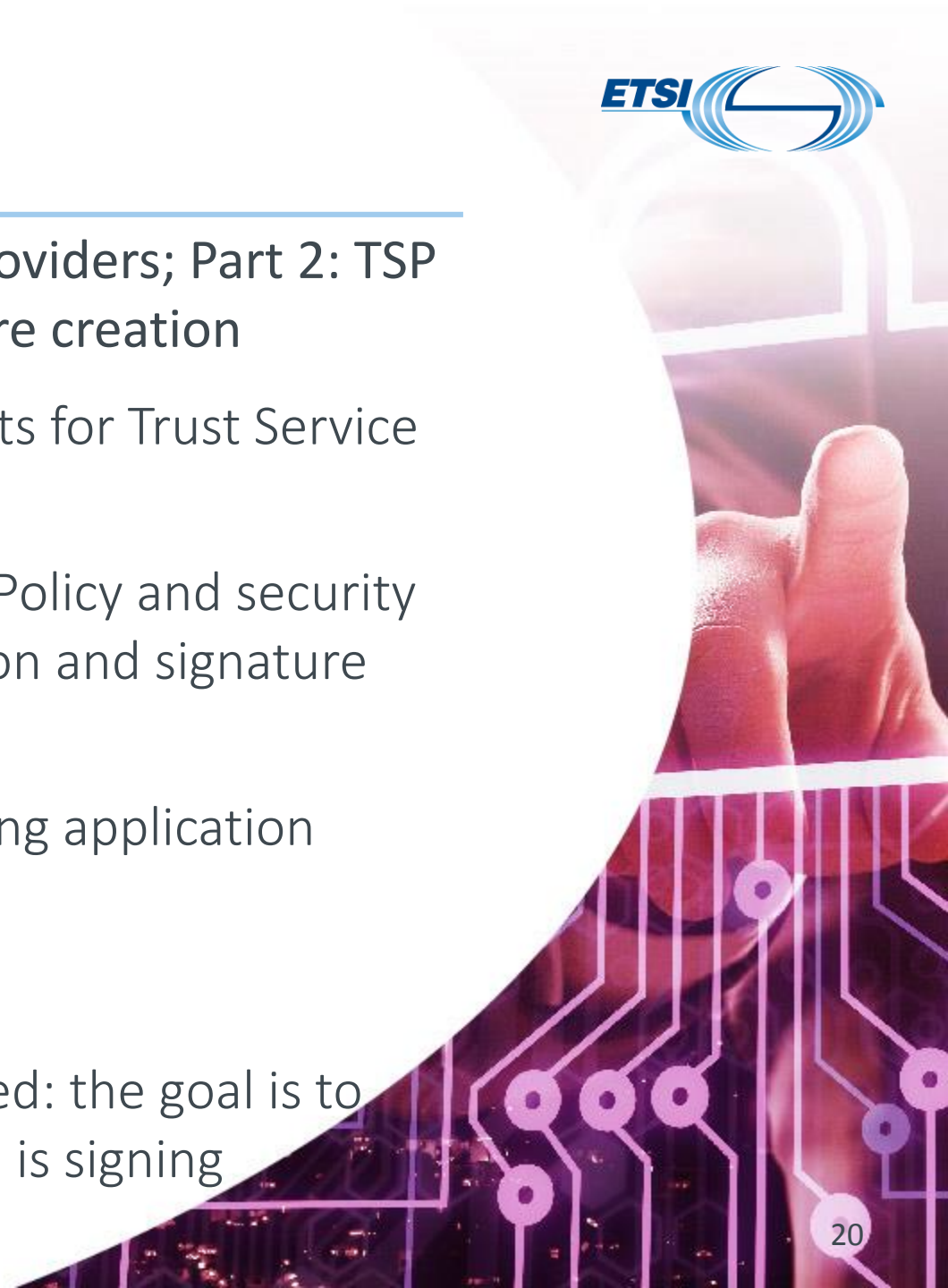
- A Lightweight SSASC Policy (LSCP) offering a quality of service less onerous than the normalized one: ***related to Sole Control Level 1 of CEN 419 241 part 1***
- A Normalized SSASC Policy (NSCP) which meets general recognized best practice for TSPs operating a remote QSCD / SCDev: ***related to Sole Control Level 2 of CEN 419 241 part 1***
- An EU Qualified SSASC Policy (EUQSCP) which offers the same quality as that offered by the NSCP but with specific requirements related to the European eIDAS Regulation: ***EU Qualified Policy requires QSCD*** (*could be met by using CEN 419 241 part 2*)

- **The main eIDAS challenge is to ensure that the remote signer is the same person that the one that has been enrolled by the CA**

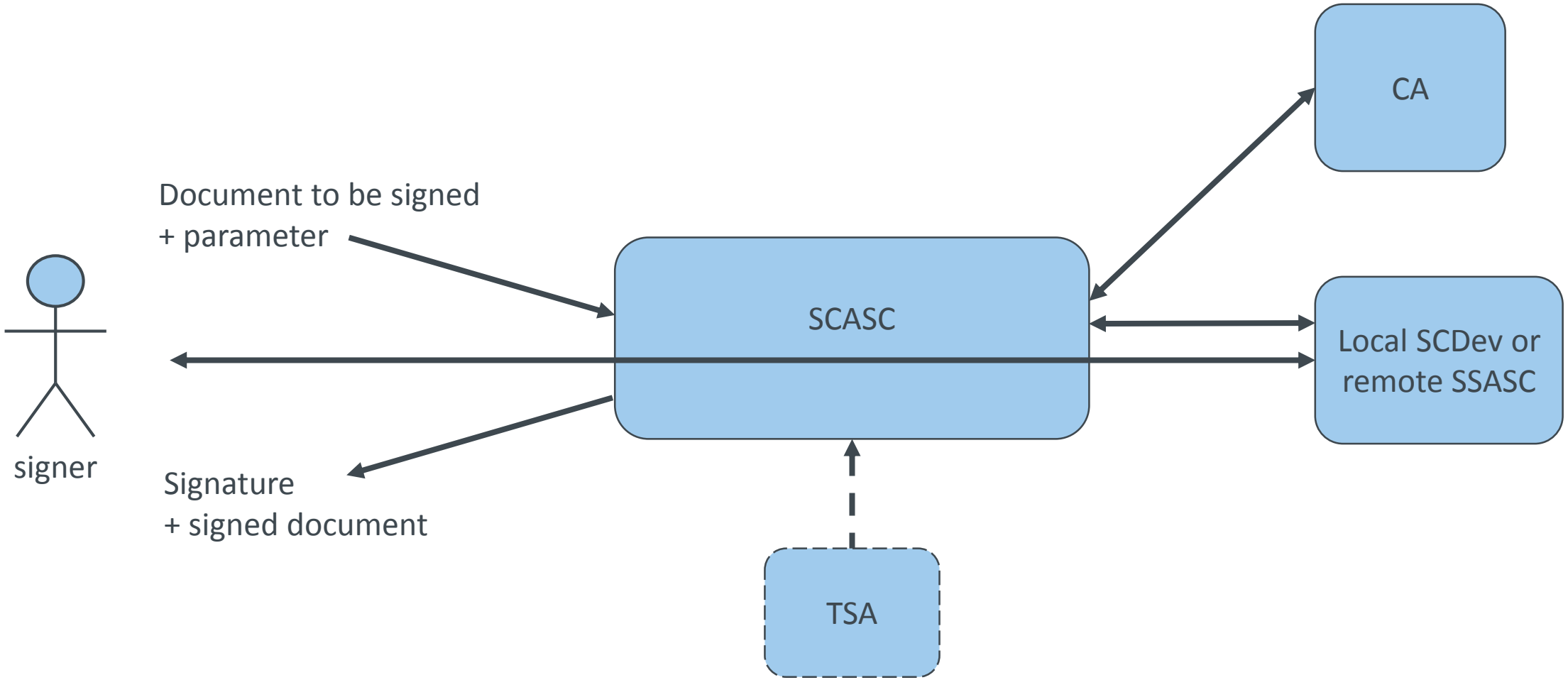
TS 119 431-2

Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation

- Based on EN 319 401 (General Policy Requirements for Trust Service Providers)
- References to some requirements of TS 119 101 (Policy and security requirements for applications for signature creation and signature validation)
- Not necessarily in combination with a server signing application service component (SSASC)
- Creates the (C/X/P)AdES signature
- Can provide presentation of document to be signed: the goal is to make sure that the signer is aware of what he/she is signing

