

WP-02-02

FITCEM Protection Profile
for the EUDI Wallet Instance

VERSION 1.01

2026.07.22

Document reference	WP-02-02
Version	V 1.01 (2026-07)
Status	FINAL
Date	22.07.2026
Document type	Protection Profile – FITCEM / EN 17640:2022+A1:2026
Parent framework	GP-02
Scheme Owner	Republic of Poland / Minister of Digital Affairs
TOE	composite TOE
TOE type	None
Primary audience	CAB-ITSEF, EUDI Wallet Provider, CAB-CB
Assurance level <evaluation>	High (CSA – assurance level “high”)
Subsidiary documents	WM-02-01, WM-02-02

History of changes

No.	Change	Version	Date
1.	Official version	1.0	2026-06-12
2.	Editorial corrections	1.01	2026-07-22

Table of Content

1	Introduction	5
1.1	Purpose of this Document	5
1.2	Relationship to Other Documents	5
2	TOE Description.....	6
2.1	TOE Overview	6
2.2	TOE Boundary.....	7
2.3	TOE Components (Composite)	7
2.4	Supported Platforms	7
3	Security Problem Definition (SPD).....	9
3.1	Assets.....	9
3.2	Threats.....	9
3.3	Assumptions on the Operational Environment	9
4	Normative references	10
5	Specific references.....	10
6	Wallet Instance specific requirements for the TOE	10
6.1	Authentication and authorization.....	11
6.2	Logging	12
6.3	Services.....	13
6.4	Local storage.....	14
6.5	Network & Interfaces	15
6.6	Documentation	15
6.6.1	User guidance documents	15
6.6.2	Secure use of the TOE.....	16
6.7	Additional security measures (Hardware Security)	17
6.8	Cryptography	17
Annex A.	Assumptions regarding end user devices.....	19
A.1	Introduction.....	19
A.2	Mobile device assumptions.....	19

1 Introduction

1.1 Purpose of this Document

- 1 This document specifies the FITCEM Protection Profile (PP) for the EUDI Wallet Instance mobile application along with its interfaces operating on Android and iOS platforms. It defines the Target of Evaluation (TOE), its security problem definition (threats, assumptions, organisational security policies), security objectives, and security requirements in accordance with EN 17640:2022 +A1:2026 (FITCEM) and the national certification scheme GP-02.
- 2 This PP is a product-layer specification within the WP-02 series. It is consumed by: (a) CAB-ITSEF as the basis for constructing an Evaluation Plan (TDS-MobileApp-EUDI) and elaborating Security Target (ST); (b) EUDI Wallet Provider as the basis for developing the conformant ST for their product; (c) CAB-CB for issuing the certificate of conformity.
- 3 The PP is structured following the EN 17640 PP conventions, adapted for a mobile application evaluation. It incorporates requirements derived from eIDAS 2.0, CIR (EU) 2024/2981, ARF 2.8.0, OWASP MASVS v2, and MITRE ATT&CK Mobile v14.

1.2 Relationship to Other Documents

Document	Title	Relationship to WP-02-02
WP-02-01	Decomposition - EUDI Wallet security requirements	Input: provides the initial decomposition of security requirements that this PP refines into security requirements
WP-02-03	EU CC Protection Profile for WSCA	Peer: covers the Wallet Secure Cryptographic Application; this PP references WSCA as a security boundary dependency
WM-02-01	Extension of FITCEM methodology to EUDI Wallet solution	Subordinate: defines how CAB-ITSEF applies FITCEM to evaluate this PP's requirements
GP-02	PL EUDI Wallet Certification System Cybersecurity certification scheme	Parent: specifies the certification scheme under the FIT PP operates in

2 TOE Description

2.1 TOE Overview

- 4 According to EN 17640:2022 + A1:2026, the composite TOE consists of two components: Wallet Instance mobile application (a dependent component) and WSCA/WSCD (considered jointly as a base component). The EUDI Wallet Instance mobile application along with its interfaces is deployed on Android and iOS mobile platforms.
- 5 The Wallet Instance enables a natural person (User) to: (a) receive and store PID, QEAs, and other attestations of attributes from EAA Providers; (b) present identity attributes to Relying Parties online and in proximity; (c) generate qualified electronic signatures; (d) manage the wallet lifecycle (onboarding, suspension, revocation).
- 6 The Wallet Secure Cryptographic Application (WSCA) is evaluated separately under WP-02-03 and referenced as a trusted component; The Wallet Secure Cryptographic Device (WSCD) is provided as already certified product from external source
- 7 The wallet provider's backend is used to operate and maintain the wallet instance. All communication between the Wallet Instance and the Provider backend is secured through robust encryption protocols. This ensures that sensitive data, such as transaction requests and identity verification details, remains confidential and tamper-proof during transit. The reference architecture is shown in Figure 1.

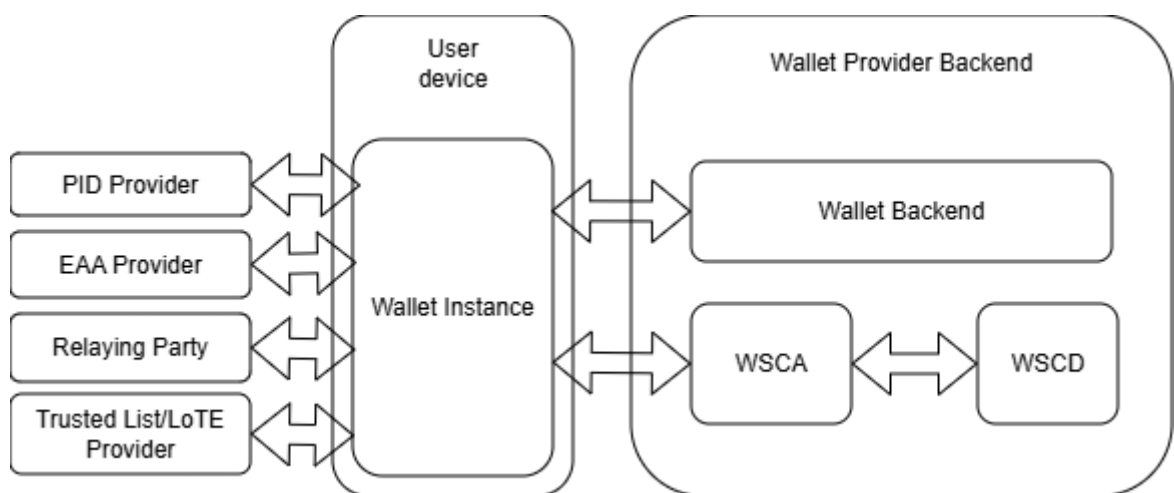


Figure 1 Reference architecture for Wallet Unit

- 8 This document forms a basis for evaluation of the Wallet Instance according to the European Standard EN 17640 Fixed-time cybersecurity evaluation methodology for ICT products [FiT CEM] within the scope of Wallet Instances. It encompasses requirement for:

- the TOE provisioning
- the TOE itself.

2.2 TOE Boundary

- 9 The TOE boundary includes all software components of the Wallet Instance application installed on the user's device, including business logic, credential management modules, protocol implementation (OpenID4VP, OpenID4VCI, ISO 18013-5 proximity), user interface components, WSCA interface layer, and (indirectly) WSCD interface layer. The TOE boundary explicitly excludes: the WSCD hardware itself; the WSCA cryptographic engine (evaluated under WP-02-03); the Wallet Backend (server-side components); Relying Party systems; and the mobile operating system.

2.3 TOE Components (Composite)

Component	Description	Scope	Evaluated under
Wallet Instance App (core)	Application code, UI, business logic, protocol stacks, credential management, WSCA/WSCD interface	Within the TOE boundary	This PP – WP-02-02
WSCA	Cryptographic application managing User's keys	Referenced as trusted component	WP-02-03 (CC Protection Profile)
WSCD	Hardware security element	Referenced as trusted component	External source
Wallet Backend	Server-side services: WUA issuance, PID provisioning, revocation	Outside the TOE boundary	WZ-03-03 (organisational)

2.4 Supported Platforms

Platform	Reference device	Module for securely storing and managing sensitive data	OS version	OEM variants
Android	-	StrongBox/TEE accompanied with API (Android Keystore)	Android 10+	All OEM variants with support for Android

Platform	Reference device	Module for securely storing and managing sensitive data	OS version	OEM variants
				Keystore, TEE or StrongBox
iOS	-	Secure Enclave accompanied with API (Keychain Services)	iOS 18+	Single vendor – no OEM variants

3 Security Problem Definition (SPD)

- 10 The security problem is described in terms of the threats the TOE is designed to mitigate, and assumptions about the operational environment.

3.1 Assets

- 11 *Note:*
Assets are defined by the Author of FIT ST.

3.2 Threats

- 12 The following threats are considered (based on the list of threats included in Annex I of CIR 2024/2981 and aligned to the architecture model where the TOE communicates with remote WSCA).

Threat	Description
T.UNAUTHORIZED_ACCESS	An attacker can gain unauthorized logical access to the TOE by bypassing or compromising user authentication mechanisms, allowing misuse of wallet functionalities and assets
T.CREDENTIAL_COMPROMISE	An attacker can extract, infer, or misuse cryptographic keys stored or used by the TOE, enabling unauthorized transactions
T.TRANSACTION_MANIPULATION	An attacker can alter transaction data in transit, causing unauthorized transfers, replay attacks, or incorrect transaction execution.
T.IDENTITY_MISUSE	An attacker can use stolen identity attributes stored in the TOE to impersonate the legitimate user towards relying parties
T.TOE_TAMPERING	An attacker can modify or replace the TOE software or configuration, compromising its security functions or disabling protections

3.3 Assumptions on the Operational Environment

Threat	Description
A.PLATFORM	The underlying mobile OS (Android/iOS) provides a secure execution environment with sandboxing, process isolation, secure boot, and has latest security patches

	installed that are available from the device manufacturer or OS provider at the time of use.
A.PERSONAL_DEVICE	The device is a personal device under the sole control of the legitimate user and is not rooted/jailbroken in normal operation.
A.REMOTE_WSCA	The remote Wallet Secure Cryptographic Application is certified at assurance level HIGH and correctly implements requested security services via the proprietary secure channel.
A.OS_UPDATES	The user/device keeps the mobile OS and system components up to date with security patches.
A.APP_INTEGRITY	The Wallet Instance is installed via trusted channels and can rely on platform attestation mechanisms (e.g., Play Integrity, App Attest).

4 Normative references

- 13 [FITCEM] EN 17640:2022+A1:2026. Fixed time cybersecurity evaluation methodology for ICT products

5 Specific references

- 14 [PL-Schem] PL EUDI Wallet Certification System
- 15 [Crypto-Annex] Requirements for the evaluation of cryptographic mechanisms
- 16 [ECCG-ACM] European Cybersecurity Certification Group (ECCG) Sub-group on Cryptography, Agreed Cryptographic Mechanisms, current version

6 Wallet Instance specific requirements for the TOE

- 17 *NOTE 1: This section defines requirements for the TOE. The definitions of terms used are defined in G-02 document.*
- 18 *NOTE 2: Typographical conventions used in relation to requirements: “Note” indicates explanation of the requirement, while ‘Application Note’ is addressed to FIT ST Authors to include more specific, implement-dependent requirement in their FIT STs.*

6.1 Authentication and authorization

Auth1	The TOE shall authenticate the user before he/she can access the TOE's functions or data provided by the TOE.
Auth2	The TOE shall support registration with a wallet provider backend service that is secured in accordance with the security requirements of the assets. Authentication factor generated during registration (e.g., cryptographic key material) may not be susceptible to manipulation, duplication, or extraction. <i>Application Note: The registration is intended to ensure that the wallet backend can unambiguously identify the TOE during subsequent operations and verify its integrity during authentication.</i>
Auth3	The TOE shall support creation and maintenance of binding between the Wallet Instance and user assigned keys managed by the WSCA.
Auth4	The TOE shall enable users to change authentication factors they have set themselves and to protect them from unauthorized access.
Auth5	The TOE shall support deletion of binding between the Wallet Instance and user assigned keys managed by the WSCA, when TOE is installed on another device or when the user deactivates the application via a dedicated deactivation option within the user interface.
Auth6	The TOE shall not disclose any confidential information or allow any inferences to be drawn regarding such information in response to an authentication request.
Auth7	The TOE shall require user re-authentication after a defined period of inactivity.
Auth8	Before the TOE transmits authentication data, the authenticity of the remote party (e.g., WSCA or wallet provider backend) shall be verified.
Auth9	The TOE shall require active confirmation by the authenticated user for the execution of a security-relevant function.
Auth10	Wallet Instance requires re-authentication if the period of inactivity is longer than defined value.
Auth11	Before executing functionality that requires active confirmation by the user, Wallet Instance shall ensure that: • the user has been transparently informed about the intended use. • the user was given the opportunity to confirm or decline the execution.
Auth12	Knowledge factors shall be stored securely so that their confidentiality and integrity are preserved.
Auth13	The input of the knowledge factor shall be protected against eavesdropping or manipulation.
Auth14	The Wallet Instance shall implement measures against brute-force attacks.

Auth15	The Wallet Instance ensures that the possession factor is used in a secure manner.
Auth16	The TOE shall establish and maintain unique, authenticated sessions for each security-relevant wallet operation. These sessions must be bound to specific transactions. The TOE shall prevent concurrent or overlapping sessions where such concurrency could compromise authentication, consent, authorization, or replay protection. <i>Application Note: Upon completion, cancellation, logout, inactivity, channel loss, security failure, or significant context change related to a transaction, the TOE shall terminate the associated session and reject attempts to reuse any previously generated confirmation data, nonces, tokens, or session identifiers.</i>
Auth17	TOE shall provide a logically isolated trusted user interaction path for all sensitive operations, including user authentication, re-authentication, transaction consent, credential disclosure authorization, credential capture or generation, presentation and signature-initiation operations. <i>Application Note: The trusted path shall display User the verified operation context and shall protect the user decision against overlay, UI spoofing, unauthorized screen capture, modification by and disclosure toby untrusted applications to the extent enforceable by the supported platform.</i>
Auth18	The TOE shall define and enforce the lifecycle of wallet user accounts, wallet instance identities, device bindings including identity proofing or equivalent evidence validation before activation or high-assurance use. <i>Application Note: The TOE requires User to provide new knowledge factors if it is reinstalled or installed on another mobile device.</i>

6.2 Logging

Log1	The TOE shall log wallet activation credential management, and presentation processes. However, specific attributes presented during these processes may not be recorded in the log. This log shall be presented to and made accessible by the respective authenticated users through the TOE's user interface.
Log2	The TOE may only grant the authorized user access to the log files. Log data shall be protected against unauthorized deletion, tampering, and unauthorized access. <i>Application Note: If national or EU regulations contain applicable provisions regarding the retention period for log data, these shall be observed.</i>
Log3	For the events listed above, the TOE shall store at least the following information:

	• timestamp • event type • result of the action that triggered the event. <i>Application Note: log files shall not contain authentication credentials or sensitive authentication data.</i>
Log4	The TOE shall generate audit and evidence records for security-relevant wallet operations, including activation, credential acquisition or generation, presentation, disclosure authorization, consent, signature initiation, attestation handling, backup or restore, trust or certificate validation, and relevant security failures. Each record shall contain sufficient tamper-evident context to later verify what was requested, authorized and performed, by which authenticated user or process, when, with what result, and under which transaction context, while avoiding unnecessary personal data.
Log5	The TOE shall detect logging failures, unauthorized local, network or remote connection indicators and security-relevant anomalies that may affect wallet security or accountability.
Log6	The TOE shall alert the authorized user, preserve available evidence, block or degrade affected security-relevant operations where mandatory evidence cannot be generated, and support incident handling through defined escalation and recovery information.

6.3 Services

Srv1	If security mechanisms (e.g., application isolation/sandboxing) are available on the mobile device, these shall be correctly integrated and utilized by the TOE. <i>Application Note: This also applies to residual data in shared resources, buffers, caches, clipboard, screenshots or IPC channels that shall be cleared, blocked or isolated before reuse</i>
Srv2	The TOE shall respond robustly to internally and externally generated data. The TOE shall not enter an undefined state at any time.
Srv3	The TOE shall protect the integrity, authenticity, and confidentiality of the transmitted data in accordance with the protection requirements. <i>Note: Implemented security functions can depend on the protection requirements (integrity, confidentiality, and authenticity) of the data.</i>
Srv4	The TOE shall validate the input and output to prevent incorrect processing. <i>Application Note: The input and output data of the TOE itself or external interfaces shall be checked for syntax, length, and content.</i>
Srv5	The TOE shall not disclose any critical information in error messages. <i>Application Note: Error messages may not contain any information helpful to potential attackers.</i>

Srv6	In its default configuration, the TOE shall enable only those functions which are strictly necessary for its intended operation. All non-essential functions shall be disabled by default or removed. If the TOE includes optional functions, it shall provide an administrative interface to enable or disable them without compromising the Secure State of the TOE.
Srv7	Only services required to provide the TOE's functions may be present on the TOE. Any information related to the development shall be removed. <i>Application Note: This requirement does not apply to the debug version of the TOE.</i>
Srv8	The TOE shall regularly check for available updates from trustworthy sources. If the update is available, the TOE shall prompt users to install it.
Srv9	The TOE shall implement state-of-the-art rooting and jailbreaking detection and, upon detection of rooted or jailbroken operating system TOE shall prevent operation.
Srv10	The TOE shall enforce that the User operates the Wallet Instance under a standard user account on the mobile device with no administrative (root/superuser) privileges. The application shall run exclusively within the standard sandboxed execution context provided by the operating system (Android or iOS).
Srv11	TOE shall provide each application user with only one role. The users have access to the same application functionality and operate with the same privileges.
Srv12	The TOE shall associate security and privacy attributes with wallet requests, credentials, attestations, presentations, confirmations, logs and communication sessions, including at least purpose, recipient or requester identity, requested and released attribute set, consent state, trust or authorization status, assurance level, session or transaction identifiers and relevant channel context. The TOE shall preserve the integrity of those attributes and enforce access-control, disclosure, validation and logging decisions based on them.
Srv13	The TOE shall provide security-relevant events or status information needed for monitoring processes performed by the Wallet Provider. <i>Note: Such information includes security alerts, advisories and directives relevant to the TOE, its dependencies, cryptographic mechanisms, supported platforms and backend interfaces.</i>

6.4 Local storage

Strg1	The TOE shall implement measures against unauthorised access to the stored data.
Strg 2	The TOE shall implement measures to maintain the confidentiality and integrity of the stored data, in particular personal data.
Strg 3	The TOE shall prevent users from backing up stored app data. It should also be impossible to transfer application data directly between phones.

Strg 4	The TOE shall ensure that PID credentials and retrieved attestations of attributes (EEAs) containing personal data are encrypted.
--------	---

6.5 Network & Interfaces

Net1	Wallet Instance shall verify the authenticity, trustworthiness and authorisation of its communication partners.
Net2	Wallet Instance shall ensure the integrity of data and processes.
Net3	The Wallet Instance shall communicate with the WSCA via an end-to-end secure channel
Net4	The channel between the Wallet Instance and the WSCA shall ensure session binding and freshness.
Net5	The WSCA interface (SCI) shall be secured with TLSv1.3. The TLS connections shall utilize strong cipher suites.
Net6	The TOE shall establish and maintain secure communication channels using TLSv1.3 with all Wallet Provider backend services.
Net7	The PID Provider interface shall be secured with TLSv1.3.
Net8	The TOE shall establish and maintain secure communication channels using TLSv1.2 or TLSv1.3 with services exposed by: • EAA (Electronic Attestations of Attributes (EAA) Provider, • Relying Party (RP), • Trusted List or LoTE Providers. The TOE shall ensure that the TLS certificate used to establish a connection with EAA, RP, TL/LoTE services are issued to these entities

6.6 Documentation

6.6.1 User guidance documents

- 19 The Wallet Provider shall provide users with clear recommendations for the safe and secure operation of the TOE. Recommendations may be included in the documentation or provided via the dedicated service of the TOE. Requirements are provided on the table below.

SUG1	The TOE shall be accompanied by recommendations for users on the secure use of the application and its configuration. This includes, at a minimum: • Restrictions on the use of the TOE, • Guidelines and recommendations for the secure configuration, installation, setup, operation, and maintenance of the TOE for users, • Secure handling of authentication factors (e.g., PIN).
SUG 2	The TOE shall be accompanied by contact information for technical support and a procedure for reporting security issues.

SUG 3	The conditions and deadlines for revoking the TOE and the availability of the revocation service shall be communicated in clear language.
SUG 4	The user shall have access to information regarding mobile device models that are compatible with the TOE and the minimum version of the operating system required by the TOE.
SUG 5	The user shall be informed of any suspension or revocation of the TOE, including the reasons and consequences of the suspension, in clear and transparent language no later than 24 hours after the event.
SUG6	The TOE shall present clear security and privacy notices before granting access to or executing any wallet function that may disclose wallet data, change wallet state, use a device feature, initiate a presentation, signature or credential operation, or otherwise affect the user's security or privacy. The notice shall identify the purpose, requester or recipient where applicable, data categories, retention or logging consequences, and required user action, and shall remain available until the user acknowledges or cancels the operation.

6.6.2 Secure use of the TOE

- 20 The Wallet Provider is required to provide comprehensive guidance on the secure use of the TOE. This documentation covers installation, configuration, typical operation, and decommissioning. Additionally, the Wallet Provider shall provide the intended use case details and the specific operating environment.

21

SecDoc1	The Wallet Provider shall document the following functions available in the TOE: • TOE interfaces, • Users, • Services and associated functions, • Activation and deactivation status for the services.
SecDoc2	The Wallet Provider shall provide a Hardware Specification for the TOE. This specification shall describe all hardware components and features that are necessary for the Target of Evaluation (TOE) to perform its security functions correctly and securely within the defined hardware environment (e.g. Camera, NFC module).
SecDoc3	The Wallet Provider shall provide a Compatibility Description of the supported end devices. This description shall specify the hardware and software configurations for which the TOE is intended to operate and shall serve as the basis for assessing whether the TOE can maintain its security properties under the defined system environment conditions. Alternatively, the Wallet Provider shall specify the list of supported mobile devices.
SecDoc4	The Wallet Provider shall provide a Software Specification that clearly defines the supported operating systems for the mobile

	devices, including their minimum required versions. Furthermore, it shall specify any additional software components or libraries required for the TOE's execution due to dependencies. The specifications shall include the minimum versions, and where applicable, the maximum versions of all supported operating systems and additional software.
SecDoc5	Dependencies: The TOE's dependencies on the system environment in the form of software packages, interfaces, libraries, database connections, APIs, or other components shall be specified.

6.7 Additional security measures (Hardware Security)

HrdwSec1	The generation, storage, and processing of cryptographic secrets by the TOE shall be protected by a hardware-based key store (Android StrongBox/TEE, iOS Secure Enclave) on the mobile device using appropriate mechanisms. These mechanisms are required for the Wallet Instance to be installed and operated properly.
HrdwSec2	The TOE shall not store program data or application content unprotected in the end device's memory. If the TOE stores data on the end device, it must be encrypted unless it is already protected by other means, such as encryption by the WSCA. The key used to encrypt the data must be stored in the end device's key store.
HrdwSec3	The TOE shall implement appropriate measures for the confidential storage of personal data on end devices.

6.8 Cryptography

Crypto1	Cryptographic algorithms and 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.
Crypto2	The TOE should encrypt communication channels to external entities using state-of-the-art technology (TLS, as a minimum).
Crypto3	The TOE shall authenticate communication entities prior to the transmission of sensitive data.
Crypto4	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).
Crypto5	The key material stored by the Wallet Instance shall only be used after successful user authentication and authorization.
Crypto6	TOE shall implement measures to protect the key material it manages.

Crypto7	The TOE shall ensure that the key material is used only for its intended purpose.
Crypto8	The TOE shall establish and manage cryptographic keys used within the Wallet Instance and its interfaces under a defined lifecycle covering generation, derivation or establishment, distribution where applicable, storage, access control, use restrictions, rotation or replacement, revocation, and destruction.
Crypto9	The TOE shall validate public-key certificates, certificate chains, trust lists, trust anchors and certificate status information according to approved certificate policies and permitted key usage or purpose constraints before relying on a communication partner, issuer, relying party, WSCA/WSCD attestation or validation source.

Annex A. Assumptions regarding end user devices

A.1 Introduction

- 1 *NOTE 1: According to CIR (EU) 2024/2981, Annex IV, Point 4, end user devices are not provided by the wallet provider. From the evaluation perspective, all requirements shall be covered by assumptions.*
- 2 *NOTE 2: Further, according to this regulation: “For each assumption, the wallet solution shall include a mechanism to verify for every wallet unit that the underlying end user device satisfies the assumption. Such mechanisms shall be considered as security controls and covered by evaluation activities to demonstrate both their suitability and their effectiveness at the appropriate assurance level.” Therefore, relevant controls are outside the scope of WP-02-02 and are included in the process of Wallet Unit activation (see WP-03-01).*
- 3 *NOTE 3: “End user device” and “mobile device” are synonyms.*
- 4 Annex A outlines technical assumptions for mobile devices that the EUDI Wallet Instance mobile application will operate on.
- 5 The mobile device is a combination of a mobile platform, built-in OEM secure components and applications that make use of them.
- 6 The mobile platform encompasses hardware, mobile operating system, applications running on the mobile operating system, and supporting security features of the platform.
- 7 Secure component is a single or multi-application environment that makes use of secure hardware platforms and secure applications within the mobile device. Secure components are based on various technologies and can be divided into hardware-based secure components. Examples of secure components are:
- iOS Secure Enclave accompanied with API (Keychain Services),
 - hardware based Android StrongBox and software-based Trusted Execution Environment (TEE) accompanied by API (Android Keystore).

A.2 Mobile device assumptions

- 8 The mobile device supports user authentication at the “high” assurance level with respect to the use of remote WSCA, ensuring compliance with the criteria outlined in Commission Implementing Regulation (EU) 2015/1502.
- 9 For functions that are required for communications with the Wallet Provider backend services and WSCA, user credentials are generated, stored and used exclusively within a secure component of the mobile device.
- 10 The Wallet Instance supported mobile devices are restricted to:
- Android mobile phones running Android 10 or higher, equipped with Android Keystore, TEE or StrongBox.

- iOS mobile phones running iOS 18.0 or higher.
- 11 Older mobile devices, devices without required secure elements or configurations are not supported.

A.3 Mobile platform assumptions

- 12 The mobile platform enables integrity checks of the mobile operating system and the applications being executed. In particular:
- Android based mobile phones b is capable of passing Android Play Integrity checks
 - iOS based mobile phones is capable of passing Device Check App Attestation
- 13 The mobile device operating system is considered as uncompromised in accordance with the attestation information provided by the mobile platform based on the integrity checks. The mobile devices failing integrity checking are not supported.
- 14 The mobile device operating system provides security mechanisms such as app isolation and secure storage areas to protect sensitive data.
- 15 The mobile device operating system has security updates applied, trusted distribution channels used, device lock enabled, and untrusted side-loaded software, overlay/automation tools and management profiles restricted where these could interfere with wallet security.
- 16 The mobile platform provides mechanisms enabling applications to store or label sensitive data in such a way that it is adequately protected during operating system backup/migration.