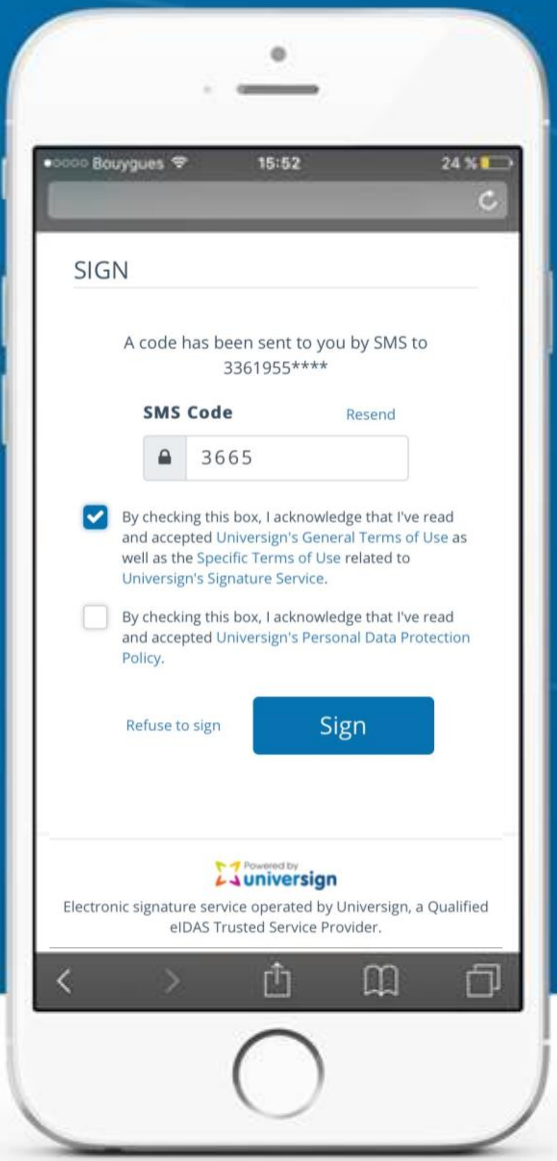


SIGN

A code has been sent to you by SMS to 3361955****

SMS Code Resend

3665

☑ By checking this box, I acknowledge that I've read and accepted Universign's General Terms of Use as well as the Specific Terms of Use related to Universign's Signature Service.

□ By checking this box, I acknowledge that I've read and accepted Universign's Personal Data Protection Policy.

Powered by universign

Electronic signature service operated by Universign, a Qualified eIDAS Trusted Service Provider.

universign

creating trust

ETSI Standardization for Preservation Services

Andrea Röck – CA day

26/09/2019

Agenda

1 General

2 Policy document and different models

3 Protocol document and different schemes

4 Questions

5

General

Preservation services in eIDAS

Regulation (EU) No 910/2014:

*a **qualified preservation service** for **qualified electronic signatures***

- *may only be provided by a **qualified trust service provider***
- *that uses procedures and technologies capable of **extending the trustworthiness** of the qualified electronic signature **beyond the technological validity period***

ETSI document on preservation services - goals

- **First goal**: to support the service as defined in eIDAS
- **Second goal**: to go beyond the service as defined in eIDAS
    - Also for non qualified electronic signatures / seals
    - Also for unsigned documents
- **Difficulties**
    - Requirements from eIDAS not very technical
    - Already different services with different models in place

ETSI document on preservation services - documents

- 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
  - Published 2019-06: https://www.etsi.org/deliver/etsi_ts/119500_119599/119511/01.01.01_60/ts_119511v010101p.pdf
- ETSI TS 119 512
  - Protocols for trust service providers providing long-term data preservation services
  - Accepted, will be published soon

