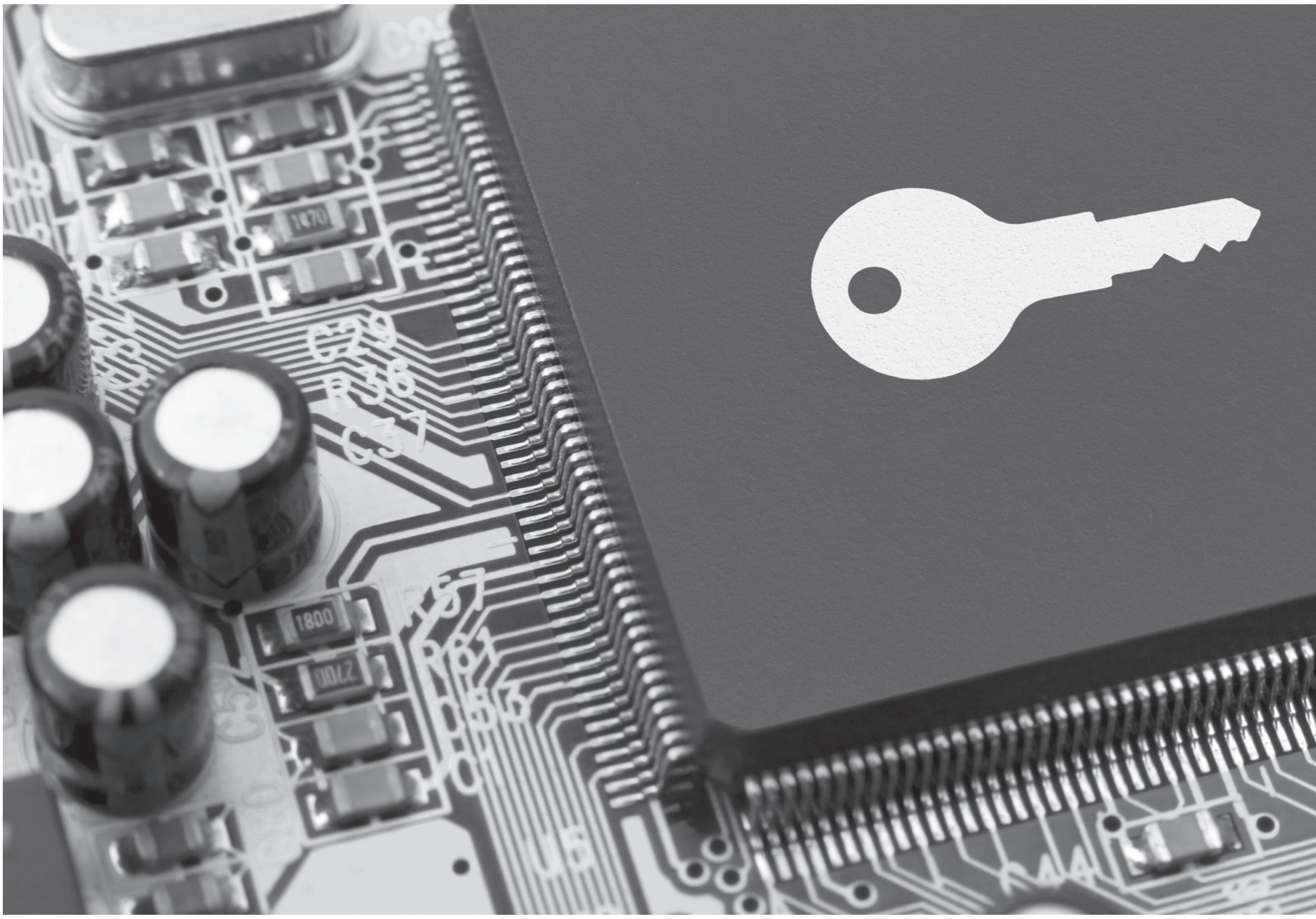
Trusted Labs

SECURITY EVALUATION OF **TRUSTED EXECUTION ENVIRONMENTS:** WHY AND HOW?

