EUDI WALLETS CERTIFICATION

Recommendations for the certification of EUDI Wallets implementations in the short term

MAY 2024

DOCUMENT HISTORY

//DRAFT ONLY - DELETE THIS SECTION AND PAGE UPON FINAL PUBLICATION

Date	Version	Modification	Author
13/12/2023	0.1	Creation	Eric Vetillard
19/12/2023	0.2	Clarification of certification scope following initial discussion	Eric Vetillard
11/01/2024	0.3	Rework of the first two chapters	Eric Vetillard
30/01/2024	0.4	Editorial changes	Alessia Krioutchkova
04/04/2024	0.5	Update of annexes, changes after comments and input from MS	Eric Vetillard
30/04/2024	0.6	Cleanup, removal of some discussion items and internal comments	Eric Vetillard
22/05/2024	0.7	Minor editorial changes, further removal of comments, renumbering of requirements in text and annex	Joran Frik

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act ,the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services, and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use certification@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Eric Vetillard, ENISA

ACKNOWLEDGEMENTS

TBD

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

Cover image © xxx, shutterstock.com

ISBN SHOULD BE PLACED HERE, DOI SHOULD BE PLACED HERE (IF APPLICABLE)

TABLE OF CONTENTS

1. LEGAL REQUIREMENTS 9

1.1 CERTIFICATION REQUIREMENT 9

1.2 CERTIFICATION SCOPE 12

1.2.1 Main articles 12
1.2.2 Other articles 21

2. SCHEME REQUIREMENTS 26

2.1 WHAT IS AN EUDI WALLET? 26

2.2 WHAT IS THE OBJECT OF CERTIFICATION? 26

2.3 HOW TO ORGANIZE CERTIFICATION? 28

2.4 CONTENT OF A SCHEME 29

2.5 CONTENT OF THE CERTIFICATION IMPLEMENTING ACT 30

3. GENERAL SCHEME CONTENT 31

3.1 SCOPE 31

3.2 PRODUCT REQUIREMENTS 32

3.2.1 Functional requirements 32
3.2.2 Security requirements 32

3.3 SELECTION OF ACTIVITIES 33

3.4 OTHER REQUIREMENTS TO BE MET BY THE CLIENT 34

3.5 REQUIREMENTS FOR CONFORMITY ASSESSMENT BODIES 34

3.6 ACCREDITATION 35

3.7 METHODS AND PROCEDURES 35

3.8 INFORMATION TO BE SUPPLIED BY APPLICANTS 35

3.9 CONTENT OF CERTIFICATE 36

3.10 CERTIFICATE USE 36

3.11 MARKS OF CONFORMITY 36

3.12 RESOURCES 37

3.13 FROM EVALUATION TO CERTIFICATION 37

3.14 NONCONFORMITIES 37

3.15 SURVEILLANCE 37

3.16 ACCESS CRITERIA 39

3.17 DIRECTORY OF CERTIFIED PRODUCTS 39

3.18 CONTRACTS 39

3.19 CERTIFICATE MAINTENANCE 39

3.20 COMPLAINTS 40

3.21 REFERENCES TO THE SCHEME 41

3.22 RETENTION OF RECORDS 41

3.23 VULNERABILITY MANAGEMENT 41

3.24 MUTUAL RECOGNITION 42

3.25 PEER ASSESSMENT 42

3.26 DOCUMENTATION FORMAT 42

3.27 NCCA INVOLVEMENT 43

4. OTHER SCHEME CONTENT 45

4.1 OVERVIEW 45

4.2 SAMPLING 45

4.3 ACCEPTANCE OF CONFORMITY ASSESSMENT RESULTS 45

4.4 OUTSOURCING OF THE CONFORMITY ASSESSMENT ACTIVITIES 46

4.5 COMPLAINTS AND APPEALS TO THE SCHEME OWNER 46

4.6 LICENSING AND CONTROL OF THE MARK 47

4.7 SURVEILLANCE 47

4.8 NON-CONFORMING PRODUCTS 47

4.9 REPORTING TO THE SCHEME OWNER 49

4.10 SUBCONTRACTING OF THE OPERATION OF THE SCHEME 49

4.11 MARKETING 49

4.12 FRAUDULENT CLAIM OF CERTIFICATION 49

4.13 REVIEW OF SCHEME OPERATION 49

4.14 CHANGES IN SPECIFIED REQUIREMENTS 50

4.15 OTHER CHANGES TO THE SCHEME 51

5. ARCHITECTURE-SPECIFIC SCHEMES 52

REFERENCES 53

A METHODS AND PROCEDURES 55

INTRODUCTION 55

SELECTION FUNCTION AND PRELIMINARY AUDIT 55

Information required 56
Architecture and risk analysis 56

DETERMINATION ACTIVITIES 57

Determination activities (product-oriented) 58
Evaluation of the WSCA 58
Evaluation of EUDI Wallets Applications 59
Assessment of the assumptions on platforms 60

DETERMINATION ACTIVITIES (PROCESS-ORIENTED) 61

Development-related processes 61
Identity lifecycle-related processes 61

B DEPENDENCY ANALYSIS 62

ASSESSING THE AVAILABILITY OF ASSURANCE DOCUMENTATION 62

ASSESSING ASSURANCE RELATED TO INDIVIDUAL REQUIREMENTS 63

CERTIFIED SUBSERVICES 63

C ACCEPTANCE CRITERIA FOR ASSURANCE INFORMATION 64

D SURVEILLANCE AND COMPLIANCE MONITORING 65

CERTIFICATION LIFECYCLE 65

EUDI Wallet versioning 65
Versioning and certificates 65
Certification schedule 66

SURVEILLANCE ACTIVITIES 67

E RECAP OF REQUIREMENTS 70

EXECUTIVE SUMMARY

TO BE FINALIZED LATER.

The present document introduces some recommendations and requirements related to the certification of EUDI Wallets implementations in the short term, *i.e.*, before the adoption of a European Cybersecurity Certification Scheme.

The document defines a general certification approach, and provides some details about the evaluation activities to be performed, and the evidence that may be accepted.

A. LEGAL REQUIREMENTS

1.1 CERTIFICATION REQUIREMENT

The main article is Article 5c – Certification of the European Digital Identity Wallets

The need for certification is established in the new eIDAS regulation, in article 5c.

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.
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[1] of the European Parliament and of the Council and referred to in the implementing acts referred to in paragraph 6 of this Article.
3. For requirements referred to in paragraph 1 of this Article that are not relevant for cybersecurity, and, for requirements referred to in paragraph 1 of this Article that are relevant for cybersecurity, to the extent that cybersecurity certification schemes as referred to in paragraph 2 of this Article do not, or only partially, cover those cybersecurity requirements, also for those requirements, Member States shall establish national certification schemes following the requirements set out in the implementing acts referred to in paragraph 6 of this Article. Member States shall transmit their draft national certification schemes to the European Digital Identity Cooperation Group established pursuant to Article 46e(1) (the 'Cooperation Group'). The Cooperation Group may issue opinions and recommendations.
4. Certification pursuant to paragraph 1 shall be valid for up to five years, provided that a vulnerability assessment is carried out every two years. Where a vulnerability is identified and not remedied in a timely manner, certification shall be cancelled.
5. Compliance with the requirements set out in Article 5a of this Regulation related to the personal data processing operations may be certified pursuant to Regulation (EU) 2016/679.
6. By 6 months from the date of entry into force of this amending Regulation, the Commission shall, by means of implementing acts, establish a list of reference standards and where necessary, establish specifications and procedures for the certification of European Digital Identity Wallets referred to in paragraph 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).
7. Member States shall communicate to the Commission the names and addresses of the conformity assessment bodies referred to in paragraph 1. The Commission shall make that information available to all Member States.
8. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 establishing specific criteria to be met by the designated conformity assessment bodies referred to in paragraph 1 of this Article.

Paragraph 1 clearly establishes the obligation for the EUDI Wallets to be certified. The scope of this obligation is quite wide, including the scope of the normative documents, i.e. the

[1] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

requirements of the EUDI Wallets whose conformity must be certified (as defined in Article 5a(4), 5a(5), 5a(8) and 5a(14)), requiring the application of standards where available/relevant and technical specifications where necessary (as established in implementing acts adopted pursuant to Article 5a(24)).

Paragraph 3 defines an optional certification according to GDPR, to be performed using a GDPR scheme. This will be out of scope of the present document.

Paragraph 2 mandates the use of EU cybersecurity certification schemes when available and applicable, and is referenced in Article 5c(6) implementing act, which is likely to be limited to EUCC by the time of adoption of the implementing act (other schemes may be referenced in later revisions of the Implement Act). Paragraph 3 complements this by mandating the use of national schemes for non-cybersecurity requirements, and for those cybersecurity requirements that are not covered by EU Cybersecurity Act (CSA) schemes or when those schemes are not available. The wording indicates that the EU schemes shall be given priority when they cover the cybersecurity requirements of EUDI Wallets.

NOTE: *Applicable means that all conditions for applying the scheme are met. For instance, CABs are available (for instance, EUCC is presently available, but not applicable). It may remain not applicable in some Member States when a CB does not reach level 'high' for instance. Also, for level 'high', the availability of a PID Provider may be required (for instance for the WSCA).*

Cert-1	*General*	Member States **shall** establish national certification schemes that cover both the cybersecurity and non-cybersecurity aspects as specified in Article 5c(3).
Cert-2	*General*	Member States **shall** consider the use of available and applicable EU cybersecurity certification schemes in their national schemes for the requirements that can be covered with these schemes.

Paragraph 4 indicates an additional constraint, mandating a vulnerability assessment every two years, which could be an issue in some cases. In particular, applying this vulnerability assessment to components that are integrated on a device that is already on the market may be difficult, will be very costly, and may lead to additional changes.

Cert-3	*Process*	The certificates of conformity EUDI Wallets with the requirements of the Regulation, issued under these national schemes **shall** have a validity that does not exceed 5 years.
Cert-4	*Process*	The (national) certification schemes that cover cybersecurity requirements **shall** require performance of a vulnerability assessment activity at least every two years.
Cert-5	*Process*	The national certification scheme **shall** require EUDI Wallet services to define and implement a process to evaluate the severity and potential impact of a vulnerability, and to design and implement a remediation plan in a timely manner.

Cert-6	*Process*	The national certification schemes **shall** require cancellation of certificates if an identified vulnerability has not been remedied commensurately to its severity and potential impact in a timely manner.

Note*: The vulnerability assessment requirement may be costly or difficult, so it would be expected to re-certify EUDI Wallets under Member State's national schemes after an even number of years (i.e. 2 or 4 years), to synchronise these assessments with recertification assessments. The maximum validity can remain five years, which leaves room to address issues that may arise in a re-certification assessment.*

Note*: The required cancelation of certificates has been linked to the severity and potential impact of a vulnerability, so the wording in the scheme is slightly less demanding as in the Regulation.*

Finally, paragraph 7 mandates Member States to notify the name and address of designated Conformity Assessment Bodies (CABs) to the Commission.

This article is completed by the definition of a CAB in Article 3(18):

> (18) 'conformity assessment body' means a conformity assessment body as defined in Article 2, point 13, of Regulation (EC) No 765/2008[2], which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides, or as competent to carry out certification of European Digital Identity Wallets or electronic identification means;

This definition establishes a requirement for accreditation. Since certification is required, the harmonised standard is EN ISO/IEC 17065[3].

Cert-7	*Process*	Conformity assessment bodies issuing certificates for the EUDI Wallets **shall** be conformity assessment body as defined in point 13 of Article 2, point 13, of Regulation (EC) No 765/2008, which is accredited to EN ISO/IEC 17065 in accordance with that Regulation as competent to carry out certification of an EUDI Wallet.
Cert-8	*Process*	The national certification schemes **should** define the parameters required to perform the accreditation of CBs, and in particular, the competence requirements and an evaluation process.

Note*: The explicit references to EN ISO/IEC 17065, the harmonised standard for certification bodies, indicates that the requirements defined in the present document apply primarily to certification bodies (CBs). A CB may subcontract other conformity assessment activities, but they remain ultimately responsible for all activities that led to the certification decision. National schemes are free to define roles for these subcontractors and accredit separately as CABs, but this is not mandatory and not covered in the present document. The term CB (Certification*

[2] REGULATION (EC) NO 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance).

[3] EN ISO/IEC 17065. Conformity assessment — Requirements for bodies certifying products, processes and services (ISO/IEC 17065:2012), ISO/IEC, September 2012.

Body) will therefore be preferred over CAB (Conformity Assessment Body) in the present document.

***Note**. The present document does not directly define requirements for CBs, in the implementing act. Nevertheless, the EN ISO/IEC 17065 standard includes many references like "as defined in the scheme", which need to be actually defined in the scheme, so many requirements of the scheme actually directly impact and are implemented by the CBs.*

1.2 CERTIFICATION SCOPE

1.2.1 Main articles

The scope of certification is defined in articles 5a(4), (5) and (8), also referring to Article 5a(14) for logical separation and to Article 5a(24) for the specifications to be applied.

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;
   (b) generate pseudonyms and store them encrypted and locally within the European Digital Identity Wallet;
   (c) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;
   (d) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard enabling the user to:

      (i) view an up-to-date list of relying parties with which the user has established a connection and, where applicable, all data exchanged;
      (ii) easily request the erasure by a relying party of personal data pursuant to Article 17 of the Regulation (EU) 2016/679;
      (iii) easily report a relying party to the competent national data protection authority, where an allegedly unlawful or suspicious request for data is received;

   (e) sign by means of qualified electronic signatures or seal by means of qualified electronic seals;
   (f) download, to the extent technically feasible, the user's data, electronic attestation of attributes and configurations;
   (g) exercise the user's rights to data portability.

The above legal requirements on the EUDI Wallets can be identified, decomposed and expressed from the verbs used in the paragraph (in red), the items to which the verb applies (in blue), the qualifiers of the verb (in orange), and in a few cases, a destination of the verb (in purple). This leads to a large number of legal requirements.

These requirements should be further defined in reference standards and technical specifications and procedures, all established by means of the Art.5a(23) implementing acts. Those requirements shall be the normative documents grouping all requirements against which the conformity of the EUDI Wallets shall be evaluated and certified by an accredited CB following a certification scheme. This certification scheme will need to map all legal requirements to the corresponding technical requirements and to refer to these technical requirements. The legal/technical requirements may encompass process, functional and cross-functional requirements (mostly security requirements, but possibly interoperability or other requirements).

In most cases, the schemes will refer to requirements defined in normative documents (standards or technical specifications). But if a legal requirement is not covered by defined technical requirements (in the normative documents), it will need to be covered by technical requirements defined in the certification scheme itself.

In the absence of technical requirements corresponding to the legal requirements (e.g. the implementing act is not yet available, the technical requirements are not defined yet in preparation of the implementing act), this should be identified and reported to the Toolbox/ARF drafting for completion of the technical specifications and input to Art.5a(23) drafting. Furthermore, the certification scheme should be required to define appropriate process, functional, and cross-functional requirements against which to evaluate the conformity of EUDI Wallets with the legal requirements.

***Note**: The functional and process requirements that need to be referred to in the scheme are listed in Annex F, and they are associated with ongoing Epics when available.*

The requirements presented below are therefore the consequence of combining the certification requirements defined in Article 5c with the requirements referred to in the paragraphs of Article 5a that are pointed to by Article 5c(1). We translated these into single atomic requirements of what the certification schemes shall cover. While this gives an extensive number of scheme requirements, it is meant as a closed list of what certification mandatorily covers according to the Regulation.

From subparagraph (a), the requirements on the national certification scheme are:

Cert-9	*Functional*	The national certification scheme **shall** refer to functional requirements on the request operation on PID and EAA.
Cert-10	*Functional*	The national certification scheme **shall** define functional requirements on the obtain operation on PID and EAA.
Cert-11	*Functional*	The national certification scheme **shall** refer to functional requirements on the select operation on PID and EAA.
Cert-12	*Functional*	The national certification scheme **shall** refer to functional requirements on the combine operation on PID and EAA.
Cert-13	*Functional*	The national certification scheme **shall** refer to functional requirements on the store operation on PID and EAA.
Cert-14	*Functional*	The national certification scheme **shall** refer to functional requirements on the delete operation on PID and EAA.
Cert-15	*Functional*	The national certification scheme **shall** refer to functional requirements on the share operation on PID and EAA.

Cert-16	*Functional*	The national certification scheme **shall** refer to functional requirements on the present operation on PID and EAA.
Cert-17	*Functional*	The national certification scheme **shall** refer to functional requirements on the online and offline authentication from an EUDI Wallet to relying parties based on PID and EAA.
Cert-18	*Functional*	The national certification scheme **shall** refer to functional requirements on the selective disclosure of PID and EAA during their processing.

***Note**: We can assume that the use of "securely" at the beginning for the basic operations also extends to the authentication. Similarly, the selective disclosure applies to all.*

***Note**: The scheme needs to cover both offline and online authentication, since it needs to cover all applicable requirements.*

***Note**: The requirements on national certification schemes stop short of suggesting how the scheme needs to implement this requirement. A scheme may in particular be tailored to a Member State's architectural choices, which may be reflected in the way in which the requirements defined here are implemented in the scheme. For instance, if a Member State uses different solutions for online and offline authentication, the scheme may explicitly refer to these distinct solutions.*

For subparagraph (b), we have:

Cert-19	*Functional*	The national certification scheme **shall** refer to functional requirements about the generation of pseudonyms.
Cert-20	*Functional*	The national certification scheme **shall** refer to functional requirements about the encryption and storage of pseudonyms within EUDI Wallets.

