

WZ-03-01

Organisational and technical requirements  
for providers of services supporting the eID  
system

**VERSION - 1.01**

2026.06.05

|                                                  |                                                                  |
|--------------------------------------------------|------------------------------------------------------------------|
| <b>Document reference</b>                        | WZ-03-01                                                         |
| <b>Version</b>                                   | V 1.01 (2026-06)                                                 |
| <b>Status</b>                                    | FINAL                                                            |
| <b>Date</b>                                      | 05.06.2026                                                       |
| <b>Document type</b>                             | Certification Scheme — Scheme Specification (ISO/IEC 17067)      |
| <b>Parent framework</b>                          | GP-03 eID Certification Scheme                                   |
| <b>Scheme Owner</b>                              | Republic of Poland / Minister of Digital Affairs                 |
| <b>Certification target</b>                      | eID system                                                       |
| <b>Primary audience</b>                          | EUDI Wallet Provider                                             |
| <b>Secondary audience</b>                        | Conformity Assessment Bodies (CABs) accredited according to G-05 |
| <b>Assurance level &lt;identity proofing&gt;</b> | High (CIR (EU) 2015/1502)                                        |
| <b>Subsidiary Documents</b>                      | WP-03, WM-03 series                                              |

# Table of content

|       |                                                                                                                                                         |    |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1     | SCOPE .....                                                                                                                                             | 5  |
| 2     | LEGAL BASIS.....                                                                                                                                        | 7  |
| 3     | GENERAL PRINCIPLES .....                                                                                                                                | 11 |
| 3.1   | Proportionality to Risk .....                                                                                                                           | 11 |
| 3.2   | Auditability .....                                                                                                                                      | 11 |
| 3.3   | National Law .....                                                                                                                                      | 11 |
| 3.4   | Normative Language.....                                                                                                                                 | 11 |
| 3.5   | Relationship with ISO/IEC 27001 .....                                                                                                                   | 12 |
| 4     | LEGAL REQUIREMENTS .....                                                                                                                                | 13 |
| 4.1   | Requirements Derived from CIR (EU) 2015/1502.....                                                                                                       | 13 |
| 4.1.1 | General Provisions (Section 2.4.1).....                                                                                                                 | 13 |
| 4.1.2 | Published Notices and User Information (Section 2.4.2).....                                                                                             | 14 |
| 4.1.3 | Information Security Management (Section 2.4.3) .....                                                                                                   | 14 |
| 4.1.4 | Record Keeping (Section 2.4.4).....                                                                                                                     | 14 |
| 4.1.5 | Facilities and Staff (Section 2.4.5).....                                                                                                               | 15 |
| 4.1.6 | Technical Controls (Section 2.4.6) .....                                                                                                                | 15 |
| 4.1.7 | Compliance and Audit (Section 2.4.7).....                                                                                                               | 16 |
| 4.2   | Requirements Derived from CIR (EU) 2024/2690.....                                                                                                       | 17 |
| 4.2.1 | Policy on Security of Network and Information Systems (Annex, Section 1).....                                                                           | 17 |
| 4.2.2 | Risk Management (Annex, Section 2).....                                                                                                                 | 18 |
| 4.2.3 | Incident Handling (Annex, Section 3).....                                                                                                               | 18 |
| 4.2.4 | Business Continuity and Crisis Management (Annex, Section 4).....                                                                                       | 19 |
| 4.2.5 | Supply Chain Security (Annex, Section 5).....                                                                                                           | 19 |
| 4.2.6 | Security in Acquisition, Development and Maintenance (Annex, Section 6) .....                                                                           | 19 |
| 4.2.7 | Effectiveness Assessment, Cyber Hygiene, Cryptography, Human Resources, Access Control, Asset Management, Physical Security (Annex, Sections 7–13)..... | 20 |
| 4.3   | Requirements Derived from CIR (EU) 2024/2981.....                                                                                                       | 23 |
| 4.3.1 | Risk Assessment and Security Criteria (Articles 4 and 8).....                                                                                           | 23 |
| 4.3.2 | Incident and Vulnerability Management (Article 5).....                                                                                                  | 23 |
| 4.3.3 | Public Information (Article 8(5) and Annex V).....                                                                                                      | 24 |
| 4.3.4 | Record Retention (Article 19).....                                                                                                                      | 25 |
| 4.4   | Requirements Derived from CIR (EU) 2025/847 .....                                                                                                       | 26 |
| 4.4.1 | Organisational requirements in case of security breach of EUDI Wallet .....                                                                             | 26 |
| 5     | PROVISIONS.....                                                                                                                                         | 28 |
| 5.1   | General and Scheme-Specific Provisions.....                                                                                                             | 28 |
| 5.1.1 | Information Security Management System.....                                                                                                             | 28 |
| 5.1.2 | Legal Entity Status and Financial Capacity .....                                                                                                        | 29 |
| 5.1.3 | Termination Planning .....                                                                                                                              | 31 |
| 5.1.4 | Published Notices and Public Information.....                                                                                                           | 31 |
| 5.1.5 | Certification Body Notification.....                                                                                                                    | 32 |
| 5.2   | Organisational Controls .....                                                                                                                           | 34 |
| 5.2.1 | Information Security Policy .....                                                                                                                       | 34 |
| 5.2.2 | Information Security Roles and Responsibilities .....                                                                                                   | 34 |
| 5.2.3 | Risk Management .....                                                                                                                                   | 35 |

|                                                                |                                                                  |    |
|----------------------------------------------------------------|------------------------------------------------------------------|----|
| 5.2.4                                                          | Supplier Relationships.....                                      | 37 |
| 5.2.5                                                          | Asset Management .....                                           | 39 |
| 5.2.6                                                          | Access Control.....                                              | 40 |
| 5.2.7                                                          | Incident Management.....                                         | 41 |
| 5.2.8                                                          | Vulnerability Management and Disclosure .....                    | 43 |
| 5.2.9                                                          | Business Continuity Management .....                             | 45 |
| 5.2.10                                                         | Compliance, Audit, and Independent Review .....                  | 47 |
| 5.2.11                                                         | Record keeping .....                                             | 47 |
| 5.3                                                            | People Controls .....                                            | 48 |
| 5.3.1                                                          | Screening .....                                                  | 48 |
| 5.3.2                                                          | Terms and Conditions of Employment.....                          | 49 |
| 5.3.3                                                          | Responsibilities After Termination or Change of Employment ..... | 49 |
| 5.3.4                                                          | Information Security Awareness, Education and Training.....      | 49 |
| 5.3.5                                                          | Disciplinary Process.....                                        | 50 |
| 5.4                                                            | Physical Controls.....                                           | 51 |
| 5.4.1                                                          | Physical Security Perimeters and Entry Controls.....             | 51 |
| 5.4.2                                                          | Environmental Protection.....                                    | 51 |
| 5.4.3                                                          | Supporting Utilities.....                                        | 51 |
| 5.4.4                                                          | Storage Media .....                                              | 52 |
| 5.5                                                            | Technological Controls.....                                      | 54 |
| 5.5.1                                                          | Privileged Access and Identity Management.....                   | 54 |
| 5.5.2                                                          | Authentication .....                                             | 55 |
| 5.5.3                                                          | Protection Against Malware .....                                 | 55 |
| 5.5.4                                                          | Logging and Monitoring .....                                     | 56 |
| 5.5.5                                                          | Network Security .....                                           | 57 |
| 5.5.6                                                          | Segregation of Networks.....                                     | 58 |
| 5.5.7                                                          | Configuration Management.....                                    | 59 |
| 5.5.8                                                          | Change Management .....                                          | 59 |
| 5.5.9                                                          | Patch Management.....                                            | 60 |
| 5.5.10                                                         | Cryptography and Key Management.....                             | 60 |
| 5.5.11                                                         | Secure Acquisition, Development and Maintenance.....             | 61 |
| 5.5.12                                                         | Security Testing .....                                           | 62 |
| ANNEX A (INFORMATIVE) — PROVISION-TO-REQUIREMENT MAPPING ..... |                                                                  | 63 |

# 1 Scope

- 1 The present document specifies the organisational and technical requirements applicable to eID-related services incorporated by the Wallet Provider, for the purposes of certification under the eID Certification Scheme (GP-03).
- 2 WZ-03-01 is one of the subsidiary documents of GP-03 and constitutes the management system requirements (WZ-series) applicable to the Wallet Provider role. WZ-03-01 is a role-specific adoption of WZ-03-03 (Organisational and Technical Requirements for EUDI Wallet Providers), which establishes the baseline requirements applicable to all services of the EUDI Wallet provider. The Wallet Provider shall comply with both WZ-03-01 (in relation to eID related services themselves and WZ-03-03 (in relation to all services provided in the EUDI Wallet ecosystem. It sets out the organisational, governance, information security and technical controls that Wallet Provider shall implement and maintain. The process-specific requirements for PID registration and lifecycle, wallet unit registration, and authentication are specified in the WP-03 series. The cybersecurity audit frameworks applicable to CABs evaluating Wallet Provider are specified in the WM-03 series.
- 3 The structure of Section 6 of this document is aligned with the control themes of ISO/IEC 27001:2022, Annex A, to facilitate integration with existing information security management systems and to support a consistent approach to auditing.
- 4 The following are outside the scope of this document:
  - I. Requirements applicable to PID Provider — see WZ-03-02.
  - II. Requirements specific to EUDI Wallet Provider role under Article 5c of eIDAS — see WZ-03-03.
  - III. Process-specific requirements for PID enrolment and lifecycle — see WP-03-01.
  - IV. Process-specific requirements for wallet unit registration — see WP-03-02.
  - V. Requirements for eID means and authentication — see WP-03-03.
  - VI. Cybersecurity certification of the wallet solution as a product — see GP-02.

VII. Functional conformity assessment of the wallet — see GP-01.

## 2 Legal Basis

5 This document is based on the following legal instruments:

- I. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, as amended by Regulation (EU) 2024/1183 (hereinafter “eIDAS”), in particular Article 8 thereof.
- II. Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on 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 (hereinafter “CIR (EU) 2015/1502”), in particular Section 2.4 of the Annex thereto.
- III. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (hereinafter “NIS 2 Directive”), in particular Article 21(2) thereof.
- IV. Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures (hereinafter “CIR (EU) 2024/2690”), in particular the Annex thereto.
- V. Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 as regards the certification of European Digital Identity Wallets (hereinafter “CIR (EU) 2024/2981”), Articles 4, 5, 8 and 19 thereof and Annexes I and V thereto.
- VI. Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules as regards person identification data issued to European Digital Identity Wallets (hereinafter “CIR (EU) 2024/2977”), in particular Articles 3 and 5 thereof.
- VII. Polish Act on the mObywatel Application (Dz.U. 2023 poz. 1234, z późn. zm.).

- VIII. Polish Cybersecurity Act (Dz.U. 2018 poz. 1560, z późn. zm.), implementing the NIS 2 Directive in Polish law.
- IX. Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 as regards the integrity and core functionalities of European Digital Identity Wallets (hereinafter “CIR (EU) 2024/2979”), published in the Official Journal of the European Union on 4 December 2024, entered into force on 24 December 2024; in particular Articles 3, 4, 5, 6, 7, 9 and 13 thereof.
- X. Commission Implementing Regulation (EU) 2025/849 of 28 February 2025 amending Implementing Regulations (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 and (EU) 2024/2982 as regards applicable standards and specifications (hereinafter “CIR (EU) 2025/849”). This amending regulation updates references to technical standards and specifications in the implementing regulations to align them with ARF v2.8.0 and the latest ETSI and ISO standards.
- XI. European Digital Identity Cooperation Group (EDICG), Architecture and Reference Framework (ARF) v2.8.0 (current version as of April 2026), maintained under Commission Recommendation (EU) 2021/946 of 3 June 2021 (OJ L 210, 14.6.2021, p. 51) (hereinafter “ARF v2.8.0”). The ARF is an informative technical reference document; it is not legally binding, but specifies the data models, protocols and interoperability requirements referenced in CIR (EU) 2024/2979 and CIR (EU) 2024/2977. The ARF is maintained by the EDICG and updated continuously; the applicable version at the time of certification shall be used.
- XII. ETSI TS 119 461 v2.1.1 (February 2025) — Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects (hereinafter “ETSI TS 119 461”). This standard is referenced in the eIDAS implementing acts on identity verification and defines the technical requirements for remote and in-person identity proofing at assurance level High, including the verification of identity evidence and liveness detection requirements.
- XIII. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with



regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”), in particular: Article 5 (principles relating to processing of personal data); Article 25 (data protection by design and by default); Article 32 (security of processing); Article 17 (right to erasure); Article 34 (communication of a personal data breach to the data subject); and Article 83 (general conditions for imposing administrative fines).

- XIV. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (hereinafter “Cyber Resilience Act” or “CRA”), entered into force on 10 December 2024; in particular Annex I thereto (essential cybersecurity requirements for products with digital elements), as incorporated by reference in Article 5(7) of CIR (EU) 2024/2981 and Article 5(3) of CIR (EU) 2024/2981 (reference to EN ISO/IEC 30111:2019 and CRA Annex I for vulnerability handling).
- XV. ISO/IEC 18013-5:2021 — Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application (hereinafter “ISO/IEC 18013-5”). This standard specifies the mdoc credential format and the mDL presentation protocol, which is one of the two mandatory data formats for PID issuance under the Annex to CIR (EU) 2024/2977 as updated by CIR (EU) 2025/849.
- XVI. ISO/IEC 29115:2013 — Information technology — Security techniques — Entity authentication assurance framework (hereinafter “ISO/IEC 29115”). This standard defines the four levels of entity authentication assurance (LoA 1–4) and provides the international normative basis for the assurance level High requirements implemented in CIR (EU) 2015/1502, Section 2.3.
- XVII. OpenID Foundation, OpenID for Verifiable Credential Issuance (OID4VCI) — draft specification referenced in ARF v2.8.0 and CIR (EU) 2024/2979 as the standard protocol for issuance of PID and electronic attestations of attributes to EUDI Wallet units; and OpenID for Verifiable Presentations (OID4VP) — draft specification referenced in ARF v2.8.0 and CIR (EU) 2024/2979 as the standard protocol for presentation of PID and attestations to relying parties. The applicable version of these specifications shall be that referenced in the current ARF v2.8.0.

