GlobalPlatform TEE Certification Workshop

Michael Lu (Trustonic)

May 2016

Agenda

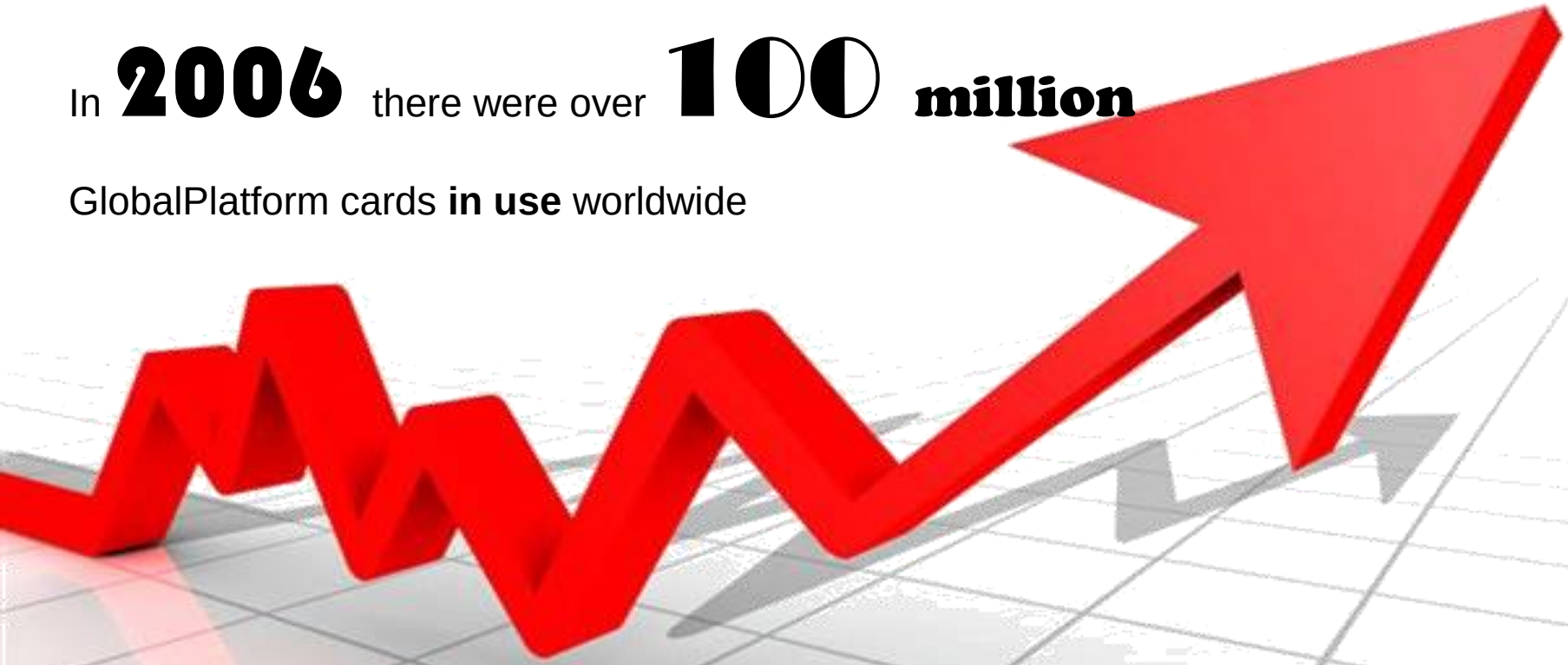
- Introduction to TEE PP, Security Objectives and TEE implementation requirements;
  - TEE保护轮廓, TEE安全等级, 实现TEE的 安全需要
- Overview of evaluation methodology and potential attacks;
  - 评价方法和潜在攻击的概述;
- Certification regime, process, labs and content;
  - 安全认证流程和安全认证实验室的认可
- Applicability of GlobalPlatform Certification in different industries;
  - GlobalPlatform 安全认证在不同行业里面的接纳和使用, FIDO和 内容保护

Strong Rate of Growth

GLOBALPLATFORM®

In **2006** there were over **100 million**

GlobalPlatform cards **in use** worldwide



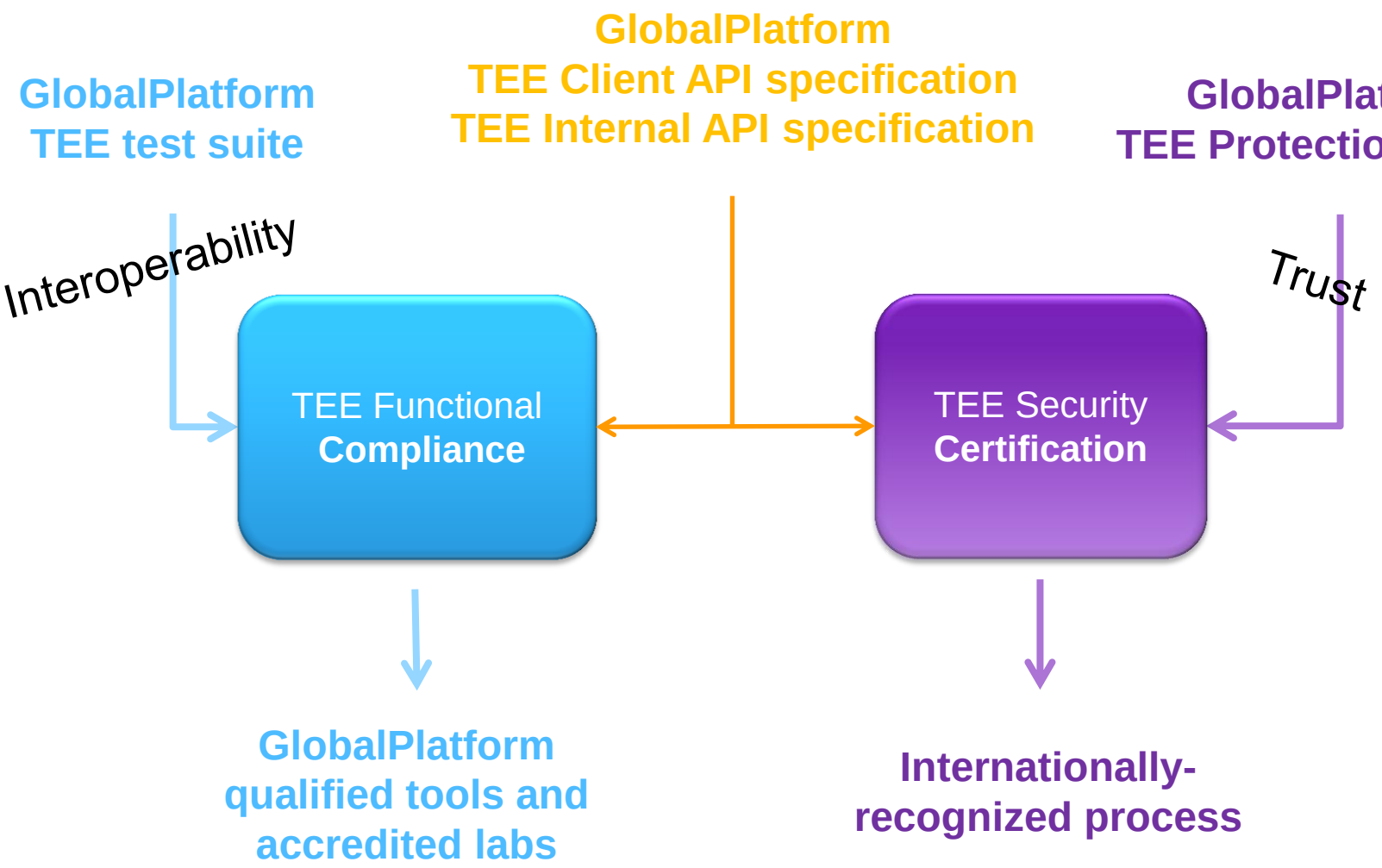
In 2014, more than **10 billion**

GlobalPlatform cards or SEs have been **produced**

Source: GlobalPlatform presentation

GlobalPlatform Mission

GLOBALPLATFORM®



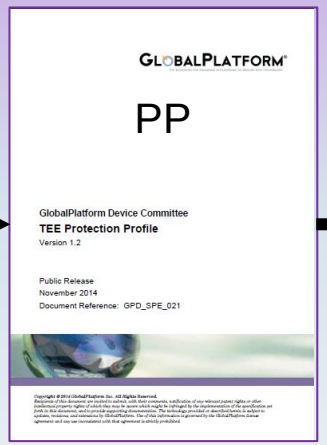
Document structure

GLOBALPLATFORM®

TEE Attack WG

Attack list

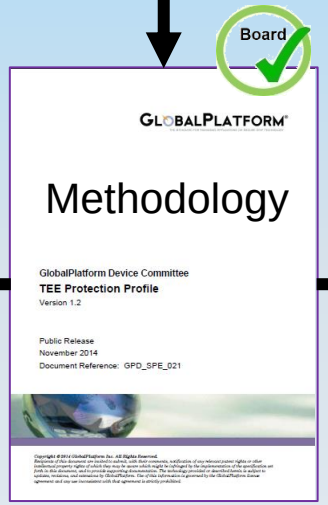
TEE Security WG



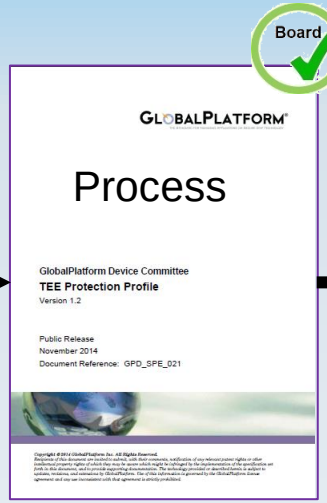
test list

Security target

TEE Lab WG

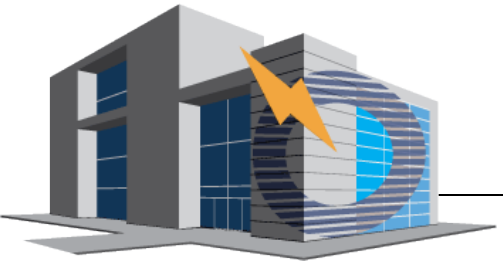


Security Evaluation Secretariat



Board

Lab & Product vendor Contracts



TEE Protection Profile Overview

- Problems TEE is designed to address
- Security Principle and Implementation Requirements
- Threat Model and Protection Profile Overview

