

WZ-03-03

**Organisational and Technical Requirements for EUDI
Wallet Providers including the requirements laid
down in Article 5c of the eIDAS Regulation**

VERSION 1.01

2026.04.27

Document reference	WZ-03-03
Version	1.01
Status	FINAL
Date	27.04.2026
Document type	Certification Scheme — Scheme Specification (ISO/IEC 17067)
Parent framework	GP-03 eID Certification Scheme
Scheme Owner	Republic of Poland / Minister of Digital Affairs
Certification target	Electronic identification programme — EUDI Wallet Provider
Primary audience	EUDI Wallet Provider
Secondary audience	Conformity Assessment Bodies (CABs) accredited according to G-05
Assurance level	High (Article 8 eIDAS; CIR (EU) 2015/1502)
Subsidiary Documents	WP-03, WM-03 series

Table of content

1	SCOPE.....	5
2	LEGAL BASIS.....	6
3	GENERAL PRINCIPLES	8
3.1	Proportionality to Risk.....	8
3.2	Auditability.....	8
3.3	National Law.....	8
3.4	Normative Language	8
3.5	Relationship with WZ-03-01 and WZ-03-02.....	8
4	LEGAL REQUIREMENTS.....	9
4.1	Requirements Derived from Article 5c of eIDAS (Regulation (EU) 910/2014).....	9
4.2	Requirements Derived from CIR (EU) 2024/2981	9
4.3	Requirements Derived from CIR (EU) 2024/2690	10
4.4	Requirements Derived from CIR (EU) 2015/1502	11
4.5	Requirements Derived from CIR (EU) 2024/2979	11
4.6	Requirements Derived from CIR (EU) 2025/847.....	12
5	PROVISIONS	15
5.1	General and Scheme-Specific Provisions	15
5.1.1	Certification Obligation	15
5.1.2	Scope of Certification.....	15
5.1.3	Open-Source Disclosure.....	16
5.1.4	Public Information.....	16
5.2	Certification and Conformity Assessment.....	16
5.2.1	Cybersecurity Certification.....	16
5.2.2	National Certification Scheme Compliance.....	17
5.2.3	Risk Register	17
5.2.4	Recertification and Continuous Compliance	17
5.3	Cryptographic and WSCD Requirements	18
5.3.1	Wallet Secure Cryptographic Device (WSCD).....	18
5.3.2	Wallet Unit Attestation (WUA).....	18
5.3.3	Key Management for Wallet Operations.....	18
5.4	Data Protection and Privacy Requirements	19
5.4.1	Logical Separation	19
5.4.2	Non-collection and non-combination	19
5.4.3	Unobservability and Unlikability	19
5.5	Operational Requirements.....	20
5.5.1	Assurance Level High	20
5.5.2	No-Cost-Base and Voluntary Use.....	20
5.5.3	Accessibility	20
5.5.4	Qualified Electronic Signatures	21
5.5.5	Technical Support and Reporting	21
5.5.6	Revocation	22
5.5.7	Record Keeping	22
5.5.8	Independent user services	22
5.5.9	Availability monitoring	23

5.6	Incident handling and Breach Notification	23
5.6.1	Security monitoring and unauthorised access detection	23
5.6.2	Notification to Users	24
5.6.3	Notification to CAB and Supervisory Bodies	24
5.6.4	Vulnerability Management	24
5.7	Relying Party and Interoperability Requirements	25
5.7.1	Relying Party Authentication	25
5.7.2	Common Protocols and Interfaces	25
5.7.3	Non-tracking of Attestation Use	26
6	ANNEX A (INFORMATIVE) — PROVISION-TO-REQUIREMENT MAPPING	27

1 Scope

- 1 The present document specifies the organisational and technical requirements applicable to EUDI Wallet Provider within the electronic identification system, for the purposes of certification under the eID Certification Scheme (GP-03), with particular reference to the requirements laid down in Article 5c of the eIDAS Regulation (Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183).
- 2 WZ-03-03 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 following are outside the scope of this document:
- 4 Organisational and technical requirements common to EUDI Wallet providers in relation to eID system — see WZ-03-01.
- 5 Requirements applicable to PID Providers — see WZ-03-02.
- 6 Process-specific requirements for PID enrolment, lifecycle, and wallet unit registration — see chapter 5.
- 7 Cybersecurity product certification of the wallet solution as a product — see GP-02.
- 8 Functional conformity assessment of the wallet — see GP-01.

2 Legal Basis

9 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 of 11 April 2024 (hereinafter “eIDAS”), entered into force on 20 May 2024, in particular Articles 5a, 5b, 5c, 5d, 5e and 8 thereof.
- II. 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”), 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, 8, 9, 10 and 19 thereof and Annexes I and V thereto.
- III. 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”), the Annex thereto, Sections 1–13.
- IV. 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 (hereinafter “CIR (EU) 2015/1502”), in particular Section 2.4 of the Annex thereto.
- V. 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.
- VI. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (hereinafter “EU Cybersecurity Act”), in particular Articles 49 to 56 thereof.
- VII. 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.

- VIII. Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. 2024 r. poz. 1275 z późn. zm.)
- IX. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 z późn. zm.).
- X. Regulation (EU) 2025/847 of the European Parliament and of the Council as regards reactions to security breaches of European Digital Identity Wallets
- XI. ETSI EN 319 401 V3.2.1 (2026-01) Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- XII. 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
- XIII. ETSI TS 119 431-2 V1.2.1 (2023-06) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation

3 General Principles

3.1 Proportionality to Risk

- 10 All provisions in this document shall be understood as requirements at assurance level High, as defined in Article 8 of eIDAS and CIR (EU) 2015/1502. 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.

