e-Signature Deep Dive
Day 2 | 14:15 – 15:00
e-Signatures are all around us

1. Typing a name at the end of an email.
2. Clicking on an "I accept" button on a website.
3. Using a scanned image of a handwritten signature.
4. Using a finger or stylus to hand write a signature on screen.
5. Digital authentication (PIN, biometric).
What is a signature anyway?

This functional view is equally valid for paper and electronic signatures.

[Diagram showing the components of a signature: Who? Why? What? When?]

- Name of the signer
- Did that person really sign?
- Intent to be bound
- Content of the document
- Date

Identity, Attribution, Endorsement, Integrity, Non-repudiation

Trust requires...

...evidence of...

...to assure...
**Electronic Signature**

“Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.”

(EIDAS Art. 2(10))

**Digital Signature**

“A value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the public key to verify the data has not been altered since it was signed by the private key.”

(INST SP 800-63B)
Use cases of e-signatures

The majority of e-signature use cases are relatively low risk. However, very high value transactions can also be signed electronically if there is enough trust.
Signatures are all around us

Sample use case: Online loan application
Sources of trust

**Pre-existing trust**

- Do I know you offline?
- Have we interacted successfully online before?
- Do we have a pre-existing contractual relationship?
- Are we members of the same professional body?
- Are we transacting on a secure communication channel?

**People**

Providers of eSignature services are trusted and vetted.

**Process**

Identity checks carried out when onboarding a signer.

**Technology**

Technical measures to protect the integrity of the signed document.
Trust framework

- Set **standards**
- Balance security and **usability**
- Clarify **roles** and responsibilities
- Promote **adoption**
- Risk-based **levels of assurance**
- **Flexible** to allow innovation
- Technology **neutral**

**People**
Providers of e-signature services are trusted and vetted.

**Process**
Identity checks carried out when onboarding a signer.

**Technology**
Technical measures to protect the integrity of the signed document.
Levels of assurance in practice

The example of the European eIDAS regulation.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signer identity</td>
<td>none</td>
<td>Signer can be identified</td>
<td>Signer can be identified</td>
</tr>
<tr>
<td>Data integrity</td>
<td>none</td>
<td>Modifications after signing detectable</td>
<td>Modifications after signing detectable</td>
</tr>
<tr>
<td>User onboarding</td>
<td>none</td>
<td>none</td>
<td>Identity verification done face to face</td>
</tr>
<tr>
<td>Technology</td>
<td>none</td>
<td>none</td>
<td>Digital certificate (PKI)</td>
</tr>
<tr>
<td>Certificate issuer</td>
<td>none</td>
<td>none</td>
<td>Audited for compliance with rigorous standards</td>
</tr>
<tr>
<td>Signing device</td>
<td>none</td>
<td>none</td>
<td>High security device from approved list</td>
</tr>
</tbody>
</table>
Legal Framework

Legal effect
- Enforceability
- Admissibility as evidence
- Presumption of validity

Mutual recognition
- Scaling trust across borders

Trust Framework

Laws
Regulations
Legal Framework

- Mutual Recognition
- National Legal Framework

Trust Framework

- Levels of Assurance
- Requirements for evidence and assurance

Sources of Trust

- Evidence of Reliability
- Pre-existing Trust
The role of **PKI**

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Role PKI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity</strong></td>
<td>none</td>
</tr>
<tr>
<td><strong>Attribution</strong></td>
<td>none</td>
</tr>
<tr>
<td><strong>Endorsement</strong></td>
<td>none</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td><strong>Hashing</strong> ensures that the content of a document has not been modified after signing.</td>
</tr>
<tr>
<td><strong>Nonrepudiation</strong></td>
<td>Verifiable <strong>timestamps</strong> ensure that the signer cannot deny having previously signed a document.</td>
</tr>
</tbody>
</table>
What is a **PKI**?
The majority of e-signature use cases are relatively low risk. However, very high value transactions can also be signed electronically if there is enough trust.
Signatures are all around us

Sample use case: Online loan application