Rationale for a TEE

GLOBALPLATFORM

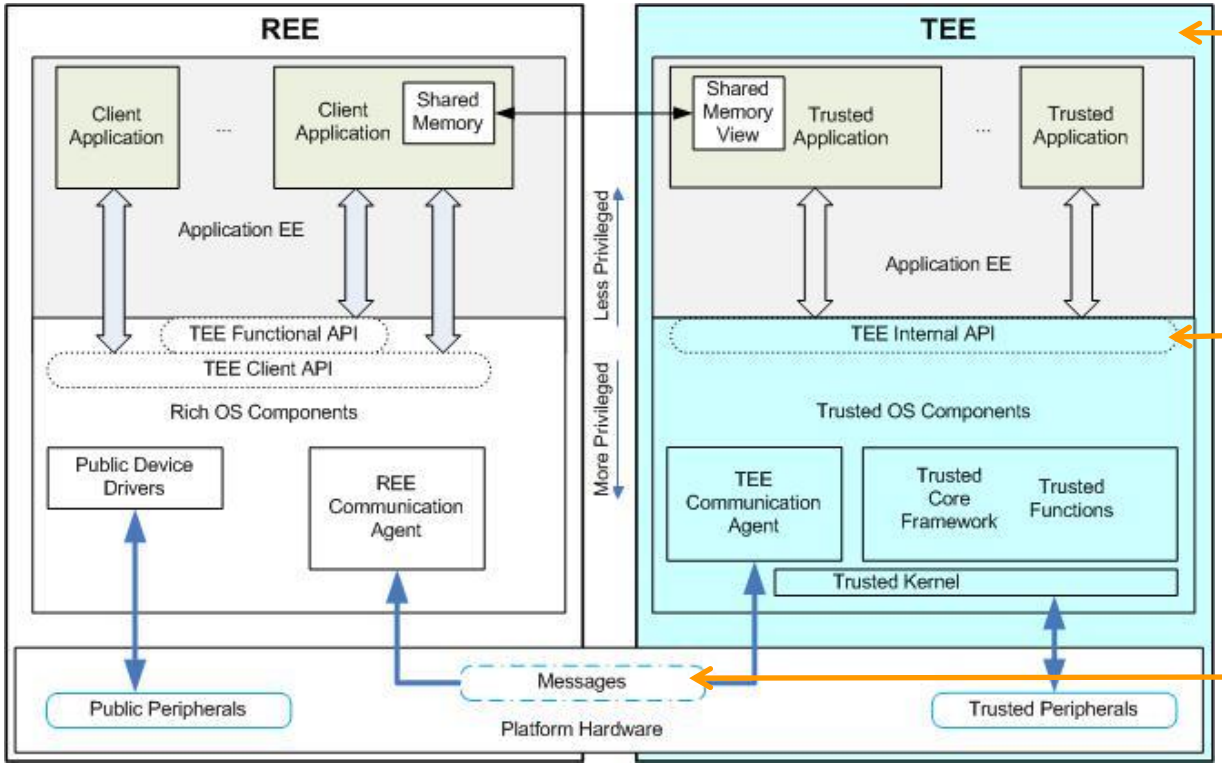
- Problem is to protect a device and its assets from faults, frauds and attacks – threats are multiple, diverse, and increasing
  - See white paper section 5.1
- Solution is to partition execution between a “normal world” (Rich OS) and a “secure world” (TEE)
  - Software running in the TEE (Trusted Application) is first authenticated and then authorized to access secure resources in order to protect confidentiality and integrity of device assets
  - Security-demanding applications running in the Rich OS can delegate secure operations to Trusted Applications (if and when authorized)
- The TEE must adhere to security principles, derived from OMTP TR1 Specification
- The current principles apply to the run-time environment and the security properties required to put that run-time environment in place.
  - Availability of TEE and its capabilities during boot will be defined in future versions.

Implementation Requirement for a Trusted Execution Environment

GLOBALPLATFORM

- The TEE is where applications run in a protected/shielded/trusted zone environment with access to Secure Resources offered by the platform
  - The level of confidence in the TEE is related to the protection of those Secure Resources – whenever possible, Secure Resources should be implemented in hardware
  - Secure Resources are accessed through a library of functions – when no hardware Secure Resources is available, those functions may substitute a software implementation
- The TEE must support
  - A Hardware Unique Key that meets OMTP TR1 requirements
  - A Kernel (*TEE Kernel*) to manage the execution of Trusted Applications and synchronization however not mandating scheduling capability
  - A set of core "OS-like" functions
  - Secure memory management and access
  - Secure storage management and access
  - Management of communications inside the TEE and with the Rich OS
  - Isolation of Trusted Application (however an inter Trusted Application communication mechanism must exist which is trusted by the TEE and allows a communication path between Trusted Applications)
  - Rich OS debugging capabilities must not be able to access the TEE
  - TEE debugging capabilities must only be enabled from sources authorized by the device/platform manufacturer
- The TEE will evolve to support:
  - Comprehensive Trusted Application LifeCycle ([de]installation, [un]loading, [de]activation, updating, [b]locking, etc.)
  - Dynamic provisioning and installation of Trusted Applications (i.e. [down]loaded at run-time)
- Characteristics
  - The TEE must be instantiated during secure boot procedure or by a trusted software component, provided this trusted component obtained trust delegation from the secure boot
  - A hardware mechanism must enforce the system wide isolation of the TEE from components outside of the TEE
    - In other words a software-only TEE does not make sense, even a pure software virtualization environment
  - Several TEE may co-exist on a device but must be isolated – no need to standardize multi-TEE – TEEs can communicate if they are mutually authenticated and can use the TEE Client API to do so

Scope of the evaluation



TOE (HW, FW, SW)

Boundary with Trusted Applications:

TEE Internal API

Boundary with Rich operating system (OS): Messaging interface

The TOE comprises:

- **All hardware, firmware and software** used to provide the TEE security functionality, including debug mechanisms (specified in the Debug module) and TEE initialization
- The **guidance** for the secure usage of the TEE after delivery

The TOE does not comprise:

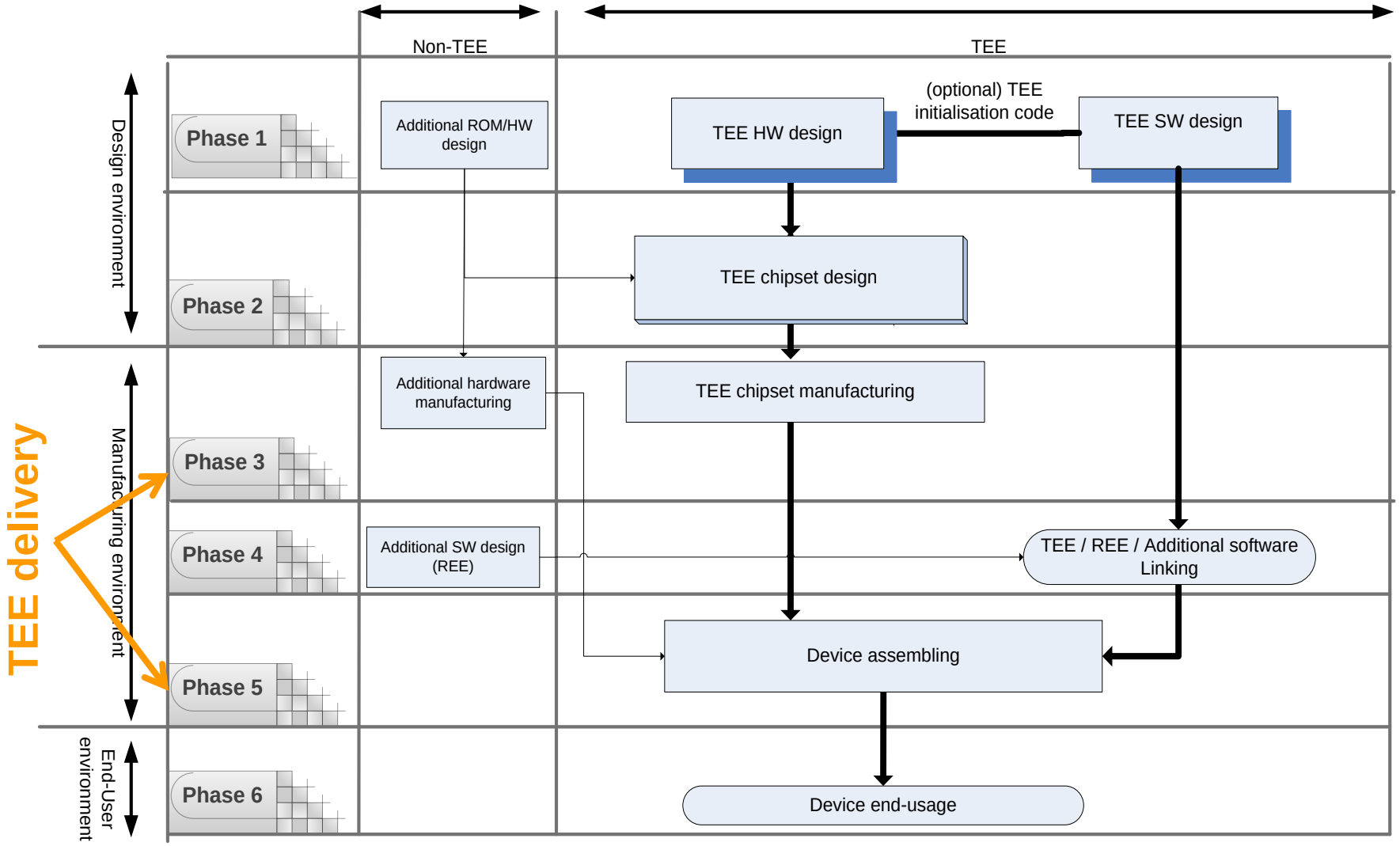
- The trusted applications
- The rich execution environment (REE)
- The client applications

TEE security functionality in the scope of evaluation

GLOBALPLATFORM®

- TEE initialization process using assets bound to the SoC, that ensures the authenticity and integrity of the TEE code running in the device (implementation-dependent)
- Authentication of TEE firmware and of Trusted Applications
- Isolation of the TEE services, the TEE resources involved and all the trusted applications (TAs) from the REE
- Isolation between TAs and isolation of the TEE from TAs
- Trusted storage of TA and TEE data and keys, ensuring consistency, confidentiality, atomicity and binding to the TEE
- Random number generator
- Cryptographic algorithms
  - specified by the implementer in the Security Target
  - chosen from those in the GlobalPlatform APIs and/or algorithms used to provide security functionality, e.g. trusted storage
- Monotonic TA instance time
- *Advanced TEE (rollback protection over resets)*
  - *Monotonic persistent time*
  - *Full integrity protection of TA data, code, keys and TEE data*

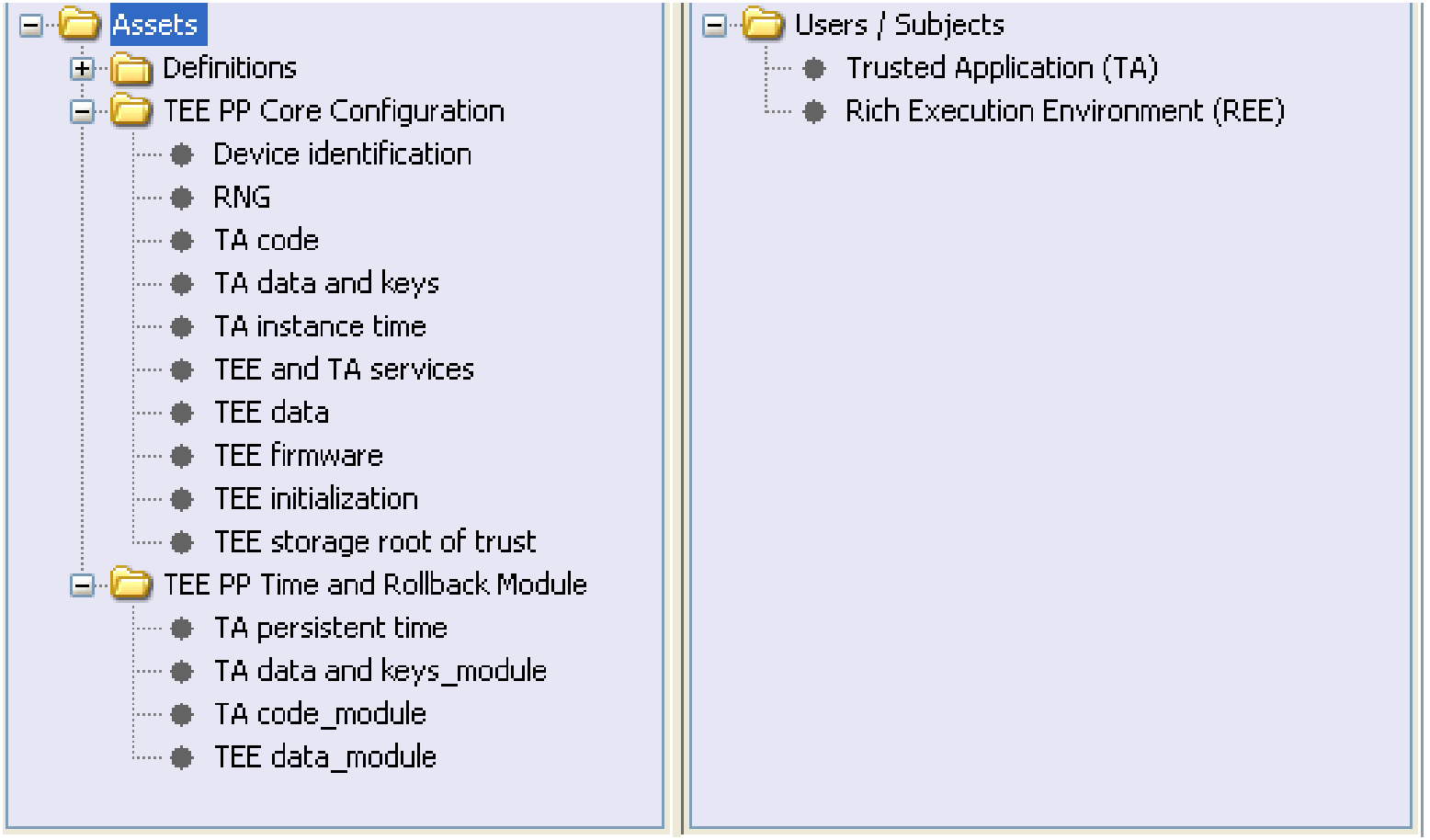
Device Lifecycle



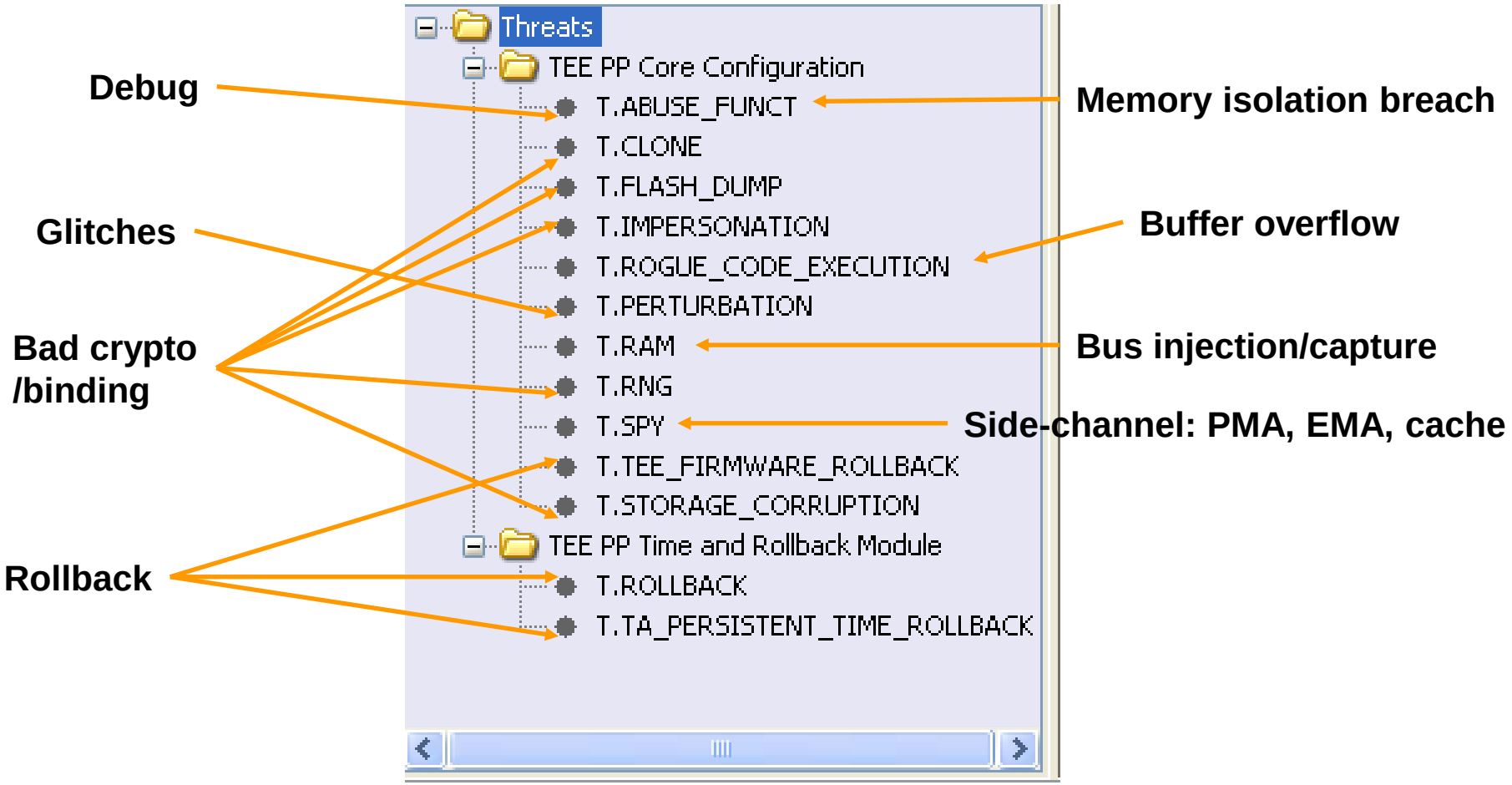
Threat model

- The TEE PP addresses threats that arise during the end-usage phase and can be achieved by software means without damaging the device
- At the identification phase
  - The attacker discovers some vulnerability, conceives malicious software and distributes it
  - No assumption holds regarding the equipment, expertise, etc. and the possibility to use more than one device, potentially in a destructive way
- At the exploitation phase
  - The attacker exploits the vulnerability by running the malicious software
  - There are two main exploitation profiles: remote attacker and basic device attacker
  - Basic, non-destructive HW attacks are also possible

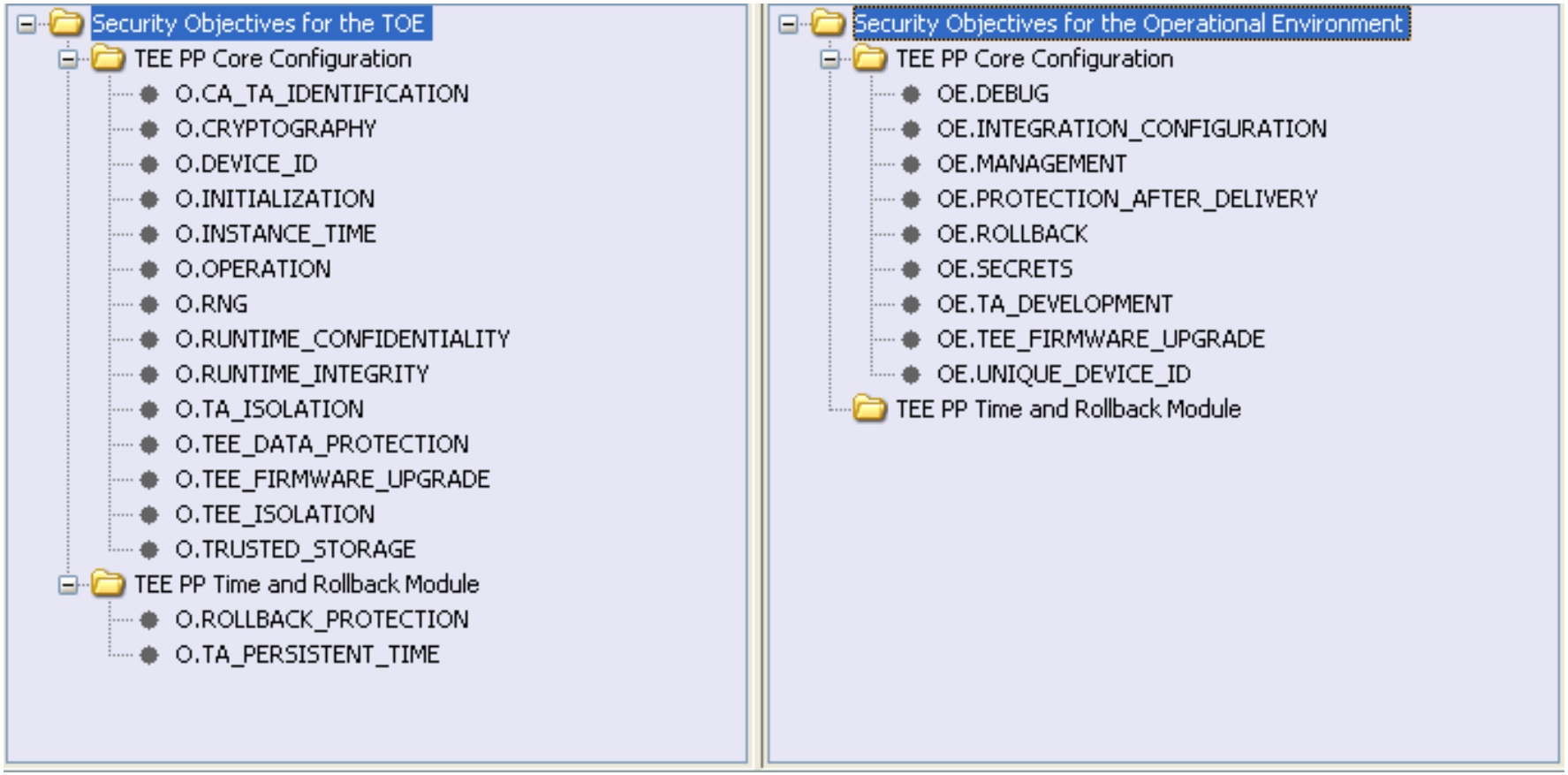
Assets and Users



Threats

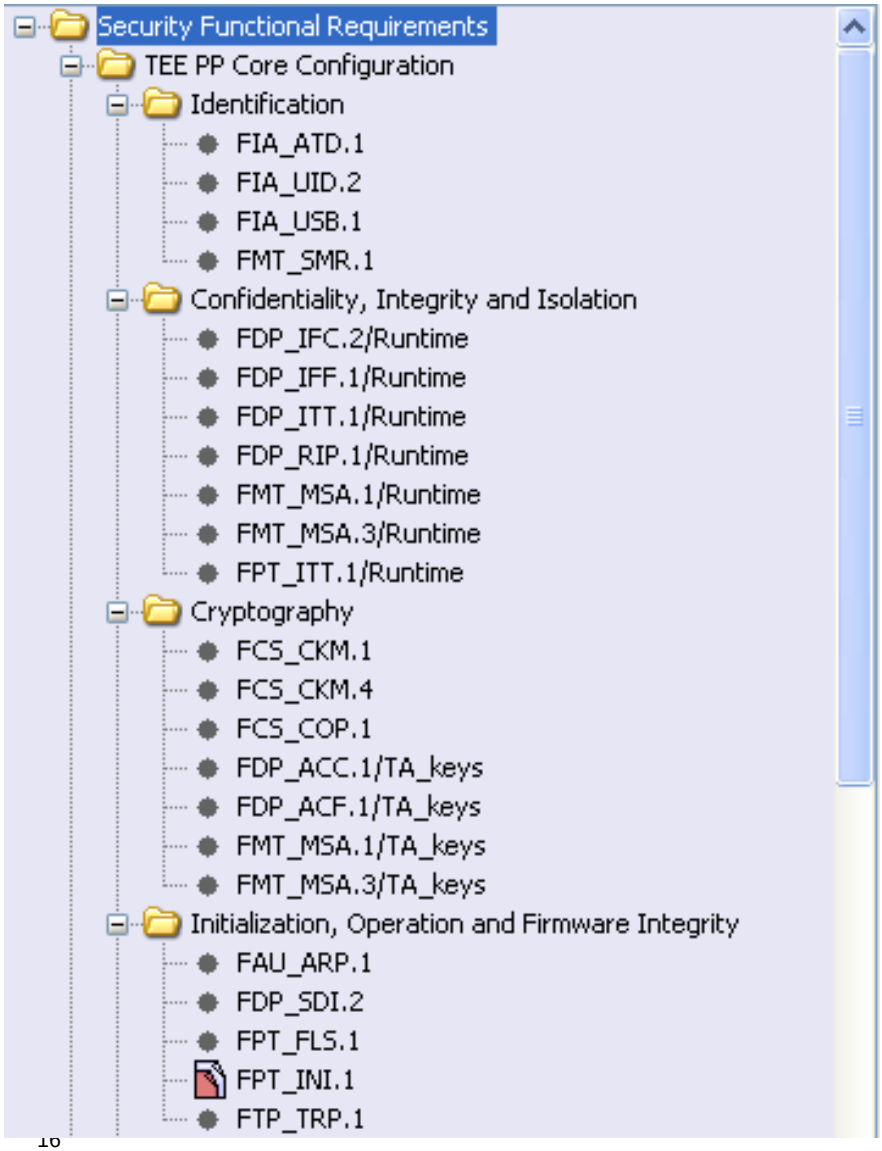

Threats
TEE PP Core Configuration
T.ABUSE_FUNCT
T.CLONE
T.FLASH_DUMP
T.IMPERSONATION
T.ROGUE_CODE_EXECUTION
T.PERTURBATION
T.RAM
T.RNG
T.SPY
T.TEE_FIRMWARE_ROLLBACK
T.STORAGE_CORRUPTION
TEE PP Time and Rollback Module
T.ROLLBACK
T.TA_PERSISTENT_TIME_ROLLBACK
Debug
Glitches
Bad crypto /binding
Rollback
Memory isolation breach
Buffer overflow
Bus injection/capture
Side-channel: PMA, EMA, cache
Fuzzing

