



Preserving the future

Preservation Strategies for Digital and Electronic Signatures

Luis Faria lfaria@keep.pt

KEEP SOLUTIONS

2024-05-28

Digital and electronic signatures

Secure and **legally binding** method for **authenticating** digital documents

Contracts, government documents, notarized agreements, etc.

Longevity and usefulness of signed documents **outlives** the signature validity

This presentation:

- What is the current **state-of-the-art** in preservation of digital signatures?
- What are the **issues** current strategies and **opportunities** coming up?

Digital signature

A **cryptographic technique** used to verify the **authenticity** and **integrity** of digital documents, messages, or transactions in electronic form.

- Uses **Public Key Infrastructure** (PKI) to manage digital certificates and sign file hashes
- It is tied to the **binary representation**
- Has an **expiration date**
- Can be **revoked at any time** by external factors

Electronic signature

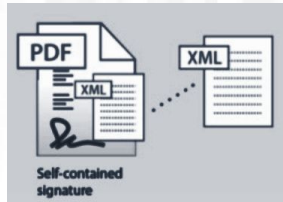
General term for any approach that uses a digital technology to provide assurances of the **signer's identity**, the **integrity** of the signed content, and **non-repudiation**.

- **Simple:** basic form such as typing your name or clicking “I accept” button;
- **Advanced:** incorporate cryptographic methods to ensure integrity and identity
- **Qualified:** include accredited digital certificates issued by trust providers (eIDAS)

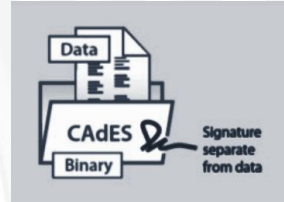
eIDAS regulation

Provides the regulatory framework in the EU for **electronic identification and trust services** for electronic transactions in the internal market.

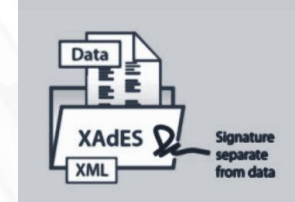
- **Standards** for formats for electronic signatures and seals
- **Certification** of Qualified Trust Service Provider
- Promotes **legal backing** in members states and across borders



PAdES



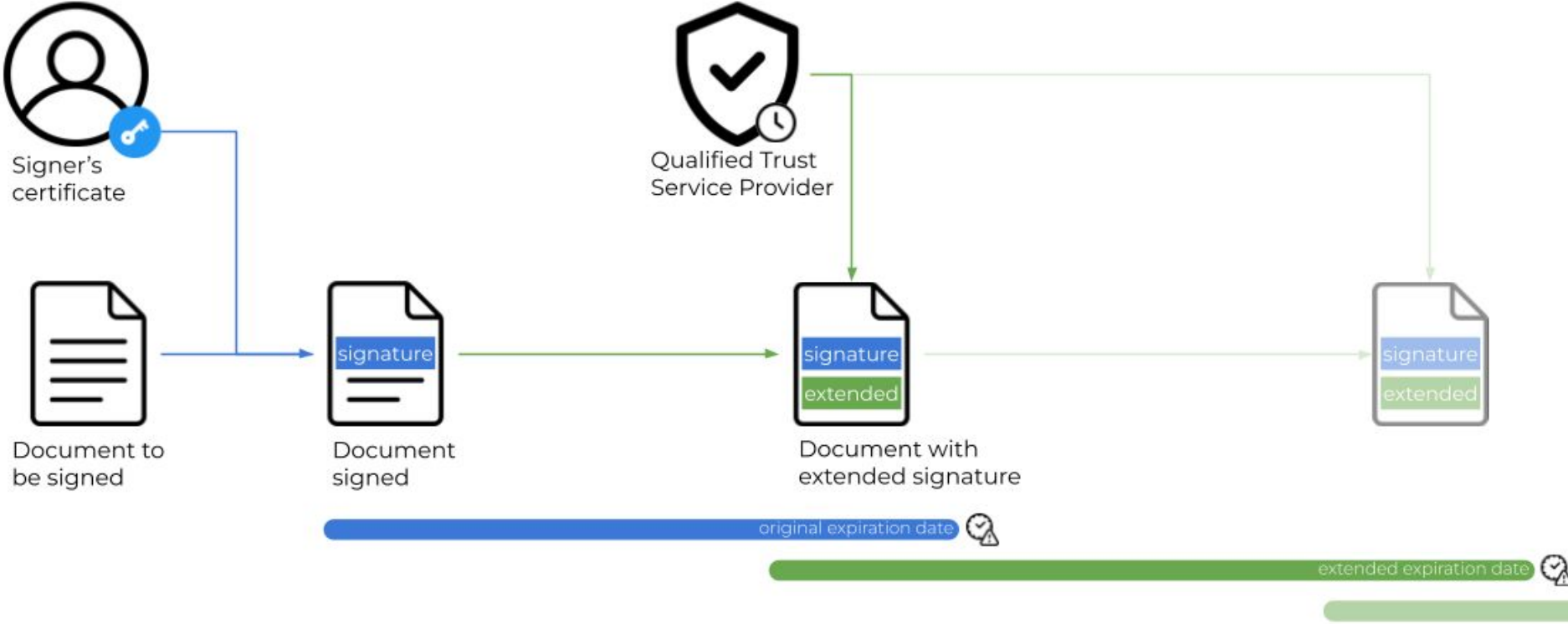
CAAdES



XAdES

Signature	Embedded in PDF	Detached binary	Detached XML or XML envelope
Standards	Part of ISO PDF	PKCS#7 (RFC 2315)	Extends W3C XML Signature
Content availability	Any PDF reader	File available for any reader	File available if detached XML
Signature validation	Some PDF readers	Requires specific software	Requires specific software
Visible graphic signature	Supported	Not supported	Not supported
Content file formats	Only PDF	Any file	Any file or bitstream

eIDAS Long-Term Validation (LTV)



LTV signature extensions

A **time-stamp token** that proves that the **signature existed at a given point in time**

All the material required for validating is incorporated into the signature info

A **time-stamp token on the long-term validation material**

Done by a **Qualified Electronic Signature Creation Device** to ensure there is **trust**

The **validation signature and time-stamp token** also have an **expiration date**

But the **process can be repeated** to extend the validity indefinitely

Visible graphic signature ↓

DEMONSTRATION FOR DLM FORUM

Signed by: **Luís Francisco da Cunha Cardoso de Faria**

Identification number: 12425806

Date: 2024.05.26 14:57:37 +0100

Location: BRAGA, PORTUGAL



Luís Francisco da Cunha Cardoso de Faria
Chave Móvel Digital de Assinatura Qualificada do
Issued by: EC de Chave Móvel Digital de Assinatura Digital
Cartão de Cidadão, subECEstado

Valid from: 2022/09/21 14:52:53 +01'00'

Valid to: 2031/09/02 23:59:59 +01'00'

Intended usage: **Non-Repudiation**






This certificate is Qualified according to EU Regulation 910/2014 Annex I

The private key related to this certificate resides in a Qualified Signature Creation Device (QSCD)

Adobe Acrobat Signature panel →

← Digital certificate secured in a QSCD

× Signatures  

▼  Rev. 1: Signed by Luís Francisco da Cunha Cardoso de Faria

Signature is valid:

Source of Trust obtained from European Union Trusted Lists (EUTL).

This is a Qualified Electronic Signature according to EU Regulation 910/2014

Document has not been modified since this signature was applied

Signer's identity is valid

The signature includes an embedded timestamp.

Signature is LTV enabled

▼ Signature Details

Reason: DEMONSTRATION FOR DLM FORUM


Location: BRAGA, PORTUGAL

[Certificate Details...](#)

Last Checked: 2024.05.26 14:58:06 +01'00'

Field: Signature2322725399 on page 9

[Click to view this version](#)

▼  Rev. 2: Signed by Serviço de Validação Cronológica do Cartão de Cidadão 000013

Signature is valid:

Source of Trust obtained from European Union Trusted Lists (EUTL).

Document has not been modified since this signature was applied

Signer's identity is valid

Signature is a document timestamp signature.

Signature is LTV enabled

> Signature Details

Last Checked: 2024.05.26 14:58:06 +01'00'

Field: Signature2076378517 (invisible signature)

[Click to view this version](#)

Long-term Preservation Challenges of LTV

Integrity is tied to the **binary representation**

Does not cope well with **technological obsolescence**, eventually we will need to change the file format

Does not cope well with **redaction**, anonymization or dataset cleansing cannot keep authenticity properties

Signer's identity is tied to the **PKI infrastructure** (and is usually nominative)

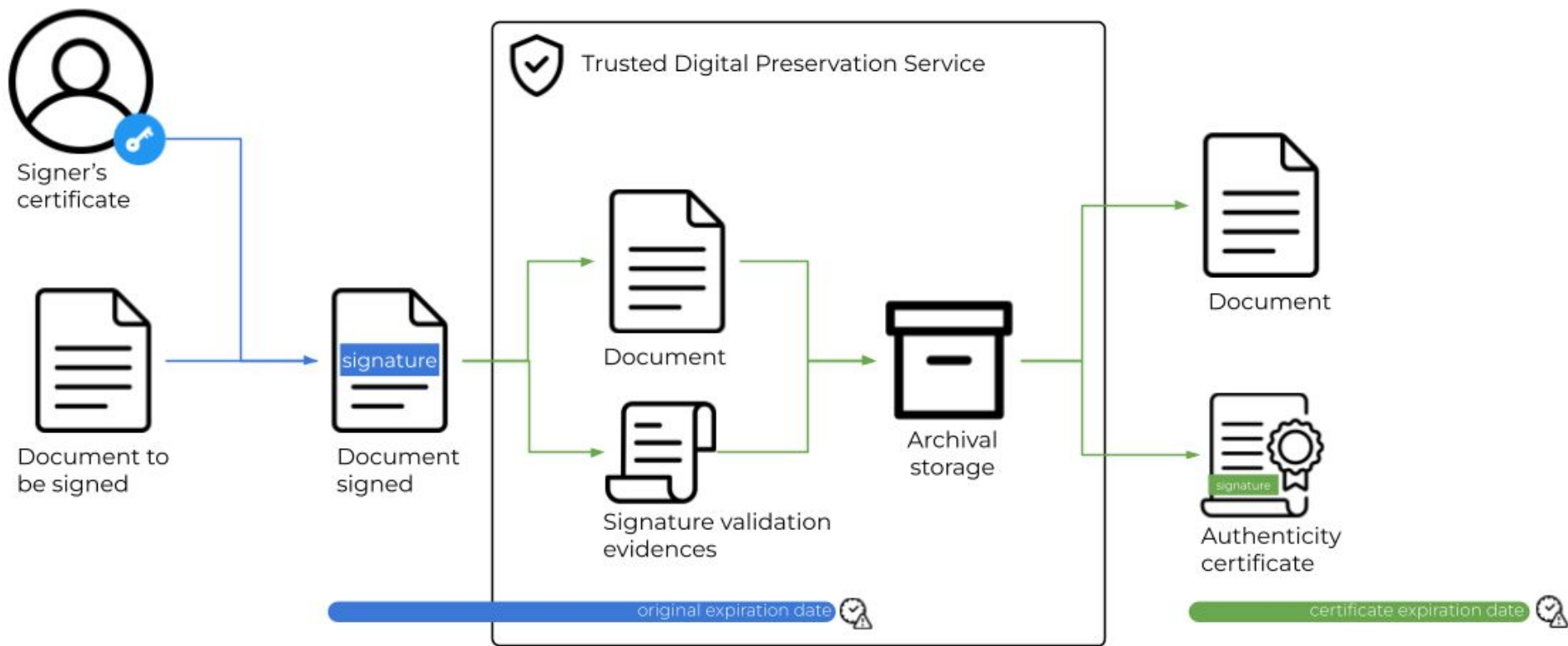
Not all documents are signed on creation but their authenticity may be ensured by other contexts

How will the signer's identity and non-repudiation outlive the PKI infrastructure?

There is a **cost per-signature and per-extension**

Qualified time-stamp tokens have a cost per token (up to 0.20€ per token)

“Trust the archive” approach



“Trust the archive” approach

Document verification upon reception

Verify the identity of the parties involved and ensure the authenticity of the electronic documents received, Document reception and verification, including the date and time of the validation and all validation material required to serve as evidence, this information should also be preserved alongside the document

Trusted digital preservation

Preserve the information in the document in a trusted digital preservation service, ensuring integrity, durability and legibility of information beyond the technological validity period, even when changing medium or electronic format.

Authenticity certificate

Whenever needed, the institution would certify the documents, which includes information such as the date and time of the document verification, the identity of the parties involved, and the institution's electronic signature, to signify its authenticity and validity.

Challenges with “Trust the archive” approach

Lack of **standardization** of signature validation process and evidence format

Work being done in **TR-ESOR** and other initiatives

How to preserve **signer’s identity** on the long term?

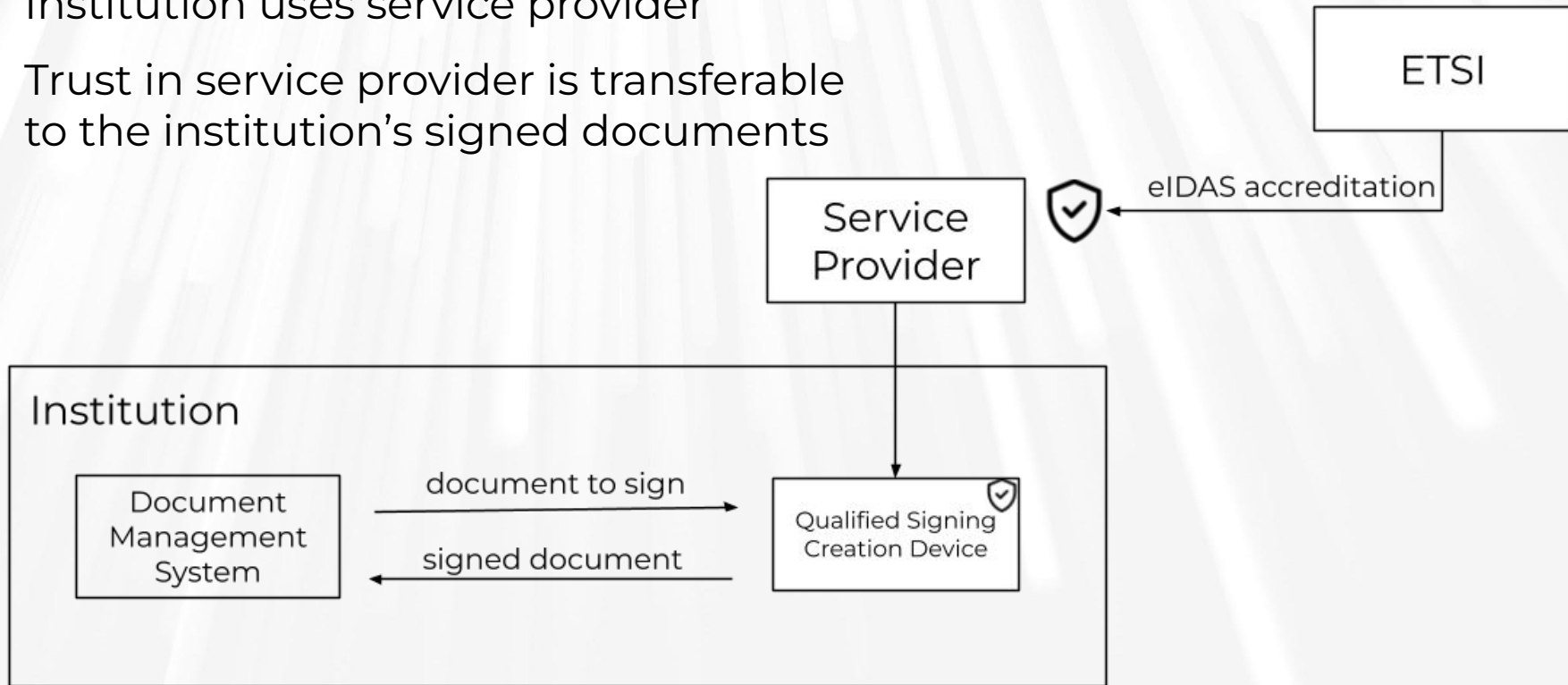
Metadata and **Archival Authority Records**

