
Global Platform™
25th Anniversary Edition
25
GlobalPlatform Annual Report 2024

Contents

Letter from the Chair of the Board

This year, GlobalPlatform celebrates its 25 year-anniversary. For a quarter of a century, we have been at the forefront of standardizing secure digital services, ensuring that billions of devices worldwide can communicate securely and reliably.

This was another pivotal year in the history of GlobalPlatform as we accelerated activity into new markets and developed specifications to meet the needs and requirements of evolving technologies. Here a some of our key achievements this year:

Key achievements

- The ratification of **SESIP** (Security Evaluation Standard for IoT Platforms) as a European Standard (EN 17927) served as a catalyst for widespread adoption. Now an internationally recognized standard for IoT security evaluation, SESIP is attracting support from a large community of component manufacturers, industry bodies, security laboratories, and other stakeholders. To support this growing adoption, GlobalPlatform launched comprehensive **SESIP Training** courses for product vendors, regulators, and scheme owners – helping to grow understanding of the SESIP methodology and its applicability. And this year, we published the mapping of SESIP security requirements to: **NIST 8425, UNECE WP.29, RED prEN 18031 and ISO/SAE 21434**.
- The EU has given the green light to advance the introduction of the cross-border European Digital Wallet (EUDI). GlobalPlatform has introduced a range of new solutions to help both EU Member States and smartphone vendors implement the scheme based on GlobalPlatform secure technologies. In collaboration with the GSMA and ENISA, we developed the **Secure Application for Mobile (SAM)** model for secure elements, and we are driving the development of the **Cryptographic Service Provider (CSP)** specification with security evaluation guidelines for the European Cybersecurity Scheme on Common Criteria (EUCC).
- We made great strides aligning GlobalPlatform technologies with automotive use cases, including collaborating with the **Society of Automotive Engineers (SAE)** to harmonize with SAE's J3101 standard – laying the foundation for secure software-defined vehicles.
- In May, we announced the release of a new standardized **Secure Channel Protocol** for secure elements. This enabled remote application and file management on constrained IoT devices and low-power networks – helping to overcome network and bandwidth limitations of devices based on lower power standards such as NB-IoT.
- We entered into liaison agreements with the **CENELEC TC 47X, FiRa Consortium** and **Wireless Power Consortium** providing further evidence of the expanding relevance of GlobalPlatform technology.

Our continuing progress is a testament to the spirit of collaboration across our diverse and growing membership as well as evidence of the robust frameworks that GlobalPlatform has developed to support world-wide adoption of secure technologies. This collaborative approach continues to drive innovation but also ensures that trust and security remain at the heart of the evolving digital landscape.

S El Rhomri

Stéphanie El Rhomri
Chair of the Board

Letter from the Executive Director

GlobalPlatform has come a long way in 25 years. But our mission remains the same: to establish and maintain a secure and interoperable infrastructure for digital services and devices. As the world grows ever more connected, success in this new age depends on the availability of standardized and trusted technologies. And we remain committed to driving new initiatives that increase trust and security in devices to enable our stakeholders to efficiently – and effectively – deliver innovative digital services.

Through collaboration with our members and industry partners, we continue to drive adoption of new security technologies and best practices to support the evolving needs of this rapidly expanding digital ecosystem. Below are some of our focus areas for the year ahead.

Strategic Initiatives for 2025:

Securing the Digital ID ecosystem to deliver the EUDI Wallet – Following our successful collaboration with the GSMA on the Secured Application for Mobile (SAM) requirements, we're now focused on the Cryptographic Service Provider (CSP) specification. This provides an easy way to certify third-party digital ID applets with a high level of assurance for smartphone-based wallets. With the EU Digital Identity (EUDI) Wallet on the horizon, the eID Wallet Task Force will continue to work with stakeholders to define deployment models and set the technology roadmap based on secure element technologies – including the launch of a dedicated training program. We are also expanding our efforts to support digital identity beyond Europe – working towards international interoperability through our participation in the SIDI (Sustainable and Interoperable Digital Identify) Hub initiative.

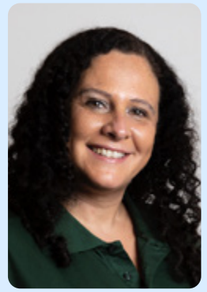
Future of financial services – As digital transformation impacts the financial world, GlobalPlatform is focusing on bringing security to digital currencies and enabling biometrics to authenticate a new era of payments.

Enabling the connected car – Through collaborations with organizations such as the Society of Automotive Engineers (SAE) and AUTOSAR, GlobalPlatform will accelerate the deployment of secure components, trusted digital architecture, and security APIs in the automotive sector.

Expanding secure IoT: We're accelerating adoption of SESIP across new markets and use cases. This includes new partnerships, expanding the number of labs and certification bodies (CB), and the creation of an adopter program. We are also expanding our efforts into supporting new isolation environments and technologies.

Supporting emerging regulations. We're engaging with regulators – such as the Cyber Security Agency of Singapore (CSA), European Union Agency for Cybersecurity (ENISA) and the National Institute of Standards and Technology (NIST) – on how GlobalPlatform technology can support emerging regulations. Our standards simplify compliance to emerging regulations and legislation such as the CSA Cybersecurity Labelling Scheme (CLS), the EU Cyber Resilience Act and the US Cyber Trust Mark program.

I encourage you to learn more about the work we are doing to address emerging security requirements and invite you to join us in developing standardized specifications to enable secure and trusted digital services and devices. Through broad industry collaboration, we can work together to secure our increasingly interconnected world.



Ana Tavares Lattibeaudiere

Ana Tavares Lattibeaudiere
Executive Director

Building the Foundation of Digital Security for 25 Years

1999 — GlobalPlatform founded to standardize secure chip technology

2000 — Publication of first specs for secure element (SE) technology, driving digitization across banking, transport, government, and more

2004 — Key Standards Bodies
Collaboration with ETSI to align GlobalPlatform with SIM technology, delivering standardized security across the mobile phone market

2007 — Ushers in the era of mobile payments with the introduction of contactless standard

2010 — First release of Trusted Execution Environment (TEE) specifications, providing a framework for secure execution of applications and data isolation

2011 — Launch of first compliance program to ensure products adhere to GlobalPlatform standards

2011 — Key Standards Bodies
Collaboration with ISO to standardize use of NFC and contactless technologies in public transit services

2012 — Publishes Secure Element Configuration V.1 to support the move from smart cards to embedded secure elements, enabling secure services in smartphone and IoT devices

2014 — Publishes first framework for IoT/M2M standardization

2014 — Entertainment industry adopts TEE for securing premium content

2015 — Signs MOU with China's Telecommunication Terminal Testing Technology Association to bring TEE to China

2015 — Key Standards Bodies
TEE Protection Profile officially certified by Common Criteria

2016 — Launches TEE compliance program

2016 — Signs MOU with Car Connectivity Consortium to bring GlobalPlatform technologies to auto industry

2016 — Half of all SEs shipped are based on GlobalPlatform specifications

2016 — GSMA adopts eSIM specification based on GlobalPlatform testing platform

2017 — Global shipments of GlobalPlatform SEs surpass 22bn

2018 — GlobalPlatform TEE adoption hits 10bn

2019 — GlobalPlatform-certified components (SE & TEE) in use surpass 53bn

2019 — Launch of first specs for integrated SE (iSE) technology, opening up new form factors

2020 — ETSI embeds GlobalPlatform iSE into secure platform for connected devices

2021 — Key Standards Bodies
GlobalPlatform certifications body achieves ISO 17065 accreditation

2022 — Key Standards Bodies
SESIP adopted by CEN and CENELEC as European standard for IoT security

2023 — 62bn GlobalPlatform compliant SEs shipped globally

2024 — 90% of all SEs shipped globally based on GlobalPlatform specs

Who is GlobalPlatform

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 Lattibeaudiere
Executive Director

Gil Bernabeu
Chief Technology Officer

Tono Aspinall
Operations Director

Francesca Forestieri
Automotive Lead

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
Vice Chair, STMicroelectronics

Claus Dietze
GlobalPlatform Treasurer and Secretary, Giesecke + Devrient Mobile Security

Rob Coombs
ARM

Eikazu Niwano
NTT Corporation

Sebastian Hans
Oracle

Jeremy O'Donoghue
Qualcomm

Guillaume Phan
Thales

Scott Migaldi
T-Mobile USA

Richard Hayton
Trustonic

Marc Kekicheff
Visa Inc.

Member company representation by geography

Why GlobalPlatform?

Evolving to meet tomorrow's digital security requirements

For 25 years, GlobalPlatform has been developing and refining the standards to enable secure digital services and devices.

As digitalization continues to drive change across multiple industries, GlobalPlatform allows device makers and service providers to use the same security framework to provide a validated level of security robustness across different devices and systems. This highly scalable approach serves to lower barriers to entry and avoid certification fragmentation, leaving OEMs and service providers to focus on delivering innovation.

Driving innovation through industry led collaboration

As a member-driven standards organization representing a diverse range of companies and industries from around the world, our members work collaboratively to develop standardized technologies that enable the efficient launch and management of innovative, secure-by-design digital services and devices for an increasingly interconnected world. As technology continues to evolve and new vertical markets are impacted, this work is supported by engagement with key industry partners. This year, we entered into liaison agreements with CENELEC TC 47X, the FiRa Consortium and the Wireless Power Consortium.

Industry Focused. Member Driven

- Non-profit, member-driven technical association
- Enables collaboration between service providers and device manufacturers
- Standardized framework - aligned with global cybersecurity regulations - ensures that devices are secure enough to protect against threats and attacks
- Enables the delivery of secure digital services to end users

New industry partners:

CENELEC
Semiconductors and Trusted Chips

FiRa | The Power to Be Precise

WIRELESS POWER CONSORTIUM

GlobalPlatform Technology

Standardizing Secure Components and Optimizing Security Evaluation

At the core of GlobalPlatform's work is the standardization of secure component technologies. This secure component is delivered as a platform combining hardware, firmware, and root of trust to distribute and manage trusted applications in different execution environments and to meet various security requirements. To meet the highest levels of assurance, GlobalPlatform has defined Secure Element (SE) as a tamper resistant environment that can be removable, embedded or integrated. For markets requiring a medium level of security and more calculation power, it defines the Trusted Execution Environment (TEE) as an isolated execution environment on the main device processor.

GlobalPlatform specifications are continually evolving to respond to the latest security threats, regulations, and chip developments. For example, GlobalPlatform is currently investigating isolated environments that offer a new execution environment with a limited or medium level of security. Furthermore, GlobalPlatform stays ahead of the latest developments in cryptography, reviews new algorithms, and defines attack methodologies for lab security assessments. GlobalPlatform stays in continuous communication with national agencies on the evolving regulations in cybersecurity.

GlobalPlatform technologies have been adopted across industries including finance, government, telecoms, and new verticals that are increasingly relying on secure connectivity. This widespread adoption has helped establish mass market products based upon common security requirements, providing portability and interoperability for trusted applications/applets.

A key part of the success in ensuring interoperability of services on a global scale has been the development of GlobalPlatform's functional and security certification programs. For connected devices, GlobalPlatform streamlines security evaluation through the Security Evaluation Standard for IoT Protocol (SESIP) methodology, which is recognized as a European standard by CEN and CENELEC (EN 17927). SESIP optimizes the reuse and composition of security certified device components (i.e., certify once, use in multiple markets).

The majority of the world's SIM cards, credit cards, identity cards, ePassports smartphones and device processors today rely on GlobalPlatform's technologies.

Secure Element (SE)

A tamper resistant execution environment, removable, embedded or integrated

Trusted Execution Environment (TEE)

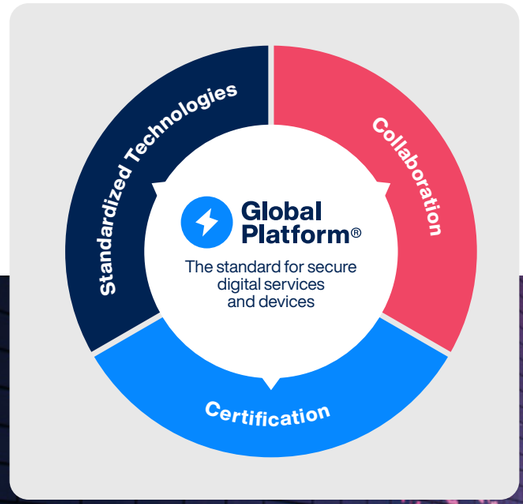
An isolated execution environment in the main chip of the device

Isolation Technologies

New technologies that create isolated execution environments

- Financial services
- Identity
- Mobile
- Consumer Electronics
- Healthcare
- Smart City
- Automotive
- Utilities
- Logistics

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.

Our Committees

Where technology is developed to address emerging market requirements and innovations

Secure Element Committee

Working Groups
SE Security
SE Specification
SE Compliance

SESIP Committee

Working Groups
Ecosystem Adoption
Governance
Technical

TES Committee

Working Groups
TES Services
TES Compliance
TES Attack Groups
TES Labs

Our Task Forces

Where requirements are gathered to determine impact to our technology roadmap

Automotive Task Force

Security Task Force
(Crypto & SBOM)

eID Wallet Task Force

Regional Task Forces
China

Regional Task Forces
Japan

Secure Element Committee

Chair:
Guillaume Phan
Thales

THALES

Mission

The SE Committee defines industry and technology neutral specifications for the secure and interoperable deployment and management of multiple embedded applications on Secure Element (SE) technology. This includes embedded and integrated SEs, SIM/UICC, smart microSD as well as smart cards.

Key Activities & Achievements

- **Secure Application for Mobile (SAM)** - The SAM specification defines a new capability for deployment and management of trusted applications on an eUICC. This year we published the SAM configuration v1.0.
- **Cryptographic Service Provider (CSP)** - CSP provides a secure and easy way to certify third-party digital ID applets with a high level of assurance by delegating sensitive cryptographic operations to a certified library embedded in the SE. The CSP specification is currently in development.
- **Post-Quantum Crypto** - Creating new agile protocols in preparation for future of post-quantum crypto migration.
- **ID document operating system updates** – Defining a standardized scheme to facilitate wide deployment of Operating System (OS) updates in ID documents.
- **Update of the protection profile** – Answering market and regulatory demands with a key focus on the deployment of CC:2022 and EUCC (European Cybersecurity Certification Scheme on Common Criteria).
- **IoT/Automotive** - Enhancing SE technology for Root of Trust on IoT devices, including compliance with SPI and I2C, and support for CoAP/DTLS for remote administration and J3101 support.
- **FIDO Alliance** - Collaboration to enhance the SE Protection Profile to support the FIDO Authenticator Level 3+ certification requirements.

Supporting deployment of EUDI Wallets through SE

GlobalPlatform is helping EU Member States better protect their citizens' identity and related data by optimizing its SE specifications for EUDI Wallet schemes. The GlobalPlatform SE is widely deployed in different form factors on smartphones, including removable SIM cards (UICC), embedded Secure Elements (eSE), embedded SIM (eUICC), and integrated SIM (iSIM). By using a technology that is already built into the vast majority of today's smartphones, the GlobalPlatform SE provides the foundation for a new digital ecosystem across Europe, unlocking new revenue opportunities for governments and industry.

SESIP Committee

Co-Chair:
Georg Stütz
NXP Semiconductors

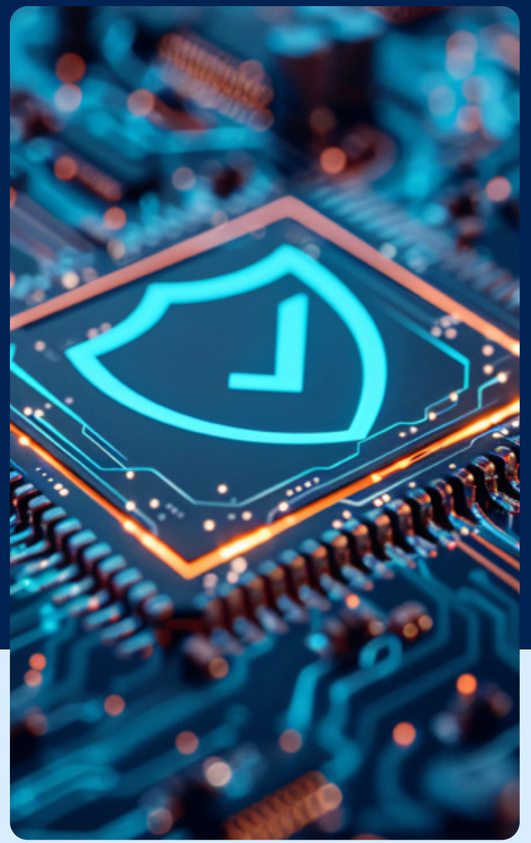
Co-Chair:
Philippe Gaudillat
STMicroelectronics

Mission

SESIP provides a common and optimized approach for evaluating the security of components and platforms from connected products looking to meet the specific compliance, security, privacy, and scalability challenges of the evolving IoT ecosystem.

The purpose of the newly established SESIP Committee is to set the strategy and deliver the required initiatives that will support the adoption and recognition of SESIP as a worldwide, multi-vertical scheme that simplifies security evaluation for OEMs, component manufacturers, and the whole ecosystem.

The primary focus of the Committee is to engage with regulators and the security evaluation ecosystem and discuss the value and applicability of the SESIP methodology as well as requirements for the future.



Simplify compliance to the Cyber Resilience Act (CRA) through SESIP

The forthcoming Cyber Resilience Act is set to introduce new regulations aimed at bolstering cyber resilience across digital markets and businesses. Adapting to the evolving regulatory landscape poses a multifaceted and resource-intensive challenge. SESIP streamlines this process by facilitating alignment with existing regulations and serves as a singular reference point for comprehensive evaluation.

The SESIP committee is prioritizing the mapping of the SESIP methodology to the requirements of the Cyber Resilience Act. They are also creating a CRA SESIP protection profile.

Key Activities & Achievements

SESIP is an internationally recognized standard for IoT security compliance - EN 17927.

SESIP has rapidly become an internationally recognized standard for security evaluation, supported by a large community of security providers, industry bodies, security laboratories, and other stakeholders – with more coming soon. SESIP (EN 17927) is supported by GlobalPlatform's large, global security ecosystem and is used by OEMs in the consumer, automotive, medtech and industrial markets.

SESIP-certified products include:

NXP · ST life.augmented · winbond

GlobalPlatform SESIP Certification Bodies:

TRUSTCB TRUST AND VERIFY · More coming soon!

GlobalPlatform SESIP-Licenses Laboratories:

Applus+ · DEKRA · riscure Driving your security forward · SERMA SAFETY & SECURITY · THALES · SGS brightsight

SESIP is recognized and referenced by:

CARCONNECTIVITY consortium® · CENELEC · Fira The Power to Be Precise · NIST National Institute of Standards and Technology · psacertified™ · WIRELESS POWER CONSORTIUM · More coming soon!

Compliance

Provide evidence of compliance to the latest regulatory developments such as RED, CRA, US Trust Mark, Singapore CSA CLS, EN303645, FDA, IEC 62443, ISO 21434 and more.

Risk Management

Access a powerful toolbox to map product security features and demonstrate targeted levels of robustness against different risk levels and risk profiles.

Differentiation

Demonstrate a product's core security capabilities as a key market differentiator – set your product apart from the market.

Global Platform™ SESIP Adopters Community

As SESIP is now being used by a range of stakeholders, GlobalPlatform has created the 'SESIP Adopters' Community' in order to inform non-members about the latest SESIP developments, provide access to relevant technical documents, and allow participants to showcase their certified products and/or support for SESIP.

TES Committee

Chair:
Richard Hayton
Trustonic

TRUSTONIC

Mission

To create and maintain documentation relating to Isolation Platforms.

Provide mechanisms enabling access to platform services offered by Isolation Platforms, both from within a device and from platforms external to it.

To define and maintain the trusted execution environment architecture, including technical specifications compliance and security certification programs.

Key Activities & Achievements

The newly created Trusted Environments & Services (TES) Committee combines the work of the previous Trusted Execution Environment (TEE) and Trusted Platform Services (TPS) Committees and focuses both on hardware secured 'environments' in which services can be run, and the definitions of those services.

The committee inherits the TEE heritage and continues to be responsible for the standardization of APIs and protection profiles for TEEs, while focusing on a broader remit to look at similar environments, such as TPMs, HSMs, MARs, etc. This is driven by the emerging need for consistent approaches to security across a wide variety of secure isolation technology platforms (in industries such as automotive). Similarly, when looking at services, we consider both horizontal and industry vertical services that could run on TEEs or other trusted platforms.

Automotive is likely to be a focus area as we build on the momentum from the Automotive Task force and collaboration with the Society of Automotive Engineers (SAE).

As technology advances, new data security and privacy requirements will continue to emerge.

By combining the work already done by the TEE and TPS Committees into a new Trusted Environments & Services (TES) Committee, GlobalPlatform is working to address evolving requirements by covering a broader range of secure isolation platforms and providing mechanisms that protect data at rest, data in use and data in transit.

By casting a wider net, the TES Committee will define services that directly address vertical sector problems and use cases, helping enable robust security across a range of secure platforms. Automotive and AI are two use cases that we are tackling first.

eID Wallet Task Force

Chair:
Jean-Daniel Aussel
Thales

THALES

Mission

The purpose of the eID Wallet Task Force is to identify and address digital identity wallet use cases where GlobalPlatform technologies can play a role, including – and specifically encompassing – security, privacy and frictionless deployment.

Key Activities & Achievements

The primary focus of the eID Wallet Task Force is to identify requirements to support the ongoing initiatives from the European Union and other governments that are engaged in large-scale ID and eID deployments. We are focused on:

- Promoting the benefits of GlobalPlatform technologies – such as SEs, TEEs and Device Trust Architecture – in support of secure identity initiatives
- Providing high-level requirements to the GlobalPlatform Technical Committees to develop new amendments or specifications to support digital identity solutions and evolving regulations
- Analyzing, identifying and positioning business requirements relating to identity to enable developers to capitalize on the secure components' ability to host secure identity services
- Proposing and comparing the benefits of different deployment models for digital identity wallets based on GlobalPlatform technology, such as hosting security anchors on embedded SIMs vs embedded Secure Elements
- Liasing with regulators, government and identity-related organizations on how GlobalPlatform technologies can fulfil the evolving needs in developing secure identity solutions

SIDI Hub

GlobalPlatform joined a number of major non-profit organizations active in digital identity to launch the **Sustainable and Interoperable Digital Identity (SIDI) Hub**.

This initiative aims to define what is needed to achieve cross-border interoperability for digital identity, to promote a common understanding of what cross-border interoperability means and define a shared approach and roadmap for success.

SIDI Hub is a community where governments, NGOs, standards bodies, private entities, multilaterals and academic organizations collaborate to follow a shared roadmap.

Automotive Task Force

Chair:
Richard Hayton
Trustonic

TRUSTONIC

Mission

Securing software defined vehicle services.

Key Activities & Achievements

GlobalPlatform's goal is to develop a common set of standardized security services to support software-defined vehicles. To achieve this, we are working with the Society of Automotive Engineer's (SAE) International, Autosar, the Car Connectivity Consortium, and Auto-Isac to coordinate on common evolving requirements for future use cases.

Working in coordination with the Society of Automotive Engineer's (SAE), we are able to demonstrate that GlobalPlatform's existing security specifications for Secure Element (SE) and Trusted Execution Environment (TEE) strongly align with SAE's J3101 recommended practices for hardware protected security environments for ground vehicles. We are assessing the development of a keystore application for automotive (in alignment with J3101). Furthermore, we are exploring the requirements for an automotive TEE for MCUs and the position of SEs as an alternative to automotive HSMs.

We are also focusing on mapping how GlobalPlatform provides security support to AUTOSAR's upper software layers as well as the utility of demonstration of integration between GlobalPlatform technologies and AUTOSAR's Crypto API.

Additionally, we are examining the ability for SESIP to support generating evidence for UNECE's Regulations 155 & 156 on cybersecurity. We are also analyzing the stages of vehicle cyberattacks to determine the objectives and methods of an attack to evaluate defense systems and then develop the appropriate safeguards.

Cybersecurity Vehicle Forum

Over the past year, we held Cybersecurity Vehicle Forum events in China, Germany, Japan and the US. At our most recent event in June, the Cybersecurity Vehicle Forum brought together representatives from automotive OEMs, Tier 1 automotive suppliers, and SoC and semiconductor companies for a highly successful event alongside AutoTech: Detroit.

GlobalPlatform CTO, Gil Bernabeu and Automotive Lead, Francesca Forestieri also represented the work of the automotive task force as speakers at ESCAR USA and AutoTech: Detroit – presenting on the alignment of GlobalPlatform specifications with SAE's J3101.

Security Task Force

Chair:
Olivier Van Nieuwenhuyze
STMicroelectronics

life.augmented

Mission

The Security Task Force engages with governments and regulators to monitor and identify emerging trends in cryptography, algorithm proposals and security requirements that impact GlobalPlatform technologies. This task force works closely with its two sub-task forces focusing on crypto and SBOM. The Security Task Force also defines GlobalPlatform's security philosophy and provides direction to the Technical Committees.

Key Activities & Achievements

- Engage and collaborate with external security organizations to ensure that security requirements from a broad range of use cases and market sectors are incorporated into GlobalPlatform specifications
- Advise the GlobalPlatform Technical Committees in security philosophies, cryptography, certification and applicability
- Facilitate collaboration with government agencies and their security experts to define market requirements
- Identify and classify secure technologies for the Internet of things (IoT)
- Maintain and update GlobalPlatform's cryptographic algorithm recommendations table, through the crypto sub-task force

Security Task Force Crypto Sub-Task Force

Chair:
Beatrice Peirani
Thales

THALES

Mission

The purpose of the Crypto Sub-Task Force is to evaluate and provide recommendations on the cryptographic mechanisms used in GlobalPlatform technology, to ensure high levels of security as cryptography trends and technologies evolve.

Key Activities & Achievements

The Crypto Sub-Task Force is focusing on the aggregation of several topics linked to post quantum cryptography (PQC) to build a complete view on this topic and support the GlobalPlatform Technical Committees in incorporating PQC into our specification updates. This includes the threat of quantum computing, the impact on GlobalPlatform specifications, the different solutions (i.e., crypto agility and hybrid crypto), the regulatory body recommendations, the state-of-the-art in terms of standards (mainly NIST PQC project), and the recommendation for strategy. To reach this target, we have engaged with our members and several standards and national organizations such as ETSI, IETF, ANSSI, BSI and NIST.

Our work has supported the SE Committee in updating the Secure Channel Protocol '04' to allow for cryptographic agility of the protocol specification. Similar work is beginning for Secure Channel Protocol '11' to a new crypto agile and PQC ready SCP12.

Security Task Force

Software Bill of Materials (SBOM) Sub-Task Force

Chair:
Laurent SUSTEK
STMicroelectronics

life.augmented

Mission

The purpose of the SBOM (Software Bill of Materials) Task Force is to analyze the impact of, and provide guidance on, the deployment of SBOM.

Key Activities & Achievements

The Software Bill of Material Sub-Task Force is analyzing the impact of the SBOM and providing guidance relating to its deployment, including a consistent means to produce, consume and exchange software transparency and assurance information. Also, in collaboration with the SESIP Committee, we plan to produce a white paper to explain the challenges software developers will face with emerging regulations and how SBOM will become the means to provide transparency to software users.

Regional Task Forces

China Task Force

Chair:
Xinmiao Chang
Huawei

Mission

The task force provides GlobalPlatform members with business interests in China with a dedicated platform to identify and agree on requirements from the region. The group also works directly with Chinese industry and standardization associations.

HUAWEI

Key Activities & Achievements

The China Task Force works to:

- Act as a focus point for all GlobalPlatform technologies and promotion within different industries in China
- Identify and establish liaisons with relevant stakeholders and organizations across a variety of sectors in the region
- Align GlobalPlatform technology with requirements from China, particularly but not exclusively related to the TEE roadmap and specification working groups
- Expand GlobalPlatform technology adoption and the certification regime in China
- Align functional and security evaluation requirements and provide input to relevant specifications, compliance and certification programs to GlobalPlatform Committees
- Identify relevant special Chinese compliance and certification programs within the Chinese market

Japan Task Force

Chair:
Eikazu Niwano
NTT

Mission

The Japan Task Force is a forum for GlobalPlatform members with business interests in Japan to gather and discuss business and functional requirements of specific market sectors within the region.

NTT

Key Activities & Achievements

The Japan Task Force works to:

- Promote GlobalPlatform activities within the region
- Exchange information with other Japanese / Asian industry associations and standardization bodies including Connected Consumer Device Security Council (CCDS), Secure IoT Platform Consortium, Next Generation IC Card System Study Group (NICSS), Association of Radio Industries and Businesses (ARIB), Japan Automotive Software Platform and Architecture (JASPAR), Asian IC Card Forum (AICF) and the Asia Pacific Smart Card Association (APSCA)
- Introduce GlobalPlatform to mobile, internet of things (IoT) and other key sectors within Japan and identify areas where the association can contribute to regional activity

Our Services

Certification

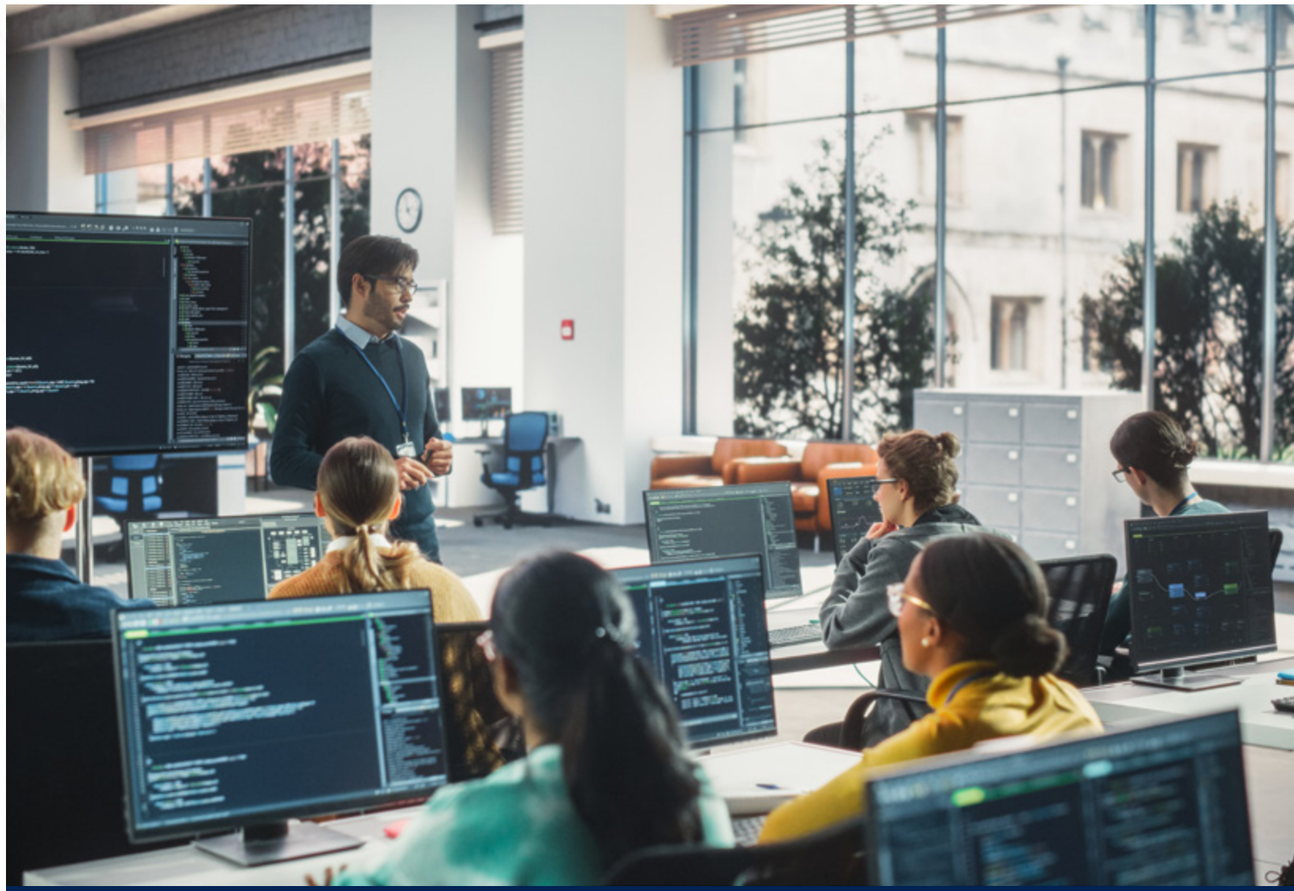
Certification schemes promote a collaborative and open ecosystem enabling trusted digital services and devices

GlobalPlatform operates functional and security certification schemes, allowing product vendors to demonstrate product adherence to GlobalPlatform's specifications, market-specific configurations and protection profiles.

The internationally recognized programs are independently operated and referenced by EMVCo, GSMA and other industry bodies, with testing of certified products provided by GlobalPlatform-approved laboratories globally.

Service providers can request the certification stamp to verify a product matches their security and privacy needs. Laboratories and test tool suppliers can work with GlobalPlatform to become accredited and offer their own GlobalPlatform-certified test services.

2LA ACCREDITED
CERT #5486.01



Training

GlobalPlatform led training sessions provide a deep-dive into the real world applications of specific security technologies

GlobalPlatform offers training courses focused on Secure Elements, Trusted Execution Environments and SESIP as well as customized in-house trainings on request.

SE for EUDI Training

This year, we have expanded our SE training offerings to include SE for Mobile eID (EUDI). The primary objective of this training is to provide delegates with a comprehensive understanding of mobile wallet and electronic identification (eID) systems, and their significance in today's digital landscape.

Shape the future of device security through GlobalPlatform membership

Join a community of security experts to drive the development of emerging security standards and contribute to the evolution of existing standards as new use cases emerge. Membership benefits include:

- Develop technical specifications and standards that address your company's security priorities
- Stand at the forefront of innovation by participating in the development of the future standardization roadmap
- Engage in knowledge sharing and access working documents as they are developed
- Network with a community of security experts from different industry verticals or parts of the device ecosystem

Member Companies and Organizations

American Express

Analog Devices

Apple Inc.

Applus+

ARM Limited

AT&T

Bactech

Beijing Unionpay Card Technology Co., Ltd.

Beijing ZhiHuiYunCe (DPLS Lab) Equipment Technology Co., Ltd

Brightsight BV

BSI - Bundesamt fuer Sicherheit in der Informationstechnik

CARIAD SE

Cartes Bancaires

CEA - Leti

Chutian Dragon Co., Ltd.

Cisco

COMPRION GmbH

Dai Nippon Printing Co., Ltd

Dekra

Department of Defense

Deutsche Telekom Security GmbH

Digital Cubes

Discover Financial Services

Eastcompeace Technology Co., Ltd

Ericsson AB

Feitian Technologies Co., Ltd

FeliCa Networks, Inc.

FIME

Galitt

Giesecke+Devrient GmbH

Google

HID Global

Honor Device Co., Ltd

Huawei Device (Dongguan) Co., Ltd.

IDEMIA

Infineon Technologies AG

Institute For Information Industry

Institute for Information Industry

Intel

Internet of Trust S.A.S.

JCB Co. Ltd.

Kaspersky Lab

Kigen (UK) Lda

KONA International

MaskTech International GmbH

Mastercard

MK Smart JSC

Monetech

Nextendis

NTT Corporation

NXP Semiconductors

Oracle

Orange

PQShield

Qualcomm Technologies Inc.

Quarkslab

Rambus

Riscure BV

Safepay Systems Ltd.

Samsung Electronics

Samsung SDS

SERMA Safety & Security

Shanghai Fudan Microelectronics Group

SK Telink

Spreadtrum Communications (Shanghai) Co., Ltd.

STMicroelectronics

Synapse Mobile Networks s.a.

TELUS Communications Company

Thales

Thales UK

T-Mobile

Toshiba Corporation

TrustCB B.V.

Trustonic

UBIVELOX

UL (Underwriters Laboratories)

Valid Soluciones Tecnológicas

Verizon Wireless

Visa

Watchdata System

Winbond Technology Ltd

Woven by Toyota

Wuhan Tianyu Information Industry, Co., Ltd.

XardPay

XCure Corp.

Xiaomi

Zwipe Germany GmbH

- 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

Asia IC Card Forum

AUTO-ISAC

AUTOSAR

Car Connectivity Consortium

CCDS

CEN

EMVCo

European Payments Council

EUROSMART

ETSI

FIDO Alliance

Fira Consortium

Global Certification Forum

GSMA

IFAA

Industrial Internet Consortium

Institute for Information Industry

ioXt Alliance

ISO

Java Card Forum

NFC Forum

NICSS

NIST

OMA SpecWorks

Mobey Forum

One M2M

PTCRB

RISC-V

SAE International

Secure Identity Alliance

Secure Technology Alliance

Smart Ticketing Alliance

TAF

Trusted Computing Group

Trusted Connectivity Alliance

Trusted Platform

W3C

Wireless Power Consortium

"Our main focus as a member of GlobalPlatform will be mobile payments and secure element (SE) technology. We will work towards aligning our testing systems with GlobalPlatform requirements in order to become an approved GlobalPlatform testing laboratory. We hope that by participating in the task forces and SE Committee we can contribute to the further improvement of technology to benefit the global payment industry."

- Guifu Fan, General Manager, BCTC

"At DEKRA, we are dedicated to upholding cybersecurity standards that foster trust in products, processes, and services. Cybersecurity certifications are more than just symbols of expertise; they are essential components in building and sustaining that trust. Certifications like SESIP go beyond demonstrating technical proficiency—they represent a commitment to rigorous standards that ensure the security of IoT devices and platforms. SESIP transcends traditional cybersecurity frameworks by addressing the unique challenges of IoT ecosystems. It offers a scalable and efficient approach to evaluating and certifying the security of connected devices, which are often more susceptible to attacks due to their widespread and sometimes overlooked deployment. This approach helps our clients find a cost-effective cybersecurity evaluation while establishing a level of security following the market's best practice."

- Rubén Lirio, Head of Cybersecurity Services, Dekra

"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."

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

Global Platform™

The standard for secure digital services and devices

→globalplatform.org