

TeleTrust-Informationstag "Elektronische Signatur und Vertrauensdienste"

Berlin, 12.11.2025

ENISA EUDI Wallet certification scheme

**Sebastian Elfors,
CSO at IDnow Trust Services
Rapporteur of ENISA EUDIW AHWG TG1**



1. The conformity of European Digital Identity Wallets and the electronic identification scheme under which they are provided with the requirements laid down in Article 5a(4), (5), (8), the requirement for logical separation laid down in Article 5a(14) and, where applicable, with the standards and technical specifications referred to in Article 5a(24), **shall be certified** by conformity assessment bodies designated by Member States.

And several other articles providing additional details, including the need to define an Implementing Act “establish[ing] a list of reference standards and where necessary, establish[ing] specifications and procedures for the certification of European Digital Identity Wallets referred to in paragraph 1, 2 and 3 of this Article”.



EUROPEAN AND NATIONAL SCHEMES

The objective is to have a European scheme, but the first step will be to establish national schemes.

ENISA has received a request to develop an EU scheme for EUDI Wallets

- The development will start in early 2025, and will take some time

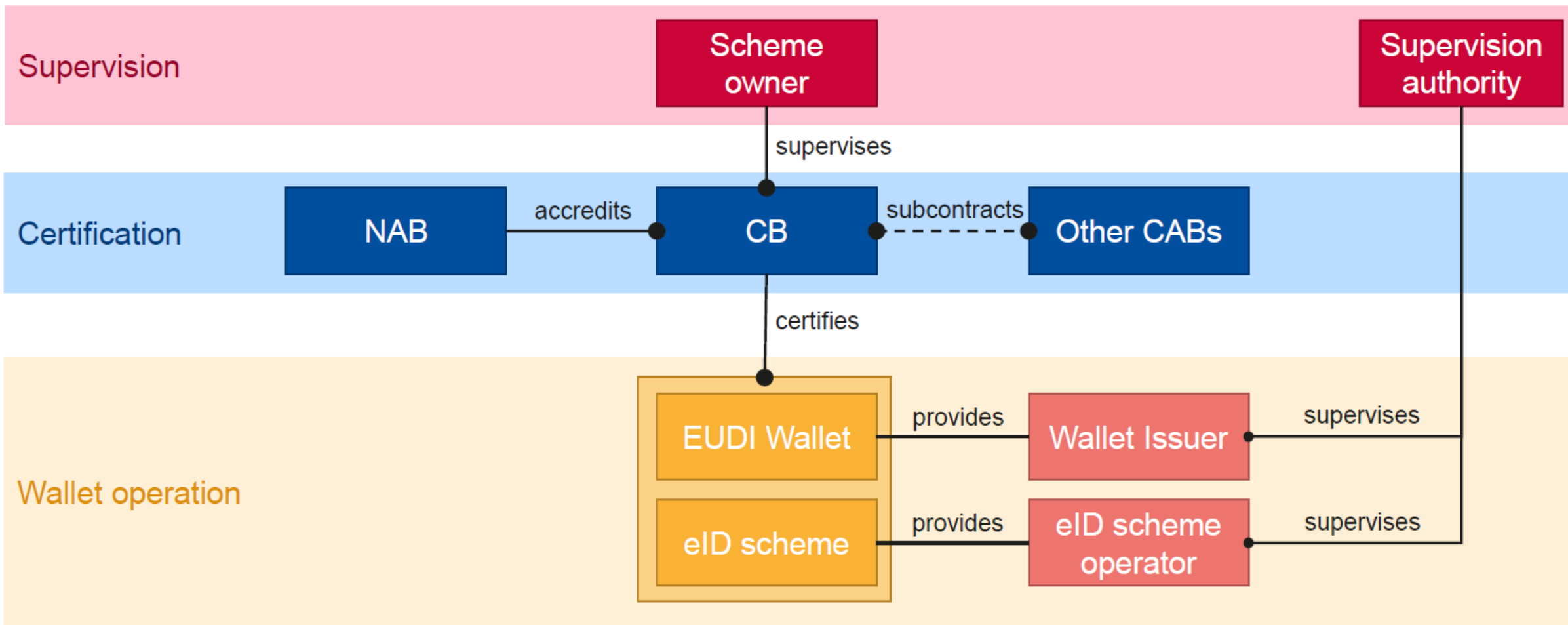
But national schemes will be required for two distinct reasons

- The European schemes will not cover functional certification, and it will arrive too late for the first generation
- The use of national schemes raises specific issues, in particular related to interoperability
- This is why the Implementing Act on 5c defines some common rules for national schemes

Work will continue in parallel on national and European schemes



A FEW ROLES IN CERTIFICATION





CERTIFYING WHAT?

Many requirements are functional

- Interfaces of the EUDI Wallet to relying parties and others
- Specifications to be defined in other epics and/or standards
- Conformity assessment to be based on interoperability test suites associated to standards/specs

Cybersecurity is mentioned, but remains implicit in most cases

- Nevertheless, many functions of the Wallet are themselves security functions (authentication), so they are covered by the requirements

Privacy?



