

GP-02/Annex A

PL EUDI Wallet Certification System

Template for Wallet Instance Security

Target

VERSION 1.01

2026.07.23

Document reference	GP-02/Annex A
Version	V 1.01
Status	FINAL
Date	23.07.2026
Document type	template
Parent framework	GP-02
Scheme Owner	Republic of Poland / Minister of Digital Affairs
Certification target	Composite TOE
Primary audience	EUDI Wallet Provider, CABs
Secondary audience	Scheme Owner
Assurance level <evaluation, EU Regulation 2019/881>	high
Subsidiary Documents	None

Table of content

<u>1</u>	<u>INTRODUCTION TO THE SECURITY TARGET TEMPLATE</u>	<u>4</u>
<u>2</u>	<u>INTRODUCTION.....</u>	<u>5</u>
2.1	Context of this document	5
2.2	Product identification	5
2.3	Components identification	6
2.4	References / acronyms.....	6
<u>3</u>	<u>PRODUCT DESCRIPTION</u>	<u>8</u>
3.1	General description.....	8
3.2	Features and interfaces.....	8
3.3	Product usage	9
3.4	Operating environment	9
<u>4</u>	<u>SECURITY PERIMETER</u>	<u>11</u>
4.1	Users	11
4.2	Assumptions	11
4.3	Assets.....	11
4.4	Threat model	12
4.5	Security functions	12
4.6	Threat coverage.....	13
<u>5</u>	<u>LIMITS OF EVALUATION</u>	<u>14</u>

1 Introduction to the Security Target template

[This section should be removed from the final Security Target]

Security Target (ST) describes the security functions, interfaces, threat model and (expected) operational environment for Wallet Instance (WI) as a component of EUDI Wallet solution. The WI, jointly with Wallet Secure Cryptographic Device, Wallet Secure Cryptographic Application and WI interfaces, constitute the composite Target of Evaluation (TOE) as defined by the Polish [cybersecurity certification programme](#) [GP02]. ST should follow the structure and contain the content specified in the following subsections of this template.

ST is a public document that is made available to TOE users. All technical terms used in the ST that are not obvious should be clearly defined. As far as possible, terminology specific to a particular manufacturer should be avoided in the description provided in the ST.

The following sections describe how the Security Target shall be organised and which content is expected in the various sections. Where applicable, a subsection provides examples and further explanation.

Unless noted otherwise, the ST shall be written in a way that the expected end customer, i.e. the person who decides about the acquisition of the product, is capable of understanding its content.

To facilitate the proper understanding, appropriate references to stable reference sources should be provided.

2 Introduction

2.1 Context of this document

Required content

This subsection shall describe why this document was created and how the content was derived.

This document constitutes the Security Target (ST) for the <TOE name and version> in the scope of the Polish [GP02] cybersecurity certification programme. The ST essentially describes the security functionalities, assets, the threat model, interfaces and operational environment of the TOE.

The following templates and the schema documents were used to create the ST:

- Template for Wallet Instance Security Target, version x.y
- <if applicable, further documents>

2.2 Product identification

Required content

This subsection shall state, without ambiguity, the name and specific version of the TOE (Target of Evaluation), including where applicable, the distinct version numbers of the software and the hardware used. It shall also state how the expected end customer can unambiguously identify the product.

Table 1. TOE identification

TOE name	<TOE name>
TOE version	<TOE version>
TOE vendor	<TOE vendor name>

The TOE is unambiguously identified by users in the following way:

<Description how the expected end customer can identify the product unambiguously.>

<List of TOE supporting documents, such as Secure User Guide, instruction documents etc.>

<Relevant diagrams, screenshots or product images may be included in this section for illustrative purposes.>

2.3 Components identification

Required content

This subsection shall present information on already evaluated or certified the following components used for composition TOE evaluation: WSCD and WSCA. This information should include a description, intended use, and configuration options of the components as well as the identification of the respective certificate, if applicable.

The composite TOE is defined in [GP02] certification scheme and covers the following components:

- <the Product itself>;
- [Wallet Secure Cryptographic Device](#) <WSCD name and version>;
- [Wallet Secure Cryptographic Application](#) <WSCA name and version>.

