EUROSMART
The Voice of the Digital Security Industry

Position paper on Security considerations for the European Digital Identity Wallet

Table of Contents

1. Introduction

The eIDAS Regulation (Regulation (EU) No 910/2014), put in force in 2014, was the first attempt to organize the recognition of electronic Identity of citizens in the Union. According to the Commission evaluation, the eIDAS Regulation has only partially fulfilled the objectives set out in 2014[1]. The substantial increase of identity thefts, IT system attacks and others raised the cost of identity fraud worldwide, namely across Europe with a total financial loss of €24 billion over two years and that reached over 20% of the population[2].

Acknowledging those threats and shortcomings of the original eIDAS Regulation[3], the European Commission proposed an amending regulation (Regulation (EU) 2024/1183) to eIDAS Regulation with the intent of offering to all natural and legal persons within the European Union a European Digital Identity and European Union Digital Identity Wallet (EUDIW) to access public and private services and when applicable usable offline.

In a previous white paper, Eurosmart depicted the risks faced by EU Member States and its citizens in a context where a low security was to be chosen for the EUDIW[4]. As a conclusion, Eurosmart made the following recommendation:

> ***"Private keys of EU citizens must be protected with Hardware meeting high level of assurance LoA High."***[5]

In this follow-up position paper, Eurosmart proposes to further investigate key security considerations for an overall secure deployment and implementation of the Digital Identity ecosystem in order to meet the security objectives set by the eIDAS2 Regulation.

Disclaimer: Figures 1 to 4 in this paper are sourced from the Architecture and Reference Framework (ARF) and are used solely for illustrative purposes, with full acknowledgment of their original source. All rights remain with their respective owners. Additionally, the terminology used in this position paper aligns with the terminology and definitions of the ARF.

2. Potential weaknesses in the EUDIW ecosystem

2.1. Several large-scale attacks on similar ecosystems demonstrate vulnerability

Over the recent years, there has been several instances of large-scale attacks with unmatched sophistication leading to identity theft in a large-scale perspective. It is crucial to analyze those attacks and implement adequate security measures to cover those aspects and ensure that the security of

[1] https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf
[2] https://www.wired.it/article/equalize-societa-dossier-pazzali-gallo/
[3] https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf
[4] https://www.eurosmart.com/low-security-in-the-european-digital-identity-wallet/
[5] Meeting LoA high for Hardware components and associated embedded Software requires a EUCC or SOG-IS Common Criteria security certification EAL4+ including AVA_VAN.5.

natural and legal persons' electronic identity is sustainably maintained. According to the literature on the topic, some recent examples of known hacks are:

- The Italian National Cybersecurity Agency that faced a sophisticated cybersecurity attack targeting key sectors in October 2024[6].
- Singpass, the Singapore wallet that has been hacked in January 2024[7].
- French telecom provider that experienced a cyberattack potentially compromising 19 million customers in October 2024[8].

Nevertheless, those recent hacks are only the tip of the iceberg, and while several key aspects can be depicted and learnt from to provide a sustainable security approach, it is important to consider that there might be further unreported security breaches.

While the amended eIDAS Regulation has generously acknowledged this aspect and planned for several key security requirements, such as ensuring a high level of security, ensuring the sole control of user, ensuring security notifications, and planning for a security certification scheme, it is crucial to take into account the following items to properly implement the relevant security measures.

2.2. Human factor as a critical aspect of security in the context of the EUDI wallet ecosystem

Human behavior and actions can significantly impact the effectiveness of security measures. Factors such as awareness, training, and behavior of users play a vital role in safeguarding sensitive information. There is also a need to ensure that individuals are educated on best security practices, such as using strong, unique passwords and recognizing phishing attempts.

Additionally, the product design shall also consider the security, as the user experience and interaction with a product needs to properly embed security aspects. A common example of it is the multi-factor authentication.

2.3. Secure operators for the EUDIW

In the European Union Digital Identity Wallet (EUDIW) ecosystem, secure stakeholder operators play a critical role in maintaining the integrity and security of digital identities. These operators, which include governmental bodies, private sector organizations, and technology providers, must adhere to stringent security standards to protect sensitive user data. Hence, implementing robust authentication mechanisms, encryption techniques, and continuous monitoring systems are essential to safeguard digital identities against unauthorized access and cyber threats. Furthermore, secure stakeholder operators must collaborate and share best practices to ensure a cohesive and resilient security framework. Regular security audits, compliance with regulations such

[6] https://www.euronews.com/next/2023/02/06/italian-authorities-issue-warning
[7] https://hackread.com/stolen-singaporean-identities-sold-on-dark-web/
[8] https://securityaffairs.com/170333/data-breach/free-suffered-a-cyber-attack.html

as the GDPR[9], and investment in advanced cybersecurity technologies are vital components of their responsibilities. By fostering a culture of security awareness and innovation, stakeholder operators can build and maintain the trust of users and relying parties, ensuring the successful implementation and adoption of the EUDI Wallet across Europe.

2.4. Inherent implementation weaknesses leave critical systems more vulnerable

The number of Common Vulnerabilities and Exposures (CVEs) has been rising significantly. In 2024, it was anticipated that the total count of published CVEs was to increase by 25%, reaching approximately 34,888 vulnerabilities[10]. This translated to around 2,900 new vulnerabilities each month[11].

This sharp increase highlights the growing challenge for cybersecurity professionals to manage and mitigate these vulnerabilities effectively. Organizations need to prioritize their patching efforts and enhance their security measures to protect against potential exploits.

Therefore, critical systems, which represent honeypot for attackers, are more vulnerable to attacks. Likewise, it is of prime importance to ensure that any critical systems are meeting the highest level of security and that they are reviewed thoroughly as part of their development and certification life cycle to avoid complaisance where a critical IT system would be partly assessed.

Digital Identity Systems, which are aiming to be the basis of the Digital Economy, and bringing global trust, will become the prime target for all attackers. With respect to its complexity, not only in terms of technology, but also in terms of operators, stakeholders and surface, will be exposed.

2.5. Adverse consequence of breaches for the electronic Digital Identity ecosystem

Breaches for the Digital Identity ecosystem are very detrimental to countries and their citizens. Breaches to the Digital Identity ecosystem have the potential to disclose the identity of all citizens leading to massive frauds and impersonation which would ultimately annihilate any Trust Services operations as a result of broken trust. One complexity is that the Digital Identity ecosystem shall be secure with high level of security from the start because a single breach would have severe future consequences. Once the system is hacked, it is very hard to ensure that the system can be trusted another time.

[9] While GDPR covers privacy preserving aspects, eIDAS2 covering identity will handle data associated to person which will therefore be subject to compliance with GDPR.
[10] This translates to around 2,900 new vulnerabilities each month
[11] https://securityaffairs.com/170333/data-breach/free-suffered-a-cyber-attack.html

2.6. Lack of clarity on the requirement of "Full Control" from the eIDAS Regulation opens the door to risks

In the eIDAS Regulation and corresponding Implementing Acts, the definition of "Full Control" is not clearly given. Additionally, some requirements also refer to "Sole Control". This, therefore, provides room for interpretations as the requirement is not unambiguously defined. Technical solutions may interpret and implement such vague requirement differently, resulting in a risk of disparate security approaches from the different wallet implementations. There is a risk that the "Full Control" requirement may only be partially met, for example, if control is delegated to IT systems.

In addition, due to the complexity of EUDI Wallet solution, there is a risk for the "Full Control" to be spread across several components making the objective of "Full Control" harder to implement. Not ensuring the "Full Control" would be detrimental to the adoption of the EUDI Wallet as it would break the User Trust.

3. Security considerations for the EUDI wallet components

In this chapter, we will review the different components and implementation of the EUDI Wallet as proposed by the ARF, while analyzing the level of trust they provide for the User Control.

3.1. The Architecture and Reference Framework

The Architecture and Reference Framework (ARF) is a live document available on GitHub[12] embracing the possible arrangements envisioned for the deployment of the European Union Digital Identity Wallet in consideration.

The figure below represents a Wallet Unit, which will be further analyzed within the next sub-chapters.

[12] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework

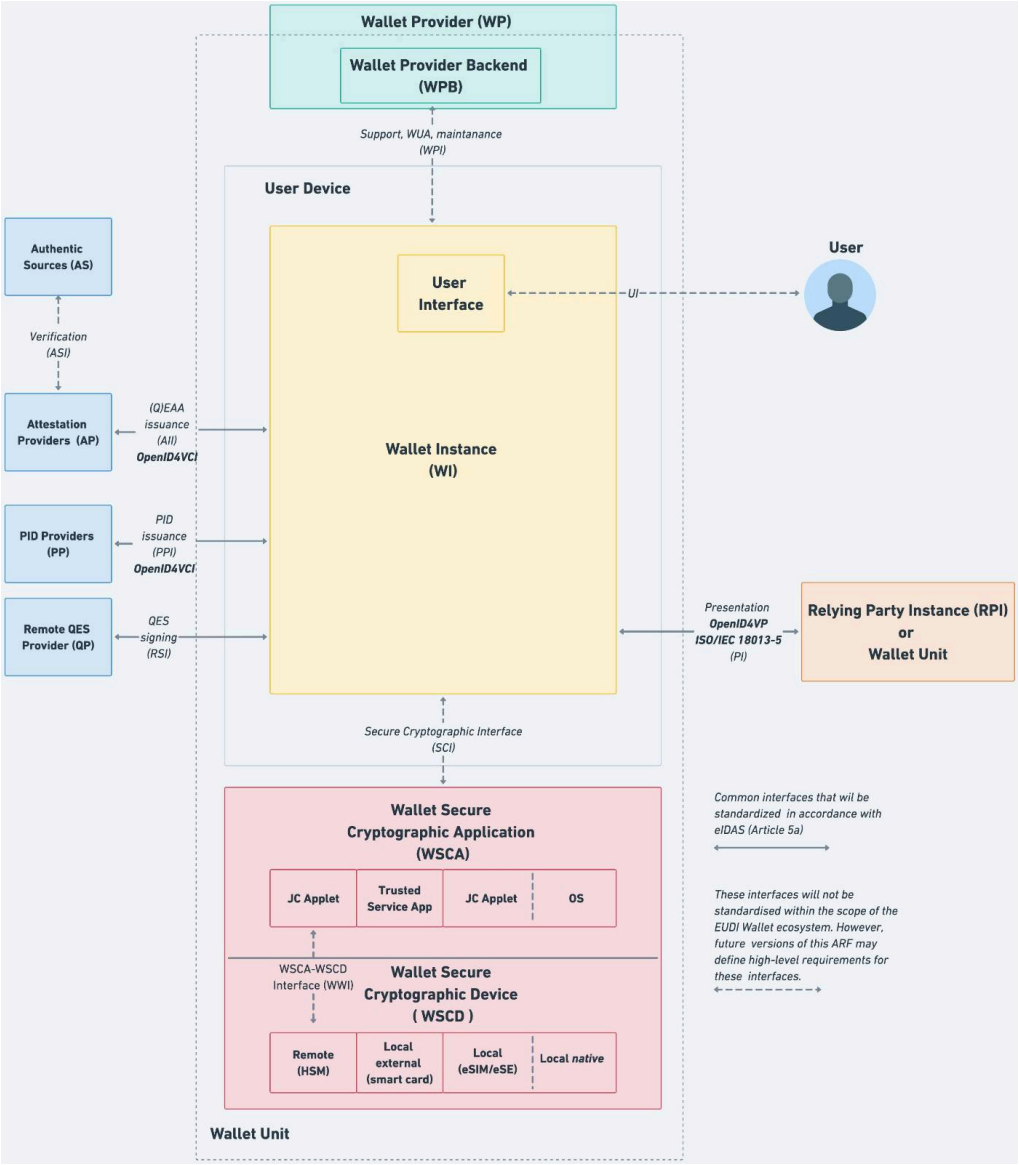

Figure 1: ARF EUDIW's architecture

There is an ongoing effort in CEN TC224 WG20 to outline a granular division of the components of the wallet to facilitate the definition of the evaluation scope. The two following projects are under preparation:

1. **Decomposition of the EUDI Wallet – part 1:** this targets a unified model for the wallet as seen from an end-user's perspective as to ensure that "the solution" can be validated/certified from a functional, legal and security point-of-view.

2. **Decomposition of the EUDI wallet – part 2:** this targets a unified model regarding the wallet provider (and its integration with the PID-issuer) as to ensure that those "supporting services" can also be validated/certified from a functional, legal and security point-of-view.

This effort has the following objectives/goals:

1. Provide a normalized model for the wallet solution and the wallet provider environment.

2. Provide clear guidance for the involved parties on “functions/features” to be certified, as well as for the applicable requirements.

3. Foster some consistency in the evaluation/certification of EUDI Wallet (environments).

3.2. Wallet Provider backend

Wallet Provider backend definition from ARF: “*The Wallet Provider backend offers Users support with their Wallet Units, performs essential maintenance, and issues Wallet Unit Attestations through the Wallet Provider Interface (WPI).”*

Security consideration for the Wallet Provider backend:

- The Wallet Provider backend shall be operated in a secure environment, under the control of relevant operators that are trusted.

- The IT system shall be regularly monitored and regularly updated to maintain an up-to-date software version with the latest security patch applied.

- Eurosmart recommends evaluating the software that will be communicating with the Wallet to ensure it fits well within the security approach of the EUDIW.

3.3. User Device (UD)

User Device definition from ARF: *“A User Device comprises the hardware, operating system, and software environment required to host and execute the Wallet Instance. The minimum hardware and software requirements for the User device will be determined by the Wallet Provider.”*

The UD is hosting the Wallet Instance (WI) which is an app or application installed on a User Device, and that is part of an EUDI Wallet Solution that belongs to and is controlled by a User. This component implements the core business logic and interfaces. In particular, the Wallet Instance directly interacts with the WSCA/WSCD to securely manage cryptographic assets and execute cryptographic functions, ensuring a high level of assurance for authentication.

Security consideration for the User Device:

- To provide additional trust within the User Device, as being the platform hosting the EUDI Wallet, it is recommended to have an evaluation of the User Device covering the overall security, for instance, MDSCert assessment methodology and the consumer Mobile Device PP [TS103732] cover threats related to the User Device.

3.4. The Wallet Secure Cryptographic Device (WSCD)

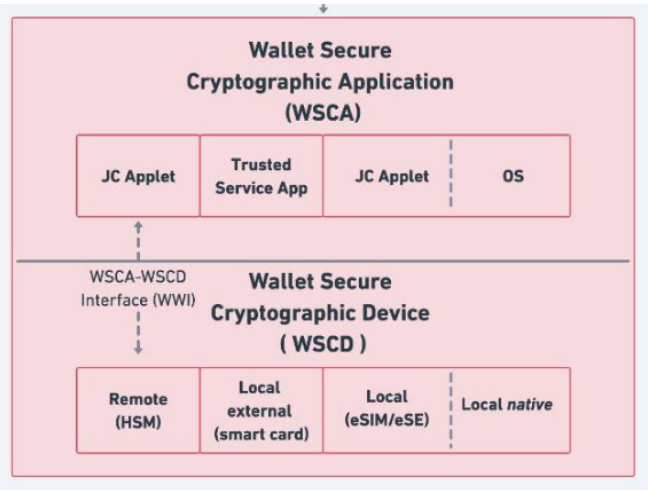

Figure 2: Extract of ARF EUDI Wallet solution reference architecture WSCD

Wallet Secure Cryptographic Device definition from ARF: *"Tamper-resistant device that provides an environment that is linked to and used by the wallet secure cryptographic application to protect critical assets and to securely execute cryptographic functions. This includes a keystore, but also the environment where the security-critical functions are executed. The WSCD is tamper-proof and duplication-proof. One WSCD may be a part of multiple Wallet Units, e.g. in case of a remote HSM. The WSCD consists of two parts: the WSCD hardware covers the hardware issued by the WSCD vendor and the WSCD firmware covers security-related software, such as an operating system and cryptographic libraries provided by the WSCD vendor. Figure 2 shows four different possible security architectures for the WSCD (for more details see Section 4.5):*

- *a remote WSCD, a remote device, such as a Hardware Security Module (HSM), accessed over a network.*
- *a local external WSCD, an external device, such as a smart card issued to the User specifically for this purpose,*
- *a local internal WSCD, a component within the User device, such as a SIM, e-SIM, or embedded Secure Element,*
- *a local native WSCD, a component embedded in the User device and accessed via an API provided by the operating system."*

As presented in the ARF, the WSCD has several possible implementations, which are not equivalent in terms of security, therefore presenting a risk harmonization of solution with the potential to hinder the trust in Digital Identity Systems that would become an obstacle to a wide adoption.

The following sub-chapters provide an analysis of each deployment and draw some security considerations.

3.4.1. Remote WSCD

Form factor addressed: HSM, cloud HSM, SE cluster/cluster of SE.

HSM technology in the context of Digital Identity is certified EAL4+ with AVA_VAN.5. This technology provides secure operation for sensitive assets but usually requires a secure operational environment for access to the device and protection against local attacks as resistance against attackers with high attack potential is not always ensured.

3.4.2. Local internal WSCD

Form factor addressed: eSIM/eSE[13], SD/microSD[14], SE[15], ...

SE technology certified EAL4+ with ALC_DVS.2 & AVA_VAN.5 is a tamper proof safe technology widely adopted to protect sensitive data. It is certified to the highest level of security to protect secrets (private keys) against disclosure, and is resistant against leakage, penetration, side-channel, fault and implementation attacks due to thorough review of source code, documentation design and heavy penetration testing by experts.

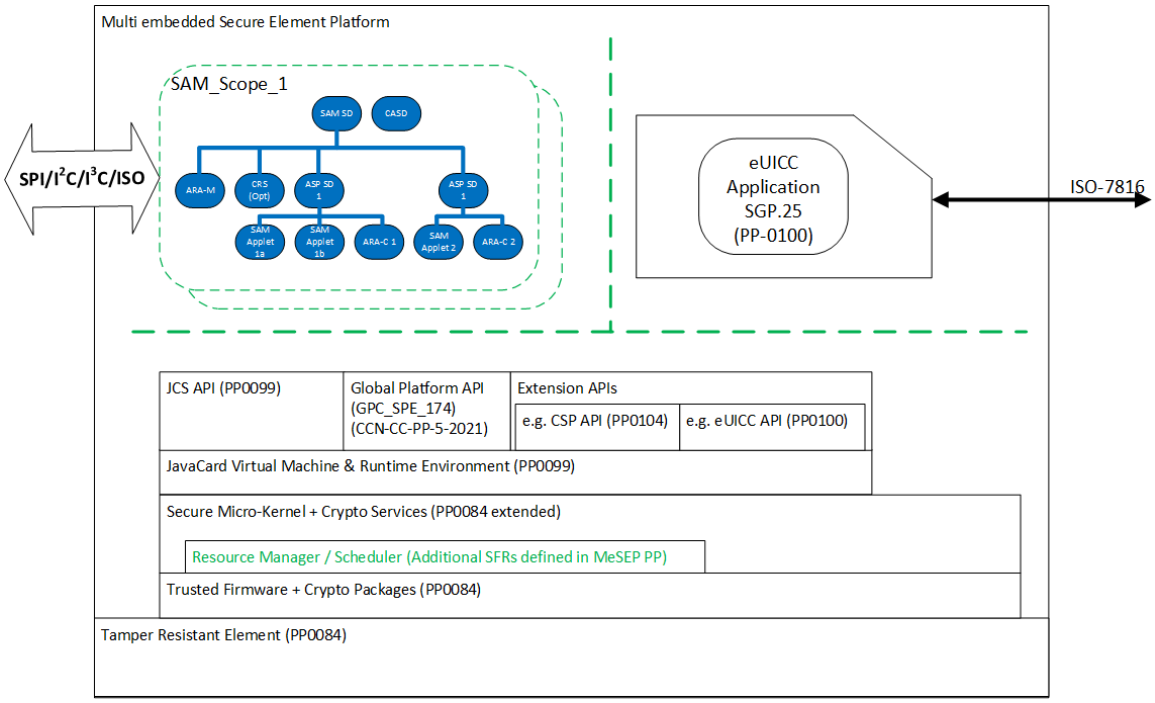

Figure 3: Local WSCD eSIM/eSE security certification layer overview

[13] eSIM/eSE = embedded SIM / embedded Secure Element.
[14] SD/microSD = Secure Digital cards.
[15] SE = Secure Element.

In terms of reach of Secure Elements, all smartphones shipped in Europe feature at least one eSE, UICC or eUICC.

The below data shows the already significant penetration of eSE and eUICC technologies, as well as the expected near-term momentum:

448.4 million Inhabitants in the European Union[16]	**Over 50%** Of smartphones to have embedded hardware security by 2025[17]	**Close to half a billion** eSIM-capable devices were shipped worldwide in 2023[18]
Over 9 billion eSIM-capable devices to be shipped worldwide by 2030[19]	**Nearly 70%** Proportion of eSIM-capable cellular devices by 2030	**474.2 million** Projected eSIM smartphone shipments in Europe by 2028[20]

Table 1: eSIM/eSE usage

3.4.3. Local external WSCD

Example: European Passport, European Identity Card, ...

SE technology is a safe and reliable technology that is used for the protection of citizens' ID across Europe and the world. That technology has been in place for many years and has not suffered any major threats. NFC can be used to establish a secure communication between the WSCD and the user device.

3.4.4. Local native WSCD

Example: Software executed in main processor environment (note: the main processor is not certified CC EAL4+).

Local native solutions are currently not meeting the highest level of security by themselves. There is an existing TEE protection profile PP-GPD_SPE_021 with AVA_VAN.2 (or AVA_VAN_AP.3, a custom designed level) but does not contain the physical attacks. Spectrum and meltdown threats are for example potential risks.

[16] https://european-union.europa.eu/principles-countries-history
[17] https://www.counterpointresearch.com/insights/podcast-50-percent-smartphones-embedded-hardware-security-2025/
[18] https://www.counterpointresearch.com/insights/
[19] https://www.counterpointresearch.com/insights/over-9-billion-by-2030/
[20] https://www.abiresearch.com/news-resources/chart-data/esim-market/

Remarks:

- While the frontier between WSCA and WSCD in the context of local native solution is not clear, they are subject to the same high level security level requirement.
- When such Local native WSCD rely on a Secure Element composed of a full native stack, the security level high compliance might be possible. However, it would need to be entirely demonstrated through security certification.

3.4.5. Security consideration for the WSCD

The table below provides an overview of the applicable protection profiles, and their main characteristics, to be used to adequately demonstrate the security of WSCD.

	Remote (HSM)	Local external (smart card)	Local (eSIM/eSE)	Local native
PP reference	PP--419-221-5	PP-0084 ; PP-0099 Note[21]	PP-0084 ; PP-0099 PP-GPC_SPE_174 ; PP-SAM scope[22] ; PP-0104 ; PP CSPv2[23]	None existing
Security Certification based on PP security level high	EAL4+ with AVA_VAN.5	EAL4+ with AVA_VAN.5 & ALC_DVS.2	EAL4+ with AVA_VAN.5 & ALC_DVS.2	None
Resistance to fault attacks / Side-Channel attacks	No (but can be added in the product[24])	Yes (included in the PP)	Yes (included in the PP)	None
Requirement to setup a secure operating environment for the	Yes, currently required by the PP[25] but a product	Not required, the TOE is self-	Not required, the TOE is self-	None

[21] The existing Protection Profile for the evaluation of the authentication, credentials, communication and interactions with the wallet instance / user device is not covered and will be inherited from the definition of the functional specifications / split of functionality between the mobile phone and external WSCD.
[22] The PP SAM-scope is currently under development at Global Platform.
[23] PP CSP v2 is currently under development at GlobalPlatform.
[24] The current HSM PP HSM is not including side-channel or fault attacks, nevertheless products can implement security features protecting against those attacks as part of the security certification. Therefore, Eurosmart recommends including those type of attacks protection within the scope of security certification.
[25] Note that the PP can be subject to evolution and TOE self-protection can be added within the scope, removing the assumption on the secure operating environment.

operation	may not require a secure operating environment	protected	protected	
User control enforcement	No, not included	Yes	Yes	No, not included
Single Point Of Failure (SPOF)[26]	Yes	No	No	No
Offline support	No	Yes	Yes	Yes

Table 2: WSCD security considerations

3.5. The Wallet Secure Cryptographic Application (WSCA)

Wallet Secure Cryptographic Application definition from ARF: *"an application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the Wallet Secure Cryptographic Device. The WSCA interfaces directly with the Wallet Instance."*

The WSCA is an application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the wallet secure cryptographic device.

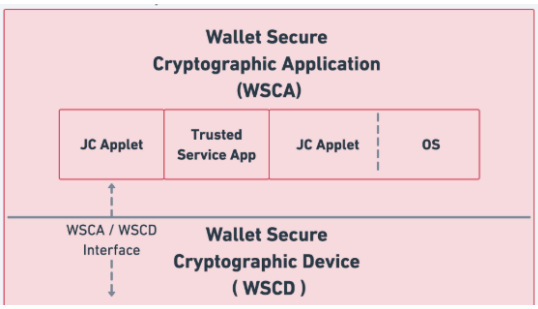

Figure 4: Extract of ARF EUDI wallet solution reference architecture

Security consideration for the WSCA:

- The CEN TC224 WG17 working group has planned to create a Protection Profile to cover the different security aspects of the WSCA and underlying WSCD dependencies. The work should cover all the possible WSCD implementation.

[26] Denial of service, risk of processing bottle neck, network disruption, issue in the case of a security flow/malfunction of a central point.

4. Conclusion on security considerations

4.1. Meeting the objectives enshrined in the amended eIDAS Regulation for the EUDI Wallet as outlined in Article 5a from the WSCD perspective

Among the objectives identified in the amended eIDAS Regulation, Article 5a contains overall security objectives that need to be met by the EUDIW.

The table below presents an extract of the objectives which are relevant from a security standpoint and shows how the EUDIW WSCDs component can help meeting them depending on their implementations.

Requirement	Remote (HSM)	Local external (smart card)	Local (eSIM/eSE)	Local native
Article 5a.1 "For the purpose of ensuring that all natural and legal persons have secure, trusted and seamless cross-border access to public and private services, while **having full control over their data**, each MS shall provide at least one EUDIW within 24 months (...)"	See NOTE 1	Yes	Yes	See NOTE 2
Article 5a.4 "EUDIW shall enable the user (...) to **a)** securely request, obtain, select, combine, store, delete, share and present **under the sole control of the user**, person identification data and, where applicable, in combination with electronic attestations of attributes, to **authenticate to relying parties online and, where appropriate, in offline mode, in order to access public and private services,** while ensuring that selective disclosure of data is possible; (...)"	See NOTE 1	Yes	Yes	See NOTE 2
Article 5a.14 "**Users shall have full control of the use of and of the data** in their European Digital Identity Wallet. (...)"	See NOTE 1	Yes	Yes	See NOTE 2
Article 5a.16 "The technical framework of the European Digital Identity Wallet shall: (...)	See NOTE 3	See NOTE 3	See NOTE 3	See NOTE 3

b) **enable privacy preserving techniques which ensure unlikability**, where the attestation of attributes does not require the identification of the user."				

Table 3: Mapping of WSCD implementations with the key objectives enshrined in the amended eIDAS regulation

NOTE 1: Remarks on Remote HSM solution

- Remote HSM does not allow offline connectivity. Nevertheless, the tokenization technology might offer some offline connectivity support (this is not standardized yet).
- To achieve full control over the data by the User/EUDIW with a Remote HSM solution, there are possibilities with a combination of technologies including software control, system design and relevant audit to ensure correct implementation.

NOTE 2: Remarks on local native solution

- Local Native solution cannot meet the security level high.
- Currently, the local native solution lacks standardization support and there is a variety of possible implementations.

NOTE 3: Remarks on privacy preserving techniques

- The standardization approach for privacy-preserving techniques is currently ongoing and there is not yet proven secure implementation.
- Note that currently, the proof of such cryptographic protocols is not globally recognized and adopted by Security Agencies.

4.2. Clear definition for "Full Control" to be included in the relevant Implementing Acts on "Integrity and Core requirements" and on "Certification"

Eurosmart calls for a proper definition of "Full Control" and "Sole Control" within eIDAS and proposes the following to be included in the Implementing Act on "Integrity and Core requirements"[27].

[27] COMMISSION IMPLEMENTING REGULATION (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets.

Eurosmart definition of "Full control":

"Full Control" designates the control by a natural or legal person over the operations it is exclusively entitled to trigger and carry out, meaning these operations are not available to any other natural or legal persons or IT systems. In particular, a "Full Control" is characterized by a technical impossibility of the solutions or systems used by the natural or legal person to exercise its control to allow a third party to circumvent the control of that natural or legal person.

Eurosmart definition of "Sole control":

"Sole Control" designates the exclusive authority of a natural or legal person over specific operations or decisions, ensuring that no other entity, including third parties or systems, shares or participates in this authority. It emphasizes exclusivity in decision-making and the execution of operations, without necessarily requiring a technical impossibility for others to circumvent this control. "Sole Control" relies on an absolute absence of shared or delegated authority, maintaining individual or organizational sovereignty over the actions in question.

Key differences between "Full control" and "Sole Control":

- **Full Control** focuses on the technical impossibility for others to interfere or circumvent the control, providing robust safeguards.
- **Sole Control** highlights the absence of shared authority, ensuring exclusivity but without a mandatory technical guarantee preventing circumvention.

In addition, the compliance of the Wallet with the aforementioned definition of "Full Control" and "Sole Control" shall be covered by the certification process as defined in the corresponding Implementing Act on "certification of European Digital Identity Wallets"[28].

[28] COMMISSION IMPLEMENTING REGULATION (EU) 2024/2981 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com