3.2 Auditability

- 11 This document is intended for use within the eID Certification Scheme (GP-03). Wallet Provider shall ensure that its implementation of the requirements in this document is documented and verifiable by the CAB. All controls and processes shall produce evidence suitable for audit in accordance with the methodology defined in GP-03.

- 12 *NOTE: In the context of this document, a CAB means certification body.*

3.3 National Law

- 13 Where national law, in particular the Polish Act on the Application and the Polish Cybersecurity Act, imposes requirements more stringent than or additional to those in this document, Wallet Provider shall comply with the applicable national law.

3.4 Normative Language

- 14 “Shall” indicates a mandatory requirement. “Should” indicates a recommendation; deviation shall be documented and substantiated. “May” indicates an option. This usage is consistent across the WZ-03 series and GP-03.

3.5 Relationship with WZ-03-01 and WZ-03-02

- 15 The requirements of WZ-03-03 are supplementary to and do not replace the requirements of WZ-03-01. Wallet Provider shall comply with the requirements of both WZ-03-01 and WZ-03-03. The CAB shall evaluate the Wallet Provider services against all applicable WZ-series documents.

4 Legal Requirements

16 This section lists the legal requirements applicable to the EUDI Wallet Provider and underlying the provisions set out in Section 5. Requirements are labelled with a unique identifier of the form REQ-[source]-[sequence], which is used in the provisions to indicate the legal basis for each requirement.

4.1 Requirements Derived from Article 5c of eIDAS (Regulation (EU) 910/2014)

17 The following requirements are derived directly from Article 5c of the eIDAS Regulation (EU) 910/2014, as amended by Regulation (EU) 2024/1183, and from the implementing acts adopted pursuant thereto, CIR (EU) 2024/2981.

Identifier	Requirement
REQ-5c-01	The conformity of European Digital Identity Wallets and the electronic identification scheme under which they are provided with the requirements laid down in Article 5a(4), (5), (8) of eIDAS, the requirement for logical separation laid down in Article 5a(14), and, where applicable, the standards referred to in Article 5a(24), shall be certified by conformity assessment bodies designated by Member States. [Article 5c (1) eIDAS]
REQ-5c-02	Certification of the conformity of the EUDI Wallet with requirements relevant for cybersecurity shall be conducted in accordance with European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 and referred to in the implementing acts adopted under Article 5c (6) of eIDAS. [Article 5c (2) eIDAS]
REQ-5c-03	For requirements not relevant for cybersecurity, and for cybersecurity requirements not fully covered by European cybersecurity certification schemes, Member States shall establish national certification schemes following the requirements set out in the implementing acts adopted under Article 5c (6). [Article 5c (3) eIDAS]
REQ-5c-04	Providers of European Digital Identity Wallets shall, prior to placing the wallet on the market, certify the conformity of their European Digital Identity Wallets under a certification scheme referred to in Article 5c (2) and (3). [Article 5c (4) eIDAS]
REQ-5c-05	Certificates of conformity shall be recognised in all Member States and shall specify the cybersecurity certification scheme used and the relevant assurance level. [Article 5c (5) eIDAS]

4.2 Requirements Derived from CIR (EU) 2024/2981

18 Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 implements Article 5c (6) of eIDAS and establishes the mandatory

framework for national certification schemes for EUDI Wallets. The following requirements are derived from its provisions.

Identifier	Requirement
REQ-2981-W01	National certification schemes shall contain cybersecurity requirements based on a risk assessment of each specific supported architecture, aimed at treating the identified cybersecurity risks and threats in the risk register set out in Annex I. [Article 8(1)]
REQ-2981-W02	National certification schemes shall specify that the certificate of conformity covers the wallet unit, the wallet secure cryptographic application (WSCA), and the wallet secure cryptographic device (WSCD) as applicable to the supported architecture. [Article 3]
REQ-2981-W03	The Wallet Provider shall apply for certification and always maintain a valid certificate of conformity while the wallet is available to users. [Article 4]
REQ-2981-W04	The holder of a certificate of conformity shall notify the certification body without undue delay of any breach or compromise of the EUDI Wallet likely to impact the conformity of the wallet. [Article 5(2)]
REQ-2981-W05	The Wallet Provider shall establish and maintain a vulnerability management policy meeting the requirements set out in Annex I to Regulation (EU) 2024/2847 (Cyber Resilience Act), as referenced in Article 5(7) of CIR (EU) 2024/2981.
REQ-2981-W06	National certification schemes shall require assessment at assurance level 'high' as defined in the EU Cybersecurity Act, with evaluation criteria covering functional correctness, resistance to attacks, and technical security. [Articles 6 and 9]
REQ-2981-W07	Public information about the certification, including the scope, the certificate identifier, the certification body, and validity period, shall be published and kept up to date. [Article 8(5) and Annex V]
REQ-2981-W08	Records relating to the conformity assessment shall be retained for the minimum period specified in Article 19 of CIR (EU) 2024/2981 and made available to the CAB and competent supervisory authorities upon request.

4.3 Requirements Derived from CIR (EU) 2024/2690

- 19 CIR (EU) 2024/2690 of 17 October 2024 implements Article 21(2) of the NIS 2 Directive and establishes mandatory cybersecurity risk-management measures applicable to Wallet Provider as an essential entity operating critical digital infrastructure. The following requirements reflect the provisions of its Annex applicable to this context.

