Qualified
Electronic Delivery Service

Mark Erlich
05. November 2021

eIDAS definition and logic

- **Trustservice** running eDelivery service – a platform operator
  - Protects from loss, theft and unauthorized access;
  - Assures integrity, sending and receiving data between 3rd parties
- **An interoperability framework** to trust and connect national electronic delivery services for cross-border data transactions.
  - A network between national gateways or service providers
  - Similar approach as with eIDAS eID – Node system
- **Qualified status assures**:
  - Integrity of the data
  - Identified sender and receiver
  - Accuracy with date and time of sending and receiving

CEF building block - eDelivery

- **Technical platform** for interoperability
  - Developed by European Commission
  - Suiting as eIDAS framework for interoperability
  - Supports both document and structured data transaction
  - Unfortunately implemented in domain specific networks
- **Examples**: mainly document based information
  - eCodex (e-justice)
  - Taxud (tax information)
  - e-invoice
  - ...etc.

ETSI standards related to Electronic Registered Delivery Services (ERDS) and AS4, the CEF eDelivery message exchange protocol, based on OASIS ebMS

- **ETSI work was accepted as ISO standard**
  - ISO 15000 Part 1
  - ISO 15000 Part 2
- **Binding to eIDAS is through:**
  - ETSI EN 319 522-1 Electronic Registered Delivery Services; Part 1: Framework and Architecture
  - ETSI EN 319 522-2 Electronic Registered Delivery Services; Part 2: Semantic Contents
  - ETSI EN 319 522-3 Electronic Registered Delivery Services; Part 3: Formats
  - ETSI EN 319 522-4-1 Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings
  - ETSI EN 319 522-4-2 Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: Evidence and identification bindings

SDG (single digital gateway)

- **EU regulation** – Currently at implementation
  https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0001.01.ENG
  - Highly recommended CEF BB: eID Node; eDelivery
  - Implementation Act (once only technical system) is in discussion
- A **“Big Driver” for CEF** eDelivery use in cross-domain data exchange
  - Today no specifications for cross domain data structures. Hence documents are used mainly
  - Domain specific semantics
  - No trust model established at the moment

X-Road vs eDelivery

- Different **messaging models**:
  - X-Road: Synchronous real-time exchange
  - eDelivery: Asynchronous non-time critical exchange
- Different **framework**:
  - X-Road: Technical and organizational framework
  - eDelivery: Technical specifications for multiple implementations
- Different **Logic Architecture**
  - X-Road: Decentralized architecture with P2P communication based on central service catalog
  - eDelivery: Centralized hub interconnecting parties with domain specific services

eDelivery support in X-Road

- **Centralized Hub** model with asynchronous data exchange is against X-Road principle and doesn’t suite X-Road logic
- eDelivery **AS4 protocol** can’t be supported at protocol level
- In the beginning 2022 the new version of eDelivery with **REST protocol** support
  - X-Road integration development planned in 2022 by NIIS (in context of SDG implementation)

Links and References

- CEF eDelivery presentation
  https://eufordigital.eu/steeringcommittee2/images/resources/Afternoon_side_event_Virtual_eDelivery_study_visit_.pdf

- CEF eDelivery documentation
  https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/How+does+eDelivery+work

- X-Road – eDelivery Gateway Concept
  https://x-road.global/xroad-edelivery-gateway
- NIIS study on implemetation of eDelivery on X-Road
  https://www.niis.org/blog/2019/9/26/x-road-and-edelivery-identical-twins-or-distant-relatives

eSignature preservation

Mark Erlich
05. November 2021

Preservation of documents and signed content

- **Paper based**:
  - Photocopy, metadata file, historical description and physical storage
- **Electronic document**:
  - Copies in multiple storage, metadata file, reading application and needed hardware
- **Hybrid**: Electronic to physical
  - Electronic document formatted to common format (e.g. PDF) printed on paper, metadata file, historical description, paper storage, common electronic file storage, common reading application and hardware

Technical Standards for eSignature preservation

- **AdES-LTA**
  - Additional Timestamp layer encapsulating signed file
  - Frequency of time-stamping defined by service policy
  - Must be done before signature or timestamp algorithm (encryption or HASH) weakens
- Supports only integrity preservation

Some examples

- **“e-Notary”** type service – a 3rd party preserving and registering original file and upon request issues warrant/certificate to proof validity of signature and file content (beyond the technological validity time)
  - Considered as a **Trust Service**
- Lithuanian **ADOC**
  - National standard, inherited from Baltic BDOC (95% ASiC)
  - Requires extra metadata: document life-cycle information
  - Required XadES-LTA level signature (archival ready)
  - Ready for national document archive service

Estonian Experience

- **DDOC format** based on SHA1 and RSA1k
  - More than 100M documents at risk
  - Around 20% of all DDOC files had long term value
- **TeRa software** for end-user and back-end integration
  https://github.com/open-eid/TeRa/
  - DDOC file search engine
  - Original signature container file encapsulated in ASiC-S container
  - No signatures, only timestamp is added

Time for Questions and Discussions

Thank You!