CEN & ETSI standards & eIDAS Compliance

Nick Pope - Thales
Vice Chair, ETSI TC Electronic Signature & Infrastructures

Jan Ulrik Kjærsgaard – Cryptomathic
Editor CEN EN 419 241-2 (Remote Signing)

eIDAS and centralised electronic signatures – transforming digitisation
London, 14th September, 2016

Agenda

eIDAS Regulation & Standards

- eIDAS compliance requirements for signatures
- Difference compliance levels and forms of signature
- eIDAS Standards Framework

Standards for Remote (centralised server) Signing

CRYPTOMATHIC

THALES

eIDAS "Levels" of Compliance Electronic Signature :

Electronic Signature

- Anything which is used to sign

Advanced Electronic Signature

- Electronic Signature with "sole control" properties such as provided by public key technology
- TSP can offer what is considered current good practice but takes on liability

Qualified Electronic Signature

- Advanced Electronic Signature which meets specific technical & security requirements as specified in the regulation
- Supervisory authority confirms that TSP meets regulatory requirements (can be demonstrated using recognised standards

CRYPTOMATHIC

THALES

eIDAS "Levels" of Compliance Electronic Seal:

Electronic Seal

- Anything which is used to ensure the origin and integrity of data.

Advanced Electronic Seal

- Electronic Seal with "control" properties
  i.e. Signing key controlled by organisation rather than individual

Qualified Electronic Seal

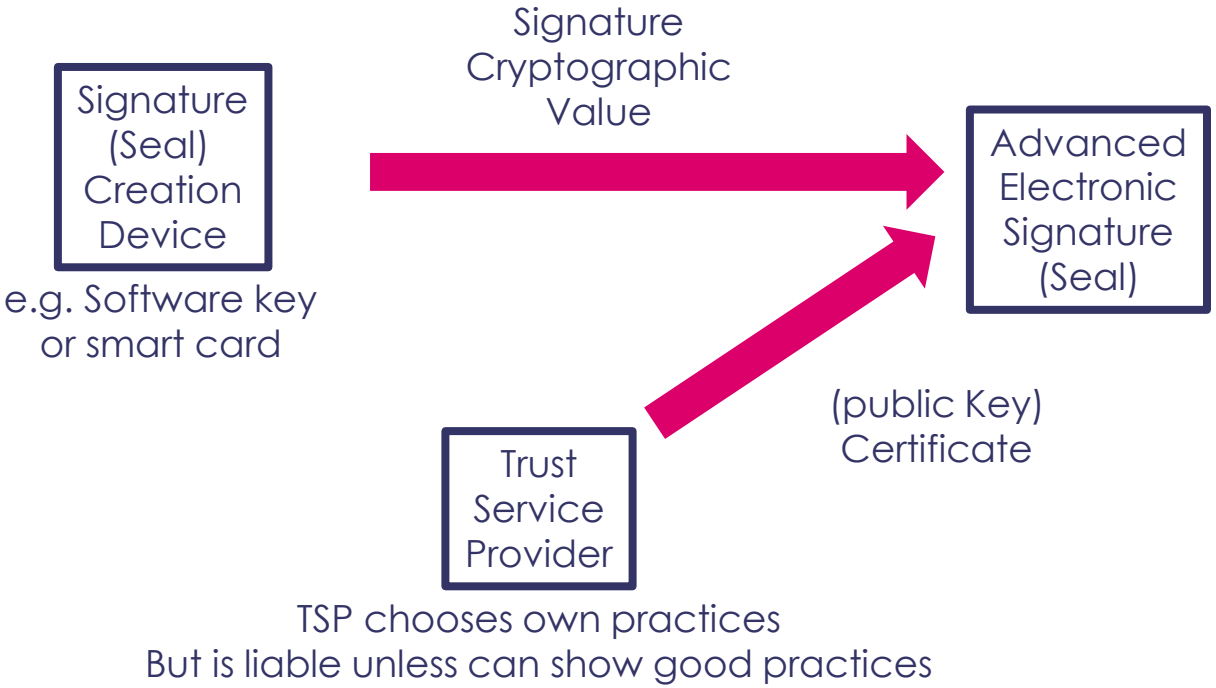
- Advanced Electronic Seal which meets specific technical & security requirements equivalent to electronic signature (mutatis mutandis).

