

Eurosmart Perspectives on EUDIW Certification and Deployment in the EU

July 2026

Introduction

The European Digital Identity Wallet (EUDIW), established by Regulation (EU) 2024/1183, is the cornerstone of the EU Digital Identity Framework. It aims to provide every EU citizen with a trusted, interoperable digital identity solution, based on decentralized identity principles and usable across borders, both online and offline, under the sole's control of every citizen.

Beyond initial deployments, the long-term success of the EUDIW depends on its ability to deliver sustainable trust, user privacy, and operational resilience in the face of evolving threats and usage scenarios. In that perspective, this paper explores future-proof security foundations for decentralized digital identity wallets, rather than short-term implementation choices.

To ensure trust, security, and scalability, certification must address the wallet as a system and not as isolated components. The Architecture and Reference Framework (ARF) defines two critical sub systems:

- **Wallet Secure Cryptographic Device (WSCD)** – the hardware anchor for cryptographic keys and sensitive operations
- **Wallet Secure Cryptographic Application (WSCA)** – the secure application layer interfacing with the WSCD to deliver wallet services

This paper focuses on security architectures capable of supporting strong guarantees on privacy, resilience, and user control over time. In particular, hardware-backed security mechanisms based on Secure Elements are examined as a future-proof step for high-assurance EUDIW implementations. Secure Elements enable decentralized identity models where cryptographic keys remain under the exclusive control of the user, while supporting critical capabilities such as offline operation, battery-off use cases, and increased resistance to large-scale or high-potential attacks.

A coherent certification approach should therefore enable an evolution towards such architectures where higher level of assurances are required, preserving interoperability, certifiability and deployment flexibility across the EUDIW ecosystem and resistant to the highest level of attacks.

I. Achieving EUDIW Security Level High: A Pragmatic System Model for Member States

Security and certification are not optional, they are the enablers of trust, cross-border recognition, and scalable deployment. To meet the EUDIW security level high, we advocate a system architecture anchored on three proven components:

- **Secure Element (SE):** A certified hardware root of trust (EUCC/SOGIS EAL4 + AVA_VAN.5) ensuring tamper resistance and cryptographic integrity designed to meet the Level of Assurance “High” as required by the eIDAS2 Regulation. Note that Secure Elements are coming in several formats such as eSE (embedded Secure Element), external Secure Element (e.g. ID card), SIM cards (UICC) or embedded SIM cards (eUICC), etc. All formats are suitable for high-assurance deployments and should be considered in national strategies
- **Cryptographic Service Provider (CSP):** A modular cryptographic layer that is designed to simplify the initial certification of the WSCA integration on top of the WSCD (SE) accelerates rollout and supports lifecycle key management. Additionally, the CSP is designed to provide all key security functionality to the WSCA. This technology may not be necessarily relevant for external Secure Element (e.g. ID card) but is very relevant in other cases (e.g. embedded Secure Element (eSE), SIM cards (UICC) or embedded SIM cards (eUICC))
- **Secure Application Module (SAM):** A secure execution environment that can isolate the WSCA and its related data independently of OS and MNO¹ constraints. This technology is mostly relevant where the SE hosts application under the control of an MNO (e.g. embedded Secure Element (eSE), SIM cards (UICC) or embedded SIM cards (eUICC))

For EUDIW deployment with an internal SE:

Internal SE are SEs which are internal to devices dedicated to host a European Digital Identity Wallet (EUDIW) e.g. a mobile phone. It designates mainly form factors such as embedded Secure Element (eSE), SIM cards (UICC) or embedded SIM cards (eUICC).

The internal SE + CSP + SAM configuration offers the most pragmatic and certifiable path for Member States and wallet providers to meet EUDIW objectives - delivering compliance, interoperability, and user trust at scale with user control, while ensuring privacy.

For EUDIW deployment with an external SE:

The architecture remains robust and certifiable, with the external SE (such as a smart card or ID card) acting as the hardware root of trust. This approach supports strong user control, facilitates cross-border interoperability, and enables modular certification pathways tailored to diverse deployment scenarios.

¹ Mobile Network Operator

I.1. Secure Elements (SEs): Certified Foundations for WSCD and WSCA

A Secure Element is a certified hardware root of trust designed to provide a high level of security for sensitive operations and data storage. It ensures tamper resistance, cryptographic integrity, and compliance with stringent security standards. In the context of eIDAS2 Regulation, Secure Elements are required to meet high assurance levels, typically certified under schemes such as EUCC/SOGIS EAL4 + AVA_VAN.5.

Secure Elements serve as the foundation for trust in digital identity and secure transactions by protecting cryptographic keys,, and sensitive data against physical and logical attacks. They are implemented in various form factors, including:

- **Embedded Secure Element (eSE)** = integrated within a device's hardware
- **External Secure Element (external SE)** = such as smart cards or ID cards
- **SIM cards (UICC)** = used in mobile devices
- **Embedded SIM cards (eUICC)** = for IoT and mobile connectivity

By combining hardware-based security with certification, Secure Elements:

1/Provide resilience against advanced attack vectors, making them essential components in trusted digital ecosystems:

- Ensuring strong user control, with data remaining in the control of the user
- Enforcing User privacy

2/Enable compliance with regulatory frameworks eIDAS2 level high:

- Secure Element meets the criteria for WSCD/WSCA as defined in the Architecture Reference Framework² (ARF)
- Reuse of existing Secure Elements evaluations for faster EUDIW certification
- Seamless integration of the WSCA with the WSCD thanks to the GlobalPlatform technology and a set of standardized APIs facilitating WSCA and WSCD binding

² [GitHub - eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework: The European Digital Identity Wallet](https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework)

I.2. Cryptographic Service Provider (CSP): Modularity and Scalability

The CSP technology 2.0³, developed by GlobalPlatform, is a new security approach for the SE focusing on the execution and evaluation of all sensitive operation within a abstract layer/platform, called the CSP and allowing the hosting of a WSCA application on top where the evaluation of the WSCA is simplified and can be done with a reduced amount of effort while allowing to claim a high level of security for the overall solution. In particular, CSP enables the following:

- A security certification of the WSCD at EAL4 + with AVA_VAN.5 to meet the security level high as required by the eIDAS Regulation
- Streamlined WSCA evaluation with reduced certification scope
- Faster development and deployment cycles
- Independent maintenance of business logic: Preserved end-to-end security via standardized APIs and security packages

A Common Criteria Protection Profile is currently under development and planned to be released in 2026. The CSP will be accompanied by Global Platform supporting documents including CSP specification (Global Platform Amendment N, GPC_SPE_034) and an evaluation methodology allowing the evaluation of applets leveraging the high level of security of the CSP (GPC_SPE_230).

I.3. GlobalPlatform SAM: Enabling Secure and Independent App Execution

SAM technology⁴ defines a secure area for WSCA within a Secure Element, enabling:

- A security certification of the WSCD at EAL4+ with AVA_VAN.5 to meet the security level high as required by the eIDAS Regulation
- Isolated execution within certified environments (e.g., eUICC, SE), allowing totally independent management of the logical part of the SE
- Decoupled trust model supporting sovereign and cross-border deployments

³ The CSP technology 2.0 (amendment N) inherits from the CSP technology 1.0 introduced by BSI³. For more information, GlobalPlatform issued the [following publication](#).

⁴ Secured Applications for Mobile SAM – GPC_GUI_217

- Standardized interfaces for integration with WSCA, LAA, and SAM Service Managers
- Standardized governance model/roles allow the MS to have a sovereign control over the SE and in particular over the keys and assets used in the Digital Identity ecosystem with independence from the OEM

A Common Criteria Protection Profile for the SAM technology (Multi-Scope Manager PP) is currently under development⁵.

For more information, GlobalPlatform issued the [following publication](#).

This technology is particularly relevant where the third party which owns the Secure Element, is different from the provider of the EUDI Wallet (and thus the WSCA). Thanks to the SAM technology, an entity can create, manage and have the sole control of an area within the Secure Element in which it can install, delete, configure and use Javacard™ applet. As such, that entity can independently install and use Javacard™ applet – including WSCA - within its area of the Secure Element independently of the third party which owns the Secure Element. The SAM technology ensures complete isolation between the two areas. It is therefore very relevant for internal SE⁶ - which are owned either by a mobile operator or the device manufacturer - in which an operator and provider of EUDI Wallet is willing to install a WSCA.

However, where the Secure Element is directly owned by or under the control of the provider of the EUDI Wallet (and thus the WSCA), this technology is not needed. This is usually the case for external Secure Elements such as smart cards or ID cards when issued by an entity which either acts as provider of EUDI Wallet or is under the control of the provider of EUDI Wallet (e.g. ministry of interior).

2. Architectural Choice for EUDIW: Balancing Certification Feasibility with Strategic Control and Autonomy

The choice of architecture for the Wallet Secure Cryptographic Device (WSCD) is pivotal to the success of EUDIW certification and deployment. Beyond early deployment phases, EUDIW must rely on security foundations capable of ensuring Strategic Control and Autonomy, certification feasibility, offline capability, privacy and user control.

In this context, Secure Element (SE)-based WSCD architectures provide a future-proof security foundation aligned with European requirements on trust, sovereignty, and user control. By anchoring cryptographic assets and sensitive operations locally within tamper-resistant hardware, SE-based

⁵ At the time of writing, the PP is under public review which will close on February 20th, 2026

⁶SE internal to device dedicated to host a European Digital Identity Wallet (EUDIW) e.g. a mobile phone. It designates mainly form factors such as embedded Secure Element (eSE), SIM cards (UICC) or embedded SIM cards (eUICC).

architectures support decentralized identity principles while enabling advanced usage scenarios that cannot be reliably achieved with purely software-based approaches.

Transitioning to an SE-based WSCD offers Europe the following strategic advantages:

- **Local control of trust anchors:** By anchoring cryptographic operations and sensitive credentials within certified hardware managed under EU jurisdiction, SE-based architectures allow Member States (not foreign vendors) to retain full control over the root of trust and wallet security policies
- **Resilience and autonomy:** SE-based architectures strengthen resilience by design, supporting offline operation, battery-off use cases, and continuity of service in constrained or disconnected environments. This capability is essential for a wide range of real-world EUDIW use cases and reinforces trust in critical situations
- **Policy enforcement and regulatory compliance:** SEs provide a controlled environment in which Member States can enforce national and EU-level security requirements. Governments can define lifecycle policies, update rules, and certification baselines without relying on external cloud infrastructures or proprietary technologies
- **Reduced geopolitical and extraterritorial exposure:** SE-based deployments minimize reliance on foreign cloud service providers or device manufacturers that may be subject to non-EU legislation (e.g., CLOUD Act). This reduces exposure to extraterritorial access requests, supply-chain dependencies, and jurisdictional risks
- **Certification efficiency and interoperability:** Existing EUCC/SOGIS certifications of SEs can be reused across Member States, ensuring harmonized assurance levels and supporting the transition to ENISA-led EU-wide schemes

SE-based WSCD architectures therefore constitute a future-proof building block for decentralized digital identity wallets enforcing European strategic control and autonomy, support strategic autonomy, and protect privacy and user control, while facilitating streamlined certification and ensuring long-term resilience.

2.1. Strategic Control and Autonomy in the context of EUDIW?

In the context of the European Digital Identity Wallet (EUDIW), *strategic control and autonomy* refer to the ability of the European Union and its Member States to maintain reliable oversight over the security foundations, trust anchors, and policy enforcement mechanisms underpinning the digital identity ecosystem - without creating unnecessary dependencies on external infrastructures or vendors which is instrumental to ensure (1) that personal and non-personal data handled by the EUDI Wallet ecosystem remain protected, genuine and confidential (e.g. not collected by non-EU entities), and (2) the availability, integrity and confidentiality of the EUDI Wallet ecosystem.

Secure Element (SE)-based architectures directly support this objective by providing a certified and highly predictable hardware environment whose security is recognized by the jurisdiction of the Member State. While sensitive credentials remain exclusively under the user's control - as mandated by the Regulation - Member States maintain strategic control through governance of the infrastructures and security policies that protect the wallet, rather than through access to user data.

SE-based architecture enables Member States to achieve the following key objectives:

- **Control over trust anchors and key management policies** = Member States define how wallet keys are generated, protected, and updated, ensuring alignment with national and EU security requirements without relying on foreign-controlled cloud or hardware environments
- **Reduced dependency on non-European operating systems and cloud providers** = By anchoring cryptographic operations in an SE, the security of the wallet becomes independent of the security posture or policy decisions of global platform providers, limiting exposure to extraterritorial legislation or unanticipated changes in foreign-managed components
- **Consistent enforcement of EU regulatory requirements** = SEs provide a controlled and certifiable execution environment in which privacy-by-design, data minimization, and security-by-design principles can be implemented uniformly across devices, supporting compliance with the GDPR and EUDIW Implementing Acts

In summary, strategic control and autonomy do not imply that Member States can access users' personal credentials - these remain strictly under the user's exclusive control.

Instead, they describe an architectural model in which Europe manages the infrastructures, trust anchors, certification schemes, and security policies that protect the EUDIW, ensuring that its integrity, confidentiality, and long-term stability remain firmly anchored within the European regulatory framework.

2.2. Direct WSCA Binding of the User

Secure Elements enable the direct binding of the Wallet Secure Cryptographic Application (WSCA) to the Wallet Secure Cryptographic Device (WSCD). This means that both wallet logic and cryptographic operations run within the same certified, tamper-resistant hardware environment, under the exclusive control of the user.

This tight binding is a key enabler for achieving high assurance for EUDIW implementations, as it ensures that:

- Sensitive wallet logic and cryptographic operations remain protected from interference by the operating system, device components or external dependencies and services
- The execution environment can be evaluated and certifiable end-to-end as a coherent security boundary

- User control over credentials and cryptographic operations is enforced in practice, rather than relying on abstract or declarative guarantees

By locally binding WSCA functionality to the WSCD, Secure Element-based architectures support decentralized identity principles while delivering a consistent and robust security model. This approach enables privacy-by-design, strengthens resilience against high-potential attacks, and facilitates demanding use cases such as offline operation or battery-off scenarios.

For Member States, the direct WSCA-WSCD binding provides a harmonized, certifiable, and interoperable security foundation. For users, it results in immediate, transparent and reliable wallet interactions that maintain trust even in constrained or disconnected environments.

2.2.1. Device binding

A foundational requirement for achieving EUDIW Security Level High is to ensure that the Wallet Secure Cryptographic Application (WSCA) operates exclusively on the intended Wallet Secure Cryptographic Device (WSCD). This binding guarantees that cryptographic keys are generated, stored, and used within the certified device boundary and that no external environment can impersonate, clone, or misuse the wallet's cryptographic functions.

In practice, binding between WSCD and WSCA can be achieved through well-established mechanisms already recognized in high-assurance ecosystems:

Trusted device logistics

Secure binding may be ensured through controlled manufacturing and provisioning processes that guarantee the authenticity and uniqueness of the WSCD. This approach relies on a secured lifecycle - from production to personalization - where device identity and trust anchors are established under strict governance. Similar models are already deployed at scale in SIM and eSIM ecosystems, where the supply chain itself provides strong assurance that cryptographic material resides in a genuine secure element under the user's control.

Cryptographic key attestation

Binding can also be supported by verifiable cryptographic attestation, whereby the device provides evidence that key material was generated inside, and remains confined to, a certified secure element. Mechanisms such as the Entity Attestation Token (EAT, RFC 9711) allow remote verification of device state and origin of cryptographic operations. This ensures that signatures or credential presentations originate from an approved WSCD, even when validation occurs across domains or borders.

Both approaches reinforce the same objective: ensuring that cryptographic operations take place within a trusted, certified hardware boundary, preventing unauthorized key usage, and supporting conformity with the eIDAS requirements applicable to high-assurance wallet deployments. They also

enable consistent interpretation of WSCD–WSCA coupling within the ARF, ensuring predictable security behavior across Member States and deployment models.

2.3. Enhanced Privacy

Secure Elements (SEs) execute all cryptographic operations locally on the user’s device or token, ensuring that private keys and sensitive data and credentials remain confined within a certified tamper-resistant hardware environment. By design, this approach minimizes exposure to networks or external infrastructures and preserves confidentiality of identity data at all times. Because no sensitive credential ever leaves the SE, exposure to networks, remote infrastructures, or external service providers is drastically reduced. This architecture eliminates the attack surfaces associated with cloud-based or remote cryptographic models, significantly lowering risks of interception, unauthorized access, or user profiling.

Local execution is a natural enabler for decentralized digital identity models, as it ensures that cryptographic material remains under the exclusive control of the user. Sensitive data is neither centralized nor externally accessible, significantly reducing the attack surface and preventing systematic exploitation or large-scale compromise.

This architecture aligns closely with GDPR principles, including data minimization, purpose limitation, and privacy-by-design. By distributing sensitive credentials across user-controlled secure devices, the system avoids single points of failure and structurally limits the feasibility of mass data breaches, including those involving highly resourced adversaries.

Through Secure Element-based protection, privacy is not enforced solely through policy or contractual measures but is embedded directly into the technical architecture. This provides a robust and sustainable foundation for a long-term trust in the EUDIW ecosystem.

2.4. Offline Capability

SEs support secure wallet operations without any reliance on network connectivity, enabling the user to authenticate, present credentials, or sign transactions in fully offline scenarios. This capability is essential for real-world deployment and for guaranteeing universal accessibility, particularly in:

- Rural or remote areas with limited network coverage
- Cross-border travel contexts
- Emergency situations where networks may be unavailable
- Critical public services requiring resilience

Offline capability also reinforces privacy, as operations occur without contacting remote servers or transmitting metadata. This ensures that user behavior, usage frequency, or transaction patterns cannot be monitored by external parties, whether public or private.

In short, SE-enabled offline support is a cornerstone of inclusion, resilience, and autonomy for the EUDIW ecosystem.

2.5. Certification Reusability

Many Secure Elements are already certified under **EUCC/SOGIS** schemes at **EAL4+ with AVA_VAN.5**, representing one of the highest assurance levels suitable for mobile and citizen-scale deployments. These existing certifications provide a robust baseline for EUDIW, offering two key benefits:

- **Accelerated deployment** = By reusing proven, audited security components, Member States avoid lengthy and costly certification from scratch
- **Seamless transition to ENISA-led EU-wide schemes** = The existing evaluations, documentation, and security evidence can be leveraged as input for the future ENISA certification schemes foreseen under eIDAS2 (wallet security certification scheme). This ensures alignment with European certification frameworks and simplifies compliance for manufacturers and wallet providers

Leveraging pre-certified SEs reduces time-to-market, lowers certification costs, and ensures harmonized assurance levels across Member States, strengthening interoperability and trust.

3. Lifecycle Security: Maintenance and Update in EUDIW Certification

Security certification must extend beyond initial compliance to cover the full lifecycle of wallet components. The EUDIW framework must embed robust maintenance and update mechanisms to ensure long-term trust, adaptability, and operational continuity.

This includes:

- **Secure Update Mechanisms:** Certified components must support authenticated, integrity-verified updates to prevent tampering and unauthorized changes
- **Patch Management Policies:** The Implementing Act on certification sets a pragmatic precedent by mandating patch management obligations, establishing expectations for EUCC and future schemes

4. Clarifying Reference Points and Closing Gaps in EUDIW Guidance

The Architecture and Reference Framework (ARF), together with the work of ENISA and its ad-hoc working group (adhwg), provides an essential foundation for the security and certification of the European Digital Identity Wallet. However, several aspects remain insufficiently specified and would benefit from further clarification to ensure consistent interpretation, effective certification, and secure deployment across Member States.

In particular, the following gaps can be identified:

- **Operational definition of “full user control”** = While user “full control” is a core principle of the EUDIW framework, its operational meaning remains insufficiently defined. This leaves room for divergent interpretations across Member States and wallet implementations. This issue has already been highlighted in a previous Eurosmart position paper⁷ on security considerations for the EUDIW and remains a key point for achieving consistent assurance
- **Clear evaluation scope for combined or multi-component wallet architectures** = Current guidance does not sufficiently clarify how interactions between different security components involved in wallet architectures should be assessed as part of the certification target. In particular, security requirements governing authentication, secure communication, and trust relationships between wallet components need to be explicitly defined to ensure that the overall security of the system is preserved and coherently evaluated
- **Fine-grained access control and issuer policy enforcement within the wallet** = The ARF does not currently specify wallet functionality enabling differentiated access control to user attributes based on contextual conditions such as roles, rights, domains, or evidence presented. As the use of Relying Party Registration Certificates is optional, there is no systematic enforcement mechanism for issuer-defined access policies. In practice, sensitive domains such as healthcare, financial services, or corporate identity require fine-grained and enforceable access control rules to protect users and comply with regulatory constraints. Some entities may also act as both issuer and relying party, requiring selective application of policies depending on the context. Wallet-embedded policy evaluation capabilities, as described for example in prCEN/TS 18297, would allow such rules to be processed locally by the wallet before granting access. This functionality should be explicitly identified as part of the wallet building blocks and included within the scope of security evaluation

Clarifying these reference points would strengthen coherence across EUDIW implementations, reduce interpretation gaps between certification schemes, and support the deployment of secure, privacy-preserving, and interoperable digital identity wallets at European scale.

⁷ [Eurosmart | The voice of the Digital Security Industry | Eurosmart’s Position paper on Security considerations for the European Digital Identity Wallet](#)

5. EU Citizen Impact: Building Trust beyond Compliance

The success of the European Digital Identity Wallet (EUDIW) will be measured not only by technical compliance but by the confidence of every EU citizen. Trust is earned through transparency. Citizens deserve clear answers to fundamental questions:

How is my data protected? Your personal information is safeguarded by certified security mechanisms that meet the highest EU standards. Every cryptographic operation is anchored in tamper-resistant hardware and secure software layers.

How does certification guarantee security? Independent evaluations under EUCC and future ENISA-led schemes ensure wallets are tested against advanced attack scenarios - providing assurance that your data remains confidential and integrity is preserved.

What responsibilities do wallet providers carry? Providers must comply with the Implementing Act and national schemes, maintain secure update processes, and guarantee lifecycle support -so your wallet stays secure and up to date.

Where is my digital identity stored? Cryptographic keys reside inside a Secure Element (SE) - a certified hardware root of trust designed to resist tampering and protect cryptographic keys. In some architectures, secure execution environments like SAM complement this protection.

Who can access my data? Only you. Wallet design enforces user sole control: no third party can access your identity without explicit consent, and all operations are governed by strong cryptographic controls.

How does EUDIW comply with GDPR? Compliance is embedded in the architecture: data minimization, explicit consent, and secure processing are mandatory. Certification validates these principles, ensuring alignment with EU privacy law.

5.1. Rules and Responsibilities = Transparency required to build Trust

Wallet providers carry a critical responsibility: ensuring compliance with the Implementing Act 2024/2981 and all applicable national schemes until the ENISA-led certification framework becomes fully operational. But compliance alone is not enough - citizens must be informed in plain, transparent terms about what this means for them.

Key commitments that must be communicated clearly:

- **Data Sovereignty – Where and how is your personal data stored and protected?** Transparency on whether sensitive data resides in a Secure Element, a Secure Application Module, or other certified environments is essential to reinforce trust and sovereignty

- **Update and Support Commitments – How long will your wallet remain secure?** Providers must disclose lifecycle guarantees: update policies, and conditions for continued compliance, so users know their wallet won't become obsolete or vulnerable

This transparency is essential to build trust and ensure informed adoption across Member States.

5.2. Why an EUDIW Wallet built with a Secure Element is the most secure solution?

SE-based wallets offer tangible security benefits that directly impact citizens:

- **Hardware-Rooted Trust** = All cryptographic operations occur inside a tamper-resistant Secure Element, providing a physical root of trust that software alone cannot match
- **Proven Resistance to High-Potential Attacks** = SEs are certified under EUCC/SOGIS at EAL4 + AVA_VAN.5, ensuring resilience against high-potential threats, including sophisticated hardware and side-channel attacks
- **Privacy-by-Design** = Sensitive data stays local within the SE, minimizing exposure to external networks or cloud infrastructures, critical for GDPR compliance and user confidence
- **Resilient to large scale hacks** = By the decentralized nature of the EUDIW, large scale attacks by hackers with significant resources are not applicable
- **User Control and Consent** = With SE technology, private keys remain under the user's exclusive control. Every operation requires explicit consent, reinforcing sovereignty and trust
- **Offline more of operation** = Thanks to the SE technology and local implementation of the EUDIW within the User mobile device, the offline mode of operation is supported, enabling significant use cases where connectivity might be an issue (white zone, underground, busy connection, etc.)

Together, these features ensure that the EUDIW is not only compliant - but also secure, sovereign, and citizen-ready.

Conclusion and Call to Action

Europe cannot afford ambiguity. The SE approach – possibly combined with HSM in a hybrid deployment - is the only certifiable, scalable architecture to deliver EUDIW Security Level High, while preserving sovereignty, interoperability, and user trust.

Eurosmart calls for immediate regulatory action to:

Enable seamless WSCA integration within SE-based WSCD: The architecture must support direct binding of the Wallet Secure Cryptographic Application (WSCA) to the WSCD, whether the SE is embedded on the mobile device (e.g. eSIM, eSE, ...) or external (e.g. SE within an ID document, ...). This integration is critical for robust security, streamlined certification, and optimal user experience. SE-based models allow wallet logic and cryptographic operations to be executed within certified, tamper-resistant environments, maximizing both security and usability.

Mandate modular certification pathways: Certification strategies should be tailored to the deployment context, enabling modular evaluation of SE, and where needed coupled with CSP, and SAM components. Leveraging existing EUCC/SOGIS certifications for SEs (regardless of format) will accelerate deployment and facilitate transition to ENISA-led EU-wide schemes.

Strengthen Strategic control and autonomy and strategic autonomy: By anchoring cryptographic operations and sensitive credentials within locally managed, certified hardware, Member States retain direct control over trust anchors and wallet logic. This empowers governments to enforce national security policies, ensure compliance with EU regulations, and minimize reliance on foreign device manufacturers or cloud service providers, thereby strengthening strategic control and autonomy and reducing exposure to extraterritorial risks.

Ensure Privacy, Usability, and Inclusion: SE-based architectures enable privacy-preserving operations, offline capability, and strong user control. These features are essential for building citizen trust, supporting GDPR compliance, and ensuring that digital identity solutions are accessible to all EU citizens.

Issue clear, harmonized guidance from ARF and ENISA, now: Immediate action is needed from the Architecture Reference Framework (ARF) and ENISA to provide clear, harmonized guidance for EUDIW certification and deployment. This will prevent fragmentation, ensure legal certainty, and support consistent implementation across Member States - safeguarding the credibility and future resilience of Europe's digital identity ecosystem. Regardless of the type of architecture used for EUDIW, the SE shall be at the core of it to ensure high level of security and privacy.

***Act decisively.** The credibility of Europe's digital identity ecosystem - and its strategic autonomy - depends on it.*

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.



www.eurosmart.com



@Eurosmart_EU



@Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 471 34 59 64 | mail Contact@eurosmart.com