

Ensuring trustworthy identification for accountability in today's distributed environments

Presented by: **Santino Foti** (*InfoCert*) Vice Chair ETSI TC ESI



TINEXTA GROUP



Agenda



- Decentralised sources of information crucial to everyday decisions
- Tools for accountability provided by eIDAS supported by ETSI ESI standards
- Trust Services
- Looking at Distributed technologies and accountability
- Conclusions
- Overall map of ETSI/ESI standards

Decentralised sources of information from the "cloud"



Use of AI
Information collected in digital
libraries scattered on the Web



Multiple systems with
cloud based resource agents
Collection of information by
specific event-driven interactions



Big data multiple sources
Information coming by definition
from myriad of sources



Global nature of the
cloud infrastructure
Information can be located in
other countries in respect to the
place where it is used



Blurs legal boundaries: Who can be held accountable for the information provided?

Responsibility of private data submitted to the "cloud"

Problem crucial to everyday decision

Who is responsible for my private data submitted to the cloud?

- Who is the data Controller?
- Who is the data Processor?

Who can I hold to account for ensuring that my data is handled as required by the data protection regulation?



Electronic Identification, Authentication and Signatures




Regulation 910/2014 on Electronic Identification, Authentication and Signatures (eIDAS – currently under revision)

Establishes legal basis for Electronic Identification, Authentication and Signatures

- European Digital Identities
- Electronic signatures / seals
- Trust service infrastructure supporting Electronic Identification, Authentication and Signatures

ETSI Standards supporting eIDAS

- Supports EU regulatory requirements within a global framework

 **eIDAS: the key of accountability**



Basic frameworks for accountability

Principles in eIDAS 2 regulation proposal for EU Digital Identity Wallets

Key elements to create social trust on European Digital Identity Wallets (EUDIW) framework

- Transparency of EUDIW
- Accountability of their issuers
- Common Technology and open-source code
- Managed on national basis

Essential tools by ETSI ESI standards to support implementation of trust services

- Identity
- Trusted List
- Digital signatures
- Public key certificates
- e-Delivery



(Qualified) Trust services supported by ETSI ESI

Example of trust service types

- Digital certificates for e-signatures and seals

- e-seals
- e-signatures

Provides accountability by identifying person / organisation sourcing data

- Digital certificates for Website authentication

- Coexistence of web browser and EU trust controls
- Identifies the person / organisation “behind” the website

Provides accountability by identifying the person / organisation responsible for website data

Provides accountability by identifying the person / organisation responsible for private data passed to the website

- 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

Provides accountability for sourcing data

Provides accountability for transfer of data

Provides accountability for receipt of data

Practice policy and security supported by ETSI ESI

Example of best practice policy and security requirements for Qualified Trust Services

- Audit and governmental supervision

- EU trust infrastructure within global environment
 - standards based on internationally recognised standards
 - publicly available specifications

- Identity proofing

- EU initiative of digital signatures (AdES) from 3rd countries

- Website authentication aligned with CA/Browser forum

- e-Delivery application and evolution
 - Elevating trust and security
 - Raising the degree of interoperability
 - Best practices
 - Evolution towards building-block approach



Moving towards distributed technologies

Example of support for distributed technologies and accountability provided by ETSI ESI

- Decentralised identity
 - Identity Wallets
- Permission distributed ledgers
 - eIDAS approved node
 - Governance of distributed nodes
- Smart contracts
 - Identification by use of EU Digital Identity Wallets and electronic signatures
 - Policy and security requirements ledgers with smart contracts as a trust service
- International trust management
 - EU Pilot for Third Country List of Trust Lists for Digital Signatures (ADES LOTL)