TRUSTED LABS WHITE PAPER 2013

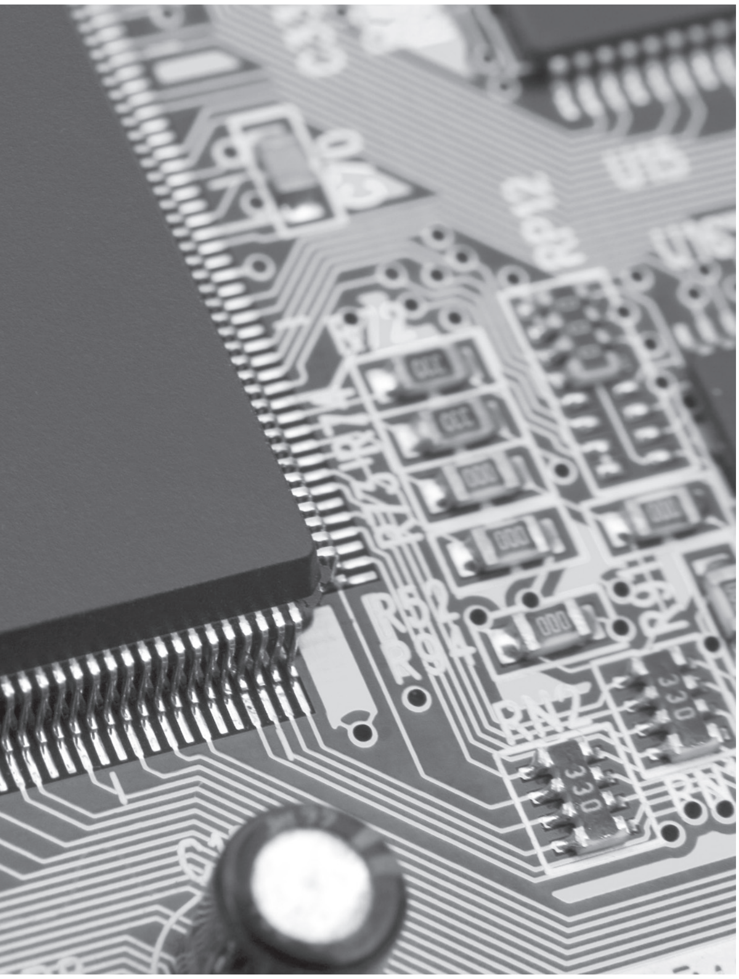


Summary

1. Executive summary p. 3
2. Why a TEE security evaluation and who could benefit from it? p. 4-5
3. What is the GlobalPlatform Protection Profile and how can it help? p. 6-10
4. How to proceed to certify a TEE? p. 11-12
5. Conclusion p. 13

About Trusted Labs p. 14

Appendix - Abbreviations p. 15



1. Executive summary

Trusted Execution Environments (TEEs) are increasingly recognized in the mobile ecosystem as a key component for the deployment of sensitive applications such as digital content protection, enterprise services or financial services on mobile devices. A TEE is an execution environment that resides in the main processor of a mobile device and ensures that sensitive data is stored, processed and protected isolated from the standard mobile Operating System (OS). Because TEEs should form an essential security building block, their evaluation is a critical step towards more secure devices allowing service providers and consumers to benefit from trustworthy environments. For this reason, defining a security certification scheme has been identified by GlobalPlatform as a key factor for the adoption of TEEs by the mobile market. To address this need, the GlobalPlatform Device Committee has defined a Common Criteria Protection Profile for TEEs. The availability of a Protection Profile (PP) greatly facilitates the preparation of an evaluation. However, a TEE interacts with many different components. It is thus necessary carefully to define its boundaries, its interactions with its environment and the assumptions made on this environment. In this White Paper we review the benefits of TEE security evaluations for all actors in the ecosystem; provide a sketch of the GlobalPlatform TEE PP and outline a methodology for the evaluation of TEEs based on this Protection Profile.

2. Why a TEE security evaluation and who could benefit from it?

Connected devices: High-security challenges

While more and more services are available on connected devices (mobile phones, tablet computers, set-top boxes, automotive infotainment systems, smart-TV etc), which have become indispensable to users, it has become clear that strong security guarantees are necessary to ensure the sustainability of this ecosystem. But ensuring the security of connected devices is not easy: because connected devices are both permanently connected and in the hands of their users, they are prone to security attacks from the outside (network) and the inside (user). In addition, they contain a lot of sensitive information about their owners and for third parties. As a result, the security stakes are very high: the benefit for attackers can be substantial and stakeholders can incur serious losses. Not surprisingly, an increasing number of security attacks on connected devices are being reported and many more are bound to occur[1]. The biggest impact for the industry might be in terms of trust: repeated stories about attacks making newspaper headlines are likely to have a detrimental effect on end-user trust, and therefore hinder the development of new services.

TEE: Key security component

The security of a connected device relies on two main types of component. The first is the Secure Element (SE), which consists of different smart card chip form factors (e.g. SIM cards for mobile phones or micro-SDs). SEs provide strong security, including physical tamper resistance, cryptographic libraries and the secure storage of data and keys. The second is the Trusted Execution Environment (TEE), promoted[2] and standardized by GlobalPlatform[3]. A TEE provides a way of enhancing the security of mobile devices and executing sensitive operations on devices running standard, general purpose, operating systems. It relies on hardware roots of trust for boot and storage; provides cryptographic functionalities; allows for the secure storage of data and keys and executes Trusted Applications (TAs) in a controlled environment separate from the mobile OS. The TEE establishes a clear boundary with the standard execution environment under the control of the general-purpose OS. Moreover, it enforces the isolation between itself and the TAs as well as between the TAs themselves. Additional services, such as Digital Right Management applications, mobile wallets and mobile TPM, represented by TAs, can run within a TEE. The GlobalPlatform standard defines the internal APIs used by TAs and the external (client) APIs to allow mobile OS applications to access the TEE through a specific driver.

(1) See, for example, ENSIA Threat Landscape - Responding to the Evolving Threat Environment - Deliverable – 2012-09-28 and F-Secure Mobile Threat Report Q1 2013.

(2) The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market, GlobalPlatform White Paper, February 2011.

(3) GlobalPlatform is a cross-industry association which develops and publishes specifications to facilitate the secure and interoperable deployment of embedded applications on secure chip technology: http://www.globalplatform.org/

In contrast to SEs, TEEs do not require tamper-resistant hardware. However, they play a key role in the protection of user interactions which is often the Achilles heel of security architectures. In some sense, they can be seen as a way to extend the security guarantees on the device itself.

Even though they are not yet widely used in smart phones, TEEs have already been deployed on millions of devices and major rollouts are expected in the near future.

Need for security evaluations

While many SEs have undergone security evaluations and have been certified, in particular with respect to the Common Criteria, the situation is quite different for TEEs, probably because their development is still relatively recent. Because of the significant security challenges posed by connected devices and the key role of TEEs in their security architecture, security evaluation is bound to become essential in this area as well.

The key benefit of a security evaluation is to enhance trust in a product. This enhanced trust is not just a matter of image (using certificates for marketing purpose): evaluation schemes, because they rely on well-established methods and capitalize on long-term expertise, can be very effective ways of improving the security of a product.

As a result, security evaluations can be beneficial to all actors involved in TEE and the connected devices ecosystem:

- Application providers would benefit from a higher level of trust from consumers, which means an enlarged market. Conversely, losing the confidence of its users can prove a death warrant for an application provider.
- Application providers would also get themselves a higher level of trust in the execution environment hosting their applications, which can be critical for their business.
- Similarly for chipset manufacturers, TEE providers and device manufacturers, security will increasingly become a differentiating factor and security evaluations a very effective investment.

The next questions that arise, then, are: what is the starting point for the evaluation of a TEE? And are there appropriate evaluation schemes and useful documents to help a candidate for a TEE certification? In the next section, we focus on the Common Criteria, a widely recognized evaluation scheme, and introduce a Protection Profile which has been recently recently defined to evaluate TEEs.

3. What is the GlobalPlatform Protection Profile and how can it help?

Common Criteria: An international standard

The Common Criteria (CC) is an international standard for the certification of the security of IT products. National schemes consist of certification bodies, which are generally governmental agencies or bureaux of the national defence ministry. Evaluations rely on competent and independent licensed laboratories. Laboratories are accredited by a national accreditation body, and licensed or otherwise approved by the national certification body. Accreditation bodies themselves have to conform to ISO requirements and their international recognition relies on multilateral recognition agreements.

The first task in the CC process is the definition of the perimeter of the product to be evaluated (TOE: Target of Evaluation), which can be software or a combination of software, firmware and/or hardware. The second is the specification of the Security Target (ST), which sets out the security functional and assurance requirements for the TOE and the assumptions on which the operational environment is based. Together, the TOE and the ST define the scope of the evaluation: its aim (the TOE) and the security properties that have to be met (the ST).

An ST includes:

- An overview of the TOE;
- The assets to be protected (e.g. the authenticity, integrity and confidentiality of cryptographic keys);
- The threats to be considered (e.g. an attacker cloning the TOE with the potential threat to all assets);
- Organizational security policies (e.g. the generation, storage, distribution, destruction and insertion of cryptographic keys into the TOE need to enforce the authenticity, integrity and confidentiality of the keys);
- Assumptions about the TOE's environment (e.g. it is assumed that the TOE is protected by the environment after delivery and before entering the final usage phase);
- Security objectives of the TOE and the environment (e.g. the TOE shall ensure that cryptographic keys are protected against unauthorized disclosure); and
- Security requirements for the TOE.

Security requirements are divided into two categories: Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

SFRs must reflect the security objectives of the TOE. The CC official documents (Part 2) provide a predefined set of components which can be used to define the SFRs. SARs define the type and level of assurance provided by the evaluation. The CC official documents (Part 3) provide predefined components which can be used to define the level that is appropriate for this TOE and also predefined sets of assurance requirements - Evaluation Assurance Levels[4] (EALs) - ranging from EAL1 to EAL7.

The ST can define and use additional functional or assurance requirements to achieve specific security goals. In addition, the ST includes a rationale:

- Showing that all security objectives are covered by SFRs (completeness);
- Showing that each SFR traces back to at least one security objective (necessity); and
- Explaining that the chosen set of SARs is appropriate (adequacy).

[4] *EALs are well-known in some IT domains, for instance in the smart card industry, where EAL4+ has become the standard. However, it is commonly admitted that the EAL paradigm alone cannot provide the basis for the comparison of very different IT products, which has to be done through the use of Protection Profiles dedicated to each type of product.*

As a result, if all SFRs, SARs and security objectives for the environment are met, then all the threats against the TOE that have been identified in the ST will be countered or mitigated.

Protection Profiles

Writing an ST from scratch could be a complex task for non-experts, but the CC provides a very useful tool to make it easier - the concept of the Protection Profile (PP). PPs are sets of security requirements for a type of product that may support different implementations. They have been defined for many categories of products including firewalls, general-purpose operating systems, smart cards, payment terminals, electronic passports, USIMs, etc[5] – and, very recently, TEEs. Typically, a PP can serve as a template to build an ST for a specific TOE. Because PPs are independent of any product, they leave open the implementation details or characteristics that are not mandatory for all these types of products. It is the role of an ST to instantiate all the requirements that are left open in the PP.

The use of PPs to address the security of a type of TOE is recommended by the CC community of consumers, developers, laboratories and certification bodies and is at the core of the new CC Recognition Arrangement.

The GlobalPlatform TEE Protection Profile

GlobalPlatform has put TEEs at the top of its list of priorities for the development of secure architectures for connected devices and promotes CC certification as a key step to standardize TEE security. To facilitate the evaluation of TEEs, the GlobalPlatform Device Committee[6] has recently published a dedicated Protection Profile[7].

Both from security and functional points of view, the TEE is an intermediate level between SEs and the standard OS. Indeed, the purpose of the TEE is to provide the processing power of the mobile device and at the same time a reasonable protection for assets that enables the deployment of sensitive services. Two main questions have driven the development of the PP:

- What are the main security properties that need to be enforced?
- What security level can the TEE reach?

This PP provides specifications, options and guidance to support the preparation of a CC evaluation, based on the experience of the key industry players involved in the Device Committee. In particular, it covers the definition of the TOE, the definition of the security problem (assets, users, threats, organizational security policies and assumptions), the security objectives and the security requirements. In addition, it provides the rationales to show that (i) all threats are covered by security objectives, (ii) all security objectives are covered by security requirements and (iii) the assurance requirements are consistent.

Because a PP defines a generic security framework which can be used for different products of the same family, it leaves room for choice and product vendors can adapt the framework to the needs of their specific product. In addition, the TEE PP introduces a methodology and guidance metrics for evaluating what a malicious actor needs to do to perform a successful attack. The attack quotation grid is inspired by the standard smart card quotation table with modifications, due to the fact that TEEs, in contrast with smart cards, are security components for general-purpose devices. Also, two different types of attackers are considered in the TEE PP: those acting during the identification phase, who can use strong means (equipment, time, expertise etc) and those acting during the exploitation phase, who have more limited resources.

(5) http://www.commoncriteriaportal.org/rss/pps.xml

(6) http://www.globalplatform.org/aboutuscommitteesdevice.asp

(7) GlobalPlatform Device Committee, TEE Protection Profile, Version 1.0, September 2013. The material in this section of the White Paper is based on this document. Readers are invited to refer to the GlobalPlatform document for a complete definition of the Protection Profile.

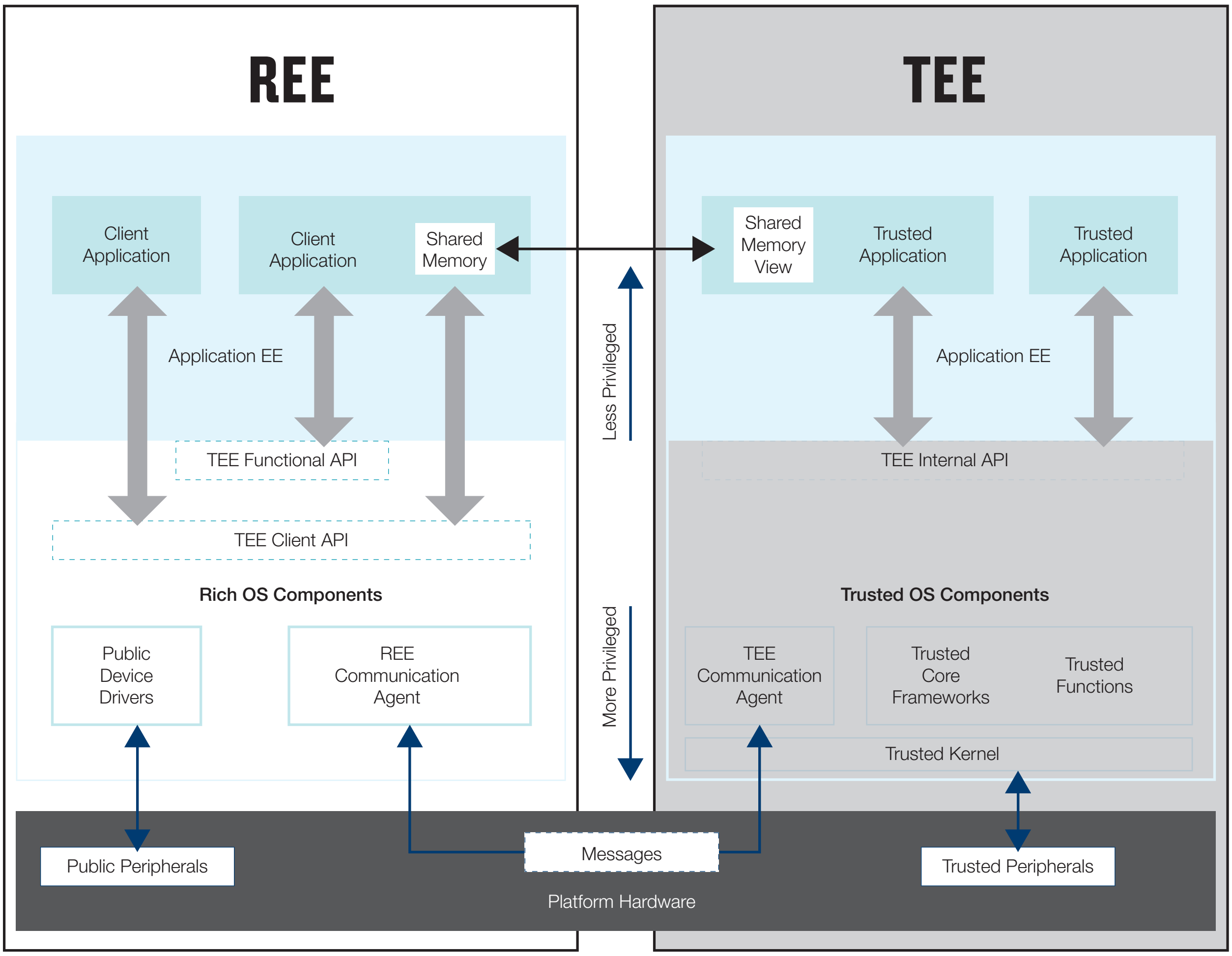
TARGET OF EVALUATION (TOE)

The TOE defines the perimeter of the product to be evaluated, its functionalities and interfaces. As far as TEEs are concerned, their main functionalities include:

- Secure initialization process based on assets bound to the SoC;
- TEE firmware integrity;
- Isolation of the TEE from the Rich Execution Environment (REE) and the TAs;
- Secure execution of Trusted Applications (TAs) and correct execution of TA services;
- Isolation of TAs (mutually and from other execution environments);
- Secure storage of the TAs, and all TEE data and keys, bound to the SoC;
- Protected communications between TAs within the TEE and with Client Applications (CAs) outside the TEE;
- Random Number Generation and cryptographic operations.

A key issue in this context is the fact that TEEs have to interact with different types of components, including:

- A Rich Execution Environment (REE);
- Untrusted Client Applications running on the top of the REE; and
- TAs running on top of the TEE itself (but not belonging to the TOE).



As a result, TEEs also provide different types of interfaces, including the TEE internal API used by TAs and a communication link between the REE and the TEE which is implementation-dependent. The TEE Client API used by Client Applications, which is under the control of the REE, is not a TEE interface in itself. Technically, the TAs and the REE are the users of the TEE, usually acting on behalf of an individual requesting a particular service.

The physical boundary of the TEE is also implementation-dependent. Indeed, the PP does not impose any specific boundary, the general rule being that any component (whether hardware, firmware or software) contributing to the overall security of the TEE has to be included in the TOE[8] to claim conformance with the PP. Usually, the physical boundary is composed of the interfaces of the package, which contains the System-on-Chip.

ASSURANCE LEVEL

The PP reflects the position of the TEE in terms of security, as an intermediate between standard mobile OS and tamper-resistant SEs. It focuses on threats arising during the end-usage phase of the TEE that can be achieved by software and the emphasis is put on non-destructive attacks that can be easily spread, for instance, through the internet. Indeed, the internet has become a common means to get unauthorized access to the assets of a device without damaging the device itself. Nevertheless, such attacks may require initial identification steps that possibly involve hardware expertise, equipment and destructive methods.

Two types of attackers are considered:

- Attackers at the identification phase who discover vulnerabilities, conceive malicious software and distribute it;
- Attackers at the exploitation phase who effectively exploit the vulnerabilities discovered during the identification phase.

The TEE PP defines a dedicated attack quotation grid based on the time required to conduct an attack, the access to the targeted devices, expertise, knowledge of the TOE and equipment. This quotation grid can be used to rate attack paths from the identification phase to the exploitation phase. The TEE is expected to resist to attacks up to 20 points, which corresponds to the Enhanced-Basic attack potential on the CC scale. The rationale for this choice is that the Enhanced-Basic level is higher than the score of known attacks against REEs. However, it is still lower than the high attack potential of SEs such as smart cards.

No assumption is made about attackers' equipment, expertise or means in the identification phase. The limitations are defined by the attack quotation grid. The PP also describes several attacker profiles in the exploitation phase, two of them particularly relevant for the software attack model that has been chosen:

- Remote attacker without physical access to the device; and
- Local layman attacker with physical access to the device but no particular means or knowledge.

The overall assurance level of the TEE PP corresponds to the predefined assurance package EAL2 in which the vulnerability analysis component (AVA_VAN.2) is refined to increase the attack potential from Basic to Enhanced-Basic[9]. The EAL2 assurance package has been chosen to comply with industry constraints: *"EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such, it should not require a substantially increased investment of cost or time."* (CC Part 3, par 99.)

CONTENT OF THE TEE PROTECTION PROFILE

The following table shows the components of the PP: assets, threats, organizational security policies, assumptions, objectives of the TEE and its operational environment, security functional and assurance requirements, and coverage rationales.

[8] This design choice for the PP provides greater flexibility and makes it possible to avoid complex composition issues that would have arisen from a fixed separation between hardware and software TOEs.

[9] The choice was made not to include AVA_VAN.3 because it requires access to the full implementation of the TOE, which may be difficult in many situations for TEEs.

ASSETS

The assets identified in the TEE PP and their security properties consist of:

- The TEE initialization process, bound to the device;
- The trust storage root, which must be unique, immutable and confidential;
- The TEE and TAs code integrity protected;
- The data and keys of the TEE and TAs, protected for authenticity, consistency, integrity, atomicity, confidentiality and bound to the TEE;
- The correct execution of the TEE and the TAs.

THREATS

The threats to the TEE include:

- Cloning the TEE;
- Impersonating TAs to gain illegal access to the services;
- Discovering confidential data through runtime attacks (e.g. exploitation of side-channels); and
- Modifying the behavior of the TEE (e.g. through buffer overflow attacks) to disclose or modify sensitive data or make the TEE execute unauthorized services.

An example of a threat in the identification phase is the unsoldering of the flash memory and dumping its content to discover secret keys that can be used in a second stage to get undue access to other similar devices.

ASSUMPTIONS

The PP identifies assumptions about:

- Debug facilities, which must be disabled for production TEEs or properly controlled;
- The management of TAs (authenticity, integrity, etc);
- The protection of the TEE between delivery and usage.

ORGANIZATIONAL SECURITY POLICIES

The organizational policies in the TEE PP include:

- The generation of the device identifier (inside or outside the TEE);
- The integration and configuration of the TEE;
- The generation, storage, distribution and injection of secret data in the TEE etc.

These policies have to be implemented by the TEE and/or its environment.

SECURITY OBJECTIVES FOR THE TEE

Typical objectives for the TEE include protecting of the identity of TAs; the management of a unique device identifier; the correct operation of security functions (access control, state management etc); the confidentiality of TEE and TA data and keys at runtime; the integrity of the TEE and TA code; the secure storage of TA data and keys; and cryptographic services.

SECURITY OBJECTIVES FOR THE TEE OPERATIONAL ENVIRONMENT

The objectives for the operational environment include the disabling or control of debug facilitates; proper integration and configuration of the TEE; secure management of TAs (authenticity, integrity); the protection of the TEE after delivery, etc.

SECURITY FUNCTIONAL REQUIREMENTS

Most of the Security Functional Requirements (SFRs) in the TEE PP are based on the catalogue of generic security functional components defined in Part 2 of the CC documentation. The TEE PP defines the following three security policies:

- The Runtime Data Information Flow Control Security Policy controls the flow of runtime data and enforces their integrity and confidentiality protection;
- The TA Keys Access Control Security Policy controls access to TA keys and enforces their integrity and confidentiality;
- The Trusted Storage Access Control Security Policy controls access to the persistent storage of TAs and enforces the binding to the TEE storage root of trust.

The TEE PP also contains other requirements, such as:

- An initialization requirement for ensuring the integrity of the TEE firmware at reset and failure management requirements;
- Requirements for the identification of the device, Client Applications and Trusted Applications;
- Open requirements about random number generation, cryptographic operations and key management that have to be instantiated in the STs.

SECURITY ASSURANCE REQUIREMENTS

The Security Assurance Requirements (SARs) of the TEE PP correspond to the predefined assurance package EAL2, in which the vulnerability analysis component (AVA_VAN.2) is refined to increase the attack potential from Basic to Enhanced-Basic. The other assurance components apply to development documentation (functional specification, design and security architecture); preparative guidance and guidance for TEE users (the REE and the TAs); life-cycle support (configuration management and delivery process); and functional testing (test plans, coverage rationale and laboratory-independent testing).

RATIONALES

The PP provides rationales showing that all threats and organizational security policies are covered by security objectives and all assumptions are covered by the objectives for the TEE operational environment.

The PP also includes a rationale showing that all the security objectives for the TEE are covered by (a combination of) SFRs and that each SFR is useful (contributes to the coverage of the security objectives).

The rationale for the SARs relies on the risk analysis which shows that TEEs are exposed to different kinds of attacks and host potentially valuable assets for attackers, which justifies the refinement of the standard EAL2 package of the CC from Basic to Enhanced-Basic.

ANNEX

The annex of the PP defines a comprehensive list of attacks in the identification phase and provides, for each of them, the assets which are threatened (directly or indirectly). An example of a threat in the identification phase is the unsoldering of the flash memory and dumping its content to discover secret keys that can be used in a second stage to get undue access to other similar devices.

The exploitation phase is addressed through the characterization and quotation of the typical attackers' profiles, in particular the remote attacker and the local layman attacker.

4. How to proceed to certify a TEE?

The availability of a dedicated PP greatly facilitates the evaluation of a TEE and ensures consistency and uniformity. Nevertheless, a number of tasks remain to be done to prepare the evaluation of a product, and a CC certification can rarely be started by a product vendor without the participation of security experts. Actually, security requirements should be taken into account as soon as possible in the design of a product and security evaluations can be turned to profit by developers at any stage of the development phase to raise their level of awareness in terms of security, to enhance their trust in the security of their product and also to improve it if needed. Using the PP as a guideline as early as possible in the design process of the TOE should make it possible to avoid iterations and therefore contribute to reducing the overall evaluation cost.

However, very often, the preparation of a CC evaluation starts at the end of the development life-cycle and the developer has to write or complete the evidence for the evaluation *a posteriori*. In this situation, understanding the gap between the security functional and assurance requirements in the TEE PP and the current TEE product[10] is the key to building a pragmatic certification plan that meets business requirements. At this point, one of the main issues is to determine the contribution of the various parts of the TEE (hardware mechanisms and components, firmware and software) to fulfill the PP requirements, which will determine the degree of involvement of the different providers (or departments, if the vendor produces the whole TEE).

The other main issue is confidence in the robustness of the TEE implementation regarding the attack spectrum[11]. If the security requirements were not taken into account in the design phase, or if the development process did not include appropriate security validation steps, then independent security pre-testing would mitigate the risk of evaluation failure. The goal is to detect potential vulnerabilities at any level - hardware, firmware or software - and to derive the most suitable solutions, especially for hardware vulnerabilities that might in some cases be mitigated by software countermeasures.

Preparation of evaluation deliverables

The certification plan includes the preparation of the evaluation deliverables, the ST and the other pieces of evidence required by the TEE PP.

To define the ST, it is necessary to identify the parts of the TEE PP that are applicable to the product to be evaluated, in particular, the threats, assumptions, policies, consistency analysis and SFRs. If compliance with the PP is claimed then all the elements of the PP are applicable and the conformity rationale must be included in the ST. As far as the assurance requirements are concerned, it is usually possible to reuse existing documents, including the GlobalPlatform TEE Internal API specifications, and to complete them in order to fulfill the CC requirements. At this stage, it is also necessary to build and carefully review the TEE test plans and potentially complete them to cover the functional specification.

[10] Including functional and design documentation, manuals, tests plans, delivery procedures and configuration management.

[11] The PP provides examples of attack paths; this no means constitutes an exhaustive list.

CC evaluation procedure

The first step consists of validating the scope of the certification with the certification body, including the perimeter of the TOE and the test environment. This is especially relevant for PPs which have not yet been certified and for STs that do not claim compliance with a PP. It is also necessary to choose an evaluation laboratory (ITSEF[(12)]) authorized by the certification body which monitors their practices in compliance with the CC Recognition Agreement[(13)] (CCRA) and internal processes. ITSEFs must also be accredited by a recognized accreditation body based on:

- impartiality;
- general technical, methodological and procedural competence; and
- specific technical competence in the IT field where the ITSEF intends to perform evaluations.

The ITSEF evaluates the security of the TEE using the CC Evaluation Methodology (CEM) and the specific supporting documents of its own domain (e.g. the TEE PP and its annexes). The evaluation results in a full Evaluation Technical Report (ETR), which summarizes all the assurance activities including – documentation, vulnerability analysis and testing – and provides a verdict for each of the evaluation tasks. The certificate is emitted by the CB in compliance with the CCRA rules upon a satisfactory ETR.

(12) Information Technology Security Evaluation Facility.

(13) The "Common Criteria Recognition Agreement" (CCRA) brings together national authorities to standardize certification schemes in the field of IT security, based on a principle of mutual trust and understanding between governmental organisations.

5. Conclusion

TEEs provide the means to enhance the security of mobile devices and to execute sensitive operations on devices running standard, general purpose, operating systems. They are called on to play a key role in the protection of user interactions which is often the Achilles heel of security architectures.

For this reason, defining a security certification scheme has been identified by GlobalPlatform as a key success factor for TEE technology adoption by the mobile market. To address this need, the Device Committee (Security Working Group) has defined a Common Criteria Protection Profile for TEEs. A key benefit in terms of trust is the independent security evaluations based on common methodology and domain-specific techniques and procedures defined in the Protection Profile, which make it possible to compare evaluation results.

The TEE PP considers the TEE as a whole execution platform and states its security properties from the end-users' point of view. However, a TEE is usually composed of hardware, firmware and software and may involve different actors – chipset manufacturer, kernel and API providers. Each of the components implements countermeasures against threats, which together constitute the security edifice. The evaluation and certification of the TEE components and the way of composing the certificates and reusing evaluation results to achieve the complete TEE certification is an open question. Fortunately, the evaluation of composite products is not new subject and several groups of interest have provided processes to address the issue[(12)].

Composition is also a relevant issue for the evaluation of the mobile device itself, including its applications. Under what conditions can a TEE certificate be reused for the evaluation of an enabled mobile device? How can such a mobile device be evaluated? What are the appropriate schemes for certifying the applications hosted by the device and what are the reuse methodologies that will allow cost-effective evaluations in a fast-evolving market?

In general, a key issue for the evaluation of composite products is to be able to provide some form of modularity to allow for the reuse of the evaluation results of individual components such as Secure Elements, TEEs or Trusted Applications to derive security guarantees for the whole product. This notion of end-to-end security is essential to ensure an appropriate level of trust in the connected services. It is the role of the technical communities to build appropriate and pragmatic evaluation frameworks that enable the deployment of these services.

(12) For instance, the smart card community has established a composite evaluation methodology that allows the incremental evaluation first of the IC then the embedded software on top of the IC, reusing the results of the IC evaluation. The embedded software itself can be decomposed in layers; for instance, a Java Card platform and a set of applets, each evaluated according to the verticals' requirements.

About Trusted Labs

Trusted Labs is a leading expert in security consulting and evaluation for the connected world with 15 years of experience in embedded systems and solutions such as smart cards, connected devices, terminals and Trusted Execution Environments.

With operations in Europe, Asia and North America, we support our customers - network operators, service providers, certification entities, issuers, developers and manufacturers - in defining, evaluating and achieving the security goals of their multi-application products, connected devices and remote management solutions and infrastructures.

A worldwide leader in scheme definition, Trusted Labs offers a unique pool of expertise in security analysis, evaluation and certification management. Our multi-sector expertise covering bank, telecoms, transport, M2M and identity markets combined with our innovation capabilities enable our clients to demonstrate and increase trust in the security of their products and solutions.

FOR FURTHER INFORMATION PLEASE CONTACT:

KARINE GANEM
Marketing Director
karine.ganem@trusted-labs.com
Tel: +33 1 30 97 26 11
www.trusted-labs.com

Appendix – Abbreviations

CA	Client Application
CC	Common Criteria
CEM	Common Criteria Evaluation Methodology
CCRA	Common Criteria Recognition Agreement
EAL	Evaluation Assurance Level
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
REE	Rich Execution Environment
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
SE	Secure Element
ST	Security Target
TA	Trusted Application
TSF	TOE Security Function
TOE	Target Of Evaluation
TEE	Trusted Execution Environment

Notes