Draft cybersecurity certification candidate scheme for EUDI Wallets

and the eID schemes under which they are provided

Eric Vetillard
Lead Certification Expert, Certification Unit

08/04/2026

Agenda

1 Legal context and status

2 Objectives of the scheme

3 Specific points of attention

4 Security requirements

5 What's next

Part 1

Legal context and status

Legal Context

A requirement from eIDAS

(EU) No 910/2014 (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.

Legal Context

A requirement from eIDAS

(EU) No 910/2014 (eIDAS)

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

(EU) No 910/2014 (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

Legal Context

A requirement from eIDAS

(EU) No 910/2014 (eIDAS)

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

A requirement from eIDAS

(EU) No 910/2014 (eIDAS)

Article 8

Assurance levels of electronic identification schemes

2. The assurance levels low, substantial and high shall meet respectively the following criteria:

(c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

Legal Context

Several applicable implementing regulations

(EU) No 910/2014	(eIDAS)
(EU) 2024/2981	(CIR 5c)
(EU) 2015/1502	(CIR)

ANNEX

Technical specifications and procedures for assurance levels low, substantial and high for electronic identification means issued under a notified electronic identification scheme

2. **Technical specifications and procedures**

The elements of technical specifications and procedures outlined in this Annex shall be used to determine how the requirements and criteria of Article 8 of Regulation (EU) No 910/2014 shall be applied for electronic identification means issued under an electronic identification scheme.

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) 2026/798	(Remote on-boarding)
(EU) 2019/881	(CSA)		
(EU) 2016/679	(GDPR)		
(EU) 2022/2555	(NIS2)		
(EU) 2024/2847	(CRA)		

Current status

Reaching maturity

ENISA received a request to develop an EU scheme at the end of 2024

The EUDIW AHWG started its work in March 2025

- Several thematic groups were established on specific topics
- First drafts were circulated from June 2025
- Many difficult topics have been addressed, some still ongoing

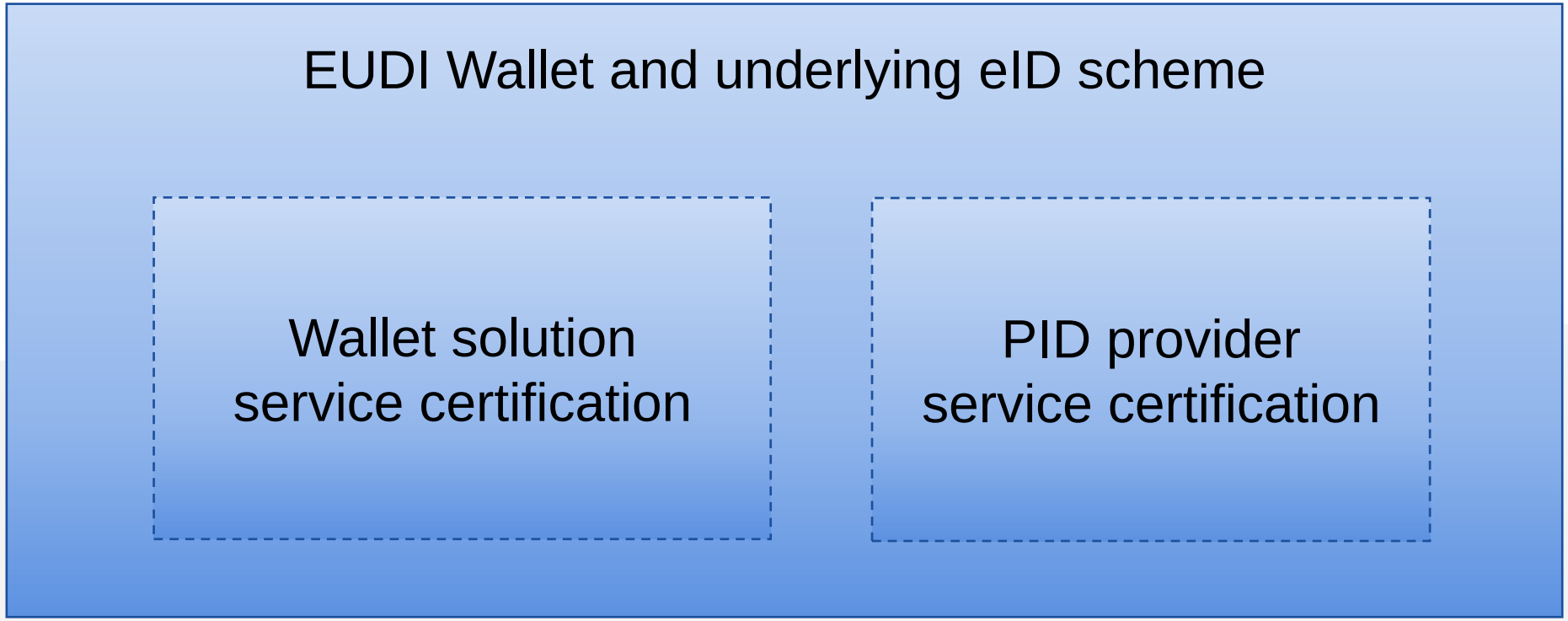
Right time for organising a public survey

- The core scheme and its principles has reached a good level of maturity
- The work on the scheme criteria is less advanced, but sufficient to get feedback