- XVIII. ETSI EN 319 401 V3.2.1 (2026-01) Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- XIX. ETSI EN 319 411-2 V2.6.1 (2025-06) Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- XX. Regulation (EU) 2025/847 of the European Parliament and of the Council as regards reactions to security breaches of European Digital Identity Wallets

## 3 General Principles

### 3.1 Proportionality to Risk

- 6 In accordance with Section 2.4 of the Annex to CIR (EU) 2015/1502, all provisions in this document shall be understood as commensurate to the risks at assurance level High.
- 7 Wallet Provider shall take due account of the degree of its exposure to risks, its size and structure as a state-owned public sector entity, the likelihood of occurrence of incidents and their severity, including their societal and economic impact, when implementing the provisions of this document. In the application of requirements derived from CIR (EU) 2024/2690, Wallet Provider shall apply them in accordance with Article 2(2) of that regulation.

### 3.2 Auditability

- 8 This document is intended for use within the eID Certification Scheme (GP-03) as defined in ISO/IEC 17067. Certification bodies assessing conformity with this document shall be accredited against ISO/IEC 17065 complemented by ETSI EN 319 403-1 pursuant to G-05. Wallet Provider shall therefore ensure that its implementation of the provisions in this document is documented, traceable and verifiable by an independent third party.
- 9 *NOTE: In the context of this document, only CABs being certification bodies are considered.*

### 3.3 National Law

- 10 Where national law, in particular the Polish Cybersecurity Act and the Act on the Application, imposes requirements that are more stringent than or additional to those set out in this document, Wallet Provider shall comply with the applicable national law. Where this document permits flexibility or defers to national arrangements, Wallet Provider shall document the applicable national provisions and demonstrate compliance with them.

### 3.4 Normative Language

- 11 The normative terms “shall,” “should” and “may” are used in this document as follows:
- (a) SHALL: indicates a mandatory requirement that the Wallet Provider is required to satisfy;
  - (b) SHOULD: indicates a recommendation; where the Wallet Provider deviates from such a recommendation, it shall document and substantiate the reasons for the deviation;
  - (c) MAY: indicates a permission or an option.

### 3.5 Relationship with ISO/IEC 27001

12           The structure of Section 6 is aligned with the control themes of ISO/IEC 27001:2022, Annex A. This alignment is intended to facilitate integration with existing information security management systems. Compliance with this document does not imply certification against ISO/IEC 27001, nor does ISO/IEC 27001 certification alone imply compliance with this document.

13           **NOTE** — *Where Wallet Provider holds a valid ISO/IEC 27001 certificate covering the platform and services at the time of the certification assessment, the CAB may take that certificate into account when determining the extent of reliance on assurance information, in accordance with Section 7.6 of GP-03. However, the CAB shall perform its own evaluation of the design and operating effectiveness of the specific controls required by this document, as the ISO/IEC 27001 certificate attests to the conformity of the ISMS itself and does not, on its own, provide sufficient assurance that those specific controls are implemented at the level of rigour required at assurance level High.*

## 4 Legal Requirements

- 14 This section lists, at a granular level, all legal requirements applicable to Wallet Provider in scope of this document. Each requirement is assigned a unique identifier for traceability. The provisions in Section 6 are mapped to these requirements.

### 4.1 Requirements Derived from CIR (EU) 2015/1502

- 15 *NOTE: The following requirements are derived from Section 2.4 (Management and organisation) of the Annex to CIR (EU) 2015/1502, at assurance level High. In accordance with the structure of that Annex, the requirements at level High incorporate the requirements at levels Low and Substantial. If Level Low/Substantial is indicated in the table below, it means the requirement is the same for Level High.*

#### 4.1.1 General Provisions (Section 2.4.1)

| Identifier  | Requirement                                                                                                                                                                                                                                                                                                                           |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ-1502-01 | Providers delivering any operational service covered by CIR (EU) 2015/1502 shall be a public authority or a legal entity recognised as such by national law of a Member State, with an established organisation and fully operational in all parts relevant for the provision of the services. [Annex, 2.4.1, Level Low, Element 1]   |
| REQ-1502-02 | Providers shall comply with any legal requirements incumbent on them in connection with operation and delivery of the service, including the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long. [Annex, 2.4.1, Level Low, Element 2]                     |
| REQ-1502-03 | Providers shall be able to demonstrate their ability to assume the risk of liability for damages, as well as their having sufficient financial resources for continued operations and providing of the services. [Annex, 2.4.1, Level Low, Element 3]                                                                                 |
| REQ-1502-04 | Providers shall be responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties. [Annex, 2.4.1, Level Low, Element 4]                                                                                        |
| REQ-1502-05 | Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be |

| Identifier | Requirement                                                                                                  |
|------------|--------------------------------------------------------------------------------------------------------------|
|            | protected, retained and destroyed in compliance with the scheme policy. [Annex, 2.4.1, Level Low, Element 5] |

#### 4.1.2 Published Notices and User Information (Section 2.4.2)

| Identifier  | Requirement                                                                                                                                                                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ-1502-06 | The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy. [Annex, 2.4.2, Level Low, Element 1]                                                              |
| REQ-1502-07 | Appropriate policy and procedures shall be in place to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service. [Annex, 2.4.2, Level Low, Element 2] |
| REQ-1502-08 | Appropriate policies and procedures shall be in place that provide for full and correct responses to requests for information. [Annex, 2.4.2, Level Low, Element 3]                                                                                                                                        |

#### 4.1.3 Information Security Management (Section 2.4.3)

| Identifier  | Requirement                                                                                                                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ-1502-09 | There shall be an effective information security management system for the management and control of information security risks. [Annex, 2.4.3, Level Low]                                                                   |
| REQ-1502-10 | The information security management system shall adhere to proven standards or principles for the management and control of information security risks. [Annex, 2.4.3, Level Substantial; Level High is same as Substantial] |

#### 4.1.4 Record Keeping (Section 2.4.4)

| Identifier  | Requirement                                                                                                                                                                                                                        |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ-1502-11 | Record and maintain relevant information using an effective record-management system, considering applicable legislation and good practice in relation to data protection and data retention. [Annex, 2.4.4, Level Low, Element 1] |

| Identifier         | Requirement                                                                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REQ-1502-12</b> | Retain, as far as it is permitted by national law or other national administrative arrangement and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed. [Annex, 2.4.4, Level Low, Element 2] |

#### 4.1.5 Facilities and Staff (Section 2.4.5)

| Identifier         | Requirement                                                                                                                                                                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REQ-1502-13</b> | The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified, and experienced in the skills needed to execute the roles they fulfil. [Annex, 2.4.5, Level Low, Element 1]                                             |
| <b>REQ-1502-14</b> | The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures. [Annex, 2.4.5, Level Low, Element 2]                                                                                 |
| <b>REQ-1502-15</b> | Facilities used for providing the service shall be continuously monitored for, and protect against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service. [Annex, 2.4.5, Level Low, Element 3] |
| <b>REQ-1502-16</b> | Facilities used for providing the service shall ensure that access to areas holding or processing personal, cryptographic, or other sensitive information is limited to authorised staff or subcontractors. [Annex, 2.4.5, Level Low, Element 4]                   |

#### 4.1.6 Technical Controls (Section 2.4.6)

| Identifier         | Requirement                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REQ-1502-17</b> | The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed. [Annex, 2.4.6, Level Low, Element 1] |
| <b>REQ-1502-18</b> | Electronic communication channels used to exchange personal or sensitive information shall be protected against eavesdropping, manipulation, and replay. [Annex, 2.4.6, Level Low, Element 2]                                              |
| <b>REQ-1502-19</b> | Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, shall be restricted to the roles and applications strictly requiring access. It                                        |

| Identifier         | Requirement                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | shall be ensured that such material is never persistently stored in plain text. [Annex, 2.4.6, Level Low, Element 3]                                                                                              |
| <b>REQ-1502-20</b> | Procedures shall exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents, and security breaches. [Annex, 2.4.6, Level Low, Element 4]  |
| <b>REQ-1502-21</b> | All media containing personal, cryptographic, or other sensitive information shall be stored, transported, and disposed of in a safe and secure manner. [Annex, 2.4.6, Level Low, Element 5]                      |
| <b>REQ-1502-22</b> | Sensitive cryptographic material, if used for issuing electronic identification means and authentication, shall be protected from tampering. [Annex, 2.4.6, Level Substantial; Level High is same as Substantial] |

#### 4.1.7 Compliance and Audit (Section 2.4.7)

| Identifier         | Requirement                                                                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REQ-1502-23</b> | The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy. [Annex, 2.4.7, Level High, Element 1] |



## 4.2 Requirements Derived from CIR (EU) 2024/2690

16 The following requirements are derived from the Annex to CIR (EU) 2024/2690, which lays down the technical and methodological requirements for cybersecurity risk-management measures. These requirements are incorporated by reference as the most detailed specification of the level of detail and rigour expected for an entity of the nature and size of Wallet Provider operating critical digital infrastructure. In accordance with Article 2(2) of CIR (EU) 2024/2690, the level of security shall be appropriate to the risks posed.

### 4.2.1 Policy on Security of Network and Information Systems (Annex, Section 1)

| Identifier  | Requirement                                                                                                                                                                                                                                                                                                                            |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ-2690-01 | The provider shall establish a policy on the security of network and information systems setting out its approach, objectives, commitment to continual improvement, resource commitment, roles, documentation requirements, topic-specific policies, indicators and measures, and formal approval by management bodies. [Annex, 1.1.1] |
| REQ-2690-02 | The policy shall be reviewed and, where appropriate, updated by management bodies at least annually and when significant incidents or significant changes to operations or risks occur. [Annex, 1.1.2]                                                                                                                                 |
| REQ-2690-03 | The provider shall lay down responsibilities and authorities for network and information system security and assign them to roles and communicate them to management bodies. [Annex, 1.2.1]                                                                                                                                            |
| REQ-2690-04 | The provider shall require all personnel and third parties to apply network and information system security in accordance with established policies. [Annex, 1.2.2]                                                                                                                                                                    |
| REQ-2690-05 | At least one person shall report directly to the management bodies on matters of network and information system security. [Annex, 1.2.3]                                                                                                                                                                                               |
| REQ-2690-06 | Network and information system security shall be covered by dedicated roles or duties conducted in addition to existing roles. [Annex, 1.2.4]                                                                                                                                                                                          |
| REQ-2690-07 | Conflicting duties and conflicting areas of responsibility shall be segregated, where applicable. [Annex, 1.2.5]                                                                                                                                                                                                                       |
| REQ-2690-08 | Roles, responsibilities, and authorities shall be reviewed and, where appropriate, updated at planned intervals and when significant incidents or significant changes occur. [Annex, 1.2.6]                                                                                                                                            |

#### 4.2.2 Risk Management (Annex, Section 2)

| Identifier  | Requirement                                                                                                                                                                                                                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ-2690-09 | The provider shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of network and information systems, including performing and documenting risk assessments and establishing, implementing, and monitoring a risk treatment plan. [Annex, 2.1.1] |
| REQ-2690-10 | The provider shall establish procedures for identification, analysis, assessment, and treatment of risks (cybersecurity risk management process), including the elements set out in Annex, 2.1.2(a) to (j). [Annex, 2.1.2]                                                                                                |
| REQ-2690-11 | When identifying and prioritising risk treatment options, the provider shall consider the risk assessment results, the cost of implementation, the asset classification, and the business impact analysis. [Annex, 2.1.3]                                                                                                 |
| REQ-2690-12 | The provider shall review and, where appropriate, update risk assessments and risk treatment plans at planned intervals, at least annually, and when significant changes or incidents occur. [Annex, 2.1.4]                                                                                                               |
| REQ-2690-13 | The provider shall regularly review compliance with its policies on network and information system security. Management bodies shall be informed of the status through regular reporting. [Annex, 2.2.1–2.2.3]                                                                                                            |
| REQ-2690-14 | The provider shall independently review its approach to managing network and information system security and its implementation, conducted by individuals with appropriate audit competence. [Annex, 2.3.1–2.3.4]                                                                                                         |

#### 4.2.3 Incident Handling (Annex, Section 3)

| Identifier  | Requirement                                                                                                                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ-2690-15 | The provider shall establish and implement an incident handling policy laying down roles, responsibilities, and procedures for detecting, analysing, containing, responding to, recovering from, documenting and reporting incidents. [Annex, 3.1.1–3.1.3] |
| REQ-2690-16 | The provider shall lay down procedures and use tools to monitor and log activities on its network and information systems. [Annex, 3.2.1–3.2.7]                                                                                                            |
| REQ-2690-17 | The provider shall put in place a simple mechanism for reporting suspicious events. [Annex, 3.3.1–3.3.2]                                                                                                                                                   |

| Identifier         | Requirement                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REQ-2690-18</b> | The provider shall assess suspicious events to determine whether they constitute incidents and determine their nature and severity. [Annex, 3.4.1–3.4.2] |
| <b>REQ-2690-19</b> | The provider shall respond to incidents in accordance with documented procedures, including containment, eradication, and recovery. [Annex, 3.5.1–3.5.5] |
| <b>REQ-2690-20</b> | The provider shall conduct post-incident reviews to identify root causes and documented lessons learned. [Annex, 3.6.1–3.6.3]                            |

