

GlobalPlatform Technology: The Cornerstone of Trust and Interoperability for the European Union Digital Identity Wallet

White Paper

February 2023

GP_WPR_141

eID Wallet Task Force

Contents

Executive Summary	3
The European Union Digital Identity (EUDI) Wallet	3
Overview of EUDI Wallet	3
GlobalPlatform Secure Components and the EUDI Wallet Framework	5
The EUDI Wallet Trustworthiness: Assurance Levels	6
GlobalPlatform	7
GlobalPlatform Core Technologies	7
GlobalPlatform Secure Elements	8
Overview of Secure Elements	8
Embedded Secure Elements	9
Embedded UICC	10
GlobalPlatform Interoperable Framework for Accessing and Managing Secure Elements	11
GlobalPlatform Certification	12
GlobalPlatform SESIP Methodology	12

Executive Summary

The European Union Digital Identity (EUDI) Wallet is a new digital identity solution on mobile devices that will provide a secure and convenient way for citizens to prove and share identity information throughout Europe. The EUDI Wallet will be used to access a wide range of online and offline services and transactions across the European Union. As such, it is important that the EUDI Wallet has been thoroughly tested and found interoperable, secure, and reliable.

GlobalPlatform has successfully developed several technologies for creating trustworthy devices and digital services and has demonstrated their interoperability. These technologies are available on the vast majority of mobile phones and can provide the foundations for trust and interoperability of the EUDI Wallet, regardless of the underlying wallet attribute or data model.

The compliance program of GlobalPlatform ensures the interoperability of its secure components, which are deployed on a range of form factors that can fit different needs of EUDI Wallet implementations.

GlobalPlatform supports the industry by developing generic security protection profiles per type of product and has developed several protection profiles for Common Criteria certification of Secure Components to demonstrate their high level of security. As such, GlobalPlatform technology will enable EUDI Wallet implementations to support the highest assurance security requirements when the ENISA certification scheme for the EUDI Wallet is defined.

GlobalPlatform technology is widely used in the identity segment and mobile phone security and will most likely play a major role in the EUDI Wallet. GlobalPlatform is committed to support the future of Digital Identity and is looking forward to help successfully implement and deploy the EUDI Wallet, as well as participate in defining security requirements and architecture, and develop technical and interoperability specifications for a better standardization of the Wallet if needed. GlobalPlatform technology can help decision makers meet the security challenges required by an ambitious project like the EUDI wallet, and give options to regulators based on GlobalPlatform experience.

The European Union Digital Identity (EUDI) Wallet

Overview of EUDI Wallet

In June 2021, the European Commission adopted a new proposal for a Regulation on a European Digital Identity, eIDAS 2, which is an evolution of the 2014 eIDAS (electronic IDentification, Authentication and trust Services) regulation that laid down the necessary foundations to safely access services and carry out transactions online and across the borders of the European Union.

With this new regulation, each of the twenty-seven member states will have to issue a digital identity wallet with a scheme recognized and accepted by the other member states, built on common technical standards, and with early pilots in 2024.

The objective of this new regulation is to ensure universal access for people and businesses to secure and provide trustworthy electronic identification and authentication using a personal digital wallet on a mobile phone.

The EUDI Wallet will provide citizens a secure and convenient way to prove their identities and share identity information with public and private online and offline services throughout Europe. This Wallet is intended to be a mobile-first system, meaning that it will primarily be accessed through mobile devices such as smartphones. The Wallet will be issued by member states or entities under their control, and it will allow users to select and share verifiable attributes with relying parties. The attributes shared online or offline will be under the sole control of the user. The EUDI Wallet will also allow for qualified electronic signatures, which can be used to electronically sign documents and transactions, as well as provide strong user authentication for online services.

GlobalPlatform provides widely accepted technologies that already enable high security for mobile devices, electronic identity documents, and applications—technologies that can bring trust, interoperability, and security to the EUDI Wallet.


Who is GlobalPlatform


GlobalPlatform is a member-driven organization that develops frameworks for creating trustworthy devices and digital services, including technologies found in mobile devices, such as secure elements and Trusted Execution Environments (TEE). GlobalPlatform core technologies are used to secure billions of mobile phone devices, electronic identity documents, payment cards, and other devices, and are very much relevant to the European Union Digital Identity (EUDI) Wallet.


GlobalPlatform develops and publishes functional and security specifications around these core technologies and maintains certification programs to ensure that products and services using these technologies meet certain standards. GlobalPlatform has over 90 member companies and works with a network of 11 accredited labs and 68 test suites to ensure the interoperability and security of its technologies.

GlobalPlatform’s goal is to create a Chain of Trust that protects both devices and digital services, and to provide service providers with the tools and frameworks they need to build secure and trustworthy systems.

GlobalPlatform is a member-driven technical community

- 

Common Goal
Our members have a common goal to develop GlobalPlatform’s specifications
- 

Established Standards
Over 200 specifications and technical documents available
- 

Successful Collaboration
20 years of implementations

Membership

2,600

Representatives from

90+


Member companies

4

Task Forces
provide strategic requirements and use cases in alignment with

34

Industry Partners



GlobalPlatform Technology is developed by

3

Technical Committees with

14

Working Groups

GlobalPlatform Secure Components and the EUDI Wallet Framework

The European Commission mandated the eIDAS expert group to develop a Toolbox, including an Architecture Reference Framework (ARF), to define common standards and specifications of the EUDI Wallet. Among other things, the ARF defines the roles, actors, and interfaces of the EUDI Wallet, as well as the underlying data models.

GlobalPlatform technologies are generic and already used to secure various applications on mobile phones, such as payment, connectivity, and digital car keys. Whenever the member states or implementer chooses to build an ARF-compliant wallet, GlobalPlatform can provide an interoperable and certifiable security foundation. In particular, GlobalPlatform can support any chosen attribute or data model, such as the one defined in ISO/IEC 18013-5/23220 or the W3C Verifiable Credentials Data Model specification.

Besides mobile application security, GlobalPlatform also provides secure protocols to remotely provision and manage sensitive applications and data, as well as update and maintain security of these applications on the field. These protocols will provide EUDI Wallet applications end-to-end security to provision the applications, sensitive data, and cryptographic material used by the EUDI Wallet.

GlobalPlatform secure components are certifiable for hosting sensitive applications and data of the EUDI Wallet. GlobalPlatform also operates a compliance program to ensure interoperability of secure components. GlobalPlatform secure components are used in several certification schemes to the highest level of security, including GlobalPlatform’s own security certification schemes.

GlobalPlatform’s interoperability, compliance program, and certifiable components provide national and European authorities an approach to both interoperability and security certification.

GlobalPlatform Certification Program

<p>The GlobalPlatform Certification confirms product adherence to functional requirements and market defined security thresholds</p> <p>Device Manufacturers can:</p> <ul style="list-style-type: none"> • Market products as meeting digital service provider needs • Prove that their digital service management capabilities meet security requirements <p>Service Providers have:</p> <ul style="list-style-type: none"> • Reassurance that certified products meet their needs <div style="display: flex; justify-content: space-around; align-items: center;">   </div>	<div style="text-align: center;"> <p>CERTIFICATION PROGRAM</p> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: center;">  <p>11 Accredited Labs</p> </div> <div style="text-align: center;">  <p>68 Test Suites</p> </div> <div style="text-align: center;">  <p>175 QUALIFIED PRODUCTS</p> </div> </div> <div style="margin-top: 20px;">  <ul style="list-style-type: none"> • Dedicated Certification Secretariats • Independent Program • Internationally Recognized </div> </div>
---	---

The EUDI Wallet Trustworthiness: Assurance Levels

The ambitious scope of use cases for the EUDI wallet, the wide range of services it is meant to support, as well as the sensitive nature of its contents, call for a careful design and testing of its security and reliability. In this sense, the European Commission proposes its certification to a high level of security.

The EUDI Wallet will be used to access a wide range of online and offline services and transactions. As such, it is important that it has been thoroughly tested and found to be secure and reliable. The concept of level of assurance is often used to evaluate the security of a product, and the European Union Cybersecurity Act defines three assurance levels for certification schemes as high, substantial, and basic.¹

The European Union Agency for Cybersecurity (ENISA) is responsible for defining the certification schemes for a particular technical domain, such as 5G or Cloud, and will be in charge of defining the certification scheme of the EUDI Wallet.

The secure storage of sensitive wallet data, as well as the storage and execution of cryptographic material, will most likely require a high level of assurance as defined in the EU Cybersecurity Act.

Whenever the EUDI Wallet certification scheme is published, GlobalPlatform secure components will be able to meet the highest assurance security requirements as is already the case in other domains.

GlobalPlatform has defined Protection Profiles for Secure Elements and Trusted Execution environments. These Protection Profiles help define the security of secure components and will enable the certification of the wallet-secure components as soon as the ENISA Wallet certification scheme is defined.

For example, GlobalPlatform secure elements are already certified under the EUCC Certification Scheme levels with the AVA_VAN 5 component, and GlobalPlatform trusted execution environment at CC levels with the AVA_VAN 3 component.

Evaluating Security Assurance

Common Criteria (CC) is an evaluation methodology that is an internationally recognized standard for evaluating the security of information technology products. The CC certification scheme is used to certify that IT products meet certain security requirements and can be trusted to protect against threats such as unauthorized access, tampering, or data loss.

AVA_VAN stands for "Assurance Validation and Verification Assurance Level," and it is used to describe the level of security assurance provided by an IT product. The AVA_VAN levels range from 1 to 5, with higher numbers indicating a higher level of security assurance.

AVA_VAN 3 indicates a basic level of security assurance, ensuring protection against attackers with an enhanced-basic potential, while AVA_VAN 5 indicates a higher level of security assurance, ensuring protection against attackers with a high potential. This means an IT product that has been certified at AVA_VAN 5 has undergone a more rigorous evaluation process and has been found to provide a higher level of security than an IT product that has been certified at AVA_VAN 3.

¹ The CSA levels of assurance are not to be confused with the eIDAS regulation Levels of Assurance (LoAs), which characterize the degree of confidence in electronic identification methods.

GlobalPlatform

GlobalPlatform Core Technologies

The Secure Element, the Trusted Execution Environment, the Trusted Platform Services, and the Device Trust Architecture are GlobalPlatform's core technologies for creating trustworthy devices and services. These technologies are used to secure billions of mobile phone devices, electronic identity documents, and payment cards.

Together, these core technologies provide trust anchors for both the operating systems and for various use cases such as connectivity, payment, digital car keys, and digital rights management.

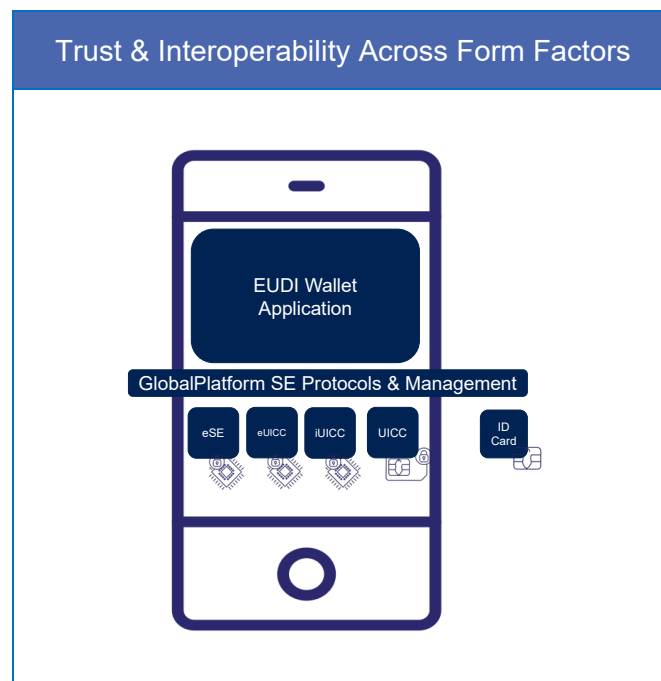


GlobalPlatform Secure Elements

Overview of Secure Elements

GlobalPlatform Secure Elements are tamper-resistant platforms used to host applications and confidential and cryptographic data. Secure Elements are widely deployed in different form factors on smartphones, including removable SIM cards (UICC), embedded Secure Elements (eSE), embedded SIM (eUICC), and integrated SIM (iSIM). All these secure elements are implemented and certified according to GlobalPlatform specifications, thus providing trust and interoperability on a wide range of form factors.

The EUDI Wallet can benefit from the large installed base of Secure Elements to secure sensitive data and applications in the mobile phone. Moreover, GlobalPlatform Secure Elements are also widely deployed in electronic passports, electronic identity cards, and electronic identification methods, and can provide secure onboarding of the user's identity within the Wallet, or to support the Wallet in achieving electronic identification and authentication, in line with the requirements of a high level of assurance (LoA) as defined by the EU's eIDAS regulation when the Wallet cannot rely on a secure element within the mobile phone.



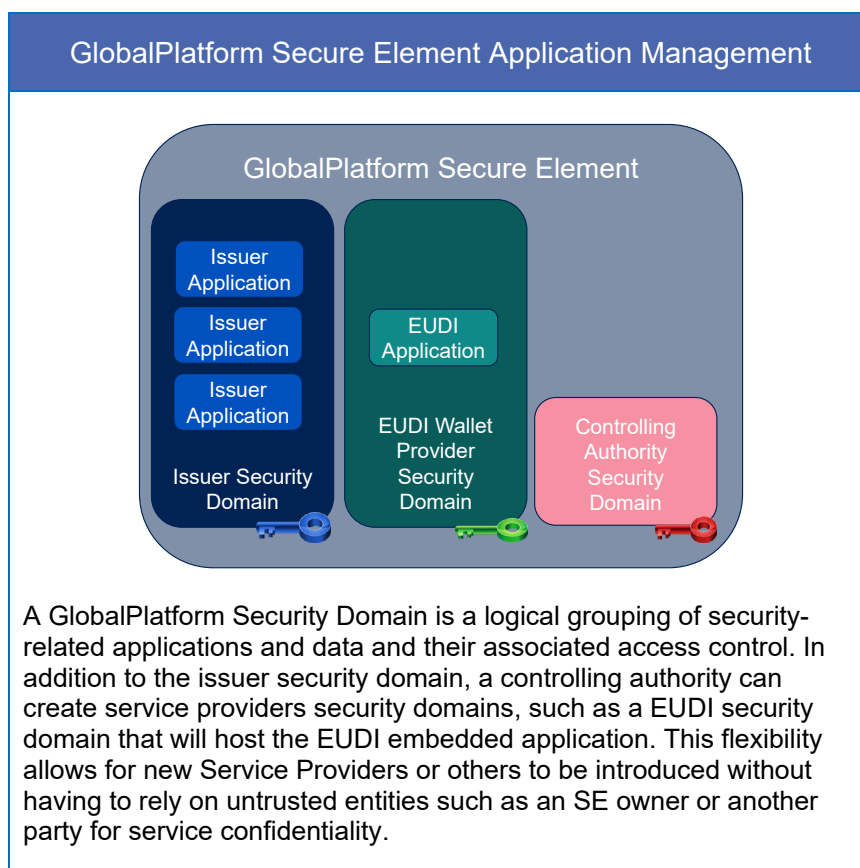
Embedded Secure Elements

Most current smartphone devices include a GlobalPlatform-compliant embedded Secure Element (eSE) that provides security to the smartphone operating system and applications. These eSEs are part of various use cases that require a high level of security, such as payments and digital car keys.

These eSEs are certified using Common Criteria or proprietary methods to a high level of assurance, such as AVA_VAN 5, with protection profiles and schemes that vary depending on the use case, such as EMVCo for payment applications.

The EUDI Wallet developers can use eSE to host the sensitive code and data of the Wallet application. These embedded Wallet applications, typically Java Card applets, can be certified to a high level of security using Common Criteria or any other scheme that will be selected by the ENISA. GlobalPlatform developed to the extent the Secure Element Protection Profile aimed to secure components implementing Java Card and GlobalPlatform Card Specifications.²

In the case of a smartphone with an embedded SE, the phone manufacturer acts as the Verification Authority that will ultimately manage the applications loaded on the secure element. This management can be performed directly or delegated to an external Controlling Authority.



² GlobalPlatform Technology Secure Element Protection Profile, GPC_SPE_174

Embedded UICC

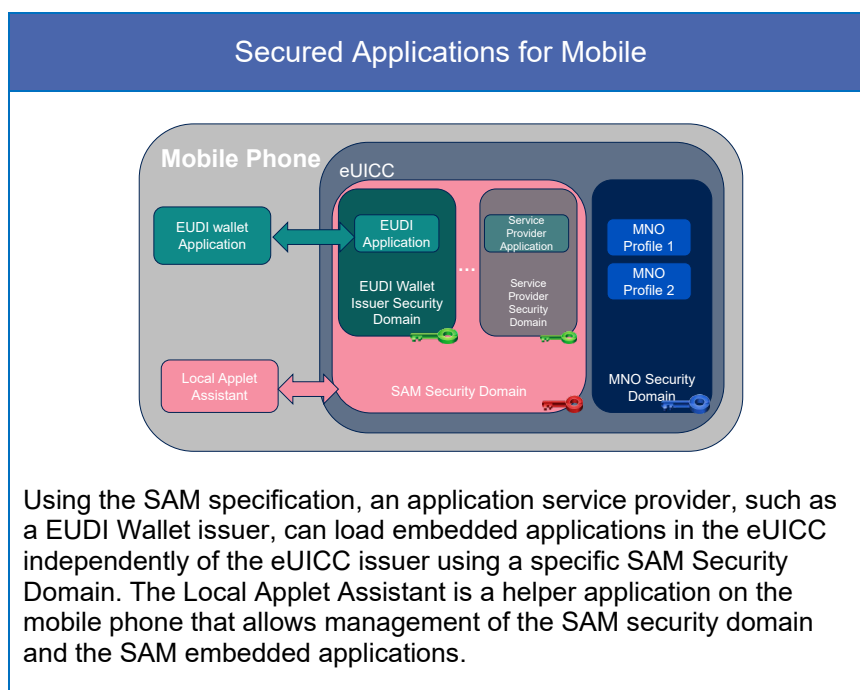
The traditional SIM Card (UICC) is increasingly being replaced by embedded UICC (eUICC) in the smartphone, and more recently by integrated UICC (iUICC). It is expected that eUICC and iUICC will soon outgrow removable UICC in terms of volume.

The eUICC is standardized by the Global System for Mobile Communications Association (GSMA), which defined the Remote Subscription Provisioning (RSP) set of specifications. RSP defines how to securely provision UICC with mobile network operator connectivity credentials and profiles. The GSMA also defined a security assurance scheme, allowing the eUICC to demonstrate high resistance to attacks. This eUICC Security Assurance (eSA) scheme is based on Common Criteria protection profiles BSI-CC-PP-0100 and BSI-CC-PP-0089-2015.

As it is anticipated that the eUICC will be present in a vast majority of smartphones, the GSMA has issued a new requirement specification called Secured Applications for Mobile (SAM) that allows third-party application providers to install and manage applets on the eUICC independently of the mobile network operator profiles.

GlobalPlatform will publish a SAM configuration specification to support the GSMA requirements for SAM. This will allow service providers, such as EUDI Wallet issuers, to host the applications and sensitive data within the eUICC secure component. As with the GSMA RSP specification, the EUDI Wallet applet and secure component can be certified to a high level of security using Common Criteria or any other scheme selected by the ENISA.

In the case of the GSMA RSP, the GSMA operates a verification authority to verify the applet security and authorize loading of profiles on the eUICC. In the same way, the EUDI Wallet issuance will need a Verification Authority to verify the security of the EUDI and authorize application loading, as well as for a Certification Authority to certify EUDI Wallet applets loaded onto the eUICC.



GlobalPlatform Interoperable Framework for Accessing and Managing Secure Elements

GlobalPlatform provides an interoperable and secure framework where wallet issuers can deploy, access, and manage wallet application and sensitive data in secure elements; this framework is interoperable and supports both secure elements in external devices such as electronic documents, and those embedded in the smartphone, in which case embedded wallet applications can be managed independently of the smartphone issuer.

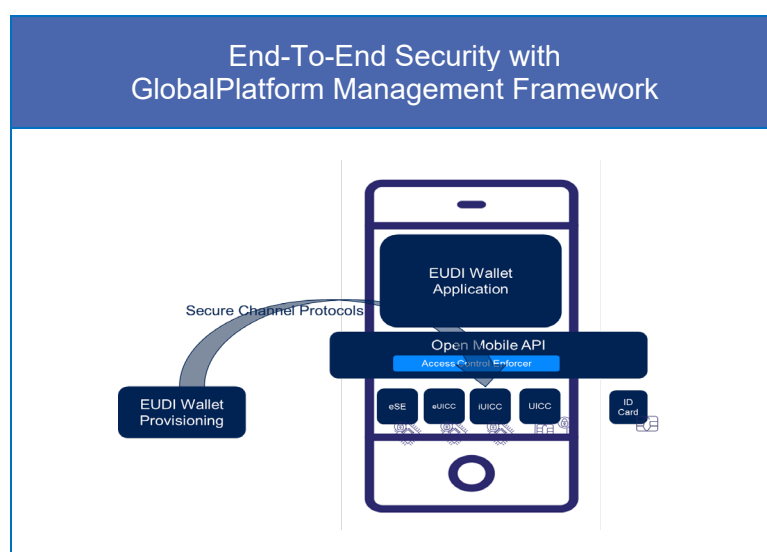
GlobalPlatform standardized the Open Mobile API specification³ to access the Secure Element from selected device applications, and this API is included on all Android smartphones. This API also includes access control specifications to restrict access to the Secure Element to only select applications.

For end-to-end security, GlobalPlatform also developed several secure channel protocols to manage the lifecycle of SE, SE applications and data, as well as to allow service providers to secure server-to-secure-element communications.

EUDI Wallet applications can benefit from this interoperable framework to install secure anchors on the secure elements as applets that will secure sensitive data and operations.

The provisioning of credentials and data for the EUDI Wallet can be secured by the management framework of GlobalPlatform. GlobalPlatform Secure Components operating systems and applets can be securely updated post-issuance to meet requirements of the Cybersecurity Act (CSA) regarding security updates to maintain the security level.

GlobalPlatform's interoperable framework is also applicable to GP compliant external electronic passport, electronic identity cards, and electronic identification methods. As such, external electronic passports, electronic identity cards, and electronic identification devices can be accessed securely using GlobalPlatform secure channel protocols by the Wallet application, providing end-to-end security with backend servers, for use cases such as electronic identification, authentication, and onboarding within the Wallet.



³ GlobalPlatform Technology Open Mobile API Specification Version 3.3, GPD_SPE_075

GlobalPlatform Certification

GlobalPlatform operates functional certification programs, enabling stakeholders to verify product adherence to the association's technical specifications and market-specific configurations, and ultimately to ensure complete interoperability across suppliers. As such, it ensures a large panel of suppliers, avoiding any vendor lock-in. This certification program is supported by several organizations such as ETSI, GSMA, and EMVCo for connectivity or payment use cases.

GlobalPlatform supports the industry by developing generic security protection profiles per type of product and based on industry needs.⁴ In particular, GlobalPlatform has developed a protection profile for Common Criteria certification of Secure Elements to demonstrate their high level of security. GlobalPlatform technology, having met the highest levels of assurance for the security schemes of different market segments such as payments and telecommunications, can surely provide the trust architecture needed by regulators like ENISA to bring the highest assurance to the EUDI wallet.

GlobalPlatform SESIP Methodology

GlobalPlatform developed the SESIP evaluation methodology, a flexible and efficient security evaluation methodology to address the unique complexities and challenges of the evolving Internet of Things (IoT) ecosystem. SESIP is a candidate to become a European Norm (EN) under CEN/CENELEC.

Although SESIP focuses on the IoT platform, it can be extended to certify a device by adding specific business-related features in an SESIP Profile. As such, the SESIP methodology can provide the basis for certification by composition of complex applications such as the EUDI Wallet. The SESIP flexible composition model can simplify the certification by composition of whole or part of the EUDI Wallet.

⁴ For example, GlobalPlatform SE, TEE, and MCU protection profiles.