Identifier	Requirement
REQ-2690-W01	Wallet Provider shall adopt a policy on the security of network and information systems covering the scope of the wallet service. [Annex, Section 1]
REQ-2690-W02	Wallet Provider shall conduct risk management activities, including identification, analysis, evaluation, and treatment of risks to the network and information systems supporting the wallet service. [Annex, Section 2]

Identifier	Requirement
REQ-2690-W03	Wallet Provider shall implement incident handling procedures covering detection, classification, response, and post-incident analysis for the wallet service. [Annex, Section 3]
REQ-2690-W04	Wallet Provider shall implement business continuity and crisis management measures ensuring availability of the wallet service at the required level. [Annex, Section 4]
REQ-2690-W05	Wallet Provider shall implement supply chain security measures covering service providers and technology components that form part of the wallet infrastructure. [Annex, Section 5]
REQ-2690-W06	Wallet Provider shall implement security measures in the acquisition, development and maintenance of wallet systems and applications. [Annex, Section 6]
REQ-2690-W07	Wallet Provider shall implement effectiveness assessment, cyber hygiene, cryptography and key management, human resources, access control, asset management, and physical security measures. [Annex, Sections 7–13]

4.4 Requirements Derived from CIR (EU) 2015/1502

20 The following requirements apply to Wallet Provider in its role as provider of an electronic identification means at assurance level High, pursuant to Section 2.4 of the Annex to CIR (EU) 2015/1502.

Identifier	Requirement
REQ-1502-W01	Wallet Provider shall maintain effective management and organisation controls, including information security policy, risk management, access controls, incident management, and record keeping, consistent with Section 2.4 of the Annex to CIR (EU) 2015/1502, at assurance level High.
REQ-1502-W02	Wallet Provider shall be responsible for the fulfilment of any commitments outsourced to another entity as if it had performed the duties itself. [Annex, Section 2.4.1(4)]

4.5 Requirements Derived from CIR (EU) 2024/2979

21 Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 on the integrity and core functionalities of European Digital Identity Wallets establishes requirements for wallet unit attestation issuance, wallet provider obligations towards users, logging and data portability. The following requirements derive from the provisions applicable to Wallet Provider.

Identifier	Requirement
REQ-2979-W01	Wallet Provider shall issue Wallet Unit Attestations (WUA) in accordance with the technical specifications of CIR (EU) 2024/2979 and maintain their validity and revocability. [Articles 3, 4]

Identifier	Requirement
REQ-2979-W02	Wallet Provider shall implement logging and data portability for users and ensure users can revoke their wallet unit. [Articles 6, 7, 9, 13]
REQ-2979-W03	Wallet Provider shall ensure that wallet users can receive qualified certificates for qualified electronic signatures or seals and that Wallet Solutions securely interface with supported signature or seal creation environments. [Article 11(1)– (2)]
REQ-2979-W04	Where signature creation applications are provided or integrated with Wallet Instances, Wallet Provider shall ensure that they support the required signing and sealing functions, mandatory formats and, where applicable, the CSC API. [Article 12 and Annex IV]

4.6 Requirements Derived from CIR (EU) 2025/847

22 Commission Implementing Regulation (EU) 2025/847 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reactions to security breaches of European Digital Identity Wallets

Identifier	Requirement
REQ-847-W01	Wallet Provider shall establish and implement the criteria for assessing a security breach in the wallet solution that include: a) the breach or compromise has caused or is capable of causing the death of a natural person or considerable damage to a natural person's health; b) a successful suspectedly malicious or unauthorised access to the network and information systems has occurred, or is capable of occurring, in a way that is capable of causing severe operational disruption, c) a wallet solution, or a part of it: — is completely or projected to be completely unavailable to wallet users or wallet-relying parties for more than 12 consecutive hours; — is unavailable or projected to be unavailable to wallet users or wallet-relying parties, for more than 16 hours calculated on a calendar week basis there is a capability of compromise or there has been a compromise of physical access restricted to trusted personnel of concerned entities, or of the protection of such physical access, to one or more of the locations of network and information systems supporting the wallet solution; d) the privacy, integrity, confidentiality or authenticity of data stored, transmitted or processed in the wallet solution is compromised, or is capable of being compromised, in one or more of the following ways: — it has an impact on more than 1 % of the wallet users of the affected wallet solution or on more than 100 000 of those wallet users, whichever number is smaller; — it is a result of a successful suspectedly malicious activity;

Identifier	Requirement
	— it is a result or is likely to be a result of one or more known vulnerabilities, including those handled in accordance with Commission Implementing Regulation (EU) 2024/2981 (1); — it is likely to impact personal data in a manner that is likely to result in a risk to the rights and freedoms of the natural persons concerned and, in particular, in case of breach of personal data as defined in Articles 9(1) and 10 of Regulation (EU) 2016/679; — it is likely to impact personal electronic communications; — it is likely to result in a high risk to the rights and freedoms of natural persons; — it is likely to impact vulnerable natural persons; e) the certification of the wallet solution has been cancelled or is projected to be cancelled; f) (h) the breach or compromise has caused or is capable of causing direct financial loss for a concerned entity, and that loss exceeds EUR 500 000 or, where applicable, 5 % of the concerned entity's total annual turnover in the preceding financial year, whichever is lower. [Annex, Point 1]
REQ-847-W02	Where the Wallet Provider provides the validation mechanisms referred to in Article 5a(8), requirements b), c) and e) of REQ-847-W01 apply to this service as well. [Annex, Point 1]
REQ-847-W03	As regards point (c) of paragraph 1, the duration of an incident affecting availability shall be measured from the moment the proper provision of the affected service is disrupted until the moment the service is restored and operational again. Where the Wallet Provider is unable to determine the moment when the disruption began, the duration of the incident shall be measured from the moment the incident was detected, or from the moment when the incident was recorded in network or system logs or other data sources, whichever is earlier. Complete unavailability of a service shall be measured from the moment the service is fully unavailable to users, to the moment when regular activities or operations have been restored to the level of service provided prior to the incident. Where the Wallet Provider is unable to determine when the complete unavailability of a service began, the unavailability shall be measured from the moment it was detected by the provider. [Annex 1 Point 3]
REQ-847-04	Where the Wallet Provider provides the validation mechanisms referred to in Article 5a(8), REQ-847-W03 applies to this service as well. [Annex, Point 3]
REQ-847-W05	Wallet Provider shall implement objective criteria for defining limited availability which shall be based on the average response times of services shall be used to assess delays in response time. [Annex, Point 4]
REQ-847-W-06	Wallet Provider shall determine direct financial losses resulting from a breach or compromise referred to in point (h) of paragraph 1. The Wallet Provider shall take into account all financial losses incurred as a result of the incident, such as costs for replacement or relocation of software, hardware or

Identifier	Requirement
	infrastructure, staff costs, including costs associated with replacement or relocation of staff, recruitment of extra staff, remuneration of overtime and recovery of lost or impaired skills, fees due to non-compliance with contractual obligations, costs for redress and compensation to customers, losses due to forgone revenues, costs associated with internal and external communication, and advisory costs, including costs associated with legal counselling, forensic services and remediation services. Costs necessary for the day-to-day operation of the business, such as costs for general maintenance of infrastructure, equipment, hardware and software, improvements and risk assessment initiatives, and insurance premiums shall not be considered as financial losses resulting from an incident. Wallet Provider shall calculate the amounts of financial losses based on available data and, where the actual amounts of financial losses cannot be determined, Wallet provider shall estimate those amounts. [Annex, Point 5]
REQ-847-W-07	Where the Wallet Provider provides the validation mechanisms referred to in Article 5a(8), REQ-847-W06 applies to this service as well. [Annex, Point 5]
REQ-847-W08	Wallet Provider shall maintain mechanisms to revoke wallet unit attestations of affected wallet units where this is required as a remedy. [Article 4(2)]
REQ-847-W09	Wallet Provider shall ensure that, upon withdrawal, wallet unit attestations of affected wallet units are revoked and cannot revert to a valid state. [Article 8(2)(a), Article 8(2)(b)]
REQ-847-W10	Wallet Provider shall ensure that, upon withdrawal, no new wallet unit attestation can be issued to existing wallet units provided under the affected wallet solution. [Article 8(2)(c)]
REQ-847-W11	Wallet Provider shall ensure that, upon withdrawal, no new wallet unit can be provided under the affected wallet solution. [Article 8(2)(d)]
REQ-847-W12	Wallet Provider shall ensure that data portability during suspension or withdrawal is technically supported only where it does not impair the security of critical assets of affected wallet units. [Article 4(4), Article 8(3)]

5 Provisions

- 23 This section establishes the provisions which Wallet Provider shall comply with for the purposes of certification of the EUDI Wallet under Article 5c of eIDAS and CIR (EU) 2024/2981. Provisions are labelled WP-xx (Wallet Provider).
- 24 Wallet Provider shall comply with all EP-series provisions of WZ-03-01 in addition to the WZR-series provisions set out below. Where a WZR-series provision addresses the same subject matter as an EP-series provision, the more specific WZR-series provision shall apply.

5.1 General and Scheme-Specific Provisions

5.1.1 Certification Obligation

25 **WZR-01**

Wallet Provider shall ensure that the EUDI Wallet solution is certified by a conformity assessment body accredited under G-05 and designated by the Republic of Poland, prior to making the wallet available to users, and shall maintain a valid certificate of conformity for the duration of the wallet's availability. The certificate shall cover the wallet unit, the wallet secure cryptographic application (WSCA) and the wallet secure cryptographic device (WSCD) components as applicable to the wallet architecture.

[REQ-5c-04; REQ-2981-W03]

Alignment with international standards — ISO/IEC 17067 (conformity assessment); ETSI EN 319 401 §7.1 (general obligations).

5.1.2 Scope of Certification

26 **WZR-02**

Wallet Provider shall define and document the scope of certification, covering all software components installed on user devices and all back-end systems that form part of the wallet unit as defined in CIR (EU) 2024/2981. Wallet Provider shall establish a documented governance framework defining management responsibility, decision-making authority, accountability and approval of wallet policies and practices. Wallet Provider shall maintain a Wallet Provider Practice Statement, or an equivalent documented set of policies and procedures, describing the controls used to provide, operate, maintain Wallet Solutions and Wallet Units. The scope shall be agreed with the CAB and shall be consistent with CIR (EU) 2024/2981.

[REQ-5c-01; REQ-2981-W02, REQ-2981-W03, REQ-2981-W04]

Alignment with international standards — ISO/IEC 17067 §6.4 (scheme scope); CIR (EU) 2024/2981 Article 3, ETSI EN 319 401, Clause 6.1.

5.1.3 Open-Source Disclosure

27 WZR-03

In accordance with Article 5a (3) of eIDAS, the source code of the application software components of the EUDI Wallet installed on user devices shall be published under an open-source licence. Where duly justified reasons exist for not disclosing the source code of specific components other than those installed on user devices, Wallet Provider shall document those reasons and notify the Ministry of Digital Affairs.

[REQ-5c-01 (Article 5a (3) eIDAS)]

Alignment with international standards — Article 5a (3) eIDAS.

5.1.4 Public Information

28 WZR-04

Wallet Provider shall make publicly available the following information: the certificate of conformity (or a reference thereto), the certification body identifier, the scope of certification, the validity period of the certificate, and the cybersecurity certification scheme applied. This information shall be electronically signed or sealed in the form suitable for automated processing. This information shall be updated without undue delay upon any change affecting it.

[REQ-2981-W07]

Alignment with international standards — CIR (EU) 2024/2981 Article 8(5) and Annex V; ISO/IEC 17067 §6.4.

5.2 Certification and Conformity Assessment

5.2.1 Cybersecurity Certification

29 WZR-05

Wallet Provider shall certify those components of the EUDI Wallet that are relevant for cybersecurity in accordance with European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 and referenced in the implementing acts under Article 5c (6) of eIDAS. Wallet

Provider shall identify the applicable scheme(s) and confirm with the CAB the coverage against the cybersecurity requirements of Article 5c (2) of eIDAS.

[REQ-5c-02; REQ-2981-W06]

Alignment with international standards — Regulation (EU) 2019/881 (EU Cybersecurity Act), Articles 49–56.

5.2.2 National Certification Scheme Compliance

30 WZR-06

For requirements not covered by European cybersecurity certification schemes, Wallet Provider shall comply with the national certification scheme established pursuant to Article 5c (3) of eIDAS and the implementing acts under Article 5c (6), as incorporated in this document and in the GP-03 framework. The CAB shall evaluate compliance with this national scheme as part of the conformity assessment.

[REQ-5c-03; REQ-2981-W01]

Alignment with international standards — CIR (EU) 2024/2981 Article 6; GP-03 §6 (evaluation methodology).

5.2.3 Risk Register

31 WZR-07

Wallet Provider shall establish and maintain a risk register for the EUDI Wallet architecture, covering the cybersecurity risks and threats identified in Annex I to CIR (EU) 2024/2981. The risk register shall be updated following any material change to the wallet architecture, a significant incident, or new threat intelligence, and shall be made available to the CAB.

[REQ-2981-W01, REQ-847-W02]

Alignment with international standards — CIR (EU) 2024/2981 Article 8(1) and Annex I; G-04 Risk Register.

5.2.4 Recertification and Continuous Compliance

32 WZR-08

Wallet Provider shall initiate recertification whenever material changes to the wallet software, cryptographic components, or operational architecture may affect conformity. The threshold for triggering recertification shall be defined in the certification plan agreed with the CAB and consistent with

Article 4 of CIR (EU) 2024/2981. Wallet Provider shall maintain continuous compliance between certification cycles.

[REQ-5c-04; REQ-2981-W03]

Alignment with international standards — CIR (EU) 2024/2981 Article 4; ISO/IEC 17067 §6.7 (surveillance).

5.3 Cryptographic and WSCD Requirements

5.3.1 Wallet Secure Cryptographic Device (WSCD)

33 WZR-09

Wallet Provider shall ensure that the EUDI Wallet uses a Wallet Secure Cryptographic Device (WSCD) and a Wallet Secure Cryptographic Application (WSCA) meeting the requirements specified in CIR (EU) 2024/2981 and the applicable cybersecurity certification scheme. The WSCD shall provide an environment for cryptographic operations in which private keys cannot be extracted and are bound to the wallet unit.

[REQ-5c-02; REQ-2981-W02]

Alignment with international standards — CIR (EU) 2024/2981 Annex I (cryptographic requirements); ARF (current version).

5.3.2 Wallet Unit Attestation (WUA)

34 WZR-10

Wallet Provider shall implement the issuance and management of Wallet Unit Attestations (WUA) in accordance with CIR (EU) 2024/2981 and CIR (EU) 2024/2979. Each wallet unit issued by Wallet Provider shall hold a valid WUA signed by Wallet Provider using a key pair protected in accordance with the cryptographic requirements applicable at assurance level High.

[REQ-5c-01; REQ-2981-W02]

Alignment with international standards — CIR (EU) 2024/2981; CIR (EU) 2024/2979 (wallet protocols and interfaces).

5.3.3 Key Management for Wallet Operations

35 WZR-11

Wallet Provider shall implement key management procedures for all cryptographic key material used in wallet operations, including WUA signing keys, cryptographic binding of PID and attestations, and keys used

for wallet-to-relying-party authentication. Key management shall comply with the requirements of WZ-03-01 (EP-55 and EP-56) and the applicable cybersecurity certification scheme.

[REQ-5c-02; REQ-2690-W07]

Alignment with international standards — ISO/IEC 27001:2022 A.8.24 (use of cryptography); ETSI EN 319 401 §7.6 (cryptographic modules).

5.4 Data Protection and Privacy Requirements

5.4.1 Logical Separation

36 WZR-12

In accordance with Article 5a (14) of eIDAS, Wallet Provider shall ensure that personal data relating to the provision of the EUDI Wallet is kept logically separate from any other data held by Wallet Provider. The implementation of this logical separation shall be documented and verifiable by the CAB.

[REQ-5c-01 (Article 5a (14) eIDAS)]

Alignment with international standards — Article 5a (14) eIDAS; ISO/IEC 27001:2022 A.8.3 (information access restriction); GDPR Article 25 (data protection by design).

5.4.2 Non-collection and non-combination

37 WZR-13

Wallet Provider shall not collect information about the use of the EUDI Wallet which is not necessary for the provision of wallet services, and shall not combine person identification data or any other personal data stored or relating to the use of the EUDI Wallet with personal data from other services offered by Wallet Provider or from third-party services, unless the user has expressly requested otherwise.

[REQ-5c-01 (Article 5a (14) eIDAS)]

Alignment with international standards — GDPR Articles 5(1)(b), (c) (purpose limitation, data minimisation); Article 5a (14) eiders.

5.4.3 Unobservability and Unlikability

38 WZR-14

In accordance with Article 5a(16) of eIDAS, Wallet Provider shall implement a technical framework that does not allow any party, after the issuance of an attestation of attributes, to obtain data that allows

transactions or user behaviour to be tracked, linked or correlated, unless explicitly authorised by the user. Wallet Provider shall implement privacy-preserving techniques enabling unlikability where the attestation of attributes does not require identification of the user.

[REQ-5c-01 (Article 5a (16) eIDAS)]

Alignment with international standards — Article 5a (16) eIDAS; ARF (current version) §6 (privacy requirements).

5.5 Operational Requirements

5.5.1 Assurance Level High

39 **WZR-16**

The EUDI Wallet shall be provided under an electronic identification scheme with assurance level High, meeting all requirements of Article 8 of eIDAS as applied to identity proofing and verification and electronic identification means management and authentication. [Articles 5a(5)(d) and 5a (11) eIDAS]

[REQ-5c-01; REQ-1502-W01]

Alignment with international standards — CIR (EU) 2015/1502 Annex Section 2; Article 8 eIDAS.

5.5.2 No-Cost-Base and Voluntary Use

40 **WZR-17**

The issuance, use and revocation of the EUDI Wallet shall be free of charge to all natural persons. [Article 5 a(13) of eIDAS] The use of the wallet shall be voluntary; access to public and private services, access to the labour market and freedom to conduct business shall not in any way be restricted or made disadvantageous to persons that do not use the EUDI Wallet. [Article 5a (15) eIDAS]

[REQ-5c-01 (Articles 5a (13) and 5a (15) eIDAS)]

Alignment with international standards — Articles 5a (13) and 5a (15) eIDAS.

5.5.3 Accessibility

41 **WZR-18**

The EUDI Wallet shall be made accessible for use by persons with disabilities, on an equal basis with other users, in accordance with Directive (EU) 2019/882 on the accessibility requirements for products and services

(European Accessibility Act). [Article 5a (21) eIDAS] Wallet Provider shall document compliance with this requirement and present evidence to the CAB during the conformity assessment.

[REQ-5c-01 (Article 5a (21) eIDAS)]

Alignment with international standards — Directive (EU) 2019/882 (European Accessibility Act); Article 5a (21) eIDAS.

5.5.4 Qualified Electronic Signatures

42 WZR-19

Wallet Provider shall ensure that natural persons have, at least for non-professional purposes, free of charge access to signature creation applications enabling the creation of qualified electronic signatures through the EUDI Wallet. The implementation shall use qualified electronic signature creation devices (QSCDs) compliant with Annex II to eIDAS and shall support the interfaces required by CIR (EU) 2024/2979. Wallet Provider shall ensure that wallet users can receive qualified certificates for qualified electronic signatures or seals and that the Wallet Solution securely interfaces with supported signature or seal creation environments, including local QSCD, external WSCD or remote QSCD qualified provider models, as applicable. Where signature creation applications are provided or integrated with Wallet Instances, they shall support the required signing and sealing functions, mandatory formats and, where applicable, the CSC API.

[REQ-5c-01 (Article 5a(5)(g) eIDAS); REQ-2979-W03; REQ-2979-W04]

Alignment with international standards — Article 5a(5)(g) eIDAS; Annex II eIDAS (QSCD requirements); CIR (EU) 2024/2979; ETSI EN 319 411- 2; ETSI TS 119 431-2.

5.5.5 Technical Support and Reporting

43 WZR-20

Wallet Provider shall ensure that users can easily request technical support and report technical problems or any other incidents having a negative impact on the use of the EUDI Wallet, as required by Article 5a (10) of eIDAS. The technical support channel shall be available continuously and shall have a documented response time consistent with the service level agreed under GP-03.

[REQ-5c-01 (Article 5a (10) eIDAS)]

Alignment with international standards — Article 5a (10) eIDAS; ETSI EN 319 401 §7.2 (subscriber agreements).

5.5.6 Revocation

44 WZR-21

Wallet Provider shall ensure that the validity of the EUDI Wallet can be revoked upon the explicit request of the user, where the security of the wallet has been compromised, or upon the death of the user or the cessation of activity of the legal person, as required by Article 5a(9) of eIDAS. Revocation shall take effect without undue delay, and the user shall be informed without delay. The Wallet Provider shall be the only entity capable of revoking Wallet Unit Attestations for Wallet Units it has provided and shall establish a publicly available revocation policy defining conditions and timeframes. Wallet Provider shall ensure that suspension or withdrawal of a Wallet Solution is reflected in the lifecycle of affected Wallet Units and Wallet Unit Attestations, including prevention of further use, provision or activation where required, revocation of affected attestations, and controlled support for data portability where it does not impair the security of critical assets.

[REQ-5c-01 (Article 5a (9) eIDAS); REQ-2981-W04; REQ-847-W16; REQ-847-W17; REQ-847-W18; REQ-847-W19; REQ-847-W20; REQ-847-W21]

Alignment with international standards — Article 5a (9) eIDAS; Article 5e eIDAS (security breach); CIR (EU) 2024/2979, Article 7.

5.5.7 Record Keeping

45 WZR-22

Wallet Provider shall maintain records sufficient to demonstrate conformity with the requirements of this document and CIR (EU) 2024/2981 for the retention period specified in Article 19 of CIR (EU) 2024/2981. Records shall include conformity assessment documentation, incident logs, security test results, and change management records, and shall be made available to the CAB and supervisory authorities upon request. Records shall include incident records, logs and other data sources sufficient to support incident detection, timing, assessment and reporting, including determination of the beginning and duration of availability incidents.

[REQ-2981-W08; REQ-1502-W01; REQ-847-W12; REQ-847-W13; REQ-847-W14]

Alignment with international standards — CIR (EU) 2024/2981 Article 19; CIR (EU) 2025/847; ISO/IEC 27001:2022 A.5.33 (protection of records); ETSI EN 319 401 §7.9.1.

5.5.8 Independent user services

46 WZR-22A

The Wallet Provider shall inform wallet users of their rights and obligations and provide mechanisms independent of Wallet Units for secure user identification and authentication, including for revocation requests.

Alignment with international standards - CIR (EU) 2024/2979, Article 6(3).

5.5.9 Availability monitoring

47 WZR-22B

Wallet Provider shall maintain availability monitoring capable of detecting complete or projected complete unavailability or limited availability of the wallet solution, validation mechanisms or electronic identification scheme or wallet-related services. Wallet Provider shall define objective criteria for assessing limited availability, including, where possible, average response times, delayed response times, unavailable functionalities, transaction failure rates and service degradation indicators. Wallet Provider shall maintain availability monitoring capable of detecting complete, projected complete and limited unavailability of the Wallet Solution, validation mechanisms and electronic identification scheme, using the thresholds and objective criteria defined in CIR (EU) 2025/847. The monitoring shall support determination of when full unavailability begins and ends.

[REQ-847-W03, REQ-847-W04, REQ-847-W05; REQ-847-W06; REQ-847-W15]

Alignment with international standards - CIR (EU) 2025/847; ISO/IEC 27001:2022 A.8.16 (monitoring activities); ISO/IEC 27001:2022 A.5.30 (ICT readiness for business continuity); ETSI EN 319 401 §7.9.1 and §7.11.

5.6 Incident handling and Breach Notification

5.6.1 Security monitoring and unauthorised access detection

48 WZR-23

Wallet Provider shall monitor and detect suspected malicious or unauthorised access to network and information systems supporting the wallet solution, validation mechanisms and the electronic identification scheme. Monitoring shall cover, at least, privileged access, administrative actions, authentication failures, abnormal network activity and unauthorised changes to security-relevant components. Wallet Provider shall monitor and detect suspected, successful or potential unauthorised logical or restricted physical access to network and information systems supporting the Wallet Solution, validation mechanisms or electronic identification scheme, including systems identified as critical components.

[REQ-847-W01; REQ-847-W02; REQ-847-W07; REQ-847-W08]

Alignment with international standards - CIR (EU) 2025/847; ETSI EN 319 401 §7.6 and §7.9.1.

5.6.2 Notification to Users

49 WZR-23A

Wallet Provider shall inform users without delay of any security breach that could have entirely or partially compromised their EUDI Wallet or its contents, if the wallet has been suspended or revoked pursuant to Article 5e of eIDAS. Notification shall describe the nature of the breach, the data potentially affected, and the remedial measures taken or recommended.

[REQ-5c-01 (Article 5a (6) eIDAS)]

Alignment with international standards — Article 5a (6) eIDAS; GDPR Article 34 (communication of personal data breach to data subject).

5.6.3 Notification to CAB and Supervisory Bodies

50 WZR-24

Wallet Provider shall notify the CAB without undue delay of any breach or compromise of the EUDI Wallet likely to impact the conformity of the wallet with the requirements of Article 5c of eIDAS, as required by Article 5(2) of CIR (EU) 2024/2981. Wallet Provider shall also notify the competent national cybersecurity authority in accordance with the Polish Cybersecurity Act and Article 23 of the NIS 2 Directive. For the purpose of determining whether a breach or compromise is notifiable and may affect the conformity or reliability of the Wallet Solution, Wallet Provider shall take into account any actual or potential compromise of the privacy, integrity, confidentiality or authenticity of data stored, transmitted or processed in the Wallet Solution, the certification status of the Wallet Solution, and direct financial losses, in accordance with CIR (EU) 2025/847.

[REQ-2981-W04; REQ-2690-W03 REQ-847-W09; REQ-847-W10; REQ-847-W11]

Alignment with international standards — CIR (EU) 2024/2981 Article 5(2); CIR (EU) 2025/847; NIS 2 Directive Article 23; Polish Cybersecurity Act.

5.6.4 Vulnerability Management

51 WZR-25

Wallet Provider shall establish and maintain a vulnerability management policy for the EUDI Wallet meeting the requirements set out in Annex I to Regulation (EU) 2024/2847 (Cyber Resilience Act), as referenced in Article 5(7) of CIR (EU) 2024/2981. The policy shall include procedures for the identification, assessment, coordinated disclosure and remediation of vulnerabilities in wallet software components.

[REQ-2981-W05; REQ-2690-W07]

Alignment with international standards — CIR (EU) 2024/2981 Article 5(7); Regulation (EU) 2024/2847 (Cyber Resilience Act) Annex I; ISO/IEC 29147.

5.7 Relying Party and Interoperability Requirements

5.7.1 Relying Party Authentication

52 WZR-26

Wallet Provider shall implement authentication mechanisms enabling the EUDI Wallet to authenticate and identify relying parties registered in accordance with Article 5b of eIDAS, in accordance with the protocols and interfaces specified in CIR (EU) 2024/2979. Wallet Provider shall ensure that the wallet does not disclose person identification data to relying parties not registered in accordance with Article 5b of eIDAS. Wallet Provider shall ensure that the Wallet Unit processes applicable embedded disclosure policies in relation to wallet-relying party requests, verifies whether the wallet-relying party complies with those policies, and presents the result of that verification to the wallet user.

[REQ-5c-01 (Article 5a(5)(c) eIDAS); REQ-2979-W02 (CIR (EU) 2024/2979, Article 10)]

Alignment with international standards — Article 5a(5)(c) eIDAS; Article 5a(5)(e) eIDAS; Article 5b eIDAS; CIR (EU) 2024/2979.

5.7.2 Common Protocols and Interfaces

53 WZR-27

Wallet Provider shall ensure that the EUDI Wallet supports all common protocols and interfaces specified in Article 5a(5)(a) of eIDAS and in CIR (EU) 2024/2979, including interfaces for issuance of PID and attestations, for relying parties to request and validate PID and attestations, for sharing and presentation of data online and in offline mode, and for wallet-to-wallet interaction as required by Article 5a(5)(a)(vi) of eIDAS.

[REQ-5c-01 (Article 5a(5)(a) eIDAS)]

Alignment with international standards — Article 5a(5)(a) eIDAS; CIR (EU) 2024/2979; ARF (current version).

5.7.3 Non-tracking of Attestation Use

54 WZR-28

In accordance with Article 5a(5)(b) of eIDAS, Wallet Provider shall ensure that the EUDI Wallet does not provide any information to trust service providers of electronic attestations of attributes about the use of those attestations. The technical implementation of this requirement shall be verified by the CAB as part of the conformity assessment.

[REQ-5c-01 (Article 5a(5)(b) eIDAS)]

Alignment with international standards — Article 5a(5)(b) eIDAS; ARF (current version) §6 (privacy requirements).

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

55 The following table provides an informative mapping between the provisions of Section 5 and the underlying legal requirements set out in Section 4.

Provision	Legal Requirements Satisfied
WZR-01	REQ-5c-04; REQ-2981-W03
WZR-02	REQ-5c-01; REQ-2981-W02; REQ-2981-W03; REQ-2981-W04
WZR-03	REQ-5c-01 (Article 5a (3) eIDAS)
WZR-04	REQ-2981-W07
WZR-05	REQ-5c-02; REQ-2981-W06
WZR-06	REQ-5c-03; REQ-2981-W01
WZR-07	REQ-2981-W01; REQ-847-W02
WZR-08	REQ-5c-04; REQ-2981-W03
WZR-09	REQ-5c-02; REQ-2981-W02
WZR-10	REQ-5c-01; REQ-2981-W02
WZR-11	REQ-5c-02; REQ-2690-W07
WZR-12	REQ-5c-01 (Article 5a (14) eIDAS)
WZR-13	REQ-5c-01 (Article 5a (14) eIDAS)
WZR-14	REQ-5c-01 (Article 5a (16) eIDAS)
WZR-15	REQ-5c-01 (Article 5a(4)(d) eIDAS); REQ-2979-W02
WZR-16	REQ-5c-01; REQ-1502-W01
WZR-17	REQ-5c-01 (Articles 5a (13), (15) eIDAS)
WZR-18	REQ-5c-01 (Article 5a (21) eIDAS)
WZR-19	REQ-5c-01 (Article 5a(5)(g) eIDAS); REQ-2979-W03; REQ-2979-W04
WZR-20	REQ-5c-01 (Article 5a (10) eIDAS)
WZR-21	REQ-5c-01 (Article 5a (9) eIDAS); REQ-2981-W04; REQ-847-W16; REQ-847-W17; REQ-847-W18; REQ-847-W19; REQ-847-W20; REQ-847-W21
WZR-22	REQ-2981-W08; REQ-1502-W01; REQ-847-W12; REQ-847-W13; REQ-847-W14
WZR-22A	REQ-2979-W02
WZR-22B	REQ-847-W03; REQ-847-W04; REQ-847-W05; REQ-847-W06; REQ-847-W15
WZR-23	REQ-5c-01 (Article 5a (6) eIDAS); REQ-847-W01; REQ-847-W02; REQ-847-W07; REQ-847-W08

Provision	Legal Requirements Satisfied
WZR-23A	REQ-5c-01 (Article 5a (6) eIDAS)
WZR-24	REQ-2981-W04; REQ-2690-W03; REQ-847-W09; REQ-847-W10; REQ-847-W11
WZR-25	REQ-2981-W05; REQ-2690-W07
WZR-26	REQ-5c-01 (Article 5a(5)(c) eIDAS)
WZR-27	REQ-5c-01 (Article 5a(5)(a) eIDAS)
WZR-28	REQ-5c-01 (Article 5a(5)(b) eIDAS)