CRYPTOMATHIC

THALES

Elements of eIDAS Advanced Electronic Signature *

* Mutatis mutandis seals

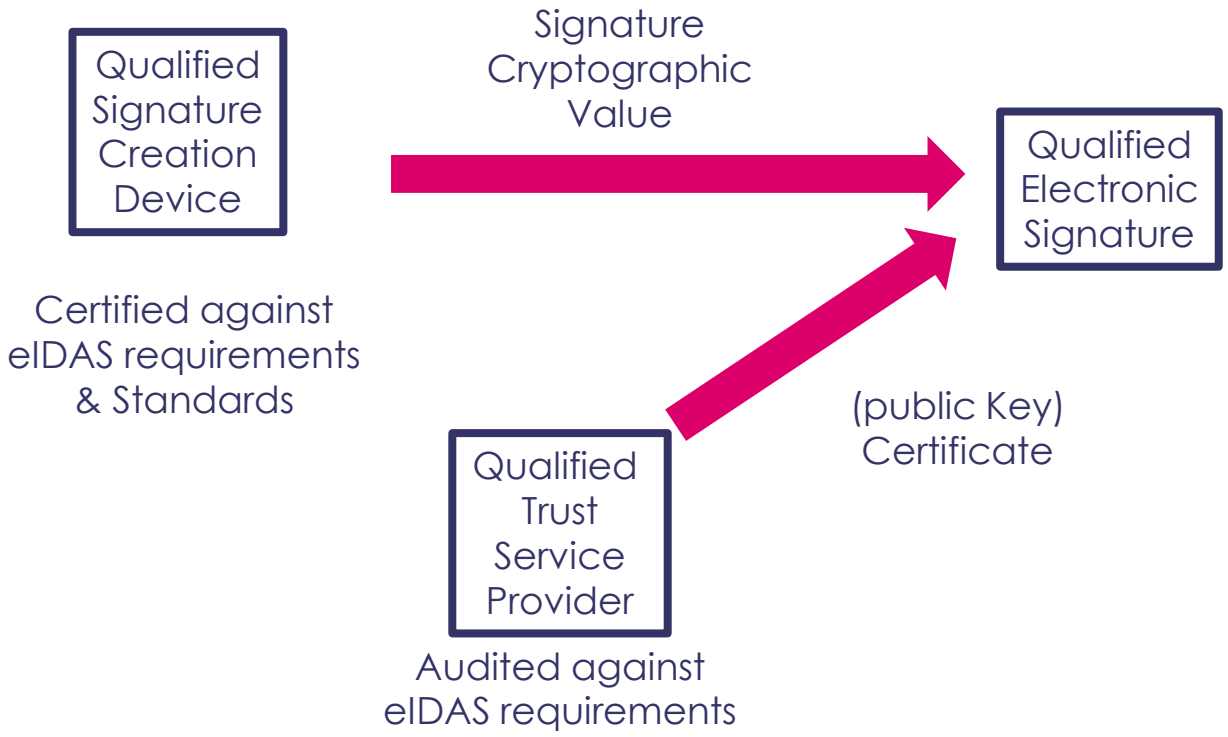


CRYPTOMATHIC

THALES

Elements of eIDAS Qualified Electronic Signature *

* Mutatis mutandis seals



CRYPTOMATHIC

THALES

eIDAS Conformance Requirements for Qualified Electronic Signatures *

Article 27: Electronic Signature Format

* Mutatis mutandis seals

- Member states shall recognise advanced and qualified electronic signature formatted as specified in implementing acts

