

WP-03-03

PL EUDI Wallet Certification System

Requirements for eID Means (Including
Authentication)

VERSION 1.01

2026.05.18

Document reference	WP-03-03
Version	V1.01 (2026-05)
Status	FINAL
Date	18.05.2026
Document type	Certification Scheme — Process Requirements (ISO/IEC 17067)
Parent framework	GP-03 eID Certification Scheme WZ-03 series
Scheme Owner	Republic of Poland / Minister of Digital Affairs
Certification target	EUDI Wallet as electronic identification means; authentication
Primary audience	EUDI Wallet Provider; PID Provider
Secondary audience	Conformity Assessment Bodies (CABs) accredited according to G-05
Assurance level	High (Article 8 eIDAS; CIR (EU) 2015/1502)
Subsidiary Documents	WM-03-1, WM-03-02, WM-03-03

Table of content

1	Scope	4
2	Legal Basis	5
2.1	Legal acts	5
2.2	Normative references	5
3	Terms and Definitions	7
4	General Principles	8
4.1	Proportionality to risk	8
4.2	Auditability	8
4.3	National law	8
4.4	Normative language	8
4.5	Relationship with WZ-03-01, WZ-03-03 and WP-03-02	9
5	Legal Requirements	10
5.1	Requirements derived from Regulation (EU) No 910/2014 as amended	10
5.2	Requirements derived from CIR (EU) 2015/1502 — eID means and authentication	10
5.3	Requirements derived from CIR (EU) 2024/2979 — authentication protocols	11
6	Provisions	12
6.1	eID means characteristics and design	12
6.2	User authentication mechanism	14
6.3	Authentication transactions with relying parties	16
6.4	Interoperability protocols	17
	Annex A (Informative) Mapping of Provisions to Legal Requirements	19

1 Scope

- 1 The document specifies requirements applicable to the EUDI Wallet as an electronic identification means (eID means) at assurance level high, including the requirements for user authentication mechanisms, authentication transactions with relying parties and interoperability of authentication protocols, for the purposes of certification under the eID Certification Scheme (GP-03).
- 2 This document applies to wallet providers insofar as those requirements concern the eID means characteristics and the authentication processes implemented within the wallet.
- 3 This document covers the following subject areas:
 - characteristics and design of the eID means (wallet unit);
 - user authentication mechanisms;
 - authentication transactions with relying parties;
 - interoperability of authentication protocols;
 - lifecycle requirements for the eID means as they relate to its use for authentication.
- 4 The organisational and management system requirements applicable to wallet providers are specified in WZ-03-01 and WZ-03-03. The process requirements for wallet unit provisioning and lifecycle management are specified in WP-03-02. The present document addresses the requirements specific to the eID means characteristics and authentication processes.
- 5 The following are outside the scope of this document:
 - Organisational and management system requirements for wallet providers — see WZ-03-01 and WZ-03-03.
 - — Process requirements for wallet unit provisioning and lifecycle — see WP-03-02.
 - — Process requirements for PID registration and lifecycle — see WP-03-01.
 - — Cybersecurity product certification of wallet components (WSCD/WSCA) — see GP-02.
 - — Functional conformity assessment of the wallet solution — see GP-01.

2 Legal Basis

2.1 Legal acts

- 6 This document is based on the following legal instruments:
- a. Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, in particular Articles 5a and 8 thereof;
 - b. Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015, in particular Sections 2.2 and 2.3 of the Annex thereto, which specify the minimum requirements applicable to the electronic identification means and the authentication mechanism at assurance level high;
 - c. Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024, in particular Articles 4 and 5 thereof;
 - d. Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024, in particular Annex I thereto;
 - e. Commission Implementing Regulation (EU) 2025/849 of 28 February 2025;
 - f. Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. 2024 r. poz. 1275 z późn. zm.);
 - g. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 z późn. zm.).

2.2 Normative references

- 7 This document is based on the following normative references:
- a. Architecture and Reference Framework (ARF) v2.8.0 (April 2026), in particular the protocol specifications for OID4VP and ISO/IEC 18013-5 proximity presentation;
 - b. ISO/IEC 29115:2013 — Information technology — Security techniques — Entity authentication assurance framework;
 - c. ISO/IEC 18013-5:2021 — Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application;
 - d. ISO/IEC 30107-3:2023 — Information technology — Biometric presentation attack detection — Part 3: Testing and reporting;
 - e. ISO/IEC 15408-1:2022 — Common Criteria for Information Technology Security Evaluation — Part 1: Introduction and general model;
 - f. ISO/IEC 18045:2022 — Common Evaluation Methodology for Information Technology Security Evaluation (CEM:2022), Revision 1;
 - g. ETSI TS 102 165-1 — Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Vulnerability, Risk Analysis (TVRA);

- h. ETSI TS 119 461 v2.1.1 — Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;
- i. CEN/TS 18098:2026 - Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets

3 Terms and Definitions

- 8 For the purposes of this document, the terms and definitions given in ISO/IEC 29115:2013 and G-02 (Vocabulary) apply.

4 General Principles

4.1 Proportionality to risk

- 9 In accordance with Section 2.2 of the Annex to CIR (EU) 2015/1502 and ISO/IEC 29115:2013, all provisions in this document shall be understood as requirements at assurance level high. The authentication mechanisms and processes implemented by the wallet provider shall be designed to resist attacks of high potential, as defined in ISO/IEC 15408-1 and ISO/IEC 18045 but limited to the identity proofing, see G-02, where definitions of assurance, in the context of Regulation (EU) 2014/910 (eIDAS) and Regulation (EU) 2019/881 (the “Cybersecurity Act”, CSA) can be found.
- 10 Wallet Provider shall carry out and document a risk assessment of the authentication mechanism. The risk assessment shall cover threats directed at the authentication mechanism and authentication factors based on possession, knowledge and inherence, as well as security measures in place to protect against these threats. The risk assessment shall consider at least an attacker with high attack potential. The attack potential may be calculated in accordance with ISO/IEC 18045, Annex B, Common Criteria CCDB 2009 03, Part 3, or ETSI TS 102 165-1, clauses 6.6 and 6.7.
- 11 The threats to be considered in the risk assessment shall include at minimum: online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay attacks, session hijacking, man-in-the-middle attacks, credential theft, spoofing and masquerading, as specified in ISO/IEC 29115:2013, Annex C. Additionally, relevant threats to identity proofing form CIR (EU) 2024/2981, Annex I shall be considered.

4.2 Auditability

- 12 Wallet Provider shall ensure that their implementation of the provisions in this document is documented, traceable and verifiable by a conformity assessment body accredited pursuant to G-05. The assessment of the authentication mechanism shall include technical testing; an assessment based solely on written documentation is not sufficient.

4.3 National law

- 13 Where national law imposes requirements more stringent than those in this document, the wallet provider shall comply with the applicable national law.

4.4 Normative language

- 14 The normative terms "shall", "should" and "may" are used in this document in accordance with the definitions in Section 3.

4.5 Relationship with WZ-03-01, WZ-03-03 and WP-03-02

- 15 The requirements of this document supplement the organisational requirements of WZ-03-01 and WZ-03-03 and the provisioning requirements of WP-03-02. All authentication processes presuppose a valid, activated wallet unit as defined in WP-03-02. Compliance with this document does not replace the requirements of WZ-03-01, WZ-03-03 or WP-03-02. Requirements related to identity proofing, remote onboarding, PID issuance and PID lifecycle are specified in WP-03-01. This document covers those aspects only where they directly affect the characteristics or use of the eID means for authentication.

5 Legal Requirements

16 *NOTE: This section lists, at a granular level, all legal requirements applicable to wallet providers in scope of this document.*

5.1 Requirements derived from Regulation (EU) No 910/2014 as amended

Identifier	Requirement
REQ-910-01	European Digital Identity Wallets shall meet the requirements set out in Article 8 with regard to assurance level high, as applied to the characteristics of the electronic identification means and the authentication mechanism. [Article 5a(5)(d)]
REQ-910-02	European Digital Identity Wallets shall support common protocols and interfaces enabling relying parties to request and validate person identification data and electronic attestations of attributes. [Article 5a(5)(a)(ii)]
REQ-910-03	European Digital Identity Wallets shall authenticate and identify relying parties registered in accordance with Article 5b of eIDAS, prior to disclosing person identification data or electronic attestations of attributes. [Article 5a(5)(c)]
REQ-910-04	European Digital Identity Wallets shall not provide any information to providers of electronic attestations of attributes about the use of those attestations. [Article 5a(5)(b)]
REQ-910-05	European Digital Identity Wallets shall support common protocols for sharing and presentation of person identification data and electronic attestations of attributes, both online and in offline mode, and for wallet-to-wallet interaction. [Article 5a(5)(a)(iv), (v), (vi)]

5.2 Requirements derived from CIR (EU) 2015/1502 — eID means and authentication

17 *NOTE: The following requirements are derived from Sections 2.2 and 2.3 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.*

Identifier	Requirement
REQ-1502-01	The electronic identification means shall use at least two authentication factors from different categories (knowledge, possession, inherence). [Annex, Section 2.2.1, Level High, Element 1]

Identifier	Requirement
REQ-1502-02	The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others. [Annex, Section 2.2.1, Level High, Element 2]
REQ-1502-03	The electronic identification means is designed in such a way that it can be assumed it is used only under the control of the person to whom it belongs. [Annex, Section 2.2.1, Level Substantial, Element 1]
REQ-1502-04	Dynamic authentication is used. [Annex, Section 2.3.1, Level High, Element 1]
REQ-1502-05	Authentication is designed to prevent disclosure of authentication data relevant to the electronic identification and to prevent authentication from being replayed or forged in any way. [Annex, Section 2.3.1, Level High, Element 2]
REQ-1502-06	The authentication mechanism, including authentication data, provides resistance against high attack potential. [Annex, Section 2.3.1, Level High, Element 3]
REQ-1502-07	The electronic identification means shall be designed and implemented to prevent duplication, tampering and unauthorised modification of the means or its authentication factors, taking into account resistance against high attack potential. [Annex, Section 2.2.1 and Section 2.3.1, Level High]
REQ-1502-08	The authentication mechanism shall enable reliable verification of the electronic identification means and its validity before person identification data are released in an authentication transaction. [Annex, Section 2.3.1, Level High]
REQ-1502-09	Person identification data and authentication data used by the electronic identification means shall be protected against loss, compromise, disclosure, unauthorised use and offline analysis. [Annex, Section 2.2.1 and Section 2.3.1, Level High]

5.3 Requirements derived from CIR (EU) 2024/2979 — authentication protocols

Identifier	Requirement
REQ-2979-01	Wallet providers shall ensure integrity, authenticity and confidentiality of the communication between wallet instances and wallet secure cryptographic applications. [Article 4(2)]
REQ-2979-02	The wallet unit shall support the presentation of person identification data and electronic attestations of attributes to relying parties online,

Identifier	Requirement
	using the OID4VP protocol as specified in CIR (EU) 2024/2979 and ARF v2.8.0. [Article 5]
REQ-2979-03	The wallet unit shall support proximity presentation using the ISO/IEC 18013-5 device retrieval protocol over BLE and NFC transport channels. [Article 5]
REQ-2979-04	The wallet unit shall support wallet-to-wallet interaction protocols as required by Article 5a(5)(a)(vi) of eIDAS and CIR (EU) 2024/2979. [Article 5]

6 Provisions

18 *NOTE 1: This chapter sets out the provisions with which wallet providers shall comply as regards the eID means characteristics of the wallet unit and authentication processes. Provisions are structured in four subsections: eID means characteristics and design (6.1), user authentication mechanism (6.2), authentication transactions with relying parties (6.3), and interoperability protocols (6.4).*

19 *NOTE 2: References to legal requirements are indicated in brackets at the end of each provision. Mapping of provisions to the legal requirements is presented in Annex A.*

6.1 eID means characteristics and design

20 *NOTE 1: The following provisions specify the characteristics that the EUDI Wallet shall exhibit as an electronic identification means at assurance level high.*

21 **EID-01**

22 The authentication factors, authentication mechanism and security measures of the EUDI Wallet shall be planned, executed and maintained so that they protect the integrity and confidentiality of the eID means. The eID means shall be able to resist at least high-level threats and attack potential in accordance with assurance level high. The resistance shall be based on a risk assessment including specific assessments of threats directed at authentication mechanisms and authentication factors based on possession, knowledge and inherence, as well as assessment of security measures in place to protect against these threats. The design shall also protect the eID means and its authentication factors against duplication, tampering and unauthorised modification.

[REQ-1502-01; REQ-1502-06; REQ-1502-07; REQ-2981-01; REQ-2981-02]

23 **EID-02**

24 The features and security measures of the EUDI Wallet shall prevent the possibility that the compromise of one authentication factor would compromise the reliability of other authentication factors. The security measures protecting the eID means

shall separate and protect the authentication factors, in particular when they are used on the same terminal device. In particular, the Wallet Provider shall ensure that PID key authentication factors, wallet unit authentication factors, and user device authentication factors are managed independently of each other.

25 *NOTE 2: Mutual independence of authentication factors requires special attention in identification means used on mobile devices.*

[REQ-1502-01; REQ-1502-02; REQ-1502-03; REQ-2981-02]

26 **EID-03**

27 The Wallet Provider shall ensure that secret data related to an eID means is not revealed to its staff under any circumstances. The wallet provider shall not make copies of any secret data related to an eID means. Person identification data and authentication data used by the eID means shall be protected against loss, compromise, disclosure, unauthorised use and offline analysis.

28 *NOTE 3: Secret information typically includes PIN codes, private keys, biometric templates and other knowledge-based or inherence-based authentication factors. This requirement is intended to address the risk of dishonest personnel.*

[REQ-1502-02; REQ-1502-09; REQ-2981-02]

29 **EID-04**

30 The EUDI Wallet shall use at least two authentication factors from different factor categories (possession, knowledge, inherence) for each authentication operation. The possession factor shall be the wallet unit cryptographically bound to the WSCD. The second factor shall be a knowledge factor (passcode) or an inherence factor (biometric), or both.

31 *NOTE 4: Any combination of possession-based, knowledge-based and inherent authentication factors is possible, provided each factor is resistant against high attack potential. PID key authentication factors and wallet unit authentication factors may differ in nature while being managed independently.*

[REQ-1502-01; REQ-2981-01]

32 **EID-04a**

33 The authentication factors of the EUDI Wallet shall be bound to the wallet unit holder in the eID scheme. The EUDI Wallet shall not be bound to a wallet user before the wallet user has passed initial identity proofing as specified in WP-03-01,

or it has otherwise been ensured that the eID means is not functional before the initial identity proofing has been performed.

34 *NOTE 5: Examples of binding the authentication factors to a person include binding of the wallet application to a person, WSCD personalisation, or the linking of a passcode or biometric template to a person.*

[REQ-1502-03; REQ-2981-01]

35 **EID-05**

36 The authentication mechanism shall use dynamic authentication. The proof of authentication shall: (a) be produced using cryptographic techniques; (b) be unique to each authentication transaction; (c) include a nonce or timestamp provided by the verifying party; (d) be bound to the context of the transaction, including the identity of the relying party; and (e) not be replayable or forgeable outside its intended context. Before person identification data are released in an authentication transaction, the authentication mechanism shall verify the electronic identification means and its validity.

[REQ-1502-04; REQ-1502-05; REQ-1502-08; REQ-2981-01; REQ-2981-02]

6.2 **User authentication mechanism**

37 *NOTE 1: The following provisions specify the requirements for the user authentication mechanism within the wallet unit.*

38 **EID-06**

39 The authentication mechanism shall be implemented so that it is highly unlikely that an attacker with high attack potential could subvert it through guessing, eavesdropping, replay attacks or manipulation of communication. The implementation shall be verified as part of the conformity assessment under GP-02 certification scheme.

[REQ-1502-04; REQ-1502-05; REQ-1502-06]

40 **EID-06a**

41 The EUDI Wallet shall employ internationally or nationally recommended cryptographic methods and protocols. The communications connection between the wallet unit and the wallet provider's systems shall employ encryption methods compliant with the applicable technical standards referenced in ARF v2.8.0 and CIR (EU) 2024/2979. Where Transport Layer Security (TLS) is used, TLS version 1.2 or higher shall be used, and only cipher suites providing forward secrecy shall

be permitted. Only cryptographic algorithms recognised as secure by national or European security authorities shall be used.

[REQ-2979-01; REQ-2981-02]

42 EID-07

43 The Wallet Provider shall ensure that the EUDI Wallet cannot be used for authentication without the successful completion of the user authentication step. The Wallet Provider shall ensure that no mechanism exists within the wallet solution that allows an authentication transaction to be completed without presentation of the required authentication factors by the wallet user, including by the Wallet Provider itself. Secret information related to the eID means shall not be accessible to the personnel or subcontractors of the wallet provider.

[REQ-1502-02; REQ-1502-03; REQ-2981-02]

44 EID-08

45 Where a knowledge-based authentication factor (PIN/passcode) is used, the Wallet Provider shall implement the following controls: (a) the PIN or password shall consist of at least 6 digits or 6 characters; (b) the wallet unit shall allow at maximum 3 consecutive false authentication attempts before imposing a lockout or equivalent delay mechanism; (c) the PIN entry shall be protected against eavesdropping and interception; (d) the wallet unit shall prevent PIN/password submission by tools such as password managers and shall ensure the passcode originates from the wallet user; (e) the PIN or password shall not be stored outside the WSCD or equivalent protected storage in an accessible form.

46 *NOTE 2: This requirement implements CIR (EU) 2015/1502, Annex, Section 2.2.1, Level High, and is aligned with the requirements of [18098], §9.5 and §9.6.*

[REQ-1502-01; REQ-1502-02; REQ-1502-06]

47 EID-08a

48 Where an inherent authentication factor (biometrics) is used, the wallet provider shall: (a) ensure the biometric system has been evaluated against ISO/IEC 30107-3 for presentation attack detection, covering high attack potential; (b) store and manage the reference biometric data within the WSCD or the trusted execution environment, and not transmit it to any external system; (c) ensure the wallet user is offered an alternative non-biometric authentication factor and their explicit and freely given consent to biometric processing is obtained; (d) ensure that different threat types that target the biometric factor are taken into account in the design of the authentication mechanism.

49 *NOTE 3: Standardisation activities to develop European requirements for biometric products, to reach the Level of Assurance required, are ongoing within CEN/TC 224/WG 18. ISO/IEC 30107-3 and ISO/IEC 19989-3 are the current starting points for evaluation of biometric systems.*

[REQ-1502-01; REQ-1502-02; REQ-1502-06]

50 EID-09

51 The Wallet Provider shall implement mechanisms to detect and respond to repeated failed authentication attempts, including temporary or permanent blocking of the wallet unit. Where the wallet unit is blocked following repeated failed attempts, the user shall be notified and a recovery procedure consistent with the assurance requirements of WP-03-02 shall be available.

[REQ-1502-06; REQ-2981-02]

52 EID-10

53 Where single sign-on (SSO) is provided by the EUDI Wallet, the wallet provider shall implement adequate security measures for the management of session length, session transfer and session termination related to single sign-on, to ensure that the security level of the authentication is maintained throughout the session and that session-related risks are mitigated.

[REQ-1502-04; REQ-1502-05]

6.3 Authentication transactions with relying parties

54 *NOTE 1: The following provisions specify the requirements for authentication transactions between the wallet unit and relying parties.*

55 EID-11

56 The EUDI Wallet shall present the user with information during each authentication event that enables the user to confirm that the authentication request received by the wallet corresponds to the user's own initiated transaction. This information shall be presented to the user before the user is asked to authorise the authentication, in wallet units that have the technical ability to do so.

57 *NOTE 2: This provision implements the requirement to enable the user to act under sole control of the wallet in a manner that is transparent and traceable, as required by Article 5a(4)(a) of eIDAS.*

[REQ-910-01; REQ-1502-05]

58 EID-12

59 The EUDI Wallet shall present the user with information concerning the relying party for whom the authentication is being carried out, during each authentication event. This information shall include at a minimum the verified identity of the relying party and shall be presented to the user before the user is asked to authorise the disclosure of any person identification data or attestation.

[REQ-910-03; REQ-1502-05]

60 EID-13

61 Before disclosing person identification data or any electronic attestation of attributes to a relying party, the EUDI Wallet shall verify that the relying party is registered in accordance with Article 5b of eIDAS, using the relying party's

registration certificate or another mechanism defined in CIR (EU) 2024/2979 and ARF v2.8.0. The wallet shall not disclose person identification data to relying parties that are not registered in accordance with Article 5b of eIDAS.

[REQ-910-03; REQ-1502-05]

62 EID-14

63 The EUDI Wallet shall implement selective disclosure, ensuring that only the attributes explicitly requested by the relying party and consented to by the user are disclosed. The wallet shall not disclose additional attributes beyond the scope of the verified and consented request.

[REQ-910-03; REQ-910-04; REQ-1502-05]

64 EID-15

65 The EUDI Wallet shall not provide any information to providers of electronic attestations of attributes about the use of those attestations by the wallet user in transactions with relying parties.

[REQ-910-04]

66 EID-16

67 The Wallet Provider shall ensure that the transaction log of the EUDI Wallet records, for each authentication transaction, at a minimum: (a) the timestamp; (b) the verified identifier of the relying party; (c) the attributes disclosed; and (d) the outcome of the transaction. The transaction log shall be accessible to the user and shall be retained for the period specified in WZ-03-01.

[REQ-910-01; REQ-2979-01]

6.4 Interoperability protocols

68 *NOTE 1: The following provisions specify the requirements for the protocols and interfaces used by the EUDI Wallet in authentication transactions.*

69 EID-17

70 The EUDI Wallet shall support online presentation of person identification data and electronic attestations of attributes to relying parties using the OpenID for Verifiable Presentations (OID4VP) protocol as specified in CIR (EU) 2024/2979 and ARF v2.8.0. The implementation shall support selective disclosure for both SD-JWT VC and ISO/IEC 18013-5 (mdoc) credential formats. The response to the relying party shall include a cryptographic proof of possession signed by the WSCD, binding the response to the nonce and the relying party identifier provided in the request.

[REQ-910-02; REQ-910-05; REQ-2979-02; REQ-1502-05]

71 EID-18

72 The EUDI Wallet shall support proximity presentation of person identification data and electronic attestations of attributes using the ISO/IEC 18013-5 device retrieval protocol over BLE and NFC transport channels, as specified in CIR (EU) 2024/2979 and ARF v2.8.0. The proximity session shall provide session encryption equivalent in security to the online protocol, protecting data in transit against eavesdropping and manipulation.

[REQ-910-05; REQ-2979-03; REQ-1502-05]

73 EID-19

74 The EUDI Wallet shall support wallet-to-wallet interaction for the purposes of presenting person identification data and electronic attestations of attributes between wallet units, in accordance with Article 5a(5)(a)(vi) of eIDAS and the protocols specified in CIR (EU) 2024/2979 and ARF v2.8.0.

[REQ-910-05; REQ-2979-04]

75 EID-20

76 The wallet provider shall ensure that all cryptographic algorithms and key lengths used in the authentication protocols comply with the cryptographic requirements applicable at assurance level high under the GP-03 scheme and as referenced in ARF v2.8.0 and the applicable cybersecurity certification scheme under GP-02. The wallet provider shall maintain a cryptographic agility policy enabling timely migration to new algorithms in the event that existing algorithms are weakened or deprecated.

[REQ-1502-06; REQ-2981-02]

77 EID-20a

78 The identification scheme and its components shall be tested comprehensively and regularly. Each material change to the authentication mechanism or authentication factors shall be tested before it is transferred to production. Negative test cases shall also be tested to prevent the generation of erroneous authentication events.

[REQ-1502-06; REQ-2981-02]

Annex A (Informative) Mapping of Provisions to Legal Requirements

Provision	Legal Requirements
EID-01	REQ-1502-01; REQ-1502-06; REQ-1502-07; REQ-2981-01; REQ-2981-02
EID-02	REQ-1502-01; REQ-1502-02; REQ-1502-03; REQ-2981-02
EID-03	REQ-1502-02; REQ-1502-09; REQ-2981-02
EID-04	REQ-1502-01; REQ-2981-01
EID-04a	REQ-1502-03; REQ-2981-01
EID-05	REQ-1502-04; REQ-1502-05; REQ-1502-08; REQ-2981-01; REQ-2981-02
EID-06	REQ-1502-04; REQ-1502-05; REQ-1502-06
EID-06a	REQ-2979-01; REQ-2981-02
EID-07	REQ-1502-02; REQ-1502-03; REQ-2981-02
EID-08	REQ-1502-01; REQ-1502-02; REQ-1502-06
EID-08a	REQ-1502-01; REQ-1502-02; REQ-1502-06
EID-09	REQ-1502-06; REQ-2981-02
EID-10	REQ-1502-04; REQ-1502-05
EID-11	REQ-910-01; REQ-1502-05
EID-12	REQ-910-03; REQ-1502-05
EID-13	REQ-910-03; REQ-1502-05
EID-14	REQ-910-03; REQ-910-04; REQ-1502-05
EID-15	REQ-910-04
EID-16	REQ-910-01; REQ-2979-01
EID-17	REQ-910-02; REQ-910-05; REQ-2979-02; REQ-1502-05
EID-18	REQ-910-05; REQ-2979-03; REQ-1502-05
EID-19	REQ-910-05; REQ-2979-04
EID-20	REQ-1502-06; REQ-2981-02
EID-20a	REQ-1502-06; REQ-2981-02