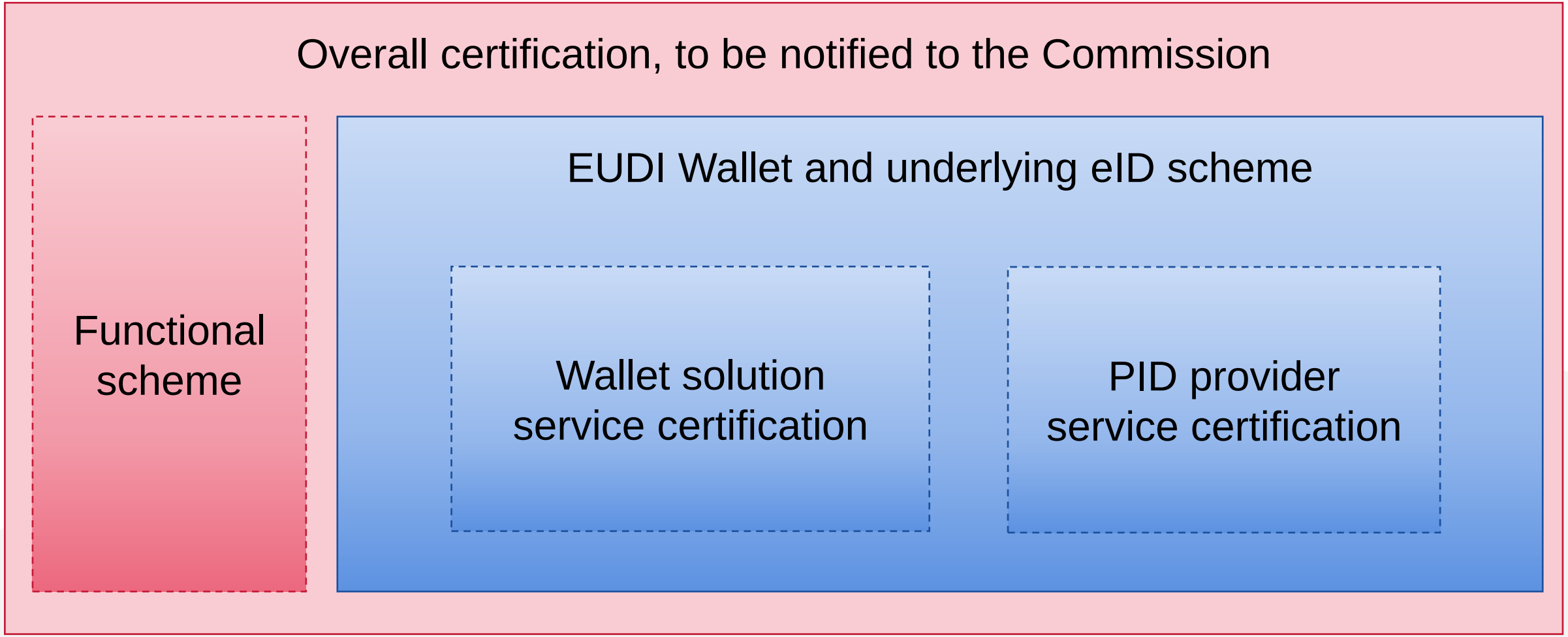
Part 2

Objectives of the scheme

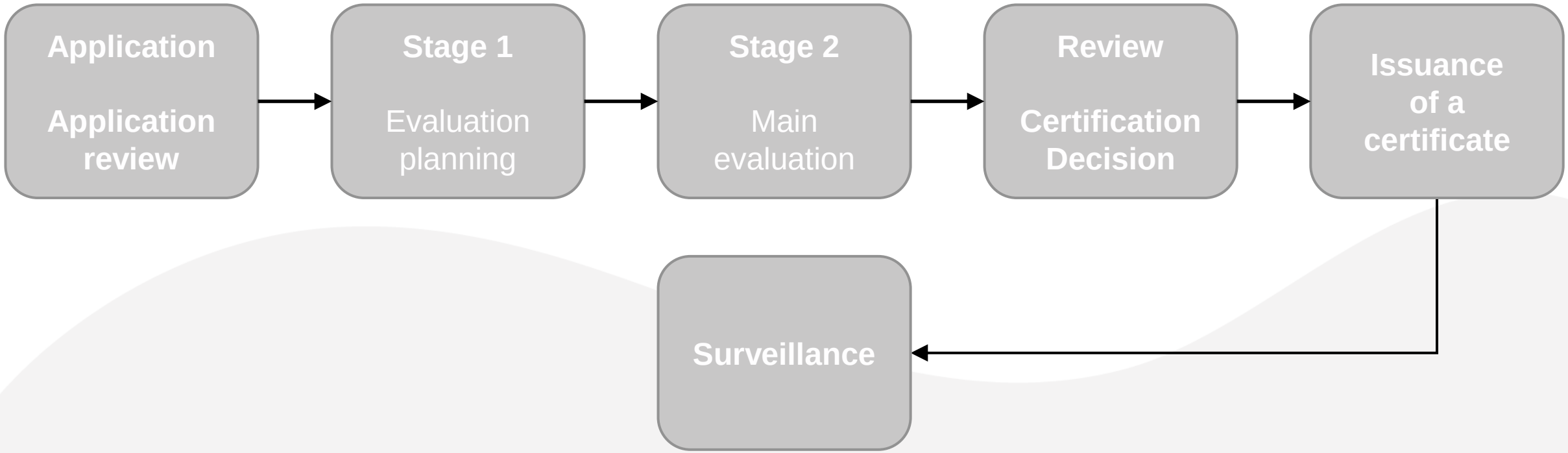
One EU scheme



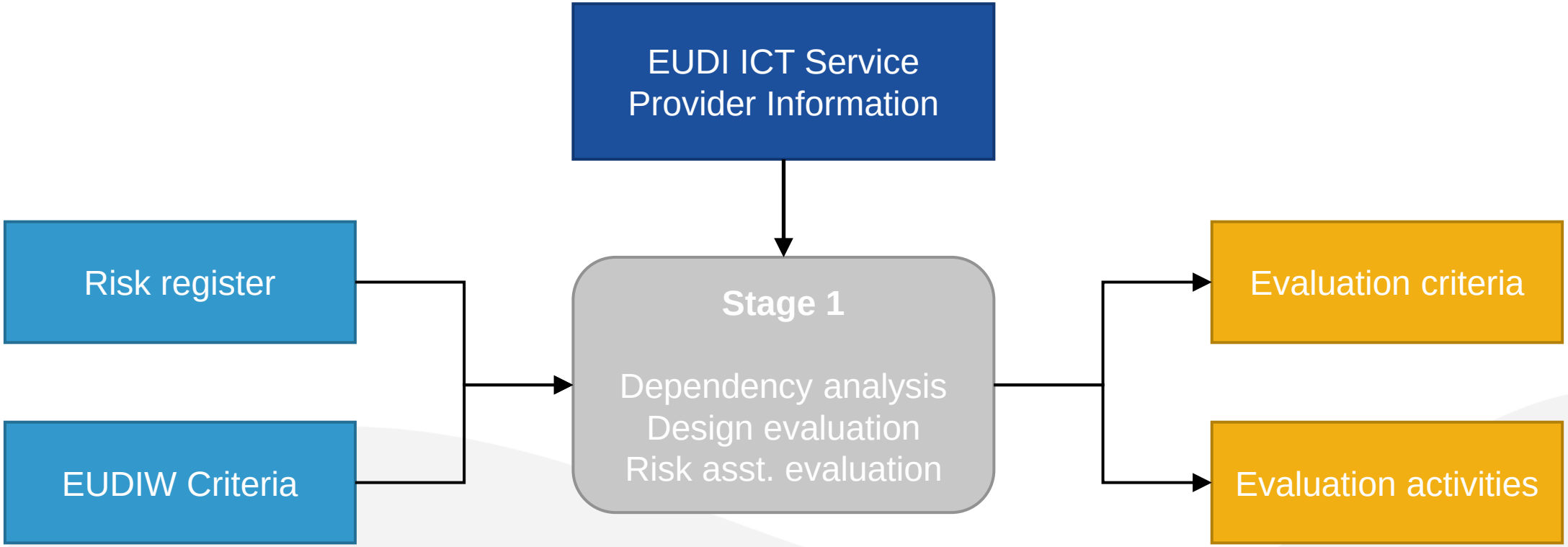
One EU scheme, 27 national certification systems



