

European Digital Identity Wallet Certification: Where Do We Stand?

Evgenia Nikolouzou
Cybersecurity Expert, Certification Unit

Legal Context

A requirement from eIDAS

Article 5c

Certification of European Digital Identity Wallets

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.

Article 5c

Certification of European Digital Identity Wallets

2. Certification of the conformity of European Digital Identity Wallets with requirements referred to in paragraph 1 of this Article, or parts thereof, that are relevant for cybersecurity shall be carried out in accordance with European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council (1) and referred to in the implementing acts referred to in paragraph 6 of this Article.

Legal Context

A requirement from eIDAS

Article 5a

European Digital Identity Wallets

4. European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to:
- (a) securely request, obtain, select, combine, store, delete, share and present, under the sole control of the user, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, in offline mode, in order to access public and private services, while ensuring that selective disclosure of data is possible;

Long list of functional requirements

Article 5a

European Digital Identity Wallets

5. European Digital Identity Wallets shall, in particular:
- (a) support common protocols and interfaces:

...
 - (d) meet the requirements set out in Article 8 with regard to assurance level high, in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication;

...

Legal Context

Scheme developed in accordance with the Cybersecurity Act

(EU) No 910/2014 (eIDAS)

(EU) 2024/2981 (CIR 5c)

(EU) 2015/1502 (CIR)

(EU) 2019/881 (CSA)

Article 49

Preparation, adoption and review of a European cybersecurity certification scheme

2. **Following a request** from the Commission pursuant to Article 48, **ENISA shall prepare a candidate scheme** which meets the requirements set out in Articles 51, 52 and 54.

4. For each candidate scheme, **ENISA shall establish an ad hoc working group** in accordance with Article 20(4) for the purpose of **providing ENISA with specific advice and expertise.**

Legal Context

Scheme developed in accordance with the Cybersecurity Act

(EU) No 910/2014 (eIDAS)

(EU) 2024/2981 (CIR 5c)

(EU) 2015/1502 (CIR)

(EU) 2019/881 (CSA)

Article 49

Preparation, adoption and review of a European cybersecurity certification scheme

3. When preparing a candidate scheme, **ENISA shall consult all relevant stakeholders** by means of a formal, open, transparent and inclusive consultation process.

6. **ENISA shall take utmost account of the opinion of the ECCG** before transmitting the candidate scheme prepared in accordance with paragraphs 3, 4 and 5 to the Commission. The opinion of the ECCG shall not bind ENISA, nor shall the absence of such an opinion prevent ENISA from transmitting the candidate scheme to the Commission.

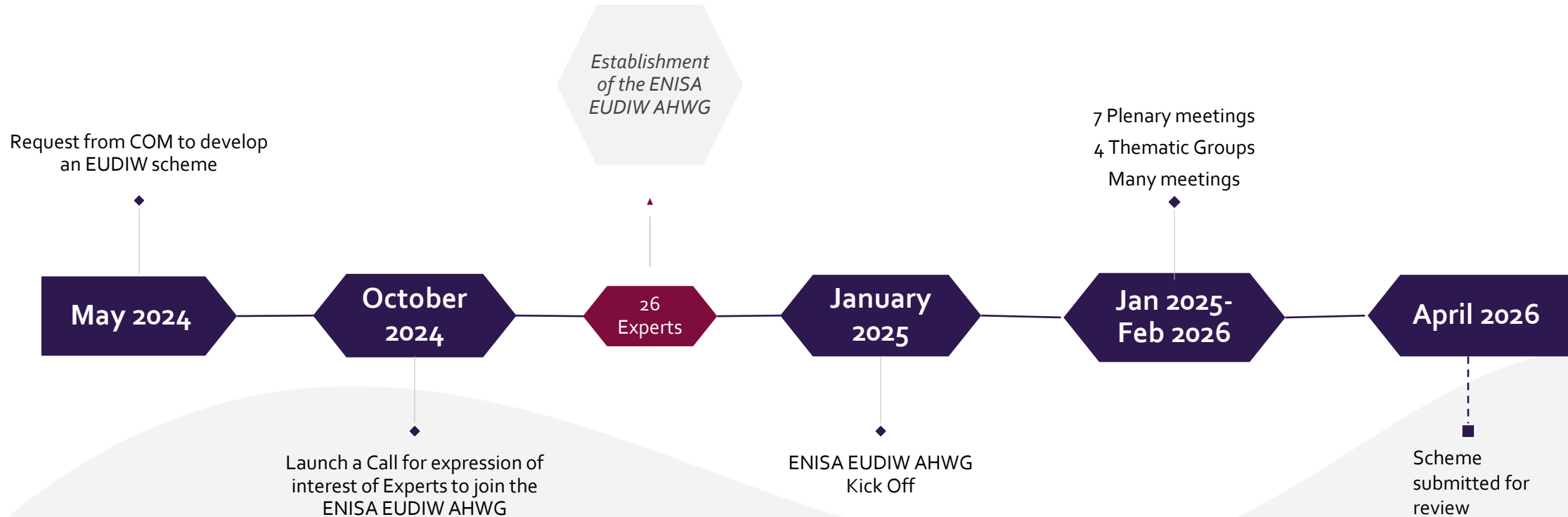
Legal Context

Many other relevant regulations

(EU) No 910/2014	(eIDAS)	(EU) 2024/2977	(PID/EAA)
(EU) 2024/2981	(CIR 5c)	(EU) 2024/2979	(Wallet functions)
(EU) 2015/1502	(CIR)	(EU) 2024/2982	(Protocols & Interfaces)
...			
(EU) 2019/881	(CSA)		
(EU) 2016/679	(GDPR)		
(EU) 2022/2555	(NIS2)		
(EU) 2024/2847	(CRA)		

Current status

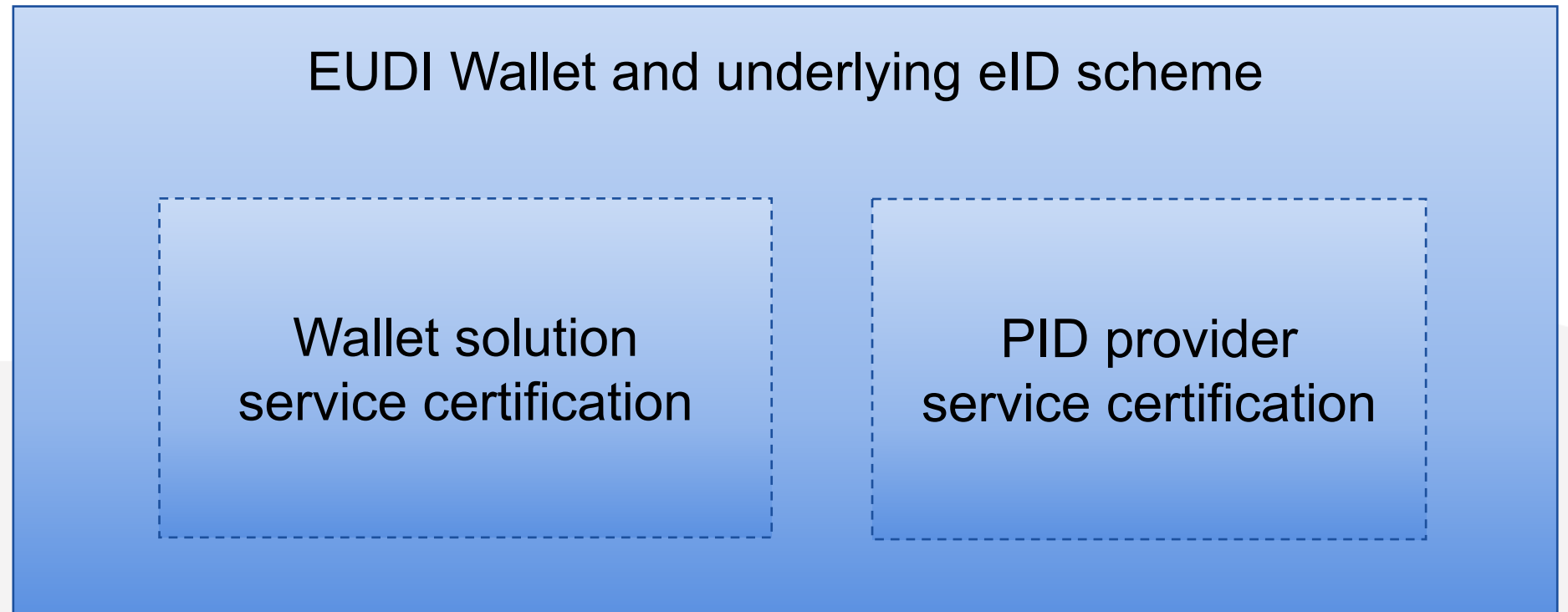
Reaching maturity



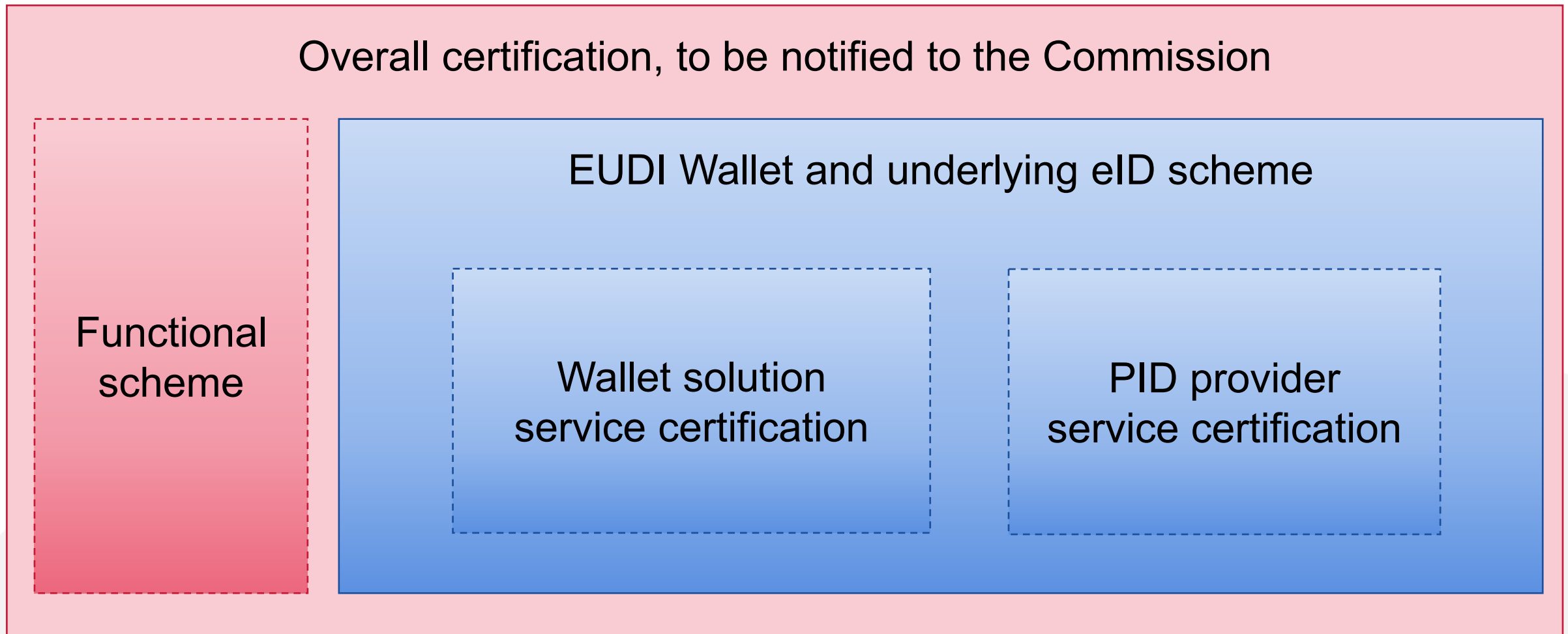
Part 2

Objectives of the scheme

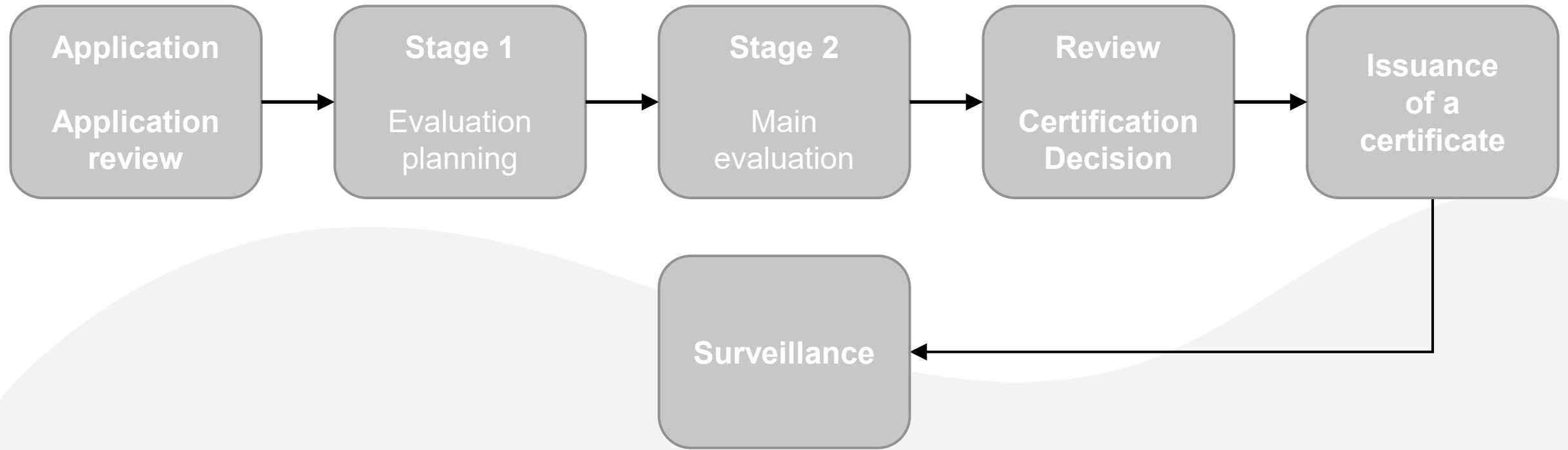
One EU scheme



One EU scheme, 27 national certification systems

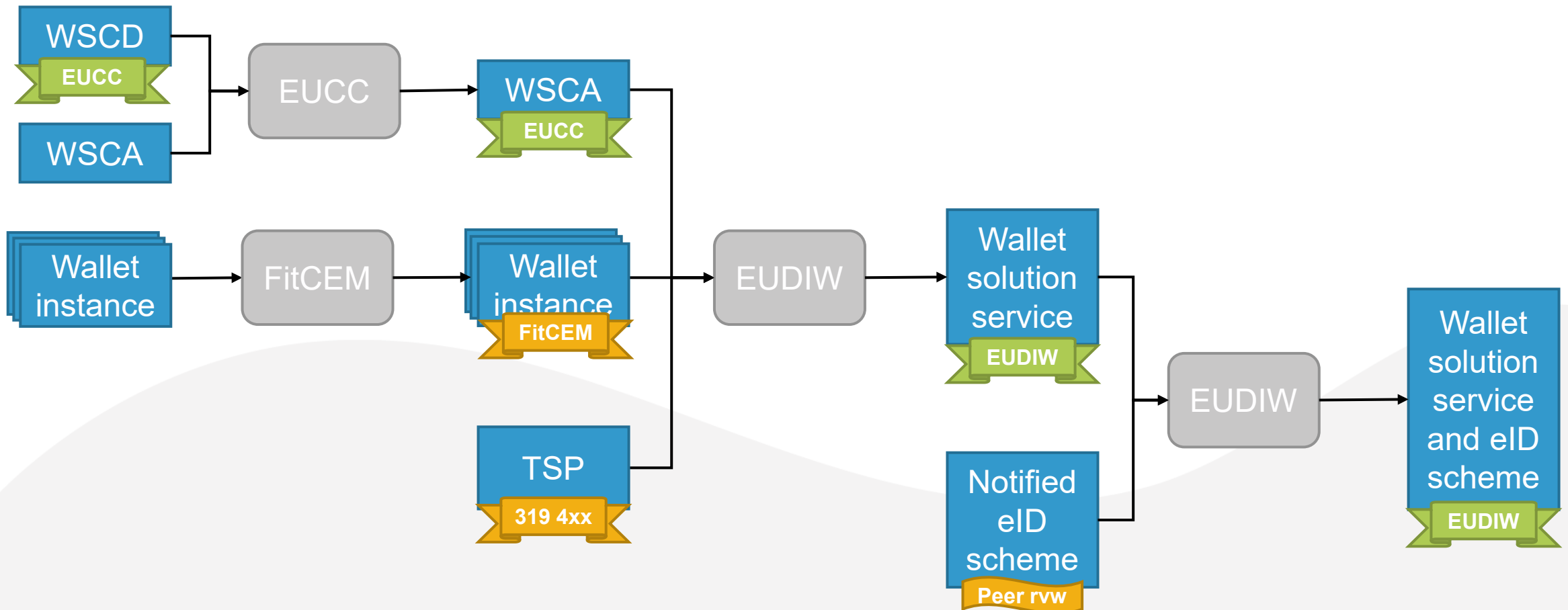


Overview of the certification process



Composition in EUDIW

Example using existing components



Part 3

Specific points of attention

Strong ties to EUCC

Integrated in the European Cybersecurity Certification Framework (ECCF)

Many elements of the scheme are inspired from EUCC (CIR (EU) 2024/482)

- The structure of the scheme itself
- Many parts of the scheme, where harmonisation is interesting, always adapted
 - Issuance, renewal and withdrawal of certificates → Certificate amendments
 - Compliance monitoring → Relation to materiality
 - Consequences of nonconformity and non-compliance → Relation to materiality
 - Peer assessment rules → No sampling rules

Composition with EUCC is simpler because of these similarities

- The EUCC certificates are fully trusted on all aspects

Level of assurance

Two different kinds of assurance level high

There are two levels of assurance applying

- From CSA, we have selected assurance level high for the entire wallet
- From eIDAS, assurance level high applies to the EUDI Wallet as eID means

And they are not the same! If we consider EUCC, for instance

- Level CSA-high covers AVA_VAN.3 to AVA_VAN.5
- Level eIDAS-high mentions attackers with high attack potential, which hints at AVA_VAN.5

What can it mean for the EUDI Wallet as a whole?

- AVA_VAN.5 level protection is required for critical assets (mostly cryptographic keys)
- AVA_VAN.3 level protection is required for about everything else (still in discussion)

Part 5

What's next?

This is a draft candidate scheme

So, it is not finished

The scheme itself is quite advanced, but it is not 100% finished

Calling for feedback

The present public review is really looking for two kinds of feedback

- Detailed feedback on the draft candidate scheme itself and on its annexes
- Feedback on the directions for the development of security requirements

There will be more opportunities to contribute before the adoption

- The Commission will have a “Have your say!” on the draft Implementing Act



Thank you for your attention



+30 28 14 40 9711



certification@enisa.europa.eu



certification.enisa.europa.eu

ENISA

European Union Agency
for Cybersecurity

Athens Office

Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office

Rue de la Loi 107
1049 Brussels, Belgium