

GP-02/Annex C

PL EUDI Wallet Certification System

Requirements for the evaluation of
functional specification and TOE design

VERSION 1.01

2026.05.15

Document reference	GP-02/Annex C
Version	1.01
Status	FINAL
Date	2026-05-15
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 contents

<u>1. INTRODUCTION.....</u>	<u>4</u>
<u>2. NORMATIVE REFERENCES.....</u>	<u>5</u>
<u>3. SPECIFIC REFERENCES.....</u>	<u>5</u>
<u>4. REQUIREMENTS FOR DOCUMENTATION.....</u>	<u>6</u>
4.1. Product documentation provided by the Applicant	6
4.2. Requirements for development documentation	6
4.2.1. Functional specification	6
4.2.2. TOE design.....	6
4.2.3. Security Architecture Specification	7
4.3. Software Bill of Materials (SBOM).....	7

1. Introduction

1 *NOTE: This chapter does not contain requirements*

2 As part of the FITCEM (EN 17640) evaluation process, the security claims of the Target of Evaluation (TOE) are assessed against specified security objectives. To facilitate this assessment, the evaluation process places significant emphasis on a review of the developer-supplied documentation. Specifically, the Security Target and the accompanying development documentation constitute the primary artefacts subject to scrutiny. The Security Target details the TOE's asserted security capabilities, identifies potential threats, and describes the corresponding security functions intended to provide protection.

3 The development documentation provides evidence supporting the implementation and effectiveness of these security functions, demonstrating the technical realization of the Security Target's stated objectives. A comprehensive evaluation of these artefacts, in conjunction with supplementary evidence, forms the basis for determining compliance with the applicable FITCEM requirements.

2. Normative references

- 4 [EN17640] EN 17640:2022. Fixed time cybersecurity evaluation methodology for ICT products
- 5 [AIS B1] Application Notes and Interpretation of the Scheme (AIS), AIS B1, Version 2.0.1, 17.11.2023, Certification body of BSI

3. Specific references

- 6 [Crypto-Annex] Requirements for the evaluation of cryptographic mechanisms
- 7 [PL-Schem] PL EUDI Wallet Certification System
- 8 [Req-ST] Requirements for ST and IAR, if applicable
- 9 [Req-UG] Requirements for secure user guide,

4. Requirements for documentation

4.1. Product documentation provided by the Applicant

- 1 The Applicant shall submit the CAB-ITSEF the TOE along with the accompanying documentation.
- 2 The Applicant shall provide the documentation described in [PL-Schem], [Req-ST], and [Req-UG]. For the sake of completeness, all necessary applicant documents are listed in this section.
- 3 The documentation shall include the following mandatory components:
 - Security Target (according to [Req-ST]), and
 - Secure User Guide (according to [Req-UG]),
- 4 The Security Target shall include or refer to the Cryptographic specification (according to the [Crypto-Annex]).
- 5 Moreover, the Applicant shall provide CAB-ITSEF with the following documentation:
 - development documentation, including:
 - Functional specification,
 - TOE design,
 - Security architecture specification,
 - Software Bill of Materials (SBOM)
- 6 The following sections outline the requirements that the development documentation must meet.

4.2. Requirements for development documentation

- 7 The development documentation shall fulfil the requirements in following subsections.

4.2.1. Functional specification

- 8 The functional specification shall encompass description of every interface that can affect security (external, internal, installation/configuration) down to exact parameters, data types, encodings, validation rules, error handling, and cryptographic bindings.

4.2.2. TOE design

- 9 The TOE design shall include:
 - a detailed architectural overview (component diagram) showing the Wallet Instance.
 - complete mapping tables with security functions architectural components and interfaces.
- 10 The TOE's dependencies on the system environment, including software packages, interfaces, libraries, database connections, APIs, and other

components, should be specified in the TOE design. The specification must reflect the operating system of the mobile devices.

4.2.3. Security Architecture Specification

- 11 Security Architecture Specification shall include description of:
 - security domains within the TOE and their separation,
 - procedures for secure initialization of the TOE
 - protection of the TOE against tampering and bypass of security functions.

4.3. Software Bill of Materials (SBOM)

- 12 The SBOM provided by the applicant shall include the vulnerability report as described in [AIS B1]. The components included in the SBOM shall comply with the TOE design.