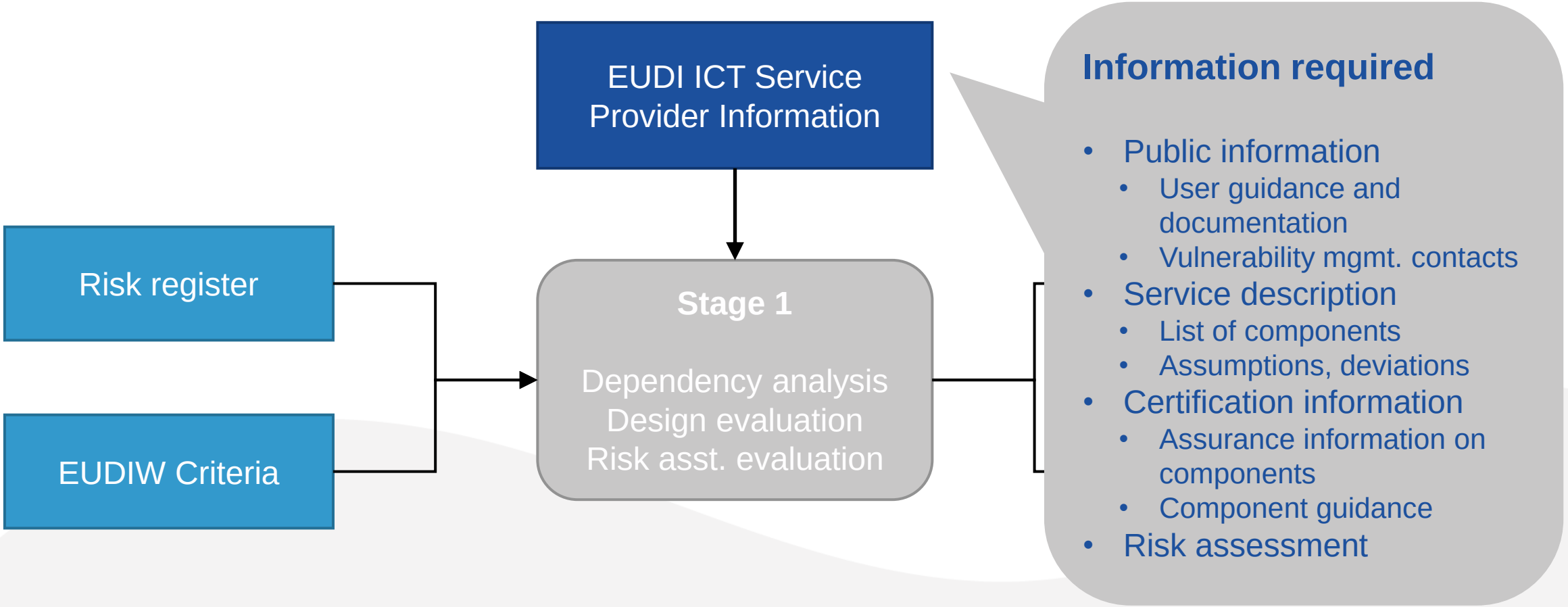
Overview of the certification process



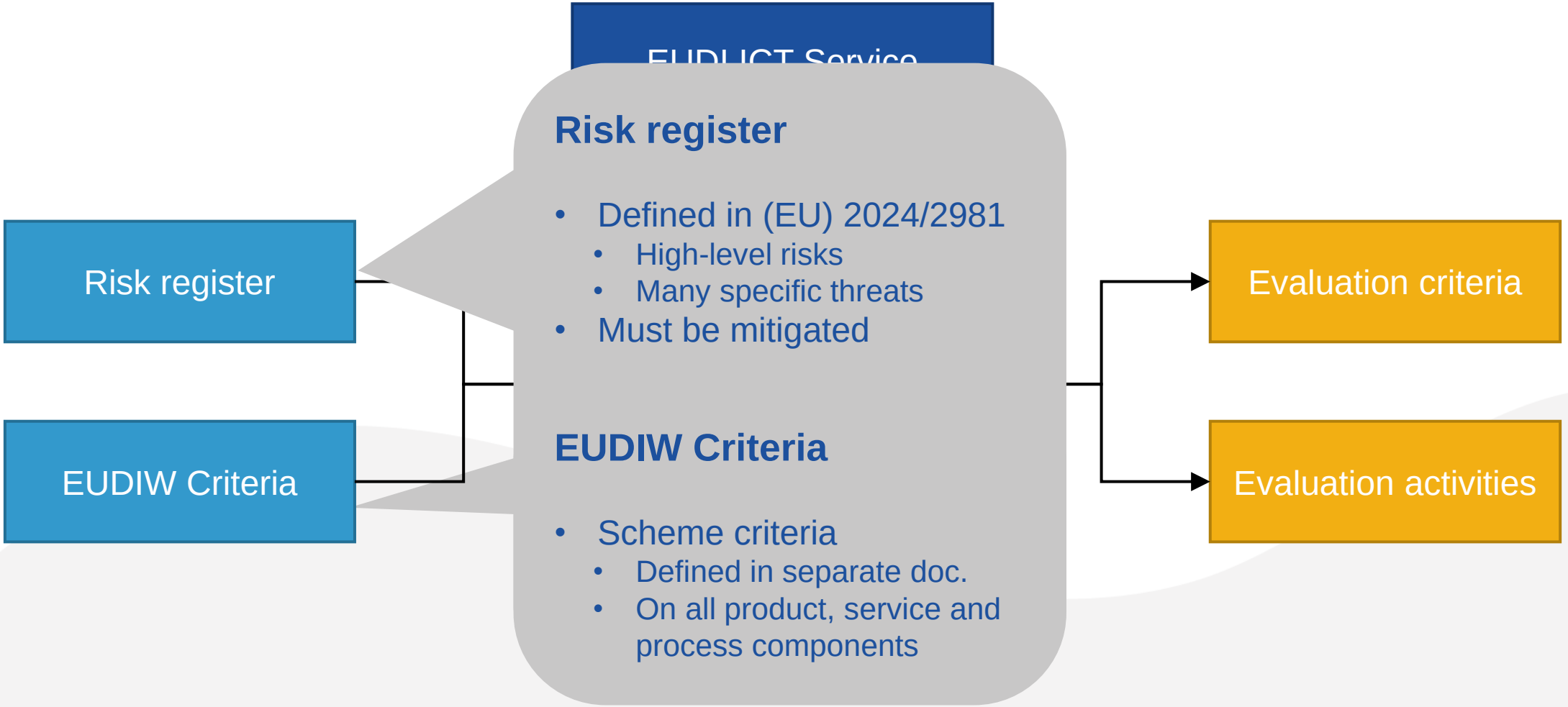
Overview of an evaluation – Stage 1



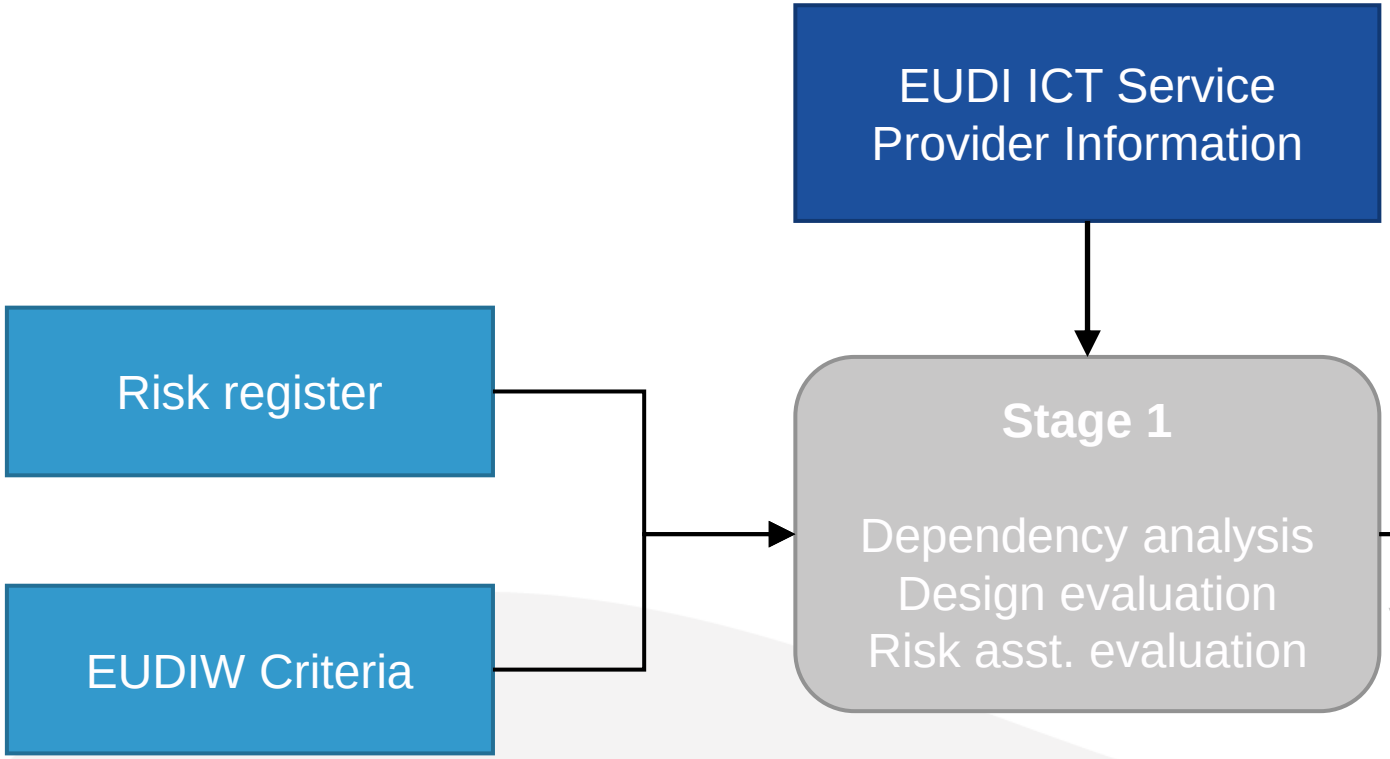
Overview of an evaluation – Stage 1



Overview of an evaluation – Stage 1