#### 4.2.4 Business Continuity and Crisis Management (Annex, Section 4)

| Identifier         | Requirement                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REQ-2690-21</b> | The provider shall lay down and maintain a business continuity and disaster recovery plan, based on risk assessment results. [Annex, 4.1.1–4.1.4]                            |
| <b>REQ-2690-22</b> | The provider shall maintain backup copies of data and provide sufficient available resources to ensure an appropriate level of redundancy. [Annex, 4.2.1–4.2.6]              |
| <b>REQ-2690-23</b> | The provider shall put in place a process for crisis management, including roles, communication means and maintenance of security in crisis situations. [Annex, 4.3.1–4.3.4] |

#### 4.2.5 Supply Chain Security (Annex, Section 5)

| Identifier         | Requirement                                                                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REQ-2690-24</b> | The provider shall establish, implement, and apply a supply chain security policy governing relations with direct suppliers and service providers. [Annex, 5.1.1–5.1.7] |
| <b>REQ-2690-25</b> | The provider shall maintain and keep up to date a registry of direct suppliers and service providers. [Annex, 5.2]                                                      |

#### 4.2.6 Security in Acquisition, Development and Maintenance (Annex, Section 6)

| Identifier         | Requirement                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REQ-2690-26</b> | The provider shall set and implement processes to manage risks stemming from the acquisition of ICT services or ICT products. [Annex, 6.1.1–6.1.3] |

| Identifier  | Requirement                                                                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ-2690-27 | The provider shall lay down rules for the secure development of network and information systems and apply them. [Annex, 6.2.1–6.2.4]                                      |
| REQ-2690-28 | The provider shall take appropriate measures to establish, document, implement and monitor configurations, including security configurations. [Annex, 6.3.1–6.3.3]        |
| REQ-2690-29 | The provider shall apply change management procedures to control changes of network and information systems. [Annex, 6.4.1–6.4.4]                                         |
| REQ-2690-30 | The provider shall establish, implement, and apply a policy and procedures for security testing. [Annex, 6.5.1–6.5.3]                                                     |
| REQ-2690-31 | The provider shall specify and apply procedures for security patch management. [Annex, 6.6.1–6.6.2]                                                                       |
| REQ-2690-32 | The provider shall take appropriate measures to protect its network and information systems from cyber threats. [Annex, 6.7.1–6.7.3]                                      |
| REQ-2690-33 | The provider shall segment systems into networks or zones in accordance with risk assessment results. [Annex, 6.8.1–6.8.3]                                                |
| REQ-2690-34 | The provider shall protect its network and information systems against malicious and unauthorised software. [Annex, 6.9.1–6.9.2]                                          |
| REQ-2690-35 | The provider shall obtain information about technical vulnerabilities, evaluate exposure, and take appropriate measures to manage vulnerabilities. [Annex, 6.10.1–6.10.4] |

#### 4.2.7 Effectiveness Assessment, Cyber Hygiene, Cryptography, Human Resources, Access Control, Asset Management, Physical Security (Annex, Sections 7–13)

| Identifier  | Requirement                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ-2690-36 | The provider shall establish, implement, and apply a policy and procedures to assess whether its cybersecurity risk-management measures are effectively implemented and maintained. [Annex, 7.1–7.3] |
| REQ-2690-37 | The provider shall ensure awareness raising and application of cyber hygiene practices for employees, management bodies, and direct suppliers and service providers. [Annex, 8.1.1–8.1.3]            |
| REQ-2690-38 | The provider shall identify employees whose roles require security-relevant skills and ensure they receive regular training. [Annex, 8.2.1–8.2.5]                                                    |

| Identifier  | Requirement                                                                                                                                                                         |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ-2690-39 | The provider shall establish, implement, and apply a policy and procedures related to cryptography, including key management. [Annex, 9.1–9.3]                                      |
| REQ-2690-40 | The provider shall ensure that employees and direct suppliers and service providers understand and commit to their security responsibilities. [Annex, 10.1.1–10.1.3]                |
| REQ-2690-41 | The provider shall ensure, to the extent feasible, verification of the background of employees. [Annex, 10.2.1–10.2.3]                                                              |
| REQ-2690-42 | The provider shall ensure that security responsibilities that remain valid after termination or change of employment are contractually defined and enforced. [Annex, 10.3.1–10.3.2] |
| REQ-2690-43 | The provider shall establish, communicate, and maintain a disciplinary process for handling violations of security policies. [Annex, 10.4.1–10.4.2]                                 |
| REQ-2690-44 | The provider shall establish, document, and implement logical and physical access control policies. [Annex, 11.1.1–11.1.3]                                                          |
| REQ-2690-45 | The provider shall provide, modify, remove, and document access rights in accordance with the access control policy. [Annex, 11.2.1–11.2.3]                                         |
| REQ-2690-46 | The provider shall maintain policies for management of privileged accounts and system administration accounts. [Annex, 11.3.1–11.3.3]                                               |
| REQ-2690-47 | The provider shall restrict and control the use of system administration systems. [Annex, 11.4.1–11.4.2]                                                                            |
| REQ-2690-48 | The provider shall manage the full life cycle of identities of network and information systems and their users. [Annex, 11.5.1–11.5.4]                                              |
| REQ-2690-49 | The provider shall implement secure authentication procedures and technologies. [Annex, 11.6.1–11.6.4]                                                                              |
| REQ-2690-50 | The provider shall ensure that users are authenticated by multiple authentication factors or continuous authentication mechanisms, where appropriate. [Annex, 11.7.1–11.7.2]        |
| REQ-2690-51 | The provider shall lay down classification levels of all assets, including information, for the level of protection required. [Annex, 12.1.1–12.1.3]                                |
| REQ-2690-52 | The provider shall establish, implement, and apply a policy for the proper handling of assets. [Annex, 12.2.1–12.2.3]                                                               |

| Identifier         | Requirement                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REQ-2690-53</b> | The provider shall establish, implement, and apply a policy on the management of removable storage media. [Annex, 12.3.1–12.3.3]                            |
| <b>REQ-2690-54</b> | The provider shall develop and maintain a complete, accurate, up-to-date, and consistent inventory of its assets. [Annex, 12.4.1–12.4.3]                    |
| <b>REQ-2690-55</b> | The provider shall establish procedures for deposit, return, or deletion of assets upon termination of employment. [Annex, 12.5]                            |
| <b>REQ-2690-56</b> | The provider shall prevent loss, damage or compromise of network and information systems due to failure of supporting utilities. [Annex, 13.1.1–13.1.3]     |
| <b>REQ-2690-57</b> | The provider shall prevent or reduce the consequences of events originating from physical and environmental threats. [Annex, 13.2.1–13.2.3]                 |
| <b>REQ-2690-58</b> | The provider shall prevent and monitor unauthorised physical access, damage and interference to its network and information systems. [Annex, 13.3.1–13.3.3] |

## 4.3 Requirements Derived from CIR (EU) 2024/2981

17 The following requirements are derived from CIR (EU) 2024/2981, which lays down rules for the certification of European Digital Identity Wallets.

### 4.3.1 Risk Assessment and Security Criteria (Articles 4 and 8)

| Identifier  | Requirement                                                                                                                                                                                                                                                                                                       |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ-2981-01 | The provider shall complement the scheme's risk assessment to identify risks and threats specific to its implementation and propose appropriate treatment measures for all relevant risks and threats. The assessment shall be shared with the certification body for evaluation. [Article 4(4)(d), Article 4(5)] |
| REQ-2981-02 | The provider shall establish and implement policies and procedures concerning the management of risks associated with the operation of a wallet solution, including the identification and assessment of risks and the mitigation of the identified risks. [Article 8(3)(b)]                                      |
| REQ-2981-03 | The provider shall establish and implement policies and procedures related to the management of changes and to the management of vulnerabilities in accordance with Article 5. [Article 8(3)(c)]                                                                                                                  |
| REQ-2981-04 | The provider shall establish and implement human resource management policies and procedures, including requirements on expertise, reliability, experience, security training, and qualifications of personnel involved in the development or operation of the wallet solution. [Article 8(3)(d)]                 |

### 4.3.2 Incident and Vulnerability Management (Article 5)

| Identifier  | Requirement                                                                                                                                                                                                                                                                                                                                                       |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ-2981-05 | The holder of a certificate of conformity shall notify the relevant supervisory body <sup>1</sup> and, where applicable, other relevant bodies, without undue delay, after becoming aware of any breach of security or loss of integrity that has a significant impact on the wallet solution provided or on the personal data maintained therein. [Article 5(1)] |
| REQ-2981-06 | The holder of a certificate of conformity shall notify their certification body without undue delay of any breach or compromise of the wallet solution, or of the electronic identification scheme under which it is provided, that is likely to impact its conformity with the requirements of the national certification scheme. [Article 5(2)]                 |

---

<sup>1</sup> Scheme Owner in this context

| Identifier         | Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REQ-2981-07</b> | The holder of a certificate of conformity shall establish, maintain, and operate a vulnerability management policy and procedures, considering the procedures set out in existing European and international standards, including EN ISO/IEC 30111:2019. [Article 5(3)]                                                                                                                                                                                                                                                                |
| <b>REQ-2981-08</b> | The holder of the certificate of conformity shall notify the issuing certification body of the vulnerabilities and changes affecting the wallet solution, based on defined criteria on the impact of these vulnerabilities and changes. [Article 5(4)]                                                                                                                                                                                                                                                                                 |
| <b>REQ-2981-09</b> | The holder of the certificate of conformity shall prepare a vulnerability impact analysis report for any vulnerability that affects the software components of the wallet solution, including: (a) the impact on the certified wallet solution; (b) possible risks associated with the proximity or likelihood of an attack; (c) whether the vulnerability can be remedied; (d) possible ways to remedy the vulnerability. The report shall be transmitted without undue delay to the certification body. [Article 5(5), Article 5(6)] |
| <b>REQ-2981-10</b> | The holder of a certificate of conformity shall establish, maintain, and operate a vulnerability management policy meeting the requirements set out in Annex I to Regulation (EU) 2024/2847 (Cyber Resilience Act). [Article 5(7)]                                                                                                                                                                                                                                                                                                     |
| <b>REQ-2981-11</b> | The holder of a certificate of conformity shall disclose and register any officially known and remediated vulnerability in the wallet solution in one of the online repositories referred to in Annex V to CIR (EU) 2024/2981. [Article 5(9)]                                                                                                                                                                                                                                                                                          |

#### 4.3.3 Public Information (Article 8(5) and Annex V)

| Identifier         | Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REQ-2981-12</b> | The provider shall make publicly available, in a clear, comprehensive and easily accessible manner: (a) any limitations on the use of the wallet solution; (b) guidance and recommendations for secure configuration, installation, deployment, operation and maintenance; (c) the period during which security support will be offered, in particular regarding cybersecurity-related updates; (d) contact information and accepted methods for receiving vulnerability information; (e) a reference to online repositories listing publicly disclosed vulnerabilities and relevant cybersecurity advisories. [Article 8(5), Annex V] |



#### 4.3.4 Record Retention (Article 19)

| Identifier         | Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REQ-2981-13</b> | The holder of the certificate of conformity shall store the following information securely for the purpose of CIR (EU) 2024/2981, and for at least five years after the cancellation or expiry of the relevant certificate of conformity: (a) records of the information provided to the certification body or any of its sub-contractors during the certification process; (b) specimens of hardware components included in the scope of certification. [Article 19(2)] |
| <b>REQ-2981-14</b> | The holder of the certificate of conformity shall make the information referred to in Article 19(1) available to the certification body or the Scheme Owner upon request. [Article 19(3)]                                                                                                                                                                                                                                                                                |

## 4.4 Requirements Derived from CIR (EU) 2025/847

### 4.4.1 Organisational requirements in case of security breach of EUDI Wallet

| Identifier | Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ-847-01 | Wallet Provider shall establish, implement and maintain decision-making procedures to evaluate whether revocation of affected wallet unit attestations or other additional remedies are necessary to react adequately to a security breach or compromise. [Article 4(2)]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| REQ-847-02 | Wallet Provider shall ensure that suspension or remedy measures do not prevent affected wallet users from exercising data portability, provided this can be done without impairing the security of critical assets of affected wallet units. [Article 4(4)]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| REQ-847-03 | Wallet Provider shall establish, implement and maintain procedures to provide clear, comprehensive and easily accessible information about suspension of a wallet solution without undue delay and no later than 24 hours after suspension. [Article 5(1)]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| REQ-847-04 | <p>Wallet Provider shall establish, implement and maintain contact and communication procedures:</p> <ul style="list-style-type: none"><li>— enabling notifications to single points of contact, the Commission, affected wallet users and registered wallet-relying parties. [Article 5(1)]</li><li>— informing relevant parties without undue delay about the re-establishment of the affected wallet solution including the following:<ul style="list-style-type: none"><li>— the date and time of remedy,</li><li>— the date and time of re-establishment,</li><li>— measures taken,</li><li>— residual impacts and mitigation measures for users.</li></ul>[Article 7]</li><li>— providing clear, comprehensive and easily accessible information about withdrawal of a wallet solution without undue delay and no later than 24 hours after withdrawal. [Article 9(1)]</li></ul> |
| REQ-847-05 | <p>Wallet Provider shall ensure that re-establishing of the provision, activation and use of the affected wallet solution without undue delay including the following:</p> <ol style="list-style-type: none"><li>1) Issuance wallet units under a new version of the wallet solution, where necessary.</li></ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Identifier        | Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>REQ-847-06</b> | <p>2) issuance of new wallet unit attestations to new or previously issued wallet units, provided that those wallet units meet the security requirements applicable after the breach or compromise has been remedied.</p> <p>[Article 6]</p>                                                                                                                                                                                                                 |
|                   | <p>Wallet Provider shall establish, implement and maintain procedures to inform relevant parties without undue delay about the re-establishment of the affected wallet solution including the following:</p> <ul style="list-style-type: none"> <li>— the date and time of remedy,</li> <li>— the date and time of re-establishment,</li> <li>— measures taken,</li> <li>— residual impacts and mitigation measures for users.</li> </ul> <p>[Article 7]</p> |
| <b>REQ-847-07</b> | <p>Wallet Provider shall withdraw affected wallet solution if a security breach or compromise having led to the suspension of the provision and the use of a wallet solution is not remedied within three months after the date of suspension of the provision and the use of that wallet solution. . [Article 8(1)]</p>                                                                                                                                     |
| <b>REQ-847-08</b> | <p>Wallet Provider shall ensure that withdrawal of the affected wallet solution and revocation of its validity without undue delay and no later than 72 hours after expiry of the three-month remediation period. [Article 8(1)]</p>                                                                                                                                                                                                                         |
| <b>REQ-847-09</b> | <p>Wallet Provider shall maintain evidence and reporting capabilities enabling the Member State to use CIRAS operated by ENISA, or an equivalent agreed system, for information exchange with the Commission and single points of contact. [Article 10]</p>                                                                                                                                                                                                  |
| <b>REQ-847-10</b> | <p>Wallet Provider shall notify planned maintenance in advance to potentially affected wallet users, wallet-relying parties and relevant competent supervisory bodies where such maintenance may affect availability or operation of wallet-related services. [Annex, Point 2(a)]</p>                                                                                                                                                                        |

