GlobalPlatform Position Paper

Securing the European Digital Identity Wallets

Meeting the challenges of technology, sovereignty, and certification

February 2025

GlobalPlatform eID Wallet Task Force

Contents

1 Executive Summary

Making a digital identity wallet available to every citizen is one of the European Union's key near-term objectives. By December 2026, each of the 27 member states must provide a digital identity wallet that is compliant with the European Digital Identity Regulation, known as eIDAS 2.0.

Member states face the twin challenges of ensuring a high security level for their wallet solution, which is crucial for establishing trust for all stakeholders, while offering an accessible and seamless user experience for citizens. Additionally, each member state will need to operate a transitional national security certification scheme to validate that their wallet meets the security requirements laid out in the regulation.

Secure elements (SE) are regarded as the best technology to help member states achieve the highest levels of security and usability when deploying their wallets to smartphones. Importantly, SEs are already standardized by GlobalPlatform and certified to stringent functional and security requirements. They provide a route to market via a widely-adopted technology and with minimal risk, enabling convenient and secure EUDI implementations that also support offline mode use cases when there is no active network connection.

SEs are widespread in smartphones and will very soon be ubiquitous. While wallet security with SEs can be achieved on today's smartphones, work is in progress to optimize scalability. This is because SEs are currently controlled by smartphone manufacturers or mobile network operators, meaning third parties, like member states, cannot independently access or modify them, limiting scalability and ease use for securing EUDIWs.

The device security industry is therefore collaborating to enable the universal and independent use of SEs for member states to protect their wallets – and citizens' identities – with the highest level of security. Industry association GlobalPlatform and its members are leading this initiative, in collaboration with major security stakeholders.

This position paper presents two standardized and interoperable frameworks from GlobalPlatform that can solve these challenges:

- Secured Applications for Mobile (SAM) – to enable member states to deploy and manage applications on embedded SE and embedded SIM across devices independently of smartphone manufacturers or mobile network operators.

- Cryptographic Service Provider (CSP) – to streamline the certification process for member states by allowing a single applet certificate for all smartphone and SE platforms supporting this technology, reducing time and costs associated with security assessment.

SAM and CSP build upon SE technology already present in billions of smartphones, allowing the EU Digital Identity Wallet (EUDIW) to take advantage of proven security infrastructure, accelerating adoption and reducing implementation costs.

They are also the foundations for the EU to establish a European authority to act as a sovereign gatekeeper for member states' access to a dedicated protected environment within SEs. This sovereign access is vital for ensuring security, interoperability, access, trust, and control over critical security components of EUDIWs.

To harness the extensive benefits that SEs can bring to EUDIW implementations, the following steps should be taken now by the key stakeholders:

- The EU Commission and regulators should establish an authority to manage access to SEs in devices, enabling member states to secure their EUDIWs.
- Member states should collaborate in pilot programs with industry partners to develop SAM/CSP compatible wallet solutions and advocate adoption in EU-level discussions and working groups.
- Wallet developers should integrate the SAM and CSP frameworks from an early stage of development and engage with GlobalPlatform to ensure successful implementations.
- Large Scale Pilots should incorporate SAM/CSP in their programs.
- Smartphone manufacturers should provide the necessary components to facilitate SAM and CSP integration.

Until SAM and CSP certified SEs are deployed, 'SAM-Ready' technology is already widely available and can provide a secure environment to host EUDIW applications that is functionally equivalent to the SAM technology noted above. Member states and large-scale pilots can immediately host EUDI wallets on SAM-Ready SEs through agreements with smartphone manufacturers, mobile network operators, SE manufacturers, or via intermediaries. This will allow them to easily and independently migrate their implementation to all smartphones as SAM and CSP eSIMs are readily available.

Stakeholders can use section three of this paper to understand the security, reach, scalability, convenience, sovereignty and cost benefits that SEs can bring to EUDIW implementations. Additionally, sections four and five set out the steps being taken to simplify the sovereign access to SEs for member states, and support the certification schemes they will need to deliver.

By taking these actions, each stakeholder group can make a significant contribution to ensure a secure, interoperable, and widely adopted digital identity solution across the European Union.

At the same time, stakeholders can benefit from a homogenous and widespread mobile ecosystem that supports secure digital identities on all devices. Smartphone vendors will benefit from an interoperable standard that supports new secure and innovative use cases, such as the EUDIW, and simplifies the deployment of these use cases at scale. Most importantly, EU citizens will be able to quickly, easily and securely authenticate or identify themselves when making online transactions or accessing government services.

2 INTRODUCTION

A central goal of the European Union 2030 Decade policy is to provide a digital identity to every citizen. Regulation 2024/1183[1] (also called eIDAS 2.0) establishes the European Digital Identity (EUDI) Framework[2] with European Digital Identity Wallets (EUDIW) at its core.

By December 2026, each of the 27 EU member states must provide[3] at least one EUDI wallet, which must be accepted by public, and selected private, services by December 2027.

The process of drafting the regulation recognized that security is key to establishing trust in EUDIWs. This is to enable successful deployments at scale and to achieve solutions that can be certified as resistant against attackers with a high attack potential.

The European Network Information Security Agency (ENISA) has a mandate to define and launch a security certification scheme for EUDI wallets that applies to the whole EU, but this will not be in place by December 2026. Implementing Act 2024/2981[4] sets the rules for the certification of EUDI Wallets using individual member states' national certification schemes, including requirements on how to achieve certification up to a high level of assurance (LoA). Once ENISA's wallet certification scheme is launched, there will be a transitional period to migrate wallet solutions from the national schemes to the pan-European scheme.

EU member states that want to offer a successful wallet solution by the end of 2026 are facing multiple challenges. Among these, GlobalPlatform has identified three main security challenges:

- **Ensuring security with the right technology** – Member states will need to create or select an EUDI wallet with a high level of security and make it available to a maximum number of their citizens without sacrificing user convenience.

- **Setting up the governance of wallet security** – Member states will need to define and enforce rules and operations for a secure management of the wallet's technology parts (e. g. hardware devices, software, sensitive data, PKI including setting up an EU Certificate Authority).

- **Establishing the transitional security certification** – Member states will have to create and operate a transitional national certification scheme to certify their wallet until the pan-European scheme is in place.

To support both the transitional phase and the later pan-European approach, this position paper explains technologies, certifications, and approaches to governance available to member states that will help them solve the above security challenges.

[1] https://eur-lex.europa.eu/eli/reg/2024/1183/oj

[2] The regulation entered into force in May 2024, and is completed by three batches of topic-specific Implementing Acts that detail the requirements of the regulation. The first batch was adopted in November 2024, the remaining two are planned for the first and second quarters of 2025.

[3] To 'provide' a wallet member states can issue, mandate or recognize a wallet.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402981

3 SOLVING THE SECURITY TECHNOLOGY CHALLENGE

This section describes how Secure Elements (SE) can be used to implement the EUDIW secure components identified in the Architecture Reference Framework[5] (ARF) and in the Certification Implementing Act 2024/2981: the Wallet Secure Cryptographic Device (WSCD) and Application (WSCA).

Key requirements for a WSCD are outlined in these documents and SEs are the best technology to meet these in the long-term.

3.1 The Wallet Security Architecture: WSCD and WSCA

The ARF identifies two key components of a secure EUDIW:

- **The Wallet Secure Cryptographic Device (WSCD)** is a trusted hardware component that provides storage for cryptographic assets (such as digital key material) and an environment for executing security-critical functions. A WSCD must be resistant to tampering and duplication and can be further sub-divided into two parts: the WSCD hardware – which covers the hardware issued by the WSCD vendor – and the WSCD firmware – which covers security-related software such as the operating system of the WSCD and cryptographic libraries provided by the WSCD vendor.
- **The Wallet Secure Cryptographic Application (WSCA)** is application software supporting the above-mentioned security-critical functions. Version 1.5 (February 2025) of the ARF states that a WSCA must run securely on a WSCD.

The Implementing Act on wallet certification details general wallet certification requirements that will have to be met by member state wallets. These are discussed in detail in section five of the paper.

While neither the Implementing Act nor the ARF mandate an explicit security architecture, the ARF identifies potential options for the WSCD (and therefore for the WSCA):

- One or more **remote WSCDs** accessible to the wallet via a network.
- A **local external WSCD** accessed from the end user’s device through a proximity connection such as near field communication (NFC).
- A **local internal WSCD**, a component integrated in an end user’s device, such as a SIM, eSIM or embedded SE.
- A **local native WSCD**, a local WSCD only accessible via a high-level API provided by the operating system of the smartphone[6].
- A **hybrid solution** with two or more of the above options.

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

[6] A local native WSCD is integrated into the user’s device and the API to access the WSCD is included in the operating system of the device. Therefore, no separate WSCA is necessary. Alternatively, the API offered by the OS may be viewed as the WSCA.

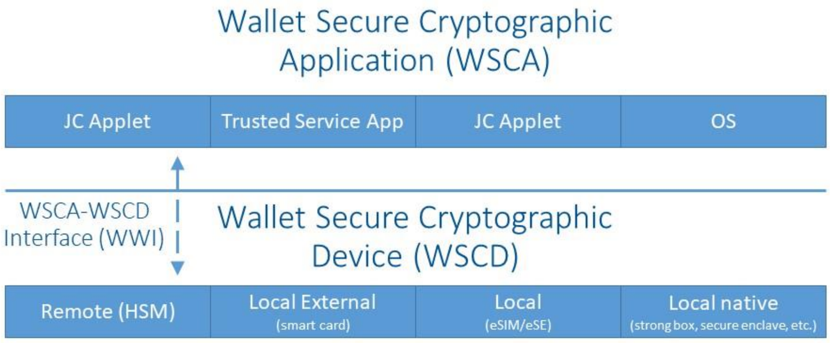
Wallet Secure Cryptographic Application (WSCA)
JC Applet
Trusted Service App
JC Applet
OS
WSCA-WSCD Interface (WWI)
Wallet Secure Cryptographic Device (WSCD)
Remote (HSM)
Local External (smart card)
Local (eSIM/eSE)
Local native (strong box, secure enclave, etc.)

Figure 1: Wallet Secure Cryptographic Devices and Applications - Extracted from the ARF Version 1.5[7]

The suitability of a WSCD technology can be determined by how well the following required properties are met:

- **Convenience:** minimum friction for wallet users.
- **Reach:** maximizing the number of citizens that can use a wallet.[8]
- **Security:** meeting the security and certification requirements for a high LoA.
- **Scalability:** minimizing the complexity to deploy the wallet on a diverse and ever-changing base of devices (especially smartphones).
- **Sovereignty:** minimizing the dependency of member states on third parties such as device or component manufacturers, or service providers, to access the WSCD.
- **Offline Use:** meeting the requirements for proximity use cases without requiring active wide-area network connectivity.
- **Maturity:** minimizing the deployment, and operational costs and risks, of wallet security through established solutions with advanced systems for managing risks and detecting fraud.

The following table maps the ARF WSCD architectures to some of the currently available technologies:

ARF WSCD architecture	Deployment technology
Local internal WSCD	Embedded Secure Element (eSE)[9]
	Embedded or removable SIM (eUICC or UICC)
Local external WSCD	External Secure Element (e.g. Smartcard or token)
Local native WSCD	eSE or eSIM accessed by an API provided by the operating system
Remote WSCD	Remote Secure Element
	Remote Hardware Security Module (HSM)
Hybrid	*Any combination of the above*

[7] Adapted from the European Digital Identity Wallet Architecture and Reference Framework: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework, licensed under CC by 4.0 [http://creativecommons.org/licenses/by/4.0/].

[8] The EU's goal is to have approximately 80 percent of European citizens using an EUDI Wallet to manage identity documents, access services, and make secure digital payments by the end of the decade.

[9] Including eSE through local native services or native wallet.

The below sections will describe these technologies and the extent to which they meet these requirements. No single technology currently maximizes all requirements, and EUDI Wallets will most likely be based on hybrid WSCD technologies with a mix evolving over time.

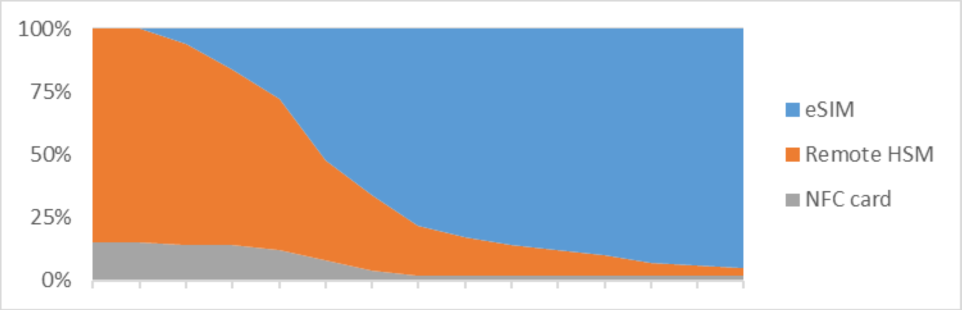

Figure 2: Example of a mix of WSCD technologies for a EUDIW evolving over time.

Figure 2 shows an example hybrid implementation of a WSCD over time, where an EUDIW uses both an external SE such as a chip-based NFC-enabled national identity card, a remote HSM or an eSIM. The NFC ID card can cover use cases that require a high LoA at the cost of some convenience, as the citizen would need to find and tap their card on their device. Remote HSM, conversely, can cover use cases that require less stringent security. Over time, as their reach is rapidly increasing, eSIM can replace both the external NFC cards and remote-HSM, providing the optimal balance of convenience and security.

3.2 Secure Elements

SE technology is a mature proven solution available in many devices, that already provides security to mass-market applications, most prominently mobile network subscriptions and contactless payments.

At its core, an SE is a tamper-resistant platform capable of securely hosting applications and their confidential and cryptographic data. As such SEs are well suited to function as an EUDIW WSCD. Most SEs in use include an application runtime environment (typically Java Card) and can execute WSCAs securely as SE applets.

SE technologies are standardized by GlobalPlatform, a standards organization, and more than 62 billion GlobalPlatform SEs have been issued to-date[10]. Most smartphones embed GlobalPlatform compliant SEs, as well as implementing GlobalPlatform specifications to securely access and manage them.

Today's smartphones (as the most obvious system to implement an EUDIW) support at least one of the following form factors of GlobalPlatform local SEs:

- **Removable Subscriber Identity Module (SIM), also called Universal Integrated Circuit Card (UICC) or pluggable SIM cards** – these SEs are owned by the MNOs and implement the SIM application standardized by the the 3rd Generation Partnership Project (3GPP).

- **Embedded SIM (eSIM), also called embedded UICC (eUICC)** – these components are owned by the smartphone manufacturers and implement the same 3GPP specifications as removable SIMs, as well as the Global System for Mobile Communications Association (GSMA) Remote Subscription Provisioning (RSP)

[10] https://globalplatform.org/wp-content/uploads/2024/08/GlobalPlatform_AnnualReport2024_R3.pdf

framework, which allows MNOs worldwide to independently install and administrate their network connectivity profiles using the same interoperable chips and without the need for removable parts[11].

- **Embedded Secure Element (eSE)** – these SEs are owned and managed by the smartphone manufacturers and are used for security-critical use cases such as contactless payments, ticketing, and virtual car keys.

For various reasons, including security, SIM, eSIM and eSEs in smartphones cannot directly be accessed and used by everybody to deploy applets and services. Their use is governed by established and evolving management schemes, and section four *Solving The Sovereignty Challenge*, describes the rules and governance needed to host a WSCD on an SE, and how GlobalPlatform's Secured Applications for Mobile (SAM) specification can solve the scalability and sovereignty challenges.

3.3 Secure Elements and WSCD key requirements

This section describes how SEs are a perfect fit for meeting the key WSCD requirements identified previously.

This section addresses each WSCD requirement in turn:

- **Convenience:** eSEs, UICCs and eUICCs bring a seamless level of convenience for device users. As everything can be downloaded, activated, and processed within the citizen's smartphone, there is no need for them to locate and use additional external devices, such as application specific cards or tokens. This optimal level of convenience explains the huge success of use cases such as mobile contactless payments and ticketing, in addition to growing use cases like mobile virtual car keys.

- **Reach:** all smartphones shipped in Europe feature at least one eSE, SIM or eSIM. The momentum for eSIM shows a tremendous penetration rate in the short term, as summarized in the table below:

Close to half a billion eSIM-capable devices were shipped worldwide in 2023[12]	**Over 9 billion** eSIM-capable devices to be shipped worldwide by 2030[13]	**Nearly 70%** Proportion of eSIM-capable cellular devices by 2030[10]	**474.2 million** Projected eSIM smartphone shipments in Europe by 2028[14] for an EU population of **448.4 million**[15]

Additionally, an increasing share of smartphones now feature both an eSIM and an eSE. Both features are sometimes combined within a single chip.

[11] Removable UICCs can also support GSMA RSP.

[12] https://www.counterpointresearch.com/insights/gd-thales-idemia-pacesetters-in-2023-esim-enablement-rankings/

[13] https://www.counterpointresearch.com/insights/over-9-billion-esim-capable-devices-to-be-shipped-by-2030/

[14] https://www.abiresearch.com/news-resources/chart-data/esim-market/

[15] https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/life-eu_en#:~:text=The%20EU%20covers%20over%204%20million%20km%C2%B2%20and%20has%20448.4%20million%20inhabitants

- **Security:** SE security is usually proven through independent security certification overseen by a certification scheme and following a certification methodology. The wallet certification Implementing Act requires that the WSCD and WSCA are certified using high standards of certification such as Common Criteria, to a level equivalent to EAL4 and an advanced methodical vulnerability analysis, comparable to AVA_VAN.5, which certifies for an "*advanced methodical vulnerability analysis and resistance against a high attack potential*".

- **Offline Use:** as SEs host data and applications locally and securely, they can also enable offline use cases where the user's device does not have an active network connection. Proximity use cases are widely used in segments such as contactless payment or ticketing and are mandated in the eIDAS 2.0 regulation[16], and possibly other use cases, such as the upcoming Central Bank Digital Currency (CBDC; in the EU also known as "Digital Euro").

- **Maturity:** mass-market applications have been deployed to SEs for some time. This means the corresponding risks, certification and costs are already well optimized, especially on mass-market consumer devices. The associated server technology for remote SE management has also reached maturity, managing major use cases such as contactless smartphone payments and mass-transit ticketing, in addition to network connectivity with eSIM. This minimizes the risks of secure wallet deployment compared to new technologies. Additionally, as most smartphones already embed an SE, the cost to use those SEs for the new EUDIW use case is minimal.

- **Scalability and sovereignty:** despite the high, and ever-growing, penetration rate of eSE and eSIM technologies, these SE are owned and managed by smartphone manufacturers[17] and currently cannot be used as the WSCD for EUDIW implementations without business agreements with the smartphone manufacturers. Although this is possible, it limits the scalability for the time being.

This clearly highlights the market need for the initiatives that are in progress within GlobalPlatform, with the objective to create a standardized, universal approach to using SEs for wallet security across all smartphones.

Section four *Solving the Sovereignty Challenge***Error! Reference source not found.**, explains how SAM is solving the scalability and sovereignty challenges, and section five, *Solving the Certification Challenge*, explains how the CSP technical specification can lower the complexity of certifying the WSCA .

3.4 Alternate technologies for WSCD

This section addresses alternate technologies identified in the ARF to implement the WSCD, and how they meet key WSCD requirements.

[16] Article 5 of the eIDAS regulation

[17] The GMSA RSP Specification allows MNOs to manage their own connectivity network profiles independently of the smartphone manufacturers.

3.4.1 External Secure Element as Local External WSCD

Today, most high-end smartphones are NFC-enabled to support mass-market use cases such as contactless payments and ticketing. This functionality, in reader mode, can also be used for authentication by tapping a government or corporate identity card, containing an SE, on the smartphone.

Dedicated SEs external to smartphones are included in the ARF v1.5 to provide strong authentication to the wallet, bind user identity in the wallet, or hold sensitive data and cryptographic material.

While external identity cards avoid the need to access, issue or manage SEs inside the smartphone, their inclusion is mostly intended to support a legacy of existing deployments and member states should not promote this as a viable long-term deployment model. Recital 29 of the eIDAS 2.0 regulation discusses that the use of certified external SEs should be a transitional measure, until availability of certified SEs within the user's device[18].

External Secure Elements and WSCD Key Requirements	
User convenience	Low - as external SEs require citizens to find their ID card and tap it on the smartphone, which introduces friction to the user experience.
Reach	Medium - limited by the availability of NFC smartphones and NFC-enabled ID cards. Most EU member states are now issuing ID cards as per EU regulation 2019/1157[19] but the penetration rate is still low, as mandatory issuance only started in August 2021, and some countries have just started rolling out ID cards with NFC.
Security	High – provided ID cards are certified with Common Criteria at EAL4+ AVA_VAN.5.
Scalability	High – member states can issue as many ID cards as needed to reach every citizen.
Sovereignty	Yes – each member state can control the issuance of the NFC ID cards, and the smartphone merely acts as a smart card reader.
Unconnected Proximity Use Cases	Yes – as no network connectivity is required to access the external NFC card.
Maturity	Yes – NFC reader mode has been deployed for a long time and several national digital ID wallets use it with contactless ID cards. Most EU member states issue contactless ID cards.

3.4.2 Secure Element Clusters as Remote WSCD

SE clusters have been developed to bring security to some market segments and address the lack of availability of tamper-resistant hardware security on smartphones. This approach bundles SEs in the backend to create large clusters of eSEs.

SE clusters provide advantages that complement implementations that also use a local SE-based WSCD:

- Simplified wallet implementation: Both the local and remote SEs have identical features and can host the same WSCA, i.e., java card applet.
- Streamlined provisioning and personalization: The process for setting up and customizing the SE is similar whether it is local or remote.

[18] Page 6, article 29: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401183

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1157

- Easier migration: As eSIMs become more accessible, as well as eSE, transitioning from remote SE clusters to local internal SE is simplified as they implement similar technology.

These advantages make SE clusters an attractive option for implementing a WSCD, until eSIM adoption reaches critical mass.

SE clusters are already used in mass-market applications, such as in eTicket[20] Germany, Germany’s digital system for train, bus and other transport ticketing.

Secure Element Cluster and WSCD Key Requirements	
User convenience	High – as long as connectivity is available.
Reach	High.
Security	High – provided the SEs in the cluster are Common Criteria certified EAL4+ AVA_VAN.5.
Scalability	High.
Sovereignty	Yes.
Unconnected Proximity Use Cases	No – this model does not support proximity use cases.
Maturity	Yes - Clusters are already used in different segments such as e-ticketing, and are based on the same SE technology. Piloting should be done to improve readiness for mass-market deployment of the EUDI wallets.

3.4.3 Remote HSM as Remote WSCD

Hardware Security Modules (HSM) are tamper-resistant devices attached to network servers that protect and manage cryptographic and sensitive data. They are widely used for encryption, decryption, digital signatures, authentication, and payment, as well as many other use cases.

In this architecture, remote security is implemented in the cloud using a HSM, separate from the user’s device. However, this architecture has limitations as it is not possible to enable proximity use cases for the wallet, as it requires network connectivity to access the remote WSCD. Most countries are therefore considering using hybrid solutions, such as a remote WSCD in the cloud combined with a local WSCD embedded in the phone. This architecture also requires some means of strong authentication or secure access to the WSCD, which is available on the network and can be subject to threats and attacks.

The GSMA’s European Identity Group[21] has discussed this approach and proposes a solution for achieving high-level certification in line with eIDAS 2.0 by integrating a wallet with a software development kit (SDK) that consolidates all privacy and security sensitive functions. This architecture, known as Architecture C in GSMA's considerations for eIDAS 2.0, includes three main components: the wallet application with the SDK, the SIM in the mobile device, and a remote back-end server hosting a HSM for signing user ID attributes.

Remote HSM and WSCD Key Requirements	
User convenience	High – as long as connectivity is available.
Reach	High.

[20] At the heart of the eTicket security are Security Access Module clusters, which are specialized Secure Element clusters https://www.eticket-deutschland.de/en/certified-sam-clusters-and-sam-servers/.

[21] https://www.gsma.com/gsmaeurope/resources/architecture-considerations-for-eidas-2-0

Security	High - provided the HSM is Common Criteria certified EAL4+ AVA_VAN.5.
Scalability	High.
Sovereignty	Yes.
Unconnected Proximity Use Cases	No – this model does not support proximity use cases.
Maturity	Yes – HSMs are used in various market segments, securing credentials for data at rest and in motion. This model, for example, is widespread for payment. Piloting should be done to improve readiness for mass-market deployment of EUDI wallets.

4 Solving the Sovereignty Challenge

As discussed in the previous section, SE technologies offer a range of benefits for the implementation of a WSCD when compared to the other potential technologies identified in the eIDAS 2.0 regulation and certification implementing act. Although wallet security with SEs can be achieved today on smartphones, GlobalPlatform and the wider industry is currently working to solve the following challenges so that wallets can be easily deployed on all devices, regardless of the manufacturer:

- SEs are currently controlled by smartphone manufacturers or MNOs. Third-party developers cannot freely access or modify them as they are partially open, or closed, systems.
- The smartphone market is diverse and SE implementations are fragmented.
- Certification of SEs is also fragmented, with different certification schemes such as EMVCo for contactless payments, or eSA for eSIMs, which may not fully satisfy the security certification requirements of the wallet regulation.

This section firstly elaborates on these challenges before discussing the GlobalPlatform Secured Applications for Mobiles (SAM) interoperable framework. This standard is now available to member states to enable the deployment of secure applications on all SEs, regardless of the smartphone manufacturer or MNO.

4.1 Overcoming a Closed Ecosystem

The regulation outlines that member states have three options when seeking to use an SE as a WSCD to secure their wallet[22]:

1. Deploying and hosting the member state applet (WSCA) on the **SE directly** or via an SE-broker[23].
2. Accessing the **SE through the native services** of the smartphone operating system[24]. The ARF refers to this as a “Local Native WSCD”, whereas a Local Internal WSCD is an SE that is directly accessible from the wallet application.
3. Hosting their applet and wallet in a smartphone **manufacturer’s wallet, if the latter uses the device’s SE to secure the WSCA.**

While the eIDAS 2.0 regulation calls for a fair and non-discriminatory access to SE[25], and efforts by the European Commission like the Digital Markets Act[26] have sought to make this a reality, the proprietary and fragmented nature of the SE market currently limits the scalability of implementations.

[22] These options apply both to eSE or eSIM, but generally secure applications such as contactless payment or ticketing are implemented in the eSE, whereas eSIM are used for securing network connectivity.

[23] An example of an SE-broker is the Trusted Service Manager System supporting the German Smart-eID, in line with the BSI TR-03165 technical guideline and based on various GlobalPlatform standards.

[24] For example, Strongbox on Android or SecureEnclave on iOS.

[25] Recital (49) of the 2024/1183 preamble.

[26] The Digital Market Act identifies large gatekeepers that should open access to SE technology in devices and, as such, does not mandate access to SEs for smaller smartphone manufacturers.

The device security industry is therefore collaborating to give member states a standardized and interoperable way to access and manage SEs and protect wallets – and citizens' identities – with the highest levels of security across all devices, regardless of manufacturer or mobile network operators. Industry association, GlobalPlatform, and its members, are leading this initiative, in collaboration with major security stakeholders.

4.2 Secured Applications for Mobile: standardized, interoperable access to SEs

eSIM technologies will soon be ubiquitous in smartphones. The GSMA recognized the value in sharing the space in eSIMs to offer security features to third parties that are not MNOs or smartphone manufacturers. To achieve this, the GSMA issued the SAM[27] requirement specification with GlobalPlatform later implementing these requirements into the SAM technical specification[28].

SAM addresses the limitations outlined at the start of this chapter by providing a standardized framework for deploying secure applications to SEs, regardless of the smartphone or MNO.

SAM enables SEs to be partitioned into separate isolated security domains. Applets from different service providers can then safely share the space within an SE. The control and access to each of these isolated security domains is done using Public Key Infrastructure (PKI) certificates.

In the context of the EUDI Wallet, a PKI certificate can simply be added to all eSIMs that will be shipped to EU countries. This PKI can then be managed by a central EU authority[29]. Based on this root certificate, each member state could have its own certificate which provides exclusive access and control for them to an isolated part of the eSIM to install and manage their WSCA.

Isolation is key to giving member states complete security over their sensitive data and code. To address this, GlobalPlatform is developing a Common Criteria Protection Profile, (CC EAL 4+ or higher), the Multi-Scope Platform PP (MSP PP), -expected to be available mid-2025- to enable SEs implementing SAM to be evaluated.

[27] https://www.gsma.com/get-involved/working-groups/wp-content/uploads/2023/11/SAM.01-v1.1-1.pdf
[28] https://globalplatform.org/product/sam-configuration-v1-0-gpc_gui_217/
[29] Member states and the EC should agree a path forward for the establishment for a central EU authority to manage the issuance of the PKI certificate for the EUDI Wallet, as was done previously for e.g. Cooperative intelligent Transport Systems (C-ITS).

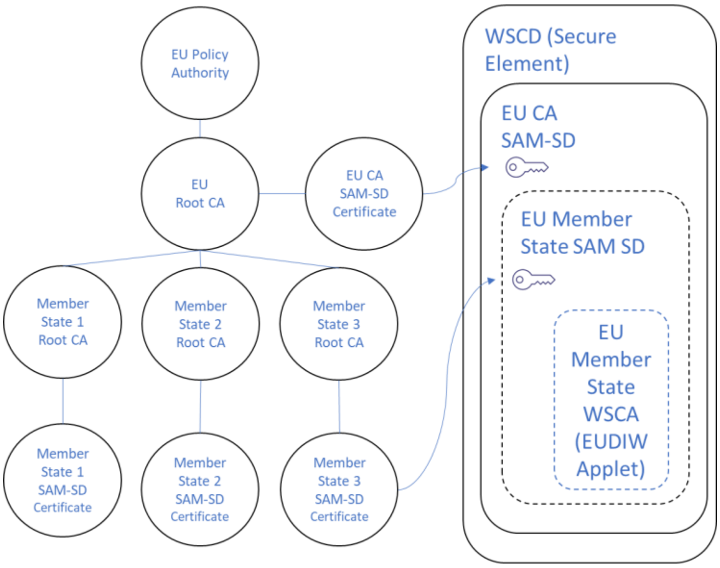

Figure 3 PKI for Securing WSCA on Secure Elements

The right-hand side describes how WSCAs are provisioned into a SAM-enabled SE acting as a WSCD. The EU Authority has the unique privilege to grant access to sub-security domains for the member states. Once created, member states have full control over their own SAM sub-security domain without any further access possible for the EU Certificate Authority. Control over the security domains is achieved through a PKI infrastructure described on the left-hand side.

The benefits of GlobalPlatform's SAM technology include:

- **Enhanced Security:** SAM provides an isolated secure environment for member states to store sensitive data and cryptographic keys, significantly reducing security risks for their wallet.
- **Remote Management**: SAM enables over-the-air deployment, update and management of the WSCA, ensuring member states can deploy and update their WSCA on devices already in the field.
- **Interoperability**: SAM supports multi-application environments, allowing different WSCAs from several member states, or even authorized private wallets, to coexist securely on the same device, enhancing user convenience.
- **Flexibility in Application Deployment**: SAM enables WSCAs to be deployed across various devices and platforms without being tied to specific manufacturers or mobile network operators.
- **Compliance with Standards**: SAM adheres to GlobalPlatform specifications, ensuring that it meets industry standards for security and interoperability, which is crucial for widespread adoption.
- **Long-term Stability and Scalability**: The standardized approach ensures that solutions can evolve in line with technological advancements, while maintaining compatibility with existing systems.
- **Sovereign Access Control**: Establishing a European root certification authority as part of SAM implementation enhances trust and security in digital identity solutions across the EU.

Long-term, this approach maximizes scalability and efficiency of EUDIW deployments for all stakeholders, ensuring devices do not need to be configured country specific.

4.2.1 Proactive steps for all stakeholders

To make the use of SEs for the EUDIW a reality, steps should be taken now by the different stakeholders:

- The EU Commission and regulators should establish an authority to manage access to SEs in devices, enabling member states to secure their EUDIWs.
- Member states should collaborate in pilot programs with industry partners to develop SAM/CSP compatible wallet solutions and advocate adoption in EU-level discussions and working groups.
- Wallet developers should integrate the SAM and CSP frameworks from an early stage of development and engage with GlobalPlatform to ensure successful implementations.
- Large Scale Pilots should incorporate SAM/CSP in their programs.
- Smartphone manufacturers should provide the necessary components to facilitate SAM and CSP integration.

4.3 The Benefits of Early Pilots & Deployment with SAM-Ready

Until SAM-certified eSIMs are deployed, most SEs that are already widely available in smartphones can provide a secure environment equivalent to what SAM aims to achieve. The key feature required for these SAM-Ready SEs, beside the support of GlobalPlatform Card Specification[30], is the support of GlobalPlatform Secure Channel Protocol (SCP) 11b[31]. SCP11b and PKI are crucial for SAM as they enable secure, authenticated communication between the SAM Security Domain and off-card entities. All eSIMs following the GSMA Remote Subscription Provisioning (RSP) specification support SCP11b, which means that all smartphones with embedded UICCs are SAM-Ready.

The following table details how these SAM-Ready SE differ from fully SAM compliant SE.

	SAM-Ready SE	Fully compliant SAM SE
EU Certificate for the EU Identity Security Domain	Must be provisioned post-issuance by the smartphone manufacturer, as eSIM/eSE are already issued.	Provisioned pre-issuance by the SE manufacturer.
Controlling Authority Security Domain (CASD)[32]	One single CASD for the eSIM/eSE, which could allow the smartphone manufacturer to erase the EU Identity Security Domain (erasing is the only operation that the manufacturer can perform but it cannot otherwise compromise or access data in the identity security domain).	One CASD per SAM Security Domain, preventing erasing by the eSE/eSIM smartphone manufacturer.

[30] https://globalplatform.org/specs-library/card-specification-v2-3-1/

[31] https://globalplatform.org/specs-library/secure-channel-protocol-11-amendment-f/

[32] The CASD is a unique, trusted entity within a SE that manages cryptographic keys and facilitates secure personalization of other security domains.

Communication Channel	All Security Domains and sub-domains use the same physical communication channel with the smartphone.	Optionally, the SAM domain can have a dedicated and separated communication channel with the smartphone.
Isolation	Isolation between Security Domains is evaluated against the GlobalPlatform SE Protection Profile.	Isolation between Security Domains is evaluated against the GlobalPlatform Multi Scope Platform Protection Profile, with additional coverage, e.g. CASDs isolation.

Member states and large-scale pilots can immediately host EUDI wallets on SAM-Ready SEs via agreements with smartphone and SE manufacturers, or SE-brokers. This will allow them to easily and independently migrate their implementation to all smartphones as SAM eSIMs hit the market. This anticipation is important for several reasons:

- **Early Adoption of Security Features**: SAM-Ready SEs are already available and can provide a high LoA for EUDI Wallets, complementing other WSCD technologies such as remote or external WSCD.
- **Incremental Transition**: This approach facilitates a gradual transition to full SAM SEs, allowing member states to adapt systems and processes incrementally rather than facing a complete overhaul later.
- **Market Readiness**: Embracing SAM-ready technology now helps member states prepare for future innovative standards and migration to SAM once fully available, ensuring relevance and compliance of implementations over time.
- **Cost Efficiency, Testing and Feedback Loops**: Member states can also test functionalities and gather citizen feedback to inform improvements and adjustments before fully transitioning to certified SAM SEs. This lowers implementation risk during SAM migration.
- **Interoperability Benefits**: SAM-Ready SEs work within existing infrastructure, promoting interoperability with current systems, and reducing integration challenges when transitioning to certified SAM SEs.
- **Enhanced User Experience**: Early adoption will improve user experiences through seamless and faster transactions, and better security features, to foster trust among citizens.
- **Competitive Advantage**: Stakeholders that adopt SAM-Ready technology early can gain a competitive edge or cost efficiencies by offering more secure and efficient services compared to those that delay implementation.
- **Adopt Public Key Infrastructure (PKI)**: Proactivity in establishing an EU and member states PKI framework to manage digital certificates will support the final SAM architecture.

By leveraging SAM-ready SE now, member states can ensure they are not only prepared for future developments but also benefiting from enhanced security and operational efficiencies today. By implementing these strategies now, stakeholders can create a robust foundation that will facilitate a smoother transition to full SAM-compliant solutions as they become available.

5 Solving the Certification Challenge

Certification of the wallet to a high LoA is key in providing security and trust to citizens, member states, and public and private sector service providers.

ENISA has started to define an EUDI Wallet Certification Scheme, a process which will take some time to complete, well beyond the mandatory issuance date of the EUDI wallet. Until then, every member state will need to operate a transitional national certification scheme to certify their EUDIW.

Although each member state is responsible for defining and operating its own wallet certification scheme, wallets need to be cross-recognized in cross-border use cases, and therefore harmonization is required. The Implementing Act 2024/2981 on Wallet Certification details the common requirements that member state wallets and certification schemes will need to meet. This chapter outlines these requirements, details the certified SE's role in meeting them and outlines the value of CSP to simplify the security evaluation process.

5.1 Composition: Simplifying the Wallet Security Certification

The wallet is composed of several components – not all under the control of the wallet issuer – working together to ensure the security of the wallet solution.

- The WSCD and the WSCA running on it.
- The wallet mobile application on the smartphone.
- The smartphone platform and its operating system.
- Any server backend where security sensitive data or cryptographic material is stored remotely.

The different components of the wallet solution are developed by different actors (including application developers, smartphone manufacturers, smartphone OS editors, SE manufacturers and others), and have different update lifecycles. With rich and varied smartphone, SE, and other offerings from different actors, certifying the component bundle of each wallet solution is simply not scalable.

Achieving wallet certification in an efficient and scalable way is therefore the key challenge facing member states. The certification of the wallet must be based on the independent certification of each of its components, and in their final composition, to certify at high LoA the wallet solution.

It is therefore essential to foster a pragmatic and sustainable security certification approach for wallets and their components, supported by security certification reuse mechanisms and composition between the different layers. This enables previously certified components to be used to build a device with in-built security assurances, without having to repeat a complete evaluation of the same component in each and every wallet solution. This will ensure an end-to-end security solution that meets the high security level required to protect citizen IDs.

5.2 Certified Secure Elements as High LoA WSCDs

To avoid certifying the full bundle of the wallet and wallet components, the certification implementing act has restricted the scope of wallet certification to the software components of the wallet instance, such as the wallet application, as well as the processes used to provide and operate the wallet solution.

The WSCD and WSCA are not necessarily in the scope of the wallet certification[33], but the Certification Implementing Act requires that they be certified to a high standard of certification, such as Common Criteria (CC)[34] EAL4 evaluation and advanced methodical vulnerability analysis comparable to AVA_VAN.5[35].

The embedded UICCs or embedded SEs present today on most smartphones are already evaluated at EAL4+ AVA_VAN.5 and are therefore a perfect fit for providing the WSCD, the foundation for a high LoA for the wallet, and protecting cryptographic material, and sensitive data or code.

Prior to the introduction of the EU Cybersecurity Certification (EUCC) scheme in early 2024, a European Commission Implementing Regulation defined a European Scheme for CC certification and was operating national schemes for CC certification. Each scheme was mutually recognized within the Senior Officials Group – Information Systems Security (SOG-IS) group[36]. The Certification Implementing Act recognizes both legacy SOG-IS certifications and the new EUCC certifications for certification of the WSCD by the transitional national certification schemes.

Although the EUCC Scheme is referenced in the Certification Implementing Act, most SEs on smartphone are not currently certified under the SOG-IS or EUCC schemes. Depending on the market segment, industry-led certification schemes are used including the GSMA eUICC Security Assurance Scheme for eSIMs, or EMVCo for eSEs used in payment use cases. The certificates issued by these industry-led security certification schemes could nevertheless provide evidence that a WSCD meets the requirements for a high LoA for the transitional national certification schemes[37].

5.3 Simplifying & Scaling WSCD/WSCA Certification with Cryptographic Service Provider (CSP)

In addition to the WSCD, the Certification Implementing Act requires that WSCAs are evaluated at a high LoA, with a vulnerability assessment at level AVA_VAN.5.

Applications on SEs are usually implemented as applets, running in a virtual machine (typically JavaCard), embedded in the SE. In the case of an EUDI wallet, secured by an SE, the SE and its virtual machine can be considered as the WSCD, whereas the EUDIW applet running on this SE can be considered as the WSCA.

For applications requiring a high LoA, such as the EUDIW, the composition of the WSCA and WSCD must be evaluated. This is not scalable, however, and increases the complexity of the certification since each combination of SE and applets would have to be evaluated together. The sheer number of smartphone models, SEs, and wallet applets with different versions and updates would render composite certification[38] practically impossible.

[33] The WSCD or WSCA are only in the scope of the certification if they are provided by the wallet solution.

[34] CC is a global mutually recognized standard for product security. In the CC methodology, products are certified to meet security requirements expressed as Protection Profile (PP) requirements.

[35] CC certification assigns a numerical grade, the Evaluation Assurance Level (EAL) from 1 to 7. Increasing levels require more stringent evaluation of a product’s security. Products can also meet additional vulnerability assessment requirements such as AVA_VAN.5, which certifies for an “advanced methodical vulnerability analysis and resistance against a high attack potential”.

[36] https://www.sogis.eu/

[37] Other schemes might also validate a high LoA, e.g. GlobalPlatform’s SESIP Level 4 and 5.

[38] Composite product evaluation and certification - https://www.sogis.eu/documents/cc/common/JIL-Composite-product-evaluation-and-certification-v1.6.pdf.

To ease this evaluation process, GlobalPlatform has developed a Cryptographic Service Provider (CSP) specification[39]. This separates the cryptographic operations and data, from the business logic implemented in the applet. The identity wallet applets are then designed to delegate all sensitive cryptographic operations to the CSP, which is certified at a high LoA. Applets are then certified at a lower LoA as they do not handle the most security-critical operations directly.

Fundamentally, CSP simplifies the certification process, as expensive time-consuming high-level certifications only need to be done once for the SE/CSP platform, rather than for each identity applet and SE combinations. Even though the applets are certified at a lower level, the overall wallet solution maintains a high LoA because the critical operations are performed by the highly certified CSP.

The CSP specification is an example of the approach detailed in the Certification Implementing Act[40], that allows lowering the LoA requirements for the certification of a WSCA if it can be justified that the overall high LoA is met.

Additionally, the draft ENISA report on the *eUICC Certification under the EUCC Scheme*[41] also identifies GlobalPlatform CSP as a solution to enable certification of applets at a lower LoA, e.g., EAL2 AVA_VAN.2, while still maintaining a high security level at EAL4+ AVA_VAN.5 and ALC_DVS.2[42] for the combined applet and SE.

The table below lists some of the protection profiles (PP) available, or soon to be available, to certify an SE acting as a WSCD. While a specific protection profile for EUDI wallet applets acting as a WSCA is not yet available, existing protection profiles for authentication (e.g., PPs for PACE[43], EAC[44], and FIDO[45] protocols) and electronic signatures (e.g., PPs for SSCD[46]) can be used until a specific PP for the EUDIW applet becomes available.

Component	Available Protection Profiles
eSE hardware	BSI-CC-PP-0084[47] for chips BSI-CC-PP-0117[48] for System on Chip
eSE Java Card Platform (JCP)	BSI-CC-PP-0099[49]
eSE JCP with GlobalPlatform framework	GPC_SPE_174[50]
SAM	GSMA SAM requirements[51] GlobalPlatform SAM specification GPC_GUI_217[52] GlobalPlatform Multiscope Platform PP (in development)

[39] At the time of writing, publication is expected mid-2025.

[40] Article 3(2) of Annex IV of the Implementing Regulation 2024/2981.

[41] https://www.enisa.europa.eu/sites/default/files/2024-11/Report_eUICC%20Specifications_Public%20consultation_1.pdf

[42] ALC_DVS.2 is a CC Security Assurance Requirement that mandates stringent development security measures.

[43] PACE (Password Authenticated Connection Establishment) is a security protocol designed to protect data in electronic travel documents, particularly ePassports.

[44] Extended Access Control (EAC) is an advanced security feature for electronic passports that protects and restricts access to sensitive personal data stored in the contactless chip.

[45] FIDO (Fast IDentity Online) is an open authentication standard designed to reduce reliance on passwords.

[46] SSCD (Secure Signature Creation Device) is a specific type of hardware for creating electronic signatures.

[47] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0084b_pdf

[48] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0117b_pdf

[49] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0099V2b_pdf

[50] https://www.commoncriteriaportal.org/files/ppfiles/CCN-CC-PP-5-2021.pdf

[51] https://www.gsma.com/get-involved/working-groups/gsma_resources/sam-01-v1-1

[52] https://globalplatform.org/specs-library/sam-configuration/

CSP	BSI-CC-PP- 0104[53] for BSI legacy CSP
	GlobalPlatform CSP PP (in development)

5.4 Smartphone Platform Certification

As above, the draft Certification Implementing Act excludes the platform on which the wallet components are executed – usually a smartphone – from the scope of the wallet certification.

Certifying the wallet application for each smartphone and operating system version is impossible, given the large array of smartphones available on the market and the frequency of software updates. It is therefore important to decouple the certification of the wallet solution from any certification of the smartphone platform, encompassing the hardware and operating system.

It is widely recognized, however, that it is essential to assess the security of the smartphone platform. This is to ensure that the platform meets the security requirements needed to host applications like digital identity wallets.

Today, software security is managed by the smartphone makers. Several initiatives at ETSI and GSMA are working to define a methodology for security certification of the smartphone platform. The ETSI standard TS 103 732[54] defines a CC protection profile for Consumer Mobile Device including essential security requirements, and GSMA published the MDSCert[55] Mobile Device Certification Scheme methodology as a lighter weight alternative to assess compliance with the TS 102 732 requirements for smartphone security.

To streamline this process for member states and other stakeholders, the required assessments can be done using the Security Evaluation Standard for IoT Platforms (SESIP)[56]. The security evaluation methodology from GlobalPlatform reduces the cost, complexity and effort required to perform security evaluation and certification. SESIP utilizes the concepts of composition and reuse, so that previously certified components can be used to build a solution with in-built security assurances, without having to repeat the same evaluations.

The SESIP methodology is already available to member states to evaluate and evidence the security of the smartphone platform as part of their transitional national certification schemes.

5.5 Wallet Application Certification

The wallet application is in the scope of the certification, as a key component of the overall wallet solution. The wallet application is referred to as the ‘wallet instance’ in the ARF and is the component that is provided by the wallet provider for installation on the user's device.

There are a number of reasons why certification of the wallet application is essential. According to the ARF, users of EUDIWs utilize the wallet instance to receive, store, and present their personal identification data (PID), Qualified Electronic Attestation of Attributes (QEAA), Public Body EAA (PuB-EAA), or EAA. This includes verifying and authenticating

[53] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0104b_pdf

[54] https://www.etsi.org/deliver/etsi_ts/103700_103799/103732/01.01.01_60/ts_103732v010101p.pdf

[55] https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-53-mobile-device-certification-scheme/

[56] https://globalplatform.org/sesip/

their identity for a variety of use cases. EUDIW users also have the capability to create Qualified Electronic Signatures and Seals (QES) and engage in wallet-to-wallet interactions.

The wallet instance also encompasses various interfaces. It operates as the user interface, communicates with the relying party and qualified trusted service providers, and engages with the WSCA/WSCD to securely manage the cryptographic assets and perform cryptographic functions to ensure a high LoA.

Additionally, each WSCA is linked with a wallet instance and manages assets, such as keys, for that specific wallet instance.

The Certification Implementing Act acknowledges that the CC methodology is not well suited for certification of the wallet instance. Member states' certification bodies can therefore select their preferred wallet instance certification methodology from:

- the Fixed-Time Cybersecurity Evaluation Methodology (FITCEM[57]).
- legacy national schemes based on similar fixed-time principles such as CSPN[58] in France or BSZ[59] in Germany.
- national schemes based on FITCEM[60].
- GlobalPlatform's SESIP[61] Methodology.

[57] EN 17640:2022 "Fixed-time cybersecurity evaluation methodology for ICT products".

[58] CSPN is a security certification issued by ANSSI, the French National Cybersecurity Agency, created as an alternative to more lengthy and costly CC evaluations.

[59] BSZ is a certification scheme developed by the German Federal Office for Information Security (BSI) that provides a faster alternative to traditional CC evaluations.

[60] On May 15, 2024, the French ANSSI and German BSI signed a new version of the mutual recognition agreement for the CSPN and BSZ based FITCEM.

[61] EN 17927:2023 "Security Evaluation Standard for IoT Platforms (SESIP)".

6 CONCLUSIONS

The European Digital Identity Wallet (EUDIW) initiative represents a significant step towards a secure, interoperable, and widespread digital identity solution for EU citizens. Ensuring a high level of security is crucial for establishing trust among stakeholders, especially citizens, member states, and public and private sector service providers. Without a high level of security, the EUDIW would be vulnerable to identity theft, fraud, and other cyber threats, potentially undermining the entire digital identity ecosystem.

This position paper has outlined the challenges and solutions to meet this high level of security, and the key takeaways include:

- **Security technology:** SEs offer the best technology to achieve the highest levels of security and usability for EUDIW implementations on smartphones long-term.
- **Sovereignty:** The SAM framework enables member states to overcome the challenges associated with deploying applications on SEs, completely independently of smartphone manufacturers and MNOs. SAM-Ready technology is already widely available, allowing member states to immediately host EUDI wallets on existing SEs while preparing for full SAM implementation. A European root certification authority, acting as a sovereign gatekeeper managing access to eSIMs in smartphones, is vital to ensure EUDIW security, interoperability, and control.
- **Certification:** The CSP specification provides an interoperable standard way to streamline the WSCA certification process, reducing time and costs associated with security assessments. More broadly, certification of wallet solution components can be simplified through composition and reuse mechanisms.

The implementation of EUDIWs will likely involve an evolving mix of technologies to ensure optimal security, usability, and reach. While remote WSCD and external ID cards may play a prominent role in the short term, embedded SEs in smartphones are rapidly becoming ubiquitous and offer significant advantages in terms of security, convenience, and offline capabilities.

It is crucial for stakeholders to begin addressing SE integration now, as this technology is poised to become the mainstream solution for securing digital wallets in the very near future, ensuring a smooth transition to more secure and user-friendly wallet implementations as the technology landscape matures.

To move forward, stakeholders should:

- Establish an EU authority to manage PKI for SAM-enabled SEs.
- Collaborate on pilot programs to develop SAM/CSP compatible wallet solutions.
- Integrate SAM frameworks early in wallet development projects.
- Incorporate SAM/CSP in Large Scale Pilots.
- Provide the necessary components to facilitate SAM integration in smartphones.

By taking these actions, the EU can create a secure, interoperable, and widely adopted digital identity solution that benefits citizens, member states, and service providers alike. The technologies and frameworks outlined in this paper provide a clear path towards achieving the EU's digital identity goals while addressing critical security and sovereignty challenges.

GlobalPlatform is looking forward to continuing supporting the EUDIW process and stands ready to support all stakeholders in making European Digital Identity successful long-term.

Annex A GET INVOLVED

GlobalPlatform eID Wallet Task Force and Secure Element Committee are actively working to support the implementation of secure and interoperable European Digital Identity (EUDI) Wallets.

GlobalPlatform is developing specifications and frameworks that leverage its Secure Element technology to meet the high security requirements of EUDI Wallets while ensuring scalability and user convenience.

For EUDI and digital identity stakeholders, engaging with GlobalPlatform offers several benefits:

- Access to proven security technologies already deployed in billions of devices.
- Ability to influence development of standards that will shape the future of digital identity.
- Opportunities to collaborate with industry leaders and policymakers.
- Early insight into emerging specifications and best practices.

To learn more or get involved, stakeholders can attend GlobalPlatform's eID Wallet seminars and training sessions or consider becoming a member to participate directly in standards development.

A.1 Follow GlobalPlatform Specifications

All GlobalPlatform specifications are free and available at: https://globalplatform.org/specs-library/). They:

- Leverage mature and interoperable specifications for secure components as the foundation for cybersecurity; and
- Rely on externally validated certification program to ensure compliance with robustness and with desired security level.

A.2 Become a GlobalPlatform Member

GlobalPlatform is a member-driven standards organization for trusted digital services and devices. Consider becoming a member if you are interested in:

- Obtaining early visibility of standards development as the evolve.
- Shaping the development of standards directly (ensuring that they answer your requirements).
- Planning your roadmap to optimize:
  - Future proofing solutions
  - Migration roadmaps for new requirements (Post Quantum Crypto, Security Regulation).
- Learning about new regulations and technologies to ascertain how they can improve your business.
- Leveraging security evaluation methodologies.

Join today!