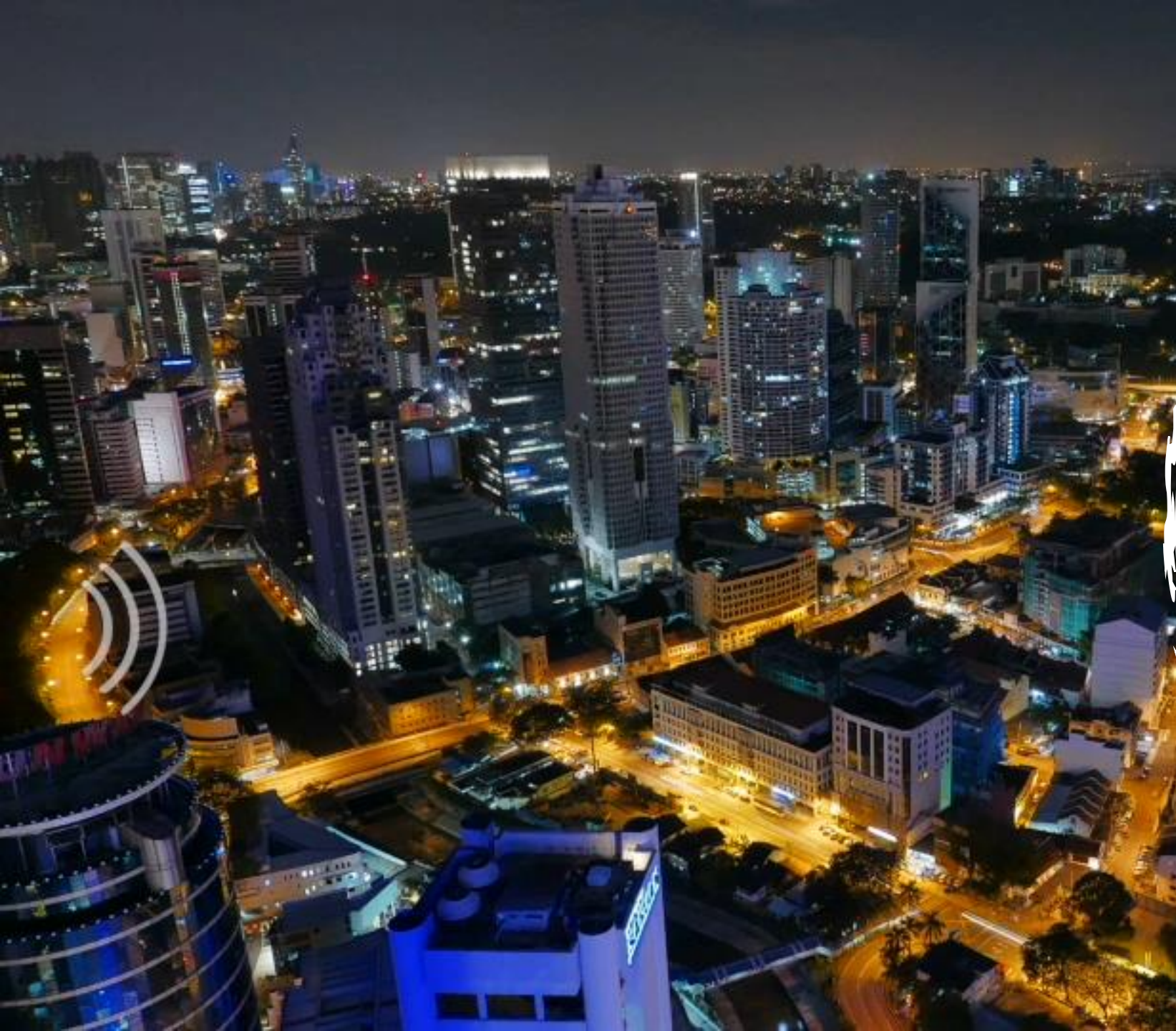

ETSI ESI on eIDAS2: new Trust Services and Digital Wallets

Presented by:
Santino Foti, **ETSI TC ESI** Vice Chair

For: **9th ENISA** Trust Services and eID forum

11/10/2023

For:

Co-organised by enisa TÜVIT TÜVNORDGROUP d-trust.