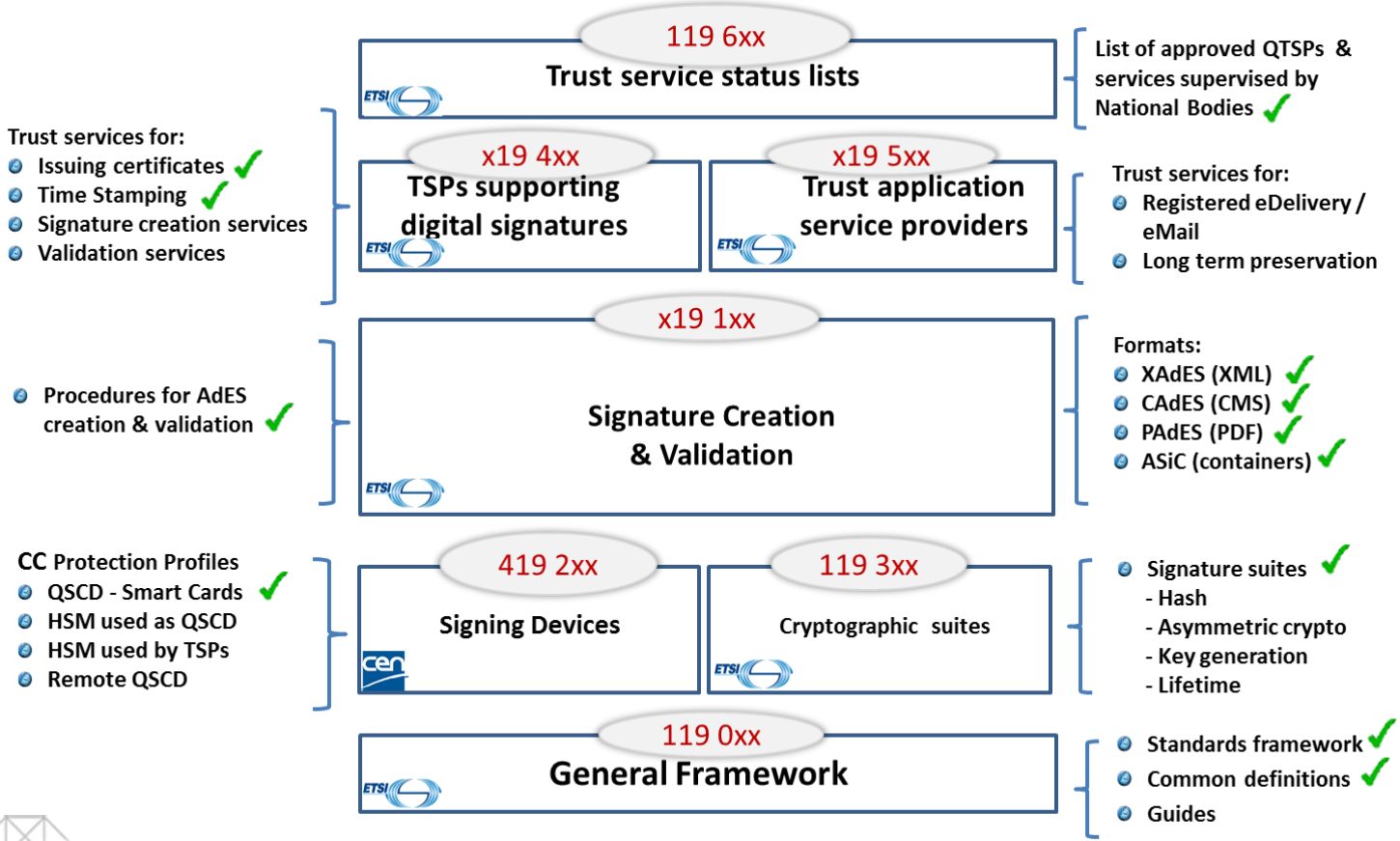
Article 20: Qualified Trust Service Providers (TSPs)

- Qualified TSPs shall be audited every 24 months to demonstrate that they fulfil eIDAS requirements
- eIDAS Standards are guidance only
  - eIDAS standards provide a clear means of demonstrating that eIDAS requirements are fulfilled
  - EU member states may add their own "guidance"

