GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Secure IoT Platforms for Consumer Internet of Things

SESIP Applicability for EN 303 645

White Paper

Security Task Force; SESIP Sub-Task Force

January 2022

SESIP™

TABLE OF CONTENTS

About Us

GlobalPlatform is a technical standards organization that enables the efficient launch and management of innovative, secure-by-design digital services and devices, which deliver end-to-end security, privacy, simplicity, and convenience to users. It achieves this by providing standardized technologies and certifications that empower technology and service providers to develop, certify, deploy, and manage digital services and devices in line with their business, security, regulatory, and data protection needs. Key offerings include secure component specifications; the Device Trust Architecture for accessing secure services within a device; the IoTopia Framework for secure launch and management of connected devices; and the SESIP Methodology for IoT device certification.

GlobalPlatform technologies are used in billions of smart cards, smartphones, wearables, and other connected and IoT devices to enable convenient and trusted digital services across market sectors, including healthcare, government and enterprise ID, payments, smart cities, industrial automation, smart home, telecoms, transportation, utilities, and OEMs.

GlobalPlatform standardized technologies and certifications are developed through effective industry-driven collaboration, led by multiple diverse member companies working in partnership with industry and regulatory bodies from around the world.

Section 1: INTRODUCTION

As a result of growing IoT cybersecurity threats, manufacturers are now requested to provide information about the implementation of security provisions. This is also being mandated by cybersecurity regulations which are under review on a global scale. ETSI EN 303 645 is one such regulation widely referenced in IoT consumer product development.

What is ETSI EN 303 645?

The ETSI EN 303 645 standard 'Cyber Security for Consumer Internet of Things: Baseline Requirements' is intended to prepare consumer IoT devices to withstand common cybersecurity threats. To do this, it outlines a set of requirements and recommendations that seek to establish a common security and privacy baseline for all consumer IoT devices by standardizing a cybersecurity code of practice for manufacturers. The standard offers a pragmatic approach to security and privacy best practice based on technical and procedural measures.

Demonstrating compliance with EN 303 645

To test consumer IoT products against the provisions outlined in EN 303 645, ETSI has published an assessment specification: ETSI TS 103 701 'Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements'. This document is intended to be used by manufacturers of consumer IoT products performing self-assessments, and by independent testing laboratories and certification bodies responsible for confirming conformance.

In order to demonstrate compliance with EN 303 645, a consumer IoT manufacturer must perform the following tasks:

- Issue an 'Implementation Conformance Statement' (ICS), defining the capabilities implemented in or supported by the IoT product.
- Issue an 'Implementation eXtra Information for Testing' (IXIT) which contains or references all of the information (in addition to that given in the ICS) related to the IoT product and its assessment environment. This will enable the test laboratory (in-house or independent) to perform appropriate test activities.
- Release a test plan, based on the ICS and IXIT.
- Perform the assessment and test activity, providing a pass or fail verdict.

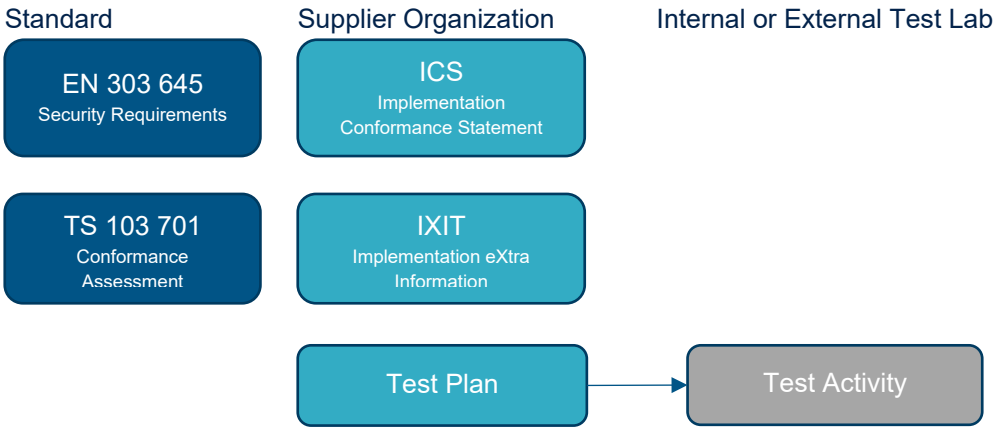

Figure 1: Using EN 303 645 conformance by means of the TS 103 701

ETSI's implementation guide, TS 103 701, gives guidance to help manufacturers and other stakeholders meet the provisions defined for consumer IoT devices in ETSI EN 303 645. It does this by defining test groups with test cases.

Listed below are two examples where the 'Security Guarantees' are the pillar of the IXIT test plans. To reduce the effort of the assessment, existing security certifications or third-party evaluations may be used partially as evidence for the conformance.

Secure communication example

Provision 5.5 in EN 303 645 states '*Communicate securely: The IoT device shall use best practice cryptography to communicate securely*'. Since security is constantly evolving, and because the appropriateness of security controls and the use of best practice cryptography is dependent on many factors, it is difficult to give prescriptive advice about cryptography or other security measures without the risk of such advice being excessive or quickly becoming obsolete. The IXIT therefore takes a holistic approach, focusing on best practice usage (protocols, operations, primitives, modes, and key-sizes) and addressing obsolescence, when known, of the applicable cryptography on the device.

The test plan addresses the appropriate measure for a 'basic-level' consumer IoT assurance:

- Focusing on what matters most, from the 'Cryptographic Details' available on the device.
- Providing focused evidence by the testing party, with flexibility for the actual implementation, depending on the use case. Checking that there are not known vulnerabilities or feasible attacks on the base of the 'Security Guarantees' on the implemented cryptography.

Software integrity example

Provision 5.7, '*Ensure software integrity: The consumer IoT device should verify its software using secure boot mechanisms*' whereby the manufacturer must show that a secure boot has been implemented to allow software to be verified on the device.

The IXIT describes the secure boot mechanisms (ID, Description, Security Guarantee, Detection Mechanisms, User Notification, Notification Functionality).

A test plan with test cases is then released:

- Assessing the conformity of design of the 'Security Guarantees' for secure boot mechanisms.
- Assessing the conformity of implementation of the secure boot mechanisms according to the 'Description' and corresponding 'Detection Mechanisms' provided by the 'Security Guarantees'.

Section 2: THE IOT DEVICE MANUFACTURER'S CHALLENGE

The great variety of IoT end-product architectures, coupled with the growing number of IoT components on the market, is introducing new challenges to the security evaluation process. IoT devices are built on blocks or modules, from hardware-level to software stack, that are not developed by end-product manufacturers. This results in IoT devices comprised of parts from multiple vendors, each containing their own intellectual property (IP) and security offerings.

As Figure 2 below shows, IoT architectures vary and involve multiple stakeholders responsible for developing and/or implementing their own security offerings.

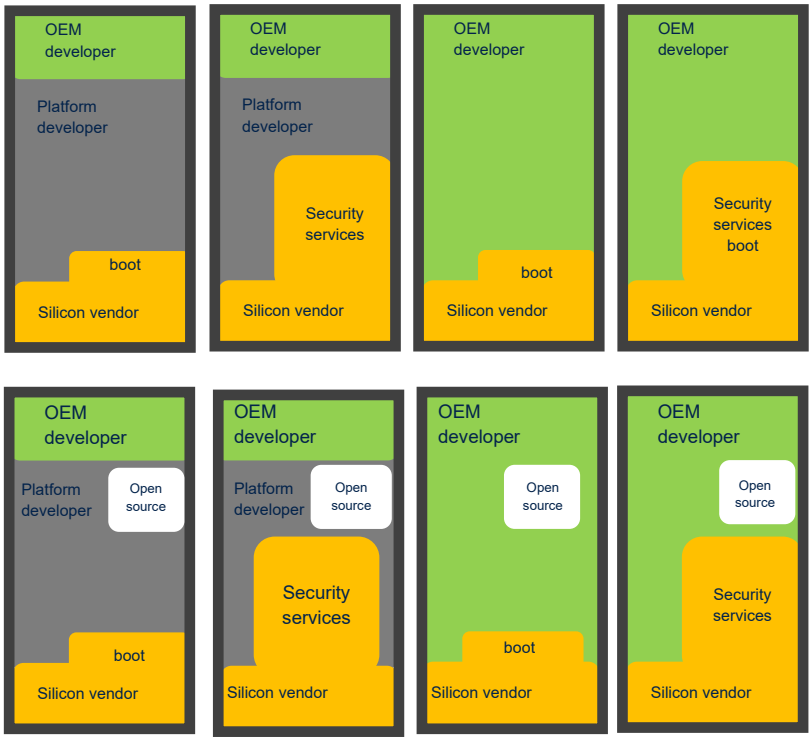

Figure 2: Examples of potential device architectures and the different stakeholders involved: Original Equipment Manufacturers (OEMs), platform developers, silicon vendors, and open-source components

The silicon component: Silicon manufacturers deliver the hardware and the boot sequence, commonly complemented by crypto libraries and security services.

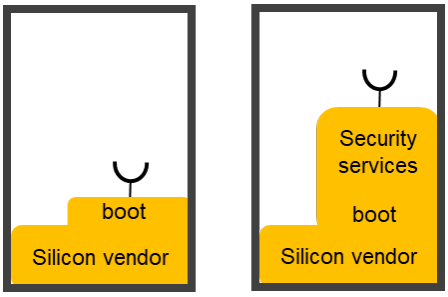

Figure 3: Silicon components in IoT devices

The software stack: Software developers and platform providers deliver the next layers of software, enriching security services that can be used by the OEM.

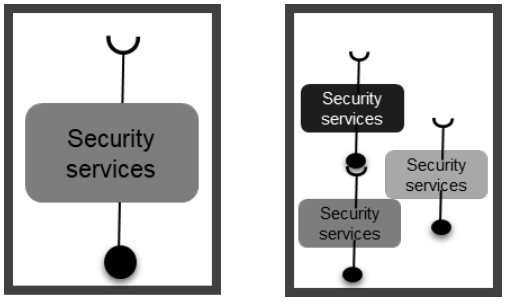

Figure 4: Software security services

The end device application developers can develop security services, or rely on underlayer security services, that are executed on the hardware platform. The latter is a more common practice as this allows each developer to focus on their core capabilities: application developers on application services and security developers on security services.

The IoT Platform: Security services, possibly delivered by different providers, are supported by the boot and other hardware security functions that can be used by the OEM to build secure solutions. This combination of hardware and software is used by the end device application developer and referred as the 'IoT Platform'.

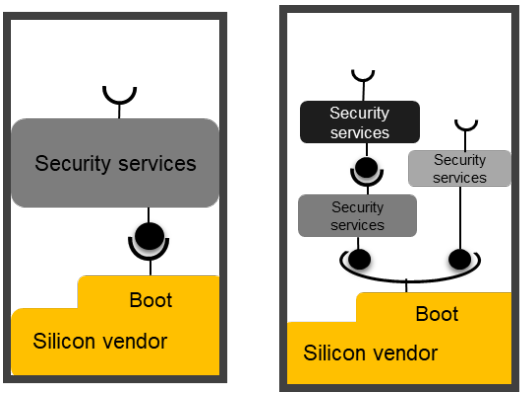

Figure 5: The IoT Platform: Hardware and software stack for security services in IoT devices

From an OEM perspective, it is challenging to demonstrate that parts from a third party conform with the necessary security requirements. OEMs may lack visibility of, or technical knowledge about, the parts integrated in their device architectures. Beyond that, due to legal, technical, and/or commercial obligations with the third parties supplying the parts, even obtaining reasonable evidence about their security functionality may fall short of demonstrating conformance with specific requirements.

Section 3: THE SECURITY EVALUATION STANDARD FOR IOT PLATFORMS (SESIP)

As outlined in section 2, IoT products are far more complex than the products addressed by traditional security evaluation approaches. The Security Evaluation Standard for IoT Platforms (SESIP) recognizes this with a common security evaluation methodology that is designed specifically for IoT platforms and the platform parts on which these products are based. It addresses the need for a standardized approach that supports a broad range of regulatory and security frameworks, while at the same time providing a methodology that's adaptable to the IoT environment and accessible to IoT developers who aren't security experts.

SESIP for security assurance

SESIP provides assurance on foundational security provided by third-party providers. It includes a catalog of Security Functional Requirements (SFRs), which allows for a consistent definition of platforms (parts) and supports a fair comparison between them. With clear and simple definitions, SFRs enable all stakeholders to understand the security functions provided by hardware components and software within IoT devices.

The SESIP SFRs define generic and intuitive security requirements with flexibility to address different use cases and the cybersecurity threats specific to them. This includes:

- Identification and Attestation: to demonstrate that the platform is the expected one and is in the expected state.
- Product Life Cycle: to secure all life cycle steps: installation, initialization, flaw remediation, secure update, decommission, field return, etc.
- Secure Communication: to allow secure communications with external entities.
- Cryptographic functionality: to assess cryptographic features.
- Compliance functionality: to assess some additional useful security features: secure storage, residual information purging, auditing, debugging, etc.
- Extra attacker resistance: to cover the different environment context of various IoT products.

The correct implementation and robustness of such SFRs are evaluated against set criteria. As demonstrated in Figure 6 below, the SESIP methodology defines five levels of assurance, constituting the Security Assurance Requirements (SARs).

To achieve SESIP certification for any one of the levels, vendors must demonstrate to an external testing laboratory that their products meet the assurance requirements outlined. It is important to note that vendors are not allowed to claim any additional requirements in a SESIP evaluation. However, a specific certification scheme may include limited refinement of the SARs in the SESIP levels.

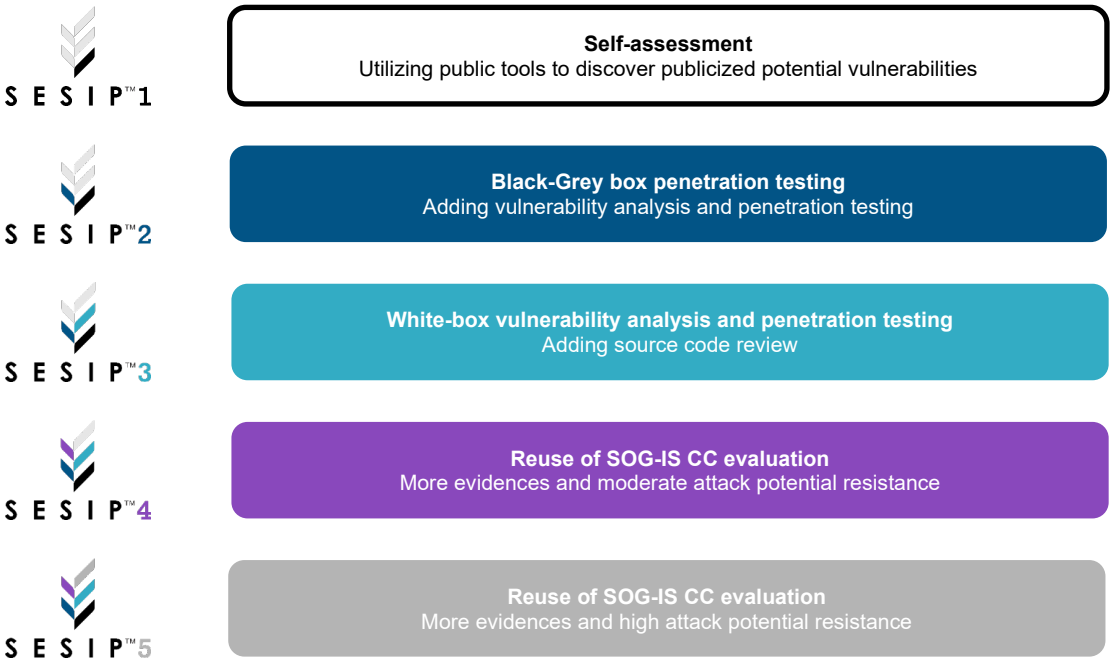

Figure 6: SESIP Assurance Levels

To summarize, SESIP is used for identifying security functionality. It provides an evaluation methodology for measuring the strength of that functionality, from different parts or components of the IoT platform, as well from the platform itself as described in section 2.

The security assurances defined in SESIP's five levels are common requirements across multiple security frameworks for IoT end devices. SESIP therefore 'plots' device security requirements against the functionality provided by the platforms and their components. This is referred to as 'mapping'. The goal of such mapping exercises is to provide evidence of the security functionality implemented at the core of the device, i.e., the IoT Platform. By mapping to other security requirements like ETSI EN 303 645, SESIP defines assurance levels that are mutually recognizable and can be reused across multiple market-specific schemes, therefore reducing time / cost of evaluation and achieving scale.

Section 4: MAPPING SESIP TO ETSI EN 303 645

SESIP is intended to work with existing standards, providing them with a framework for the evaluation of their requirements. As discussed in section 3 above, it does this by defining security requirements that can be implemented by developers and addressed in SESIP evaluations. Those requirements have been expressed at a level that covers the main features of IoT Platforms. As a result, requirements of existing standards can easily be mapped to SESIP requirements.

Demonstrating baseline security

Manufacturers wanting to demonstrate that their products meet baseline security requirements can do so through self-assessment or with a third party. This assessment is based on documented evidence and declarations, as well as technical testing of the physical device. As a result of a successful evaluation the manufacturer will receive a 'certificate of conformity'.

In general, most manufacturers are not security experts and they therefore rely on security features or services delivered by third parties. SESIP allows developers of different parts or components of the IoT platform, as well as the platform itself, to get assurance on the 'correctness' and 'effectiveness' of security features that are used to support the end device security provisions. Such developers will report and document the usage of evaluated and certified SFRs.

EN 303 645 provisions can be categorized in security mechanisms to be implemented in the end device and rules to be followed by the manufacturer. These are also applicable for developers from the software and hardware stacks.

SESIP provides:

- Assurance on the correctness and effectiveness of the implementation of security functions provided by the IoT platform, or platform parts, that are 'used' by the IoT OEM.
- Assurance that these parts, not under direct control of the end device manufacturer, are developed following rules and processes required by the norm.

Applying the provisions of ETSI EN 303 645

As the consumer IoT landscape is so broad, it is recognized that the applicability of provisions is dependent on each device. ETSI EN 303 645 provides a degree of flexibility by defining mandatory and recommended provisions. There are, however, cases where a provision is not applicable or not fulfilled by the consumer IoT device. For example, in constrained devices or for devices providing a very limited functionality, implementation of certain security measures is not possible or not appropriate to the identified risk. The SESIP approach to the evaluation of individual SFRs provides an equivalent degree of flexibility, mapping security functionality from components into ETSI EN 303 645 requirements.

To ensure that the end device is compliant with the provisions, the manufacturer will have to review each provision and identify 1) if the provision is fully developed by them, 2) if the provision, while developed by them, relies strongly on supporting capabilities developed by others, or 3) if the provision relies completely on third-party IPs.

GlobalPlatform is here to support IoT device makers and certification bodies to adopt the SESIP methodology. The organization has prepared a mapping of SESIP SFRs and SARs versus EN 303 645 provisions. Since each end device will have different functionality, the end device manufacturer will have to identify what security functionality is fully under their control either from functionality supported or by relying on mechanisms developed by other parties.

There are two important considerations for this mapping exercise: the evidence of core security capabilities (SESIP SFRs), and how to make use of such evidence.

Section 5: SECURITY REQUIREMENTS: EN 303 645 VS. SESIP SFRS

Mechanisms to be implemented by the product

To prove compliance with EN 303 645, the device manufacturer first needs to identify the security capabilities implemented, filling the table provided in an Annex of EN 303 645. The manufacturer should also provide an Implementation Conformance Statement (ICS). Some provisions can be mapped directly to a SESIP Security Functional Requirement (SFR); e.g., securely storing sensitive data can be mapped to a functional requirement of secure storage. Other provisions may require supporting security functions (e.g., communicating securely relies on the cryptographic capability of the products).

In the ICS document, the device manufacturer can refer to security functions provided by a vendor (IC vendor, OS vendor, IoT platform provider). For example, security functions such as secure storage or cryptography are used as 'black box' by the manufacturer.

'Security Guarantees' provide the foundation to address specific provisions. According to the IXIT, SESIP SFRs belong to the category of 'Security Guarantees' and guidance is provided to application developers to ensure correct implementation. With this guidance, application developers are able to address the different provisions.

An example of this is provision 5.5, '*Communicate securely: The IoT device shall use best practice cryptography to communicate securely*', with specific references to 'Cryptographic Details' as a 'Security Guarantee' expected within the provision.

SESIP certification provides evidence, in an understandable manner, of the 'Security Guarantees' provided by each component. This allows application developers to address the ICS step with a higher degree of confidence on the availability and completeness of certain security requirements.

ETSI EN 303 645 provisions are intended to be fulfilled by the application of an IoT end device. From that perspective, SESIP SFRs are not evidence of conformance, as such, against the provisions. Instead, they are the evidence of the 'Security Guarantees' used by the application for fulfilling the provisions.

Section 6: INTEGRATION RULES TO BE FOLLOWED BY THE DEVELOPER, MANUFACTURER, AND/OR VENDOR

As the conformance assessment moves into the IXIT phase, parties performing the test plan rely on the evidence of the 'Security Guarantees' provided by SESIP-certified components, using manual or automated tools to verify the proper implementation of the 'Security Guarantees'. This reduces the evaluation effort without compromising assurance in the same way that a lighter product evaluation may.

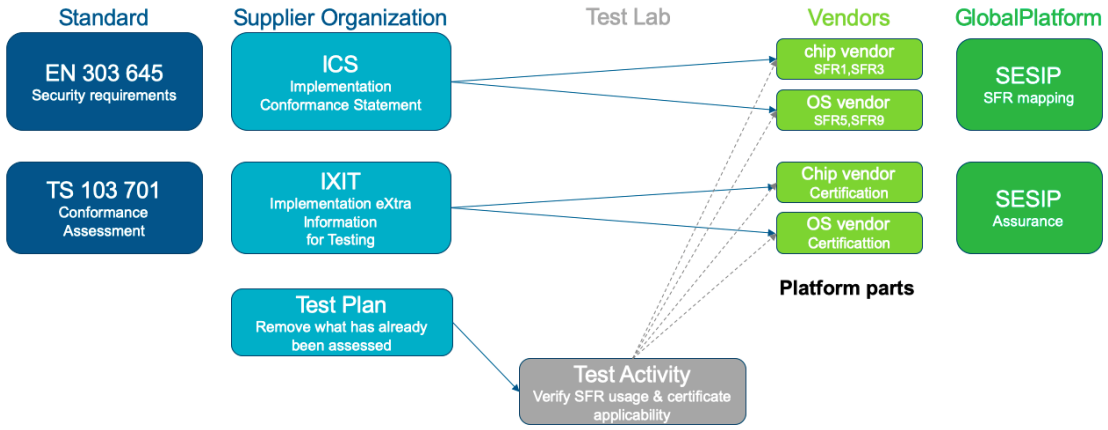

Figure 7: Using SESIP-certified sub-components reduces the effort for labs to test 'conformity of design' and 'conformity of implementation', as well as risk of non-conformity for the supplier

Using the example of provision 5.5, the 'Security Guarantees' can be deemed appropriate for the use case of secure communication only when they meet a threshold of implementation and integration. This is the case when all cryptographic details are considered as best practice for the use case and the cryptographic details used are not known to be vulnerable to a feasible attack.

As part of the test plan, the testing party will focus on verification of the adequate integration and applicability to the use case in question. When the IoT device application limits its contribution, and proper integration of suitable cryptography provided by a SESIP-certified component or platforms can be attested, then the evidence provided by the component will be deemed to address the rest of the criteria required to issue a PASS.

Similarly, provision 5.7 aims to ensure that:

- Every secure boot mechanism provides the 'Security Guarantees' of integrity and authenticity verification of the device software.
- Every secure boot mechanism and its detection mechanisms are suitable to provide the described security guarantee.

As the SESIP-certified component addresses the 'Security Guarantees' need for secure boot from a RoT, and because the application relies on the component to implement measures and countermeasures for the verification of the device software authenticity, the testing party can trust the evidence it provides and will focus on the verification of the mechanism.

Section 7: CONCLUSIONS

In summary, SESIP establishes a consistent and flexible way for IoT developers to demonstrate the security capability of their IoT products and for service providers to select a product that matches their security needs. It helps reduce the effort required by developers to demonstrate conformance to ETSI EN 303 645 by providing an approach to conformance assessments that is time-effective, cost-effective, and scalable.

The SESIP approach maps EN 303 645 provisions to SESIP SFRs, which helps developers to understand whether 'Security Guarantees' are implemented; the assurance from them; conformance to the norm; and the security dependencies of parts used as 'black boxes', not under IoT devices manufacturers' control. This minimizes the effort required from the device manufacturer when writing the conformance statement and reduces the risk of not being compliant.

SESIP also provides an efficient and swift solution for IoT device certification. The evidence provided by SESIP-certified components can be used for conformance assessments by IoT device testing parties. This is the case with the upcoming ETSI TS 103 701, where SESIP evaluations provide 'ready to use' evidence or information that simplifies the effort required by the testing laboratory undertaking the assessment tasks.

GlobalPlatform has 20 years' experience in establishing and managing security certification schemes. Through the work of its Security Task Force and SESIP sub-task force, the organization is now supporting the IoT device security certification ecosystem with the adoption of the SESIP methodology. The objective is to build consistency across IoT certification schemes (regional or vertical) to facilitate product evaluation and certificate recognition. Download the methodology here.

Section 8: ACRONYMS AND ABBREVIATIONS

Abbreviation	Meaning
CC	Common Criteria (ISO 15408)
DUT	Device Under Test
EN	Europäische Norm a.k.a. European Standard
ETSI	European Telecommunications Standards Institute
IC	Integrated Circuit
ICS	Implementation Conformance Statement
ID	Identifier
IoT	Internet of Things
IP	Intellectual Property
IXIT	Implementation eXtra Information for Testing
OEM	Original Equipment Manufacturer
OS	Operating System
RoT	Root of Trust
SAR	Security Assurance Requirement
SESIP	Security Evaluation Standard for IoT Platforms
SFR	Security Functional Requirement
SOG-IS	Senior Officials Group Information Systems Security (agreement)

Section 9: REFERENCES

Reference	Document
ETSI TS 103 645	"CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements" Version 2.1.2, 2020-06.
ETSI EN 303 645	"CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements" Version 2.1.1, 2020-06.
ETSI TS 103 701	"CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements" Version 1.1.1, 2021-08.
SESIP	Security Evaluation Standard for IoT Platforms (SESIP) v1.1, GP_FST_070, Published Mar 2020

Section 10: TABLE OF FIGURES