## 5 Provisions

18 This chapter contains provisions the Wallet Provider shall comply with for the purposes of certification. The provisions are structured in five subsections: general and scheme-specific provisions (6.1), organisational controls (6.2), people controls (6.3), physical controls (6.4) and technological controls (6.5). Subsections 6.2 to 6.5 are aligned with the control themes of ISO/IEC 27001:2022, Annex A.

19 Each provision is mapped to the legal requirements listed in Section 5. The mapping is indicated in brackets at the end of each provision.

### 5.1 General and Scheme-Specific Provisions

20 This subsection contains provisions derived from legal requirements that are specific to the certification scheme or to the regulatory framework governing electronic identification, and that do not correspond directly to the control themes of ISO/IEC 27001:2022, Annex A.

21 **EP** denotes an identifier of scheme-specific provisions defined in this document.

#### 5.1.1 Information Security Management System

##### 22 **EP-01**

Wallet Provider shall establish, operate, and maintain an information security management system (ISMS) that governs the implementation, monitoring and continual improvement of the controls set out in Sections 6.2 to 6.5 of this document. The ISMS shall adhere to proven standards or principles for the management and control of information security risks.

**NOTE** — ISO/IEC 27001 is a well-known and proven standard that satisfies this requirement. Other established standards or national schemes that demonstrably fulfil the requirements of this section may also be used.

In addition to the controls set out in Section 6, the ISMS shall address, as a minimum, the following:

- I. understanding the context of the organisation, including the needs and expectations of interested parties relevant to the provision of the wallet solution, and determining the scope of the ISMS accordingly;
- II. establishing requirements for documented information, including the creation, update, control and retention of documented information necessary to support the operation of the ISMS and to provide evidence of the results achieved;

- III. establishing a process for internal and external communication relevant to the ISMS, including what to communicate, when, with whom, and by what means;
- IV. conducting management reviews of the ISMS at planned intervals by top management, considering the results of audits, the status of corrective actions, changes in the context of the organisation, and feedback on information security performance, and making decisions on opportunities for improvement;
- V. establishing a process for handling nonconformities and implementing corrective actions, including identifying nonconformities, determining their causes, evaluating the need for action to ensure they do not recur, implementing corrective actions, and reviewing their effectiveness;
- VI. continual improvement of the suitability, adequacy and effectiveness of the ISMS;
- VII. assessing, at planned intervals, the effectiveness of the ISMS to ensure that it continues to be suitable, adequate and effective for the management and control of information security risks at assurance level High, and reporting the results to top management as input to the management review referred to in point (d);
- VIII. ensure that the resources needed for the ISMS and for the provision of the wallet-related services are available, including sufficient personnel and subcontractors with the competences needed to operate and resource the service according to its policies and procedures.

[REQ-1502-09; REQ-1502-10; REQ-1502-14; REQ-2690-09]

**Alignment with international standards** — ISO/IEC 27001:2022 cl. 4.1–4.4 (context & scope), cl. 5.1–5.3 (leadership), cl. 6.1–6.3 (planning), cl. 8.1 (operational planning), cl. 9.1–9.3 (performance evaluation), cl. 10.1–10.2 (improvement); A.5.1 (IS policies). | ETSI EN 319 401 §7.1 (Security policy); EN 319 411-1 §6.9.1 (Organisational); EN 319 411-2 §6.9.1 (Organisational requirements for QTSPs).

**Additional standards and references** — ARF v2.8.0 §6 (security architecture requirements for Wallet Providers and PID Providers); GDPR Article 25 (data protection by design and by default — ISMS scope shall encompass all personal data processing in the wallet-related services).

**Additional standards and references** — ARF v2.8.0 §6 (security architecture and operational requirements for Wallet Providers and PID Providers); GDPR Article 25 (data protection by design and by default — the ISMS scope shall encompass all personal data processing activities related to the wallet-related services).

## 5.1.2 Legal Entity Status and Financial Capacity

23

EP-02

Wallet Provider shall be a public authority a budgetary economy institution or a legal entity recognised as such by the national law of the Republic of Poland. Wallet Provider shall have an established organisation and be fully operational in all parts relevant for the provision of the wallet-related services within the scope of this document.

[REQ-1502-01]

**Alignment with international standards** — ISO/IEC 27001:2022 cl. 5.1 (leadership & commitment), cl. 7.1 (resources). | ETSI EN 319 401 §7.1 (Organisational security); EN 319 411-1 §6.9.1 (Organisational).

24

### EP-03

Wallet Provider shall comply with all applicable legal, regulatory and contractual requirements in connection with the operation and delivery of the wallet-related services, including but not limited to requirements governing the types of information that may be collected, how identity proofing is conducted, what information may be retained and for how long, and applicable data protection legislation including Regulation (EU) 2016/679.

[REQ-1502-02]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.31 (legal, statutory, regulatory & contractual requirements); A.5.36 (compliance with policies and standards). | ETSI EN 319 401 §7.4-§7.8 (Compliance); EN 319 411-1 §6.9.1 (Organisational); §6.8.15 (Compliance with applicable law).

**Additional standards and references** — GDPR Article 5(1)(e) (storage limitation); GDPR Article 17 (right to erasure — termination plan shall include procedures for fulfilling user erasure requests upon service termination); ARF v2.8.0 §6 (wallet lifecycle termination and data portability requirements).

25

### EP-04

Wallet Provider shall be able to demonstrate its ability to assume the risk of liability for damages arising from the provision of the wallet-related services, providing the CAB with a formal statement of budgetary guarantees or proof of insurance coverage appropriate to its legal form; Wallet Provider shall have sufficient financial resources, within the framework applicable to it as a state-owned budgetary unit (jednostka budżetowa) or a budgetary economy institution (instytucja gospodarki budżetowej), to ensure continued operations and service provision.

**NOTE** — As a state-owned budgetary unit under the Ministry of Digital Affairs, the financial framework applicable to Wallet Provider is governed by national law. The liability framework applicable to Wallet Provider in the context of eIDAS Article 11 and Article 5a (19) shall be documented and made available to the CAB as part of the certification assessment.

[REQ-1502-03]

**Alignment with international standards** — ISO/IEC 27001:2022 cl. 5.1 (leadership commitment — resources); cl. 7.1 (resources). | ETSI EN 319 401 §7.1 (Organisational security policy); EN 319 411-1 §6.9.1 (Organisational); §6.8.2 (Financial responsibility).

### 5.1.3 Termination Planning

26

#### EP-05

Where the electronic identification scheme is not constituted by national law, Wallet Provider shall have in place an effective termination plan for its services. The termination plan shall include:

- I. orderly discontinuation of service or continuation by another provider;
- II. the way relevant authorities and end users are informed, ensuring the electronic identification scheme stakeholders are notified at least three months before the planned cessation of a service provision;
- III. details on how records are to be protected, retained and destroyed in compliance with the Trust Framework established under G-03.

The termination plan shall cover foreseeable circumstances leading to a discontinuation of the service, including cessation by Wallet Provider and shut down by external authorities.

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.29 (IS during disruption); A.5.30 (ICT readiness for business continuity); cl. 8.1 (operational planning and control). | ETSI EN 319 401 §7.11 (Business continuity); EN 319 411-1 §6.4.9 (CA/RA termination).

### 5.1.4 Published Notices and Public Information

27

#### EP-06

Wallet Provider shall publish a service definition for the wallet-related services that includes all applicable terms, conditions, and fees, including any limitations of usage. The service definition shall include a privacy policy. In addition, Wallet Provider shall make publicly available, in a clear, comprehensive, and easily accessible manner, security information about the wallet solution, including at a minimum:

- I. any limitations on the use of the wallet solution;
- II. guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the wallet solution;
- III. the period during which security support will be offered to end users, as regards the availability of cybersecurity-related updates;

- IV. contact information and accepted methods for receiving vulnerability information from end users and security researchers;
- V. a reference to online repositories listing publicly disclosed vulnerabilities related to the wallet solution and to any relevant cybersecurity advisories.

[REQ-1502-06; REQ-2981-12]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.36 (compliance with policies); A.5.31 (legal requirements). | ETSI EN 319 401 §7.3 (Classification and handling of information); EN 319 411-1 §6.1 (Publication and repository responsibilities); §5.2 (CPS requirements); EN 319 411-2 §6.1 (Publication and repository responsibilities for QTSPs).

28

#### EP-07

Wallet Provider shall have appropriate policies and procedures in place to ensure that interested parties and the Scheme Owner are informed in a timely and reliable fashion of any changes to the service definition, ensuring the Scheme Owner is notified at least one month before implementing any important change including changes to the terms, conditions, and privacy policy.

[REQ-1502-07]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.36 (compliance with policies, rules, and standards); A.8.32 (change management). | ETSI EN 319 401 §7.3 (Information handling); EN 319 411-1 §6.1 (Publication and repository responsibilities); §5.2 (CPS requirements).

29

#### EP-08

Wallet Provider shall have appropriate policies and procedures in place to provide full and correct responses to requests for information from interested parties and competent authorities.

[REQ-1502-08]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.36 (compliance with policies, rules, and standards). | ETSI EN 319 401 §7.3 (Classification and handling of information).

### 5.1.5 Certification Body Notification

30

#### EP-09

Wallet Provider shall notify the Scheme Owner (Ministry of Digital Affairs) and, through the established notification procedure, the CAB, without undue delay of any breach or compromise of the wallet solution or of the electronic identification scheme under which it is provided, that is likely to impact its conformity with the requirements of GP-03 or its subsidiary documents.



**NOTE** — This notification obligation is without prejudice to Wallet Provider's obligations under Regulation (EU) 2016/679 with respect to notification of personal data breaches and any obligations under the Polish Cybersecurity Act with respect to significant incident notification to the national CSIRT (CERT Polska).

[REQ-2981-06]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.24 (planning & preparation of IS incident management); A.5.26 (response to IS incidents). | ETSI EN 319 401 §7.9 (Incident management); EN 319 411-1 §6.4.8 (Compromise and disaster recovery); EN 319 411-2 §6.4.8 (Compromise and disaster recovery for qualified services).

## 5.2 Organisational Controls

31 This subsection is aligned with the organisational control theme (A.5) of ISO/IEC 27001:2022, Annex A.

### 5.2.1 Information Security Policy

32 **EP-10**

Wallet Provider shall establish an information security policy for the wallet-related services. The policy shall:

- I. be appropriate for the purposes of providing the wallet-related services in scope of this document;
- II. set out information security objectives;
- III. include a commitment to satisfy the requirements of this document;
- IV. include a commitment to continual improvement of information security.

The policy shall have been adopted by top management, be reviewed and, where appropriate, updated by top management at least annually and when significant incidents or significant changes to operations or risks occur.

[REQ-1502-17; REQ-2690-01; REQ-2690-02]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.1 (policies for information security); A.5.2 (IS roles and responsibilities). | ETSI EN 319 401 §7.1 (Organisational security policy); EN 319 411-1 §6.9.1 (Organisational).

### 5.2.2 Information Security Roles and Responsibilities

33 **EP-11**

Wallet Provider shall define and assign information security responsibilities and authorities to roles, in accordance with its operational needs, including the mandatory trusted roles of: Security Officers, System Administrators, System Operators, and System Auditors, and communicate them to top management. Wallet Provider shall ensure that:

- I. all personnel and contracted parties apply information security in accordance with the established policies;
- II. at least one person reports directly to top management on matters of information security;
- III. information security matters are covered by dedicated roles or, depending on the specific function, by duties carried out in addition to existing roles;

IV.conflicting duties and conflicting areas of responsibility shall be segregated, where applicable, with clearly defined methods for managing them.

Roles, responsibilities, and authorities shall be reviewed and, where appropriate, updated at planned intervals and when significant changes occur.

[REQ-2690-03; REQ-2690-04; REQ-2690-05; REQ-2690-06; REQ-2690-07; REQ-2690-08]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.2 (IS roles & responsibilities); A.5.3 (segregation of duties). | ETSI EN 319 401 §7.1 (Organisational security); EN 319 411-1 §6.4.4 (Personnel controls).