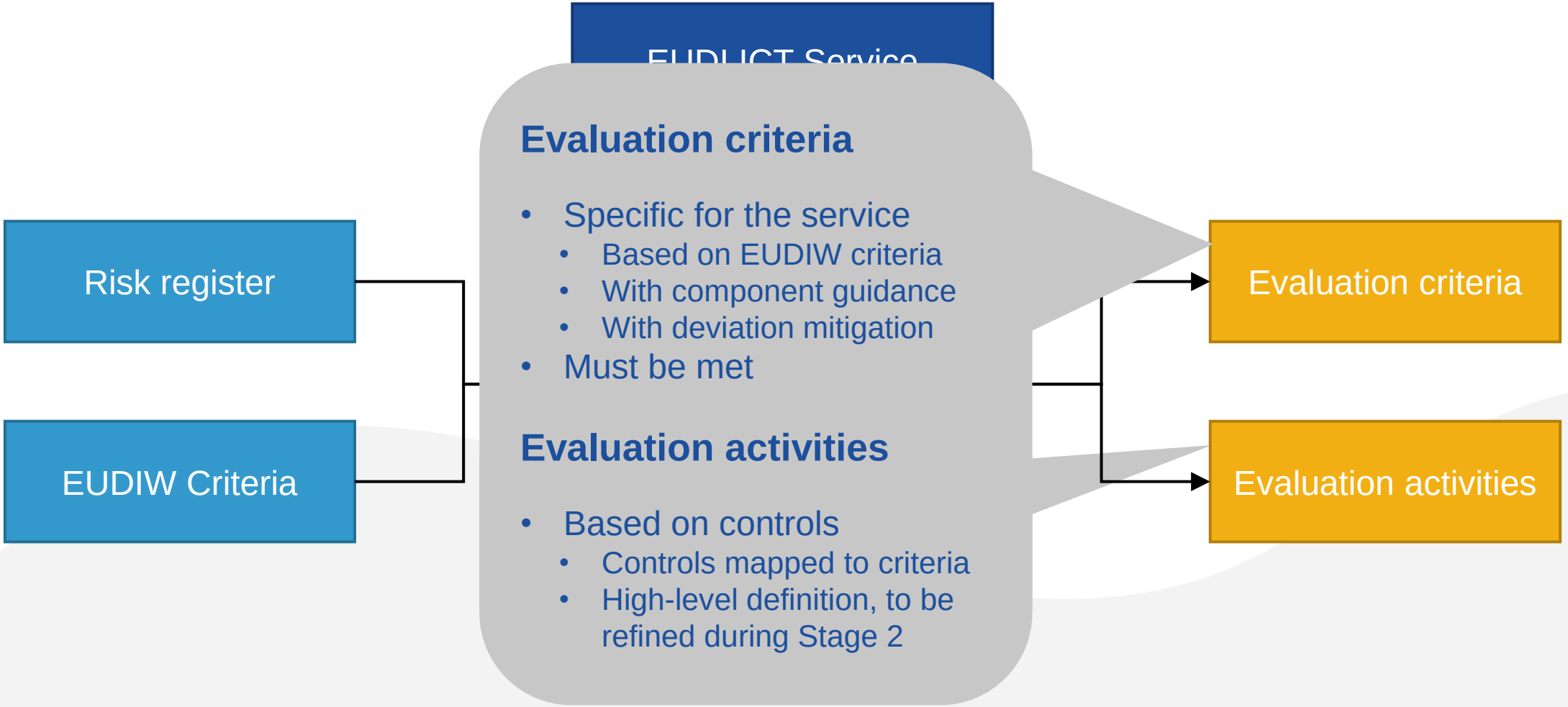
Overview of an evaluation – Stage 1



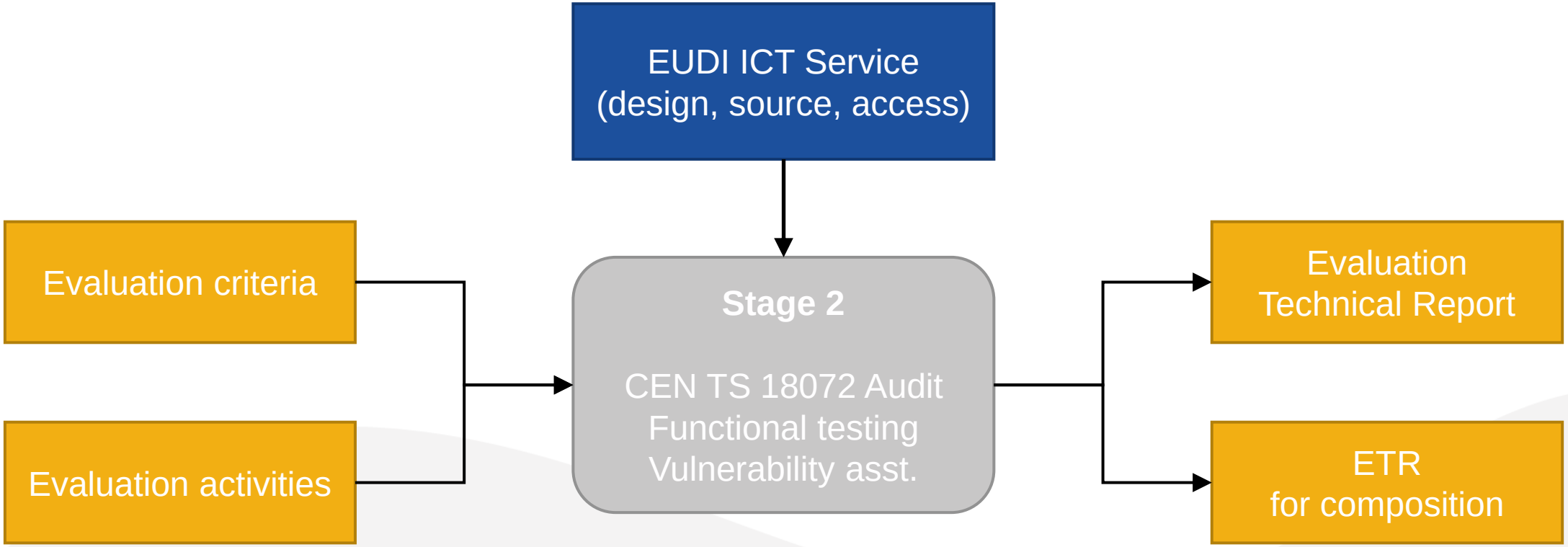
Stage 1 evaluation

- Dependency analysis
  - Analysing assurance information
  - Determining requirements from assumptions/guidance
- Design evaluation
  - Reviewing the documentation
  - Validating deviations
  - Determining requirements from deviation mitigation
- Risk assessment evaluation
  - Ensuring that risk register is covered
  - Reviewing the risk assessment
  - Conforming mitigations of all risks

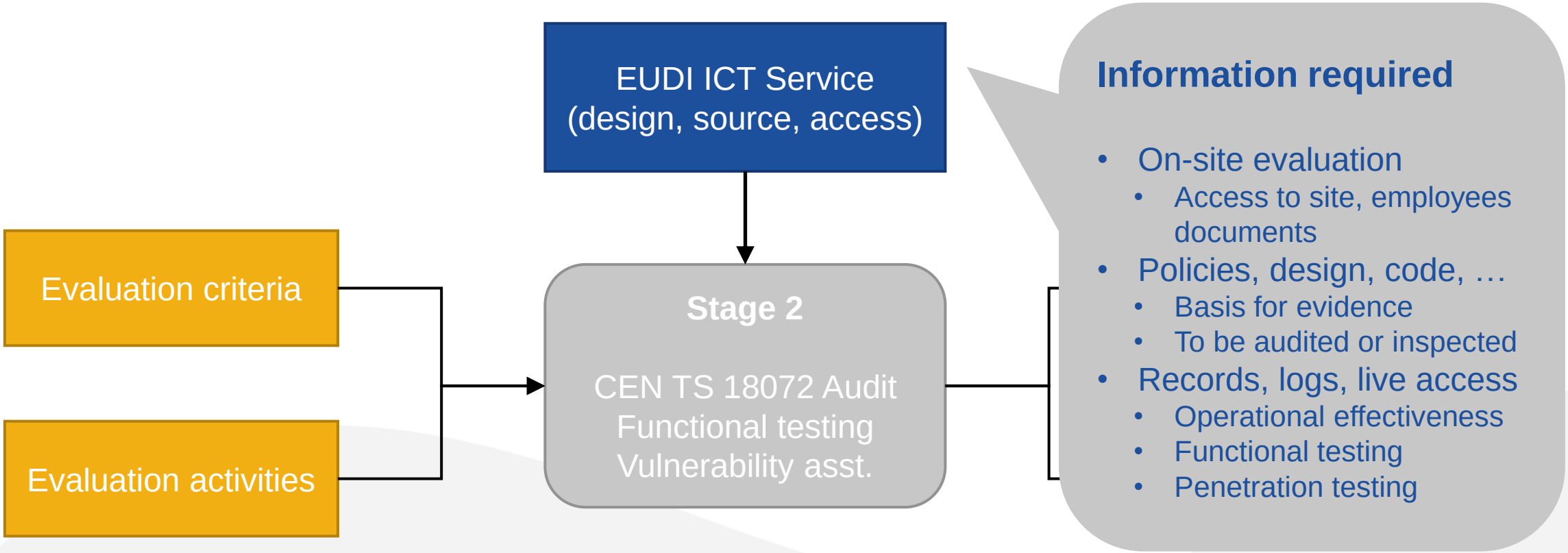
Overview of an evaluation – Stage 1



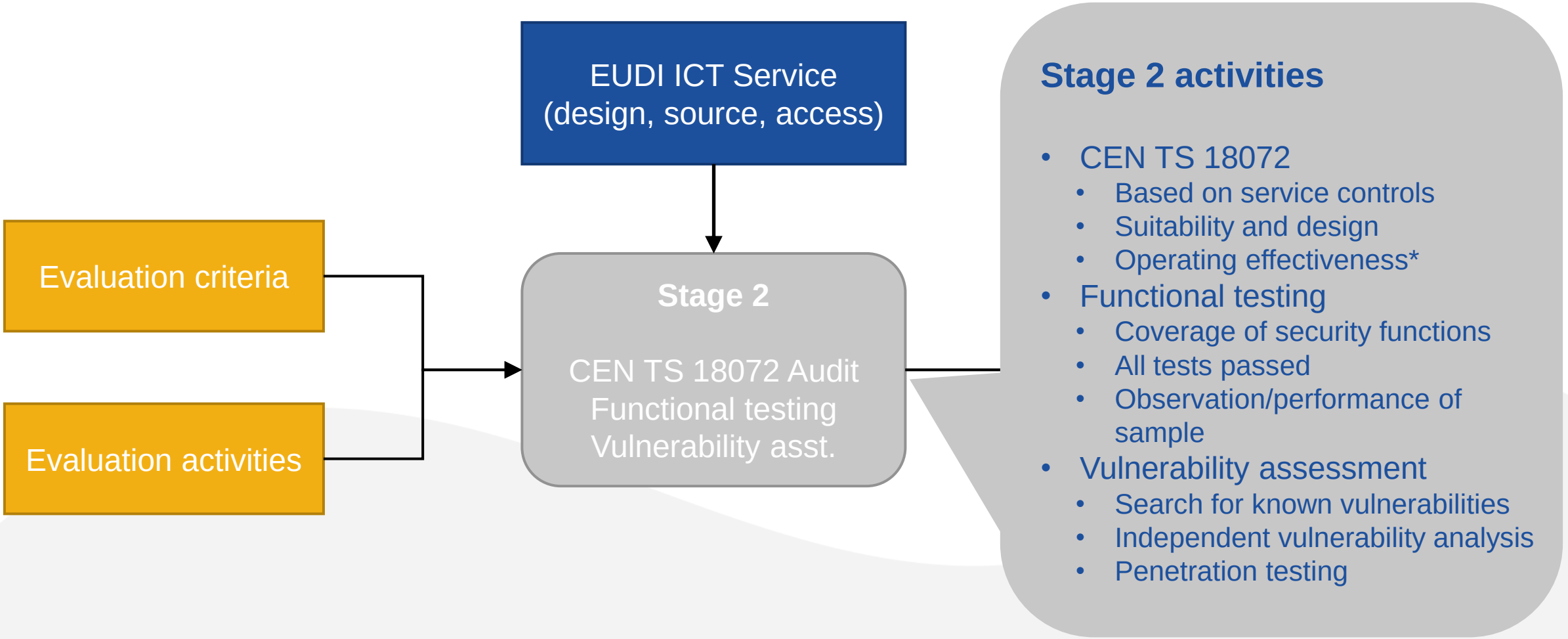
Overview of an evaluation – Stage 2



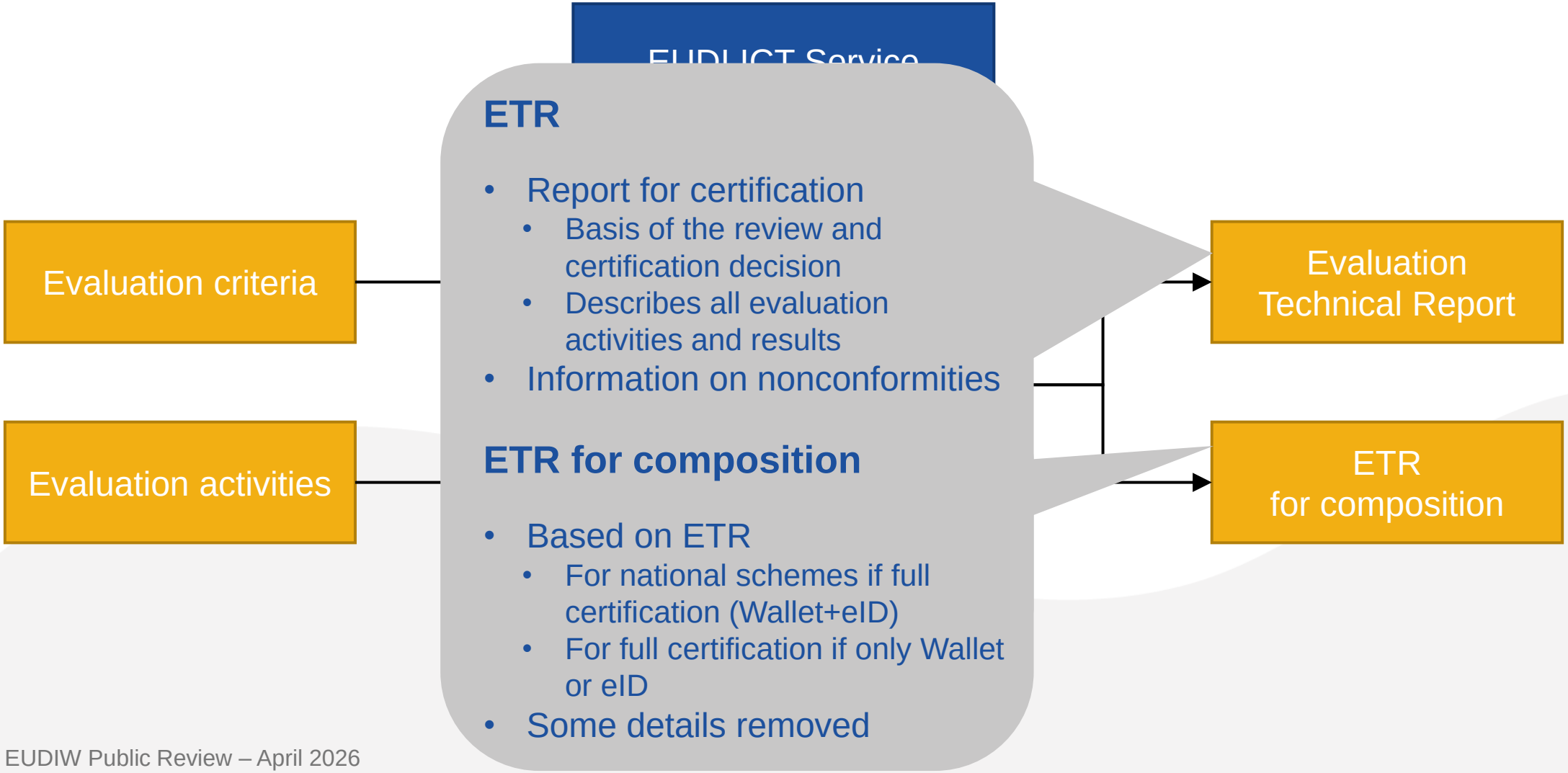
Overview of an evaluation – Stage 2



Overview of an evaluation – Stage 2

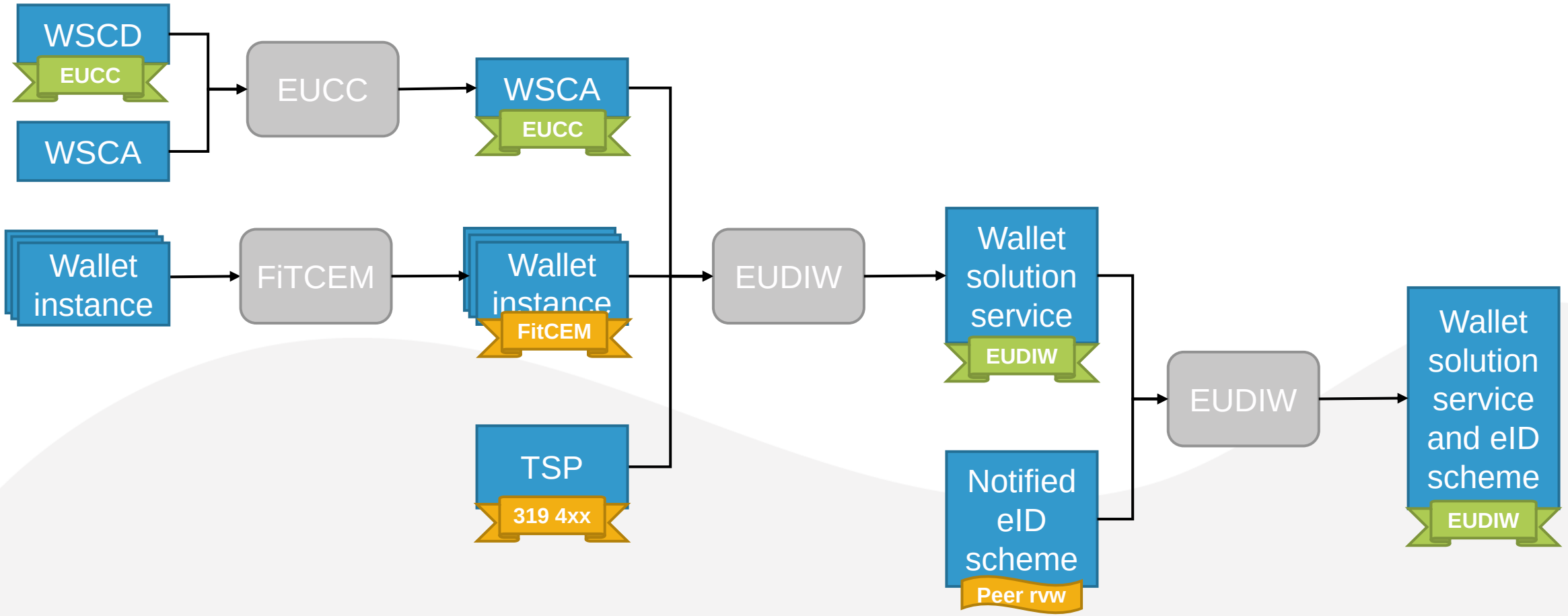


Overview of an evaluation – Stage 2



Composition in EUDIW

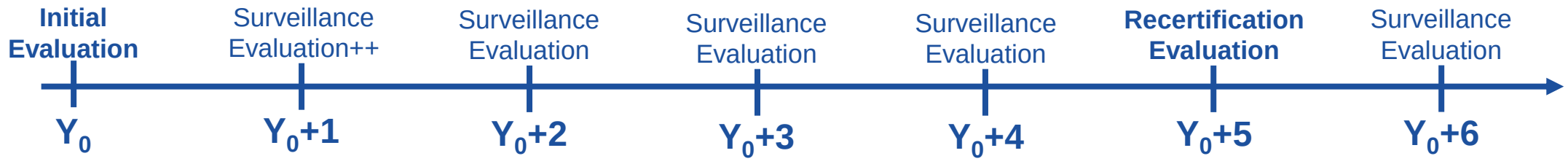
Example using existing components



A simplified certification lifecycle

Combining annual evaluation and vulnerability assessment

The proposed certification lifecycle is:



The main attention points are

- The validity of certificates is up to 5 years, in line with eIDAS requirements (Article 5c(4))
- Only one type of surveillance evaluation, which includes an update of the vulnerability assessment
- The first surveillance evaluation (at Y_0+1) also includes a full evaluation of operating effectiveness

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)

Level of assurance

But what about the services and processes?

It’s much less common to have assurance levels for services and processes

- We worked on it before for cloud services, and this led to CEN TS 18072
- This is why this method is being used (at assurance level high, naturally)
- But it does not solve everything…

Example 1: The WSCA and its AVA_VAN.5 certification

- If running on a secure element of HSM, no problem at all
- If running outside of a secure element (*e.g.*, next to a HSM), then two possibilities
  - Evaluate at AVA_VAN.5 with a strong assumption on the environment → Requirements on environment
  - Evaluate at AVA_VAN.3 and justify a deviation with a strong environment → Requirements on environment
- The environment (a service component) now complements the product component evaluation

CAB requirements

Based on ETSI EN 319 403-1, but with authorisation

Both the EUDI wallet and the eID scheme under which it is provided look a lot like TSPs

- The objective is to reuse the CABs that are already accredited to ETSI EN 319 403-1
- Simply extending the scope of their accreditation
- The same standard may be used for national schemes, further simplifying the accreditation

The scheme also defines an authorisation process, led by the NCCA

- The objective is to validate some competencies, ideally in sync with the accreditation process

The competences are very specific

- Design evaluation (including analysis of deviations)
- Dependency analysis (including all specific criteria)
- Combining all assurance information into assurance for a wallet-related service
- Vulnerability assessment, including penetration testing

Functional testing

Strongly inspired from Common Criteria's ATE Class

The obligation is on all the security functions

- The developer needs to demonstrate that the test coverage is sufficient
- They also need to show a record of a fully successful test campaign (all tests passed)
- The CAB should reperform or observe a reperformance of a subset of the tests

How does this compare to functional conformance testing?

- This testing scope is different
  - It covers the proprietary protocols and internal security functions
  - It does not cover some requirements, in particular related to data protection
- This testing is under the responsibility of the developer, with only a partial reperformance
- Conclusions
  - A functional conformance certificate can be used as evidence for all external interfaces
  - This could be used as conformance testing, but only with additions (add'l tests, full reperformance by CAB)

Part 4

Security requirements

Guiding principle

Scheme reference and application notes

The document is a first attempt at defining security requirements to be used as scheme criteria

- The objective is to define a reference without too much details
- Standards and technical specifications may define further details, their use should remain optional

This version is based on the ARF (waiting for the updated implementing acts)

- It starts from the functional view provided by the HLRs
- Keeping only the requirements that cannot be tested with functional testing
- It therefore includes notes on the conformity assessment of requirements (where relevant)

It is incomplete, and it only covers

- The lifecycle of the wallet
- The provisioning, presentation and lifecycle of eID and attestations

How to define the security requirements?

Legal basis?

- The requirements are rooted in the various Implementing Acts that are defined around the wallet.
- They can be based on:
  - (EU) 2015/1502
  - (EU) 2024/2690
  - (EU) 2024/2977, -79, -82
  - (EU) 2024/2981
  - (EU) 2026/798
- Are they detailed enough?

Functional basis?

- The requirements are rooted in the functional specifications defined in the functional Implementing Acts
- This is the current approach, through the ARF
- Are they generic enough?

Based on EN 319 401?

- ETSI EN 319 401 is used as a basis for TS/TSP requirements, in its latest version, adapted to NIS2.
- This is the current approach
- Are they sufficient for the wallet's assurance level?

Working assumptions

User authorisation

The “main” user authentication gives access to the main application

- All operations that are not related to issuance or presentation of PID and attestations
- All issuance and presentation of attestations on keystores
- There is a possibility to add wallet unit-specific mechanism, like a PIN (wallet or user choice)

The “WSCD” authentication is required when the WSCD is used

- For every issuance or presentation of PID and attestation, just after the user confirmation
- It has to satisfy the requirements on authentication from (EU) 2015/1502 at LoA eIDAS-‘high’
- As discussed before, it may cover several operations, but is required after each user confirmation

Working assumptions

Assurance level of user authorisation

About the assurance level of the “main” user authentication

- By default, being part of the wallet instance, the required level would be AVA_VAN.3 (overall)
- It has to be two-factor authentication, and it has to include an idle timeout

Reaching the assurance level

- We are missing assurance about OS-level authentication. Are there assumptions that we can make?
- Could we make the use of the wallet unit-specific mechanism mandatory when assurance is missing, or when OS-level authentication is known weak?

7 Wallet provider management and operation

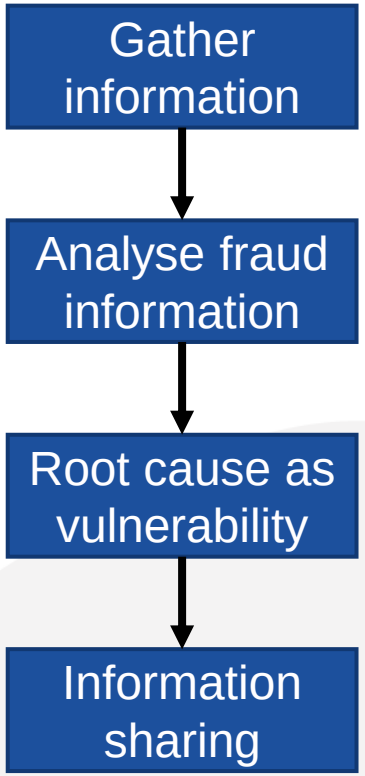
Main addition is fraud management

GEN-7.9.6-01: The EUDI provider shall keep itself informed about fraud and fraud attempts on the services it provides.

GEN-7.9.6-02: The EUDI provider shall analyse the fraud or fraud attempt, and identify, where possible, the opportunity exploited by the malicious agent and the root cause in the implementation of their service.

GEN-7.9.6-03 [CONDITIONAL]: If a root cause has been identified that creates an opportunity for fraud, it shall then be managed as a vulnerability.

GEN-7.9.6-04 [CONDITIONAL]: If a fraud or fraud attempt is managed as a vulnerability, the EUDI provider shall share the resulting impact assessment report and proposed mitigation with the certification body, regardless of the materiality of the impact.



8 Wallet Unit requirements

Covering the entire Wallet Unit

Covers the following topics

- General and lifecycle requirements → Wallet lifecycle, WUA
- Handling of PID and attestations → Provisioning, presentation, re-issuance, revocation
- Horizontal requirements → User authentication, orchestration, authenticity
- Wallet instance requirements → Protection of assets, user interface, mobile/Web
- WSCA requirements → High-level requirements
- Keystore requirements → Assurance guarantees

A few open questions on these requirements

- Need and sufficiency of the horizontal requirements
- Separate document or not?

9-10 Wallet and PID provider requirements

Rather basic things

Wallet provider requirements

- Wallet unit activation and monitoring → Initialisation, device checks
- Issuance and management of WUAs → WUAs from the server side
- Revocation of WUAs → Publication of revocation lists
- Issuance and management of WIAs → Initialisation, device checks

PID provider requirements

- Issuance of PID (as eID means) → Including on-boarding (currently light coverage)
- Management of PID → Including re-issuance
- Revocation of PID → Publication of revocation lists

Not many general debates on these chapters

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

- The main focus has been on completing the proposed mechanisms
- The “parameters” remain to be clarified
  - The reference assurance levels are not fully finalised
    - ~AVA_VAN.5 for critical assets (WSCD), CSA-’high’ or CSA-substantial for identity-critical systems
    - CSA-’substantial’ for handling other non-critical assets, AVA_VAN.3 (CSA-’high’) for the wallet instance
  - More information on the reuse of evidence from more sources
- The content of the annexes needs to be consolidated (annexes, SoTA documents, other)

The requirements are not as mature, and may be fully reconsidered

- Suggestions are welcome on the proper way to define them
- We will also work closely with the ESOs

Contribute, now and later!

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
- We will do another public review of more mature draft security requirements

And it will continue after the adoption of the scheme

- ESOs will continue to work on the requirements, also on more detailed ones
- A maintenance structure will be set up, more open than the AHWG

Thank you for your attention

 +30 28 14 40 9711

 certification@enisa.europa.eu

 certification.enisa.europa.eu

ENISA
European Union Agency
for Cybersecunty

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium