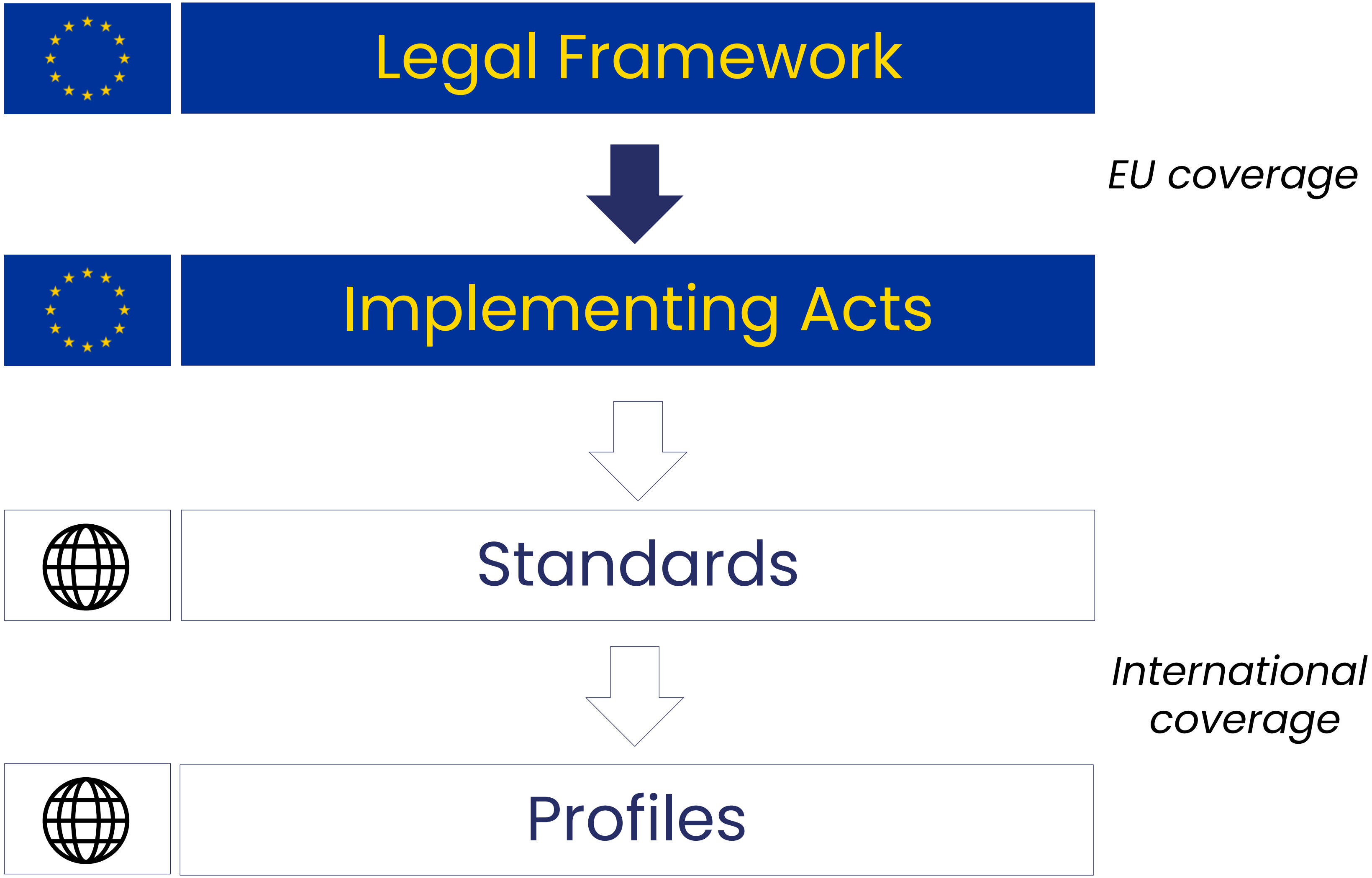
iDAKTO

Profiles for achieving interoperability in the EUDIW ecosystem

Andreea Prian – Standardisation Officer

TDI 2025

Requirements for the EUDIW



Legal Framework

Implementing Acts

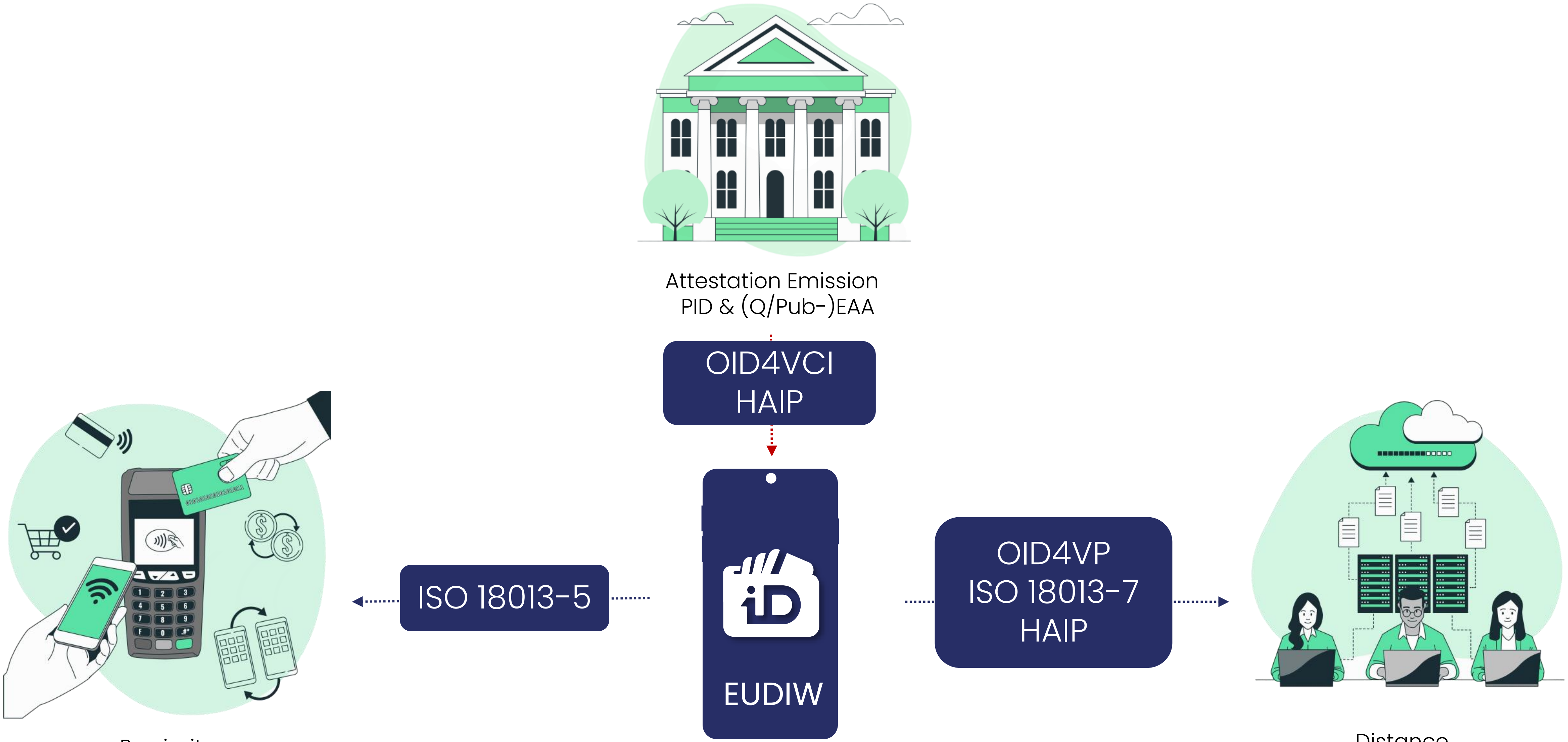
Standards

Profiles

EU coverage

International coverage

Current state of play



Attestation Emission
PID & (Q/Pub-)EAA

OID4VCI
HAIP

EUDIW

ISO 18013-5

OID4VP
ISO 18013-7
HAIP

Proximity
verification

Distance
verification

Current state of play

What we have:

Commission Implementing Regulation (EU) 2024/2982

- ISO/IEC 18013-5:2021
- ISO/IEC TS 18013-7:2024

European Digital Identity Wallet Architecture and Reference Framework

- OpenID4VC High Assurance Interoperability Profile

What we need:

- eIDAS compliance
- GDPR compliance
- EU governance

A user-centric wallet

eIDAS *« Sole control of the user »*

What we need :

Consent Management key points:

- **Consent Process**: how consent is obtained.
- **Information Display**: data, processing purpose, retention period, access certificate.
- **Scope of the Consent**: Selective disclosure, intent to retain, signing.
- **Consent Duration**
- **Technical Implementation**

Data processing

Further aspects for GDPR compliance

“intent_to_retain”

How should this field be used in relation to the relying party policy?

Relying parties requirements

eIDAS *“**Authenticate** and **identify** relying parties”*

What we need:

- Mandate the relying party authentication
- Mandate sending signed requests
- Specify what is a valid signature (cryptographic validation, attributes checks)
- Specify what is a valid certificate (validation model, extensions, trust list)

Wallets as relying parties

eIDAS

*“**Authenticate** and **validate** wallet unit attestations of other wallet units”*

🕒 What we need

<u>Request sender wallet:</u>

- Specify how the request is built
- Specify if/how the request is signed

<u>Recipient wallet:</u>

- Specify how to validate a wallet unit attestation
- Specify how to enforce the « right-to-ask » of another wallet

Authenticating PID Providers

eIDAS

“PID providers shall identify themselves to wallet units using their wallet-relying party access certificate or by using ***another authentication mechanism*** *in accordance with an electronic identity scheme notified at assurance level high.”*

🕓 **What we need**

How to implement an eID scheme-based authentication mechanism?

Trust ecosystem

Trusted lists

eIDAS

- *Wallet Providers*
- *PID Providers*
- *QEAA Providers*
- *PuB-EAA Providers*
- *EAA Providers*

- *Access Certificate Authorities for:*
  - *Relying Parties*
  - *PID Providers*
  - *QEAA Providers*
  - *PuB-EAA Providers*

🕓 What we need

For every authentication (and therefore certificate validation) we should know **what list to use** and **what information to extract and analyze.**

Trust ecosystem

Trusted lists

eIDAS

- *Wallet Providers*
- *PID Providers*
- *QEAA Providers*
- *PuB-EAA Providers*
- *EAA Providers*

- *Access Certificate Authorities for:*
  - *Relying Parties*
  - *PID Providers*
  - *QEAA Providers*
  - *PuB-EAA Providers*

What we need

How to implement the establishment of trust in the WSCD?

Algorithms

Further aspects for EU governance

What we need

Accepted algorithms recognized by the EU taking into account :

- Technical limitations due to WSCD types
- A limited set to improve cumbersome algorithm negotiation between wallet & relying party

Conclusion

- We have incomplete profiles that do not address all regulatory requirements.

- We need specific profiles for the EUDIW built on top of the existing standards/profiles.

Why:

- Technical interoperability, but also:
- Legal compliance and legal equivalence

iDAKTO

Thank you