



**Global  
Platform®**

Securing the digital future

# **GlobalPlatform Annual Report 2025**





# Contents

<b>Letter from the Chair of the Board</b>	<b>02</b>
<b>Letter from the Executive Director</b>	<b>03</b>
<b>GlobalPlatform Technology Deployments</b>	<b>04</b>
<b>GlobalPlatform Executive Team &amp; Board of Directors</b>	<b>06</b>
<b>Securing the Digital Future</b>	<b>08</b>
<b>Global member representation</b>	<b>09</b>
<b>Our Technology</b>	<b>10</b>
<b>Strategic Focus Areas</b>	<b>11</b>
<b>Our Work</b>	<b>12</b>
<b>Our Services</b>	<b>22</b>
<b>Emerging Topics</b>	<b>25</b>
<b>The Value of GlobalPlatform Membership</b>	<b>26</b>
<b>Membership Companies and Organizations</b>	<b>27</b>
<b>Industry Partners</b>	<b>28</b>
<b>Member Testimonials</b>	<b>29</b>



# Letter from the Chair of the Board

This year, GlobalPlatform advanced its mission to secure digital services and build trust across connected ecosystems. As connected technologies scale rapidly, we expanded into new markets and developed specifications, frameworks, and partnerships that ensure security and interoperability.

**Highlights from the past 12 months include:**

- **Enabling the future of digital life:** Our technologies are being deployed across an increasing number of use cases, spanning digital identity, finance, automotive and travel. This includes emerging digital ID schemes such as the European Union Digital Identity (EUDI) wallet, where we are providing the secure foundations for digital payments and identity.
- **Advancing Digital ID with new technologies:** GlobalPlatform developed two key configurations for secure digital ID deployment: Secure Application for Mobile (SAM) and the Cryptographic Service Provider (CSP). SAM standardizes the deployment of ID applets on Secure Elements (SEs), while the GlobalPlatform CSP enables applets to be certified once and used across any EUCP-certified platform.
- **Driving automotive security alignment:** The Automotive Task Force made significant strides in understanding Software Defined Vehicle (SDV) requirements and aligning security compliance across the automotive supply chain. New global OEMs and key ecosystem players joined GlobalPlatform to accelerate delivery of new automotive solutions.

- **Advancing CRA readiness via SESIP:** Europe's Cyber Resilience Act (CRA) came into force and IoT manufacturers are adopting SESIP as a cost-effective method to demonstrate conformance. SESIP provides a proven methodology for conducting security evaluations across products and supply chains. We also added new Certification Bodies (CB) and Laboratories and expanded into new verticals.
- **Strengthening engagement in China:** We signed MoUs with both China's National Financial Technology Certification Center (NFTC), paving the way for SESIP adoption across China's IoT sector; and also the Global Computing Consortium (GCC) to collaborate with the confidential computing ecosystem.

As industries and regulations evolve, GlobalPlatform remains uniquely positioned to lead with agility, collaboration, and expertise.

I would also like to recognize the invaluable contributions of all our members in helping us create a community of security experts to support our mission.



*Stéphanie El Rhomri*

**Stéphanie El Rhomri**  
Chair of the Board

# Letter from the Executive Director

GlobalPlatform's mission is clear: to enable secure, interoperable, and trusted digital services. As connected technologies grow, we continue to unite stakeholders around standardized security frameworks that simplify compliance and fuel innovation. Looking ahead, we aim to deepen technical alignment, expand use cases, and accelerate adoption across critical sectors—made possible through collaboration and a shared commitment to trusted digital infrastructure.

**Our strategic priorities moving forward include:**

- **Harmonizing IoT labeling and conformance:** We are aligning the IoT industry (such as the PSA Certified ecosystem) around one security evaluation methodology that can be re-used in multiple security schemes. This work will reduce fragmentation and simplify compliance, giving stakeholders a more consistent path to demonstrate security levels of connected products.
- **Scaling remote attestation:** GlobalPlatform is collaborating with other industries based on IETF RATS to support scalable attestation models based on root of trust that verify device integrity across sectors.
- **Future isolated technologies:** GlobalPlatform is working to adapt its root of trust technologies to respond to different needs and operational environments by providing innovative solutions such as MicroTEEs and CSP.
- **Evolving SE technologies to support PQC:** Building on the new card specification release, we continue to work on the future need to address post-quantum requirements, ensuring resilience for Secure Elements used in payment, mobile, identity and IoT.

- **Supporting CRA compliance with SESIP:** In supporting industries to conform with the CRA, we continue to align the cybersecurity ecosystem behind SESIP as a flexible, component-based certification methodology that reduces duplication and supports scalable regulatory alignment.
- **Supporting the future of eID wallets and digital currencies:** We are committed to evolving Secure Element technologies to meet the requirements of government and central banks.
- **Advancing automotive security:** We're deepening engagement with auto OEMs and suppliers to meet fast-evolving cybersecurity requirements and deliver technologies that will facilitate the migration towards the Software Defined Vehicle.

We invite you to collaborate with GlobalPlatform as we build the next generation of trusted digital infrastructure.



*Ana Tavares Lattibeaudiere*

**Ana Tavares Lattibeaudiere**  
Executive Director



# GlobalPlatform Technology Deployments

GlobalPlatform technologies secure the digital economy, with over 95 billion devices worldwide using its certified Secure Elements (SEs) and Trusted Execution Environments (TEEs) to protect transactions, authentication, and sensitive data.

 Secure Elements

**80 billion+**

GlobalPlatform SEs shipped in smartphones, smartcards, and IoT devices, providing a tamper-proof solution for digital transactions and cryptographic processing

 Trusted Execution Environments

**15 billion+**

devices shipped with GlobalPlatform TEEs, creating an isolated environment that enables secure payment, biometric authentication, content protection, and more

# GlobalPlatform technology is used by billions of consumers every day:



**9 billion+**

active SIMs authenticating users and devices on mobile networks



**13 billion+**

active bank cards providing secure, flexible payment experiences



**1.1 billion+**

electronic passports and identity documents issued by governments



**\$1.6 trillion+**

of contactless payments processed using GP TEEs on smartphones in 2024



**400 million**

secure components following GP standards deployed in vehicles to date - representing an increase of almost 40% since the chip shortage of 2021



# GlobalPlatform Executive Team & Board of Directors

The Executive Team is responsible for the development and adoption of GlobalPlatform's technical specifications, driving awareness and understanding of our work and managing day-to-day operations.



**Ana Tavares  
Lattibaudiere**  
Executive Director



**Gil Bernabeu**  
Chief Technology Officer



**Tono Aspinall**  
Operations Director



**Francesca Forestieri**  
Head of Automotive



**Bonnie Martin**  
Operations Manager

As a member-led organization, GlobalPlatform is governed by a Board of Directors that consists of eleven representatives from GlobalPlatform's Full Member companies. The Board develops and oversees the execution of GlobalPlatform's strategy in support of its vision and mission.



**Stéphanie El  
Rhomri**  
GlobalPlatform Chair,  
FIME



**Olivier Van  
Nieuwenhuyze**  
GlobalPlatform  
Vice Chair,  
STMicroelectronics



**Jürgen  
Hirschinger**  
GlobalPlatform  
Treasurer and  
Secretary,  
G+D



**Rob Coombs**  
ARM



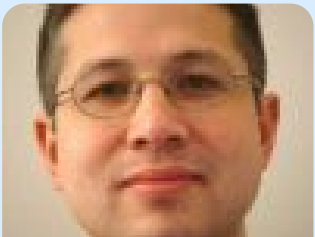
**Eikazu Niwano**  
NTT Corporation  
*\*retired March 31st*



**Sebastian Hans**  
Oracle



**Jeremy  
O'Donoghue**  
Qualcomm



**Guillaume Phan**  
Thales



**Scott Migaldi**  
T-Mobile USA



**Richard Hayton**  
Trustonic



**Marc Kekicheff**  
Visa Inc.





# Securing the Digital Future

**GlobalPlatform is building the foundation for a secure, trusted, and interoperable digital future.**

By establishing and driving adoption of leading-edge standards, we empower governments, organizations, and industries to deliver secure devices and innovative services with confidence, enabling users to engage in a digital ecosystem built on privacy, security, and trust.



## Technology

**Delivering leading-edge, standards-based security technology**

From banking chip cards to mobile devices to e-passports, GlobalPlatform secures critical digital services and personal data.



## Industry

**Deploying secure devices and services across industries**

GlobalPlatform's security technologies, which revolutionized banking and mobile, are now ready to support every industry on their path to digitalization.



## Certification

**Certifying digital technologies to meet evolving regulations**

GlobalPlatform provides the tools and frameworks for high-quality, independent certifications, enabling governments, businesses, and consumers to trust digital technology and use it with confidence.

# Global member representation

**GlobalPlatform membership unites key stakeholders across the digital ecosystem to foster a collaborative approach to security and certification.**





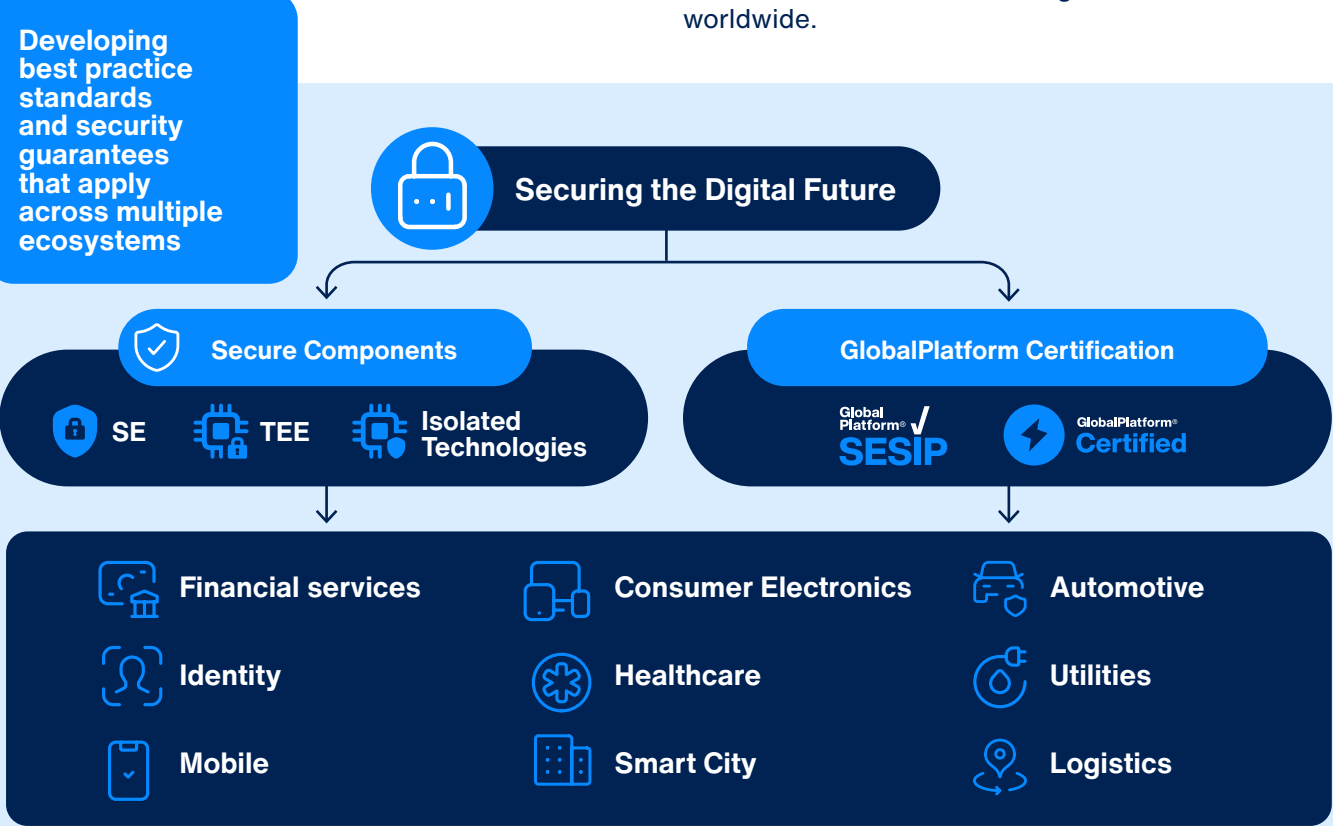
# Our Technology

## GlobalPlatform is securing the digital future through a combination of security standardization and certification

GlobalPlatform is securing the digital future through secure components and certification frameworks that deliver best practice standards and security guarantees. This enables vendors to reduce the cost of security without compromising quality. GlobalPlatform defines and maintains foundational technologies (SEs and TEEs) that protect digital services today while developing the solutions of tomorrow. Its vendor-neutral standards serve as the backbone for secure, scalable, and interoperable systems, and are also referenced by a variety of standards organizations and industry bodies—including the Car Connectivity Consortium (CCC), EMVCo, GSMA, ETSI, NIST, PSA Certified, OSIA, and ISO—to ensure consistency across technologies and markets.

Proven in mobile and banking, GlobalPlatform technologies now support digitalization in government, healthcare, automotive, and industrial IoT. Secure components protect critical data within the device, enabling seamless and trusted interactions. Certification frameworks such as SESIP and GlobalPlatform's security schemes validate that products meet the highest benchmarks—building trust, simplifying compliance, and lowering costs.

Developed openly and independently, GlobalPlatform standards give stakeholders sovereignty and flexibility while helping future-proof against emerging threats like quantum computing and AI. From secure identity in public services to the EUDI wallet, GlobalPlatform is a vital bridge between devices and services that foster trust and accelerate secure digital transformation worldwide.



# Strategic Focus Areas

## Automotive

GlobalPlatform has aligned our technical roadmap to protect the hardware and software of SDVs.

Modern vehicles are facing growing cybersecurity risks and are being required to comply with strict emerging regulations, thus creating a need for standardized, certifiable security solutions. GlobalPlatform is bridging the gap between regulatory requirements and real-world implementation. We have mapped our SE and TEE specifications directly to SAE J3101 hardware protected security environments, enabling automakers and suppliers to meet nearly 100% of J3101 via GlobalPlatform standardized solutions. Additionally, security certification through SESIP allows the automotive ecosystem to demonstrate compliance to hardware-security criteria and at the same time, we are working to provide certification for software as we develop SESIP profiles for ECUs.

## eID Wallet

GlobalPlatform is committed to working with industry stakeholders and government regulators in preparing for the deployment of digital wallets globally.

GlobalPlatform is playing a key role in securing EUDI wallets by providing mature, standardized technologies (i.e., SEs) that protect sensitive identity data within user devices. Our specifications enable strong, hardware-based security, trusted application management, and seamless interoperability, helping ensure that eID wallets meet the highest requirements for privacy, authentication, and data integrity. As part of its commitment to supporting digital identity initiatives globally, GlobalPlatform continues to evolve its specifications to address emerging needs to support the secure deployment of digital wallets around the world.

## Security Evaluation Standard for IoT Platforms (SESIP)

The SESIP methodology offers component manufacturers and device makers the ability to deliver software and hardware security at scale.

As European standard EN 17927, SESIP enables a component-based, reusable approach to security evaluation—allowing manufacturers to demonstrate conformance with key regulations like the EU Radio Equipment Directive (RED) and the upcoming CRA. By building with SESIP-certified components, organizations can reduce redundant testing and accelerate time-to-market.

Recognized by standards bodies such as ETSI, NIST, and ENISA, SESIP offers a scalable, risk-based path to compliance that supports innovation while ensuring robust security in connected devices.



# Our Work



GlobalPlatform standardized technologies and certifications are developed through cross-industry collaboration across our technical committees and task forces. This work is led by diverse member companies working in partnership with industry and regulatory bodies.

## Innovation through collaboration

### Our Committees

Where technology is developed to address emerging market requirements and innovations. Participation in our committees is open to full and participating members.



**Secure Element Committee**

#### Working Groups

SE Security  
SE Specification  
SE Compliance



**SESIP Committee**

#### Working Groups

Ecosystem Adoption  
Governance  
Technical  
Automotive



**TES Committee**

#### Working Groups

TES Platforms  
TES Compliance  
TES Security  
TES Services

### Our Task Forces

Where requirements are gathered to determine impact to our technology roadmap. Participation in our task forces is open to all members.



**Automotive Task Force**



**Security Task Force**

(Crypto, Software  
Attack Expert, xBOM)



**eID Wallet Task Force**



**Regional Task Forces**

**China**



**Regional Task Forces**

**Japan**



## Secure Element Committee



Chair:  
**Guillaume Phan**  
Thales

**THALES**

### Mission & Objectives

The SE Committee defines specifications for the secure deployment and lifecycle management of applications on Secure Elements (e.g., eSE, UICC, smart cards). It maintains technical standards, promotes certification, and supports collaboration with industry bodies to ensure interoperability and trusted device security across markets.

### Key Initiatives

- **Secure Application on Mobile (SAM):** Enables secure app deployment on eSIM/eSE with support from GSMA and MNOs.
- **OS Updates:** Defines standardized SE OS update processes to meet regulatory requirements like EUCC.
- **IoT Root of Trust:** Expands SE use in IoT, adding support for common hardware interfaces and secure remote management.
- **FIDO Integration:** Aligns SE Protection Profiles with FIDO Level 3+ certification for strong authentication.
- **Post-Quantum Readiness:** Prepares SEs for future cryptographic challenges with agile, quantum-resistant protocols.
- **European Union Digital Identity (EUDI):** Supports secure, device-agnostic deployment of digital wallets using SAM and Cryptographic Service Providers.



### Specifications published this year:

- Secure Element Protection Profile and extensions v2.0 (July 31, 2025)
- Secure Channel Protocol '04'; Card Specification v2.3 - Amendment K (June 30, 2025)
- Protection Profile for FIDO2 SE v1.0 (March 24, 2025)
- GlobalPlatform Card API v1.8 (March 18, 2025)
- Secure Element Management Service – Amendment I v1.2 (October 22, 2024)

### Impact

The SE Committee delivers trusted, certifiable technology that secures sensitive data across industries—from mobile and IoT to identity and automotive. Its work strengthens interoperability, compliance, and innovation, positioning secure elements as a foundation for digital trust.

## SESIP Committee



Co-Chair:  
**Georg Stütz**  
NXP Semiconductors

**NXP**



Co-Chair:  
**Philippe Gaudillat**  
STMicroelectronics

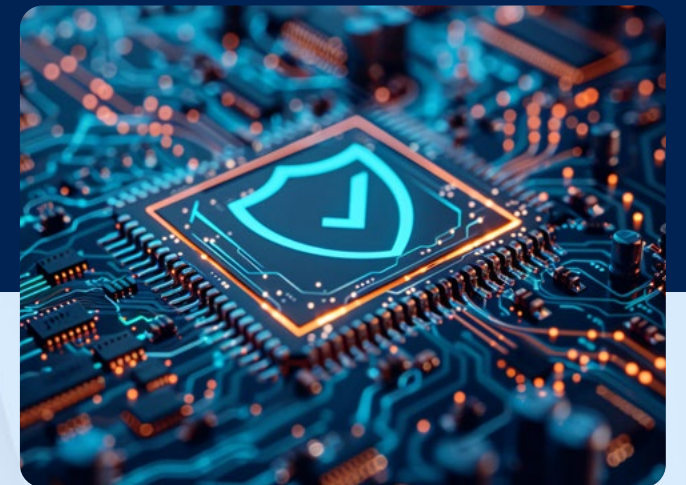
**ST** life.augmented

### Mission & Objectives

The SESIP Committee drives the global adoption of the **Security Evaluation Standard for IoT Platforms (SESIP)** – a flexible methodology to meet the cybersecurity, privacy, and regulatory needs of hardware and software components and platforms. The committee promotes SESIP across industries, supports certification reuse, and aligns with global standards to simplify security evaluation and improve trust in connected devices.

### Key Initiatives

- **Expanded Ecosystem:** Added new labs and certification bodies and growing the “SESIP Adopters” community.
- **Updated Governance:** Released SESIP Governance v1.2 to clarify certification processes and promote consistent application.
- **New Profiles & Mappings:** Published an updated SESIP Profile for Secure MCUs/MPUs and mappings to key standards like RED, NIST, IEC 62443, and UNECE WP.29.
- **European Standardization:** SESIP is European standard EN 17927 and supports compliance with RED, CRA, and other frameworks.
- **Global Reach:** Collaborations with regional authorities (e.g., NFTC in China) and ongoing efforts to enable mutual recognition with other schemes.
- **Cross-Industry Utility:** Used in automotive, healthcare, industrial, and consumer IoT applications to streamline certification and reduce costs.



### Specifications published this year:

- SESIP Profile for Secure MCUs and MPUs v1.1 (June 2, 2025)
- SESIP to IEC 62443-4-2 Mapping v1.0 (May 21, 2025)
- SESIP to SSIPS Mapping v1.0 (April 16, 2025)

### Impact

SESIP enables efficient, scalable, and regulation-ready IoT certification, reducing complexity for manufacturers and accelerating product time-to-market. As steward of SESIP, GlobalPlatform ensures its continued technical development and global relevance.





Chair:  
**Richard Hayton**  
Trustonic

TRUSTONIC

## Mission & Objectives

The TES Committee develops and maintains GlobalPlatform's standards for isolation platforms (in particular TEEs), ensuring secure access to trusted services both within devices and externally. It drives technical specifications, threat modelling, certification programs, and industry collaboration to support secure execution environments.

## Key Initiatives

- **Platform Specification Maintenance:** Evolves TEE and TPS specs via TES Platforms and TES Services working groups, supporting MCUs to high-end CPUs.
- **Certification & Compliance:** Develops TEE Compliance and Security Certification Programs for portability, interoperability, and validated evaluations.
- **Automotive Security:** Supports emerging regulations (e.g., UNECE 155/156), aligns with SAE J3101 key management, and proposes MCU CPU scaled protection profiles.
- **Cross-Platform Integration:** Works with SE and SESIP committees and the Automotive Task Force to align trusted platform services and certifications.



## Specifications published this year:

- TEE API Call Validation v1.0 (June 2, 2025)
- TPS Client API Specification v1.0 (April 14, 2025)
- TPS Keystore Protocol Specification v1.0 (April 14, 2025)
- Secure Element Access Control v1.2 (Jan 9, 2025)

## Impact

The TES Committee delivers robust, multi-tier isolation standards that underpin secure services on diverse platforms—spanning mobile, automotive, IoT, scalable compute, and AI. Its unified specs and certification programs accelerate innovation, ensure compliance with emerging regulations, and foster a trusted, interoperable ecosystem for secure applications.



Co-Chair:  
**Bill Mazzara**  
Stellantis

STELLANTIS



Co-Chair:  
**Richard Hayton**  
Trustonic

TRUSTONIC

## Mission & Objectives

The Automotive Task Force brings together OEMs, suppliers, and ecosystem partners to align GlobalPlatform's SE and TEE technologies with evolving automotive cybersecurity requirements. Its mission is to develop a collaborative, standards-driven ecosystem and engage key stakeholders to ensure GlobalPlatform technologies are relevant, deployable, and impactful across the automotive value chain.

## Key Initiatives

- **Standards Alignment with SAE:** Demonstrating how GP's SE/TEE meet the SAE requirements for hardware protected security requirements through J3101-5.
- **Collaboration with AUTOSAR:** Collaborating to ensure alignment and incorporating GP technologies to extend AUTOSAR's security document.
- **Liaison with Car Connectivity Consortium:** Leveraging the SE in vehicles for securing the digital car key and in support of other security use cases.
- **Advanced Automotive security services:** Replacing or augmenting automotive HSMs for performance, crypto agility, and other flexible security services.
- **Cybersecurity Vehicle Forum:** Convening automotive security experts through a series of global forums to collaborate on key priorities for automotive cybersecurity and validate GlobalPlatform's results.

## Impact

The Task Force facilitates the alignment of GlobalPlatform's SE/TEE technologies for automotive ecosystems while bringing the critical benefits of security functional interoperability and the flexibility required to face future needs. The ATF identifies key opportunities for GlobalPlatform's technologies to resolve current automotive security challenges, prioritizes relevant use cases, details automotive technical requirements for GlobalPlatform's Technical Committees, and promotes the relevance of GlobalPlatform solutions in addressing the security, privacy, and regulatory needs of next-generation vehicles. Through the active evolution of specifications, standards alignment and cross-industry collaboration, the Task Force supports the secure evolution of software-defined vehicles.

## Cybersecurity Vehicle Forum

The Cybersecurity Vehicle Forum events support GlobalPlatform's commitment to advancing comprehensive automotive cybersecurity—spanning priority automotive security use cases, assurance levels, compliance, certification for hardware protected security environments, and standardized APIs—through highly technical content and discussion with security decision makers from around the world. In 2025, we delivered events in China, Europe, Japan, and North America.





Chair:  
**Jean-Daniel Aussel**  
Thales



### Mission & Objectives

The eID Wallet Task Force identifies digital identity wallet use cases where GlobalPlatform's technologies can deliver security, privacy, and seamless deployment. It clarifies GlobalPlatform's role in addressing EU and global eID initiatives, evangelizes benefits, analyzes deployment models (e.g. eSIM vs. eSE), and liaises with standards bodies and identity stakeholders to drive long-term adoption.

### Key Initiatives

- **Regulatory alignment for EUDI Wallet deployment:** Focused on secure elements to meet high assurance ("LoA") under the EU eIDAS 2.0 regulation.
- **Requirements Analysis:** Defining high-level technical requirements for upcoming GlobalPlatform specifications to better support digital identity wallets.
- **Stakeholder Engagement:** Engaging wallet developers, regulators, member states, and standardization bodies (e.g. GSMA, ENISA, CEN CENELEC) to promote GP tech and support pilot deployments.
- **Implementation Guidelines:** Developing technical and strategic guidelines for governments and commercial wallet developers in using GlobalPlatform technologies to provide the best balance in security, reach, scalability and sovereignty for the EUDI wallet.



### Impact

The eID Wallet Task Force is laying the security and interoperability groundwork for large-scale national and pan-EU digital identity deployments. By defining technical models (SAM, CSP), engaging key stakeholders, and shaping certification approaches, it's accelerating secure digital ID pilots and deployments toward the 2026 EUDI Wallet rollout.



Chair:  
**Olivier Van Nieuwenhuyze**  
STMicroelectronics



### Mission & Objectives

The Security Task Force sets GlobalPlatform's overall security philosophy, contributing to secure, interoperable implementations. It collaborates with the Crypto and xBOM Sub Task Forces, SESIP Committee, and government entities to define security requirements to support meeting new cybersecurity regulations and maintain cryptographic algorithm recommendations.

### Key Initiatives

- **External Collaboration:** Works with ENISA, government bodies (i.e. ANSSI, BSI, NIST and NSA) and industry to ensure GlobalPlatform's security requirements cover diverse applications and align with cybersecurity frameworks.
- **Consulting Technical Committees:** Advises on cryptography, certification, and secure application across GlobalPlatform technical committees.
- **Secure Technology Identification:** Classifies secure technologies within various markets and drives crypto algorithm and key size updates via the Crypto Sub Task Force.
- **TPM Synergy:** Researches combining GlobalPlatform technology with TPM and equivalent libraries.



### Published this year:

- Cryptographic Algorithm Recommendations v3.0.1 (May 27, 2025)
- Cryptographic Algorithm Recommendations v3.0 (April 11, 2025)

### Impact

The Security Task Force shapes GlobalPlatform's security architecture—driving cryptographic agility, transparency, and alignment with regulatory standards. Its sub task forces ensure robust, coordinated strategies for cryptography and Bill Of Materials (BOM), supporting secure design, evaluation, and deployment across industries.





**Software Attack Expert Sub-Task Force**



Chair:  
**Jeremy O'Donoghue**  
Qualcomm




### Purpose


Maintains and develops GlobalPlatform's attack methodology at AVA\_VAN.2 and AVA\_VAN.3, supporting labs certifying under TEE and SESIP schemes.

### Scope


Develop a state-of-the-art attack catalogue at moderate levels of security assurance: to ensure that security evaluations on products are performed at a consistent and rigorous level and vendors are aware of the attack environment in which their products will be evaluated and to spread knowledge of effective countermeasures against attacks. Maintain close methodology alignment with regulatory groups at the same level of security assurance, particularly Euro-ISAC JHAS.



**Crypto Sub-Task Force**



Chair:  
**Beatrice Peirani**  
Thales




### Purpose


Reviews GlobalPlatform's cryptographic algorithms and protocols and recommends updates.

### Scope


Track cryptography trends, evaluate algorithms, and propose enhancements. Promote crypto agility and hybridization for post-quantum crypto transitioning and integration. Published "Cryptographic Algorithm Recommendations" v3.0.1 | GP\_TEN\_053 in May 2025.



**xBOM Sub-Task Force**



Chair:  
**Laurent Sustek**  
STMicroelectronics

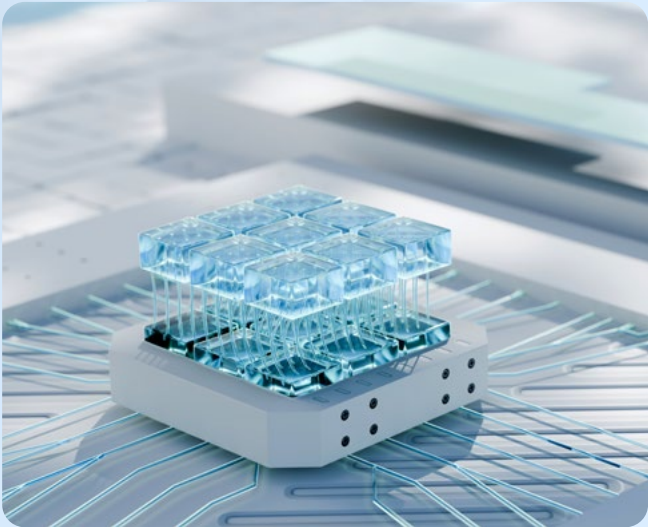


### Purpose

Guides deployment of Software, Hardware, and Crypto bills of materials (SBOM, HBOM, CBOM).

### Scope

Standardize transparency and assurance for software/hardware components. Provide BOM best practices covering risk analysis, DevSecOps, and vulnerabilities. Collaborate with SESIP and external bodies (IETF, OWASP, etc.) to enhance certification conformance.





**Regional Task Force: China**



Chair:  
**Yi Qiang**  
Huawei



### Mission & Objectives

The region-specific China task force gives members a platform to align GlobalPlatform's technologies and certifications (i.e. SE, TEE, SESIP) with Chinese market and regulatory requirements. It works closely with local industry, standards bodies, and certification frameworks to drive adoption and membership growth in the region.

### Key Initiatives

- **Regional Technology Adaptation:** Identify and address China specific needs such as TEE roadmaps, SE/TEEs use cases beyond payments, and certification requirements.
- **Stakeholder & Standards Engagement:** Liaise with Chinese standards organizations (e.g. Spark Link, CCSA, TAF, GCCO to influence requirements and ensure alignment.
- **Localized Promotion & Certification:** Boost adoption through China tailored marketing, educational materials, and promotion of GlobalPlatform's certification schemes.

### Impact

The China Task Force ensures that GlobalPlatform's technology stack and certification remains aligned with Chinese market needs, supporting widespread adoption, effective localization, and active engagement with domestic certification and standardization authorities.



**Regional Task Force: Japan**



Acting Chair:  
**Takanobu Ishibashi**  
Toshiba



### Mission & Objectives

The Japan Task Force is a forum for GlobalPlatform members with business interests in Japan to promote GlobalPlatform technologies in the region. It gathers market and functional requirements from Japanese industries and collaborates with regional standardization bodies.

### Key Initiatives

- **Industry & Standards Engagement:** Collaborates with regional standards bodies to align GlobalPlatform specifications with local standards and use cases.
- **Market Expansion:** Introduces GlobalPlatform across mobile, IoT, healthcare, smart city, and Industry 4.0 sectors; actively recruits members in Japan.
- **Use-Case & Tech Mapping:** Shares GlobalPlatform updates, analyzes specific regional use cases, and creates Japan-specific GlobalPlatform technology maps and use-case libraries.

### Impact

The Japan Task Force serves as GlobalPlatform's regional hub, ensuring the SE, TEE, and related technologies are tailored to Japanese market needs. Through strong local partnerships, education, and forums, it strengthens adoption and expands GlobalPlatform's influence in Japan's secure platform ecosystem.



# Our Services

## GlobalPlatform Certification: Creating a Trusted and Scalable Ecosystem

Certification is essential for building trust and reliability across technology ecosystems. By demonstrating compliance through GlobalPlatform's certification and qualification schemes, vendors prove that their products are trusted, interoperable, and secure.



## The Trusted Mark of Functional Compliance and Security

As an ISO/IEC 17065 accredited Certification Body (No. 5486.01), GlobalPlatform offers well-established functional and security certification schemes for products using SEs and TEEs. Certification testing is performed using approved tools by qualified laboratories worldwide, under the oversight of our independent Certification Secretariat.

**A GlobalPlatform certificate assures that a product performs reliably and meets key business, security, and regulatory requirements.**

## Supporting Global Certification Programs

GlobalPlatform certification services support leading technical associations such as EMVCo, GSMA, and the Secure Identity Alliance. Our schemes help vendors prove compliance with specifications such as EMVCo Approval, SGP.24, and OSIA, ensuring expected functionality and interoperability.



## New in 2025: Managed Certification & Qualification Services

To further support digital security, GlobalPlatform now offers ISO-accredited managed certification and qualification services for partner associations. These services help organizations efficiently launch and manage their own compliance programs.

## Available Services

Services can be deployed individually or combined:

- **Certification Secretariat Services:** We provide independent administration, legal, accounting, and verification support—quickly and cost-effectively.
- **Functional Test Strategy & Implementation:** From specification to tool validation and lab onboarding, we enable third-party evaluations.
- **Security Evaluation Support:** We help clarify lab requirements and evaluation processes to ensure effective security assessments.





## GlobalPlatform certification has been sought by 60+ organizations

To date, GlobalPlatform has issued:

**600+**  
Certificates

**130+**

Certificates have been issued for the GSMA test suite:

**27** **110**  
eUICC M2M eUICC Consumer

**8**

GlobalPlatform accredited laboratories in China, France, Spain, UK and Netherlands



**95bn+**

GlobalPlatform compliant secure components issued worldwide

## Training

### GlobalPlatform Technical Training: Delivered by Experts

GlobalPlatform offers technical training programs covering SEs, TEEs, and SESIP. Modular courses provide deeper insight into practical applications across payments, mobile, identity, and IoT. All programs can be customized and delivered in-house.



### Supporting EU Digital Identity Readiness

With the 2026 deadline approaching for EU member states to provide at least one EUDI wallet, GlobalPlatform is supporting issuers and developers through its SE for EUDI training. This two-day course has been delivered in Brussels (October 2024, March 2025), with a third session planned for October 2025.

The program helps EU representatives and partners understand how GlobalPlatform's proven technology delivers the security, scalability, and interoperability required for EUDI wallets—technology that is ready and available for immediate deployment.

For more information, contact:  
[secretariat@globalplatform.org](mailto:secretariat@globalplatform.org).

## Emerging Topics



### Artificial Intelligence

While AI has not been a traditional focus for GlobalPlatform, our mission to secure digital assets—applications, cryptographic keys, and trusted components—naturally extends to protecting AI models, data inputs, and outputs. As AI becomes part of critical infrastructure and consumer technologies, we are beginning to explore how our standards can ensure the integrity, confidentiality, and resilience of AI components. At the same time, we are leveraging AI to enhance secure component protection, detecting and mitigating novel attack vectors. This dual focus—securing AI and using AI for security—signals a new chapter in our commitment to trusted digital innovation.



### Attestation

Attestation is an emerging area of focus for GlobalPlatform as digital systems increasingly require proof of trustworthiness. At the foundation of attestation is a Root of Trust — a secure component that provides the essential building blocks for verifying the integrity of devices and software. GlobalPlatform's standardized technologies are ideally suited to support attestation services across diverse industries and use cases. By collaborating with other industry and standards organizations, GlobalPlatform helps ensure that attestation frameworks are interoperable, scalable, and secure.



### Post-Quantum Cryptography

GlobalPlatform is actively evaluating and updating the cryptographic foundations of its technologies to ensure long-term resilience against emerging threats, including those posed by quantum computing. As part of this effort, the organization is providing guidance on the integration of new cryptographic algorithms and supporting the industry's migration toward PQC. This includes assessing the impact of quantum-safe algorithms on secure components (SEs and TEEs) and updating specifications to support crypto-agility. By collaborating with global stakeholders and standardization bodies, GlobalPlatform is helping to future-proof security solutions and ensure a smooth, interoperable transition to PQC across ecosystems.





# The Value of GlobalPlatform Membership

Join GlobalPlatform to play a pivotal role in shaping a secure, trusted, and interoperable digital future.

GlobalPlatform membership empowers technology leaders to shape the future of secure digital services by contributing to the development of next-generation specifications. Members benefit from direct access to industry experts—from device makers to vertical market specialists—gaining valuable insights and deep security expertise to stay ahead in a rapidly evolving landscape. Through expert-led training and collaboration, companies are equipped to meet emerging technologies and regulatory demands. Members also play a key role in addressing transformative challenges like AI and quantum computing, while ensuring GlobalPlatform’s standards remain practical, robust, and future-ready.

# Member Companies and Organizations

Arun Jayadharan	<b>FIME</b>	Samsung SDS
American Express	<b>Galitt</b>	SERMA Safety & Security
<b>Analog Devices</b>	<b>Giesecke+Devrient GmbH</b>	Shanghai Fudan Microelectronics Group
<b>Apple Inc.</b>	<b>Google</b>	<b>Shanghai Uni-Sentry Intelligent Technology Co., LTD</b>
Applus+	<b>HID Global</b>	SK Telink
<b>ARM Limited</b>	<b>Huawei Device (Dongguan) Co., Ltd.</b>	Spreadtrum Communications (Shanghai) Co., Ltd.
AT&T	<b>IDEMIA</b>	<b>Stellantis</b>
AustriaCard	<b>Infineon Technologies AG</b>	<b>STMicroelectronics</b>
Bactech	Institute For Information Industry	Synapse Mobile Networks s.a.
<b>Beijing Unionpay Card Technology Co., Ltd.</b>	Internet of Trust S.A.S.	<b>Thales</b>
<b>Beijing ZhiHuiYunCe (DPLS Lab) Equipment Technology Co., Ltd</b>	JCB Co. Ltd.	Thales UK
BrightSight by SGS	Kaspersky Lab	<b>T-Mobile</b>
<b>BSI - Bundesamt fuer Sicherheit in der Informationstechnik</b>	<b>Keysight</b>	Toshiba Corporation
Bundesdruckerei GmbH	Kigen (UK) Lda	TrustCB B.V.
CARIAD SE	KONA International	<b>Trustonic</b>
Cartes Bancaires	Licel Corporation	UBIVELOX
CEA - Leti	Linaro	UL (Underwriters Laboratories)
COMPRION GmbH	MaskTech International GmbH	UNISOC
CPSEC (National Institute of Advanced Industrial Science and Technology)	<b>Mastercard</b>	Valid Soluciones Tecnológicas
Dai Nippon Printing Co., Ltd.	MK Smart JSC	<b>Visa</b>
DEKRA	Monetech	Watchdata System
Department of Defense	Nextendis	<b>Winbond Technology Ltd</b>
<b>Deutsche Telekom Security GmbH</b>	NthPermutation Security LLC	Wise Security Technology (Guangzhou) Co., Ltd.
Digital Cubes	<b>NTT Corporation</b>	Woven by Toyota
Discover Financial Services	<b>NXP Semiconductors</b>	Wuhan University
Eastcompeace Technology Co., Ltd	<b>Oracle</b>	XardPay
ETAS	Orange	XCure Corp.
Feitian Technologies Co., Ltd	PQShield	Xiaomi
<b>FeliCa Networks, Inc.</b>	<b>Qualcomm Technologies Inc.</b>	Zwipe Germany
	Quarkslab	
	Rambus	
	Renesas	
	Safepay Systems Ltd.	
	<b>Samsung Electronics</b>	

- Full members indicated in bold





# Industry Partners

- L'Agence nationale de la sécurité des systèmes d'information (ANSSI)

L'Alliance pour la Confiance Numérique (ACN)

APSCA

AUTO-ISAC

AUTOSAR

Car Connectivity Consortium

CCDS

CEN

Cenelec

EMVCo

European Payments Council

EUROSMART

ETSI

FIDO Alliance

Fira Consortium

Global Certification Forum

Global Computing Consortium

GSMA

IoT Connectivity Alliance

IFAA
- Institute for Information Industry

ioXt Alliance

ISO

Java Card Forum

National Financial Technology Certification Center

NFC Forum

NICSS

NIST

OMA SpecWorks

Mobey Forum

One M2M

PTCRB

RISC-V

SAE International

Secure Identity Alliance

Secure Technology Alliance

Smart Ticketing Alliance

Trusted Computing Group

Trusted Connectivity Alliance

W3C

Wireless Power Consortium

# Member Testimonials

Fime offers a range of world leading test solutions, lab certifications and advisory services in the payments, telecoms, mobility and digital identity industries. We provide a unique global cross-industry perspective acting as an innovation enabler to help our customers launch their solutions. As an active contributor to the Secure Element Technical Committee, we provide qualified test suites covering the full range of GlobalPlatform's Secure Element test plans and GlobalPlatform qualified lab services for our customers to test and certify their payment, UICC, eUICC and embedded Secure Element (eSE) Secure Element solutions. Fime is also at the forefront of evolving Digital Identity technologies, delivering innovative tools, consulting, and compliance testing services to advance Digital Identity solutions and ensure seamless global interoperability in line with GlobalPlatform's vision.

 | Iain Maxwell,  
Product Manager, Fime

Google is committed to fostering a secure and innovative Android OEM ecosystem, and we value the powerful framework GlobalPlatform's technologies provide for our partners. For critical use cases like the EUDI Wallet, the Secure Element offers a robust and proven path to building a certifiable and tamper-resistant foundation. The forthcoming Cryptographic Service Provider (CSP) specification is a critical next step. It allows our SE partners to enhance their StrongBox applet/ service efficiently on top of their foundational CSP certification. By making this CSP-backed StrongBox service accessible through the canonical Android Keystore API, we help ensure that all EUDI Wallet developers, whether public or private, can easily build upon the strongest hardware-backed security. Ultimately, our goal is to help the entire digital wallet ecosystem thrive, bringing innovation and great user experiences to people everywhere. Our collaboration with GlobalPlatform helps us fulfill our vision of a more private and resilient digital future.

 | Dave Kleidermacher,  
VP of Engineering, Android Security & Privacy, Google



## Member Testimonials

GlobalPlatform standards have always been very relevant and important to us, right from the very start of our journey. Our team has extensive experience building operating systems for smart cards, for example. And more recently, our Virtual Trusted Execution Environment (vTEE) has been evaluated and approved under EMVCo SBMP TEE - which is based on GlobalPlatform's TEE specification. We are looking forward to beginning our exploration with GlobalPlatform and specifically participating in the eID Wallet Task Force Workgroup, which is an important strategic area of focus for us.

 **Licel** | Mikhail Dudarev,  
Co-founder and CTO, Licel

At Quarkslab, we bring together cutting-edge expertise in offensive and defensive software security, both through our consulting services and our dedicated software protection product.

Our participation in GlobalPlatform aims to highlight the critical importance of software protection and to share our know-how with the community.

We are committed to helping members strengthen the security of their IoT devices, platforms, and services by embedding effective software protection into standards like SESIP. As a key milestone, in 2025 we led the drafting of a white paper on software countermeasures, set to be published by the end of the year.

 **Quarkslab** | Béatrice Creusillet,  
Product R&D Manager,  
Quarkslab

## Member Testimonials

As a provider of secure OS solutions, we at Trustonic understand the critical role that standards play in driving industry-wide adoption—both at scale and at speed. GlobalPlatform is instrumental in this effort, setting the benchmark for secure technology and enabling seamless portability across industries. A great example of this is the impactful work being done by the Automotive Task Force.

For silicon vendors and device manufacturers, having the confidence that their solutions can provide highest levels of protection is essential. GlobalPlatform delivers this assurance through its robust standards and certification programs.

Supporting the ongoing evolution of GlobalPlatform standards has been central to our development strategy for many years—and we fully expect it to remain a core focus well into the future.

 **TRUSTONIC** | Andrew Till, GM,  
Secure Platform, Trustonic

“Thales Digital Identity & Security is a global leader in digital security, bringing trust to an increasingly connected world. Our technology is at the heart of modern life, from payments to enterprise security and the internet of things, and enables our clients to deliver secure digital services for billions of individuals and things. Successful deployment of such mass-market products and services requires outstanding standards, as well as stringent functional compliance and security certification. Thales is leading and participating into several standardization bodies and initiatives, and GlobalPlatform is one of the most important standardization setting organizations, as it defines key industry standards at the heart of the security of billions of devices, and from which we, at Thales, can build a future we can all trust.”

 **THALES** | Jean-Daniel Aussel,  
Head of Standardization,  
Thales Digital Identity  
& Security.





**Global  
Platform®**

Securing the digital future

→ [globalplatform.org](https://globalplatform.org)