### 5.2.3 Risk Management

#### 34 EP-12

Wallet Provider shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of its information systems supporting the wallet-related services. Wallet Provider shall perform and document risk assessments and, based on the results, establish, implement, and monitor a risk treatment plan. Risk assessment results and residual risks shall be accepted by the risk owner or by top management.

[REQ-2690-09; REQ-2981-02]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.7 (threat intelligence); cl. 6.1.2 (IS risk assessment); cl. 6.1.3 (IS risk treatment); cl. 8.2–8.3 (operational risk assessment and treatment). | ETSI EN 319 401 §7.1 (Risk management); EN 319 411-1 §6.9.1 (Organisational).

#### 35 EP-13

As part of the risk management framework, Wallet Provider shall establish a risk assessment process for the identification, analysis, evaluation, and treatment of information security risks. The process shall, as a minimum:

- I. follow a recognised risk management methodology;
- II. establish and maintain risk assessment criteria;
- III. apply risk acceptance criteria that are consistent with the risk profile of assurance level High as defined in CIR (EU) 2015/1502, ensuring that residual risks do not exceed the level acceptable for the offered assurance level;
- IV. in line with an all-hazards approach, identify and document the risks posed to the security of information systems, taking into account the risks and threats listed in the risk register set out in Annex I to

CIR (EU) 2024/2981 and in G-04, information collected through threat intelligence and vulnerability management procedures, risks from third parties and risks that could lead to disruptions in availability, integrity, authenticity and confidentiality, and the identification of single points of failure;

V. evaluate the risks based on the established risk assessment criteria, including threat, likelihood, impact and the resulting risk level;

VI. identify and prioritise appropriate risk treatment options and controls, where the chosen risk treatment is documented in a risk treatment plan;

VII. set out timelines and identify responsibility for the implementation of the risk treatment plan;

VIII. continuously monitor the implementation of the risk treatment plan;

IX. assess the effectiveness of the risk treatment measures implemented and formally accept residual risks, ensuring that they remain within the limits set out in point (c).

[REQ-2690-10; REQ-2690-11; REQ-2690-36]

**Alignment with international standards** — ISO/IEC 27001:2022 cl. 6.1.2 (IS risk assessment); cl. 8.2 (operational risk assessment). | ETSI EN 319 401 §7.1 (Risk management framework); EN 319 411-1 §6.9.1 (Organisational).

36

#### EP-14

Wallet Provider shall complement the scheme-level risk assessment maintained by the Ministry of Digital Affairs with an assessment of risks and threats specific to its own implementation of the wallet platform. Wallet Provider shall use the risk register set out in Annex I to CIR (EU) 2024/2981 and based on the template contained in G-04 as mandatory inputs and identify any additional risks and threats arising from the specific architecture, operational environment, and supply chain of the platform. Wallet Provider shall propose appropriate treatment measures for all identified risks and threats and share the implementation-specific risk assessment with the CAB for evaluation.

**NOTE** — The implementation-specific risk assessment required by this provision complements the scheme-level risk assessment and does not replace it.

[REQ-2981-01]

**Alignment with international standards** — ISO/IEC 27001:2022 cl. 6.1.2 (IS risk assessment); cl. 8.2 (operational); A.5.7 (threat intelligence). | ETSI EN 319 401 §7.1 (Risk management); EN 319 411-1 §6.9.1 (Organisational).

37

#### EP-15

Wallet Provider shall review and, where appropriate, update the risk assessment results and the risk treatment plans at planned intervals, at least annually, and when significant changes to operations or risks occur.

[REQ-2690-12]

**Alignment with international standards** — ISO/IEC 27001:2022 cl. 6.1.2 (risk assessment update); cl. 8.2 (operational review); cl. 9.3 (management review). | ETSI EN 319 401 §7.1 (Review of security policy); EN 319 411-1 §6.9.1 (Organisational).

### 5.2.4 Supplier Relationships

38

#### EP-16

Wallet Provider shall remain responsible for the fulfilment of any commitments outsourced to another organisation, and for compliance with the Trust Framework established by the Ministry of Digital Affairs under G-03, as if Wallet Provider had performed the duties itself.

[REQ-1502-04; REQ-2690-24]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.19 (IS in supplier relationships); A.5.20 (addressing IS within supplier agreements). | ETSI EN 319 401 §7.14 (Supply chain security); EN 319 411-1 §6.8.6 (Representations and warranties); §6.9.1 (Organisational).

39

#### EP-17

Where Wallet Provider outsources operational functions to third parties in connection with the wallet-related services, Wallet Provider shall ensure that contractual arrangements with such third parties include, as appropriate:

- I. information security requirements applicable to the third party, consistent with the requirements of this document including an explicit requirement for the third party to acknowledge and confirm in writing (in documentary form) that they have read and understood Wallet Provider's relevant security policies;
- II. requirements regarding awareness, competence and training of the third party's personnel;
- III. requirements regarding screening of the third party's personnel;
- IV. an obligation on the third party to notify Wallet Provider without undue delay of incidents presenting a risk to the security of Wallet Provider's information systems;
- V. the right to audit or to receive audit reports;

VI. an obligation on the third party to handle vulnerabilities presenting a risk to Wallet Provider;

VII. requirements regarding subcontracting by the third party;

VIII. obligations at the termination of the contract, including retrieval and disposal of information.

[REQ-1502-04; REQ-2690-24]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.19 (IS in supplier relationships); A.5.20 (addressing IS within supplier agreements). | ETSI EN 319 401 §7.14 (Supply chain security); EN 319 411-1 §6.8.6 (Representations and warranties); §6.9.1 (Organisational).

40

#### EP-18

Wallet Provider shall establish, implement, and apply a supply chain security policy governing its relations with its direct suppliers and service providers involved in the provision of the wallet-related services, to mitigate identified risks to the security of information systems. The policy shall include criteria for the selection and contracting of suppliers and service providers, taking into account their information security practices, their ability to meet information security specifications set by Wallet Provider, the overall quality and resilience of provided products and services, and the ability of Wallet Provider to diversify sources of supply and limit vendor lock-in, where applicable.

[REQ-2690-24]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.21 (managing IS in ICT supply chain); A.5.22 (monitoring and review of supplier services). | ETSI EN 319 401 §7.14 (Supply chain security policy); EN 319 411-1 §6.8.6 (Representations and warranties); §6.9.1 (Organisational).

41

#### EP-19

Wallet Provider shall maintain and keep up to date a registry of its direct suppliers and service providers involved in the wallet-related services, including contact points and a list of ICT products, ICT services and ICT processes provided.

[REQ-2690-25]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.9 (inventory of information and other associated assets); A.5.21 (ICT supply chain). | ETSI EN 319 401 §7.3 (Asset management); EN 319 411-1 §6.9.1 (Organisational); §6.8.6 (Representations and warranties).

42

#### EP-20

Wallet Provider shall review its supply chain security policy and monitor, evaluate and, where necessary, act upon changes in the information security practices of its suppliers and service providers, at planned intervals, and when significant changes to operations or risks occur and when significant incidents related to the provision of ICT services or having impact on the security of ICT products acquired from suppliers occur.

[REQ-2690-24]

## 5.2.5 Asset Management

43

### EP-21

Wallet Provider shall develop and maintain a complete, accurate, up-to-date, and consistent inventory of its assets supporting the wallet-related services, recorded in a traceable manner. The inventory shall include the list of operations and services and their descriptions, and the list of information systems and other associated assets. The inventory shall enable identification of relevant relationships between operations, services, information systems and associated assets supporting the wallet related services. Where information on such assets is maintained in more than one record, repository or document, Wallet Provider shall ensure that such information remains consistent and traceable across those records.

[REQ-2690-54]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.9 (inventory of information and other associated assets); A.5.10 (acceptable use of assets). | ETSI EN 319 401 §7.3 (Asset management); EN 319 411-1 §6.4.5 (Audit logging procedures); §6.4.6 (Records archival).

44

### EP-22

Wallet Provider shall define and apply an information classification scheme for all assets, including information, commensurate with the level of protection required. The classification shall be based on confidentiality, integrity, authenticity, and availability requirements, taking into account the sensitivity, criticality, risk and business value of the assets and shall be aligned with the delivery and recovery objectives in the business continuity and disaster recovery plan. The classification assigned to assets and information shall be recorded or referenced in a manner consistent with the asset inventory maintained under EP-21. Wallet Provider shall review the classification levels at planned intervals and update them where appropriate.

[REQ-2690-51]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.12 (classification of information); A.5.13 (labelling of information). | ETSI EN 319 401 §7.3 (Classification and handling of information); EN 319 411-1 §6.4.6 (Records archival).

Wallet Provider shall establish, implement, and apply a policy for the proper handling of assets, covering their entire life cycle including acquisition, use, storage, transportation, and disposal. The policy shall provide rules on safe use, safe storage, safe transport, irretrievable deletion and destruction of assets, and secure transfer in accordance with the type and classification of the asset. The policy shall be communicated to anyone who uses or handles assets. Wallet Provider shall review and, where appropriate, update the policy at planned intervals and when significant incidents or significant changes to operations occur.

[REQ-2690-52]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.10 (acceptable use of assets); A.8.10 (information deletion); A.7.7 (clear desk and clear screen policy). | ETSI EN 319 401 §7.3 (Information handling); EN 319 411-1 §6.4.5 (Audit logging procedures); §6.5.1 (Key pair generation and installation).

## 5.2.6 Access Control

Wallet Provider shall establish, document, and implement logical and physical access control policies for access to its information systems supporting the wallet-related services, based on business and information security requirements. The policies shall address access by persons (personnel, visitors, external parties such as suppliers and service providers) and access by information systems. Access shall only be granted to users and processes that have been adequately authenticated.

[REQ-1502-16; REQ-2690-44]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.15 (access control); A.5.16 (identity management); A.5.17 (authentication information). | ETSI EN 319 401 §7.4-§7.8 (Access control); EN 319 411-1 §6.4.3 (Procedural controls); §6.4.4 (Personnel controls); EN 319 411-2 §6.4.3 (Procedural controls for qualified services).

Wallet Provider shall provision, modify, revoke and document access rights in accordance with its access control policy. Access rights shall be assigned and revoked based on the principles of need-to-know, least privilege and segregation of duties. Wallet Provider shall maintain a register of access rights granted and apply logging to the management of access rights. Access rights shall be reviewed at planned intervals.

[REQ-2690-45]



**Alignment with international standards** — ISO/IEC 27001:2022 A.5.18 (access rights); A.8.2 (privileged access rights). | ETSI EN 319 401 §7.4-§7.8 (Access management); EN 319 411-1 §6.4.3 (Procedural controls); §6.4.4 (Personnel controls).

## 5.2.7 Incident Management

48

### EP-26

Wallet Provider shall establish and implement an incident management policy laying down the roles, responsibilities, and procedures for detecting, analysing, containing, or responding to, recovering from, documenting and reporting incidents in a timely manner. The policy shall be coherent with the business continuity and disaster recovery plan referred to in EP-35 and shall include:

I.a categorisation scheme for incidents that incorporate specific thresholds specified by the wallet provider under CIR (EU) 2025/847;

II. effective communication plans, including for escalation and reporting in line with the legal and contractual obligations of Wallet Provider, including obligations under the Polish Cybersecurity Act, CIR (EU) 2024/2981 and CIR (EU) 2025/847;

III. assignment of roles for incident detection and response to competent personnel;

IV. documented information to be used during incident detection and response, such as incident response plans, escalation procedures, contact lists and templates.

The policy shall also define how incident handling activities are coordinated with related security procedures, including vulnerability management, change management and business continuity arrangements.

The roles, responsibilities and procedures shall be evaluated and reviewed, and where appropriate updated, at planned intervals and after significant incidents.

[REQ-1502-20; REQ-2690-15; REQ-847-01]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.24 (planning & preparation of IS incident management); A.5.25 (assessment and decision on IS events); A.5.26 (response to IS incidents); A.5.27 (learning from IS incidents). | ETSI EN 319 401 §7.9 (Incident management); EN 319 411-1 §6.4.8 (Compromise and disaster recovery); EN 319 411-2 §6.4.8 (Compromise and disaster recovery for qualified services).

49

### EP-27

Wallet Provider shall put in place a mechanism allowing its personnel, suppliers, and customers to report information security events. Wallet Provider shall

ensure that all personnel are explicitly informed of the rules and procedures for reporting incidents. Wallet Provider shall, where appropriate, communicate the event reporting mechanism to its suppliers and customers, and shall regularly train personnel on its use.

[REQ-2690-17,REQ-847-4]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.25 (assessment & decision on IS events); A.6.8 (reporting of IS events). | ETSI EN 319 401 §7.9 (Reporting of incidents); EN 319 411-1 §6.4.8 (Compromise and disaster recovery).

50

#### EP-28

Wallet Provider shall assess information security events to determine whether they constitute incidents and, if so, determine their nature and severity. The assessment shall be based on predefined criteria and shall include a triage for prioritisation. Wallet Provider shall assess the existence of recurring incidents on a regular basis.

[REQ-2690-18]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.25 (assessment & decision on IS events). | ETSI EN 319 401 §7.9 (Incident classification); EN 319 411-1 §6.4.8 (Compromise and disaster recovery).

51

#### EP-29

Wallet Provider shall respond to incidents in accordance with documented procedures, including containment, eradication, and recovery stages. Wallet Provider shall log incident response activities and record evidence.

[REQ-2690-19]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.26 (response to IS incidents). | ETSI EN 319 401 §7.9 (Handling of incidents); EN 319 411-1 §6.4.8 (Compromise and disaster recovery).