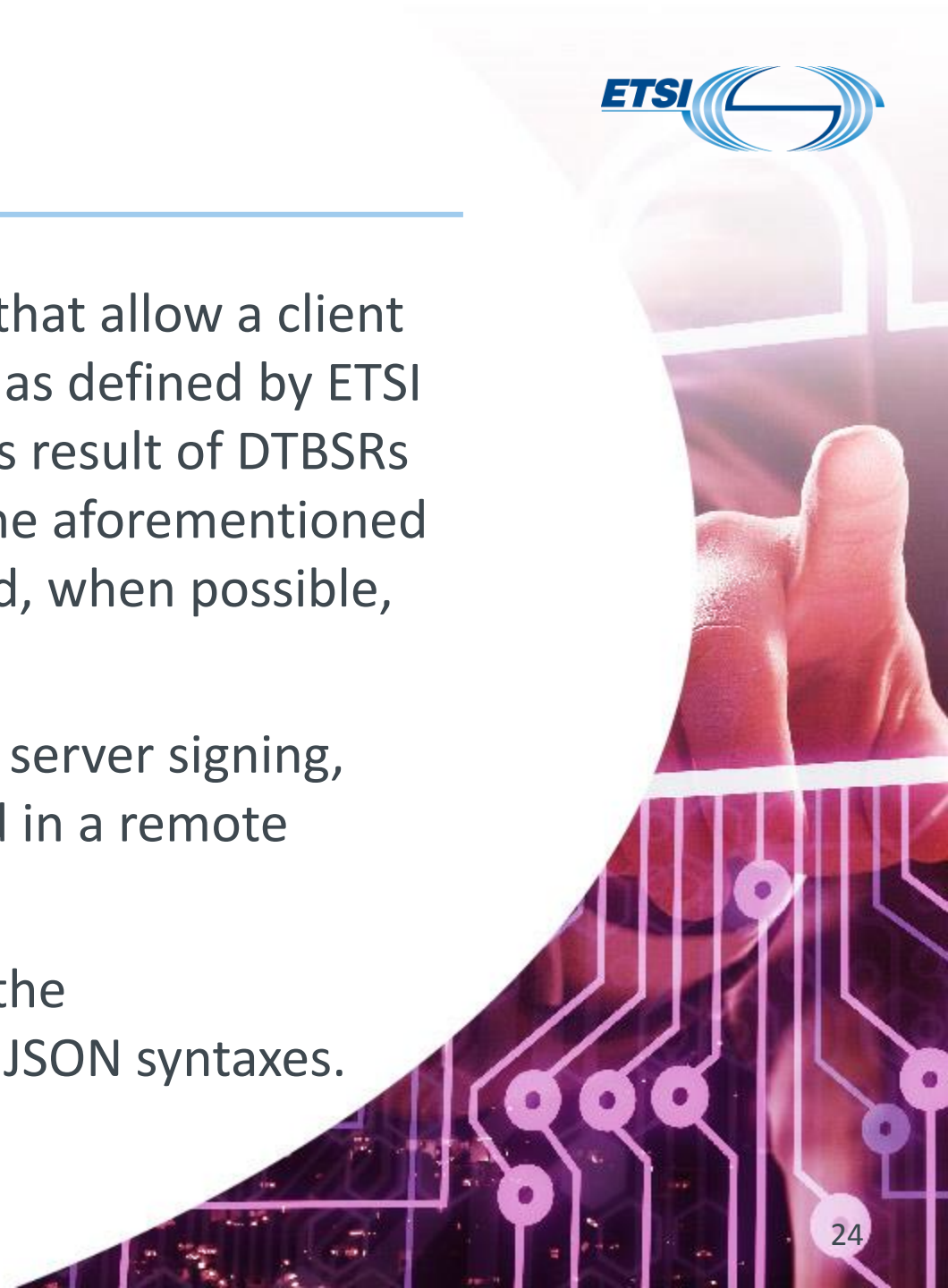


Architecture



TS 119 432

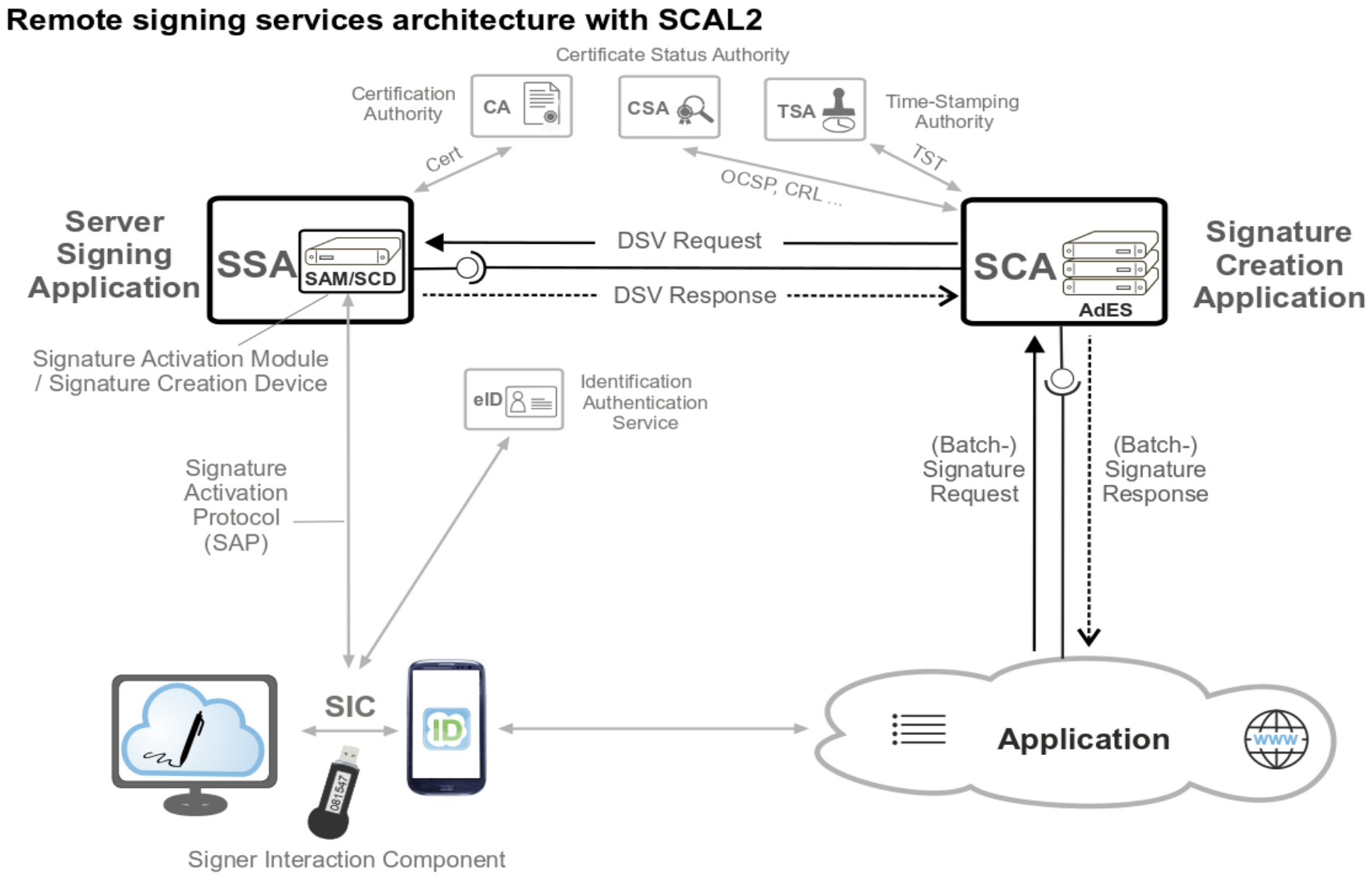
- ETSI TS 119 432 defines protocols and interfaces that allow a client to request the creation of AdES digital signatures as defined by ETSI EN 319 102-1 and/or a Digital Signature Values, as result of DTBSRs signature, to a remote signing server and allow the aforementioned server to return the signature creation results and, when possible, the AdES or DSV requested.
- ETSI TS 119 432 specification is limited to remote server signing, that is the context in which the signing key is held in a remote shared service.
- ETSI TS 119 432 defines two implementations of the aforementioned protocol, one in XML and one in JSON syntaxes.



Scope

- The protocol allows to request creation and return creation result for the following types of digital signatures:
  - Digital Signature Values
  - CAdES signatures
  - PAdES signatures
  - XAdES signatures
- The protocol supports both synchronous and asynchronous management of requests and responses.
- The protocol supports the creation of enveloping, enveloped and detached signatures.

Signature creation process



Implementations

- The implementations of the protocol defined in ETSI TS 119 432 take as starting point the protocols specified by.
  - OASIS Digital Signature Services eXtended Technical Committee;
  - Cloud Signature Consortium.
- The implementations of the protocol in XML are profiles of the OASIS DSS-X TC core document version 2.0 which is under production by OASIS.
- The implementations of the protocol in JSON are profiles of the CSC document “Architectures, Protocols and API Specifications for Remote Signature applications” version 1.0.3.0.