SCOPE OF CYBERSECURITY CERTIFICATION

In scope

Components

- All wallet-specific components
- Wallet + eID processes
- Integrated as a service

Conformity assessment

- Methods and procedures
- Overall assessment

WSCA

EUCC* certified
Based on a PP
WSCD assumptions

Wallet App

Specific assessment
Device and WSCA
assumptions

eID + EUDIW
management

Mostly audit
With effectiveness

Out of scope

Components

- All user-provided devices
- Generic IT/ISMS/Cloud (?)

Conformity

- Dependency analysis
- Assumptions / Requirements
- Recommended assurance

WSCD

EUCC* certified
Based on VAN.5 domain

Device
platform

Assurance doc
Ad hoc evidence

ISMS / IT /
Cloud

Assurance doc
Ad hoc evidence



SCOPE OF CYBERSECURITY CERTIFICATION

In scope

Components

- All wallet-specific components
- Wallet + eID processes
- Integrated as a service

Conformity assessment

- Methods and procedures
- Overall assessment

WSCA

EUCC* certified
Based on a PP
WSCD assumptions

Wallet App

Specific assessment
Device and WSCA
assumptions

eID + EUDIW
management

Mostly audit
With effectiveness

Processes

Components

- Specific ID processes
- Development & deployment
- Maintenance

Conformity

- Existing certification
- Specific audits, with regular ones

On-boarding

Schemes exist
as a basis

Provisioning
Deployment

Mostly audit
With effectiveness

Development
Operations

Mostly audit
With effectiveness



INITIAL FOCUS ON FOUR TOPICS

Standardisation gaps

We are looking at the ongoing standardisation efforts and analysing the gaps related to the security.

Gap analysis is available, now deep-diving into the security requirements to refine the gaps.

Object of certification

The object of certification “EUDI Wallet and the eID scheme under which it is provided” is very wide, so we worked on that

Secure apps, mobile and Web apps, IT systems, ISMS, processes, etc.

Assessment of components

Every component of the object of certification needs to be assessed.

EUCC, FitCEM, FR MIE, MASA, ISO 27001, etc.

Main scheme and more

This includes the key questions about a scheme, as well as the global evaluation activities.

Certification lifecycle, monitoring and compliance, etc.

Vulnerability assessment, risk assessment, evidence assessment, etc.



MANY STAKEHOLDERS INVOLVED

Commission

- Implementing Acts
- ARF

ESOs (CEN, ETSI)

- Requirement standards
- Methodology standards

Member States

- National EUDI schemes
- Other national schemes

CABs

- Labs and CBs for component
- Labs and CBs for “main” certificate

Vendors

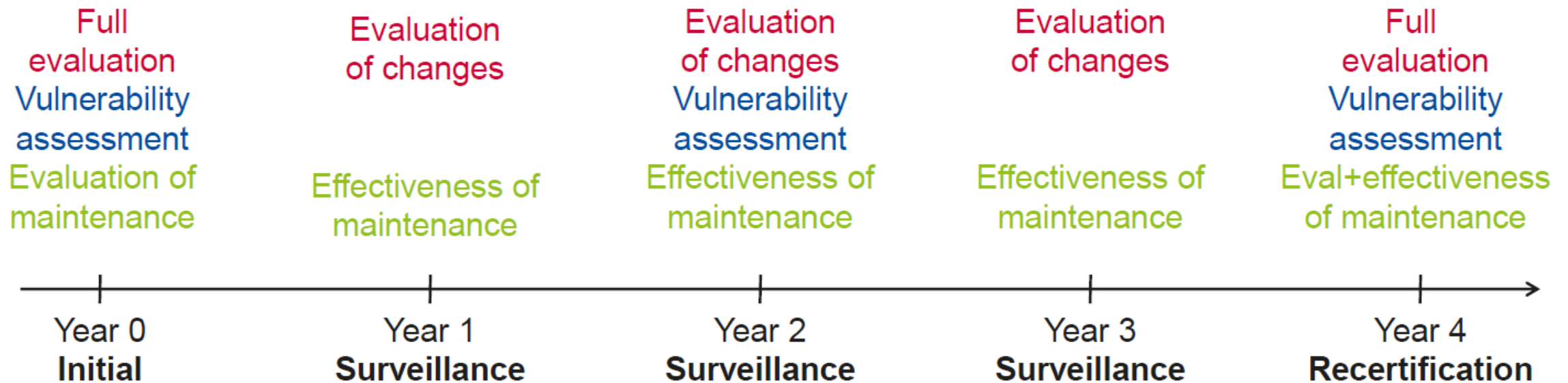
- Wallet developers/providers
- Component developers/providers

ENISA communities

- EUDIW Ad Hoc Working Group
- EUCC maintenance group



CERTIFICATION LIFECYCLE



All products need to include an update feature

Maintenance processes include at least version control, update, and vulnerability management

References.

Eric Vetillard's [presentation](#) at CEN ETSI plenary in Sophia Antipolis on September 12, 2024.

Eric Vetillard's [presentation](#) at ENISA Trust Services Forum in Split on September 24, 2025.



THAT'S IT!

Thank you!



Stay in touch!

[Click Here](#)

Sebastian Elfors
CSO
IDnow Trust Services