Article 30: Qualified Signature Creation Device (QSCD)

- Shall used QSCD as per standards as specified in implementing acts
- If no recognised EU standards available QSCD can be evaluated by national body using "comparable security levels"

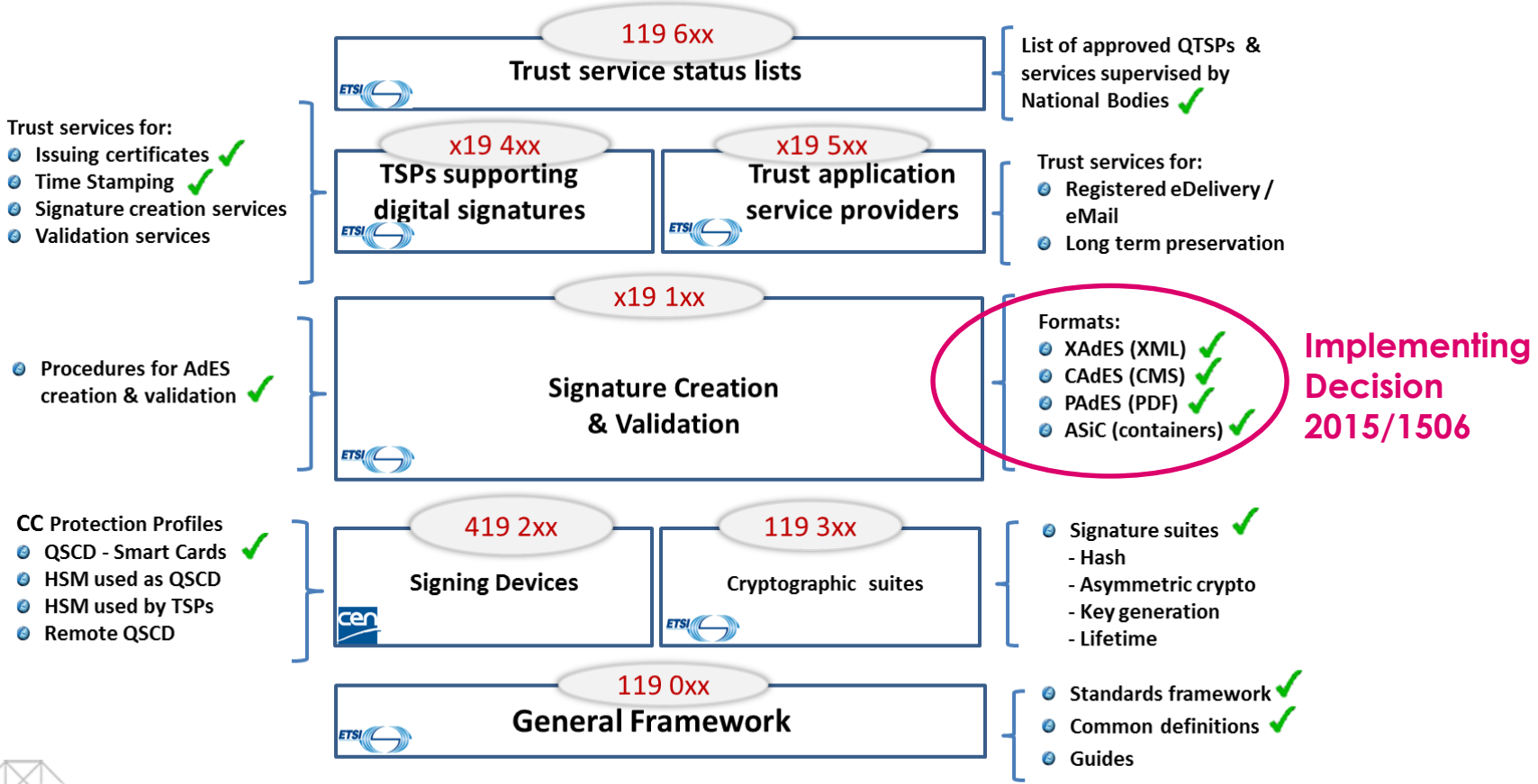
eIDAS Standards Framework



CRYPTOMATHIC

THALES

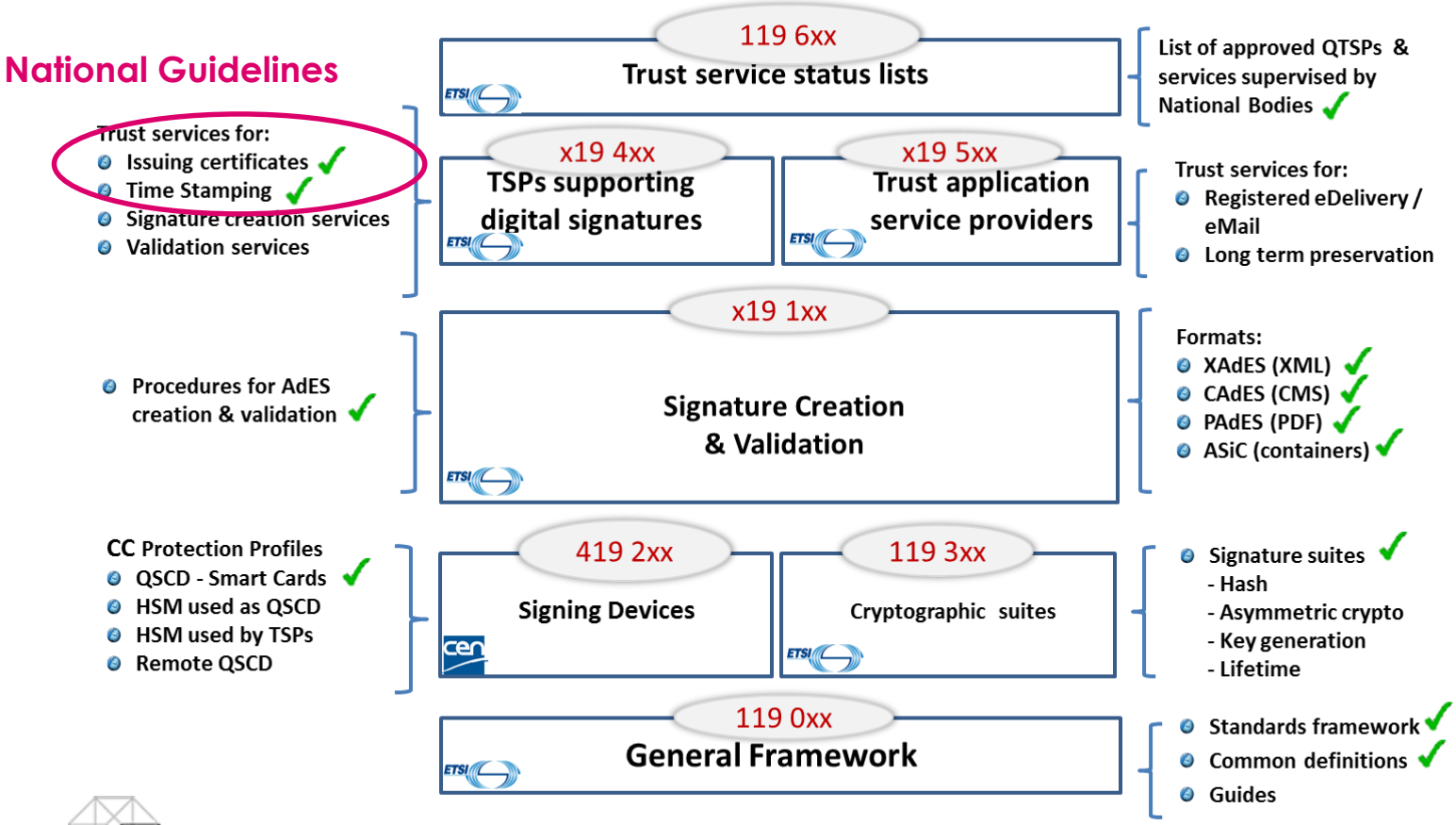
eIDAS Standards Framework – Advanced e-Signature / e-Seal Formats



CRYPTOMATHIC

THALES

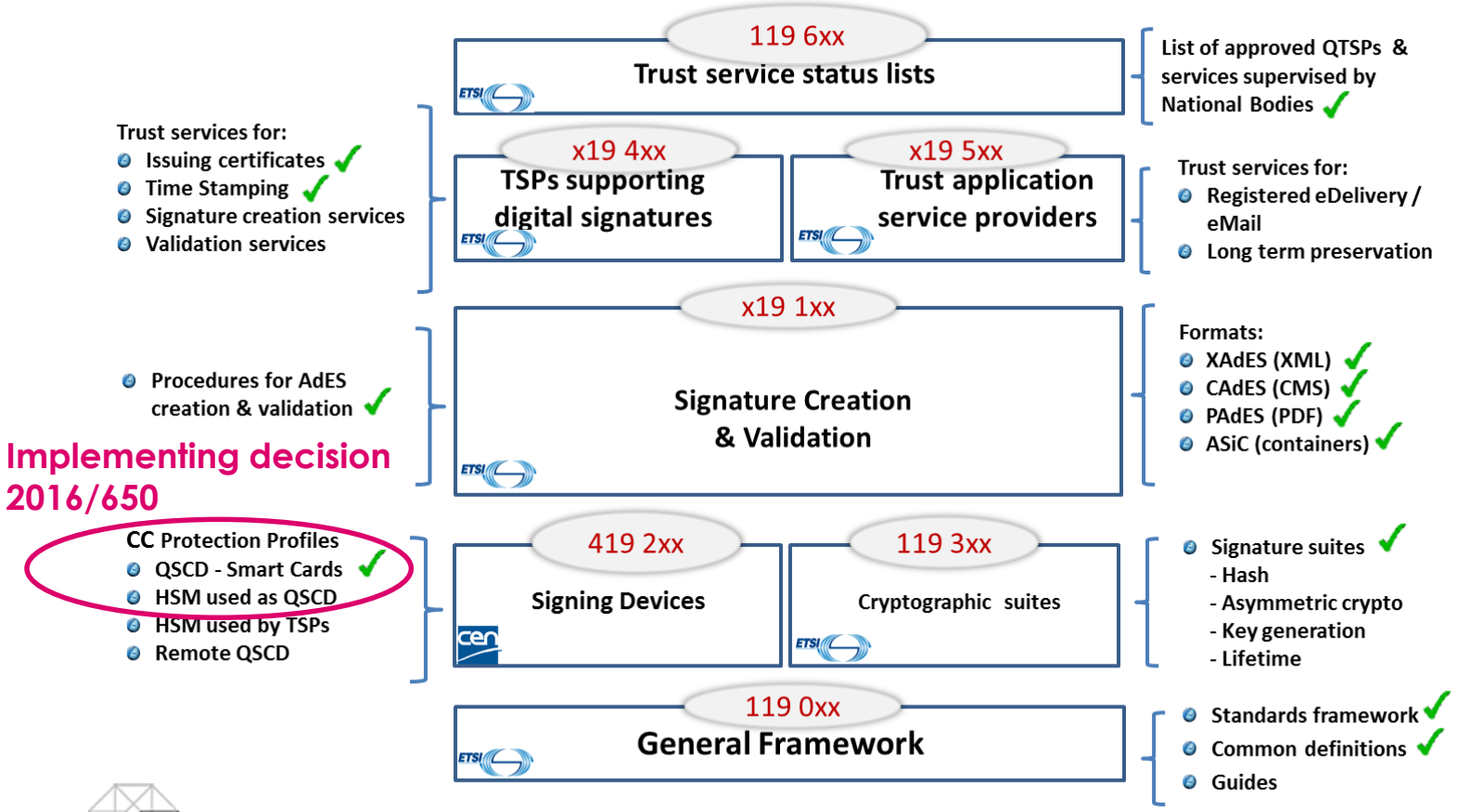
eIDAS Standards Framework – Trust Services supporting signatures



CRYPTOMATHIC

THALES

eIDAS Standards Framework – Trust Services supporting signatures



CRYPTOMATHIC

THALES

Implementing Decision 2016/650 on Qualified Signature / Seal Creation Devices

Reference made to:

- Common Criteria evaluation standards
- EN 419 211 – Protection Profiles for QSCD mainly applied to smart cards

For HSMs used by TSPs mentions other certification schemes are generally used

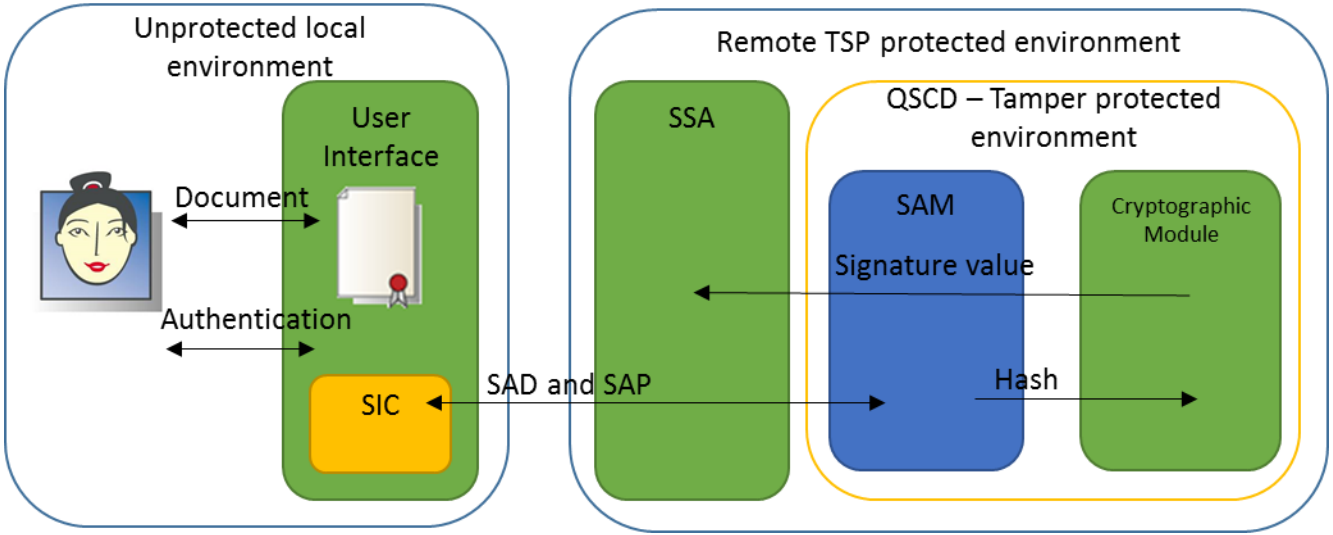
- Preference for Common Criteria certified HSMs over FIPS 140-2
- Standard based on Common criteria (EN 419 221-5) nearing approval
- May be accepted as Qualified Signature / Seal device

For Remote (centralised server) signing repeats statement from eIDAS regulation that in the absence of standards QSCD can be evaluated by national body using “comparable security levels”

- Expect upcoming standard (EN 419 241) to be recognised

Devices certified by nations under Directive accepted

Basic idea: Remote/Central/Cloud Signing



CRYPTOMATHIC

THALES

Sole Control Requirements

eIDAS

- Annex II, section 1.d: The private key can only be used by the owner.

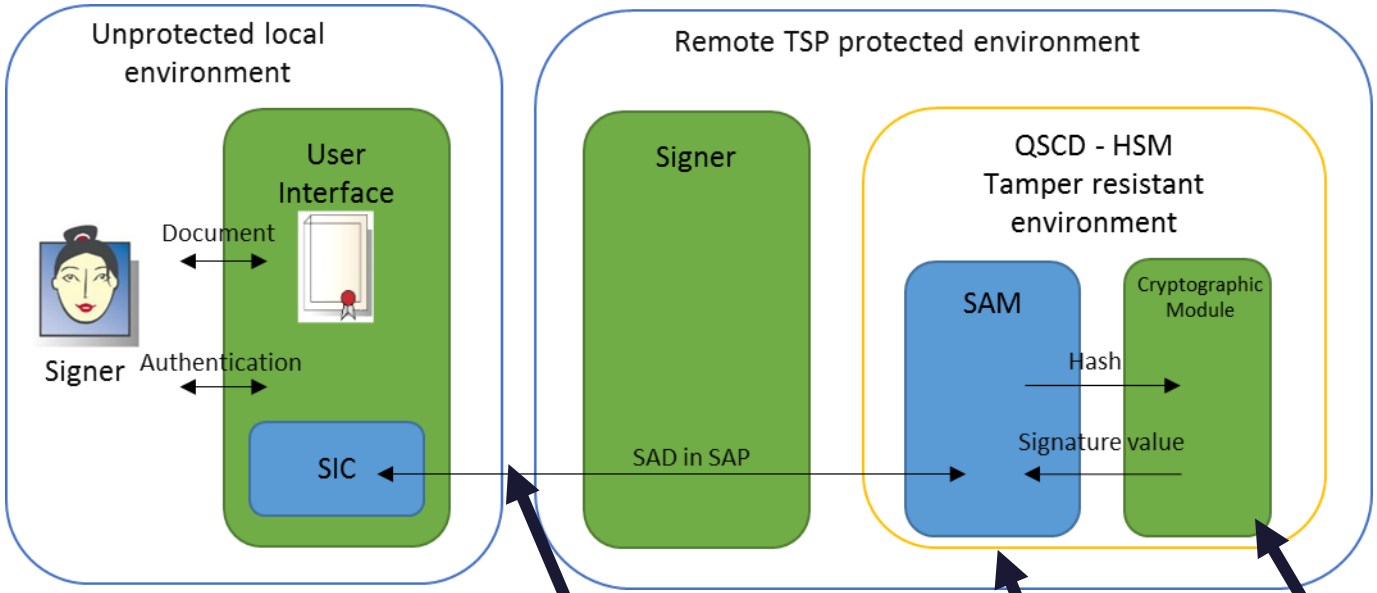
CEN TC 224 WG 17

- Signature Activation Protocol (SAP)
- Signature Activation Data linking:
  - User identification
  - Document to be signed (hash)
  - Signature key identifier

CRYPTOMATHIC

THALES

EN 419 241



TS 419 241-1
Security Requirement for Trustworthy Systems Supporting Server Signing

PP 419 241-2
QSCD for Server Signing

PP 419 221-5
Cryptographic Module for Trust Services
Server Signing

QSCD:

- HSM + SAM

Signature Activation Module

- Checks the SAD:
  - User is authenticated
  - The hash
  - Key identifier
- Uses a CM for signature operation

CRYPTOMATHIC

THALES

Important Standards

Certified SAM

- SAM shall be certified to CEN PP EN 419 241-2
- Draft PP written by Cryptomathic, planned for evaluation Q1 2017.
- Sets requriement on environment:
  - Certified HSM
  - Audited TW4S

Certified HSM

- HSM certifed CEN PP EN 419 221-5
- SAM can be implemented as an extension (SEE) to Thales nShield product

Audited TW4S

- TW4S is audited against CEN EN 419 241
- Or interim standard TS 419-241

Conclusions

- **Standards nearing completion for Remote Signing**
- **The Cryptomathic solution , running on Thales nShield HSM, is already aligned with the draft standards**
- **Expecting remote standards to be adopted in revision to implementing act**
- **Number of countries accepting remote signing solutions pending agreement of standards**
- **Obtaining copies of standards:**
  - For free download of ETSI standards: http://www.etsi.org/standards-search
  - For CEN standards access national standards organisation

CRYPTOMATHIC

THALES