There is **no legal backing** for institutions **not acting as archives**

See ETSI standardization and **eIDAS 2.0**

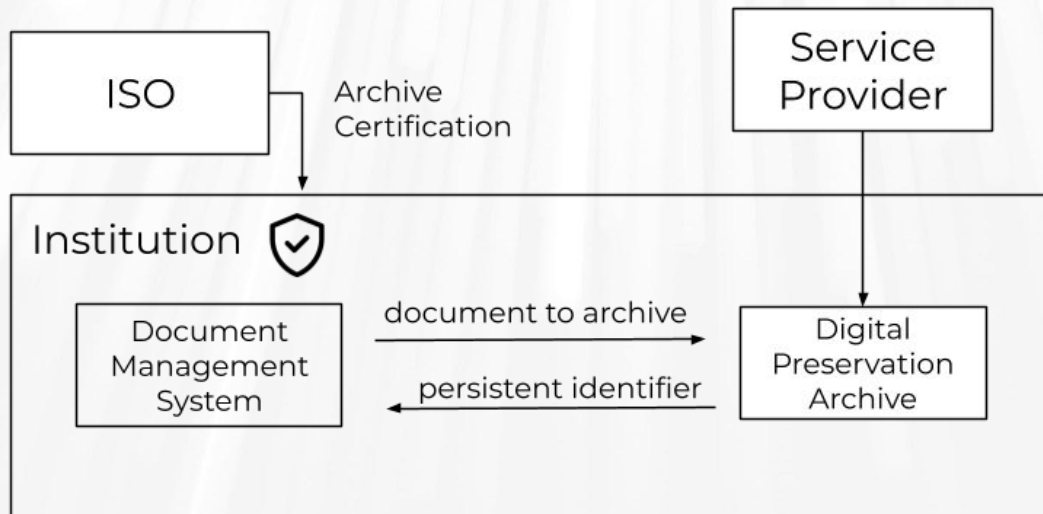
eIDAS service provider-oriented approach

- Service provider is certified
- Institution uses service provider
- Trust in service provider is transferable to the institution's signed documents



ISO 16363 institution-oriented approach

- Service provider provides digital preservation services
- Institution uses service provider
- Institution must be certified to be trusted



Certification requirements:

- ❑ Organisational
- ❑ Staff
- ❑ Financial
- ❑ Technical
- ❑ Software
- ❑ Infrastructure
- ❑ Security risk management

Problems with institution-oriented certification

Certification is very hard to acquire

Requires trained staff and constant technological watch

A service provider-oriented is more adequate for the market

Problems with service provider-oriented certification

Current digital preservation **trust certification frameworks do not fit well service providers**

Digital preservation is a more complex process:

- Momentary access to content vs. long-term storage of content
- Confidentiality must be maintained
- Continuity, succession and takeout or handoff

eArchiving seal will be instrumental

eIDAS 2.0 (April 2024)

- Introduces **Qualified Electronic Archiving Services**
- Provided by **Qualified Trust Service Providers**
- Using the **“Trust the archive”** approach

Article 45j, 2.

*By **21 May 2025**, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic archiving services.*

ELI: <http://data.europa.eu/eli/reg/2024/1183/oj>

Call to Action!

Come and talk with **EC eArchiving** about the eIDAS implementing acts

Talk with your **member state representative** about eIDAS 2.0

Ensure **EU regulations** are in line with digital preservation practices

Ensure **legislation in your member state** will follow digital presentation practices

Let's ensure a bright new future for **digital preservation for all!**

Thank you for your attention

Questions or opinions? Speak now!