***Note**: There is no mention of security in this requirement, but pseudonyms can be considered as security functions, for which the security aspect always needs to be addressed.*

From subparagraph (c), we have:

Cert-21	*Functional*	The national certification scheme **shall** refer to functional requirements about the authentication of another EUDI Wallet.
Cert-22	*Functional*	The national certification scheme **shall** refer to functional requirements about the authentication to another EUDI Wallet.
Cert-23	*Functional*	The national certification scheme **shall** refer to functional requirements about receiving and sharing of PID and EAA between two EUDI Wallets.

***Note**: The paragraph does not explicitly mention the authentication of an EUDI Wallet to another EUDI Wallet, but it is implicit and needs to be covered.*

From subparagraph (d), we have:

Cert-24	*Functional*	The national certification scheme **shall** refer to functional requirements about a log of all transactions carried out through an EUDI Wallet.
Cert-25	*Functional*	The national certification scheme **shall** refer to functional requirements about a common dashboard to access the log of transactions carried out through an EUDI Wallet.
Cert-26	*Functional*	The national certification scheme **shall** refer to functional requirements about viewing an up-to-date list of relying parties with whom the user has established a connection through an EUDI Wallet.
Cert-27	*Functional*	The national certification scheme **shall** refer to functional requirements about viewing all data exchanged with relying parties with whom the user has established a connection through an EUDI Wallet.
Cert-28	*Functional*	The national certification scheme **shall** refer to functional requirements about requesting the deletion of data to a relying party.
Cert-29	*Functional*	The national certification scheme **shall** refer to functional requirements about the ease of requesting the deletion of data to a relying party.
Cert-30	*Functional*	The national certification scheme **shall** refer to functional requirements about reporting a relying party to a national data protection authority where an allegedly unlawful or suspicious request of data is received from that relying party.
Cert-31	*Functional*	The national certification scheme **shall** refer to functional requirements about the ease of reporting a relying party to a national data protection authority where an allegedly unlawful or suspicious request of data is received from that relying party.

***Caution**: The use of absolute terms like "all" and "up to date" requires appropriate definitions in order to better qualify their meaning. For instance, it is important to understand whether the loss of a device may affect the availability of logs.*

***Caution**: The nature and location of the log and dashboard need to be defined, as the paragraph does not specify how the logs are supposed to be maintained and consolidated in a dashboard. We may assume that the log is local, but it is not explicit, and has consequences on its ability to include "all" transactions.*

From subparagraph (e), we have:

Cert-32	*Functional*	The national certification scheme **shall** refer to functional requirements about signing by means of qualified electronic signatures.

Cert-33	*Functional*	The national certification scheme **shall** refer to functional requirements about sealing by means of qualified electronic seals.

Note*: The paragraph does not define the relationship between the qualification of the electronic signature or seal and its integration into the EUDI Wallet. We here assume that the qualification of the electronic signature or seal is* ***not*** *in scope of the EUDI Wallets certification, so the role of the EUDI Wallets' CB will only be to ensure that a valid qualification for electronic signature and seals is available.*

Note: *The fact that that signing (resp. sealing) occurs with qualified electronic signatures (resp. seals) does not necessarily means that there will not be any requirement related to signing or sealing defined on the EUDI Wallets. However, the EUDI Wallet certification will be able to leverage the assurance information available on qualified electronic signatures and seals.*

From paragraph (f), we have:

Cert-34	*Functional*	The national certification scheme **shall** refer to functional requirements about downloading users' data, EAA and configurations.

From paragraph (g), we have:

Cert-35	*Functional*	The national certification scheme **shall** refer to functional requirements about exercising a user's right to data portability.

Note: *The scope of data portability needs to be understood in the same context as defined in GDPR.*

Paragraph 5 adds a variety of requirements:

> 5. European Digital Identity Wallets shall, in particular:
>
> (a) support common protocols and interfaces:
>
> (i) for issuance of person identification data, qualified and non-qualified electronic attestations of attributes or qualified and non-qualified certificates to the European Digital Identity Wallet;
>
> (ii) for relying parties to request and validate person identification data and electronic attestations of attributes;
>
> (iii) for the sharing and presentation to relying parties of person identification data, electronic attestation of attributes or of selectively disclosed related data online and, where appropriate, in offline mode;
>
> (iv) for the user to allow interaction with the European Digital Identity Wallet and display an EU Digital Identity Wallet Trust Mark;
>
> (v) to securely onboard the user by using an electronic identification means in accordance with Article 5a(24);

(vi) for interaction between two persons' European Digital Identity Wallets for the purpose of receiving, validating and sharing person identification data and electronic attestations of attributes in a secure manner;
(vii) for authenticating and identifying relying parties by implementing authentication mechanisms in accordance with Article 5b;
(viii) for relying parties to verify the authenticity and validity of European Digital Identity Wallets;
(ix) for requesting a relying party the erasure of personal data pursuant to Article 17 of Regulation (EU) 2016/679);
(x) for reporting a relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for data is received;
(xi) for the creation of qualified electronic signatures or seals by means of qualified signature or seal creation devices;

(b) not provide any information to trust service providers of electronic attestations of attributes about the use of those electronic attestations;
(c) ensure that the relying parties can be authenticated and identified by implementing authentication mechanisms in accordance with Article 5b;
(d) meet the requirements set out in Article 8 with regards to assurance level high, in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication;
(e) in the case of the electronic attestation of attributes with embedded disclosure policies, implement the appropriate mechanism to inform the user that the relying party or the user of the European Digital Identity Wallet requesting that electronic attestation of attributes has the permission to access such attestation;
(f) ensure that the person identification data, which is available from the electronic identification scheme under which the European Digital Identity Wallet is provided, uniquely represents the natural person, legal person or the natural person representing the natural or legal person, and is associated with that European Digital Identity Wallet;
(g) offer all natural persons the ability to sign by means of qualified electronic signatures by default and free of charge.

Notwithstanding point (g) of the first subparagraph, Member States may provide for proportionate measures to ensure that the use of qualified electronic signatures free-of-charge by natural persons is limited to non-professional purposes.

For subparagraph (a), the requirements are not detailed, since there is an implicit reference to standards or technical specifications ("common protocols and interfaces"), so the requirement is simple:

Cert-36	*Functional*	The national certification scheme **shall** refer to functional requirements about conformity to those common protocols and interfaces defined in the reference standards, technical specifications and procedures established by means of the implementing acts adopted pursuant to Art.5a(24).

***Note**: There is an open question about the security aspects. An integration of complex solutions, will be considered that includes both security and privacy risks against which national certification schemes need to be compared to. Eventually, these security and privacy risks will be transformed into cross-functional requirements in the final CSA EUDI Wallets certification scheme.*

Caution*: It is very important that the technical specifications are precise enough for certification. To take a simple example, the EUDI Wallet Trust Mark needs by definition to be "verifiable, simple and recognisable". The "verifiable" aspect needs to be addressed in a way that satisfies certification requirements at the desired assurance level ('high' by default), which is not an easy task.*

From subparagraph (b), we have:

Cert-37	*Functional*	The national certification scheme **shall** refer to functional requirements about not providing any information to trust service providers of EAA about the use of these attributes.

From subparagraph (c), we have:

Cert-38	*Functional*	The national certification scheme **shall** refer to functional requirements about the validation of the identity of relying parties using a <u>common mechanism</u> for the identification and authentication of relying parties.

Note*: The reference to Article 5b is annoying, since this article is normally out of scope, but the reference is acknowledged in Article 5b(2), which also refers to a common mechanism. The content of Article 5b(2) has been underlined in this requirement.*

From subparagraph (d), we have a reference to Article 8 and the definition of assurance level 'high', and this article refers to implementing acts, so the requirements are complex.

The implementing act (EU) 2015/1502[4] defines the requirements for all assurance levels, including assurance level 'high'. The requirements cover different aspects of eID means and of the eID scheme used to issue them, but the requirements are defined independently for each aspect.

Note*: We need to map the security requirements identified for the national schemes to the requirements of (EU) 2015/1502, and to consider how much of this should be covered by the implementing act beyond the reference to (EU) 2015/1502.*

From subparagraph (e), the requirement seems insufficient, since it only requires information when an access can be granted, without requirements on the check or on the actions if the access is denied: We have:

Cert-39	*Functional*	The national certification scheme **shall** refer to functional requirements about the mechanisms used to inform a party that they have the permission to access an EAA.

[4] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

***Note**: This is most likely incomplete, as it would seem from a cybersecurity viewpoint that the most important aspect is to ensure that access is only granted when it should. We expect the technical specifications to fill this gap.*

Paragraph (f) introduces a link between the EUDI Wallet and the underlying electronic identification scheme:

Cert-40	*Functional*	The national certification scheme **shall** refer to functional requirements about how the eID scheme under which the EUDIW is provided ensures that the PID available from the electronic identification scheme, under which the EUDI Wallet is provided, uniquely represents the user of the EUDI Wallet.

***Note**: This requirement is not exactly equivalent to the subparagraph, so it needs to be checked thoroughly, as it may be missing some aspects.*

Certification can only assess conformity to part of the requirement in paragraph (g), since it may be hard to know whether or not a service is offered free of charge:

Cert-41	*Functional*	The national certification scheme **shall** refer to functional requirements about the availability of signature by means of qualified electronic signatures to all natural persons by default.
Cert-42	*Functional*	The national certification scheme **shall** refer to functional requirements about the availability of signature by means of qualified electronic signatures to all natural persons free-of-charge.

Article 5a(8) defines validation mechanisms:

> 8. Member States shall provide validation mechanisms free-of-charge, in order to:
>
> (a) ensure that the authenticity and validity of European Digital Identity Wallets can be verified;
>
> (b) allow users to verify the authenticity and validity of the identity of relying parties registered in accordance with Article 5b.

There is a potential issue in these requirements, which stem from the fact that the responsibility for providing the validation mechanism lies with the Member States, and not with the EUDI Wallet providers.

***Caution**: The requirements below are provided as reference, but with the current wording of the regulation, they can probably not be included in the certification scheme for EUDI Wallets, since they are not obligations of the provider of the object of certification. A separate scheme (or sub-scheme), applying specifically to these validation mechanisms, will need to be defined.*

Cert-43	*Functional*	The national certification scheme **shall** refer to functional requirements about the effective provision by Member States of mechanisms for the verification of the authenticity and validity of an EUDI Wallet.

Cert-44	*Functional*	The national certification scheme **shall** refer to functional requirements about the effective provision by Member States of mechanisms for the verification of the authenticity and validity of an EUDI Wallet free-of-charge.

***Caution**: The definitions of the authenticity and validity of EUDI Wallets need to be defined precisely in order to avoid potential discussions on the extent of the checks to be performed.*

Cert-45	*Functional*	The national certification scheme **shall** refer to functional requirements about the effective provision by Member States of mechanisms for the verification of the authenticity and validity of the identity of registered relying parties.
Cert-46	*Functional*	The national certification scheme **shall** refer to functional requirements about the effective provision by Member States of mechanisms for the verification of the authenticity and validity of the identity of registered relying parties free-of-charge.

***Caution**: Like the other requirements, the EUDI Wallet provider is **not** responsible for the mechanisms to be assessed, so these requirements cannot be covered by the certificate of an EUDI Wallet. A distinct certificate will need to be issued, to the entity within the Member State in charge of providing these mechanisms.*

Paragraph 14 defines among other things a separation principle between data related to the EUDI Wallets and other data held by its provider, which is in scope for certification:

> 14. Users shall have full control of the use and of the data in their European Digital Identity Wallet. The provider of the European Digital Identity Wallet shall neither collect information about the use of the European Digital Identity Wallet which is not necessary for the provision of the European Digital Identity Wallet services, nor combine person identification data or any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by that provider or from third-party services which are not necessary for the provision of European Digital Identity Wallet services, unless the user has expressly requested otherwise. Personal data relating to the provision of the European Digital Identity Wallet shall be kept logically separate from any other data held by the provider of the European Digital Identity Wallet. If the European Digital Identity Wallet is provided by private parties in accordance with paragraph 2, points (b) and (c), of this Article, the provisions of Article 45h(3) shall apply mutatis mutandis.

Cert-47	*Functional*	The national certification scheme **shall** refer to functional requirements on the logical separation between personal data relating to the provision of an EUDI Wallet and any other data held by the EUDI Wallet provider.

Paragraphs 23 and 24 define what the Commission needs to define in implementing acts:

> 23. By … [6 months from the date of the entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards

and, where necessary, establish specifications and procedures for the requirements referred to in paragraphs 4, 5, 8 and 18 of this Article on the implementation of the European Digital Identity Wallet. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

24. The Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish technical specifications and procedures in order to facilitate the onboarding of users to the European Digital Identity Wallet either by electronic identification means conforming to assurance level 'high' or by electronic identification means conforming to assurance level 'substantial' in conjunction with additional remote on-boarding procedures that together meet the requirements of assurance level 'high'. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Note*: We do not need to make this into a requirement. Obeying to implementing acts should be obvious, and we have no information about their content at this stage that would help us to define more precise requirements.*

Caution*: There is no mention of Article (5a)23 in Article 5c(1), but only to 5a(24), which could have some consequences.*

1.2.2 Other articles

Many paragraphs have been added around the paragraphs of Article 5a, which may be somewhat relevant to certification, and some other paragraphs of this Article are also relevant.

Two paragraphs have been added between paragraphs 5 and 8. Although they do not define requirements and are not mentioned in Article 5c, their content may have some impact on certification:

6. Member State shall inform users, without delay, of any security breach that could have entirely or partially compromised their European Digital Identity Wallet or its content, in particular if their European Digital Identity Wallet has been suspended or revoked pursuant to Article 5e.
7. Without prejudice to Article 5f, Member States may provide, in accordance with national law, for additional functionalities of European Digital Identity Wallets, including interoperability with existing national electronic identification means. Those additional functionalities shall comply this Article.

Note*: Paragraph 6 is about the security breach of EUDI Wallets. This is not directly related to certification, but serious security breaches, if they are not corrected, should also lead to the revocation of the associated certificate.*

Note*: Paragraph 7 is about cross-border reliance on EUDI Wallets, so the present paragraph reaffirms that the European nature of EUDI Wallets should take precedence over the national aspects.*

These articles are not in scope of the certification, but the obligations of paragraph 6 are at least partly supported by corresponding measures in the scheme about non-conforming products (see '4.8 Non-conforming products').

Two paragraphs have also been added as paragraphs 9 and 10:

9. Member States shall ensure that the validity of the European Digital Identity Wallet can be revoked in the following circumstances:

(a) upon the explicit request of the user;
(b) when the security of the European Digital Identity Wallet has been compromised;
(c) upon the death of the user or cease of activity of the legal person.

10. Providers of European Digital Identity Wallets shall ensure that users can easily request technical support and report technical problems or any other incidents having a negative impact on the use of services of European Digital Identity Wallets.

Paragraph 11 is very relevant as well, as it sets one of the most significant constraints.

11. European Digital Identity Wallets shall be provided under an electronic identification scheme with assurance level high.

***Note**: This paragraph raises the point of the relationship between EUDI Wallets and the electronic identification scheme under which it is provided. The sentence leaves no doubt that the EUDI Wallet and the eID scheme are distinct, but it is not explicit about their relationship. This is discussed in the following chapter.*

Paragraph 12 could also be considered as a basis for security certification:

12. European Digital Identity Wallets shall ensure security-by-design.

***Note**: This is now a CRA requirement, so this may become relevant. However, the scheme is about a service, not a product, so this requirement is not an obligation at this stage.*

Paragraph 13 is not relevant for certification:

13. European Digital Identity Wallets shall be issued, used and revoked free of charge to all natural persons.

Paragraphs 15 to 19 are not relevant to certification. However, paragraph 16 is likely to have an influence on the EUDI Wallets' normative documents, and it could be covered through this means. In addition, although this Paragraph is related to personal data management, it is strongly linked to access control and could benefit from being in scope of EUDI Wallets certification.

Paragraph 20 refers to an article that defines requirements to be applied to EUDI Wallets and its associated eID scheme. These requirements are highly relevant for the security of EUDI Wallets, but they are not included in the scope of certification:

20. Article 24(2), points (b), and (d) to (h) shall apply mutatis mutandis to the providers of European Digital Identity Wallets.

The mentioned paragraphs of Article 24 (*mutatis mutandis*) are as follows (with the changes to apply it to EUDI Wallets):

2. A [provider of EUDI Wallets] shall:
(b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;
(d) before entering into a contractual relationship, inform, in a clear, comprehensive and easily accessible manner, in a publicly accessible space and individually any person

seeking to use [an EUDI Wallet] of the precise terms and conditions regarding the use of that [EUDI Wallet], including any limitations on its use;

e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them, including using suitable cryptographic techniques;

(f) use trustworthy systems to store data provided to it, in a verifiable form so that:

(i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,

(ii) only authorised persons can make entries and changes to the stored data,

(iii) the data can be checked for authenticity;

(fa) notwithstanding Article 21 of Directive (EU) 2022/2555, have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the [EUDI Wallet], including at least measures related to the following:

(i) registration and on-boarding procedures for a [Wallet];

(ii) procedural or administrative checks;

(iii) the management and implementation of [EUDI Wallets];

(fb) notify the supervisory body, the identifiable affected individuals, other relevant competent bodies where applicable and, at the request of the supervisory body, the public if it is of public interest, of any security breaches or disruptions in the provision of the service or the implementation of the measures referred to in point (fa), (i), (ii) or (iii) that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any event within 24 hours of the incident.

(g) take appropriate measures against forgery, theft or misappropriation of data or, without right, deleting, altering or rendering data inaccessible;

(h) record and keep accessible for as long as necessary after the activities of the [provider of a certified EUDI Wallet] have ceased, all relevant information concerning data issued and received by the [provider of a certified EUDI Wallet], for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;

All these requirements apply to the EUDI Wallet provider, and they are not in the scope of EUDI Wallets certification. On the other hand, non-compliance to these requirements will make it impossible in most cases to comply to the certification requirements to EUDI Wallets.

Because of this strong dependency, and because EUDI Wallets certification is likely to be the most suitable framework in which to verify conformity to these requirements, and because other aspects of EUDI Wallets certification will need to rely on these requirements being verified, the proposal is to include some of these requirements in scope of certification.

However, another issue is here that there aren’t any implementing acts being developed to cover these issues, which means that they need to be addressed by referring to other standards, like EN ISO/IEC 27001[5] or CEN/TS 18026[6].

For point (b), the requirement would be as follows:

Cert-48	*Process*	The national certification scheme **shall** refer to requirements about human resource management policies and procedures, including at least requirements

[5] EN ISO/IEC 27001. Information security, cybersecurity and privacy protection (ISO/IEC 27001:2022), ISO/IEC, October 2022.

[6] CEN-CENELEC EN 18026. Three-level approach for a set of cybersecurity requirements for cloud services (CEN-CENELEC EN 18026:2024), CEN/CENELEC, November 2023.

		on expertise, reliability, experience, and qualifications of personnel about .appropriate training regarding security rules, and appropriate management procedures.

Point (d) is actually a functional requirement about the information of uses:

Cert-49	*Functional*	The national certification scheme **shall** refer to requirements about the information made available to any person seeking to use an EUDI Wallet of the precise terms and conditions regarding the use of that service, including any limitations on its use, and about the availability of this information in a clear, comprehensive and easily accessible manner, in a publicly accessible space.

Point (e) is about the security of the systems used. Point (f) focusses on the storage of data, mentioning access control and authenticity options, which complements point (e).

***Note**: These paragraphs are highly relevant for the security of EUDI Wallets, but are not in scope of this document.*

Point (fa) focus on the management of risks related to the operation of EUDI Wallets' services.

Cert-50	*Process*	The national certification scheme **shall** refer to requirements about the definition and implementation of policies and procedures related to the management of risks related to the operation of an EUDI Wallet, including the identification and assessment of risks and the treatment of the identified risks.

About point (fb)**,** the CB which issued the certificate needs to be considered as one of the "other relevant competent bodies" in paragraph (fb), as expressed in the requirement below.

Cert-51	*Process*	The national certification scheme **shall** require notification to the CB of security breaches and disruptions within 24 hours of the incident.

***Note**: This specific requirement is needed even if we don't consider the inclusion of the other requirements in the scheme, since it concerns the consideration of the CB as a competent body.*

***Note**: This requirement only adds the CB to the list of "other relevant competent bodies" mentioned in point (fb), so it is expected that EUDI Wallet providers will have more notification obligations in case of security breaches or disruptions.*

Point (g) is also about classical security issues, which do not lead to a requirement, as they are expected to be covered by the risk registry (see next).

***Caution**: Point (g) covers availability, which is notoriously difficult to achieve at high levels of assurance, in particular in combination with authenticity. This point of the regulation has to be considered carefully to understand its relation to certification. It may be safer to ignore or weaken the requirement for certification.*

Finally, point (h) is about keeping records, with very strict provisions:

Cert-52	*Functional*	The national certification scheme **shall** refer to requirements about recording and keeping accessible for as long as necessary after the activities of the [provider of a certified EUDI Wallet] have ceased, all relevant information concerning data issued and received by the provider of a certified EUDI Wallet, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically.

B. SCHEME REQUIREMENTS

2.1 WHAT IS AN EUDI WALLET?

There are many different types of certifications. The EN ISO/IEC 17065 standard covers products, services and processes, and the Cybersecurity Act restricts this to ICT products, ICT processes and ICT services (and may soon support managed security services).

It is also possible to certify management systems, following EN ISO/IEC 17021-1[7], and other types of systems, like quality systems.

The scope of certification covers the “EUDI Wallets and the eID scheme under which they are provided” (Art.5c(1)).

The definition of an EUDI Wallet in the regulation is as follows in Article 3(42) and Article 3(2) respectively:

> (42) ‘European Digital Identity Wallet’ means an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals;
> (2) ‘electronic identification means’ means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service;

These definitions, in particular the eID means, clearly define a product.

The next aspect is the “electronic identification scheme under which it is provided”. An electronic identification is defined as follows:

> (4) electronic identification scheme’ means a system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons;

This definition points towards a management system or a service, focusing on the management of electronic identification means.

Overall, in the articles defining the requirements on EUDI Wallets and its eID scheme, the product-related and service/process-related requirements are very much mixed. In addition, the management of EUDI Wallets itself will require additional processes, for instance related to the management of updates and to the management of vulnerabilities.

2.2 WHAT IS THE OBJECT OF CERTIFICATION?

The next step in the definition of an EUDI Wallet is to determine the object of certification, together with its lifecycle and the lifecycle of the corresponding certificates.

[7] EN ISO/IEC 17021-1. Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements (ISO/IEC 17021-1: 2015), ISO/ IEC, July 2015.

The EUDI Wallet is necessarily a composite scheme, in the sense that all known architectures require several application parts running on different hardware platforms (even if these platforms are integrated in a single device). In addition, the scheme also needs to cover non-product aspects, which means that some of its components will be processes or services, maybe even management systems.

However, an EUDI Wallet (or at least a part of its components) is likely to exist in several versions, targeting different hardware platforms (mobile platforms, PC platforms, etc.). This raises two essential questions:

- **Are the different versions of an EUDI Wallet to be considered as independent EUDI Wallets, or as components of the same EUDI Wallet?**
  If each version is considered as an EUDI Wallet, this may lead to many certificates with a lot in common, but if not, the certificates may be extremely complex, and it may be very complex for stakeholders to follow maintenance and vulnerabilities.
  Also, this may not be a simple question, as intermediate solutions could be considered, where versions that are "close" (TBD) could be considered as a single product.
- **How are the updates to an EUDI Wallet (and its components) to be considered by the scheme?**
  As a composite product based on rapidly evolving platforms, EUDI Wallets are likely to be updated very regularly. The EUCC has defined the notion of patch management, which simplifies the management of updates with no/limited impact on security, but it remains a significant burden, with the issuance of a new certificate for each update, and a complex management of the cancelation of older versions (mandatory if the version fixes a vulnerability, but not mandatory if it is just a functional change, potentially leading to a large number of "active" versions).The EUCC approach is not practical, and we will need to consider alternative approaches, in which dedicated processes are used to manage the different versions of an EUDI Wallet.

The first question is more difficult to answer. However, since the scope of the scheme also needs to include a set of processes and services, it is easier to define a global scheme that covers all the requirements, which does not forbid the creation of sub-schemes to handle specific components of the object of certification, so all versions of the same EUDI Wallet are to be covered by a single certificate.

For the second question, the fact that processes related to the management of EUDI Wallets are already in scope, the easiest answer is to consider additional processes to manage versioning adequately, rather than issuing many certificates.

Overall, the proposal is to define the requirements for a scheme covering an entire EUDI Wallet solution. The easiest way to define that solution is as a service to be provided, including many subcomponents that may be products or processes.

Cert-53	*Process*	The national certification scheme **shall** define as object of certification a service that includes the provision and operation of EUDI Wallets.

Note*: This is about the "main" scheme, which will be a composite certification, relying on many other schemes (for instance, schemes for QSCDs). The objective is here to define the EUDI Wallet as a service in order to cover many different components, including processes.*

In addition, the scheme needs to include specific policies and procedures related to the maintenance of the certificates, and in particular related to vulnerability management and to the management of changes.

Cert-54	*Functional*	The national certification scheme **shall** require providers of certified EUDI Wallets to define and implement policies and procedures related to the management of changes.
Cert-55	*Functional*	The national certification scheme **shall** require providers of certified EUDI Wallets to define and implement policies and procedures related to the management of vulnerabilities.
Cert-56	*Process*	The national certification scheme **shall** include requirements for the providers of certified EUDI Wallets to notify the CB who issued the certificate about the vulnerabilities and changes affecting the service they provide, based on criteria about the impact of the vulnerabilities and changes.

***Note**: These two requirements are quite different. The first one is a "functional" requirement (i.e., a feature of the object of certification) about a process in place, and the second one is a requirement on the scheme itself to include requirements for notifying CBs on significant vulnerabilities and changes.*

2.3 HOW TO ORGANIZE CERTIFICATION?

The proposal is to write a single set of scheme requirements, for a scheme that would cover all the requirements on EUDI Wallets and on the associated eID scheme, including in particular the functional and process requirements, applied to both product and process components.

The objective is here to define for these overarching scheme requirements over a number of important aspects, as defined in EN ISO/IEC 17067[8], including but not limited to:

- Any information about the scheme itself (see below)
- References to other schemes whose certificates or statements of conformity can be recognized, and under which conditions.
- References to other type of evidence that can be recognized, and under which conditions.

The description also includes recommendations for organizing the conformity assessment activities, in particular by identifying different types of activities that may be assigned to specific conformity assessment bodies. This document stops short, however, of defining requirements for the organisation of the conformity assessment activities in each Member State.

Considering the terminology introduced in EN ISO/IEC 17000[9], this can be considered as defining a certification system that would be used as a basis for all the national certification schemes. In that case, in addition to the scheme owner for every national scheme, there is a system owner, which could be the European Commission. The present document does not

[8] EN ISO/IEC 17067. Conformity assessment – Fundamentals of product certification and guidelines for product certification schemes (ISO/IEC 17067:2013), ISO/IEC, August 2013.

[9] EN ISO/IEC 17000. Conformity assessment – Vocabulary and general principles (ISO/IEC 17000:2020), ISO/IEC , December 2020.

mandate the definition of an EU-wide certification system, but this could be considered in the future as a way to organise some activities like scheme surveillance, which will be difficult to organise at national level on a very limited number of CBs and certified products.

Cert-57	*Process*	The national certification scheme owner **shall** be clearly identified and in charge of supervising the operations of the scheme. It **may** be the Art.46a(1) national supervisory body responsible for the supervision of the provision of an EUDI Wallet and of the electronic identification scheme used to provide an EUDI Wallet.
Cert-58	*Process*	The national certification scheme **shall** be established and maintained in compliance with the implementing acts adopted pursuant to Art.5c(11).

In article 5c(3) we have:

> (1) … Member States shall transmit their draft national certification schemes to the European Digital Identity Cooperation Group established pursuant to Article 46e(1) (the 'Cooperation Group '). The Cooperation Group may issue opinions and recommendations.

Cert-59	*Process*	The national certification scheme **shall** require the scheme owner to be in contact with the representative designed by the Member States to the EDICG, and to take utmost account of the opinions and recommendations issued by the EDICG.

2.4 CONTENT OF A SCHEME

Although the scheme is defined as a scheme for services, there is an important product component into it, so the starting point is the recommended content from both ISO/IEC TR 17028[10]and EN ISO/IEC 17067[11], splitting this content into two main groups:

- **General content**
  Answers to the 22 questions in section 6.5.1 of EN ISO/IEC 17067 (complementing with the different wording of questions in ISO/IEC TR 17028)), ranging from scoping to retention of records, augmented by the additional questions included in the CSA for the definition of EU schemes.
- **Other topics**
  Remarks on the 11 additional sections of EN ISO/IEC 17067, ranging from sampling to fraudulent claim of certification, and on section 6.4 of ISO/IEC TR 17028.

These documents are only making recommendations (using 'should'), but the expectation by default is that all national schemes have to provide this content.

[10] EN ISO/IEC TR 17028. Conformity assessment – Guidelines and examples of a certification scheme for services (ISO/IEC TR 17028:2017), ISO/IEC, June 2017.

[11] ISO/IEC TR 17028 is dedicated to services, but its s only a technical report, and many of its elements are very similar to the elements in EN ISO/IEC 17067, which focuses on the certification of products and is a European standard.

Cert-60	*Process*	The national certification scheme **shall** include the content recommended in section 6.5 of EN ISO/IEC 17067, unless otherwise specified in the following requirements.

The present document will recall all of these recommendations in Chapters 3 and 4, and will then define additional constraints if required.

2.5 CONTENT OF THE CERTIFICATION IMPLEMENTING ACT

Article 5c(6) defines the content of the implementing act in a very abstract way:

> 6. By … [6 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the certification of European Digital Identity Wallets referred to in paragraph 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

The first part is a list of reference standards, which will be a small part, to be complemented by "specifications and procedures" when needed to bridge gaps. This is extremely wide, but we need to keep this distinction between specifications (requirements) and procedures (conformity assessment activities).

Specifications will be mostly defined in other Implementing Acts to be adopted in the same time frame, and a few significant procedures are defined in the Annexes to the present document and referred to in its requirements.

As mentioned before, the proposal follows the organisation of a certification scheme and identifies the constraints on the national schemes to be implemented.

Finally, some of the requirements on the scheme, like most of those identified in Chapter 1, will refer to requirements on EUDI Wallets itself. These requirements are mostly expected to be defined in other implementing acts, specifications and procedures, which will need to be referenced as well, as mentioned above.

C. GENERAL SCHEME CONTENT

Each section in the present chapter refers to an element required in ISO/IEC 17067, section 6.5. In addition, this section is dependent on the content of Article 5a requirements.

3.1 SCOPE

a) the scope of the scheme, including the type of products covered;

A proposal for the scope has been provided in Chapter 2, which should be used here. Additional requirements on the scope can be proposed, in order to clarify the content.

Cert-61	*Process*	The scope of the national certification scheme **shall** include the software components that implement the features of an EUDI Wallet.
Cert-62	*Process*	The scope of the national certification scheme **shall** include the hardware and platforms on which are running the software components that implement the features of an EUDI Wallet, if they are provided by the EUDI Wallet provider and if they are required to achieve the desired assurance level for that software component.
Cert-63	*Process*	The scope of the national certification scheme **shall** include the processes that support the provision of an EUDI Wallet, including the user on-boarding processes.

***Note**: This is a first attempt at defining constraints on the scope They are here minimal, but they may need to be complemented by additional ones.*

Regarding the type of product, since the regulation implies surveillance activities and since the certification is likely to rely on services and processes for which surveillance activities may be mandated, the scheme should be a Type 6 scheme (in the EN ISO/IEC 17067 definition), allowing a wide combination of surveillance activities (assessment of the production, the delivery of the process or the operation of the process, management system audits combined with random tests or inspections).

Cert-64	*Process*	The national certification scheme **shall** be defined as a Type 6 scheme, as defined in EN ISO/IEC 17067, 5.3.7.

***Note**: We could alternatively require a Type 5 scheme, which would allow two additional surveillance activities (testing or inspection of samples from the open market, testing and inspection of samples from the factory), which are not the most relevant in the context of EUDI Wallets.*

3.2 PRODUCT REQUIREMENTS

b) the requirements against which the products are evaluated, by reference to standards or other normative documents; where it is necessary to elaborate upon the requirements to remove ambiguity, the explanations should be formulated by competent people and should be made available to all interested parties;

Note: *Further guidance on how to formulate specified requirements is provided in ISO/IEC 17007*[12]*.*

The requirements are to be defined based on the analysis in Chapter 1, referring to Article 5a(4),(5),(8) and (14) of the Regulation which are further refined by the provisions laid down in Article 5a(23) implementing acts. We will need to distinguish between functional and security requirements, and the requirements may be applicable to a product component or to a process component.

3.2.1 Functional requirements

Functional product requirements are at least of two different natures:

- requirements related to the presence of a feature in the implementation, and
- requirements related to conformity of a feature or function to a standard or technical specification.

The first category can be handled easily through audit or inspection, based on the evaluator's judgement. The second category, related to interoperability, should be handled through testing, based on a defined procedure, relying on interoperability test suites.

Cert-65	*Process*	The national certification scheme **shall** mandate the use of standardized test suites for any referenced protocol or API for which a standardized test suite is available.

Note*: The implementing acts defining the protocols and APIs can be referenced, but this is likely to be insufficient. Such test suites will not be available at the time of adoption of the EUDI Wallets implementing act, so they cannot be referenced. The wording should be usable to mandate the use of test suites when they are released, without necessarily waiting for an update of the scheme.*

3.2.2 Security requirements

The security requirements are not yet defined, and there is no complete clarity on the extent of these requirements, as Article 5a does not systematically refer to security. Assumptions have been made that security requirements need to apply on all functions and features defined in Article 5a, since most data and functions are sensitive and require some security.

Note*: Currently, there are no detailed requirements. It is possible to leave their definition to the different schemes, but this would reduce the extent of harmonisation between them. On the other hand, defining these detailed requirements would require a significant amount of work.*

[12] EN ISO/IEC 17007. Conformity assessment — Guidance for drafting normative documents suitable for use for conformity assessment (ISO/IEC 17007:2009), ISO/IEC, September 2009.

3.3 SELECTION OF ACTIVITIES

> c) the selection of the activities appropriate to the purpose and scope of the scheme; as a minimum, a certification should include the function and activities I, II, III, IV and V a);

EN ISO/IEC 17067 defines several categories of activities, as well as different categories of products. In the case of the EUDI Wallets, the scheme is hybrid with product and process components, so things are slightly different.

From a high level, activities I (Selection), II (Determination of characteristics), III (Review), IV (Decision on certification) and a subset of V (Attestation, licensing) are required.

For I, III and IV, no additional selection is required. However, for I (Selection), if methods or procedures are defined to perform the selection based on an analysis of the design of an EUDI Wallet, it is preferable to mandate the activity that they implement.

Cert-66	*Process*	The national certification scheme **shall** define at least the following selection activity: Audit of the design and validation plan, as defined in Annex A.

Note*: This is mostly a hook to the method and procedure, indicating where it should be applied.*

Note*: In this particular case, the list of determination activities is included in the "validation plan" proposed by the EUDI Wallet provider, and confirmed as appropriate in this first phase.*

For the determination function (II), it is difficult to figure out exactly what activities will be performed. Testing is likely (if standardized tests are available), as well as inspection, design appraisal, and activities like audit linked to the assessment of processes. In addition, ISO/IEC TR 17028 provides a list of evaluation activities for services that could be interesting here.

> Evaluation activities that can be selected for the evaluation of service and service provider can include
>
> - validation of design of the service delivery process (including any required risk assessment, preventive planning and contingency arrangements);
> - audit, inspection and testing of service delivery processes and service outputs;
> - interview and communication with service personnel, which may include the assessment of their competence;
> - anonymous observation or witnessing of the service being delivered (e.g., "mystery shoppers");
> - obtaining and assessing feedback on the service being delivered and customer experience (e.g. customer satisfaction survey)
> - assessing resources used in the delivery of services (e.g. access to adequate numbers of competent personnel, facilities, equipment and technology);
> - assessing contractors, subcontractors, franchisees, etc. where the service delivery is contracted or outsourced;
> - audit of any management system that enables the service provider to manage its provision of its service, and to respond effectively to complaints and nonconformities with appropriate correction and corrective actions;
> - assessing the management and control of documentation, including any necessary aspects to address confidentiality and privacy requirements;
> - on-site or remote visits, either at the physical location at which the service is being provided, or at any virtual locations where the services are provided (e.g. a specific internet site).

***Note**: For the determination function (II), many different activity types are possible, and there is limited interest in making some activities mandatory in the implementing act, since the selection of activities is driven by the nature of the assessment to be performed.*

For V, activity a) is the only one that is relevant.

Cert-67	*Process*	The national certification scheme **shall** define at least the following attestation and licensing activities: issuing a certificate of conformity (V a) in EN ISO/IEC 17067 Table 1).

For VI, activity d) is closest to what is needed.

Cert-68	*Process*	The national certification scheme **shall** define at least the following surveillance activities: - surveillance evaluation of processes combined with random tests or inspections (Inspired from VI d) in EN ISO/IEC 17067 Table 1).

***Note**: The original activity VI d) calls for management system audits, which has here been replaced by surveillance evaluations of processes.*

3.4 OTHER REQUIREMENTS TO BE MET BY THE CLIENT

d) other requirements to be met by the client, e.g., the operation of a management system or process control activities to assure the demonstration of fulfilment of specified requirements is valid for the ongoing production of certified products;

What is considered "other" requirements are here already included in the service requirements, which cover the product aspects as well as the service used to deploy the products, so there is nothing to add here.

3.5 REQUIREMENTS FOR CONFORMITY ASSESSMENT BODIES

e) the requirements for certification bodies and other conformity assessment bodies involved in 5c(6the certification process; these requirements should not be in contradiction to the requirements of the applicable standards for conformity assessment bodies;

The main requirement is the use of EN ISO/IEC 17065 for CBs (which requires compliance to the other standards of the 17000 series for performing conformity assessment activities), since there is no requirement to use other CABs, but this is already required as a consequence of the definition of a CAB in the regulation.

We can add a requirement outlining a few topics to be covered by accreditation, to make sure that the CABs are competent.

Cert-69	*Process*	The national certification scheme **shall** include requirements related to minimal competences to be checked in accreditation, covering at least:

– deep technical understanding of EUDI Wallet architectures, threats and risk management;
– knowledge of security solutions available and of their properties, mapping them to the requirements of (EU) 2015/1502;
– knowledge about the activities performed under certificates applied to components of the object of certification.

***Note**: It is likely that NABs will gather much more precise requirements from the definition of the scheme, but these define a baseline. Also, we cannot ask for much specific testing competences, since testing and other conformity assessment activities may be performed in the context of another certificate, in which case the accredited CB would only have to review the results, not perform the activities themselves.*

3.6 ACCREDITATION

f) whether conformity assessment bodies involved in the scheme (e.g., testing laboratories, inspection bodies, testing bodies, bodies auditing manufacturer's management systems) are to be accredited, participate in peer assessment or qualified in another manner; if the cabscheme is to require that conformity assessment bodies are accredited, the appropriate references should be specific, e.g. that the accreditation body is a member of a mutual recognition arrangement between accreditation bodies;

The definition of a conformity assessment body in the regulation refers to EU 765/2008, which requires accreditation by a national accreditation body. This is already a requirement in the regulation (Cert-7).

3.7 METHODS AND PROCEDURES

g) the methods and procedures to be used by the conformity assessment bodies involved in the certification process, so as to assure that integrity and consistency of the outcome of the conformity assessment process;

Requirements on methods and procedures will be a key element in these requirements on schemes. An initial proposal is defined in Annex A.

Cert-70	*Process*	The national certification scheme **shall** define methods and procedures, based on best practices, to be used by the conformity assessment bodies involved in the certification process.
Cert-71	*Process*	The national certification scheme **shall** include the methods and procedures defined in Annex A to the document.

3.8 INFORMATION TO BE SUPPLIED BY APPLICANTS

h) the information to be supplied to the certification body by an applicant for certification;

This information provided needs at least to include the information required by the methods and procedures defined in the Annexes.

Cert-72	*Process*	The national certification scheme **shall** include requirements for the applicant for certification to provide to the CB the following information: – a description of the service to be certified, including a description of the EUDI Wallet and of the processes and systems used for the provision and support of the EUDI Wallet; – an analysis of the architecture of the service, together with a mapping of the generic risks for EUDI Wallets to the components of the architecture and a description of the measures taken to mitigate these risks; – a validation plan for the EUDI Wallet and associated eID scheme, which covers the components of the architecture described above at a level of assurance sufficient to mitigate the identified risks; – a complete list of the certificates and other assurance information used as evidence.

***Note**: This information needs to be in sync with the content of the Annexes, and it may even be defined in the Annexes and referred to.*

3.9 CONTENT OF CERTIFICATE

i) the content of the statement of conformity (e.g., certificate) which unambiguously identified the product in which it applies;

There is no need to include specific information in the certificates beyond the requirements of EN ISO/IEC 17065.

3.10 CERTIFICATE USE

j) the conditions under which the client may use the statement of conformity or marks of conformity;

The certification is a prerequisite to the deployment of an EUDI Wallet, as required by Article 5c(1). It is not planned to be used in any other circumstances, so there is no need to define conditions for certificate use.

3.11 MARKS OF CONFORMITY

k) where marks of conformity may be used, the ownership, use and control of the marks; the requirements of ISO/IEC 17030[13] should be applied;

The EU Digital Identity Wallet Trust Mark, as defined in Article 3, could be considered as a mark of conformity:

(50) 'EU Digital Identity Wallet Trust Mark' means a verifiable indication in a simple, recognisable, and clear manner that a European Digital Identity Wallet has been provided in accordance with this Regulation;

It could therefore be considered problematic or confusing to introduce another mark of conformity.

[13] EN ISO/IEC 17030. Conformity assessment — General requirements for third-party marks of conformity (ISO/IEC 17030:2021), ISO/IEC, September 2021.

Cert-73	*Process*	The scheme **shall** not use any mark of conformity different from the EU Digital Identity Wallet Trust Mark.

***Note**: This is a negative requirement, since the EU Digital Identity Wallet Trust Mark plays a similar role as a mark of conformity, so there is no need to refer to ISO/IEC 17030 and to apply the requirements from this standard.*

3.12 RESOURCES

l) the resources required for the operation of the scheme, including impartiality and competence of the personnel (internal and external), the evaluation resources, and the use of subcontractors;

There is no specific need to go beyond the requirements of EN ISO/IEC 17065, and the generic requirement above. The accreditation framework will ensure that the competences available are sufficient, and that the organization of the conformity assessment activities (with or without contractors, with or without accreditation of subcontractors) is appropriate.

3.13 FROM EVALUATION TO CERTIFICATION

m) how the results of the determination (evaluation) and surveillance stages are to be reported and used by the certification body and the scheme owner;

There aren’t many constraints about the relations within a scheme. However, there may be constraints about reporting to the EU-wide certification system:

Cert-74	*Process*	The scheme **shall** define how results are to be reported in the certification report.
Cert-75	*Process*	The scheme **shall** require the CB to include in the certification report a summary of the preliminary audit of the audit and validation plan.

***Note**: This would need to be refined with additional details in order to be useful, but the key question is to know whether there is an interest to share some information about the evaluation with the public.*

3.14 NONCONFORMITIES

n) the question of how non-conformities with the certification requirements, which include product requirements, are to be dealt with and resolved;

The proposal is to not include definitions of nonconformities in the present document.

***Note**: Is there a specific interest in constraining how nonconformities are handled? Should there be any reporting? We could have defined a notion of minor/major nonconformities, similar to those defined in EN ISO/IEC 17021-1, together with the separation between corrections (removing the nonconformity) and corrective actions (removing the root cause of the nonconformity). However, agreeing on the definition of a minor nonconformity would lead to lengthy and difficult discussions.*

3.15 SURVEILLANCE

o) surveillance procedures, where surveillance is part of the scheme;

There should at least be an obligation to consider incidents and vulnerability management:

Cert-76	*Process*	The national certification scheme **shall** mandate that the provider of a certified EUDI Wallet notifies its CB when a breach affects a certified EUDI Wallet, as defined in Article 5da(1).
Cert-77	*Process*	The national certification scheme **shall** mandate that the provider of a certified EUDI Wallet defines and operates a vulnerability management policy.

***Note**: The requirement on notification is only one of the obligations of EUDI Wallets in case of a breach, and other bodies will need to be notified.*

***Note**: The Cyber Resilience Act (CRA) includes requirements on vulnerability management that will eventually need to be enforced, so the EUDI Wallet providers are invited to define and implement a policy that satisfies the CRA requirements.*

We should probably include some rules similar to those included in the EUCC implementing act (Chapter V):

Cert-78	*Process*	The national certification scheme **shall** mandate the scheme owner to monitor the compliance of (a) the certification body with their obligations pursuant to regulation eIDAS2 and to this scheme; (b) the holders of a certification issued according to this scheme with their obligations pursuant to regulation eIDAS2 and to this scheme; (c) the certified EUDI Wallet(s) with the requirements set out in this scheme; (d) the assurance expressed in the certificate addressing the evolving threat landscape.
Cert-79	*Process*	The national certification scheme **shall** mandate the scheme owner to perform its monitoring activities in particular on the basis of: (a) information coming from certification bodies, national accreditation bodies and relevant market surveillance authorities; (b) information resulting from its own or another authority's audits and investigations; (c) complaints received.

***Note**: We have removed the reference to sampling, because the number of certificates will not be sufficient for sampling.*

Cert-80	*Process*	The national certification scheme **shall** explicitly allow the scheme owner, that has sufficient reason to believe that a certified EUDI Wallet is no longer in compliance with this scheme or with regulation eIDAS2, to carry out investigations and make use of any monitoring powers set out in this scheme.
Cert-81	*Process*	The national certification scheme **shall** mandate the scheme owner that identifies that an ongoing investigation concerns an EUDI Wallet that is certified by certification bodies established in other Member States, to inform thereof the

		scheme owner of the relevant Member States in order to collaborate in the investigations, where relevant, and to also notify the European Commission and the EDICG of the cross-border investigations and the subsequent results.

***Note**: This is missing a procedure for performing a specific review as part of the investigation, but this is due to the fact that the EDICG does not have the powers of a NCCA.*

3.16 ACCESS CRITERIA

p) the criteria for access of conformity assessment bodies to the scheme and for the access of clients to the scheme;

There are conditions to be met in order to provide an EUDI Wallet, so the access of clients to the scheme is limited to the entities meeting these conditions.

Cert-82	*Process*	The national certification scheme **shall** limit access to EUDI Wallet providers that meet one of the conditions of Article 5a(2).

3.17 DIRECTORY OF CERTIFIED PRODUCTS

q) content, conditions, and responsibility for publication of the directory of certified products by the certification body or the scheme owner;

Article 5d(1) mandates the Member State to notify the Commission and EDICG of certified EUDI Wallets, but the article also mentions the provision of EUDI Wallets, so this obligation is not directly linked directly to the scheme, but to another authority (see section ‘2.2,

Cert-83	*Process*	The scheme **shall** mandate the CB to notify the national supervisory body for EUDI Wallets of the issuance and cancelation of certificates on EUDI Wallets.

3.18 CONTRACTS

r) the need for; and content of, contracts, e.g. between scheme owner and certification body, scheme owner and clients, certification body and clients: the rights, responsibilities and liabilities of the various parties should be defined in contracts;

No additional requirements.

3.19 CERTIFICATE MAINTENANCE

s) general conditions for maintaining, continuing, extending the scope of, reducing the scope of, suspending, and withdrawing certification: this includes requirements for discontinuation of advertising and return of certification documents and any other action if the certification is suspended, withdrawn, or terminated;

Cert-84	*Process*	The national certification scheme **shall** define the maximal duration of certificates as five (5) years.

Cert-85	*Process*	The national certification scheme **shall** mandate surveillance evaluations including at least a vulnerability assessment every two (2) years and following the schedule defined in Annex D.

***Note**: The initial proposal was here to set the standard duration as 4 years, with a surveillance evaluation after 2 years (Article 5c(2b) mandates 5 and 2 years), because the vulnerability assessment after 4 years could be problematic, and also because the evolution of technology is likely to limit the lifetime of an EUDI Wallet. It is better to keep the 5-year limit, but EUDI Wallet providers may nevertheless encouraged to perform a recertification evaluation after 4 years, leaving them one year to fix issues if they encounter an issue.*

If an EUDI Wallet lasts for more than 5 years, it may be recertified:

Cert-86	*Process*	The national certification scheme **shall** include provisions for the recertification of an EUDI Wallet, by performing a dedicated evaluation before the expiry of the initial certificate, which shall include at least a vulnerability assessment and an evaluation of the EUDI Wallet's threat model.

***Note**: The list of mandatory components may be increased. Here, the focus is on "resetting" the vulnerability assessment requirement and on ensuring that the threat mode and risk assessment are up to date (which is likely to trigger many more activities).*

Special evaluations (often triggered by a critical vulnerability, changes in the EUDI Wallet or by changes in the threat environment or in the test requirements) are likely to be mandatory as well:

Cert-87	*Process*	The national certification scheme **shall** define a process for special evaluations, including a selection of activities to be performed to address the specific issue that triggered the recertification.
Cert-88	*Process*	The national certification scheme **shall** define requirements for performing special evaluations within a defined period after the revision of the scheme, or after the release of new specifications or standards to which the EUDI Wallet must conform.

***Note**: There may be more mandates to trigger a special evaluation.*

3.20 COMPLAINTS

t) the way in which the clients' complaints records are to be verified if such verification is part of the scheme;

The scheme needs to follow up on complaints:

Cert-89	*Process*	The national certification scheme **shall** require CBs to establish procedures to effectively lodge and handle complaints, including regular reporting to the scheme owner.

3.21 REFERENCES TO THE SCHEME

u) the way in which the clients make reference to the scheme in their publicity material;

The scheme needs to define how to refer to certificates, but they need to refer to the EU legal framework:

Cert-90	*Process*	The national certification scheme **shall** define requirements on how providers of certified EUDI Wallets can make reference to the scheme, which **shall** at least include references to the amending Regulation requirements and the certification Implementing Act.

3.22 RETENTION OF RECORDS

v) retention of records by scheme owner and certification bodies;

The typical requirement would be a few years after the cancelation or expiry of certificates:

Cert-91	*Process*	The national certification scheme **shall** require CBs to store records related to a certificate for at least five (5) years after the withdrawal or expiry of the certificate.

***Note**: Five years is the value used in the EUCC and proposed for the EUCS. Note that the count is not starting from the withdrawal of the first certificate, but from the withdrawal of the last certificate that depends on the record.*

In addition, there may be additional requirements related to the protection of information, as an extension of the default requirements from EN ISO/IEC 17065:

Cert-92	*Process*	The national certification scheme **shall** include a requirement for all parties to ensure the security and protection of business secrets and other confidential information, including trade secrets, as well as preserving intellectual property rights, and take the necessary and appropriate technical and organisational measures.

***Note**: This text is from the EUCC's Article 43*[14].

3.23 VULNERABILITY MANAGEMENT

This element is from the Cybersecurity Act, Article 54(1):

[14] COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

> (m) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;

It is difficult to define these requirements without getting in a lot of details:

Cert-93	*Process*	The rules on management of vulnerabilities **shall** at least require compliance to the requirements of CRA's Annex I on vulnerability management.

***Note**: We have chosen to use the CRA requirements as a basis, since they form a good baseline, and they will become a reference.*

3.24 MUTUAL RECOGNITION

This element is from the Cybersecurity Act, Article 54(1):

> (t) conditions for the mutual recognition of certification schemes with third countries;

Since each national scheme may be designed to target specifically the EUDI Wallet design choices made in a specific Member State, there is no expectation of mutual agreement, although of course, some Member States may decide to establish mutual recognition agreements with other Member States.

No requirement is needed on this topic.