OASIS DSS-X and CSC profiles

OASIS DSS-X

- A XML Schema definition of the component is provided if the component is not taken from OASIS DSS-X specifications, OR
- A reference to the XML Schema definition of the component is provided if the component is defined in some OASIS DSS-X specification and is further profiled here.
- The specification of the processing model for the server is provided if the component is not taken from OASIS DSS-X specifications OR the component is taken from some OASIS DSS-X specification but it is further profiled here.

CSC

- A JSON Schema definition of the component is provided.
- The specification of the processing model for the server is provided if the component is not taken from CSC specifications OR the component is taken from CSC specification but it is further profiled here.

What's coming next

TSP requirements evolvements: EN 319 411-x EN 319 412-y

- 319 412-2 & 3 Clarification on key usage for signature and seals
- 319 412-1 Validity assurance for short term / key controlled certificates
- 319 412-2 Update on requirements for root certificates / trust anchor and authority information access
- 319 412-3 Update to allow shortening of organisation names > 64 characters
- 319 412-5 QCStatement for non-EU countries

Qualified Certificates under PSD2

Directive 2015/2366/EU aimed at regulating payment services

ETSI joint work with ECB ERPB PIS WG / Open Banking Europe taking into account input from European Banking Authority

Qualified Certificate profiles

- PSD2 Qualified Website Authentication Certificates
- PSD2 Qualified Seal Certificates

CA Policy Requirements for PSD2 Qualified Certificate

- Requirements for validation of PSD2 specific attributes
- Revocation of PSD2 certificate due to change in PSD2 attribute status
- Involves interaction with National (Financial) Competent Authority

Long-Term (signature/seal) Preservation

Near completion:

- TS 119 511 Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
- TS 119 512 Protocols for trust service providers providing long-term data preservation services

Signature Formats & Validation: JSON Signatures

- New work item to define equivalent to CAdES / PAdES / XAdES for JSON data format as commonly used in Web environment

Signature Validation

Standards:

- TS 119 102-2: Signature Validation Report - Published
- TS 119 441 (2018-08): Policy Requirements for TSPs Providing Signature Validation Services (including annex for qualified service) - Published
- TS 119 442 (2019-02): Protocol for Signature Validation Services - Published
- TS 119 172-4: Signature Validation Policy for European Qualified Electronic Signatures/Seals Using Trusted Lists – Draft for approval

Protocol features:

- Supports both XML and JSON exchanges
- Aligned with OASIS DSS V2.0

Trusted Lists

- TS 119 615 Standard near completion
  - on the use of information within a Trusted List by relying parties,
  - how to process a trusted list in order to obtain information about a QTSP and QTS(s) it provides
  - Building blocks
    - for validating a qualified signature/seal (see also upcoming TS 119 172-4)
    - To link trusted list information to evidences produced by some types of trust services: validation service, preservation service, electronic registered delivery services
- TS 119 612 / 602 Updates
  - Work deferred – new version not expected before 2020

TSP audits: EN 319 403

Revised draft EN 319 403 Part 1 under public review :

- Audit of component services
- Clarification regarding handling of TSP requiring corrective actions
  - Audit report issued identifying corrective actions required.
  - Not declared as conformant
- New Annex giving guidance on expected time to carry out audited
- Other minor changes

Aim to publish as EN by end 2019

CAB may not be required to apply new standard for up to 2 years

New Activities

Machine-processible signature policy formats

- TS 119 172-2: XML format for signature policies
- TS 119 172-3: ASN.1 format for signature policies

Timescale:

- Drafts for public review: June 2019
- Published: End November 2019

Global acceptance of European Trust Services

Study report on Global Acceptance of EU Trust Services

- Analysis of international, regional and sector specific communities adopting Public Key Infrastructure technology

International co-hosted workshops:

- Target regions; Japan, North America, South America, Africa

Identity Proofing of trust service subjects

New work on TS about “Policy and security requirements for trust service components providing identity proofing of trust service subjects.

- Can be a separate “component service”
- Subject may be for remote registration
- Supporting:
  - EN 319 411-1/2: TSP issuing certificates
  - EN 319 521 / 532: ERDS / REM
  - TS 119 431: Remote signing

Conclusions

Information on available standards and current activities:
https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

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

CEN standards: available through National Standards Organisations

Updates on standardisation:
https://list.etsi.org/scripts/wa.exe?SUBED1=e-signatures_news&A=1