52

#### EP-30

Wallet Provider shall, where appropriate, conduct post-incident reviews after recovery from incidents. The reviews shall identify, where possible, the root cause of the incident and result in documented lessons learned. Wallet Provider shall ensure that post-incident reviews contribute to improving its approach to information security, risk treatment, and incident management procedures.

[REQ-2690-20]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.27 (learning from IS incidents). | ETSI EN 319 401 §7.9 (Lessons learned from incidents); EN 319 411-1 §6.4.8 (Compromise and disaster recovery).

**Additional standards and references** — GDPR Article 33 (notification of personal data breach to supervisory authority within 72 hours); GDPR Article 34 (communication of breach to data subjects); CRA Annex I Part II §5(1) (handling and coordinated disclosure of vulnerabilities).

**Additional standards and references** — GDPR Article 33 (notification of personal data breach to supervisory authority within 72 hours of becoming aware); GDPR Article 34 (communication of the breach to the affected data subjects without undue delay where the breach is likely to result in high risk); CRA (Regulation (EU) 2024/2847) Annex I Part II §5(1) (handling and disclosure of vulnerabilities, including coordinated disclosure obligations).

## 5.2.8 Vulnerability Management and Disclosure

53

### EP-31

Wallet Provider shall establish, maintain, and operate a vulnerability management process. The process shall include, as a minimum:

- I. procedures for the identification of vulnerabilities in the Wallet Provider information systems, including through monitoring of appropriate channels such as announcements of CSIRTs (e.g., CERT Polska), competent authorities, and information provided by suppliers;
- II. procedures for the evaluation and prioritisation of identified vulnerabilities based on their severity and potential impact on the wallet solution and related services;
- III. procedures for associating identified vulnerabilities, where applicable, with the affected information systems, software components or other assets supporting the wallet-related services, and with the corresponding treatment decision, remediation action or mitigation plan;
- IV. procedures for the timely remediation or mitigation of vulnerabilities, ensuring that critical vulnerabilities are addressed without undue delay within timeframes defined in the vulnerability management policy;
- V. procedures for the verification that remediation or mitigation measures have been effectively applied;
- VI. where appropriate, performance of vulnerability scans on public and private IP addresses at least once per quarter with evidence of the results recorded.

The vulnerability management process shall be aligned with Wallet Provider's change management, patch management, risk management and incident

management procedures, and shall consider the procedures set out in EN ISO/IEC 30111:2019 and the requirements set out in Annex I to Regulation (EU) 2024/2847 (Cyber Resilience Act).

[REQ-2690-35; REQ-2981-07; REQ-2981-10]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.8 (management of technical vulnerabilities). | ETSI EN 319 401 §7.9 (Vulnerability management); EN 319 411-1 §6.4.8 (Compromise and disaster recovery).

54

## EP-32

Wallet Provider shall prepare a vulnerability impact analysis report for any vulnerability that affects the software components of the wallet solution and submit it to the Scheme Owner without undue delay. The report shall include:

- I. the impact of vulnerability on the certified wallet solution;
- II. possible risks associated with the proximity or likelihood of an attack;
- III. whether the vulnerability can be remedied using available means;
- IV. where the vulnerability can be remedied, possible ways to remedy it.

The Wallet Provider, acting together with the Scheme Owner, shall determine, based on defined criteria established in accordance with this document, whether notification to the CAB is required.

[REQ-2981-08; REQ-2981-09]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.8 (technical vulnerability management); A.5.26 (response to IS incidents). | ETSI EN 319 401 §7.9 (Vulnerability analysis); EN 319 411-1 §6.4.8 (Compromise and disaster recovery).

**Additional standards and references** — CRA (Regulation (EU) 2024/2847) Annex I Part I §2(i) (policy on coordinated vulnerability disclosure as essential cybersecurity requirement); ARF v2.8.0 §6.4 (vulnerability management for wallet solution components).

**Additional standards and references** — CRA (Regulation (EU) 2024/2847) Annex I Part I §2(i) (essential cybersecurity requirement to have a policy on coordinated vulnerability disclosure); ARF v2.8.0 §6.4 (vulnerability management requirements specific to wallet solution components, including wallet instance and WSCD firmware).

55

## EP-33

Wallet Provider shall disclose and register any officially known and remediated vulnerability in the wallet solution in one of the online repositories referred to in Annex V to CIR (EU) 2024/2981. Wallet Provider shall lay down a procedure for disclosing vulnerabilities in accordance with applicable national coordinated vulnerability disclosure policy.

[REQ-2981-11]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.8 (technical vulnerability management). / ETSI EN 319 401 §7.9 (Vulnerability disclosure); EN 319 411-2 §6.4.8 (Compromise and disclosure for qualified services).

## 5.2.9 Business Continuity Management

56

### EP-34

Wallet Provider shall determine its requirements for the continuity of the wallet-related services in adverse situations. Wallet Provider shall identify the critical services and the information systems supporting those services, assess the potential impact of disruptions, and establish recovery objectives, including recovery time objectives and recovery point objectives, for those critical services ensuring sufficient availability by providing at least partial redundancy for network systems, facilities, communication channels, and personnel with necessary competence.

[REQ-1502-05; REQ-2690-21]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.29 (IS during disruption); A.5.30 (ICT readiness for business continuity); cl. 8.1 (operational planning). / ETSI EN 319 401 §7.11 (Business continuity); EN 319 411-1 §6.4.8 (Compromise and disaster recovery); §6.4.9 (CA/RA termination); EN 319 411-2 §6.4.8 (Compromise and disaster recovery for qualified services).

57

### EP-35

Wallet Provider shall establish and maintain a business continuity and disaster recovery plans to be applied in the case of incidents. The plan shall be based on the results of risk assessments and a business impact analysis, and shall include, where appropriate:

- I. purpose, scope and audience;
- II. roles and responsibilities;
- III. key contacts and communication channels;
- IV. conditions for plan activation and deactivation;
- V. order of recovery for operations;
- VI. recovery plans for specific operations, including recovery objectives;
- VII. required resources, including backups and redundancies;
- VIII. restoring and resuming activities from temporary measures.

The plan shall be evaluated, reviewed and, where appropriate, updated at planned intervals and following significant incidents or significant changes.

[REQ-1502-05; REQ-2690-21]

58

#### EP-36

Wallet Provider shall maintain backup copies of data at planned intervals commensurate with the criticality of the data and service recovery objectives, ensuring that critical data and logs are backed up according to a defined backup policy at least once a day and provide sufficient available resources, including facilities, information systems, and personnel, to ensure an appropriate level of redundancy. Wallet Provider shall establish backup plans that address recovery times, backup completeness and accuracy, storage in safe locations, access controls, restoring procedures, and retention periods. Wallet Provider shall perform regular integrity checks on backup copies and regular testing of recovery.

[REQ-2690-22]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.13 (information backup). | ETSI EN 319 401 §7.10 (Backup and recovery); EN 319 411-1 §6.4.8 (Compromise and disaster recovery); EN 319 411-2 §6.4.8 (Compromise and disaster recovery for qualified services).

**Additional standards and references** — GDPR Article 32(1)(d) (regularly testing and evaluating effectiveness of security measures); ARF v2.8.0 §6.4 (audit logging requirements for wallet unit lifecycle events and server-side infrastructure).

**Additional standards and references** — GDPR Article 32(1)(d) (processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing, including logging and monitoring); ARF v2.8.0 §6.4 (audit logging requirements for wallet unit lifecycle events and server-side infrastructure).

59

#### EP-37

Wallet Provider shall put in place a process for crisis management that addresses:

- I. roles and responsibilities for personnel and, where appropriate, suppliers and service providers, in crisis situations;
- II. appropriate communication between Wallet Provider and relevant competent authorities, including the Scheme Owner, Supervisory Body and CERT Polska;
- III. application of appropriate measures to ensure the maintenance of information security in crisis situations.

Wallet Provider shall implement a process for managing and making use of information received from CSIRTs or competent authorities concerning incidents,

vulnerabilities, threats, or mitigation measures. The crisis management plan shall be evaluated, reviewed and, where appropriate, updated on a regular basis.

[REQ-2690-23]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.29 (IS during disruption); A.5.30 (ICT readiness for business continuity). | ETSI EN 319 401 §7.10 (Crisis management); EN 319 411-1 §6.4.8 (Compromise and disaster recovery).

## 5.2.10 Compliance, Audit, and Independent Review

60

### EP-38

Wallet Provider shall regularly review its compliance with the requirements imposed on it as Wallet Provider through periodical independent internal audits, scoped to include all parts relevant to the provisioning of the wallet-related services. The independent internal audits shall be conducted by an auditor with appropriate competence who is not in the line of authority of the personnel of the area under review. Top management shall be informed of the result of the compliance review based on audit results by means of regular reporting. The audits shall be performed at planned intervals and when significant changes to operations or risks occur.

**NOTE** — The certification assessment performed by the CAB under the eID Certification Scheme (GP-03) constitutes the external audit for the purposes of this document. The internal audits required by this provision are complementary to the certification assessment.

[REQ-1502-23; REQ-2690-13; REQ-2690-14]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.35 (independent review of IS); A.5.36 (compliance with policies); cl. 9.2 (internal audit). | ETSI EN 319 401 §7.4-§7.8 (Internal audit); EN 319 411-1 §6.9.1 (Organisational); EN 319 411-2 §6.9.1 (Organisational requirements for QTSPs).

## 5.2.11 Record keeping

61

### EP-39

Wallet Provider shall record and maintain relevant documented information using an effective record-management system, considering applicable legislation and good practice in relation to data protection and data retention, including the Act of 14 July 1983 on national archival records and archives (Dz.U. 2020 poz. 164, z późn. zm.) as applicable.

[REQ-1502-11]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.33 (protection of records); A.5.34 (privacy and protection of PII). | ETSI EN 319 401 §7.3 (Document and records management); EN 319 411-1 §6.4.6 (Records archival); §5.2 (CPS requirements).

62

### EP-40

Wallet Provider shall, as far as permitted by national law, retain and protect records for as long as they are required for the purpose of auditing and investigation of security breaches. After the required retention period, records shall be securely destroyed, and such action shall be documented.

[REQ-1502-12]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.33 (protection of records); A.5.34 (privacy and protection of PII). | ETSI EN 319 401 §7.3 (Records retention); EN 319 411-1 §6.4.6 (Records archival).

63

#### EP-41

Wallet Provider shall store securely, for at least five years after the cancellation or expiry of the relevant certificate of conformity:

- I. records of the information provided to the CAB or any of its sub-contractors during the certification process;
- II. specimens of hardware components that have been included in the scope of certification for the wallet solution.

Wallet Provider shall make this documented information available to the CAB or to the Scheme Owner in its capacity as the supervisory body pursuant to Article 46a (1) of Regulation (EU) No 910/2014, upon request.

[REQ-2981-13; REQ-2981-14]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.33 (protection of records); A.5.34 (privacy and protection of PII). | ETSI EN 319 401 §7.3 (Long-term archiving); EN 319 411-1 §6.4.6 (Records archival); EN 319 411-2 §6.4.6 (Records archival for qualified services).

## 5.3 People Controls

This subsection is aligned with the people control theme (A.6) of ISO/IEC 27001:2022, Annex A.

### 5.3.1 Screening

64

#### EP-42

Wallet Provider shall ensure, to the extent feasible and in accordance with applicable Polish law, verification of the background of its personnel, reviewing and updating the background verification policy at least every two years and where applicable of direct suppliers and service providers, where necessary for their role, responsibilities, and authorisations. Wallet Provider shall establish criteria setting out which roles require background verification, considering applicable laws, regulations, and ethics in proportion to risk and the classification of the information systems to be accessed.



[REQ-2690-41]

**Alignment with international standards** — ISO/IEC 27001:2022 A.6.1 (screening); A.6.2 (terms and conditions of employment). | ETSI EN 319 401 §7.4-§7.8 (Personnel security — verification); EN 319 411-1 §6.4.4 (Personnel controls).

**Additional standards and references** — ARF v2.8.0 §6.3 (availability and resilience for WUA issuance and validity status services); GDPR Article 32(1)(b) (resilience of processing systems and services).

**Additional standards and references** — ARF v2.8.0 §6.3 (availability and resilience requirements for WUA issuance services and validity status services); GDPR Article 32(1)(b) (ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services as an appropriate technical measure).

### 5.3.2 Terms and Conditions of Employment

65      **EP-43**

Wallet Provider shall ensure that all personnel and direct suppliers and service providers understand and commit to their information security responsibilities, as appropriate for the services offered and their role, and in line with Wallet Provider 's information security policy.

[REQ-2690-40]

**Alignment with international standards** — ISO/IEC 27001:2022 A.6.2 (terms and conditions of employment); A.6.5 (responsibilities after termination or change of employment). | ETSI EN 319 401 §7.4-§7.8 (Personnel obligations); EN 319 411-1 §6.4.3 (Procedural controls); §6.4.4 (Personnel controls).

### 5.3.3 Responsibilities After Termination or Change of Employment

66      **EP-44**

Wallet Provider shall ensure that information security responsibilities and duties that remain valid after termination or change of employment are contractually defined and enforced.

[REQ-2690-42]

**Alignment with international standards** — ISO/IEC 27001:2022 A.6.5 (responsibilities after termination or change of employment). | ETSI EN 319 401 §7.4-§7.8 (post-employment obligations); EN 319 411-1 §6.4.4 (Personnel controls).