***Note**: There is no need for mutual recognition of the certificates issued for EUDI Wallets for national schemes, but the regulation mandates mutual recognition of the EUDI Wallets themselves.*

***Note**: This is only true for national certification schemes. If/when an EU scheme is established, its certificates will have to be recognised by all Member States.*

3.25 PEER ASSESSMENT

This element is from the Cybersecurity Act, Article 54(1):

> (u) where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59;

Once again, this particular provision is used as a reminder that a peer assessment mechanism between the CBs in the various national schemes could be considered, at least to verify that they apply the requirements defined in the certification implementing act.

There is no need for such a requirement for national certification schemes, because each scheme is likely to have a limited number of active CBs.

However, ENISA recommends that Member States consider the establishment of a voluntary peer assessment program between CBs operating in different national schemes in order to improve harmonisation.

3.26 DOCUMENTATION FORMAT

This element is from the Cybersecurity Act, Article 54(1):

> (v) format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.

This is related to Article 55, which mandates some information to be shared publicly:

> Article 55 – Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes
>
> 1. The manufacturer or provider of certified ICT products, ICT services or ICT processes or of ICT products, ICT services and ICT processes for which an EU statement of conformity has been issued shall make publicly available the following supplementary cybersecurity information:
>   (a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services;
>   (b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates;
>   (c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;
>   (d) a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any relevant cybersecurity advisories.
> 2. The information referred to in paragraph 1 shall be available in electronic form and shall remain available and be updated as necessary at least until the expiry of the corresponding European cybersecurity certificate or EU statement of conformity.

Since this will be made mandatory when an EU scheme will be available, it could be interesting to make the transparency of documentation mandatory in the early national schemes.

Cert-94	*Process*	The national certification scheme **shall** require all EUDI Wallet providers to make publicly available security information about their product, including at least: (a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the EUDI Wallet; (b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates; (c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers; (d) a reference to online repositories listing publicly disclosed vulnerabilities related to the EUDI Wallet and to any relevant cybersecurity advisories..

***Note**: This exact list of required documentation may not be the same as for the CSA.*

3.27 NCCA INVOLVEMENT

This element is from the Cybersecurity Act, Article 54(6):

> 6. Where a European cybersecurity certification scheme adopted pursuant to Article 49 requires an assurance level 'high', the European cybersecurity certificate under that scheme

> is to be issued only by a national cybersecurity certification authority or, in the following cases, by a conformity assessment body:
>
> (a) upon prior approval by the national cybersecurity certification authority for each individual European cybersecurity certificate issued by a conformity assessment body; or
>
> (b) on the basis of a general delegation of the task of issuing such European cybersecurity certificates to a conformity assessment body by the national cybersecurity certification authority.

This article requires the involvement of a NCCA in the issuance of certificates at assurance level ‘high’, which can be achieved either by issuing the certificate themselves, or by delegating the issuance to private Certificate Bodies, with two models. Adopting a requirement in that direction would be a step toward the Cybersecurity Act.

***Note**: This requirement has been removed following the latest discussion with the Certification subgroup, whose members did not deem it appropriate, but the section is kept as a reference.*

D. OTHER SCHEME CONTENT

4.1 OVERVIEW

In addition to the list of basic content listed in the previous chapter, EN ISO/IEC 17067 lists a number of topics that need to be covered in the scheme. These topics all represent key questions in the context of the certification of EUDI Wallets.

4.2 SAMPLING

This is section 6.5.2 of EN ISO/IEC 17067:

> Where applicable, the scheme should define the extent to which sampling of the product to be certified is required, and on what basis such sampling should be undertaken both at the selection and surveillance stages. The scheme should define when sampling is required and who is permitted to undertake it.

In the EUDI Wallets certification scheme, sampling will be required for at least some of the components which may be expected to run on many different types of mobile devices, in order for those components and the EUDI Wallet to be considered certified. The applications (software) components of the EUDI Wallet are all supposed to be independent of the underlying platform to a certain degree, which should determine how testing should occur. Testing of all components on all devices would be unpractical, so sampling will be required.

Cert-95	*Process*	The national certification scheme **shall** define sampling rules allowing functional and security tests to be performed only on a sample of target EUDI Wallet components on a sample of target devices and including requirements for CBs to justify the selection of target components and devices.

***Note**: The question that remains open is to understand how much we want to constrain these sampling rules. The requirement for justification is the minimal requirement.*

Sampling is also likely to be useful for the evaluation of processes, but these uses do not need to be harmonised beyond standard practices, as they are quite common.

4.3 ACCEPTANCE OF CONFORMITY ASSESSMENT RESULTS

This is section 6.5.3 of EN ISO/IEC 17067:

> In some cases, clients might have obtained the results of determination activities, such as testing, inspection or auditing, prior to making an application for certification. In such a situation, the conformity assessment result may be from a source not within the contractual control of the certification body. The scheme should define whether and under what conditions such conformity assessment results can be considered in the certification process.

This is a truly essential part of the scheme, since it is composite, and it will need to rely on evidence originating from outside the scheme. In some cases, this evidence may be associated to certificates from other certification schemes, national or private, but in other cases, it will be associated to other kinds of assurance documentation, such as audit reports from public auditors, or documentation provided by vendors to place their products on the market (as required by the Cyber Resilience Act).

There are here two aspects to cover:

- The process used to assess the assurance information.
  Agreeing on the way in which assurance information needs to be considered and assessed before being accepted as evidence.
- The criteria used to constrain the acceptability of information.
  A list of criteria defining the assurance information that may be accepted (possibly including negative criteria leading assurance information to be considered unacceptable).

Both aspects need to be covered in the scheme in accordance to the EU-level certification system:

Cert-96	*Process*	The national certification scheme **shall** define a methodology to assess the acceptability of information assurance provided by the EUDI Wallet developer, including the provisions defined by the EUDI Wallets certification system, including at least the provisions defined in Annex B.
Cert-97	*Process*	The national certification scheme **shall** define criteria for acceptability of information assurance provided by the EUDI Wallet developer, including the provisions defined by the EUDI Wallets certification system, including at least the criteria defined in Annex C.

4.4 OUTSOURCING OF THE CONFORMITY ASSESSMENT ACTIVITIES

This is section 6.5.4 of EN ISO/IEC 17067:

> If the scheme permits outsourcing (subcontracting) of conformity assessment activities such as testing, inspection or auditing, then the scheme should require these bodies to meet the applicable requirements of the relevant International Standards. For testing, it should meet the applicable requirements of ISO/IEC 17025; for inspection, it should meet the applicable requirements of ISO/IEC 17020; and for management systems auditing, it should meet the applicable requirements of ISO/IEC 17021-1. The scheme should state the degree to which prior agreement to outsourcing needs to be obtained from the scheme owner or the client whose products are being certified under the scheme.

There should not be specific requirements beyond those stemming from the definition of methods and procedures. Note that some methods and procedures may be linked to a particular kind of activity (testing, audit, inspection).

***Note**: We would recommend not to include a requirement for independent accreditation of the subcontractors, as this may become quite heavy, but there should not be any requirement forbidding it in national schemes.*

4.5 COMPLAINTS AND APPEALS TO THE SCHEME OWNER

This is section 6.5.5 of EN ISO/IEC 17067:

> The scheme owner should define the complaints and appeals process and who is responsible for undertaking the process.

> Appeals against the decision of the certification body and complaints about the certification body should be addressed to the certification body in the first instance.
> Appeals and complaints that have not been, or cannot, be resolved by the certification body can be addressed to the scheme owner.

The only requirement here would be to transform the last statement into an obligation:

Cert-98	*Process*	The national certification scheme **shall** require that all complaints that have not been, or cannot, be resolved by the CB shall be addressed to the scheme owner.

4.6 LICENSING AND CONTROL OF THE MARK

This is section 6.5.6 of EN ISO/IEC 17067:

> Where the scheme provides for the use of certificates, marks or other statements of conformity, there should be a license or other form of enforceable agreement to control such use. Licenses can include provisions related to the use of the certificate, mark or other statement of conformity in communications about the certified product, and requirements to be fulfilled when certification is no longer valid. Such licenses may be between two or more of the scheme owners, the certification body, and the client of the certification body.

No specific requirements unless the European Commission wants to establish a mark, but this role seems to be played by the EUDI Wallet Trust Mark.

4.7 SURVEILLANCE

This is section 6.5.7 of EN ISO/IEC 17067:

> If surveillance is included, the scheme should define the set of activities (see function 6 of Table 1) that make up the surveillance functions. When deciding upon the appropriate surveillance activities, the scheme owner should consider the nature of the product, the consequences and probability of nonconforming products and the frequency of the activities.

Surveillance and compliance monitoring need to be organised following rules that are at least partly common to all certification schemes and defined in the EU-wide certification system:

Cert-99	*Process*	The national certification scheme **shall** require CBs to undertake surveillance according to a CB-defined surveillance plan and the scheme **shall** define requirements for such surveillance and compliance monitoring, including the provisions defined by the EUDI Wallets certification system, including at least the requirements defined in Annex D.

4.8 NON-CONFORMING PRODUCTS

This is section 6.5.8 of EN ISO/IEC 17067:

> The scheme should define requirements that apply when a product no longer fulfils certification requirements, such as product recall or providing information to the market.

The regulation already has provisions in place in case of certificate withdrawal or security incident. These regulatory requirements can be used as a basis for the scheme's requirements.

Article 5e:

1. Where European Digital Identity Wallets provided pursuant to Article 5a, the validation mechanisms referred to in Article 5a(8) or the electronic identification scheme under which the European Digital Identity Wallets are provided are breached or partly compromised in a manner that affects their reliability or the reliability of other European Digital Identity Wallets, the Member State that provided the European Digital Identity Wallets shall, without undue delay, suspend the provision and the use of European Digital Identity Wallets.
   Where justified by the severity of the security breach or compromise referred to in the first subparagraph, the Member State shall withdraw European Digital Identity Wallets without undue delay.
   The Member State shall inform the users affected, the single points of contact designated pursuant to Article 46c(1), the relying parties and the Commission accordingly.

Article 5e(1) requires the Member State to inform users of any security breach related to EUDI Wallets, which means that certification stakeholders have an obligation to inform them if they become aware of such an incident.

Cert-100	*Process*	The national certification scheme **shall** require providers of certified EUDI Wallets to notify their CB, without delay, of any security breach that may have entirely or partially compromised their EUDI Wallet or its content.
Cert-101	*Process*	The national certification scheme **shall** require CBs to notify the EUDI Wallet national authority of any security breach reported by providers of certified EUDI Wallets.

***Note**: We may want the CB to perform a few tasks to assess the incident before reporting it, but this version of the requirement is the "**safe**" one.*

Article 5e(1) requires an EUDI Wallet to be suspended and then withdrawn in case of an incident:

Cert-102	*Process*	The national certification scheme **shall** require a CB to suspend without delay the certificate of an EUDI Wallet after the confirmation of a breach or compromise of the EUDI Wallet that affects their reliability or the reliability of other EUDI Wallets.
Cert-103	*Process*	The national certification scheme **shall** require a CB to cancel the certificate of an EUDI Wallet that has been suspended following a breach or compromise that has not been remedied in a timely manner.

***Note**: These requirements are less constraining than the previous one, because they are conditional to an analysis of how the breach or compromise affects the reliability of EUDI Wallets. As a result, notification of users may occur without suspension or withdrawal of the certificate.*

4.9 REPORTING TO THE SCHEME OWNER

This is section 6.5.9 of EN ISO/IEC 17067:

> When reporting to the scheme owner is required, the content and the frequency of reporting should be defined. Such reporting may be for the purpose of scheme improvement, for control purposes and for monitoring the extent of conformity by clients.

No specific requirements.

4.10 SUBCONTRACTING OF THE OPERATION OF THE SCHEME

This is section 6.5.10 of EN ISO/IEC 17067:

> If the scheme owner subcontracts all or part of the operation of the scheme to another party, it should have a legally binding contract defining the duties and responsibilities of both parties. A governmental scheme owner can subcontract operation of the scheme by regulatory provisions.

Cert-104	*Process*	The national certification scheme **shall** require the scheme owner who subcontracts all or part of the operation of the scheme to another party to have a legally binding contract defining the duties and responsibilities of both parties.

Note*:*
This requirement has been added to ensure that such subcontracting would be properly defined.

4.11 MARKETING

This is section 6.5.11 of EN ISO/IEC 17067:

> The scheme should define the policies and procedures related to marketing, including the extent to which certification bodies can make reference to the scheme.

No specific requirements.

4.12 FRAUDULENT CLAIM OF CERTIFICATION

This is section 6.5.12 of EN ISO/IEC 17067:

> Actions and responsibilities for situations where certification under the scheme is being claimed fraudulently should be described.

Cert-105	*Process*	The national certification scheme **shall** describe actions and responsibilities for situations where certification under the scheme is being claimed fraudulently.

Note: *Since the certification is solely used for the purpose of providing an EUDI Wallet and needs to be complemented by notification, this is quite unlikely, but it is better to cover this case.*

4.13 REVIEW OF SCHEME OPERATION

This is section 6.6.1 of EN ISO/IEC 17067:

> The scheme owner should define a process for reviewing the operation of the scheme on a periodic basis in order to confirm its validity and to identify aspects requiring improvement,

> taking into account feedback from stakeholders. The review should include provisions for ensuring that the scheme requirements are being applied in a consistent manner.

This text is interesting because of the specific structure of this scheme, where there may be very few certificates issued, likely a single certificate in some countries. In such circumstances, consistency of application is impossible to assess, because there is no sufficient data.

***Note**: This may be better addressed at the EU level by organizing a certification system, as mentioned in section '2.3 How to organize certification?'.*

Additional details are defined in ISO/IEC TR 17028:

> The review should at least consider the following:
> – any requests for clarification related to scheme requirements;
> – feedback from stakeholders and other interested parties;
> – responsiveness of scheme owners to requests of information;
> – the need for integrity programmes (e.g. validation audit or other checks)

The proposal is to use these as the basis for requirements for the review.

Cert-106	*Process*	The national certification scheme **shall** require the scheme owner to define a process for reviewing the operation of the scheme on a periodic basis in order to confirm its validity and to identify aspects requiring improvement, taking into account feedback from stakeholders.
Cert-107	*Process*	The review of the national certification scheme **shall** include provisions for ensuring that the scheme requirements are being applied in a consistent manner.
Cert-108	*Process*	The review of the national certification scheme **shall** at least consider the following: • – any requests for clarification related to the certification scheme requirements; • – feedback from stakeholders and other interested parties; • – responsiveness of the certification scheme owners to requests of information; • – the need for integrity programmes (e.g. validation audit or other checks)

4.14 CHANGES IN SPECIFIED REQUIREMENTS

This is section 6.6.2 of EN ISO/IEC 17067:

> The scheme owner should monitor the development of the standards and other normative documents which define the specified requirements used in the scheme. Where changes in these documents occur, the scheme owner should have a process for making the necessary changes in the scheme, and for managing the implementation of the changes (e.g., transition period) by the certification bodies, clients and, where necessary, other stakeholders.

Such rules are needed in a scheme, in particular in early stages, where it is likely that reference documents will evolve at a higher pace.

Cert-109	*Process*	The national certification scheme **shall** include provisions for monitoring reference documents and procedures for the evolution of the scheme's reference versions, including at least trial and transition periods.

Note: *The provisions defined in the requirement below apply to the drafting of the implementing act, not the national certification scheme.*

*"The national certification scheme **shall** include provisions for the recertification of EUDI Wallets, by performing a dedicated evaluation before the expiry of the initial certificate, which shall include at least a vulnerability assessment and an evaluation of the EUDI Wallet's threat model."*

Note*: We could also consider to weaken this last requirement by only providing common directions at the certification system level, or by allowing the measures associated to specific documents to be adopted at the certification system level.*

4.15 OTHER CHANGES TO THE SCHEME

This is section 6.6.3 of EN ISO/IEC 17067:

> The scheme owner should define a process for managing the implementation of other changes to the rules, procedures and management of the scheme.

It is definitely interesting to consider such a process, in particular for schemes that are rather new.

Cert-110	*Process*	The national certification scheme **shall** define a process for managing other changes in the scheme or in the national certification system.

E. ARCHITECTURE-SPECIFIC SCHEMES

National certification schemes do not need to cover every possible implementation of an EUDI Wallet, in particular if a Member State has already decided the architecture(s) that they want to develop. In such a case, they may define a scheme that is specialised for a given architecture, or several sub-schemes specialised for each of the architecture that they would consider deploying.

In such a case, the architecture analysis that is defined in Annex A.2 would need to be performed as part of the definition of the scheme, and the relevant information would need to be made available as part of the scheme.

Cert-111	*Process*	A national certification scheme that is specialised for a given architecture **shall** include at least information about the architecture of the targeted EUDI Wallet architecture, a list of security functions associated to assurance levels and required security elements, a mapping of these functions to the components of the architecture, and a validation plan tailored to the EUDI Wallet's architecture.

***Note**: The objective of this requirement is to ensure that sufficient information is available when the Member State submits its draft certification scheme to the EDICG, which will the use this information to provide an opinion and possible recommendations on the draft certification scheme.*

We can also consider going a step further by mandating the definition of architecture-specific (sub-)schemes for every architecture considered by a Member State.

Cert-112	*Process*	The national certification scheme **shall** be specialised for a given architecture, or it shall include different sub-schemes, each specialised for a given architecture.

REFERENCES

CEN-CENELEC EN 17640. Fixed-time cybersecurity evaluation methodology for ICT products (CEN-CENELEC EN17640:2022), CEN-CENELEC, April 2023.

