

GP-02/Annex B

PL EUDI Wallet Certification System

Requirements for the evaluation of Secure

User Guide

VERSION 1.01

2026.06.12

Document reference	GP-02/Annex B
Version	1.01
Status	FINAL
Date	2026-06-12
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, 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. APPLICATION NOTES AND INTERPRETATION.....</u>	<u>6</u>
3.1. Requirements for Secure User Guidance	6
3.1.1. Comprehensive	6
3.1.2. Concise	7
3.1.3. Clearly separated from other information.....	7
3.1.4. Unambiguous.....	7
3.1.5. Easy to find.....	7
3.1.6. References to risk information if deviating from the secure state	7
3.2. Format of the Secure User Guidance.....	7

1. Introduction

- 1 *NOTE: Introduction does not contain requirements.*
- 2 The Security Target (ST) describes the Target of Evaluation (TOE) and specifies its security functionality. The effectiveness of the functionality described depends on the secure configuration of the TOE and its operational environment.
- 3 It is therefore essential that users can establish and maintain secure configuration. Failure to do so can result in certain functionalities or interfaces being (de)activated in a manner that compromises the secure operation of the TOE.
- 4 The Secure User Guide (SUG) is the documentation of the secure configuration of the EUDI Wallet Instance with its relevant interfaces. It can either be part of the Applicant documentation or provided as a separate document.
- 5 As indicated in EN 17640, Section 6.6, the evaluation encompasses the task aiming at verification that the TOE can be installed as described in the Secure User Guide.

2. Normative references

- 6 [EN17640] EN 17640:2022. Fixed time cybersecurity evaluation methodology for ICT products
- 7 [AIS-B3] BSI AIS-B3. 15.11.2025. Requirements for user guidance Version 2.1

3. Application notes and interpretation

3.1. Requirements for Secure User Guidance

8 The SUG shall fulfil the requirements in following subsections.

3.1.1. Comprehensive

9 *NOTE 1: The SUG addresses the users of TOE. Thus, it is essential that it provides sufficient guidance to enable users to properly set up the TOE according to the secure configuration.*

10 The SUG shall assist end users with the secure configuration, installation, operation and maintenance of TOE certified secure configuration.

11 Language and complexity shall be adapted to the audience. The SUG shall be provided in the language(s) of the expected users.

12 *NOTE 2: The following guidelines can be used:*

- *Layperson, e.g., commercial off-the-shelf (COTS) products: no specific IT or information security skills and knowledge,*
- *Experienced user, e.g., products sold for a certain well-described user group: knowledge of main IT (but not necessarily information security) concepts in the domain of the product,*
- *Administrator, e.g., products targeting professional managed environments: general and domain specific knowledge of IT and network concepts, ability to configure connected devices, not necessarily information security knowledge and skills.*

13 *NOTE 3: The SUG should include publicly available information about the TOE as required by the Commission Implementing Regulation (EU) 2024/2981 in Annex V or should link this information. Specifically, it will include:*

- *any limitations on the use of a wallet solution,*
- *the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity-related updates,*
- *contact information of the Wallet Provider and accepted methods for receiving vulnerability information from end users and security researchers,*
- *a reference to online repositories listing publicly disclosed vulnerabilities related to wallets and to any relevant cybersecurity advisories.*

3.1.2. Concise

- 14 The SUG shall be limited to information necessary for the evaluated secure configuration. Any other configurations or features are described in separate guidance (linked from the SUG).

3.1.3. Clearly separated from other information

- 15 The SUG shall be clearly identifiable (e.g., as a dedicated chapter or a separate document). Users shall know exactly where the security guidance starts and ends.

3.1.4. Unambiguous

- 16 The SUG shall unambiguously describe how to achieve and maintain the secure configuration. Descriptions shall match the actual user interface (menu labels, colors, steps, etc.).

3.1.5. Easy to find

- 17 The SUG shall be easily available and readable in a format suitable for the TOE (e.g., in-app help, PDF, first-launch wizard).

3.1.6. References to risk information if deviating from the secure state

- 18 If the TOE is allowed to operate in a non-secure state or users can deviate, SUG shall reference further information describing the associated end-user risks and how to return to the secure state.

3.2. Format of the Secure User Guidance

- 19 *NOTE 4: The SUG can be provided in a format and delivered on a medium suitable for the TOE. For example, it can be delivered with the TOE as a hard copy, as part of an online user help system, or on a separate medium.*