### 5.3.4 Information Security Awareness, Education and Training

67      **EP-45**

Wallet Provider shall have procedures in place to ensure that personnel and subcontractors are sufficiently trained, qualified, and experienced in the competences needed to execute the roles they fulfil in connection with the wallet-related services. Wallet Provider shall ensure that personnel whose roles require

security-relevant competence receive regular training on information security, ensuring that personnel in trusted roles receive updates on new threats and current security practices at least every 12 months. Wallet Provider shall establish, implement, and apply a training programme in line with its information security policy, which shall:

- I. be relevant to the job function of the person;
- II. include instructions regarding the secure configuration and operation of information systems;
- III. include briefing on known threats;
- IV. include training on behaviour when information security events occur.

The effectiveness of training shall be assessed. Wallet Provider shall ensure that personnel involved in the development or operation of the wallet solution meet the requirements on expertise, reliability, experience, security training, and qualifications established in its human resource management policies.

[REQ-1502-13; REQ-2690-38; REQ-2690-40; REQ-2981-04]

**Alignment with international standards** — ISO/IEC 27001:2022 A.6.3 (IS awareness, education, and training). | ETSI EN 319 401 §7.4-§7.8 (Personnel competence); EN 319 411-1 §6.4.4 (Personnel controls).

68

#### EP-46

Wallet Provider shall ensure awareness raising and application of cyber hygiene practices for its personnel, including members of top management, as well as for direct suppliers and service providers where appropriate. Wallet Provider shall offer an awareness raising programme that is scheduled over time, established in line with its information security policy, and covers relevant threats, information security risk treatment measures, contact points and resources for additional information, and cyber hygiene practices.

[REQ-2690-37]

**Alignment with international standards** — ISO/IEC 27001:2022 A.6.3 (IS awareness, education, and training); A.5.4 (management responsibilities). | ETSI EN 319 401 §7.4-§7.8 (Security awareness); EN 319 411-1 §6.4.4 (Personnel controls).

### 5.3.5 Disciplinary Process

69

#### EP-47

Wallet Provider shall establish, communicate, and maintain a disciplinary process for handling violations of information security policies.

[REQ-2690-43]

**Alignment with international standards** — ISO/IEC 27001:2022 A.6.4 (disciplinary process). | ETSI EN 319 401 §7.4-§7.8 (Policy violations); EN 319 411-1 §6.4.4 (Personnel controls).

## 5.4 Physical Controls

70 This subsection is aligned with the physical control theme (A.7) of ISO/IEC 27001:2022, Annex A.

### 5.4.1 Physical Security Perimeters and Entry Controls

71 **EP-48**

Facilities used for providing the wallet-related services service shall ensure that access to areas holding or processing personal, cryptographic, or other sensitive information is limited to authorised personnel or subcontractors. Wallet Provider shall define and use security perimeters, protect areas by appropriate entry controls and access points, design and implement physical security for offices, rooms, and facilities, and continuously monitor its premises for unauthorised physical access.

[REQ-1502-16; REQ-2690-58]

**Alignment with international standards** — ISO/IEC 27001:2022 A.7.1 (physical security perimeters); A.7.2 (physical entry); A.7.3 (securing offices, rooms, and facilities); A.7.4 (physical security monitoring). | ETSI EN 319 401 §7.4-§7.8 (Physical security); EN 319 411-1 §6.4.2 (Physical security controls); EN 319 411-2 §6.4.2 (Physical security controls for qualified services).

### 5.4.2 Environmental Protection

72 **EP-49**

Facilities used for providing the wallet-related service shall be continuously monitored for, and protected against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service.

[REQ-1502-15; REQ-2690-57]

**Alignment with international standards** — ISO/IEC 27001:2022 A.7.5 (protecting against physical and environmental threats). | ETSI EN 319 401 §7.4-§7.8 (Environmental protection); EN 319 411-1 §6.4.2 (Physical security controls).

### 5.4.3 Supporting Utilities

73 **EP-50**

Wallet Provider shall prevent loss, damage or compromise of information systems or interruption to their operations due to the failure and disruption of supporting utilities. Wallet Provider shall, where appropriate:

- I. protect facilities from power failures and other disruptions caused by failures in supporting utilities;
- II. consider the use of redundancy in utility services;
- III. protect utility services that transport data or supply information systems against interception and damage;
- IV. monitor utility services and report events outside control thresholds;
- V. conclude contracts for emergency supply;
- VI. ensure continuous effectiveness, monitor, maintain and test the supply of the information systems necessary for operation.

[REQ-2690-56]

#### 5.4.4 Storage Media

74

##### EP-51

All media containing personal, cryptographic, or other sensitive information shall be stored, transported, and disposed of in a safe and secure manner.

[REQ-1502-21]

**Alignment with international standards** — ISO/IEC 27001:2022 A.7.10 (storage media); A.7.14 (secure disposal or re-use of equipment). | ETSI EN 319 401 §7.3 (Handling of media); EN 319 411-1 §6.4.2 (Physical security controls); §6.4.6 (Records archival).

75

##### EP-52

Wallet Provider shall establish, implement and apply a policy on the management of removable storage media, providing for the technical prohibition of connection of removable media unless there is an organisational reason, disabling of self-execution, scanning for malicious code, measures for controlling portable storage devices, and use of cryptographic techniques where appropriate.

[REQ-2690-53]

**Alignment with international standards** — ISO/IEC 27001:2022 A.7.10 (storage media); A.8.11 (data masking). | ETSI EN 319 401 §7.3 (Removable media); EN 319 411-1 §6.4.2 (Physical security controls).

76

##### EP-53

Wallet Provider shall establish procedures for the deposit, return, or deletion of assets upon termination of employment.

[REQ-2690-55]

***Alignment with international standards*** — ISO/IEC 27001:2022 A.6.5 (responsibilities after termination); A.7.10 (storage media). | ETSI EN 319 401 §7.4-§7.8 (Return of assets); EN 319 411-1 §6.4.4 (Personnel controls).

## 5.5 Technological Controls

77            *NOTE: This subsection is aligned with the technological control theme (A.8) of ISO/IEC 27001:2022, Annex A.*

### 5.5.1 Privileged Access and Identity Management

#### 78            **EP-54**

Wallet Provider shall maintain policies for the management of privileged accounts and system administration accounts supporting the wallet-related services. The policies shall establish strong identification, authentication and authorisation procedures for such accounts, set up specific accounts for system administration operations exclusively, individualise and restrict system administration privileges, and provide that system administration accounts are used only to connect to system administration systems.

System administration of components that process or manage critical assets shall be subject to dual control, requiring at least two authorised persons to act together for such operations. Wallet Provider shall document the procedures and roles subject to dual control.

*[REQ-2690-46; REQ-2690-47; REQ-1502-17]*

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.2 (privileged access rights); A.5.17 (authentication information); A.5.3 (segregation of duties). | ETSI EN 319 401 §7.4-§7.8 (Privileged accounts); EN 319 411-1 §6.4.3 (Procedural controls); §6.5.2 (Private key protection and cryptographic module engineering controls); EN 319 411-2 §6.5.2 (Private key protection for qualified services).

#### 79            **EP-55**

Wallet Provider shall manage the full life cycle of identities of information systems and their users, including setting up unique identities, linking user identities to a single person, ensuring oversight of identities, and applying logging to the management of identities. Identities assigned to multiple persons shall only be permitted where necessary for business or operational reasons and shall be subject to explicit approval and documentation. Wallet Provider shall regularly review identities of information systems and their users and deactivate identities that are no longer needed without delay.

*[REQ-2690-48]*

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.16 (identity management); A.8.3 (restriction of access to information). | ETSI EN 319 401 §7.4-§7.8 (Identity management); EN 319 411-1 §6.4.3 (Procedural controls); §6.4.4 (Personnel controls).

**Additional standards and references** — ARF v2.8.0 §6.2 (cryptographic requirements for WUA signing, PID signing and relying party authentication); CIR (EU) 2025/849 (updated

cryptographic standards); ENISA 'Agreed Cryptographic Mechanisms' (ECSG Sub-group on Cryptography).

**Additional standards and references** — ARF v2.8.0 §6.2 (cryptographic requirements for wallet unit attestation signing, PID signing and relying party authentication, including algorithms, key lengths and certificate formats); CIR (EU) 2025/849 (updated cryptographic standards references for EUDI Wallet ecosystem); ENISA 'Agreed Cryptographic Mechanisms' (ECSG Sub-group on Cryptography, published by ENISA).

## 5.5.2 Authentication

### 80 EP-56

Wallet Provider shall implement secure authentication procedures and technologies. Wallet Provider shall ensure that the strength of authentication is appropriate to the classification of the asset to be accessed. Wallet Provider shall, to the extent feasible, use state-of-the-art authentication methods and unique authentication information.

[REQ-2690-49]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.5 (secure authentication). | ETSI EN 319 401 §7.4-§7.8 (Personnel authentication); EN 319 411-1 §6.4.3 (Procedural controls).

### 81 EP-57

Wallet Provider shall ensure that users are authenticated by multiple authentication factors or continuous authentication mechanisms for accessing the information systems supporting the wallet-related services, where appropriate, in accordance with the classification of the asset to be accessed.

[REQ-2690-50]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.5 (secure authentication). | ETSI EN 319 401 §7.4-§7.8 (Strong authentication); EN 319 411-1 §6.4.3 (Procedural controls); EN 319 411-2 §6.4.3 (Procedural controls for qualified services).

## 5.5.3 Protection Against Malware

### 82 EP-58

Wallet Provider shall protect its information systems against malicious and unauthorised software by implementing measures that detect or prevent the use of such software. Wallet Provider shall, where appropriate, ensure that its systems are equipped with detection and response software that is updated at least daily.

[REQ-2690-34]

*Alignment with international standards — ISO/IEC 27001:2022 A.8.7 (protection against malware). | ETSI EN 319 401 §7.4-§7.8 (Software protection); EN 319 411-1 §6.4.3 (Procedural controls); §6.5.5 (Computer security controls).*

## 5.5.4 Logging and Monitoring

83

### EP-59

Wallet Provider shall lay down procedures and use tools to monitor and log activities on its information systems to detect events that could constitute incidents. Monitoring shall, to the extent feasible, be automated and conducted either continuously or at periodic intervals. Wallet Provider shall maintain, document and review logs, ensuring that the time used to record events in the audit log is synchronized with UTC at least once a day, which shall include, where appropriate:

- I. relevant outbound and inbound network traffic;
- II. creation, modification or deletion of users;
- III. access to systems and applications;
- IV. authentication-related events;
- V. all privileged access activities;
- VI. access or changes to critical configuration and backup files;
- VII. event logs from security tools;
- VIII. use of system resources;
- IX. physical access to facilities;
- X. access to network equipment and devices;
- XI. activation, stopping and pausing of the various logs;
- XII. environmental events.

Logs shall be regularly reviewed, alarm thresholds shall be laid down where appropriate, and logs shall be maintained, backed up, and protected from unauthorised access or changes for a predefined period.

[REQ-2690-16]

*Alignment with international standards — ISO/IEC 27001:2022 A.8.15 (logging); A.8.16 (monitoring activities). | ETSI EN 319 401 §7.4-§7.8 (System monitoring); EN 319 411-1 §6.4.5 (Audit logging procedures); EN 319 411-2 §6.4.5 (Audit logging for qualified services).*



### 5.5.5 Network Security

84

#### EP-60

Wallet Provider shall respond appropriately to protect its network infrastructure and communication channels from threats. Wallet Provider shall in particular:

- I. document the architecture of the network in a comprehensible and up-to-date manner;
- II. determine and apply controls to protect internal network domains from unauthorised access;
- III. configure controls to prevent access and network communication not required for the operation of the wallet-related services;
- IV. determine and apply controls for remote access to information systems;
- V. not use systems used for administration of the security policy for other purposes;
- VI. explicitly forbid or deactivate unneeded connections and services;
- VII. where appropriate, exclusively allow access by devices authorised by Wallet Provider;
- VIII. allow connections of service providers only after an authorisation request and for a set period;
- IX. establish communication between distinct systems only through trusted channels that are isolated and provide assured identification of endpoints and protection of channel data;
- X. apply best practices for DNS security, Internet routing security and routing hygiene.
- XI. establish and implement a plan for the transition towards latest generation network layer communication protocols, where applicable;
- XII. adopt an implementation plan for the deployment of internationally agreed and interoperable modern e-mail communication standards, where applicable;

Wallet Provider shall review and, where appropriate, update network security measures at planned intervals and when significant incidents or significant changes to operations occur.

[REQ-2690-32]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.20 (networks security); A.8.21 (security of network services). / ETSI EN 319 401 §7.4-§7.8 (Network security); EN 319 411-1 §6.5.7 (Network security controls).

### 5.5.6 Segregation of Networks

85

#### EP-61

Wallet Provider shall segment its systems into networks or zones in accordance with the results of risk assessments. Wallet Provider shall segment its systems and networks from third parties' systems and networks, and shall in particular:

- I. grant access to a network or zone based on an assessment of its security requirements;
- II. keep systems critical to Wallet Provider 's operation in secured zones;
- III. deploy a demilitarised zone for secure communication;
- IV. restrict access and communications between and within zones to those necessary for operation;
- V. separate the dedicated network for administration from the operational network;
- VI. separate production systems from development and testing systems.
- VII. define traffic segregation rules taking to account the functional, logical and physical relationship, including location, between trustworthy systems and services;
- VIII. separate network administration channels from other network traffic;

Wallet Provider shall review and, where appropriate, update network segmentation at planned intervals and when significant incidents or significant changes to operations occur.

[REQ-2690-33]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.22 (segregation of networks). | ETSI EN 319 401 §7.4-§7.8 (Network architecture); EN 319 411-1 §6.5.7 (Network security controls).