CEN-CENELEC EN 17927. Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products (CEN-CENELEC EN 17927:2023), CEN-CENELEC, April 2023.

CEN-CENELEC EN 18026. Three-level approach for a set of cybersecurity requirements for cloud services (CEN-CENELEC EN 18026:2024), CEN/CENELEC, November 2023.

COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

EN ISO/IEC 17000. Conformity assessment – Vocabulary and general principles (ISO/IEC 17000:2020), ISO/IEC , December 2020.

EN ISO/IEC 17007. Conformity assessment — Guidance for drafting normative documents suitable for use for conformity assessment (ISO/IEC 17007:2009), ISO/IEC, September 2009.

EN ISO/IEC 17021-1. Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements (ISO/IEC 17021-1: 2015), ISO/ IEC, July 2015.

EN ISO/IEC 17029. Conformity assessment – General principles and requirements for validation and verification bodies (ISO/IEC 17029:2019), ISO/IEC, November 2019.

EN ISO/IEC 17030. Conformity assessment — General requirements for third-party marks of conformity (ISO/IEC 17030:2021), ISO/IEC, September 2021.

EN ISO/IEC 17065. Conformity assessment — Requirements for bodies certifying products, processes and services (ISO/IEC 17065:2012), ISO/IEC, September 2012.

EN ISO/IEC 17067. Conformity assessment – Fundamentals of product certification and guidelines for product certification schemes (ISO/IEC 17067:2013), ISO/IEC, August 2013.

EN ISO/IEC 27001. Information security, cybersecurity and privacy protection (ISO/IEC 27001:2022), ISO/IEC, October 2022.

EN ISO/IEC TR 17028. Conformity assessment – Guidelines and examples of a certification scheme for services (ISO/IEC TR 17028:2017), ISO/IEC, June 2017.

REGULATION (EC) NO 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance).

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

A METHODS AND PROCEDURES

***NOTE**: We first need to agree on the principles of the content of this annex before we move on to the more detailed definition of the methods and procedures.*

INTRODUCTION

The requirements should contain some indications on the methods to be used. Here are a few candidates:

- The first activity in the assessment should be to analyse the input provided by the vendor, including a description of the architecture, a mapping of the assets, a risk assessment, and a validation plan specific to the architecture. This activity should lead to the development of the evaluation plan, based on the validation plan provided by the vendor.
- Article 5c(4) requires a vulnerability assessment, so this activity may need to be defined or at least constrained by requirements.
- We may as well define an activity similar to EUCS' dependency analysis, to analyse assurance information available about the components that are not assessed directly in the evaluation.
- More specific activities may be required, in particular to analyse how to assemble different components into an EUDI Wallet.

The evaluation is split between selection and determination. The first bullet is likely to be associated to selection, and the others to determination.

***Note**: The high-level descriptions provided in the following sections need to be replaced by more precise requirements on the activities that will be mandated in the national schemes.*

SELECTION FUNCTION AND PRELIMINARY AUDIT

The selection function is defined in EN ISO/IEC 17067 as follows:

> planning and preparation activities in order to collect or produce all the information and input needed for the subsequent determination function;

In many certification schemes, the selection function is rather simple because the determination activities are fixed or they vary little. In the certification scheme for EUDI Wallets, the functional part of the certification scheme will be a bit like that, since it focuses on the external interfaces and on the functionality as experienced by the users, independently of the underlying architecture.

For the security aspects, however, the selection function will be much more complex, because the determination activities to be performed will depend on the architecture of the EUDI Wallet and of the way the EUDI Wallet and associated eID scheme are managed.

The proposal is here to let the EUDI Wallet provider define a validation plan that is appropriate for its architecture and design, so the selection function consists in a validation of this validation plan by the CB.

Cert-113	*Process*	The national certification scheme **shall** define a selection function to audit the design of the EUDI Wallet and associated eID scheme, as well as the proposed validation plan covering this design.

Information required

Because the object of conformity assessment is complex, selection activities need to include at least some analysis of information provided by the EUDI Wallet provider, as follows:

- **Architecture information**
  For every component of the EUDI Wallet (including product, process and service components), a description of its essential security properties, including its external dependencies.
- **Functions, assurance level and required security elements**
  The Annex of CIR (EU)2015/1502 defines a number of technical specifications and procedures that apply to the various functions implemented by eID means, defining for each assurance level the security elements that need to be implemented.
- **Justified mapping of functions to architecture components**
  The functions will be implemented by architecture components, based on a rationale explaining why a given assurance level is required, and how the function is implemented with all required security elements at the appropriate level.
- **Justified validation plan for every component of the solution, and for their integration**
  This last part is a proposal of validation plan to be performed by the CB to confirm that the implementation of the EUDI Wallet and its eID scheme meet the requirements of the scheme.

Cert-114	*Process*	The selection function defined in the national certification scheme **shall** require the EUDI Wallet provider to provide a detailed description of the EUDI Wallet and associated eID scheme, including at least information about the architecture of the EUDI Wallet, a list of security functions associated to assurance levels and required security elements, a mapping of these functions to the components of the architecture, and a validation plan tailored to the EUDI Wallet's architecture.

***Note:** Since the certification scheme covers more than just products, the architecture goes beyond the hardware/software architecture, and also includes the essential characteristics of the management systems in which key processes are implemented.*

Architecture and risk analysis

The information provided by the EUDI Wallet provider, and in particular the validation plan, should be sufficient to select determination activities. In addition, the mapping between the security functions and the EUDI Wallet components should make it easy to determine the sufficiency of the proposed validation plan.

The result of the architecture analysis is a full evaluation program, including determination activities that are adapted to the risks identified for EUDI Wallets.

A risk-based approach is envisioned as the basis for certification by Member States. The risk-based approach proposes that Member States schemes should require Wallet Providers to evaluate relevant risks and propose appropriate mitigations in a dedicated risk assessment that will be evaluated by CABs.

To establish harmonised requirements, a common risk registry will be developed, which contains a comprehensive but non-exhaustive list of security and privacy risks. These risks are architecture-agnostic and provide a benchmark overview of the most critical risks. In other words, a minimum set of risks to be mitigated is required at European level.

The methodology to perform the individual RA will be up to the Member States, as long as it demonstrates taking into account the risks identified in the common risk register.

The common risk register will be jointly drafted by the European Commission and MS to achieve the right level of harmonisation.

Cert-115	*Process*	The national certification scheme **shall** require the audit of the design and validation plan to be based on the latest available risk registry for EUDI Wallets made available, complemented where needed by implementation-specific risks.

***Note**: There is an open question on how to make a generic risk assessment and an architecture-specific risk assessment complement each other. The generic risk assessment brings harmonisation, but may miss risks that are specific to a given implementation. The proposal in the requirement above is to start from the generic assessment, and to only allow the addition of risks. In that view, risks that are "automatically" mitigated by architectural choices will still be documented and their mitigation explained.*

***Note**: There is no specific requirement on the methodology to be used, but this could be performed using the EN ISO/IEC 17029[15] harmonised standard for verification and validation.*

***Note**: This is not contradictory with the requirements defined on schemes specialised for a given architectures. A specific EUDI Wallet implementation will always have made additional architectural choices that will lead to differences in the documentation provided, although the volume of work in this task is expected to be much lighter with an architecture-specific scheme.*

There are no specific requirements on the way to perform this audit. Of course, in the course of an analysis, a CB should ensure that they have all the competencies to perform the activities that they include in the determination plan, but once again, this is a basic requirement of EN ISO/IEC 17065, which does not need to be specified further.

DETERMINATION ACTIVITIES

The determination function is defined in EN ISO/IEC 17067 as follows:

[15] EN ISO/IEC 17029. Conformity assessment – General principles and requirements for validation and verification bodies (ISO/IEC 17029:2019), ISO/IEC, November 2019.

may include conformity assessment activities such as testing, measuring, inspection, assessment of processes and services and auditing to provide information regarding the product requirements as input to the review and attestation functions;

The determination activities will include a wide variety of activities, but a few of them can be identified already:

- Testing and inspection activities to determine whether the product components of an EUDI Wallet meet the requirements of the scheme, i.e., testing activities based on predefined test suites and inspection activities based on standardised inspection procedures, which may require professional judgment.
- Validation of the suitability and existence of processes, i.e., activities to validate that the processes have been designed to meet the scheme requirements, and that an implementation exists;
- Verification of the operating effectiveness of processes, i.e., activities to verify that the processes have been operating over a period of time as designed, effectively meeting the scheme requirements;
- Audit of the management systems underlying the implementation of processes.
- Dependency analysis, as defined in Annex C, to confirm the validity of assurance information from other sources.
- Vulnerability assessment activities, including penetration testing, to be performed at least on the overall solution, and if needed on individual components and functions.

The following section describe some of the most commonly used determination activities for the evaluation of EUDI Wallets.

Determination activities (product-oriented)

The first set of determination activities are related to the evaluation of product components of EUDI Wallets. The essential components developed by the EUDI Wallet provider are software components, but there are also strong dependencies on hardware components that are outside of the scope of certification, and the requirements associated to every software component are determined by the EUDI Wallet's architecture.

Evaluation of the WSCA

The WSCA is expected to host the most sensitive parts of the application, strongly associated to the underlying WSCD and its operating environment. Although the WSCD would typically be expected to be evaluated with Common Criteria with a high-level vulnerability assessment (AVA_VAN.5), there may be duly justified cases where the WSCA is evaluated at a lower level of assurance, for instance:

- When using an eUICC with CSP for sensitive operations, some EUDI Wallet providers may justify that the WSCA can be evaluated at a lower level of assurance.
- When using an HSM operating in a secure environment, some EUDI Wallet providers may justify that the WSCA running on a secure server and interacting with the HSM can be evaluated at a lower level of assurance.

***Note**: This analysis and the evidence supporting is provided as part of the architecture information used to perform the selection of activities, and it is validated together with the architecture.*

Cert-116	*Process*	The national certification scheme **shall** require the evaluation of the WSCA with the EUCC European scheme, or if not available, with a National certification scheme based on Common Criteria.
Cert-117	*Process*	The national certification scheme **shall** require the evaluation of the WSCA to include a vulnerability assessment at level AVA_VAN.5 unless it is duly justified that the security characteristics of the WSCA execution environment (including but not limited to the WSCD) allow to use a lower assessment level while keeping the same overall level of assurance.
Cert-118	*Process*	The national certification scheme **shall** require the security target used for the evaluation of the WSCA to cover all security functions implemented by the WSCA.

***Note**: The requirement on security targets is intended to ensure that platforma is appropriate with respect to the selected architecture. It does not preclude the development of Protection Profiles that would cover (some of) the security functions implemented by the WSCA.*

***Note**: In some architectures, there may be several implementations of the WSCA, typically corresponding to several different types of WSCDs. Similarly, in some hybrid architectures, the implementation of the WSCA may be split into several parts, each hosted on different WSCDs. In such cases, there will be several evaluations, possibly at different levels, depending on the characteristics of the underlying WSCD.*

Regarding the WSCA, there may be opportunities for optimisation of the certification requirements, since the electronic signature offered by EUDI Wallets has to be a qualified signature as defined in the Regulation, the WSCA may be an extension of the application used in the QSCD, so a single certification can meet both requirements.

Evaluation of EUDI Wallets Applications

An EUDI Wallet application is the application that includes the interaction with the different stakeholders, including at least the physical interaction with the user and the remote interaction with the relying parties.

The evaluation of an EUDI Wallet application faces several challenges, including in particular:

- Most EUDI Wallets will include several versions of the EUDI Wallet application, targeting different platforms. In some cases, these versions will be very similar, for instance differing only by the interface used to access the WSCA.
- With mobile (or desktop) applications, we should expect regular updates of these applications, in particular during the first deployments, where features are likely to be unstable.

These two characteristics are likely to make the use of Common Criteria unrealistic, in particular of the short term, both because of the certification-related costs and because of the expected limited availability of ITSEFs to perform the evaluation work, at least for the first EUDI Wallet deployments.

In the absence of a fully standardised certification scheme that meets the requirements of all implementations, many solutions may be considered, including the following:

- **Fixed-time evaluations**
  Such certification schemes exist in several Member States (France, Germany, Netherlands, Spain) and the methodology has been standardised (CEN-CENELEC EN 17640[16]). The certification scheme is based on a limited evaluation of products, focused specifically on vulnerability assessment, and could be used here.
- **SESIP**
  The IoT-oriented methodology, recently adopted as standard as CEN-CENELEC EN 17927[17], could also be used, in particular if the underlying platform has been assessed using the same methodology.
- **Common Criteria**
  Although EUCC is not suitable for all EUDI Wallet applications, it may be suitable for some implementations.

Another possibility would be to reference the high-level requirements defined in the Cyber Resilience Act, if it is adopted in time. These provide a good baseline for security, and compliance to them will be required in the near future anyway.

In addition, the amending Regulation requires the EUDI Wallet application to be released as open source, so approaches based on ethical hacking and bug bounties could be considered.

Considering all these possibilities, we propose to require an assessment of the conformity to the CRA's essential requirements (as defined in CRA's Annex I, ideally with a direct reference), complemented with some kind of vulnerability assessment at the appropriate level.

Cert-119	*Process*	The national certification scheme **shall** include for EUDI Wallet applications an assessment of their conformity to the essential cybersecurity requirements defined in the Annex I of the Cyber Resilience Act.
Cert-120	*Process*	The national certification scheme **shall** include for EUDI Wallet applications a vulnerability assessment at the appropriate level, including a review of the design and source code and some testing, which **can** take the form of a bug bounty program.

***Note**: If the CRA is not adopted in time to allow a reference to it, we can easily define an Annex with similar requirements in the implementing act.*

***Note**: We could extend these requirements to all software components, but this needs to be considered carefully.*

Assessment of the assumptions on platforms

The security of EUDI Wallets' implementation will depend not only on security of the components developed by the EUDI Wallet providers, but also on the security of the components used in the EUDI Wallet's operating environment (under the responsibility of the EUDI Wallet provider), and also on the security of the components used to run EUDI Wallet software on user devices (under the control of the end user).

[16] CEN-CENELEC EN 17640. Fixed-time cybersecurity evaluation methodology for ICT products (CEN-CENELE EN17640:2022), CEN-CENELEC, April 2023.
[17] CEN-CENELEC EN 17927. Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products (CEN-CENELEC EN 17927:2023), CEN-CENELEC, April 2023.

For the platform components under the responsibility of the EUDI Wallet provider, the suggestion is to require the EUDI Wallet provider to make available some kind of assurance documentation (certificates with report, audit report, etc.), and then to use a process inspired from the dependency analysis used in the European Scheme for Cloud Services (EUCS), described in Annex B.

Cert-121	*Process*	The national certification scheme **shall** require the EUDI Wallet provider to make available assurance documentation about the components that they use and provide to support the operation of EUDI Wallet components, and to submit this assurance documentation to a dependency analysis, as defined in Annex B.

Things are far more difficult for the components that are under the responsibility of the user. In this particular case, assurance documentation may not be available, so the assumptions need to be defined in terms that allow them to be enforced, and a justification needs to be provided that the enforcement mechanism is sufficient to ensure that the assumption is met.

Cert-122	*Process*	The national certification scheme **shall** require the EUDI Wallet provider to include for each assumption made on end user equipment a description of the mechanism that they use to enforce the assumption, as well as a justification that the mechanism is sufficient to ensure that the assumption is met.

Note: *This is a first proposal, to be discussed and enhanced.*

DETERMINATION ACTIVITIES (PROCESS-ORIENTED)

TBD

Development-related processes

TBD

Identity lifecycle-related processes

TBD

B DEPENDENCY ANALYSIS

***Note**: This is a copy of Annex B from the "Requirements for conformity assessment bodies certifying cloud services", currently being considered for adoption by CEN-CENELEC JTC13 WG3[18].This is provided as an example, and we need to define how we want to harmonise these requirements.*

The objective of the dependency analysis is to verify that the assurance documentation (assurance reports, certificates) available for the subservices operated by internal or external subservice organisations used by the client in the operation of its cloud service are adequate.

For every subservice that has been handled with the carve-out method, the basis for this dependency analysis is the risk assessment of the subservice performed by the client.

The evaluation team shall determine whether the assurance documentation available for a given subservice is adequate to provide assurance corresponding to the targeted evaluation level.

ASSESSING THE AVAILABILITY OF ASSURANCE DOCUMENTATION

Evaluators shall list the assurance documentation available for every relevant subservice. Then, evaluators shall assess the overall relevance of each assurance documentation for the dependency review.

The following elements shall be considered in the analysis:

a) about the assurance documentation itself:
  1) type of assurance documentation, with all required details;

***Example**: Examples for such documents could be certificates according to EN ISO/IEC 27001 or Type 1 or Type 2 for an ISAE report.*

  2) period covered or period of validity;

***Note:** Period may be complemented with bridge letter or similar statements.*

***Note:** Bridge letter is a document made available by a subservice organization to cover a period of time between the reporting period end date of the current ISAE report and the release of a new ISAE report.*

  3) applicable framework (e.g. existing standard or private framework);
  4) inclusion of a mapping to EUCS in the assurance documentation;
b) about the assurance report issuer's professional competence and impartiality:
  1) name of the CB or evaluation organization, if available, name of the evaluator lead;
  2) evidence of the CB/evaluation organization's and the evaluator's competence (e.g. accreditation, personal certification, etc.);

[18] CEN/CLC/JTC 13/WG 3 – Working group on Cybersecurity and Data protection: Security evaluation and assessment

3) evidence of the CB/evaluation organization's and the evaluator's impartiality (e.g. accreditation, etc.).

ASSESSING ASSURANCE RELATED TO INDIVIDUAL REQUIREMENTS

Evaluators shall verify that the assurance documentation available for the subservice is adequate to determine that the subservice provider meets the expectations of the client relative to the certification scheme's individual requirements.

This assessment shall be performed for every relevant subservice, and then for every security requirement for which the client has declared to rely partially or fully on the assurance provided by the subservice provider, by formulating an assumption on the subservice's control.

The evaluation team shall for each such assumption determine whether or not the assurance provided in the available assurance documentation is adequate.

There are several ways to reach a conclusion that the assurance is adequate:

a) the required information is available with the expected assurance level in the assurance documentation;
b) the information available in the assurance documentation does not cover the full scope of the requirement, but additional controls implemented by the subservice provider or compensating controls (i.e.: internal control that reduces the risk of an existing or potential control weakness) implemented by the client allow the evaluators to determine that the information is adequate;
c) the information available in the assurance documentation does not offer the expected level of assurance but the controls implemented by the client to assess and monitor the subservice provider allow the evaluators to determine that the information is adequate.

Finally, if the assurance documentation mentions nonconformities on the controls used to meet an assumption, the corrective measures proposed and implemented by the subservice provider and reviewed by its evaluators shall be adequate to guarantee that the assumption is indeed met.

CERTIFIED SUBSERVICES

When a subservice has been certified in a certification scheme recognized by the targeted certification scheme, the processes defined above shall be simplified:

a) the evaluator's competence and impartiality does not need to be assessed;
b) the report can be considered as being fully compliant with the rules of the certification scheme for the assurance level of the report;
c) no mapping to the certification scheme's security requirements is needed.

If the certification scheme includes specific requirements for composition, and if the service and its subservice both satisfy these requirements, the assessment may be simplified further.

C ACCEPTANCE CRITERIA FOR ASSURANCE INFORMATION

***NOTE**: We first need to agree on the principles of the content of this annex, before to move on to the more detailed definition of the criteria*

Criteria need to be defined in order to clarify how to consider assurance documentation from specific conformity assessment schemes, or other categories of assurance documentation.

For each scheme or category considered, the acceptance criteria shall define:

- Under which conditions the documentation may be accepted, and with which level of confidence;
- Which parts of the document or which requirements covered by the documents can be accepted as evidence;
- Conditions on the validity of the assurance documentation.

Note that these criteria also apply to certificates used in composition, and that the conditions of validity also cover the expiration date of certificates, and the obligation to maintain and renew certificates on which EUDI Wallets certification depends.

D SURVEILLANCE AND COMPLIANCE MONITORING

Following an EUDI Wallet's initial certification, the certification body and the other parties need to perform activities to ensure continued compliance to the scheme's requirement.

These activities are defined hereunder, and they may include surveillance activities as well as conformity assessment activities, for instance in the context of special evaluations.

CERTIFICATION LIFECYCLE

EUDI Wallet versioning

An EUDI Wallet is made of several components, running on different platforms, which may evolve in different ways, using different tools, which has two consequences:

- The main application has to ensure that the versions of the different components are consistent before performing any operation.
- The number of updates of an EUDI Wallet may be quite significant, with many of them impacting security to various degrees.

In order to provide guarantees in terms of security, and also as support to the integrity and authenticity verification of EUDI Wallets required in Article 5a(4)(a), we therefore need specific checks to be done, and they will have to be enforced by the scheme:

Cert-123	*Functional*	The national certification scheme **shall** require EUDI Wallet implementations to include consistency checks between the various components of the EUDI Wallet to be performed before conducting operations on the EUDI Wallet.
Cert-124	*Functional*	The national certification scheme **shall** require EUDI Wallet implementations to include measures to ensure that the version of the EUDI Wallet that is being used is currently certified.

Versioning and certificates

In order to satisfy the requirements above, the EUDI Wallet providers need to maintain an up-to-date list of versions that are currently covered by the certification. In particular, they need to ensure that versions that include an unmitigated and impactful vulnerability are not included.

There are two main ways to achieve this:

- Define a "patch management" mechanism at the scheme level (like in the EUCC), issue a new certificate for each version, and cancel certificates that are not up-to-date.
- Require the EUDI Wallet provider to define a version management policy and related procedures, to maintain such a list of "acceptable" versions.

The first solution has been designed for slowly evolving products, but it would not be suitable for products that are updated monthly or more frequently, as we expect from EUDI Wallets. The focus is therefore on the second option.

The principle for this second option is as follows:

- The EUDI Wallet provider needs to have a version management process that includes the notion of certification.
- The EUDI Wallet provider needs to include in all relevant components an update mechanism, supported by an appropriate update service and processes.
- The CB needs to evaluate the version management process and all the update-related elements during the initial evaluation.
- The CB needs to evaluate the operating effectiveness of the version management processes and update processes regularly in surveillance evaluations.

This represents quite a departure from typical product certification schemes, which reflects the more dynamic nature of such complex composite products, as well as the increasing importance of product maintenance processes for cybersecurity.

Note that the addition of regular surveillance evaluations will also offer an opportunity to include other processes, such as vulnerability management, in the scope of surveillance, reducing further the required interactions between the EUDI Wallet provider and the CA throughout the year.

Certification schedule

The proposal would here be to have a 4-year cycle, as follows, starting from Year 0, which is the year when the certificate is first issued:

Time	Eval. type	Activities
Year 0	Initial	• Full evaluation of the product, including vulnerability assessment ○ Including an update feature on each component • Evaluation of the maintenance processes, without operating effectiveness • Issuing of the certificate and start of the 4-year cycle.
Year 1	Surveillance	• Evaluation of the operating effectiveness of maintenance processes ○ At least version control, update, vulnerability management • Evaluation of changes impacting the security of the product
Year 2	Surveillance	• Vulnerability assessment of the full solution • Evaluation of the operating effectiveness of maintenance processes ○ At least version control, update, vulnerability management • Evaluation of changes impacting the security of the product
Year 3	Surveillance	• Evaluation of the operating effectiveness of maintenance processes ○ At least version control, update, vulnerability management • Evaluation of changes impacting the security of the product
Year 4	Recertification	• Full evaluation of the product, including vulnerability assessment ○ Simplified evaluation for features/processes that have not evolved ○ Including an update feature on each component • Evaluation of the maintenance processes, including operating effectiveness

Table 1: A full 4-year evaluation cycle

The four-year cycle includes three main types of activities:

- the evaluation of the product itself (in blue), including the evaluation of its changes over time;
- the evaluation of the maintenance processes, including the validation of their suitability (in dark red) and the verification of their operating effectiveness (in orange);
- the vulnerability assessments explicitly required in the regulation every two years (in green)

These activities are all classical components of product evaluations, although processes are typically related to production rather than maintenance. Operating effectiveness of processes is typically limited in scope in product security certification, but often covered by specific schemes (like for instance GSMA's SAS schemes).

***Note**: The schedule is a 4-year schedule because it matches the requirement of a vulnerability assessment every two years. The recommended duration of certificates is 5 years, which gives an opportunity to fix issues that could arise during the recertification evaluation without getting in trouble with the validity of the certificate.*

In addition, schemes would need to define a threshold on the nature or impact of changes to the EUDI Wallet that would trigger a mandatory special evaluation to assess the conformity of the changes performed, rather than wait for the next surveillance evaluation.

Requirements related to maintenance have already been defined in section 3.19, Certificate maintenance. In order to follow the schedule above, they need to be reinforced:

Cert-125	*Functional*	The national certification scheme **shall** refer to functional requirements on update mechanisms for every software component of an EUDI Wallet.
Cert-126	*Process*	The national certification scheme **shall** require in the initial evaluation the validation of the suitability and existence of maintenance processes, including at least version management, update management and vulnerability management.
Cert-127	*Process*	The national certification scheme **shall** require an annual surveillance evaluation including at least the verification of the operating effectiveness of the maintenance processes, including at least version management, update management and vulnerability management.
Cert-128	*Process*	The national certification scheme **shall** define a process for managing the changes in a certified EUDI Wallet, including a subprocess to decide whether a given change should be covered by a special evaluation or by the verification of the operating effectiveness of the maintenance processes.

***Note**: The important thing is here to establish that most updates are to be handled without recertifying the wallet, but only by regular assessment of maintenance processes. The details can be worked out in the national schemes.*

SURVEILLANCE ACTIVITIES

There are no specific requirements for surveillance activities for the certification scheme (*i.e.*, surveillance of the operation of the scheme), because it is likely that at least some national certification schemes will not issue enough certificates to establish a surveillance process.

***NOTE**: Surveillance activities are often based on comparison between CBs in a scheme, re-examination of a sample of certified products/service, but it is not clear how to do this on schemes that have a single CB and ca single certificate*

E COMPETENCIES

TBD

F RECAP OF REQUIREMENTS

Nr.	Category	Requirement	Corresponding EPIC	Page nr.
Cert-1	*General*	Member States **shall** establish national certification schemes that cover both the cybersecurity and non-cybersecurity aspects as specified in Article 5c(3).	EPIC 55	10
Cert-2	*General*	Member States **shall** consider the use of available and applicable EU cybersecurity certification schemes in their national schemes for the requirements that can be covered with these schemes.	EPIC 55	10
Cert-3	*Process*	The certificates of conformity EUDI Wallets with the requirements of the Regulation, issued under these national schemes **shall** have a validity that does not exceed 5 years.	EPIC 55	10
Cert-4	*Process*	The (national) certification schemes that cover cybersecurity requirements **shall** require performance of a vulnerability assessment activity at least every two years.	EPIC 55	10
Cert-5	*Process*	The national certification scheme **shall** require EUDI Wallet services to define and implement a process to evaluate the severity and potential impact of a vulnerability, and to design and implement a remediation plan in a timely manner.	EPIC 55	10
Cert-6	*Process*	The national certification schemes **shall** require cancellation of certificates if an identified vulnerability has not been remedied commensurately to its severity and potential impact in a timely manner.	EPIC 55	11
Cert-7	*Process*	Conformity assessment bodies issuing certificates for the EUDI Wallets **shall** be conformity assessment body as defined in point 13 of Article 2, point 13, of Regulation (EC) No 765/2008, which is accredited to EN ISO/IEC 17065 in accordance with that Regulation as competent to carry out certification of an EUDI Wallet.	EPIC 55	11
Cert-8	*Process*	The national certification schemes **should** define the parameters required to perform the accreditation of CBs, and in particular, the competence requirements and an evaluation process.	EPIC 55	11
Cert-9	*Functional*	The national certification scheme shall refer to functional requirements on the request operation on PID and EAA.	TBD	13

Cert-10	*Functional*	The national certification scheme **shall** define functional requirements on the obtain operation on PID and EAA.	TBD	13
Cert-11	*Functional*	The national certification scheme **shall** refer to functional requirements on the select operation on PID and EAA.	TBD	13
Cert-12	*Functional*	The national certification scheme **shall** refer to functional requirements on the combine operation on PID and EAA.	TBD	13
Cert-13	*Functional*	The national certification scheme **shall** refer to functional requirements on the store operation on PID and EAA.	TBD	13
Cert-14	*Functional*	The national certification scheme **shall** refer to functional requirements on the delete operation on PID and EAA.	TBD	13
Cert-15	*Functional*	The national certification scheme **shall** refer to functional requirements on the share operation on PID and EAA.	TBD	13
Cert-16	*Functional*	The national certification scheme **shall** refer to functional requirements on the present operation on PID and EAA.	TBD	13
Cert-17	*Functional*	The national certification scheme **shall** refer to functional requirements on the online and offline authentication from an EUDI Wallet to relying parties based on PID and EAA.	EPIC 06	13
Cert-18	*Functional*	The national certification scheme **shall** refer to functional requirements on the selective disclosure of PID and EAA during their processing.	EPIC 1, 2, 3, 4	14
Cert-19	*Functional*	The national certification scheme **shall** refer to functional requirements about the generation of pseudonyms.	EPIC 11	14
Cert-20	*Functional*	The national certification scheme **shall** refer to functional requirements about the encryption and storage of pseudonyms within EUDI Wallets.	EPIC 11	14
Cert-21	*Functional*	The national certification scheme **shall** refer to functional requirements about the authentication of another EUDI Wallet.	EPIC 30	14
Cert-22	*Functional*	The national certification scheme **shall** refer to functional requirements about the authentication to another EUDI Wallet.	EPIC 30	14
Cert-23	*Functional*	The national certification scheme **shall** refer to functional requirements about receiving and sharing of PID and EAA between two EUDI Wallets.	EPIC 30	14
Cert-24	*Functional*	The national certification scheme **shall** refer to functional requirements about a log of all transactions carried out through an EUDI Wallet.	EPIC 11	15

Cert-25	*Functional*	The national certification scheme **shall** refer to functional requirements about a common dashboard to access the log of transactions carried out through an EUDI Wallet.	EPIC 19	15
Cert-26	*Functional*	The national certification scheme **shall** refer to functional requirements about viewing an up-to-date list of relying parties with whom the user has established a connection through an EUDI Wallet.	EPIC 19	15
Cert-27	*Functional*	The national certification scheme **shall** refer to functional requirements about viewing all data exchanged with relying parties with whom the user has established a connection through an EUDI Wallet.	EPIC 19	15
Cert-28	*Functional*	The national certification scheme **shall** refer to functional requirements about requesting the deletion of data to a relying party.	EPIC 48	15
Cert-29	*Functional*	The national certification scheme **shall** refer to functional requirements about the ease of requesting the deletion of data to a relying party.	EPIC 48	15
Cert-30	*Functional*	The national certification scheme **shall** refer to functional requirements about reporting a relying party to a national data protection authority where an allegedly unlawful or suspicious request of data is received from that relying party.	EPIC 50	15
Cert-31	*Functional*	The national certification scheme **shall** refer to functional requirements about the ease of reporting a relying party to a national data protection authority where an allegedly unlawful or suspicious request of data is received from that relying party.	EPIC 50	15
Cert-32	*Functional*	The national certification scheme **shall** refer to functional requirements about signing by means of qualified electronic signatures.	EPIC 16, 37	15
Cert-33	*Functional*	The national certification scheme **shall** refer to functional requirements about sealing by means of qualified electronic seals.	EPIC 16, 37	15
Cert-34	*Functional*	The national certification scheme **shall** refer to functional requirements about downloading users' data, EAA and configurations.	EPIC 33	16
Cert-35	*Functional*	The national certification scheme **shall** refer to functional requirements about exercising a user's right to data portability.	EPIC 34	16
Cert-36	*Functional*	The national certification scheme **shall** refer to functional requirements about conformity to those common protocols and interfaces defined in the reference standards, technical	EPIC 06, 07,08,09,10,12,16,18, 19,20, 21, 22,23,24,28,29,30,31,35,37,38,46	17

		specifications and procedures established by means of the implementing acts adopted pursuant to Art.5a(24).	,47,48,49,50,51, 42	
Cert-37	*Functional*	The national certification scheme **shall** refer to functional requirements about not providing any information to trust service providers of EAA about the use of these attributes.	EPIC 1,2,3,4	18
Cert-38	*Functional*	The national certification scheme **shall** refer to functional requirements about the validation of the identity of relying parties using a common mechanism for the identification and authentication of relying parties.	EPIC 27	18
Cert-39	*Functional*	The national certification scheme **shall** refer to functional requirements about the mechanisms used to inform a party that they have the permission to access an EAA.	EPIC 43	18
Cert-40	*Functional*	The national certification scheme **shall** refer to functional requirements about how the eID scheme under which the EUDIW is provided ensures that the PID available from the electronic identification scheme, under which the EUDI Wallet is provided, uniquely represents the user of the EUDI Wallet.	EPIC 10, 23	18
Cert-41	*Functional*	The national certification scheme **shall** refer to functional requirements about the availability of signature by means of qualified electronic signatures to all natural persons by default.	EPIC 16	19
Cert-42	*Functional*	The national certification scheme **shall** refer to functional requirements about the availability of signature by means of qualified electronic signatures to all natural persons free-of-charge.	EPIC 16	19
Cert-43	*Functional*	The national certification scheme **shall** refer to functional requirements about the effective provision by Member States of mechanisms for the verification of the authenticity and validity of an EUDI Wallet.	EPIC 9, 38	19
Cert-44	*Functional*	The national certification scheme **shall** refer to functional requirements about the effective provision by Member States of mechanisms for the verification of the authenticity and validity of an EUDI Wallet free-of-charge.	EPIC 9, 38	19
Cert-45	*Functional*	The national certification scheme **shall** refer to functional requirements about the effective provision by Member States of mechanisms for the verification of the authenticity and validity of the identity of registered relying parties.	EPIC 6, 27	20
Cert-46	*Functional*	The national certification scheme **shall** refer to functional requirements about the effective provision by Member States of mechanisms for the verification of the authenticity and validity of the identity of registered relying parties free-of-charge.	EPIC 6, 27	20

