SESIP DELIVERS COST-EFFECTIVE SECURITY EVALUATION FOR IOT

SECURITY IS AN ESSENTIAL COMPONENT OF A TRUSTED RELIABLE CONNECTED WORLD.

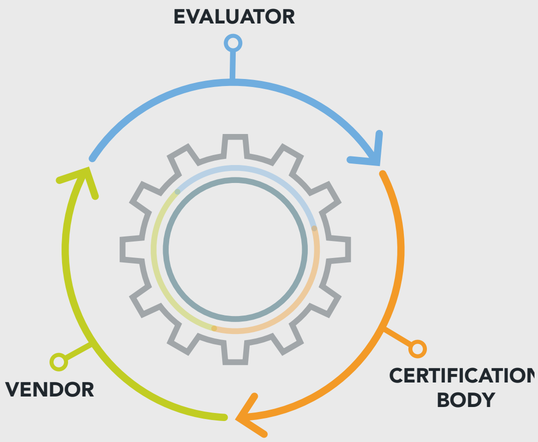
The new GlobalPlatform certification standard SESIP brings system level security validation to the IoT.

HOW DO YOU KNOW A DEVICE CAN BE TRUSTED AND SECURE?

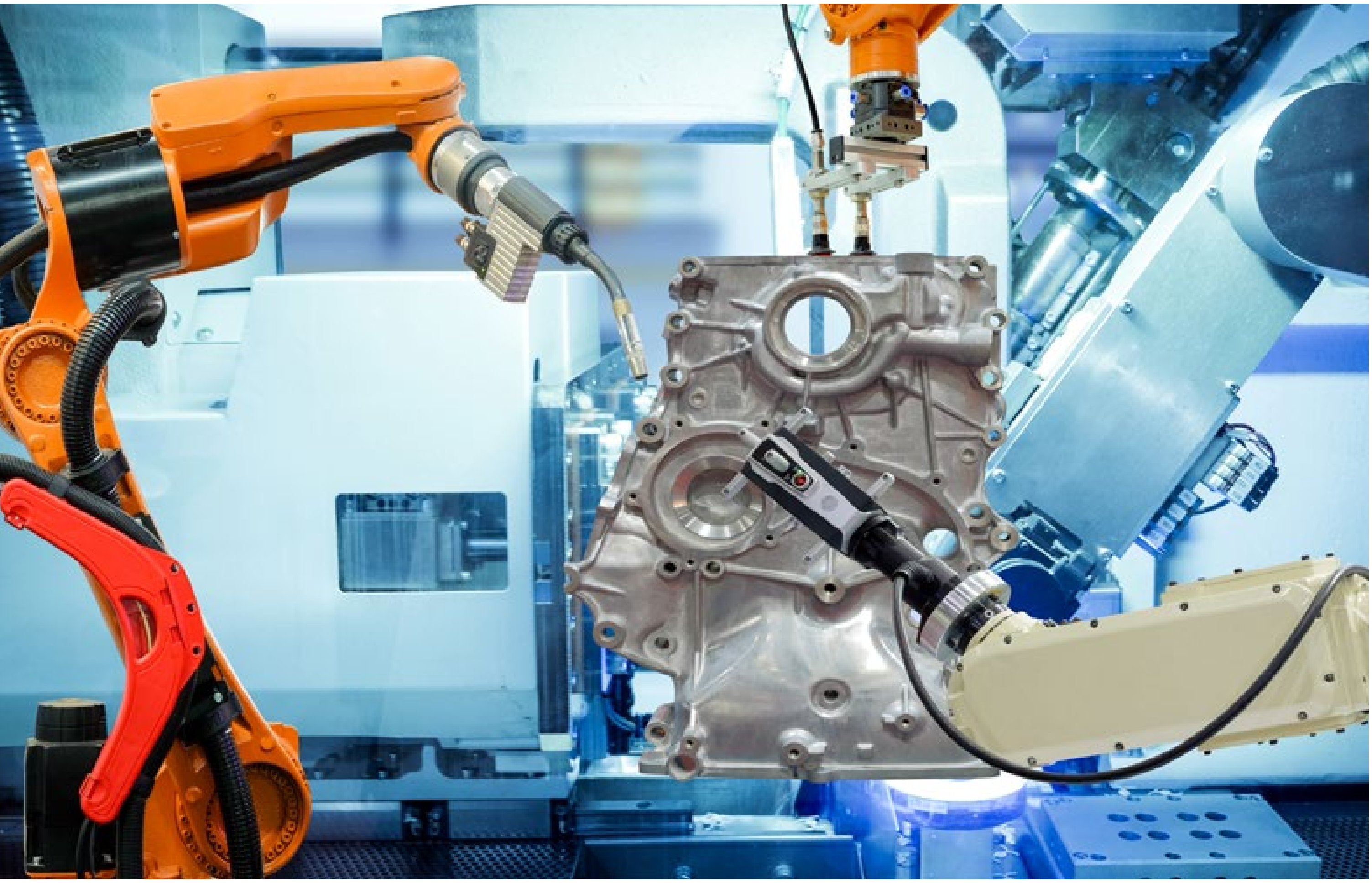
When making a purchase, and deciding which product or service to trust, third-party certifications that verify product capabilities can help narrow the options. Third-party certification can make it easier for a user to arrive at an informed, confident decision and it allows your solution to stand out. This is especially important when purchasing is based on risk mitigation, third party certification is a proven tool to aid risk assessors.

INDEPENDENCE ENSURES OBJECTIVITY

To help maintain objectivity, and avoid claims of internal bias or outside influence, the certification ecosystem needs to be free from internal company pressures and the economic demands of the marketplace. Responsibilities are typically divided between an evaluator and the certification body. The evaluator (often an independent lab) analyzes the product to determine compliance, and products that pass evaluation are then reviewed by the certification body. If the evaluator's results meet the necessary criteria, the certification body issues a certification that the vendor can use with their product.



As the Internet of Things (IoT) continues to grow, and more companies offer IoT devices of all kinds, third-party security certifications have become more important than ever. Not just because we need to verify that any given IoT device can be trusted, from a privacy and safety standpoint, but because we need to be sure the device is equipped with evaluated security capabilities. Now, more than ever, being certain that a device will protect data and withstand attempts to tamper with its operation is an essential part of the buying decision, especially when you consider the benefits a hacker can gain from remotely accessing devices and systems.



RISKY BUSINESS

Security has become a necessary feature in devices because they are potential attack targets. For example, the private information housed in the device itself may be of value to a criminal but, more to the point, the device can be an entry point for unauthorized access to the wider network. Simply put, any device that connects to another device or a network is at risk, because it's a potential starting point for mounting an attack, spreading malware, manipulating operation, or stealing information.

A secure foundation is important – and it starts at the chip level.

GAPS IN SECURITY

Dozens of standards, regulations, and security requirements from public and private sectors address issues of interoperability, accountability, and liability intended to help make connected devices more secure. There are also a number of third-party certifications that protect various aspects of IoT operation.

Together, these approaches address a number of important aspects of IoT security, but because they were developed for different reasons, at different times, and weren't really designed to work together, coverage is inconsistent. For example, there are certifications that verify only the root of trust within a device, and there are certifications that confirm device security for specific use cases, such as mobile payments. The patchwork of certifications may leave gaps in IoT device protection because only part of the security concerns may be addressed on the device.

Complicating the situation is the fact the IoT devices have become highly complex systems. What started a simple device, equipped with a few sensors and minimal computational performance, has become a sophisticated high-performance system that performs advanced computing tasks at the edge of the network. Present-day security certifications aren't designed to evaluate these highly complex devices without introducing significant costs and time-to-market delays to the device maker.

What's more, the individual sub-components of these devices are often developed by different design groups or vendors, and may be re-used across several products as a way to save on development effort and deployment cost. Having to certify a sub-component each time it's used in a new system can further increase cost and delay product introductions.

Taken as a whole, the current assembly of certifications don't address the system-level complexity of a device, or offer the level of flexibility needed by today's development cycles, and as a result can't be relied upon for an overall assessment of security. This makes it difficult for device manufacturers to demonstrate security and verify their claims of protection, and makes it difficult for end users to know which devices they can trust and which they should avoid.

ENTER SESIP

To close the gaps in IoT device security, address complexity, and verify security at the platform level, a unified yet flexible approach to security certification is needed.

One organization that has been working to define this kind of certification is GlobalPlatform, a widely respected industry forum that has maintained standards for secure digital services and devices for more than 20 years.

In March 2020, GlobalPlatform announced a new certification standards that promises to give the IoT what has been missing. Called the Security Evaluation Standard for IoT Platforms (SESIP), the new standard is defined for connected devices and meets the unique complexities and challenges of IoT device security.

WHY GLOBALPLATFORM?

As an industry-driven standards organization dedicated to security, GlobalPlatform maintains more than 180 specifications and technical documents that address a range of authentication, connectivity, privacy, and security operations. Billions of GlobalPlatform-certified products are already used in a wide range of security-sensitive applications, including biometric payment cards, cellular network connectivity, connected car, Industry 4.0, mobile authentication, premium content protection, transportation, and wearables.

- Secure financial services in multi-application smartcards and smartphones
- Secure processing with Trusted Execution Environments (TEEs)
- Secure and shareable digital car keys
- Secure mobile authentication and wearable devices
- Secure multi-application smartcards

UNIQUELY IOT-FOCUSED

The SESIP approach to IoT security certification is different from others. To begin with, it builds on the methodology used by Common Criteria (CC), the de facto standard for security certification in IT products. The CC methodology is known for being remarkably strict in its approach, with each variable, parameter, and factor given a precise definition.

SESIP uses a similar strong style of formalism in creating a universal definition for a connected platform, but SESIP uses a simplified language that offers a more understandable approach. With SESIP, a baseline of what makes a connected platform, as well as the operation of standard security capabilities, are also precisely defined.

Using the definition of a connected platform as a starting point, SESIP then identifies the threat models most relevant to the IoT ecosystem and defines the unique life-cycle stages of IoT devices that need protection. SESIP also includes support for certification re-use, so design elements can be repurposed without needing recertification, and offers several levels of certification to answer to different security market requirements (e.g. not everything needs to be super secure).

The simplified and optimized certification process of SESIP allows for cost efficiency when device makers certify a product or process.

SESIP ADVANTAGES

- Clear and lean methodology
- Concise definition of connected platform
- Protection for IoT-specific building blocks (MCUs, libraries, drivers, real-time operating systems)
- Defense against IoT-specific attacks
- Coverage for IoT-specific life-cycle phases
- Designed for re-use
- Flexible certification levels
- a supportive community of evaluators and vendors hosted in GlobalPlatform

Here's a closer look at some of the details.

Platform definition

SESIP brings together common security requirements that a secure system should implement. This allows a component's certification to be re-used if it is integrated into other devices, such as secure microprocessors, connectivity libraries, and operating systems that provide the foundation for running connected applications.

SESIP Scope

The SESIP threat model aims to protect personal data on the device, such as authentication credentials. It also protects data in transit, software code, as part of an application or platform, and data relating to product identity, configuration, system operation, and device life cycle.

Threats addressed

The ability to prevent, recover, and learn from attacks are part of the robustness assessment. Assessment covers baseline threat scenarios and may cover extended threat scenarios.

EXTENDED THREAT
BASELINE THREAT

BASELINE THREAT SCENARIO	EXTENDED THREAT SCENARIOS
• A scalable attack exploited by a remote connection	• Devices are deployed outside a physically protected area (e.g., on an external wall of a building) • People, such as service providers, are given temporary physical access to a product • Delivery of a compromised product or target into the supply chain • Someone, either an end user or an attacker, loads new software into the device

Life cycle covered

The SESIP standard recognizes that IoT devices require protection throughout their life cycle. Most IoT devices follow a basic pattern that can be broken into stages.

1 **VENDOR PROVISIONING** – The point in the supply chain when the device is assigned credentials that will be shared with the vendor's backend when accessing the network.

2 **USER PROVISIONING** – The initial deployment and personalization, when the product is put to use by the end user. This also includes equipping the user's own credentials and data that lets the device represent the end user.

3 **NORMAL USAGE** – when the device is active in the field. This phase can be terminated by a factory reset, which removes all user-related data and credentials and lets the device be used by someone else, as part of a resale, a return, or a period of temporary storage. This phase can also end with decommissioning which, if not done properly, can make confidential data stored on the device accessible even after the device is taken out of service.

4 **UPDATES** – when the vendor requires to securely update the security functionality of the device. It is essential that the device software can verify the update is genuine and it's from an authentic source.

Flexibility and Re-use

To address the fact that IoT devices are often built by assembling pre-existing hardware and software components, the SESIP methodology defines ways to independently evaluate a subset of components, and reuse the evaluation in a device. That way, subcomponents that protect critical assets and need to be evaluated at a high assurance level, can be certified once but used many times. This saves on development effort and cost.

Five levels of SESIP assurance, ranging from self-assessment to gradations of more stringent analysis, let device manufacturers choose the best match for their needs and ultimately helps device manufacturers enhance their devices.

LEVEL 1: SELF-ASSESSMENT
Utilizing public tools to discover publicized potential vulnerabilities

LEVEL 2: BLACK-GREY BOX PENETRATION TESTING
Adding vulnerability analysis and penetration testing

LEVEL 3: WHITE BOX VULNERABILITY ANALYSIS AND PENETRATION TESTING
Adding source code review

LEVEL 4: REUSE OF S0G-IS CC EVALUATION
More evidence and higher attack potential

LEVEL 5: REUSE OF S0G-IS CC EVALUATION
More evidence and higher attack potential (ex. for secure element)

SESIP is the first certification standard designed specifically to address IoT device security

THE NXP POINT OF VIEW

At NXP, we think SESIP is critical to the growth and success of the IoT because it will help build safety and trust. It’s practical, easy to use, and easy to reuse, and is backed by the strength of a recognized industry organization that operates on an international scale.

SESIP makes it easier for device manufacturers to verify the security of their offerings, and therefore increases trust in the end-user community. SESIP uses a common-sense approach, maps to major standards, and includes a library of levels and security profiles. SESIP delivers the core flexibility needed to certify a complete IoT product while being able to tailor requirements to match the needs and constraints of each vertical market.

NXP has a long history of technical collaboration and supports the idea of using third-party certifications to further industry goals. We are a long-time member of GlobalPlatform and an active participant in the SESIP Working Group. The initial SESIP standard builds on intellectual property that NXP donated to GlobalPlatform, and reflects our deep commitment to open, industry-verified security mechanisms.

As SESIP continues to develop, we will continue to help establish it as a global standard. Our IoT experts are already working with SESIP in mind, and we are actively working with our customers to evaluate SESIP for their designs.

www.nxp.com

Document Number: SESIPBR REV 0