universign

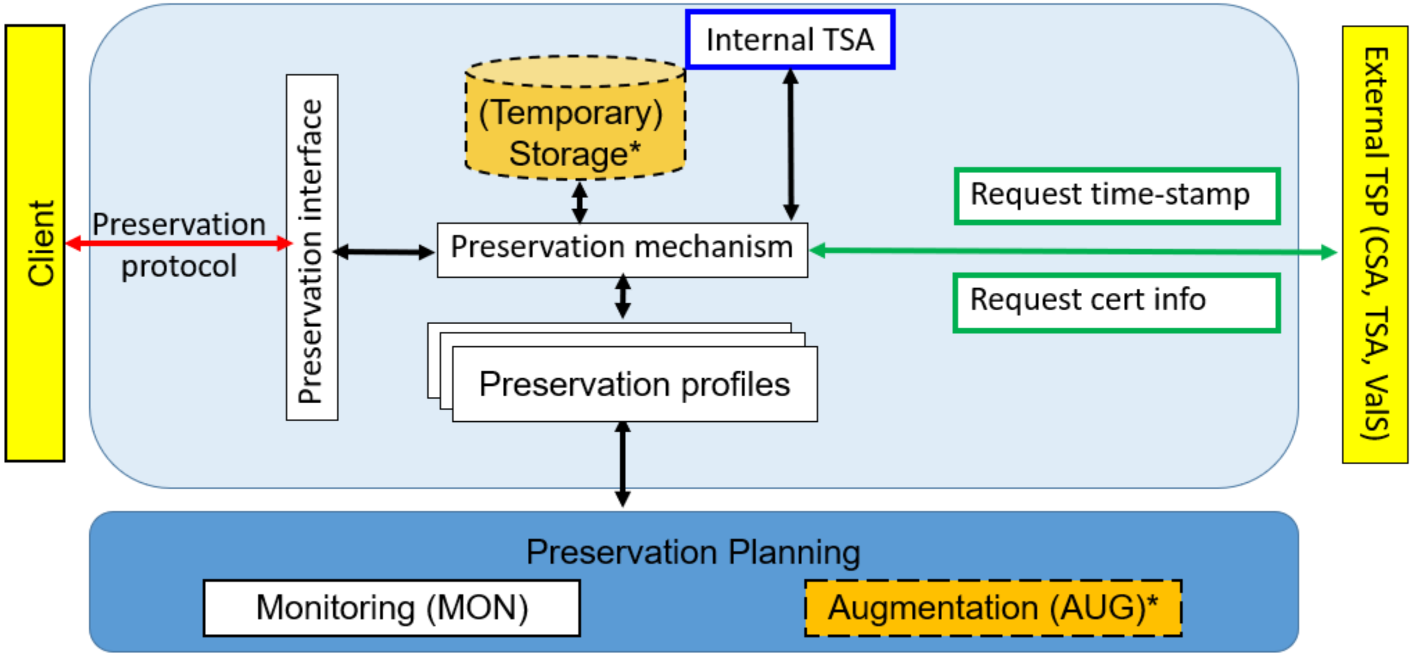
Policy document and different models

ETSI TS 119 511

- Based on ETSI EN 319 401 for general
- General requirements in the main document
- Requirements aimed for qualified preservation service
  - It must be possible to have an entry in the trusted list
  - Preserver evidence needed to decide if a signature / seal is qualified
- Specific functionalities are required, protocol is only recommended
- Preservation profile
  - Details on how preservation is done

Different preservation storage models

- Preservation storage models
  - **With storage** – store the data to be preserved and the evidence (*)
  - **With temporary storage** – keep data to be preserved only as long needed to create the evidence, keep evidence only as long as needed to be retrieved by the client (*)
  - **Without storage** – create synchronously the evidence and send it back



Different functional goals

- Functional goals
  - Preservation / proof of existence of general data
  - Preservation of signatures and associated signed data
  - Augmentation of evidence sent to preservation service (useful for moving data from one service to another)

Protocol document and different schemes

ETSI TS 119 512

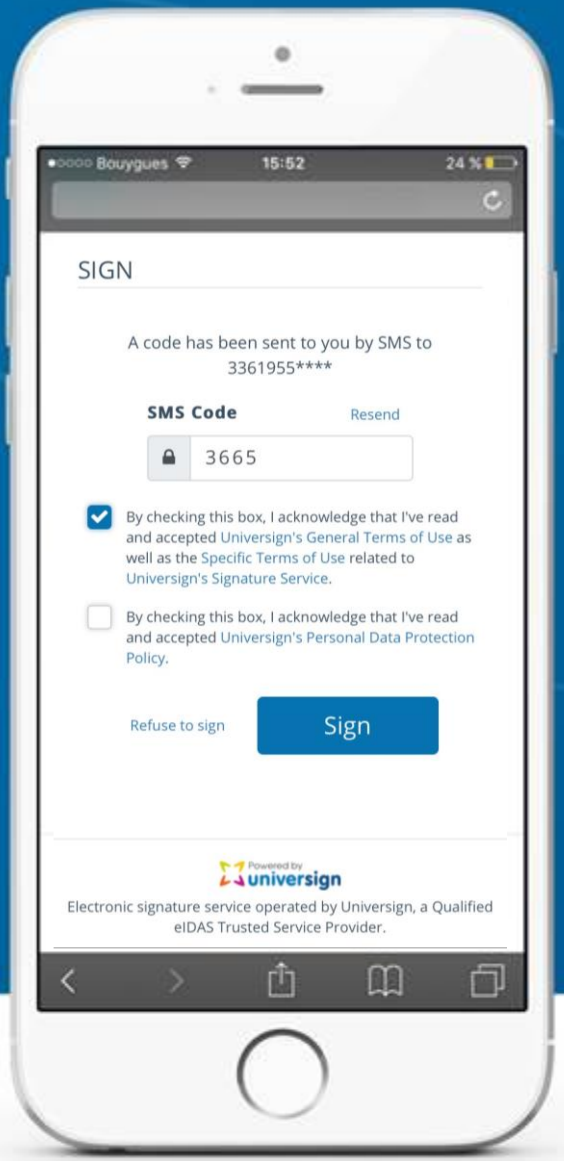
- Protocol for preservation service
- Machine readable version of preservation profile
- Implementation in XML and JSON
- Use OASIS standard to describe digital signature service metadata
  - Need to wait for publication
- Defines ASN.1 attributes which can be added in preservation evidence
  - Preservation service
  - Preservation evidence policy
  - Preservation profile

Examples of preservation schemes

- Preservation scheme with storage based on evidence records
- Preservation scheme with temporary storage based on evidence records
- Preservation scheme with signature augmentation and with storage
- Preservation scheme with signature augmentation and without storage

universign

Questions?



SIGN

A code has been sent to you by SMS to 3361955****

SMS Code

Resend

3665

☑ By checking this box, I acknowledge that I've read and accepted Universign's General Terms of Use as well as the Specific Terms of Use related to Universign's Signature Service.

□ By checking this box, I acknowledge that I've read and accepted Universign's Personal Data Protection Policy.

Refuse to sign

Sign

Powered by universign

Electronic signature service operated by Universign, a Qualified eIDAS Trusted Service Provider.

universign

creating trust

Contact

andrea.rock@universign.com

+33.6.61.47.21.41

www.universign.com