Agenda

- Overview on new Trust Services, eIDAS 2.0 and EU Digital Wallet
- Overall map of ETSI/ESI standards
- General and evolution maintenance of existing ETSI/ESI standards
- Conclusion: possible new standards for support of eIDAS 2.0 EUDIW

Secure and trusted access to public/private services

Overview on core elements for a seamless access to EU services – what's in store (*)

- European Digital Identity (eID)
- European Digital Identity Wallets (EUDIW)

A new paradigm for a framework implementing a real shared social trust

- Global access to both citizens and enterprises
- Trustworthy (national and integrated) identification schemes
- Electronic attestation attributes for cross-border controlled sharing of identity data
- Moving towards personal mobile digital identity wallets
- Extension of the current qualified trusted services including emerging technologies and needs (electronic ledgers, remote signature, e-seals creation devices)

Principles in eIDAS 2 regulation proposal for EU Digital Identity Wallets

- Secure authentication and access to the services
- Great attention to be always updated and ready against cybersecurity threats

Acts in cybersecurity regulation and integrated national certification schemes

(*) *Council of the EU Press release 29 June 2023*

(Qualified) Trust services currently supported by ETSI ESI

- **Digital certificates, validation and preservation for digital signatures**
  - e-seals
  - e-signatures
- **Digital certificates for Website authentication**
  - Coexistence of web browser and EU trust controls
  - Identifies the person / organisation “behind” the website
- **Digital (S/MIME) certificates for secure e-Mail**
  - Sign/verify/encrypt/decrypt email messages
  - CA/Browser forum baseline requirements for compliance with major IT (Microsoft, Apple, Google, etc).
- **Registered e-Delivery**
  - ERDS – general requirements for registered e-Delivery
  - REM – specific application to registered electronic mail
  - Baseline and high degree of (cross-border) interoperability
- **Best practices policy and security requirements for Qualified Trusted Services**
  - Audit
  - EU trust infrastructure within global environment
  - Identity proofing
  - EU initiative on trusted lists for digital signatures (AdES) from 3rd countries

ETSI & CEN standards supporting eIDAS – overall map

Trust services:
- TSP Audit ✓
- Issuing certificates ✓ (Rev)
- Time Stamping ✓
- Signature creation services ✓
- Signature validation services ✓
- Identity proofing ✓ (Upd)
- Open Banking ✓ (Upd)
- Support for NIS 2 (New)
- S/MIME ✓ (New)
- Attribute Attestations (New)

- AdES creation & validation
  - Part 1: procedures ✓ (Upd)
  - Part 2: signature validation report ✓ (Rev)

CC Protection Profiles ✓
- QSCD - Smart Cards ✓
- HSM used as QSCD ✓
- HSM used by TSPs ✓
- Remote QSCD ✓

119 6xx
Trust service status lists

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

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

Trust services for:
- Registered eDelivery / eMail ✓ (Upd)
- Long term preservation ✓

Interop tests

x19 1xx
Signature Creation & Validation

Formats + Interop test:
- XAdES (XML) ✓ (Rev)
- CAdES (CMS) ✓ (Rev)
- PAdES (PDF) ✓ (Upd)
- ASiC (containers) ✓ (Upd)
- JAdES (JSON) ✓ (Upd)
- CB-AdES (CBOR) (New)

419 2xx
Signing Devices

119 3xx
Cryptographic suites

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

119 0xx
General Framework

- Standards framework ✓
- Common definitions ✓
- Guides ✓

✓	Published
(Rev)	Recently revised
(Upd)	Update in progress
(New)	New

Trust service – issuing digital certificates

STANDARDS TECHNOLOGIES COMMITTEES MEMBERSHIP EDUCATION ABOUT IPR MORE

Back

ETSI releases standard for IT solution providers to comply with EU regulation on electronic signatures in email messages

News | Press Releases | News and Press Releases | Magazine | Blogs | Press contact

Sophia Antipolis, 20 September 2023

ETSI has published a new standard on "Requirements for trust service providers issuing publicly trusted S/MIME certificates" (ETSI TS 119 411-6) helping Trust Service Providers comply with new standards for S/MIME certificates that are enforced since 1 September 2023. Secure MIME (S/MIME) certificates are used to sign, verify, encrypt, and decrypt email messages.

Since the 1st of September 2023, all TSPs issuing digital certificates used for S/MIME that are publicly trusted in certain operating systems and root certificate programs must comply with the S/MIME Baseline Requirements published by the CA/Browser Forum. The new ETSI standard will assist Trust Service Providers in asserting their compliance, when required. It will enable the same public key certificate used for signing electronic mail accepted by major IT solution providers (e.g., Microsoft, Apple, Google) to be also recognized as meeting the EU requirements for electronic signatures, issued to individual persons, and electronic seals, issued to organizations.

This new standard supports the EU regulation for electronic identities, authentication, and signatures (eIDAS – Regulation (EU) 910/2014) and builds on the policy requirements for Trust Service Providers (TSPs), the ETSI EN 319 411 series of standards used for eIDAS audits.

Trust service – policies for QWACs

CA / Browser Forum Alignment & Qualified Website Authentication Certificates (QWAC) Policies

- **Q-EVCP-w**
  - Fully aligned with the CA/Browser forum Guidelines for the Issuance and Management of Extended Validation Certificates
  - Meets the requirements for EU qualified certificate
- **QNCP-w**
  - Fully aligned with the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
  - Meets the requirements for EU qualified certificate
- **QNCP-w-gen**
  - Specific requirements for domain name validation as specified by CA/Browser Forum
  - Meets requirements for EU qualified certificates

Trust service – support of NIS 2

Trust services:

- TSP Audit ✓
- Issuing certificates ✓ (Rev)
- Time Stamping ✓
- Signature creation services ✓
- Signature validation services ✓
- Identity proofing ✓ (Upd)
- Open Banking ✓ (Upd)
- Support for NIS 2 (New)
- S/MIME ✓ (New)
- Attribute Attestations (New)

- AdES creation & validation
  - Part 1: procedures ✓ (Upd)
  - Part 2: signature validation report ✓ (Rev)

CC Protection Profiles ✓

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

119 6xx
Trust service status lists

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

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

Trust services for:

- Registered eDelivery / eMail ✓ (Upd)
- Long term preservation ✓

Interop tests

NIS2 and Trust Services:

- TR 119 404: NIS2 and its impact on eIDAS standards
  Available: https://www.etsi.org/standards-search
- Revised EN 319 401: General Policy Requirements for Trust Service Providers
  - Updates existing requirements to support NIS 2 requirements
  - Includes “Supply Chain”
  - Aim to specify in a way which does not require update to existing trust service standards

  Aim to be available for National EN Approval end 2023

✓	Published
(Rev)	Recently revised
(Upd)	Update in progress
(New)	New

Agenda

- Overview on new Trust Services, eIDAS 2.0 and EU Digital Wallet
- Overall map of ETSI/ESI standards
- General and evolution maintenance of existing ETSI/ESI standards
- Conclusion: new standards for support of eIDAS 2.0 EUDIW

Areas of ETSI ESI standardisation for EUDI Wallet

Highlight on potential areas of interest for ETSI ESI

- DTS 119 471: Policy and Security requirements for TSPs issuing Electronic Attestation of Attributes
- DTS 119 472: Profiles for Electronic Attestation of Attributes
- DTS 119 462: Wallet Interfaces for trust services and signing
- TR 119 476: Analysis of selective disclosure and zero-knowledge proofs applied to Electronic Attestation of Attributes
  Published – revision in progress

Areas of common interest between ETSI ESI / CEN TC 224

Potential areas of common interest ETSI ESI & CEN that could be synergically leveraged

- Interoperability of credentials
- Identity proofing and biometrics
- Levels of authentication
- Certification and protection profiles

Further information

Sources of further information on ESI / CEN

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

Presented by: **Santino Foti (InfoCert)** - *santino.foti@infocert.it*

For: **9th ENISA** Trust Services and eID forum

Thank you for your attention

Follow us on: