The Standards People

Other Trust Application standards

REM, ERDS, preservation

Presented by: **Andrea Caccia (SBS),**
Juan Carlos Cruellas (UPC),
Andrea Röck (Universign)

For: **ETSI Standards Training Webinar**

01.06.2021

Agenda for ERDS and REMS

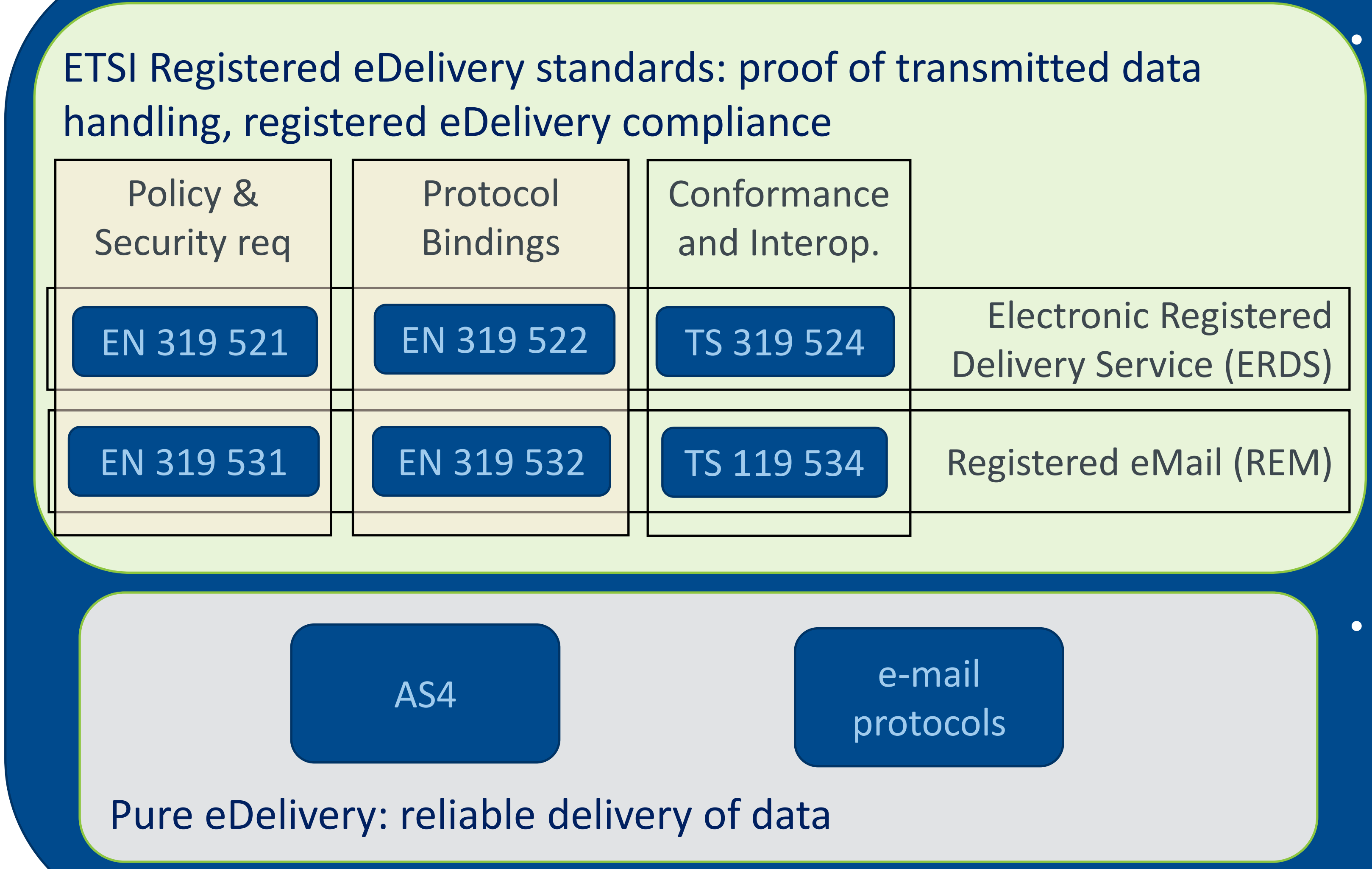
- Electronic Registered Delivery and Registered Electronic Mail Services
- Being an ERDS or a REMS provider: Policy documents
- ERDS. Achieving interoperability:
  - Technical specifications. Events and ERDS Evidence
  - Technical specifications. Formats and bindings
  - Technical specifications. Conformance and Interoperability
- REMS. Achieving interoperability:
  - Technical specifications. Formats and bindings
  - Technical specifications. Conformance and Interoperability
- The concept of REM Baseline
- Started yesterday: REM Baseline Plugtests© organized by ETSI

Agenda for Preservation

- Preservation service
- Preservation service vs. archival service
- Preservation services with storage
- Preservation services with temporary storage
- Preservation services without storage
- Preservation service standards

Electronic Registered Delivery and Registered Electronic Mail Services

Electronic Registered Delivery and Registered Electronic Mail Services



ETSI Registered eDelivery standards: proof of transmitted data handling, registered eDelivery compliance

Policy & Security req	Protocol Bindings	Conformance and Interop.	
EN 319 521	EN 319 522	TS 319 524	Electronic Registered Delivery Service (ERDS)
EN 319 531	EN 319 532	TS 119 534	Registered eMail (REM)

Pure eDelivery: reliable delivery of data

- **Electronic Registered Delivery Service (ERDS)** is an electronic service that:
  - **transmits data** between a sender and recipients by electronic means,
  - **provides evidence** relating to the handling of the transmitted data, including proof of sending and receiving the data, and that
  - **protects transmitted data** against the risk of loss, theft, damage or any unauthorized alterations.
- **Registered Electronic Mail Service (REMS):** electronic registered delivery service which builds on the formats, protocols and mechanisms used in ordinary e-mail messaging.
  - REM is a special type of ERDS

Being an ERDS or a REMS provider: Policy documents

- Not any Electronic Delivery Service provider or Electronic Mail Service provider may be considered ERDS and REMS Providers respectively.

- ERDS providers must fulfil the requirements defined in **ETSI EN 319 521**: "Policy and security requirements for Electronic Registered Delivery Service Providers".

- REMS providers must fulfil the requirements defined in ETSI EN 319 531: "Policy and security requirements for Registered Electronic Mail Service Providers ".

- Any Electronic Delivery Service provider that meets the requirements defined in ETSI EN 319 521 **is** an Electronic Registered Delivery Service provider.

- Any Electronic Mail Service provider that meets the requirements defined in ETSI EN 319 531 **is** a Registered Electronic Mail Service provider.

Being an ERDS or a REMS provider: Policy documents

- ETSI EN 319 521 and ETSI EN 319 531 define requirements for:
  - General provisions on policies and practices (service provider practice statement, terms and conditions, information security policy).
  - General provisions on the services (integrity, confidentiality, time reference, evidence, interoperability)
  - Risk Assessment
  - Service provider management and operation (internal organization, human resources, asset management, access control, cryptographic controls, physical and environmental security, operation security, network security, incident management, etc).

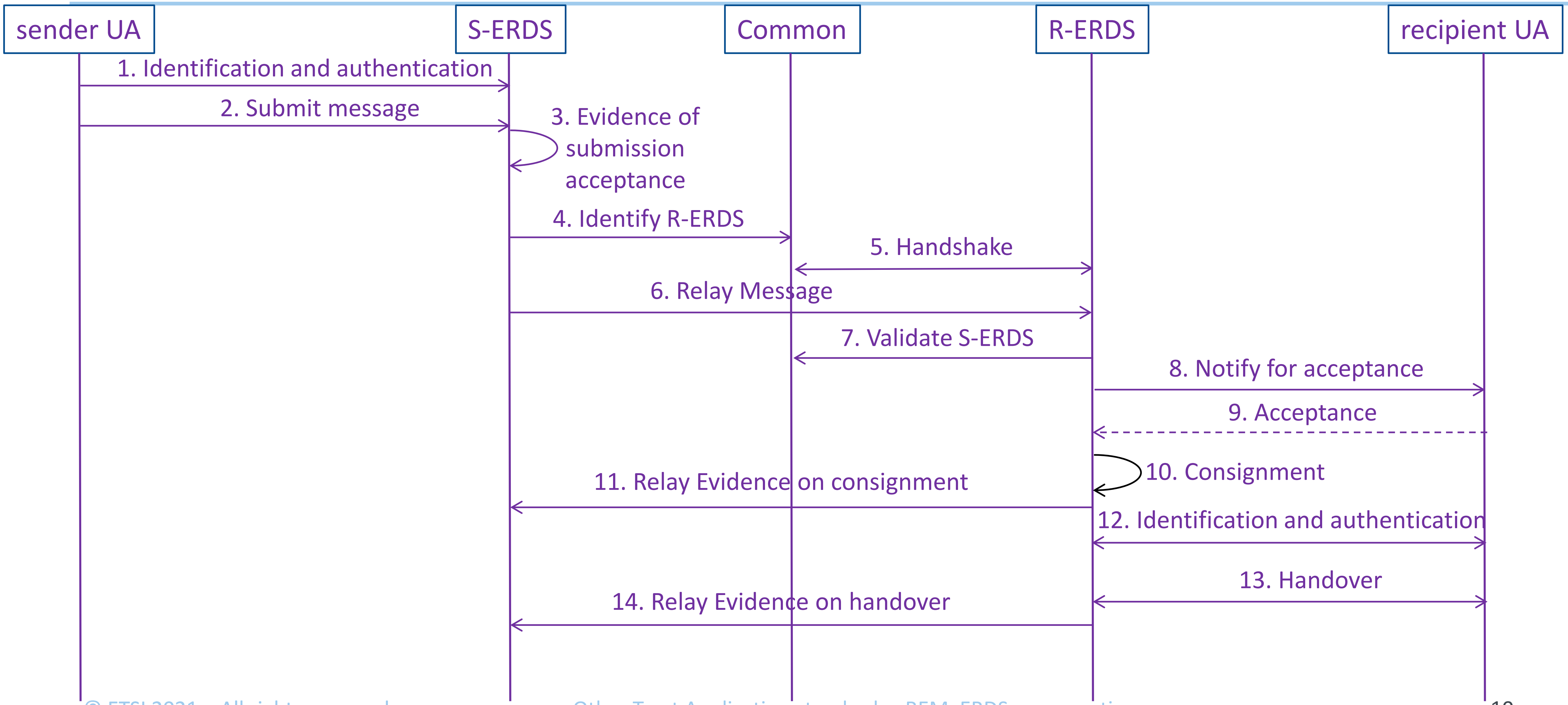
ERDS. Achieving interoperability: technical specifications. Events and ERDS Evidence

- ETSI EN 319 522 is a technical specification aiming at facilitating interoperability among ERDSs
  - Multipart document
  - Part 1: Defines ERDS models:
    - Black-box: one service provider serves both sender and recipient.
    - 4-Corner: sender is served by one provider (S-ERDS), and recipient by another provider (R-ERDS). SERDS and RERDS know each other and exchange messages directly.
    - Extended: sender is served by one provider (S-ERDS), and recipient by another provider (R-ERDS). They exchange messages with the help of intermediary ERDSs.

ERDS. Achieving interoperability: technical specifications. Formats and bindings

- Part 1: Defines relevant events occurring during the exchange of messages and the associated ERDS Evidence set (critical tokens provided by the service).
  - Sender's message accepted by S-ERDS: SubmissionAcceptance.
  - ERD message relay accepted by R-ERDS: RelayAcceptance.
  - R-ERDS notifies the recipient availability of message: NotificationForAcceptance.
  - Recipient accepts to receive the message: ConsignmentAcceptance.
  - R-ERDS makes the message available to recipient: ContentConsignment
  - The list also includes evidence for situations when one entity rejects to carry out some event, or when one of the events just fails for certain reasons.
  - The set of ERDS Evidence is identical for REMS.

ERDS. Achieving interoperability: technical specifications. Formats and bindings



ERDS. Achieving interoperability: technical specifications. Conformance and Interoperability

- Defines binding to messaging protocols and specifically for AS4 profile of ebMS 3.0 (ISO 15000):
  - Part 2: Defines the semantics of the data that flow between ERDSs.
  - Part 3: Defines the formats for ERDS Evidence and other components for their use in AS4 binding
  - Part 4: Bindings (for ERD messages, for ERDS Evidence and identification, for capability)

- ETSI EN 319 524 is a technical specification for testing conformance and interoperability.

REMS. Achieving interoperability: technical specifications.

- ETSI EN 319 532 is a technical specification aiming at <u>facilitating interoperability among REMSs</u>
  - Multipart document
  - Part 1: Defines REMS models:
    - Black-box: one service provider serves both sender and recipient.
    - 4-Corner: sender is served by one provider (S-REMS), and recipient by another provider (R-REMS). SERDS and RERDS know each other and exchange messages directly.
    - Extended: sender is served by one provider (S-REMS), and recipient by another provider (R-REMS). They exchange messages with the help of intermediary ERDSs.
  - Relevant events and evidence set: similar to the ones in ETSI EN 319 522 with some few additional ones for specific events in REMS provision.

REMS. Achieving interoperability: technical specifications. Formats and bindings

- ETSI EN 319 532 defines a binding for electronic mail standards:
  - Part 2: Defines the semantics of the data that flow between REMSs.
  - Part 3: Defines the formats for REM Messages (MIME structures). Format for ERDS Evidence: the one defined in EN ETSI 319 522-3.
  - Part 4: Define interoperability profiles.
- An update of part 4 including the new "REM Baseline" is under development in ETSI ESI.
- REM Baseline is available as draft ETSI EN 319 532-4 v1.1.3 and ready for testing. It will be shortly presented in the next slides.

- ETSI TS 119 534 is a technical specification for testing conformance and interoperability.

The concept of REM Baseline

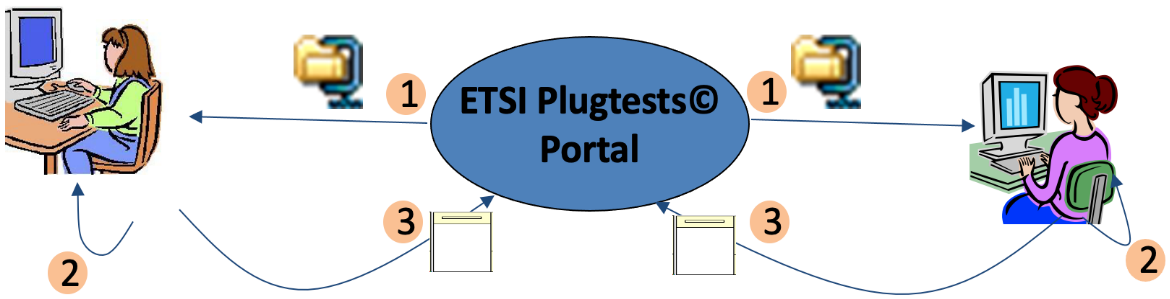
- REM standards include many features and are flexible to support different business requirements, but this can become an obstacle to interoperability and in defining an appropriate common trust level.
- The issue that REM Baseline aims to solve is:
  - Support mutual recognition, trust and interoperability between different REMS Domains, for example between different countries/different jurisdictions
  - Support basic common trusted delivery service requirements enabling the provision of a broad number of services, this is often a public sector requirement
- REM Baseline tackles this issues with a baseline technical specification profiling and augmenting as needed the REM interoperability profiles (actual Part 4) to ensure maximal interoperability and a qualified-grade trust across REM service domains.

The concept of REM Baseline

- REM Baseline fully addresses:
  - The requirements to secure the proof of sending and receiving the data leveraging on the application of basic trust services to REM evidences, i.e. advanced electronic signature or seal and timestamp
  - The specification of a baseline Common Service Interface (CSI) in REM messaging guaranteeing a trusted interconnection between REMS and common trust framework.
- The benefit for all the providers is a baseline trust and interoperability that helps on one hand to spread the use of the service, while on the other hand to enable competition on other added value features from the entire ERDS framework

Started yesterday: REM Baseline Plugtests© organized by ETSI

- REM Baseline is an update of ETSI EN 319 532 Part 4 (interoperability profiles) under development but fully implementable
- ETSI Centre for Testing and Interoperability (CTI) organises 2 times per year Plugtests© events on signature formats, signature verification and (now) REM.
- An ETSI Plugtests© event is a unique opportunity for implementor to get together with peers and test interoperability in a neutral environment.
- Also an opportunity for ETSI to improve the quality of standards have closer contact with the market



Package contains:

Definitions of test cases

Any other material as required for conducting the plugtest

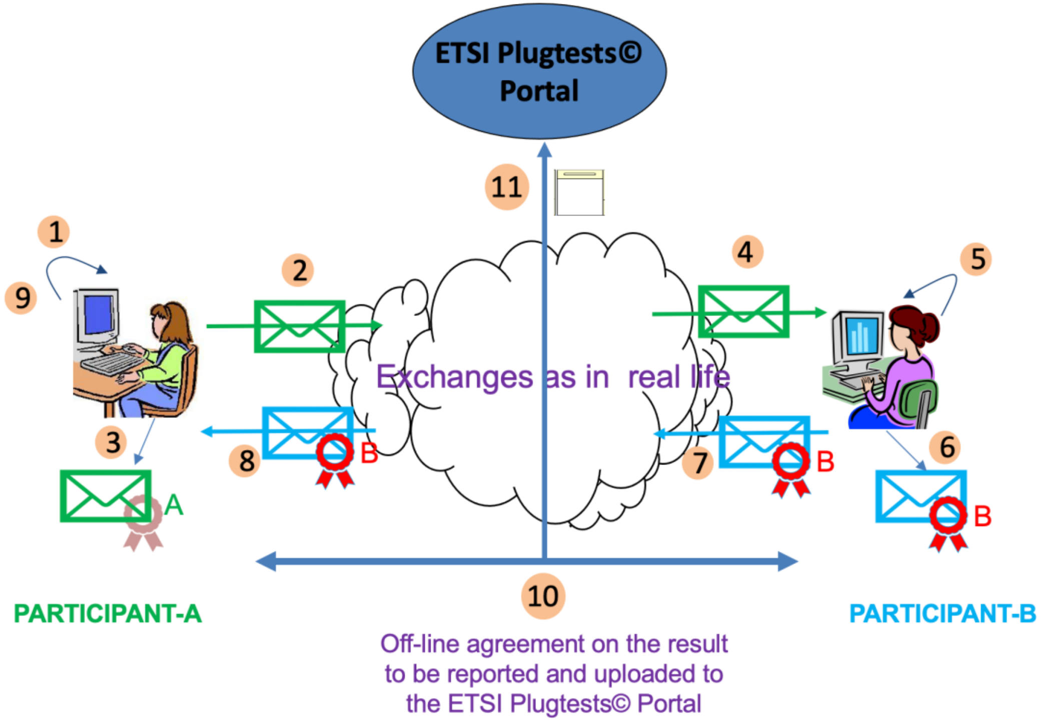
Started yesterday: REM Baseline Plugtests© organized by ETSI

Type 1 tests: Generation and cross-verification of ERDS Evidences.

Type 2 tests: Generation and cross-checks of REM Dispatches and/or REMS Receipts.

Type 3 tests: Real life tests on REM protocol.

Type 4 tests: tests on REM protocol simulations


ETSI Plugtests© Portal
11
1
9
2
4
5
Exchanges as in real life
3
8
B
7
B
6
B
A
10
PARTICIPANT-A
PARTICIPANT-B
Off-line agreement on the result to be reported and uploaded to the ETSI Plugtests© Portal

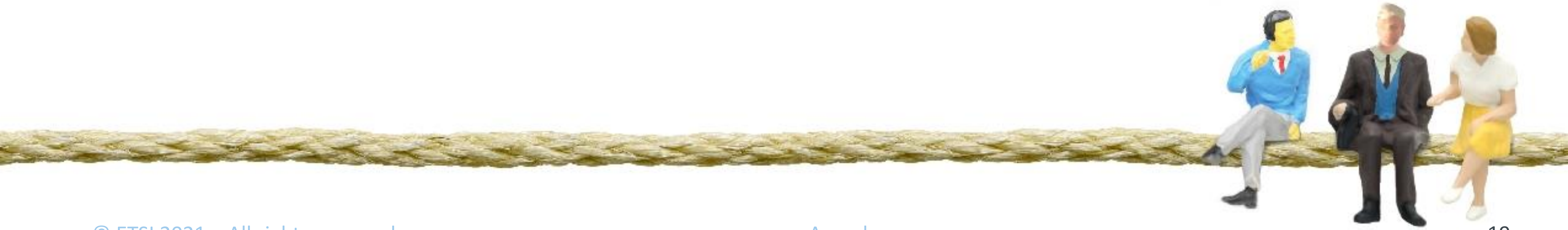
- The REM Baseline Plugtests© event is conducted remotely and online, for more information: https://www.etsi.org/events/1899-rem-plugtests

- It is still possible to register as observers

PRESERVATION

Agenda for Preservation

- Preservation service
- Preservation service vs. archival service
- Preservation services with storage
- Preservation services with temporary storage
- Preservation services without storage
- Preservation service standards



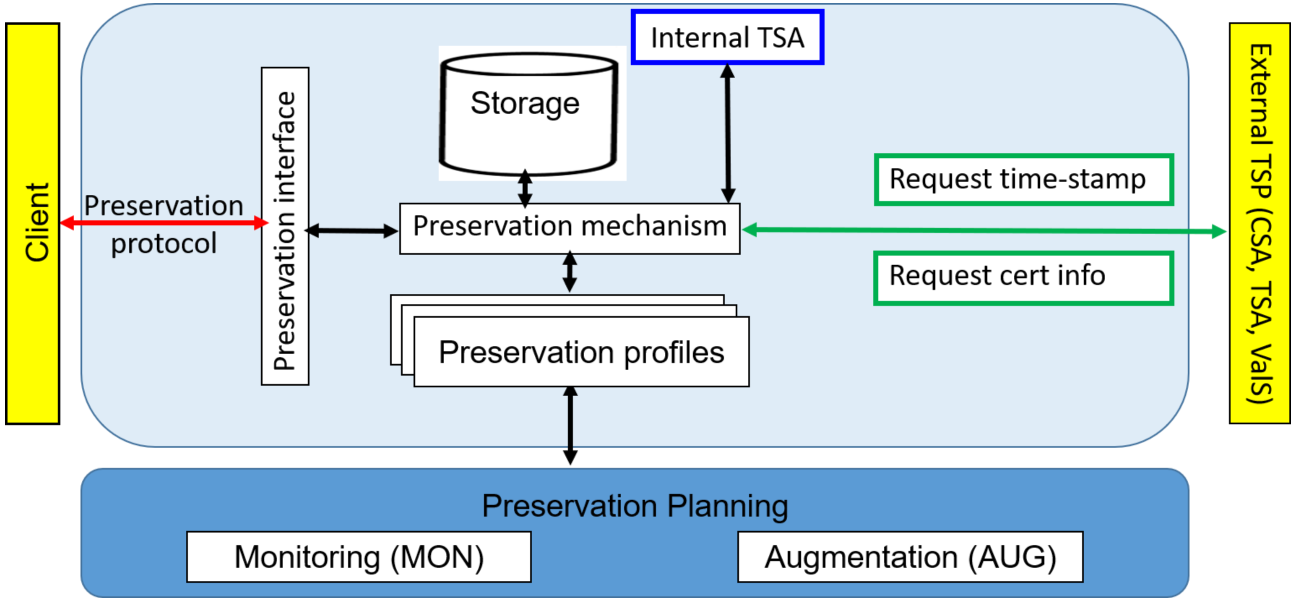
Preservation service

- **Preservation service:** has two possible goals, both achieved using **digital signature techniques**
- Extending the validity status of a digital signature over long periods of time
  - Not only provide proof of existence of signed data & signature BUT ALSO of **information needed to extend the validity status of the digital signatures**, e.g. certificates, CRLs, OCSP responses, validation report, …
- Providing proofs of existence of data over long periods of time
- Standard needed to handle many different use cases

Preservation service vs. archival service

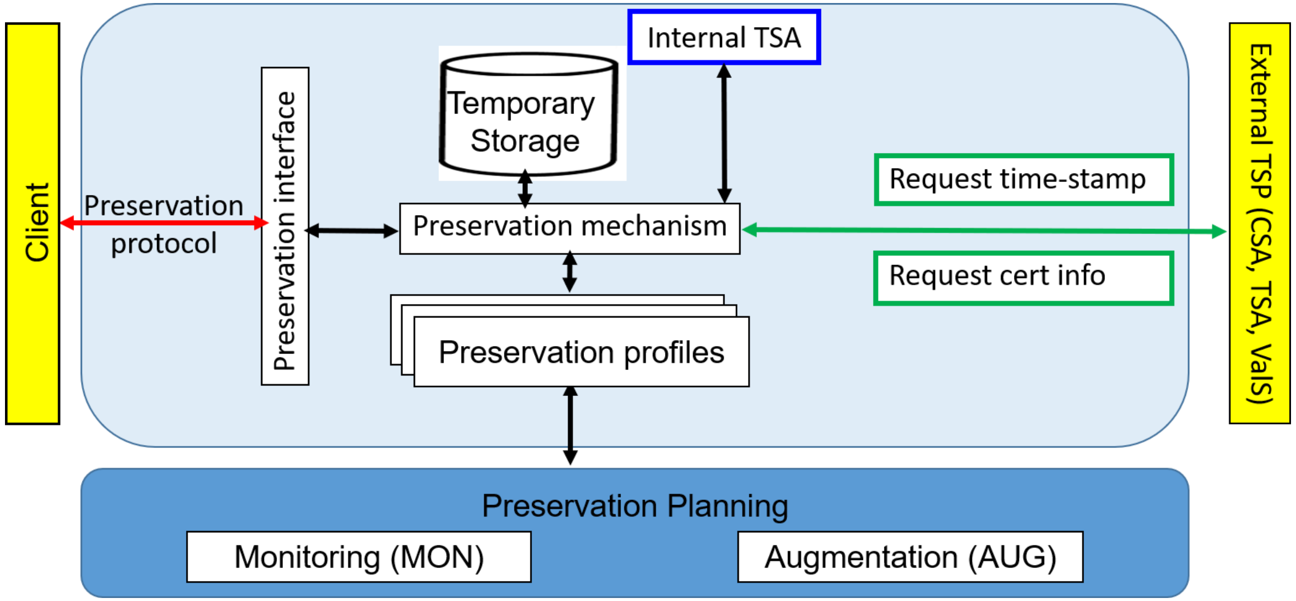
- An archival service may use digital signature techniques to provide proofs of existence for some data but is not required to use them.
- An archival service without a preservation service does not capture nor verify any validation data associated with a digital signature.
- An archival service can use a preservation service to provide proofs of existence of data based on digital signature techniques. However, it needs to manage all the metadata required by an archival service, e.g. the Archival Information Package (AIP) as defined in the Open Archival Information System (OAIS) Reference Model (ISO 14721)
- A preservation service with storage (WST) can use an archival service for the goal of storing data.
- A preservation service does not transform the original data