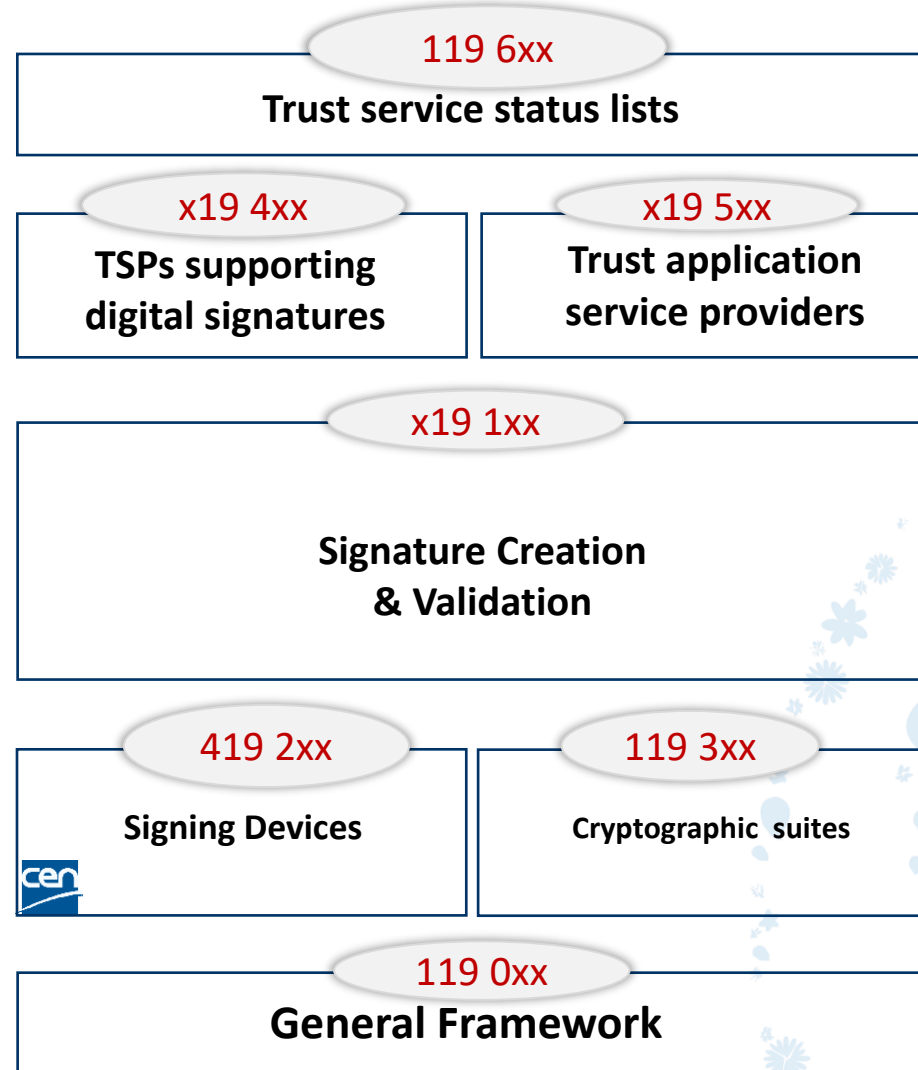
ETSI & CEN standards supporting eIDAS – overall map

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 ✓



- Trusted list ✓
- Using & interpreting trusted list ✓
- Validation policy using trusted list ✓
- Trust services for:
 - Registered eDelivery / eMail ✓ (Upd)
 - Long term preservation ✓
 - Interop tests
- Formats + Interop test:
 - XAdES (XML) ✓ (Rev)
 - CAdES (CMS) ✓ (Rev)
 - PAdES (PDF) ✓ (Upd)
 - ASiC (containers) ✓ (Upd)
 - JAdES (JSON) ✓ (Upd)
 - CB-AdES (CBOR) (New)
 - Signature suites ✓ (Upd)
 - Hash
 - Asymmetric crypto
 - Key generation
 - Lifetime
 - Schema for algorithm catalogues ✓ (New)
- Standards framework ✓*
- Common definitions ✓
- Guides ✓

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

Accountability in cloud environment

Summary of the main points

- With the move to a highly distributed cloud-based environment it is difficult to identify who is accountable for:
 - Data provided to data consumers
 - The privacy of data passed into the cloud

- eIDAS (Electronic Identities, Authentication and Signatures) provides a regulatory basis for providing accountability, supported by ETSI standards

- Providing accountability with a distributed trust environment is a goal we would like to achieve



ETSI TC ESI activities

Sources of further information on ESI

- ESI general portal:
<https://portal.etsi.org/tb.aspx?tbid=607&SubTB=607#/>
- Information on current activities:
<https://portal.etsi.org/TB-SiteMap/esi/esi-activities>
- Information on available standards (for free download):
<https://www.etsi.org/committee/esi>
- Slides of last webinar on ESI activities
<https://www.etsi.org/esi-training>





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

For: **ETSI Security Conference 2023**

Thank you for your attention



Follow us on:

