Replacing the Norwegian «Kravspesifikasjon for PKI i offentlig sektor» by recommended standards

Jon Ølnes, Product Manager Nordics, Signicat AS

Norstella eID Forum

2018-04-12

SIGNICAT

Disclaimer

Please note that this presentation is for information purposes only, and that Signicat has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation.

The future strategy and possible future developments by Signicat are subject to change and may be changed by Signicat at any time for any reason without notice.

This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Signicat assumes no responsibility for errors or omissions in this document.

«Kravspesifikasjon for PKI i offentlig sektor» (1)

- Norwegian, national specification based on standards
- Mandatory, reference catalogue of government IT-standards
  - But not included among the government standards mandated by regulation
- Base for highest assurance level for eID
  - Means a Norwegian «level 4» eID today must be PKI-based

- Seriously outdated – latest version is June 2010
  - Refers old and obsolete standards
  - Not compatible with eIDAS requirements

«Kravspesifikasjon for PKI i offentlig sektor» (2)

- Two purposes:
  - Self-declaration of conformace with supervision according to «regulation on voluntary self-declaration for certificate issuers»
    - » Ticket to trade for delivery of PKI-based services to the public
    - » In reality also ticket to trade in private sector
  - Base for procurement of PKI-services to the public sector

- Self-declaration is a requirement in the brand new «regulation on anti money-laundry», pointing at electronic signature (and not eID)
  - § 4-3 (4) Elektronisk signatur er gyldig legitimasjon for fysisk person når identiteten ikke skal bekreftes ved personlig fremmøte. Elektronisk signatur må tilfredsstille kravene i forskrift 21. november 2005 nr. 1296 om frivillige selvdeklarasjonsordninger for sertifikatutstedere § 3 og som er oppført på publisert liste i henhold til § 11 første ledd i nevnte forskrift.

The requirements

- Three classes of certificates:
  - Person-High, builds on qualified certificate (according to the e-signature directive), certificates for authentication/encryption need not be qualified
  - Person-Standard, builds on ETSI standard LCP (Lightweight Certificate Policy)
  - Enterprise, corresponding to eIDAS e-seal
- Requirements are:
  - A: Mandatory
  - B: Recommended – may be turned to mandatory for procurements
  - V: Conditional – the supplier may choose to deliver, in which case requirements become A or B requirements

What does eIDAS regulate?

- Trust services regulated EU wide (including national level)
  - Based on the open market principle
  - Limited opportunities for further national regulation
  - Standards/profiles may be recommended (not mandated) nationally
  - Sectorial laws/regulations/rule-sets may require specific trust services or specific levels of signatures/seals
- eID is only regulated cross-border for public services
  - National regulation on eID is a national competence
  - Alignment of national regulation with eIDAS recommended
  - Cross-border eID for private sector encouraged but not mandated

eIDAS and standards

- Standards not mandatory – fulfilment of eIDAS is enough to be qualified
  - Intention is to build on standards
  - Conformity assessment is very hard unless standards are used
- Commission may devise implementing acts referring standards
  - Compliance with referenced standards imply presumption of eIDAS conformance – but still not mandatory to use the standards
  - Commission has been reluctant to use this mechanism, done for
    - Trusted List format
    - Signature formats for public sector
    - QSCD certification

The «requirements PKI» and eIDAS

- eIDAS separates eID and e-signatures/seals
  - «Requirements PKI» assumes they are bundled with eID PKI-based
- Standards cannot be mandatory for eIDAS
  - Means «requirements PKI»'s mandatory status is not allowed for qualified trust services
  - Self-declaration also not allowed for eIDAS qualified trust services
  - Still possible to have mandatory national standards for eID and non-qualified
- eIDAS implementing acts pose standards requirement
  - «Requirements PKI» has outdated specs for QSCD (then SSCD)
  - And outdated specs for signature formats (although «requirements PKI» does not mandate any specific format)

What to do?

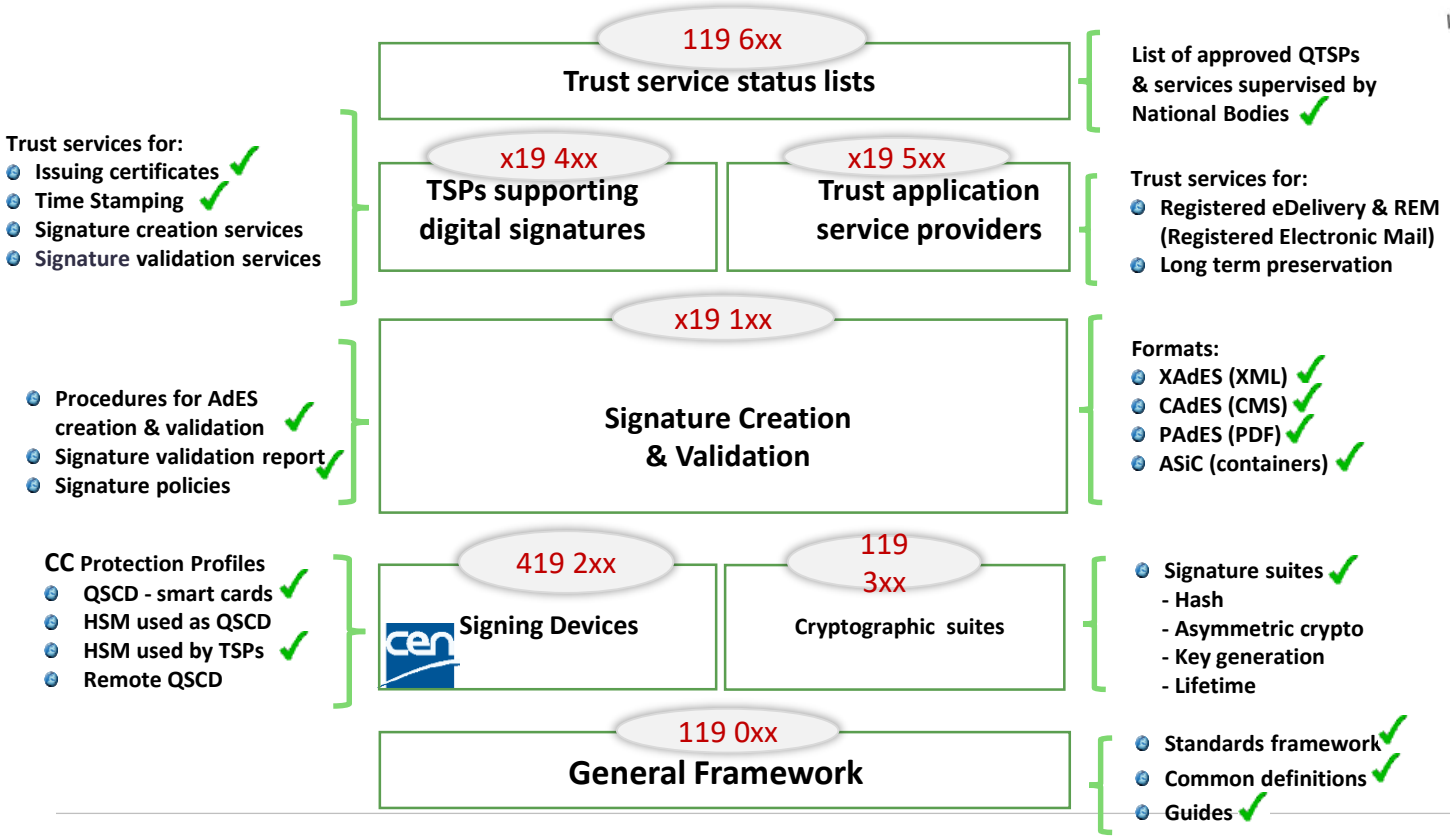
- Regulate eID technologically neutral and aligned with eIDAS
  - New assurance level framework for public sector (but see next slide)
- Change self-declaration to point to new assurance level framework
  - Revised regulation on self-declaration
  - Changes in other laws and regulations
- Recommended standards for trust services, signatures, seals
  - As far as standards are mature
  - Cover both qualified and non-qualified
  - Government standards should be OK – probably not worthwhile to promote to full national standards

Suggestions for eID regulation in Norway

- Do not pose sectorial requirements for use of eID or trust services unless it is really needed (from risk evaluation)

- eID should be regulated for society, not only for government!
  - Proposal is assurance level framework for government
  - Formal status of framework unclear, not founded in law or regulation?
  - Assumed effect for society – but the formalities are not that clear
- Better approach: Assurance level framework **for eID in society**
  - Plus ensure that the «broker» role is regulated: Signicat, Idfy, Nets, ID-porten etc.
  - Finland: «law on strong electronic identity» and Finnish Trust Network
  - Denmark: upcoming regulation of MitID including mandatory broker role
  - Denmark, Finland: brokers are supervised (and even audited in Denmark)

ETSI trust services standards framework

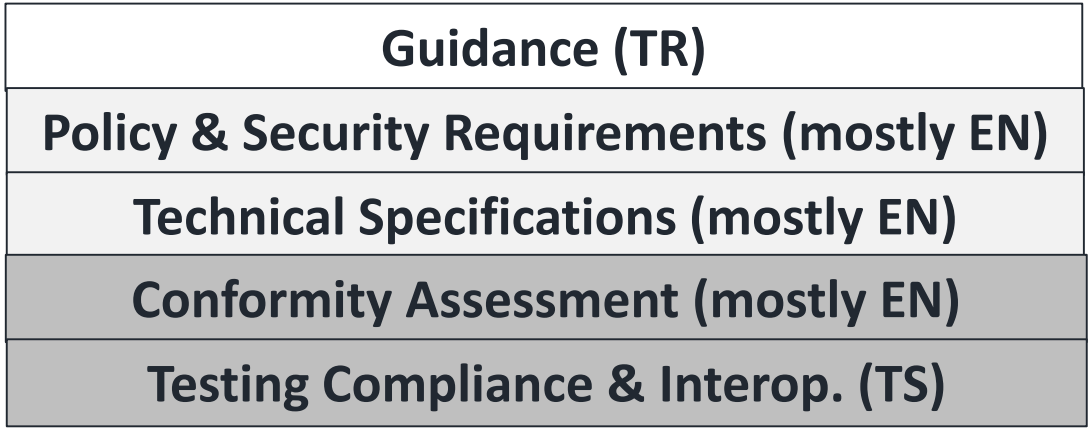


Those not ticked are under publication or near publication

When completed, all eIDAS trust services are covered

SIGNICAT

Stack of documentation



EN: European Norm – full European Standard
TS: Technical Specification – less formal standard
TR: Technical Report – guidelines etc., no normative requirements
SR: Special Report – study report of an area (e.g. mobile signatures)

Recommended standards area by area

- Red text means recommended
- Black text means for future consideration
- Standards for conformity assessment and testing may be added

- Versions of standards must also be set for government standards

Area 1: Signature creation and validation

- Formats:
  - ETSI EN 319 122-1, ETSI EN 319 132-1 (XAdES), ETSI EN 319 142-1 (PAdES), ETSI EN 319 162-1 (ASiC)
  - Possibly also conformance and testing specifications
  - Implementing decision (EU) 2015/1506 specifies mandatory formats and becomes Norwegian regulation – additional formats to those above
    - » Outdated – refers to older versions of the ETSI specifications
    - » Has some really problematic openings for non-standard formats
- Procedures for signing and validation:
  - ETSI EN 319 102-1 (consider ETSI TS 119 102-2 on validation report)
- Signature policies:
  - Framework for specifying «what, why, by whom, and how»
  - Consider ETSI TS 119 172-1 and other policy specifications

Area 2: Signing and other devices

- QSCD covered by implementing decision (EU) 2016/650
  - Will become Norwegian regulation
  - CEN EN 419 211-1-6 for smart card type equipment
- Consider: Certification for the QTSPs
  - CEN TS 419 221-1-4 (crypto module certification)
  - CEN EN 419 221-5 (HSM certification for QTSP use)
  - CEN TS 419 261 systems managing certificates and time-stamps

- Upcoming: Server signing, so keep an eye on:
  - CEN EN 419 241-1-2 (server signing system)
  - CEN EN 419 221-5 (again – this time HSM for server signing)
  - These may soon be added to (EU) 2016/650

Area 3: Cryptography

- Crypto requirements should be stated
  - Crypto is a national competence – some countries are strict on this
  - Public key algorithms and key lengths, hash functions, support functions like key generation, padding etc.
  - NSM (national security authority) recommendations
  - SOG-IS recommendations – EU advisory group
  - ETSI aligns with SOG-IS, ETSI TS 119 612

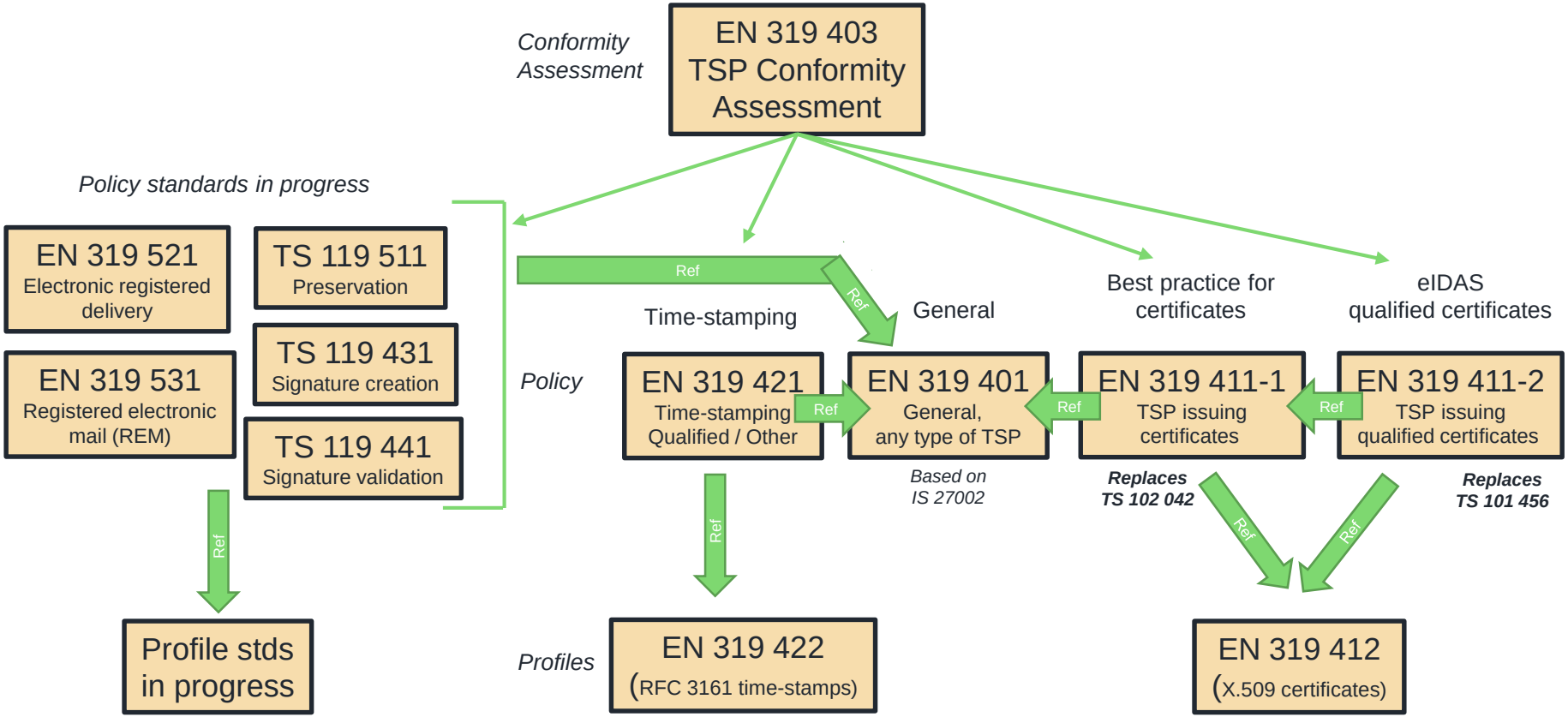
Area 4: Trust services supporting digital signatures

- Conformity assessment (for all trust services)
  - ETSI EN 319 403 (maybe a Norwegian Accreditation decision)

- Certificate authorities
  - Certificates for electronic signature, electronic seal, and website authentication
    - » Consider requirements for QWAC for government services?
  - Certificate policies:
    - » ETSI EN 319 401 – base policy for all trust services
    - » ETSI EN 319 411-1 – certificate issuing, choose relevant policy levels (is there a need to map policy levels to eID levels in the assurance level framework?)
    - » ETSI EN 319 411-2 – certificate issuing, qualified certificates
  - Certificate profiles:
    - » ETSI EN 319 412-1-5
    - » Specification on encoding of names and identifiers (SEID-1 and SEID-2) still needed
  - Consider later CEN EN 419 221-5 for crypto equipment (HSM) and other CEN CC profiles

Area 4: Continued

- Time-stamp services:
  - ETSI EN 319 421 – time-stamp policy
  - ETSI EN 319 422 – time-stamp protocol, builds on RFC 3161
  - Consider later CEN EN 419 221-5 for crypto equipment (HSM)
  - Consider later CEN EN 419 231 on CC-evaluation of time-stamping system
- Validation services (for e-signatures and e-seals)
  - Not now, standards are brand new and immature
  - ETSI TS 119 441 (policy) and ETSI TS 119 442 (protocol)
- Signing services
  - Not now, standards are not yet published and are immature
  - ETSI TS 119 431-1 (policy for service operating remote SCdev/QSCD), ETSI TS 119 431-2 (policy for service generating xAdES format) ETSI TS 119 432 (protocols, for both)
  - See also CEN protection profiles for remote signing (the SCdev/QSCD alternative)
  - ETSI M-COMM specifications are also in use (e.g. BankID Mobile)


Conformity Assessment
EN 319 403 TSP Conformity Assessment
Policy standards in progress
EN 319 521 Electronic registered delivery
TS 119 511 Preservation
EN 319 531 Registered electronic mail (REM)
TS 119 431 Signature creation
TS 119 441 Signature validation
Ref
Profile stds in progress
Policy
Time-stamping
General
Best practice for certificates
eIDAS qualified certificates
EN 319 421 Time-stamping Qualified / Other
EN 319 401 General, any type of TSP
EN 319 411-1 TSP issuing certificates
EN 319 411-2 TSP issuing qualified certificates
Based on IS 27002
Replaces TS 102 042
Replaces TS 101 456
Profiles
EN 319 422 (RFC 3161 time-stamps)
EN 319 412 (X.509 certificates)

Area 5: Other trust services

- Electronic Registered Delivery Services
  - Not now, standards are under publication and immature
  - ERDS base standards: ETSI EN 319 521 (policy), ETSI EN 319 522 (protocol)
  - REM (Registered Electronic Mail): ETSI EN 319 531 and ETSI EN 319 532
  - Consider base standards later – secure digital mail and more
  - REM is not relevant for Norway
- Preservation service (primarily for e-signatures and e-seals)
  - These are not archiving standards
  - Not now, standards are not published and immature
  - ETSI TS 119 511 (policy), ETSI TS 119 512 (protocol)

Area 5: Trusted lists

- Covered by implementing decision (EU) 2015/1505
  - Becomes Norwegian regulation
  - Refers an old version of ETSI TS 119 612 – should have been updated
  - Weakness: no policy and security requirements for TL issuers
  - New specifications upcoming on how to use TLs

End of presentation

jon.olnes@signicat.com
https://signicat.com