

GP-02/Annex D

PL EUDI Wallet Certification System

Requirements for the evaluation of
cryptographic mechanisms

VERSION 1.01

2026.05.20

Document reference	GP-02/Annex D
Version	1.01
Status	FINAL
Date	2026-04-20
Document type	Technical specification
Parent framework	GP-02
Scheme Owner	Republic of Poland / Minister of Digital Affairs
Certification target	EUDI Wallet Solution
Primary audience	EUDI Wallet Provider, PID Provider, CABs
Secondary audience	Scheme Owner
Assurance level <evaluation, EU Regulation 2019/881>	high
Subsidiary Documents	None

Table of Content

<u>1</u>	<u>SPECIFIC REFERENCES.....</u>	<u>4</u>
<u>2</u>	<u>REQUIREMENTS FOR DOCUMENTATION.....</u>	<u>5</u>
2.1	Security Target and Secure User Guide	5
2.2	Cryptographic specification	5
2.3	Noise source description.....	6
2.4	Key management description	6
2.5	Implementation representation	7
<u>3</u>	<u>TOE SECURITY REQUIREMENTS</u>	<u>8</u>
<u>4</u>	<u>EVALUATION OF CRYPTOGRAPHIC FUNCTIONS.....</u>	<u>9</u>
4.1	Conformity assessment and vulnerability analysis.....	9
4.2	Penetration testing.....	10
<u>5</u>	<u>TABLE OF CRYPTOGRAPHIC MECHANISMS</u>	<u>11</u>
<u>6</u>	<u>REFERENCE DOCUMENTS.....</u>	<u>13</u>

1 Specific references

- 1 [PL-Schem] PL EUDI Wallet Certification System
- 2 [GP-02] Cybersecurity Certification Scheme for [PL-Schem]
- 3 [Req-ST] Requirements for ST and IAR, if applicable
- 4 [Req-UG] Requirements for secure user guide

2 Requirements for documentation

- 1 *GENERAL NOTE: The auxiliary verb "should" be used to indicate a recommendation. However, if the applicant or evaluators choose other options than the one used in recommendation, the justification is mandatory.*
- 2 The Applicant shall provide the documentation described in [PL-Schem], [Req-ST], and [Req-UG].
- 3 *NOTE: For the sake of completeness, all necessary applicant documents are listed in this section.*

2.1 Security Target and Secure User Guide

- 4 The Applicant shall provide a Security Target (ST) (according to [Req-ST]), a Secure User Guide (SUG) (according to [Req-UG]), and the overview of the TOE architecture. In the case of a re-evaluation or re-certification, the Applicant shall further provide an Impact Analysis Report (IAR) (in accordance with [Req-ST] and G-01).

2.2 Cryptographic specification

- 5 The Applicant shall provide a cryptographic specification for the cryptographic mechanisms that are used to enforce the security functionality of the TOE. An overview of the cryptographic mechanisms used shall be presented in a table as shown in Section 5. The cryptographic specification shall be provided as a separate document named "Crypto-Annex" and shall contain the contents mentioned in lines 4 to 7.
- 6 Cryptographic algorithms and mechanisms used by the TOE shall be selected from the agreed algorithms listed in the ECCG catalogue [ECCG-ACM].
- 7 Cryptographic protocols used by the TOE that are standardized and publicly specified shall be identified by the developer and shall be accepted by CAB-CB before the start of the evaluation.
- 8 For cryptographic protocols that are not standardized and are specific to, designed for, or introduced by the TOE developer, the developer shall provide sufficient technical information to enable construction of a formal symbolic model of the protocol under the Dolev–Yao adversary model. Such information shall include, as applicable, the protocol roles, message flows, message formats, cryptographic operations, key material and its lifecycle, trust assumptions, security objectives, and all conditions relevant to protocol execution and error handling.

- 9 The description of a cryptographic mechanism shall be categorized by interfaces and shall contain the following information:
- References to accessible standards that unequivocally define the mechanism, together with selected options or parameters (e.g., key lengths, domain parameters);
 - The security functionality enforced by the mechanism (mapping to the security functions claimed in the security target);
 - The security objective achieved by the mechanism (e.g., confidentiality, integrity, authenticity).

2.3 Noise source description

- 10 If the cryptographic specification contains random number generators, the Applicant shall provide a noise source description as chapter of the “Crypto-Annex” document for the noise sources that are used for seeding.
- 11 The description of a noise source should contain information about its type (physical or non-physical) and operating principle.
- 12 If multiple noise sources are used, a justification that the sources are independent shall be provided.
- 13 The noise source description shall contain a justification that random bits used for seeding have at least 125 bits of min-entropy. If a CC-certified physical random number generator is used, a reference to the certification ID is sufficient.

2.4 Key management description

- 14 The Applicant shall provide a key management description as chapter of the “Crypto-Annex” document containing information about cryptographic keys and parameters that are used by the TOE for cryptographic operations.
- 15 The description of a key shall contain information about its type, generation, distribution, usage, storage, destruction, validity period, and protection requirements.
- 16 The key management description shall also contain information on other parameters including domain parameters, initialization vectors, counters, and tweaks.
- 17 The key management description shall highlight hierarchical relations between keys (e.g., whether a key is derived from another key, or whether a key is encrypted using another key).

2.5 Implementation representation

- 18 The Applicant shall provide the CAB-ITSEF with an implementation representation for the cryptographic mechanisms that are used to enforce the security functionality of the TOE. If the Applicant cannot provide the implementation representation for one or more cryptographic mechanisms, this shall be discussed with the CAB-CB before the evaluation starts.
- 19 *NOTE: The implementation representation should consist of source code or pseudocode.*
- 20 If source code is provided, it shall be the code that was used to build the TOE. If pseudocode is provided, it shall be at a level of detail that closely resembles the actual implementation (in particular, it shall include side-channel countermeasures, if implemented).
- 21 The implementation representation shall cover the implementation of cryptographic functionality itself as well as the parts of the implementation where the cryptographic functionality is invoked.
- 22 If the implementation uses open-source cryptographic libraries, the implementation representation shall include information about their origin, version and all changes applied by the Applicant. The Applicant shall provide a key management description as chapter of the “Crypto-Annex” document containing information about cryptographic keys and parameters that are used by the TOE for cryptographic operations.

3 TOE security requirements

- 23 *NOTE 1: Cryptographic mechanisms used by the TOE should implement the recommended procedures and configurations specified in [ECCG-ACM] and, where applicable, [TR-03116-4]. Other procedures may not be used unless they are explicitly permitted. The current version of [ECCG-ACM] or [TR-03116-4] applies in each case. In the event of contradictions between [ECCG-ACM] and [TR-03116-4], [ECCG-ACM] takes priority.*
- 24 *NOTE 2: The TOE should encrypt communication channels to external components using state-of-the-art technology, at a minimum using TLS.*
- 25 The TOE shall authenticate communication partners prior to the transmission of sensitive data.
- 26 The TOE shall meet the requirements for lifecycle security regarding keys and lifecycle requirements for critical assets specified in the Security Target provided by the Applicant.
- 27 *NOTE 3: The TOE's cryptographic methods should be designed so that they can be adapted to new cryptographic findings (e.g., by changing cryptographic primitives or key lengths).*

4 Evaluation of cryptographic functions

28 *NOTE: The cryptographic evaluation consists of conformity assessment, vulnerability analysis, and penetration testing.*

4.1 Conformity assessment and vulnerability analysis

29 The aim of the conformity assessment in the context of the cryptography evaluation is to establish that the cryptographic mechanisms of the test object comply with [ECCG-ACM], Section 3.1 of this document and [TR-03116-4], and that the implementation of the test object is in conformity with the applicant's documentation.

30 *NOTE 1: The aim of vulnerability analysis in the context of cryptographic evaluation is to determine that cryptographic implementation does not contain exploitable implementation weaknesses. To identify potential flaws in the implementation, the evaluators should use their experience and any information at their disposal. In particular, the evaluators should start searching for potential vulnerabilities during the conformity assessment activities.*

31 CAB-ITSEF shall identify findings and document them in the ETR.

32 CAB-ITSEF shall execute work unit 1 from Section 6.12 [FITCEM] (6.12.4.1).

33 The CAB-ITSEF shall examine the noise source description to determine that the Applicant claim regarding entropy is plausible.

34 CAB-ITSEF shall execute work unit 2 from Section 6.12 [FITCEM] (6.12.4.1).

35 *NOTE 2: Conformance testing should achieve a high coverage of the externally accessible cryptographic algorithms, schemes, and protocols.*

36 *NOTE 3: Standardized cryptographic protocols used for communication via external interfaces should be evaluated using automated test tools to save evaluation time for the aspects that require human analysis.*

37 *NOTE 4: CAB-ITSEF should take the following publicly available sources of information into consideration: ECCG guidance: [ECCG-ACM], Security considerations in cryptographic standards, Academic literature, CVE entries, security advisories of CERTs or vendors, change logs of cryptographic libraries, blogs of security researchers, information on potential vulnerabilities provided by CAB-CB itself.*

38 *NOTE 5: CAB-ITSEF should take the following types of attack into consideration: Bypass of cryptographic functionality, Logical attacks, Reaction/oracle attacks, timing attacks.*

39 CAB-ITSEF shall take the impact of the operational environment of the TOE on the identification of potential flaws into consideration.

- 40 *NOTE 6: Vulnerabilities in cryptographic implementations may arise due to misuse of mechanisms, implementation weaknesses/errors, or side-channels. Whether a vulnerability or side-channel leads to an attack depends, among other things, on the ability of the attacker to operate in the operational environment of the TOE. This might lead to additional types of attacks, e.g.:*
- *Side-channel attacks: power consumption, electromagnetic emanation, sound emanation*
 - *Fault attacks,*
 - *Micro architectural attacks: cache attacks, branch prediction, speculative execution,*
 - *Cold boot attacks.*

4.2 Penetration testing

- 41 *NOTE 1: The aim of penetration testing is to determine that the cryptographic implementation resists attacks, i.e., the cryptographic implementation does not contain vulnerabilities that could be exploited by attackers with “enhanced basic” attack potential [FITCEM] (5.4).*
- 42 CAB-ITSEF shall attempt to bypass or break the cryptographic security functionality. The evaluator shall set up a risk-based sampling strategy for this, considering the time allocated for this step. The testing strategy shall be based on the results of previous steps of the evaluation, including the conformity assessment, the identification of potential flaws, and the evaluation steps described in [GP-02].
- 43 *NOTE 2: The testing strategy should be continuously updated, especially when results, including those from the other steps, become available. If more time is needed for this step than initially allocated, CAB-ITSEF shall record this fact and provide a rationale for this in the ETR.*

5 Table of cryptographic mechanisms

44 Informative examples of officially approved cryptographic mechanisms for standardized communication protocols are included in subsequent tables.

1. Purpose	2. Cryptographic Mechanism	3. Standard of Implementation	4. Key Size in Bit
Trusted Channel to ... via HTTPS with TLS 1.3 [RFC 8446]			
Authenticity	RSA-signature generation and verification (RSASSA-PSS) using SHA-256	[PKCS#1 v2.2] (RSA), [FIPS 180-4] (SHA)	Modulus length = 3072
Authentication	RSA signature generation and verification (for RSASSA-PSS)	[RFC 5246] (TLS) [RFC 3447] (PKCS#1 v2.1)	3072, 4096
Key Agreement	ECDHE curves: secp256r1 secp384r1	[RFC 5246] (TLS) [RFC 8422] (TLSECC) [IEEE P1363] (ECDH)	256, 384
Key Agreement	DHE groups: ffdhe3072 ffdhe4096	[RFC 5246] (TLS) [RFC 7919] (DHE)	3072, 4096
Confidentiality	AES in GCM mode	[RFC 5246] (TLS) [RFC 5288] (AESGCM) [RFC 5289] (AES-GCM) [FIPS 197] (AES) [SP800-38D] (GCM)	128, 256
Confidentiality	AES in CBC mode	[RFC 5246] (TLS) [FIPS 197] (AES) [SP800-38A] (CBC)	128, 256
Integrity	HMAC with SHA-2	[RFC 5246] (TLS) [FIPS 180-2] (SHA)	256, 384
Random Number Generator	Deterministic RNG DRG.3	[AIS-20]	

1. Purpose	2. Cryptographic Mechanism	3. Standard of Implementation	4. Key Size in Bit
Trusted Channel to Command Line Interface (CLI) with SSH [4251]			
Key Exchange (Agreement)	diffie-hellman-group15-sha512	[RFC 4253] (Key Exchange Methods) [RFC 8268] (more DH for SSH) [RFC 3526] (group specification)	3072
Authentication	Elliptic curve digital signature algorithm with SHA-256 and nistp256 (ecdsa-sha2-256)	[RFC 5656]	256
Confidentiality	AES in CTR mode	[RFC 4344] (SSH Encryption Modes)	128, 192, 256
Integrity	HMAC with SHA-2 (hmac-sha2-256)	[RFC 4253] (SSH) [RFC 6668] (SHA-2 Integration) [RFC6234] (SHA-2 Definition)	256
Random Number Generator	/dev/urandom		

6 Reference documents

- 1 [FITCEM] Fixed-time cybersecurity evaluation methodology for ICT products (FIT CEM), EN 17640:2022
- 2 [ECCG-ACM] European Cybersecurity Certification Group (ECCG) Sub-group on Cryptography, Agreed Cryptographic Mechanisms, current version
- 3 [TR-03116-4] BSI TR-03116-4 wer. 1.0 PL, Specyfikacja kryptograficzna projektów realizowanych przez organizacje: Metody komunikacji w aplikacjach <https://www.gov.pl/web/baza-wiedzy/bsi-tr-03116-4-wer-10-pl>