Preservation services with storage



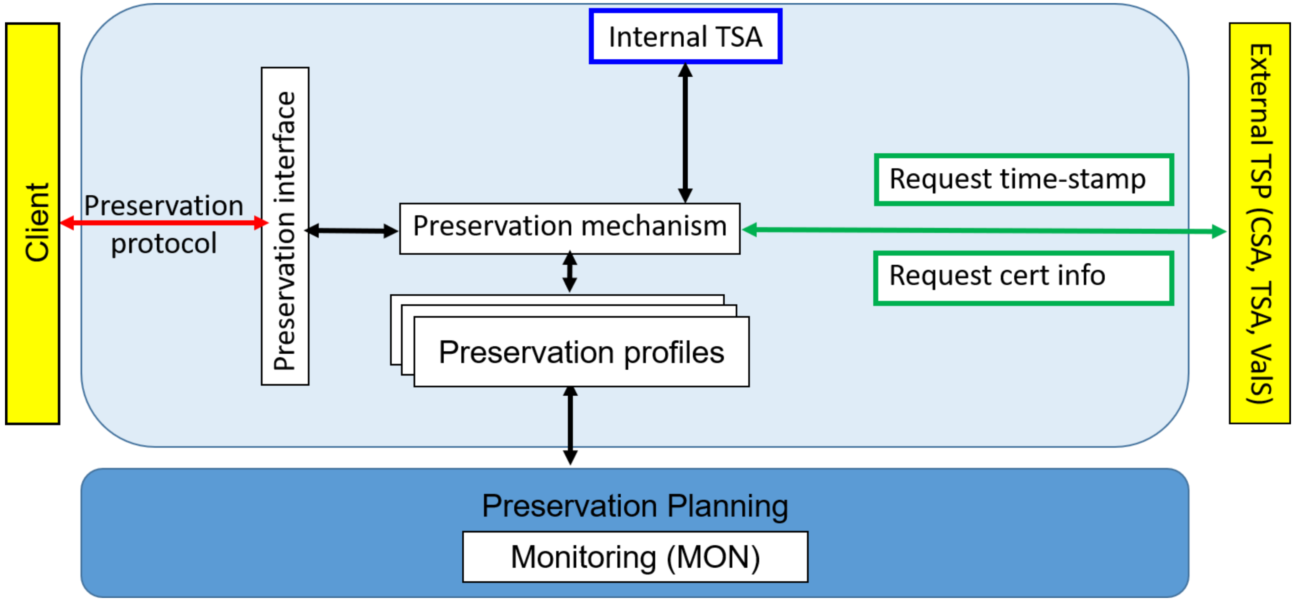
- Stores the submitted data object(s) and the associated preservation evidences
- Evidences and the preserved data are delivered upon request to the client
- Evidences are augmented if needed

Preservation services with temporary storage



- Data to be preserved is stored on client side
- Service keeps the data (or hash) only until the evidence is produced
- Evidences are produced asynchronously and retrievable for a limited time

Preservation services without storage



- Data to be preserved is stored on the client side
- Preservation service stores neither the submitted data nor the evidences
- Evidences are produced synchronously

Preservation service standards

- ETSI TS 119 511: Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
- ETSI TS 119 512: Protocols for trust service providers providing long-term data preservation services
  - JSON and XML version