<Relevant information on WSCA, WSCD and WI interfaces.>

2.4 References / acronyms

Required content

This subsection shall list all acronyms used.

This subsection shall contain all references, e.g. to implemented standards or to further documents of the vendor. If further documents of the vendor are referenced, they need to be available to all customers free of charge.

All content required by this document shall appear in the ST document itself and not in referenced documents, except for the cryptographic specification which shall be supplied separately.

Table 2. List of acronyms

Acronym	Explanation
SCI	Secure Cryptographic Interface
ST	Security Target
TOE	Target of Evaluation
WSCA	Wallet Secure Cryptographic Application
WSCD	Wallet Secure Cryptographic Device
<acronym>	<acronym definition>

References

[GP02] GP-02 PL EUDI Wallet Certification System, Cybersecurity Certification Scheme

3 Product description

3.1 General description

Required content

This subsection shall contain a general description of the TOE suitable for publications on websites or in product databases.

TOE is a Wallet Instance, i.e. the app or application installed on a user device, which is an instance of a Wallet Solution and belongs to and is controlled by a User. This component implements the core business logic and interfaces of the EUDI Wallet ecosystem. User guidance and user interaction with the Wallet take place via Wallet Instance. The Wallet Instance directly interacts with the WSCA to securely manage critical assets and execute cryptographic functions. It interfaces with one or more key stores for the management of non-critical cryptographic assets.

<Further general information on the TOE/product and product type>.

<Illustrative figures may be included in this section, which cover the Wallet Solution architecture.>

3.2 Features and interfaces

Required content

This subsection shall list and describe the features and interfaces of the TOE that are relevant to the evaluation. The terms used shall be defined if they are not self-explanatory. Definitions can be given in the main section or by references to stable and accessible sources under public domain.

The description shall avoid company specific terminology where possible.

Any communication interfaces shall be listed and described in this subsection.

Features and interfaces which are not accessible for testing shall be clearly marked as such.

The TOE provides the set of interfaces as defined in Table 3.

Table 3. TOE interfaces

Physical interface	Logical interface	Protocol	Description	Evaluation scope
<If applicable: Name of the physical interfaces for direct interaction with the TOE>	Secure Cryptographic Interface (SCI) <Name of the logical interfaces for direct interaction with the TOE> <If applicable: Specify as client/server>	<Name of the protocol> <If applicable: further information on the interface>	Enables the Wallet Instance to communicate with the WSCA. <Information on the interface> <internal interface or external interface?>	Yes <Is the interface within the scope of the evaluation? Is it necessary for typical use? Is it active?>

3.3 Product usage

Required content

This subsection shall describe in natural language the intended product usage, jointly with description of typical users of the TOE. The details of the operating environment shall be stated in the subsequent subsections.

[Wallet Instance is an application designed for use on mobile devices \(smartphone app\). It serves as an interface for various stakeholders and components within the wallet ecosystem \(e.g., wallet users, wallet providers, PID providers, relying parties\). User interaction with the Wallet takes place via the TOE.](#)

[Users of the TOE are the users of the wallet application. They install the TOE on a mobile device and, through a guided process, register the TOE with a backend system of the wallet provider, which also includes the WSCA and WSCD.](#)

<further information on the use of the TOE/product>

3.4 Operating environment

Required content

This subsection shall state the required operating environment of the TOE, i.e. technical environment, expected users, expected threats.

Specific hardware or software required to operate the TOE shall be stated in this subsection.

If several environments are possible (e.g. several versions of some background systems or operating systems), it shall be clearly stated which version is to be used for evaluation.

The system environment should be described by its requirements and dependencies of the TOE from such environment . Minimum and, where necessary, maximum requirements for hardware and software that ensure the secure operation of TOE shall be specified and indicated in the hardware and software specifications.

Note: Requirements for the system environment, which lead to potentially large combinations in the design of hardware and software, may require increased test effort and exceed the complexity limit or maximum test duration for a certification in the certification procedure.

[The TOE is intended for use on mobile devices.](#)

<Information on the specific hardware and software required to operate the TOE, including description of the supported devices/types of devices and operating system versions here.>

<Description of the structure, operating concept, and operators of the wallet provider backend system.>

4 Security perimeter

4.1 Users

Required content

This subsection shall describe the users or roles the TOE supports. The users or roles are not limited to those explicitly defined in the TOE. They might also be defined implicitly by the interface they act on. This subsection shall describe the characteristics of each user or role, i.e. which kind of tasks it is associated with, if it has certain privileges in the TOE, if access is limited to certain ports/services etc.

The mandatory role is the user of the TOE.

Note: Depending on the complexity of the TOE or its operational environment, roles can also be implemented through different users. If the TOE also offers other internal roles, such as users of databases, this should be described in detail. When multiple roles are grouped into a single user, it is important that the access rights remain separate. I.e. the application software cannot be operated with the rights of an administrator.

4.2 Assumptions

Required content

The TOE might require a certain environment to fulfil its security properties. This environment may consist of personal attributes (e.g. required knowledge and skills of certain users), logical requirements (e.g. network topology), physical measures (e.g. physical access restrictions) organisational necessities (e.g. rights and roles) or IT-related assumptions (e.g. encryption used on network links). A brief colloquial rationale for the existence of these assumptions shall be provided in this subsection.

Note: This subsection shall be consistent with all other subsections, especially Subsection 3.3 Product usage. For example, requiring certain knowledge of the user of the TOE is inconsistent with a product description, which claims that the product is intended for the general public.

Each assumption shall be uniquely identifiable (for example by using unique Id, e.g. "Asmpt-1").

4.3 Assets

Required content

This subsection shall list and describe the assets of the TOE or protected by the TOE, whose security properties (i.e. confidentiality, integrity or availability) are worthy of protection.

Each asset shall be uniquely identifiable (for example by using unique Id, e.g. "Ast-1").

4.4 Threat model

Required content

This subsection shall describe the attackers assumed in the threat model. They shall be the most likely expected attackers of the TOE in the intended environment.

Each attacker shall be uniquely identifiable (for example by using unique Id, e.g. "Attck-1").

This subsection shall describe the threats (i.e. adverse actions performed by attackers), which are countered by the security functions of the TOE.

Each threat shall be uniquely identifiable (for example by using unique Id, e.g. "Thrt-1").

4.5 Security functions

Required content

This subsection shall contain a description of the security functions of the TOE to protect the assets against the threats. It shall reference where necessary the technical information (for example *Layer 2, Protocol xy*), where possible by referencing the appropriate and active standards. Stable online references should be used.

This subsection may refrain from using end customer language as long as technical terms suitable for average experts are used.

The TOE shall have sufficient own security functions that can be evaluated through external interfaces.

If the ST designates security functions that are fully or partially implemented by the system environment, they shall be specified in the document describing the dependencies to the system environment. The indication of a user for the security function from the role model is necessary if the TOE requires separate rights for the call or implementation of the security function. It shall be clearly described which parts of the security functionality are realised by the system environment and how these parts are integrated or used by the TOE to provide the security function to be tested.

In addition to the security functions provided by the TOE itself, security functions that are fully or partially implemented by the system environment shall also be indicated in the ST as security functions used. The designation of the security function shall clearly

allow a distinction between those provided by the TOE itself and the security function implemented in the system environment.

Each security function shall be uniquely identifiable (for example by using unique Id, e.g. "SecFun-1").

4.6 Threat coverage

Required content

This subsection shall contain a table mapping of all threats to the associated attackers, the affected assets and the involved TOE security functions. For complex relationships, it may contain a terse rationale.

Table 4. Mapping of threats, attackers, assets and security functions

Threat	Attackers	Assets	TOE Security Functions
<threat from section 4.4>	<attackers from section 4.4>	<assets from section 4.3>	<security functions from section 4.5>

5 Limits of evaluation

Required content

This subsection shall contain all features, functions, services and interfaces that are out of scope of this certification. The excluded items may not contradict the intended usage of the TOE.

If the TOE security functions require dynamic content to operate (e.g. from remote databases), the ST shall clearly state that the remote system providing the content is not part of the evaluation. However, the security function requiring the content shall be part of the evaluation.