Cert-47	*Functional*	The national certification scheme **shall** refer to functional requirements on the logical separation between personal data relating to the provision of an EUDI Wallet and any other data held by the EUDI Wallet provider.	TBD	20
Cert-48	*Process*	The national certification scheme **shall** refer to requirements about human resource management policies and procedures, including at least requirements on expertise, reliability, experience, and qualifications of personnel about appropriate training regarding security rules, and appropriate management procedures.	EPIC 55	23
Cert-49	*Functional*	The national certification scheme **shall** refer to requirements about the information made available to any person seeking to use an EUDI Wallet of the precise terms and conditions regarding the use of that service, including any limitations on its use, and about the availability of this information in a clear, comprehensive and easily accessible manner, in a publicly accessible space.	TBD	24
Cert-50	*Process*	The national certification scheme **shall** refer to requirements about the definition and implementation of policies and procedures related to the management of risks related to the operation of an EUDI Wallet, including the identification and assessment of risks and the treatment of the identified risks.	EPIC 55	24
Cert-51	*Process*	The national certification scheme **shall** require notification to the CB of security breaches and disruptions within 24 hours of the incident.	EPIC 55	24
Cert-52	*Functional*	The national certification scheme **shall** refer to requirements about recording and keeping accessible for as long as necessary after the activities of the [provider of a certified EUDI Wallet] have ceased, all relevant information concerning data issued and received by the provider of a certified EUDI Wallet, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically.	TBD	25
Cert-53	*Process*	The national certification scheme **shall** define as object of certification a service that includes the provision and operation of EUDI Wallets.	EPIC 55	27
Cert-54	*Functional*	The national certification scheme **shall** require providers of certified EUDI Wallets to define and implement policies and procedures related to the management of changes.	TBD	28
Cert-55	*Functional*	The national certification scheme **shall** require providers of certified EUDI Wallets to define and implement policies and procedures related to the management of vulnerabilities.	TBD	28
Cert-56	*Process*	The national certification scheme **shall** include requirements for the providers of certified EUDI Wallets to notify the CB who	EPIC 55	28

		issued the certificate about the vulnerabilities and changes affecting the service they provide, based on criteria about the impact of the vulnerabilities and changes.		
Cert-57	*Process*	The national certification scheme owner **shall** be clearly identified and in charge of supervising the operations of the scheme. It **may** be the Art.46a(1) national supervisory body responsible for the supervision of the provision of an EUDI Wallet and of the electronic identification scheme used to provide an EUDI Wallet.	EPIC 55	29
Cert-58	*Process*	The national certification scheme **shall** be established and maintained in compliance with the implementing acts adopted pursuant to Art.5c(11).	EPIC 55	29
Cert-59	*Process*	The national certification scheme **shall** require the scheme owner to be in contact with the representative designed by the Member States to the EDICG, and to take utmost account of the opinions and recommendations issued by the EDICG.	EPIC 55	29
Cert-60	*Process*	The national certification scheme **shall** include the content recommended in section 6.5 of EN ISO/IEC 17067, unless otherwise specified in the following requirements.	EPIC 55	29
Cert-61	*Process*	The scope of the national certification scheme **shall** include the software components that implement the features of an EUDI Wallet.	EPIC 55	31
Cert-62	*Process*	The scope of the national certification scheme **shall** include the hardware and platforms on which are running the software components that implement the features of an EUDI Wallet, if they are provided by the EUDI Wallet provider and if they are required to achieve the desired assurance level for that software component.	EPIC 55	31
Cert-63	*Process*	The scope of the national certification scheme **shall** include the processes that support the provision of an EUDI Wallet, including the user on-boarding processes.	EPIC 55	31
Cert-64	*Process*	The national certification scheme **shall** be defined as a Type 6 scheme, as defined in EN ISO/IEC 17067, 5.3.7.	EPIC 55	31
Cert-65	*Process*	The national certification scheme **shall** mandate the use of standardized test suites for any referenced protocol or API for which a standardized test suite is available.	EPIC 55	32
Cert-66	*Process*	The national certification scheme **shall** define at least the following selection activity: Audit of the design and validation plan, as defined in Annex A.	EPIC 55	33

Cert-67	*Process*	The national certification scheme **shall** define at least the following attestation and licensing activities: issuing a certificate of conformity (V a) in EN ISO/IEC 17067 Table 1).	EPIC 55	34
Cert-68	*Process*	– The national certification scheme **shall** define at least the following surveillance activities: - surveillance evaluation of processes combined with random tests or inspections (Inspired from VI d) in EN ISO/IEC 17067 Table 1).	EPIC 55	34
Cert-69	*Process*	The national certification scheme **shall** include requirements related to minimal competences to be checked in accreditation, covering at least: – deep technical understanding of EUDI Wallet architectures, threats and risk management; – knowledge of security solutions available and of their properties, mapping them to the requirements of (EU) 2015/1502; – knowledge about the activities performed under certificates applied to components of the object of certification.	EPIC 55	35
Cert-70	*Process*	The national certification scheme **shall** define methods and procedures to be used by the conformity assessment bodies involved in the certification process.	EPIC 55	35
Cert-71	*Process*	The national certification scheme **shall** include the methods and procedures defined in the scope of A to the document.	EPIC 55	35
Cert-72	*Process*	The national certification scheme **shall** include requirements for the applicant for certification to provide to the CB the following information: – a description of the service to be certified, including a description of the EUDI Wallet and of the processes and systems used for the provision and support of the EUDI Wallet; – an analysis of the architecture of the service, together with a mapping of the generic risks for EUDI Wallets to the components of the architecture and a description of the measures taken to mitigate these risks; – a validation plan for the EUDI Wallet and associated eID scheme, which covers the components of the architecture described above at a level of assurance sufficient to mitigate the identified risks; – a complete list of the certificates and other assurance information used as evidence.	EPIC 55	36
Cert-73	*Process*	The scheme **shall** not use any mark of conformity different from the EU Digital Identity Wallet Trust Mark.	EPIC 55	37

Cert-74	*Process*	The scheme **shall** define how results are to be reported in the certification report.	EPIC 55	37
Cert-75	*Process*	The scheme **shall** require the CB to include in the certification report a summary of the preliminary audit of the audit and validation plan.	EPIC 55	37
Cert-76	*Process*	The national certification scheme **shall** mandate that the provider of a certified EUDI Wallet notifies its CB when a breach affects a certified EUDI Wallet, as defined in Article 5da(1).	EPIC 55	38
Cert-77	*Process*	The national certification scheme **shall** mandate that the provider of a certified EUDI Wallet defines and operates a vulnerability management policy.	EPIC 55	38
Cert-78	*Process*	The national certification scheme **shall** mandate the scheme owner to monitor the compliance of (a) the certification body with their obligations pursuant to regulation eIDAS2 and to this scheme; (b) the holders of a certification issued according to this scheme with their obligations pursuant to regulation eIDAS2 and to this scheme; (c) the certified EUDI Wallet(s) with the requirements set out in this scheme; (d) the assurance expressed in the certificate addressing the evolving threat landscape.	EPIC 55	38
Cert-79	*Process*	The national certification scheme **shall** mandate the scheme owner to perform its monitoring activities in particular on the basis of: (a) information coming from certification bodies, national accreditation bodies and relevant market surveillance authorities; (b) information resulting from its own or another authority’s audits and investigations; (c) complaints received.	EPIC 55	38
Cert-80	*Process*	The national certification scheme **shall** explicitly allow the scheme owner, that has sufficient reason to believe that a certified EUDI Wallet is no longer in compliance with this scheme or with regulation eIDAS2, to carry out investigations and make use of any monitoring powers set out in this scheme.	EPIC 55	38
Cert-81	*Process*	The national certification scheme **shall** mandate the scheme owner that identifies that an ongoing investigation concerns an EUDI Wallet that is certified by certification bodies established in other Member States, to inform thereof the scheme owner of the relevant Member States in order to collaborate in the investigations, where relevant, and to also notify the European Commission and the EDICG of the cross-border investigations and the subsequent results.	EPIC 55	39

Cert-82	*Process*	The national certification scheme **shall** limit access to EUDI Wallet providers that meet one of the conditions of Article 5a(2).	EPIC 55	39
Cert-83	*Process*	The scheme **shall** mandate the CB to notify the national supervisory body for EUDI Wallets of the issuance and cancelation of certificates on EUDI Wallets.	EPIC 55	39
Cert-84	*Process*	The national certification scheme **shall** define the maximal duration of certificates as five (5) years.	EPIC 55	40
Cert-85	*Process*	The national certification scheme **shall** mandate surveillance evaluations including at least a vulnerability assessment every two (2) years and following the schedule defined in Annex D.	EPIC 55	40
Cert-86	*Process*	The national certification scheme **shall** include provisions for the recertification of an EUDI Wallet, by performing a dedicated evaluation before the expiry of the initial certificate, which shall include at least a vulnerability assessment and an evaluation of the EUDI Wallet’s threat model.	EPIC 55	40
Cert-87	*Process*	The national certification scheme **shall** define a process for special evaluations, including a selection of activities to be performed to address the specific issue that triggered the recertification.	EPIC 55	40
Cert-88	*Process*	The national certification scheme **shall** define requirements for performing special evaluations within a defined period after the revision of the scheme, or after the release of new specifications or standards to which the EUDI Wallet must conform.	EPIC 55	40
Cert-89	*Process*	The national certification scheme **shall** require CBs to establish procedures to effectively lodge and handle complaints, including regular reporting to the scheme owner.	EPIC 55	41
Cert-90	*Process*	The national certification scheme **shall** define requirements on how providers of certified EUDI Wallets can make reference to the scheme, which **shall** at least include references to the amending Regulation requirements and the certification Implementing Act.	EPIC 55	41
Cert-91	*Process*	The national certification scheme **shall** require CBs to store records related to a certificate for at least five (5) years after the withdrawal or expiry of the certificate.	EPIC 55	41
Cert-92	*Process*	The national certification scheme **shall** include a requirement for all parties to ensure the security and protection of business secrets and other confidential information, including trade secrets, as well as preserving intellectual property rights, and take the necessary and appropriate technical and organisational measures.	EPIC 55	41

Cert-93	*Process*	The rules on management of vulnerabilities **shall** at least require compliance to the requirements of CRA's Annex I on vulnerability management.	EPIC 55	42
Cert-94	*Process*	The national certification scheme **shall** require all EUDI Wallet providers to make publicly available security information about their product, including at least: (a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the EUDI Wallet; (b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates; (c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers; (d) a reference to online repositories listing publicly disclosed vulnerabilities related to the EUDI Wallet and to any relevant cybersecurity advisories..	EPIC 55	43
Cert-95	*Process*	The national certification scheme **shall** define sampling rules allowing functional and security tests to be performed only on a sample of target EUDI Wallet components on a sample of target devices and including requirements for CBs to justify the selection of target components and devices.	EPIC 55	45
Cert-96	*Process*	The national certification scheme **shall** define a methodology to assess the acceptability of information assurance provided by the EUDI Wallet developer, including the provisions defined by the EUDI Wallets certification system, including at least the provisions defined in Annex B.	EPIC 55	46
Cert-97	*Process*	The national certification scheme **shall** define criteria for acceptability of information assurance provided by the EUDI Wallet developer, including the provisions defined by the EUDI Wallets certification system, including at least the criteria defined in Annex C.	EPIC 55	46
Cert-98	*Process*	The national certification scheme **shall** require that all complaints that have not been, or cannot, be resolved by the CB shall be addressed to the scheme owner.	EPIC 55	47
Cert-99	*Process*	The national certification scheme **shall** require CBs to undertake surveillance according to a CB-defined surveillance plan and the scheme **shall** define requirements for such surveillance and compliance monitoring, including the provisions defined by the EUDI Wallets certification system, including at least the requirements defined in Annex D.	EPIC 55	47
Cert-100	*Process*	The national certification scheme **shall** require providers of certified EUDI Wallets to notify their CB, without delay, of any	EPIC 55	48

		security breach that may have entirely or partially compromised their EUDI Wallet or its content.		
Cert-101	*Process*	The national certification scheme **shall** require CBs to notify the EUDI Wallet national authority of any security breach reported by providers of certified EUDI Wallets.	EPIC 55	48
Cert-102	*Process*	The national certification scheme **shall** require a CB to suspend without delay the certificate of an EUDI Wallet after the confirmation of a breach or compromise of the EUDI Wallet that affects their reliability or the reliability of other EUDI Wallets.	EPIC 55	48
Cert-103	*Process*	The national certification scheme **shall** require a CB to cancel the certificate of an EUDI Wallet that has been suspended following a breach or compromise that has not been remedied in a timely manner.	EPIC 55	48
Cert-104	*Process*	The national certification scheme **shall** require the scheme owner who subcontracts all or part of the operation of the scheme to another party to have a legally binding contract defining the duties and responsibilities of both parties.	EPIC 55	49
Cert-105	*Process*	The national certification scheme **shall** describe actions and responsibilities for situations where certification under the scheme is being claimed fraudulently.	EPIC 55	49
Cert-106	*Process*	The national certification scheme **shall** require the scheme owner to define a process for reviewing the operation of the scheme on a periodic basis in order to confirm its validity and to identify aspects requiring improvement, taking into account feedback from stakeholders.	EPIC 55	50
Cert-107	*Process*	The review of the national certification scheme **shall** include provisions for ensuring that the scheme requirements are being applied in a consistent manner.	EPIC 55	50
Cert-108	*Process*	The review of the national certification scheme **shall** at least consider the following: • – any requests for clarification related to the certification scheme requirements; • – feedback from stakeholders and other interested parties; • – responsiveness of the certification scheme owners to requests of information; • – the need for integrity programmes (e.g. validation audit or other checks)	EPIC 55	50
Cert-109	*Process*	The national certification scheme **shall** include provisions for monitoring reference documents and procedures for the evolution of the scheme's reference versions, including at least trial and transition periods.	EPIC 55	51

Cert-110	*Process*	The national certification scheme **shall** define a process for managing other changes in the scheme or in the national certification system.	EPIC 55	51
Cert-111	*Process*	A national certification scheme that is specialised for a given architecture **shall** include at least information about the architecture of the targeted EUDI Wallet architecture, a list of security functions associated to assurance levels and required security elements, a mapping of these functions to the components of the architecture, and a validation plan tailored to the EUDI Wallet's architecture.	EPIC 55	52
Cert-112	*Process*	The national certification scheme **shall** be specialised for a given architecture, or it shall include different sub-schemes, each specialised for a given architecture.	EPIC 55	52
Cert-113	*Process*	The national certification scheme **shall** define a selection function to audit the design of the EUDI Wallet and associated eID scheme, as well as the proposed validation plan covering this design.	EPIC 55	56
Cert-114	*Process*	The selection function defined in the national certification scheme **shall** require the EUDI Wallet provider to provide a detailed description of the EUDI Wallet and associated eID scheme, including at least information about the architecture of the EUDI Wallet, a list of security functions associated to assurance levels and required security elements, a mapping of these functions to the components of the architecture, and a validation plan tailored to the EUDI Wallet's architecture.	EPIC 55	56
Cert-115	*Process*	The national certification scheme **shall** require the audit of the design and validation plan to be based on the latest available risk registry for EUDI Wallets made available, complemented where needed by implementation-specific risks.	EPIC 55	57
Cert-116	*Process*	The national certification scheme **shall** require the evaluation of the WSCA with the EUCC European scheme, or if not available, with a National certification scheme based on Common Criteria.	EPIC 55	59
Cert-117	*Process*	The national certification scheme **shall** require the evaluation of the WSCA to include a vulnerability assessment at level AVA_VAN.5 unless it is duly justified that the security characteristics of the WSCA execution environment (including but not limited to the WSCD) allow to use a lower assessment level while keeping the same overall level of assurance.	EPIC 55	59
Cert-118	*Process*	The national certification scheme **shall** require the security target used for the evaluation of the WSCA to cover all security functions implemented by the WSCA.	EPIC 55	59
Cert-119	*Process*	The national certification scheme **shall** include for EUDI Wallet applications an assessment of their conformity to the essential	EPIC 55	60

		cybersecurity requirements defined in the Annex I of the Cyber Resilience Act.		
Cert-120	*Process*	The national certification scheme **shall** include for EUDI Wallet applications a vulnerability assessment at the appropriate level, including a review of the design and source code and some testing, which **can** take the form of a bug bounty program.	EPIC 55	60
Cert-121	*Process*	The national certification scheme **shall** require the EUDI Wallet provider to make available assurance documentation about the components that they use and provide to support the operation of EUDI Wallet components, and to submit this assurance documentation to a dependency analysis, as defined in Annex B.	EPIC 55	61
Cert-122	*Process*	The national certification scheme **shall** require the EUDI Wallet provider to include for each assumption made on end user equipment a description of the mechanism that they use to enforce the assumption, as well as a justification that the mechanism is sufficient to ensure that the assumption is met.	EPIC 55	61
Cert-123	*Functional*	The national certification scheme **shall** require EUDI Wallet implementations to include consistency checks between the various components of the EUDI Wallet to be performed before conducting operations on the EUDI Wallet.	EPIC 55	65
Cert-124	*Functional*	The national certification scheme **shall** require EUDI Wallet implementations to include measures to ensure that the version of the EUDI Wallet that is being used is currently certified.	EPIC 55	65
Cert-125	*Functional*	The national certification scheme **shall** refer to functional requirements on update mechanisms for every software component of an EUDI Wallet.	EPIC 55	67
Cert-126	*Process*	The national certification scheme **shall** require in the initial evaluation the validation of the suitability and existence of maintenance processes, including at least version management, update management and vulnerability management.	EPIC 55	67
Cert-127	*Process*	The national certification scheme **shall** require an annual surveillance evaluation including at least the verification of the operating effectiveness of the maintenance processes, including at least version management, update management and vulnerability management.	EPIC 55	67
Cert-128	*Process*	The national certification scheme **shall** define a process for managing the changes in a certified EUDI Wallet, including a subprocess to decide whether a given change should be covered by a special evaluation or by the verification of the operating effectiveness of the maintenance processes.	EPIC 55	67

XX-00-00-000-XX-X

ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector, and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 000-00-0000-000-0
doi: 0000.0000/000000