GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Security Evaluation Standard for IoT Platforms (SESIP)

Quantifying Benefits of SESIP Reuse

White Paper

May 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: PURPOSE

The objective of developers of Internet of Things (IoT) devices is to bring to market products that aim to operate a specific use case (home appliance, automotive, industrial, entertainment, etc.). When this use case does not have a security or safety purpose, developers focus more on functionality, usability, and performance than on security, a domain in which they generally have limited competency. However, security increasingly becomes a concern in the IoT space, as devices, users, and service providers are subject to a growing number of attacks.[1] The consumers of those devices and services, in consumer and enterprise markets, are directly affected by these security shortfalls.

As IoT device developers implement protection mechanisms in their products to raise the consumers' trust, it is important to verify that those mechanisms are adequate through self-assessment or formal evaluation by a third party, a process that can increase costs and delays.

The Security Evaluation Standard for IoT Platforms (SESIP) is a methodology designed for IoT that leverages the concepts of composition and reuse, allowing developers to focus on their core job and to reduce the pain of security assessment.

This paper aims to explain the benefits – in time, effort, and cost – of using SESIP when evaluating the security features of IoT components, platforms, and products.

Note: As this paper illustrates, adoption of SESIP can significantly reduce the burden of time, cost, and expertise required to bring secure products to market. SESIP is not, however, a substitute for in-house security expertise and ongoing support.

[1] The first six months of 2021 saw more than 100% growth in cyberattacks against Internet of Things (IoT) devices *[https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/]*

Section 2: INTRODUCTION

The core capability of an IoT device developer is generally in a particular domain outside of security. For example, an IP camera developer knows about image compression and little about data encryption. However, to serve the camera surveillance market, the security of the camera requires encryption of the video streams. It makes sense that the developer acquires this security capability from an existing security component, rather than trying to develop it independently. To make this possible, the developer needs to understand the security capability of the component (what it does), the strength of that capability for their specific use case (how good it is), and whether it helps to meet the business and use cases from compliance, risk management, and accountability standpoints.

The possibility of adding specific security functionality by integrating existing security components into their devices helps IoT device developers to focus on their core job and to rely on security specialists to bring the necessary protection mechanisms to their devices. However, IoT device developers need to ensure that the security components they integrate have been properly evaluated to prove they offer the necessary level of protection against the threats they are intended to counter.

On the other side, for security component providers, the methodology used to evaluate their security products needs to ensure that the time, effort, and cost invested in such evaluation are acceptable to guarantee the affordability and timeliness of their products.

The SESIP methodology allows security evaluations to be performed in a cost and time effective manner and has been specifically designed for IoT platforms and components. The simplicity of the language used to express security functional requirements, the applicability to an IoT threat model, and the user-friendliness make SESIP an easy-to-use evaluation methodology. In addition, by supporting composition and reuse, SESIP further reduces the cost and time of such an evaluation.

Although a ‘simple’ IoT product may not look very complex, it is generally an assembly of several individual hardware and software components providing functionalities such as encryption/decryption, memory management, random number generation, operating system, boot, and of course applications that perform the actual functions of the product. Each of these components can offer many potential entry points for attacks that might result in compromise of the entire product.

Any security vendor can claim to provide excellent security capabilities, while its competitors can claim the same. For IoT device developers, a first challenge is therefore to identify the components with the security capabilities that meet their needs. Another challenge is that even when IoT device developers select appropriate security components or platforms, they need to ensure that the components or platforms are integrated in a way that provides the needed security assurance to the final IoT device.

A previous GlobalPlatform white paper about SESIP Composition[2] outlined the importance of reusing evaluation results[3] to support the certification of Information and Communications Technology (ICT) products which are more and more built as composite products assembling a number of lower-level components.

The security evaluation of composite products comprising already evaluated elements, as well as reuse of evaluation results across certification schemes, can reduce the cost and duration of security certifications.

[2] Composition and Reuse White Paper – Introducing the Security Evaluation Standard for IoT Platforms (SESIP) [*https://globalplatform.org/wp-content/uploads/2021/06/GP_Composition_and_Reuse_WP_v1.0_PublicRelease.pdf*]

[3] Evaluation results consist of certificates and composition guidance.

Section 3: BUSINESS DRIVERS FOR SECURITY EVIDENCE

As the number of IoT devices grows rapidly, with predictions ranging from 50 to 70 billion by 2025, up to 1 trillion by 2035,[4] the number of security incidents involving IoT products grows accordingly. This increase of incidents results in consumer distrust, which is a major inhibiting factor to the deployment of billions of IoT devices in the coming years.[5]

Demonstrating the security capabilities of IoT devices becomes a solution to reduce this distrust, and security testing/evaluation is a means to achieve this demonstration.

As an evaluation methodology specially developed for IoT, SESIP is the tool that will facilitate the success of this demonstration to bring to market IoT products that are secure, protect the users' confidentiality and privacy, and protect the access and communication to remote services.

Before presenting the benefits of SESIP, this chapter looks at the multiple business drivers that require developers of IoT devices to demonstrate the security assurance level of their products. Some drivers result from external demand such as compliance with regulatory obligations and industry standards, or conformity to market access requirements and particularly to rules established by service providers. Other drivers result from internal requirements such as accountability, risk management, and differentiation.

The figure below represents those various business drivers, which are further described in the subsequent sections.

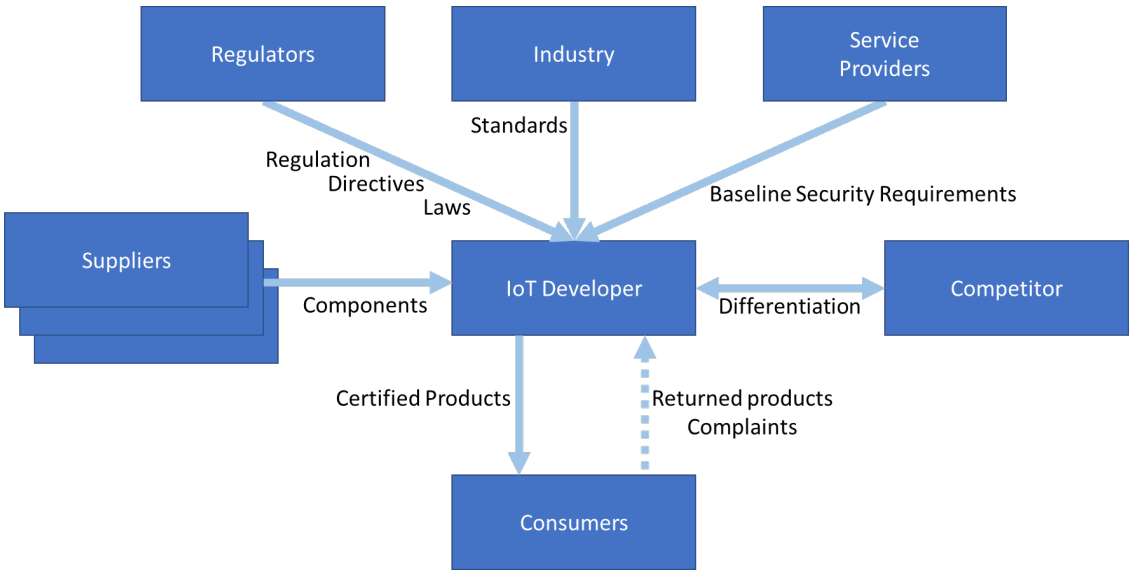

Figure 1 – Business Drivers for Security Evidence

[4] The outlook for IoT investment to 2035, Philip Sparks, June 2017 [https://community.arm.com/cfs-file/__key/telligent-evolution-components-attachments/01-1996-00-00-00-01-30-09/Arm-_2D00_-The-route-to-a-trillion-devices-_2D00_-June-2017.pdf]

[5] Harald Bauer, Ondrej Burkacky, and Christian Knochenhauer, "Security in the Internet of Things", McKinsey & Company, May 2017 [https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things]

3.1 COMPLIANCE

Compliance aims to protect consumers, but it is also a major obstacle for IoT developers. In an extremely fragmented market, with different security requirements per verticals and regions, this represents a huge challenge. Developers are confronted with hard decisions such as where they want to sell their products, and eventually pass the cost of the compliance effort to the consumer.

Device manufacturers and their suppliers face the challenge of proving compliance to existing and emerging regulations and standards in the IoT domain, since evaluating the trustworthiness of IoT devices will need more manpower than available worldwide.[6] Even if we were able to test each of those potential trillion devices at the rate of one per second, it would take thousands of years to complete the task.

3.1.1 REGULATION

In Europe, the European Union (EU) Commission has adopted a Delegated Act under the Radio Equipment Directive (RED) to expand cybersecurity requirements. The EU Commission has shown an interest in developing an open standardization request for essential requirements for a horizontal EU regulation on cybersecurity under the NLF (New Legislative Framework), with a more generic scope, specifying strategic objectives to cover cybersecurity requirements for multiple directives and regulations. Based on such open standardization requests, the European Standardization Organizations (ESOs) will develop the necessary standards which specify the security measures to support these requirements. Additionally, the Cyber Security Act (CSA) provides the framework for certification of devices, processes, and services while additional, complementary regulation such as the NIS (Network and Information Security) Directive can provide the enforcement mechanism for such certifications.

In the US, California Senate Bill 327 (CA SB-327) mandates 'reasonable security features' for connected devices. Other states such as Oregon, Illinois, Maryland, New York, and Virginia are expected to release cybersecurity regulations. After publication of 'H.R.1668 - IoT Cybersecurity Improvement Act of 2020', in 2021 the National Institute of Standards and Technology (NIST) introduced associated guidance as NIST SP 800-213. Currently, the Cyber Shield Act proposal is being considered for IoT devices. Executive Order (EO) 14028, "Improving the Nation's Cybersecurity", tasks NIST, in coordination with the Federal Trade Commission (FTC) and other agencies, to develop a proposal for baseline security criteria for consumer IoT devices, based on the NIST standard NISTIR 8259A 'IoT Device Cybersecurity Capability Core Baseline'.

[6] (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2019; Strategies for Building and Growing Strong Cybersecurity Teams [*https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482*]

3.1.2 INDUSTRY

In order to satisfy new legislation mentioned in section 3.1.1, standards bodies launch the development of certification frameworks (e.g. ETSI EN 303 645) and some countries (e.g. Singapore, Finland, Germany) introduce security labels awarded to ICT products that meet pre-defined security criteria.

Trade associations and members of the Testing, Inspection and Certification (TIC) community maintain private labels as evidence of conformance to basic cyber security hygiene, while the market expects to see some consolidation of those requirements.

3.2 ACCESS TO REMOTE SERVICES

Section 3.1 addressed compliance from the perspective of meeting regulations and/or industry standards. However, ICT products must also guarantee smooth connection and access to remote services, and must therefore demonstrate conformity to rules and protocols used by providers of such remote services.

The digital economy results from billions of everyday online connections among people, businesses, devices, data, and processes. The backbone of the digital economy is hyper connectivity which means growing interconnectedness of people, organizations, and machines in the IoT.

IoT devices are the entry point to remote services and collect data fueling those services. Untrustworthy IoT devices can provide bad data that impacts the quality of services. The ability of service providers to maintain the quality of their services has a direct impact on their bottom line, and their capacity to live and thrive in the digital ecosystem.

The IoT device market being characterized by quick time to market, price sensitivity, and low (hardware) margins, particularly for ‘simple’ IoT devices, profitability is likely to be achieved on the services. Hence the interest of service providers in managing a delicate balance: on one hand, as a transactional business, to maximize the number of operations or transactions by increasing the number of devices from multiple OEMs; on the other hand, to manage the inherent risk created by accepting access to the service from multiple devices outside of their security perimeter.

For years, service providers and device vendors have prioritized maximizing the number of users and entry points. The trend now is for service providers to create their own definition of baseline security for devices to access their services. As a result, IoT device developers need to prove that their devices implement the minimum-security capabilities that the service providers require.

3.3 SUPPLY CHAIN

Product security requirements might differ per market, per region, per use case, but they have common foundational security capabilities such as secure storage, cryptography, trusted execution, etc. This foundation generally constitutes the baseline requirements mentioned in section 3.2. The semiconductor industry provides chips with security features while software developers provide the upper security layers and IoT platforms, targeting a worldwide market. All these security foundations are implemented to support standards that may differ per region.

To understand how IoT device manufacturers shall comply with these new cybersecurity requirements, it is essential to understand the role and dependencies of multiple actors in the security development supply chain.

As an example, for billions of IoT products, secure software updates will be requested according to new EU CSA legislation article 51(j). As IoT devices manufacturers are not security experts, they usually rely on a few hundred IoT platforms providing a 'secure update' function. IoT platform developers may not be crypto experts either, so they usually rely on a few dozen chip semiconductor vendors, providing cryptography capabilities to secure the update.

Demonstrating the provenance of components as a mechanism for securing the supply chain is becoming mainstream. This provenance is not limited to hardware components. One example of the adoption of this requirement is given by the Software Bill Of Materials (SBOM) from the National Telecommunications and Information Administration (NTIA).[7]

Semiconductor vendors develop and provide cryptographic functions, to be easily used as 'black box' by non-crypto experts. Most chip vendors use the same cryptographic block in multiple products.

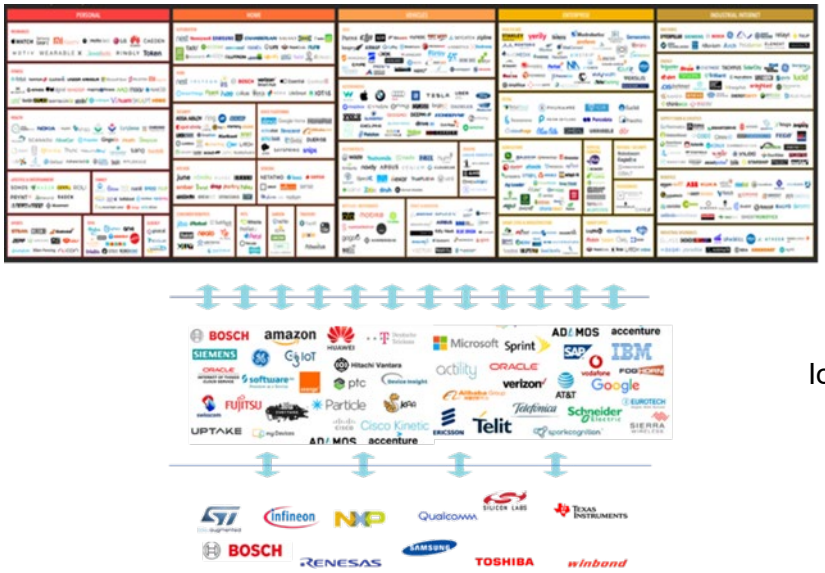

Figure 2 – Supply Chain

[7] https://www.ntia.gov/SBOM

Thus, a single security assessment of the cryptography capability done by the chip vendor provides assurance on state-of-the-art cryptography for millions of devices. Each actor in the IoT development chain should only have to prove that it effectively uses the security functions available and follows user guidance. The SESIP methodology answers that need with composition and reuse.

When IoT developers can identify the platforms and components that already implement the security features they need, they obtain security capabilities without having to develop in-house security expertise. Certain evaluation models allow for self-assessment, making use of certified platforms not just as a simple model for compliance but also as ones with evidence. For certification of IoT devices, 3rd party assessment laboratories will be in the position to perform time- and cost-effective evaluations by looking into the implementation of the certified platforms and evaluating new security functionality added on top of them.

3.4 ACCOUNTABILITY AND RISK MANAGEMENT

As explained in the introduction to this chapter, in order to enhance consumer confidence, developers of IoT devices need to implement security features in their products to minimize the risks of attacks such as:

- Theft of credentials used to operate the device and/or access remote services, and that may also be used for other products and services
- Disclosure of sensitive and private data about the owner of the product
- Unauthorized access to the network or other devices that the device connects to
- Unauthorized access to remote servers that 'trust' the IoT device, as well as potential theft of data and resources hosted by these servers
- Ability to generate network traffic that can be used for denial-of-service attacks on other systems

Connected IoT devices need to be secured not only for device protection, but also to protect the owner's assets stored on the device and ultimately the whole ecosystem (the network, other connected devices, remote services and assets, etc.)

In the event of an IoT device being compromised, it will affect the users' assets and trust, creating damages to people and companies, and potentially trigger fines, claims, recalls, financial and reputation harm. IoT developers may be accountable for these consequences and need to manage this risk.

Security evaluations provide assurance by giving tools to IoT developers to perform due diligence in risk assessment. Moreover, IoT developers making use of certified platforms inherit security functionality and strength proportionate to the risk specific to the target use cases (e.g. home, entertainment, gaming, wearables, etc.), thus demonstrating security capabilities proportionate to the risk. SESIP aims to ensure that security features implemented provide the targeted level of robustness against a given attack potential; i.e. that the technology used is appropriate to the risks identified.

Even developers who understand security cannot always be sure of the security of their devices, unless security capability and strength of the device have been evaluated by a third party, or using self-assessment, to claim a certain security assurance level. Going through an evaluation process demonstrates a willingness to be perceived as a responsible developer who performed due diligence on the security capabilities of its products. Evaluation can also create differentiation from competitors who would not act in the same way, driving the market perception that all products do not suffer the same flaws.

Section 4: SESIP TOOLBOX

The effort required by device vendors conducting security evaluations of their devices – for conformance or compliance reasons, for accountability, or for better risk management – can be greatly simplified by exploiting composition.

SESIP facilitates device security self-assessment or certification by supporting composition of certified components and reuse of certifications across different evaluations. 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 is adaptable to the IoT environment and accessible to IoT developers who are not security experts.

SESIP reduces complexity, cost, and time-to-market for IoT stakeholders by offering a methodology that's mappable to device evaluation and self-assessment, and compliant with multiple standards and regulations. SESIP security functions can be mapped to device security requirements. This mapping is already prepared for consumer IoT (ETSI EN 303 645).[8]

The benefits presented in this section apply to all SESIP assurance levels. However, while a SESIP4 or SESIP5 evaluation must be performed as a complement to a SOG-IS/EUCC certification, the cost and effort needed to prepare and execute the prerequisite Common Criteria evaluation are not taken into consideration in the savings analysis.

[8] SESIP Applicability for EN 303 645 [*https://globalplatform.org/specs-library/secure-iot-platforms-for-consumer-internet-of-things-white-paper-sesip-applicability-for-en-303-645/*]

4.1 SAVINGS IN REDUCING COMPLEXITY

The SESIP methodology reduces complexity of certification.

In the table below, we list the main benefits of SESIP and how they address the business drivers identified in chapter 3 for all stakeholders.

Table 1 – Savings in Reducing Complexity

SESIP Principle	Benefit	Beneficiary	Business Driver
SESIP supports mapping to various IoT standards (e.g. ETSI, ISO/IEC, NIST), making the reuse of SESIP evaluation results applicable to other evaluations.	Enables an easy translation of a SESIP evaluation into a specific evaluation required in a given vertical domain.	IoT developers Service providers Policy makers Device OEMs IP providers	Compliance Accountability
	Enables an efficient compliance demonstration against product regulatory requirements, and therefore accelerates time to market.	IoT developers Service providers Policy makers Device OEMs IP providers	Compliance Remote services Risk management
	Optimizes the use of resources and the learning curve.	IoT developers System integrators IP providers Evaluators	Compliance
An objective of SESIP is to build a complete environment that defines and controls a consistent use of the methodology (consistent laboratory evaluation and consistent certification body management).	Standardizes the evaluation methodology for security products and capabilities across the value chain.	IoT developers Service providers Policy makers Device OEMs IP providers Evaluators	Compliance Supply chain Risk management
	Supports a simple and coherent governance.	IoT developers Service providers Policy makers Device OEMs IP providers	Compliance
	Optimizes the certification process.	IoT developers Policy makers Evaluators	Compliance

SESIP Principle	Benefit	Beneficiary	Business Driver
SESIP is a robust methodology established by experienced hardware and software developers and laboratories.	Provides recognized security assurance with a simple and controlled methodology and governance.	IoT developers Service providers Policy makers Device OEMs IP providers	Compliance Remote services Accountability
	Reduces the time and effort that developers need to invest on security evaluations compared to having to learn complex terms and methodologies.	IoT developers Device OEMs IP providers	Accountability & Risk management
	Helps developers certify their products to the current-best-practice security. Allows them to efficiently create evidence needed for certification.	IoT developers Device OEMs IP providers	Accountability & Risk management
SESIP supports a composition and reuse approach.	Allows developers to source qualified and proven components to integrate in their products.	IoT developers Service providers Device OEMs IP providers	Supply chain Compliance Remote services
	Allows developers to certify secure products, based on previously certified secure components.	IoT developers Device OEMs IP providers Evaluators	Compliance Accountability & Risk management
	Allows developers to focus on their core job and to reduce the pain of security assessment.	IoT developers IP providers	Accountability & Risk management

4.2 SAVINGS IN PREPARING FOR EVALUATION

SESIP allows IoT product developers to specify the security properties of the product being evaluated (Security Target or ST) in an easy and efficient way. This also allows the laboratories to be fast and effective in reading and analyzing the ST.

By simplifying the structure and formalism of Security Functional Requirements (SFRs) and maintaining a strict catalog of those SFRs, SESIP turns the development of STs into a selection of those SFRs that are needed to meet the security objectives of the product.

The efficiency gain indicated in the rightmost column of the following table represents an estimate of the typical savings (expressed as a reduction of cost spent, effort expended, and time consumed) compared to a more complex evaluation methodology such as Common Criteria.

Table 2 – Savings in Preparing for Evaluation

SESIP Principles	Benefits	Beneficiaries	Typical Efficiency Gain
The SESIP SFRs are tailored for simplicity and accessibility, and they are written in plain English rather than in a formal language.	Optimizes communication with all stakeholders in the market.	IoT developers' marketing Evaluators	High
	Optimizes time and effort needed to learn the methodology.	IoT developers Service providers Device OEMs IP providers	Medium to High depending on the depth of learning
	Optimizes time and effort needed to write Security Targets.	IoT developers IP providers	High
	Optimizes time and effort needed to analyze and integrate components.	IoT developers Device OEMs	Low
Each SESIP SFR targets a full security purpose by itself, rather than being split into low level generic mechanisms.	Allows the Security Target writer an intuitive understanding of the security requirements, which saves time in analysis. *Note: Accessibility does not imply oversimplification; the semantics of SESIP SFRs is precisely defined, so there is no ambiguity about the meaning of the SFR, even expressed in plain language.*	IoT developers, Device OEMs, IP providers Service providers Evaluators	Low to Medium Low Low

SESIP Principles	Benefits	Beneficiaries	Typical Efficiency Gain
SESIP maintains a catalog of SFRs as an essential part of the methodology, which allows for consistency and reuse. This catalog defines a set of security features that are essential, and for which there is a shared understanding in the community, likely to be accessible to IoT developers.	Simplifies reusability while maintaining SESIP's formalism, which saves time in Security Target writing.	IoT developers Service providers Policy makers Device OEMs IP providers	Low to Medium depending on complexity
The catalog of SFRs will evolve over time, following the evolution of IoT security challenges and the growing usage of SESIP methodology. IoT developers may also want to differentiate their offering by including specific or innovative security features to enrich the catalog.	Promotes reuse and accelerates the development of Security Targets through enrichment of the catalog of SFRs.	IoT developers Service providers Device OEMs IP providers	Incremental gains over evaluation iterations

4.3 SAVINGS IN EXECUTING THE EVALUATION

As a result of the composition approach, evaluating a compound product that assembles already evaluated components will generate savings in cost (thanks to the effort reduction) and in time (generated by an acceleration of the evaluation itself).

For example, when performing an EN 303 645 evaluation, following the companion document TS 103 701 'Conformance Assessment of Baseline Requirements', use of a SESIP composition approach addresses two key elements:

- At the beginning of the evaluation, developers assess the security capability of their products to complete the 'Implementation Conformance Statement' (ICS).
    - Making use of IoT certified platforms, developers gain insights into the functionality of the security capabilities available in their product, and reflect on their own usage and the level of assurance provided by that security capability.
    - Without SESIP composition, developers must assess the security functionality of their products based on information available from the suppliers of the different software and hardware components, plus the security capability they themselves developed, as well as their integration, in order to complete the inventory of security functionalities in place.
- Test plans are developed using input from the 'Implementation eXtra Information for Testing' (IXIT) as an initial inventory of the security functionality evidence.
    - Making use of IoT certified platforms simplifies the test plan, reducing the time and effort by focusing on proper usage of the security capability provided by the platform, rather than preparing to test the robustness of such capability.
    - Without SESIP composition, evaluation parties have to create test plans to address the security functionality provided and its robustness. Moreover, with EN 303 645, developers provide their own self-assessment results without third-party check. SESIP1 supports a self-declaration exercise with a third-party check and certification, providing harmonization criteria for all developers.[9]

The efficiency gain indicated in the rightmost column of the following table represents an estimate of the typical savings (expressed as a reduction of cost spent, effort expended, and time consumed) compared to a more complex evaluation methodology such as Common Criteria.

[9] SESIP Applicability for EN 303 645 [https://globalplatform.org/specs-library/secure-iot-platforms-for-consumer-internet-of-things-white-paper-sesip-applicability-for-en-303-645/]

Table 3 – Savings in Executing the Evaluation

SESIP Activities	Benefits	Beneficiaries	Typical Efficiency Gain
Documentation analysis	• Reuse of component evaluation results • Linking/pointing to previous evaluation results	IoT developers Service providers Policy makers Device OEMs IP providers	Medium to High
Hardware review	• Reuse of evaluation results of components already evaluated when integrated into a compound • Reduce meetings, calls, and Q&A	IoT developers Device OEMs IP providers	Medium
Code review	• Reuse of evaluation results of components already evaluated when integrated into a compound • Reduce meetings, calls, and Q&A	IoT developers Device OEMs IP providers	Medium to High
Test strategy definition	• Leverage previously defined strategies • Reduce time needed to define test strategy • Reduce interaction with developer	Evaluators	Medium to High
Vulnerability assessment	• Leverage previously assessed components	IoT developers IP providers Evaluators	Medium
Test plan development	• Leverage previously defined test plans	Evaluators	Medium to High
Test campaign	• Reduce number of tests executed • Additional testing limited to features added by composition • Reduce fix/retest loops with developer	IoT developers Device OEMs IP providers Evaluators	Low
Report writing	• Reuse sections from previously evaluated components	Evaluators	Medium

Thanks to the composition and reuse promoted by the SESIP methodology, evaluators will be more effective in performing their evaluation activities. The expectation is that this reduction in effort will be reflected in savings for the IoT developer, where savings include time, money, and even resources involved in the evaluation. In addition, the developer will obtain a certificate more quickly, ultimately benefiting the go-to-market of the certified product.

Although it may appear that saving in evaluation effort may result in a loss for the laboratories, it can actually be expected that with certification becoming faster and cheaper, the number of products to evaluate will increase, generating more work for the labs. This is exactly the virtuous circle needed to bring to market products which are safer and more secure.

Section 5: COMPOSITE EVALUATIONS: THE BOTTOM LINE

The economic benefits from composite evaluations of IoT devices come from multiple grounds since there are direct and indirect cost implications. By definition, security evaluations have an implicit cost and IoT developers are looking to offset the cost with a clear benefit, to achieve a positive Return On Investment (ROI). In that sense, costs are calculated as the initial cost, or cost of the evaluation itself, plus the running cost, or subsequent cost of supporting the developer's customers in their own certifications.

Consider the scenario:

- A device needs to demonstrate the use of a TLS stack (TLS) during a security evaluation.
- The developer of this TLS stack, Developer A, uses a crypto library (CL) from another developer, Developer B.
- Developer B uses an AES engine from crypto hardware (CH) developed by Developer C

When Developer A is looking to certify his TLS stack, it is cheaper to certify the combination of the whole TLS+CL+CH as a single product. When this evaluation is one-off, there is no business case to justify the individual evaluation of three different components from three different developers.

The IoT market is different in that regard. A single component, hardware and/or software, can end up in hundreds of different applications and used by a large number of IoT developers that will make use of that evaluation evidence across multiple compliance and risk management scenarios, not to mention the differentiator element.

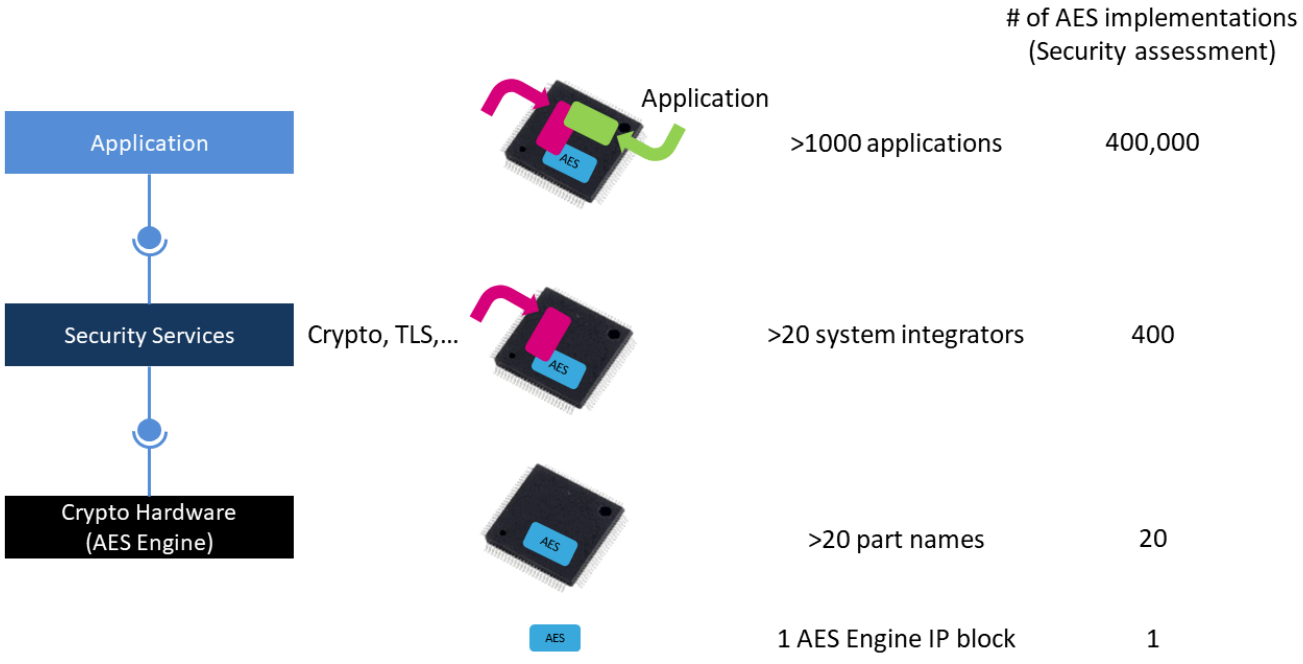

Figure 3 – Scalability of Business Benefits of SESIP

From the above example, we can assume there are *n* number of TLS developers, Developer A*n*, and *m* number of crypto library vendors, Developer B*m*.

- Developer C certifies the crypto hardware (CH) once.
- Developer C creates distribution/certification packages for CH, including composition manuals and other materials that help each purchaser to certify its own product, while reducing the effort from Developer C during each of those evaluations. Developer C spreads the cost of certification across the anticipated number of sales to Developer B*m*.
- The certification as a key market differentiator appeals to Developer B*m* as the alternative to uncertified crypto hardware from developers other than Developer C.
- Developer B*m* calculates the risk of having the right support from any crypto hardware developer versus mitigating the risk by using the certified crypto hardware from Developer C.
- Developer B*m* purchases the crypto hardware from Developer C and develops a crypto library (CL) that incorporates the crypto hardware.
- Developer B*m* certifies the CL compound.
    - Developer B*m* and Developer C can use different laboratories.
- Developer B*m* creates distribution/certification packages for CL, including composition manuals and other materials that help each purchaser to certify its own product, while reducing the effort from Developer B*m* during each of those evaluations. Developer B*m* spreads the cost of certification across the anticipated number of sales to Developer A*n*.
- Developer B*m* sells their CL to Developers A*n*.
- When Developer A*n* certifies their TLS, besides the time and cost-effective evaluation under composition, they obtain the additional benefit of not having two or more different developers involved in a single evaluation, minimizing their risk on issues with IP, division of costs, uncertainty about who has an issue when a vulnerability is found, etc.

With more and more components being certified, the evaluation of compound products that combine several components will be even faster and easier, reducing both the time spent for evaluation, and the cost of this evaluation since the necessary effort will be lessened:

- A vendor reusing the same evaluated component(s) in multiple compounds will realize multiple savings through all compounds evaluated.
- The developer of a final product that needs to be evaluated will be encouraged to look for proper implementations of already evaluated components, reducing the time and cost of the evaluation of the final product.
- The evaluation of a compound assembling one or several components previously evaluated will diminish the necessary test coverage of the compound.

A virtuous circle is created since reduction of the cost and time of component evaluations will stimulate more developers to evaluate their components, and more integrators to assemble components into products that will themselves become evaluated products, increasing the number of certified components, further reducing the cost and time of composite evaluations.

The concept of reusing previously evaluated components introduces some ROI analysis into the certification process, something which is rarely done today where certification is seen as a pure cost. Indeed, a fraction of the cost of evaluation of one component can be charged back (or factored in) on all compounds using this component. Therefore, the evaluation of one component can significantly encourage its reuse in compounds and devices.

Section 6: BENEFITS OF SESIP EVALUATIONS

As mentioned earlier, SESIP and its composition model will benefit multiple actors throughout the value chain. This chapter provides examples of direct and indirect benefits to various stakeholders.

6.1 BENEFITS TO CHIPMAKERS

- Increase the overall security value of a chipset
  - A security evaluation helps to assess the security capabilities and performance of hardware and software components present in a chipset, reducing post market risk while improving in-house security knowledge and capabilities.
- Reduce operational costs
  - Core security capabilities can be certified and reused across chipset families and tiers.
  - Reduced need to support developers who want to perform security evaluations using the chips, as they can reuse evaluation results and make use of the guidelines
- Clear market differentiator
  - Clear definition of security capabilities against competitors based on evaluation results

6.2 BENEFITS TO SOFTWARE DEVELOPERS

- Increase software value by leveraging certified hardware protection mechanisms
- Offer software components with security capabilities clearly evaluated
- Deliver certified software components with evaluation results that can be directly re-used through the composition model by a customer or by themselves in another software component.

6.3 BENEFITS TO SYSTEM INTEGRATORS

- Encourage integration of certified components with evaluation results that can be re-used, instead of (re)developing capabilities in-house
  - Cost related to research, design, development, and testing of security functionality is diverted to the use of products with proven core capabilities.
- Reduce evaluation cost and time by re-using evaluation results from integrated components.
- Improve time to market by reducing development and evaluation duration.
- Reduce the risks of expensive recalls and lawsuits.

- Relying on certified components for critical security related functions of the product reduces risk.

6.4 *BENEFITS TO OEMS AND SERVICE PROVIDERS*

- Meet compliance
  - Meet device security functionality requirements thanks to demonstrable security capabilities provided by incorporated components/platforms.
  - In the case of self-assessment, identify components implementing the necessary security functionality and produce evidence based on component certification.
  - In the case of 3rd party evaluation, upon recognition by the relevant scheme of the evaluation results, the evaluation laboratory leverages the component results for evaluating the device rather than re-evaluating the components.
- Reduce cost and time
  - Composition encourages the use of security features from evaluated components rather than developing that capability in-house, allowing more devices to access services safely.
- Reduce cyber disaster impact and recovery
  - Using certified components reduces the risks of security failures on the device as well as on the services that the device uses.

6.5 *BENEFITS TO CONSUMERS*

- Reduce the threats and the risks of fraud, leakages, flaws, etc.
  - Consumer devices that integrate components providing certified security capabilities are less prone to security problems and more resistant against attacks.
- Help the consumer to identify devices with the desired level of protection.
  - When certification of IoT devices becomes mainstream, implementing labeling programs on devices will be an easy and friendly way to provide security information to the consumer.
- Trusted services and privacy
  - Consumers are willing to adopt digital services and digital technology, and trust is a key component of this adoption. A consistent and trusted methodology for evaluation, plus a recognized system of security labeling, will enable consumers to expect that security on the devices they select is given, transparent, out of the box, and reliable.

Section 7: CONCLUSION

The Security Evaluation Standard for IoT Platforms (SESIP) is a methodology designed for IoT that leverages the concepts of composition and reuse, allowing developers to focus on their core job and to reduce the pain of security assessment.

This paper briefly discusses composition and reuse in the development and evaluation of IoT products, and outlines specific benefits of these approaches to a variety of stakeholders.

Benefits range from reduced cost, effort, and duration of evaluations – affecting all in the IoT supply chain – to enhanced customer confidence in the security being offered to them.

The composition approach multiplies these benefits as more and more components are used in compounds that themselves become components in higher level compounds, and so on.

GlobalPlatform welcomes collaboration from the entire ecosystem. Interested parties can download the methodology from https://globalplatform.org/sesip/ and contact GlobalPlatform at secretariat@globalplatform.org to help the organization encourage the expansion of security certification to a wider set of products, without compromising the quality of evaluations.

Section 8: TABLE OF FIGURES

Section 9: TABLE OF TABLES