### 5.5.7 Configuration Management

86

#### EP-62

Wallet Provider shall take appropriate measures to establish, document, implement and monitor configurations, including security configurations of hardware, software, services, and networks supporting the wallet-related services. Wallet Provider shall establish and ensure secure configurations and implement processes and tools to enforce them for newly installed systems as well as for systems in operation. Wallet Provider shall review and, where appropriate, update configurations at planned intervals and when significant incidents or significant changes to operations occur.

[REQ-1502-20; REQ-2690-28]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.9 (configuration management). | ETSI EN 319 401 §7.4-§7.8 (System configuration); EN 319 411-1 §6.4.3 (Procedural controls); §6.5.5 (Computer security controls).

### 5.5.8 Change Management

87

#### EP-63

Wallet Provider shall apply change management procedures to control changes to information systems supporting the wallet-related services. The procedures shall apply to releases, modifications and emergency changes of any software and hardware in operation and to changes to configuration. Changes shall be documented and based on risk assessment, evaluated and assessed and, where appropriate, tested in view of their potential impact on the wallet-related service, related security controls and configurations, before implementation. Where emergency procedures are followed, the result and reasons shall be documented. Wallet Provider shall review the change management procedures at planned intervals and when significant incidents or significant changes to operations occur, and shall update them where appropriate.

Wallet Provider shall notify the Ministry of Digital Affairs of changes to the certified wallet solution. Wallet Provider shall obtain the necessary certification maintenance and, where applicable, demonstrate continued compliance with the Trust Framework before deploying new versions of the wallet solution within the scheme.

[REQ-1502-20; REQ-2690-29; REQ-2981-03]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.32 (change management). | ETSI EN 319 401 §7.4-§7.8 (Change management); EN 319 411-1 §6.4.3 (Procedural controls); EN 319 411-2 §6.4.3 (Procedural controls for qualified services).

### 5.5.9 Patch Management

88

#### EP-64

Wallet Provider shall specify and apply procedures for security patch management, ensuring that:

- I. security patches are applied within a reasonable time after they become available;
- II. security patches are tested before being applied in production systems;
- III. security patches come from trusted sources and are checked for integrity;
- IV. additional measures are implemented and residual risks are accepted where a patch is not available or not applied.

Wallet Provider may choose not to apply a security patch where the disadvantages outweigh the information security benefits, provided the reasons are documented and substantiated.

[REQ-1502-20; REQ-2690-31]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.8 (management of technical vulnerabilities); A.8.19 (installation of software on operational systems). | ETSI EN 319 401 §7.4-§7.8 (Updates and patching); EN 319 411-1 §6.4.3 (Procedural controls); §6.5.6 (Life cycle security controls).

### 5.5.10 Cryptography and Key Management

89

#### EP-65

Wallet Provider shall establish, implement, and apply a policy and procedures related to cryptography, ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and integrity of data processed in connection with the wallet-related services. The policy shall establish, as a minimum:

- I. type, strength and quality of cryptographic measures required, based on the classification of assets;
- II. protocols, algorithms, cipher strengths, and cryptographic solutions approved for use;
- III. approach to key management, covering the full key life cycle including generation, issuance, distribution, storage, change, revocation, recovery, backup, destruction, logging and auditing.

The policy shall be reviewed and updated at planned intervals, considering the state of the art in cryptography.

**NOTE** — *The information classification scheme referred to in EP-22 shall ensure that personal or sensitive information is classified at a level that requires cryptographic protection of electronic communication channels against eavesdropping, manipulation, and replay.*

[REQ-1502-18; REQ-1502-19; REQ-1502-22; REQ-2690-39]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.24 (use of cryptography); A.8.25 (secure development life cycle). | ETSI EN 319 401 §7.4-§7.8 (Cryptographic policy); EN 319 411-1 §6.5.1 (Key pair generation and installation); §6.5.2 (Private key protection and cryptographic module engineering controls); EN 319 411-2 §6.5.1 (Key pair generation for qualified services); §6.5.2 (Private key protection for qualified services).

90

## EP-66

Access to sensitive cryptographic material used for issuing electronic identification means and authentication in the scheme shall be restricted to the roles and applications strictly requiring access. Such material shall never be persistently stored in plain text. Sensitive cryptographic material shall be protected from tampering.

Key management operations on cryptographic material that constitutes critical assets, including key generation, activation, backup, recovery, and destruction, shall be subject to dual control, requiring at least two authorised persons to act together. Wallet Provider shall maintain records of all such operations.

**NOTE** — *Protection from tampering should include implementation of both physical and logical security controls throughout the full key life cycle. Hardware security modules (HSMs) certified under recognised schemes are good practice for this purpose. Products should be sourced from a trusted vendor and commissioned in a manner that ensures the chain of custody from manufacture to production use.*

[REQ-1502-19; REQ-1502-22]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.24 (use of cryptography); A.5.17 (authentication information — key protection). | ETSI EN 319 401 §7.4-§7.8 (Key protection); EN 319 411-1 §6.5.1 (Key pair generation and installation); §6.5.2 (Private key protection and cryptographic module engineering controls); EN 319 411-2 §6.5.2 (Private key protection for qualified services).

## 5.5.11 Secure Acquisition, Development and Maintenance

91

## EP-67

Wallet Provider shall set and implement processes to manage risks stemming from the acquisition of ICT services or ICT products for components critical to the security of its information systems, throughout their life cycle. The processes shall

include security requirements, update requirements, component information, security function documentation, compliance assurance, and validation methods. Wallet Provider shall review and, where appropriate, update these processes at planned intervals and when significant incidents occur.

[REQ-2690-26]

**Alignment with international standards** — ISO/IEC 27001:2022 A.5.21 (managing IS in ICT supply chain); A.8.30 (outsourced development). | ETSI EN 319 401 §7.14 (Security of procurement); EN 319 411-1 §6.9.1 (Organisational); §6.8.6 (Representations and warranties).

92

#### EP-68

Before developing information systems, including software, in connection with the wallet-related services, Wallet Provider shall establish rules for secure development. Where Wallet Provider develops systems in-house or outsources development, the rules shall cover all development phases and shall include security requirements analysis, secure engineering and coding principles, security testing processes, and appropriate handling of test data.

[REQ-2690-27]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.25 (secure development life cycle); A.8.26 (application security requirements); A.8.27 (secure systems architecture and engineering principles); A.8.28 (secure coding). | ETSI EN 319 401 §7.4-§7.8 (Secure development); EN 319 411-1 §6.5.6 (Life cycle security controls); EN 319 411-2 §6.5.6 (Life cycle security controls for qualified services).

### 5.5.12 Security Testing

93

#### EP-69

Wallet Provider shall establish, implement, and apply a policy and procedures for security testing of the information systems supporting the wallet-related services. Wallet Provider shall establish, based on risk assessment, the need, scope, frequency, and type of security tests, and shall conduct security tests including penetration tests performed at least once per year, document the results, and apply mitigating measures for critical findings. Wallet Provider shall regularly review and, where appropriate, update the security testing policy and procedures.

[REQ-2690-30]

**Alignment with international standards** — ISO/IEC 27001:2022 A.8.29 (security testing in development and acceptance). | ETSI EN 319 401 §7.4-§7.8 (Security testing); EN 319 411-1 §6.5.6 (Life cycle security controls); EN 319 411-2 §6.5.6 (Life cycle security controls for qualified services).

## Annex A (Informative) — Provision-to-Requirement Mapping

94 The following table provides an informative mapping of the provisions in Section 6 to the legal requirements listed in Section 5.

| Provision | Title                                           | Legal basis (Section 5)                            |
|-----------|-------------------------------------------------|----------------------------------------------------|
| EP-01     | Information security management system          | REQ-1502-09; REQ-1502-10; REQ-1502-14; REQ-2690-09 |
| EP-02     | Legal entity status                             | REQ-1502-01                                        |
| EP-03     | Legal compliance                                | REQ-1502-02                                        |
| EP-04     | Financial capacity                              | REQ-1502-03                                        |
| EP-05     | Termination planning                            | REQ-1502-05                                        |
| EP-06     | Published notices and public information        | REQ-1502-06; REQ-2981-12                           |
| EP-07     | Service definition changes                      | REQ-1502-07                                        |
| EP-08     | Responses to information requests               | REQ-1502-08                                        |
| EP-09     | Certification body notification                 | REQ-2981-05; REQ-2981-06                           |
| EP-10     | Information security policy                     | REQ-1502-17; REQ-2690-01; REQ-2690-02              |
| EP-11     | Information security roles and responsibilities | REQ-2690-03 to REQ-2690-08                         |
| EP-12     | Risk management framework                       | REQ-2690-09; REQ-2981-02                           |
| EP-13     | Risk assessment process                         | REQ-2690-10; REQ-2690-11; REQ-2690-36              |
| EP-14     | Implementation-specific risk assessment         | REQ-2981-01                                        |
| EP-15     | Periodic risk review                            | REQ-2690-12                                        |
| EP-16     | Outsourcing responsibility                      | REQ-1502-04; REQ-2690-24                           |
| EP-17     | Third-party contractual requirements            | REQ-1502-04; REQ-2690-24                           |
| EP-18     | Supply chain security policy                    | REQ-2690-24                                        |
| EP-19     | Supplier registry                               | REQ-2690-25                                        |
| EP-20     | Supply chain monitoring                         | REQ-2690-24                                        |
| EP-21     | Asset inventory                                 | REQ-2690-54                                        |
| EP-22     | Information classification                      | REQ-2690-51                                        |
| EP-23     | Asset handling policy                           | REQ-2690-52                                        |
| EP-24     | Access control policy                           | REQ-1502-16; REQ-2690-44                           |
| EP-25     | Access rights management                        | REQ-2690-45                                        |

| Provision | Title                                     | Legal basis (Section 5)                            |
|-----------|-------------------------------------------|----------------------------------------------------|
| EP-26     | Incident management policy                | REQ-1502-20; REQ-2690-15                           |
| EP-27     | Event reporting mechanism                 | REQ-2690-17                                        |
| EP-28     | Incident assessment                       | REQ-2690-18                                        |
| EP-29     | Incident response                         | REQ-2690-19                                        |
| EP-30     | Post-incident review                      | REQ-2690-20                                        |
| EP-31     | Vulnerability management process          | REQ-2690-35; REQ-2981-07; REQ-2981-10              |
| EP-32     | Vulnerability impact analysis report      | REQ-2981-08; REQ-2981-09                           |
| EP-33     | Vulnerability disclosure                  | REQ-2981-11                                        |
| EP-34     | Business continuity requirements          | REQ-1502-05; REQ-2690-21                           |
| EP-35     | Business continuity and DR plan           | REQ-1502-05; REQ-2690-21                           |
| EP-36     | Backups and redundancy                    | REQ-2690-22                                        |
| EP-37     | Crisis management                         | REQ-2690-23                                        |
| EP-38     | Compliance, audit, and independent review | REQ-1502-23; REQ-2690-13; REQ-2690-14              |
| EP-39     | Record keeping system                     | REQ-1502-11                                        |
| EP-40     | Record retention and destruction          | REQ-1502-12                                        |
| EP-41     | Certification records retention           | REQ-2981-13; REQ-2981-14                           |
| EP-42     | Screening                                 | REQ-2690-41                                        |
| EP-43     | Terms and conditions of employment        | REQ-2690-40                                        |
| EP-44     | Post-employment responsibilities          | REQ-2690-42                                        |
| EP-45     | Training and qualifications               | REQ-1502-13; REQ-2690-38; REQ-2690-40; REQ-2981-04 |
| EP-46     | Cyber hygiene awareness                   | REQ-2690-37                                        |
| EP-47     | Disciplinary process                      | REQ-2690-43                                        |
| EP-48     | Physical security perimeters              | REQ-1502-16; REQ-2690-58                           |
| EP-49     | Environmental protection                  | REQ-1502-15; REQ-2690-57                           |
| EP-50     | Supporting utilities                      | REQ-2690-56                                        |
| EP-51     | Storage media                             | REQ-1502-21                                        |
| EP-52     | Removable media policy                    | REQ-2690-53                                        |



| Provision    | Title                                  | Legal basis (Section 5)                            |
|--------------|----------------------------------------|----------------------------------------------------|
| <b>EP-53</b> | Asset return on termination            | REQ-2690-55                                        |
| <b>EP-54</b> | Privileged access management           | REQ-2690-46; REQ-2690-47; REQ-1502-17              |
| <b>EP-55</b> | Identity management                    | REQ-2690-48                                        |
| <b>EP-56</b> | Authentication methods                 | REQ-2690-49                                        |
| <b>EP-57</b> | Multi-factor authentication            | REQ-2690-50                                        |
| <b>EP-58</b> | Protection against malware             | REQ-2690-34                                        |
| <b>EP-59</b> | Logging and monitoring                 | REQ-2690-16                                        |
| <b>EP-60</b> | Network security                       | REQ-2690-32                                        |
| <b>EP-61</b> | Network segregation                    | REQ-2690-33                                        |
| <b>EP-62</b> | Configuration management               | REQ-1502-20; REQ-2690-28                           |
| <b>EP-63</b> | Change management                      | REQ-1502-20; REQ-2690-29; REQ-2981-03              |
| <b>EP-64</b> | Patch management                       | REQ-1502-20; REQ-2690-31                           |
| <b>EP-65</b> | Cryptography and key management policy | REQ-1502-18; REQ-1502-19; REQ-1502-22; REQ-2690-39 |
| <b>EP-66</b> | Cryptographic material protection      | REQ-1502-19; REQ-1502-22                           |
| <b>EP-67</b> | Secure acquisition                     | REQ-2690-26                                        |
| <b>EP-68</b> | Secure development                     | REQ-2690-27                                        |
| <b>EP-69</b> | Security testing                       | REQ-2690-30                                        |