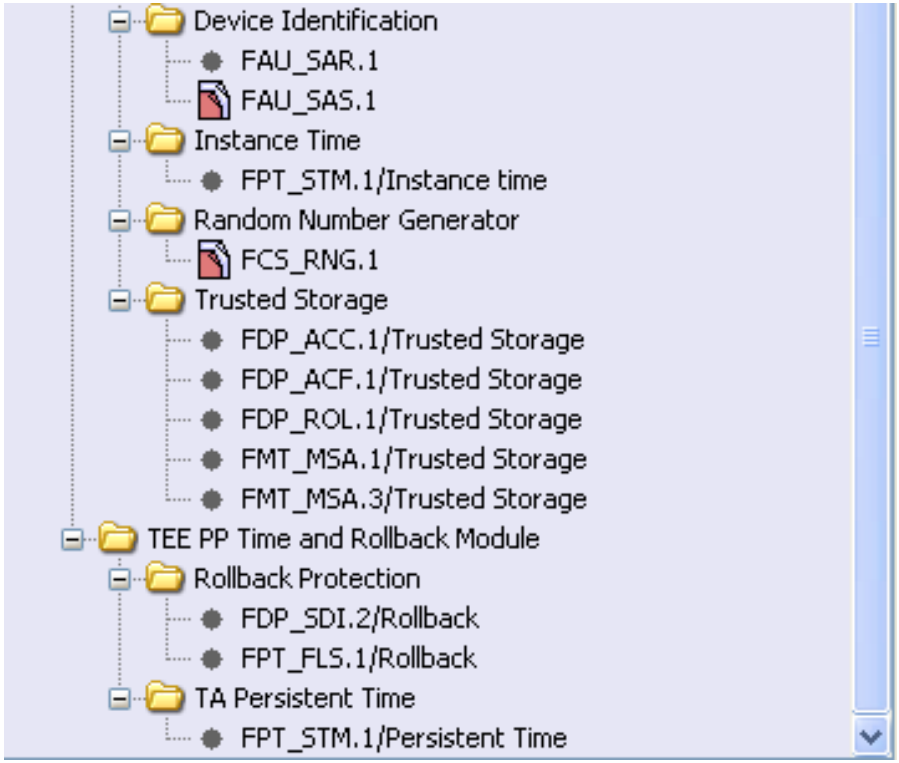
Security Objectives



Security Functional Requirements Overview

GLOBALPLATFORM®





Attack Potential

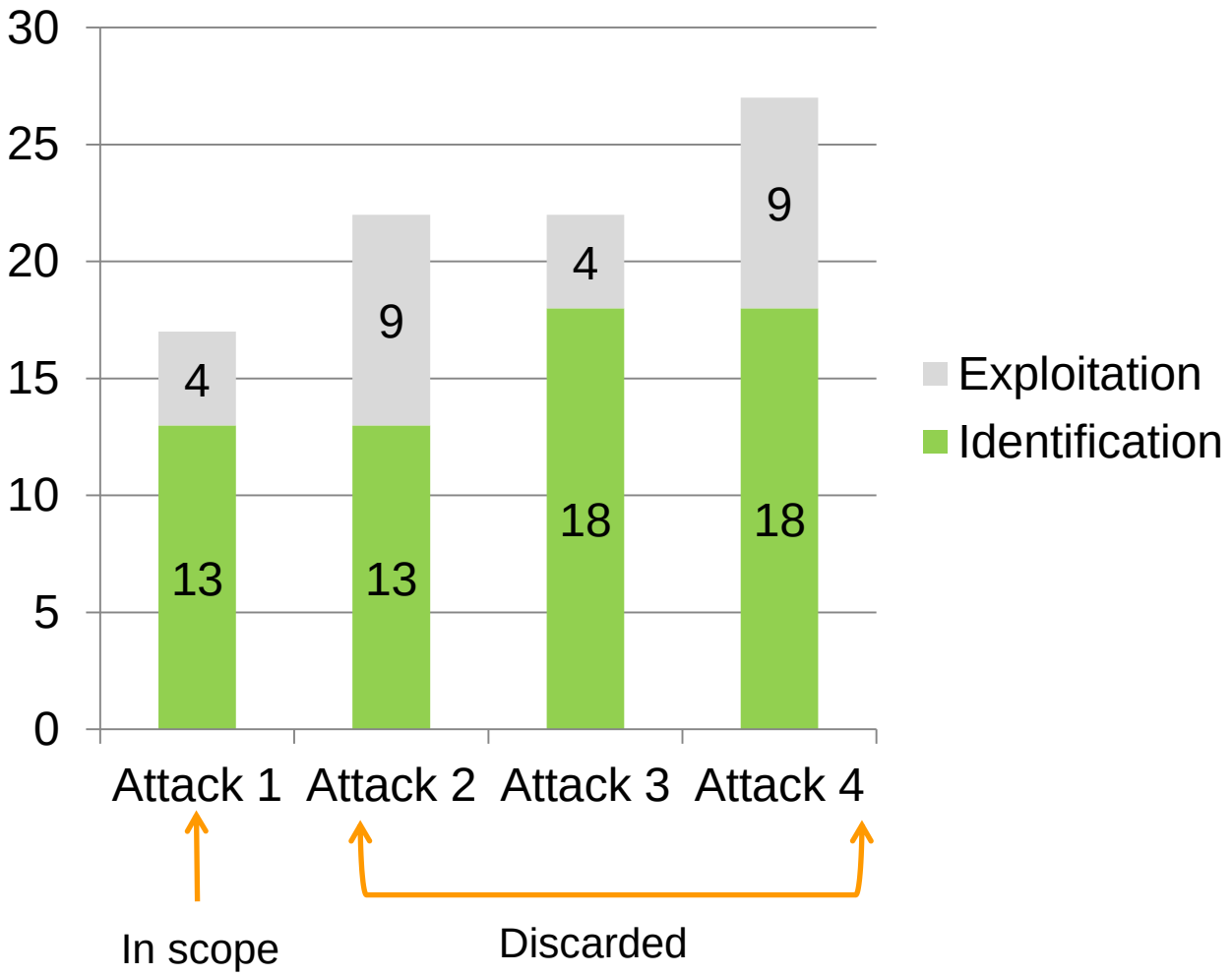
- The TEE PP provides:
  - The TEE attack quotation table for rating full attack paths from identification to exploitation
  - The description and quotation of four representative exploitation profiles
  - A list of illustrative attacks at identification phase

- The TEE PP states the attack potential at **« Enhanced-Basic »**
  - Higher than the score of known attacks to Rich OS devices
  - Lower than the **« High »** attack potential of secure elements

Below or Above the Attack Potential

- Two identification paths, at 13 pts and 18 pts.
- Two corresponding exploitation profiles, at 4 pts and 9 pts, with 4 the minimum required

Enhanced-Basic



TEE attack experts sub-WG

- Within the TEE Security WG, a subgroup has been created to define the threat model and the attacks that a TEE implementation should resist
- A document, separate from the PP, that lists these attacks with their detailed quotation, is available within GP, subject to specific sharing rules (i.e. kept encrypted and accessible to only one delegate per company)

Assurance approach (Common Criteria): EAL2+

GLOBALPLATFORM®

- **Documentation** : Lab reviews the TEE documentation provided by the vendor
  - Security Target
  - Security Architecture
  - Functional Specification
  - Design Specification
  - Configuration management system
  - User Manual
  - Installation Procedures
  - Delivery procedures
- **Functional Testing** : Lab reviews the TEE test plan, results and coverage analysis provided by the vendor
- **Penetration Testing** : Lab performs independent vulnerability analysis, defines the security test plan and performs the testing
  - The security level corresponds to 20 points of attack potential
  - No source code required

Security Level

- Attacks split into identification and exploitation phases:
  - ‘break once, break only once’ rule – ie one exploitation shall break only one device/one subscription
- Resistance to attacks up to 20 points
  - combined score of equipment, time, expertise, number of devices for an attack path
- Expected to cover usual fault and side-channel attacks

The PP allows a layered TEE Certification

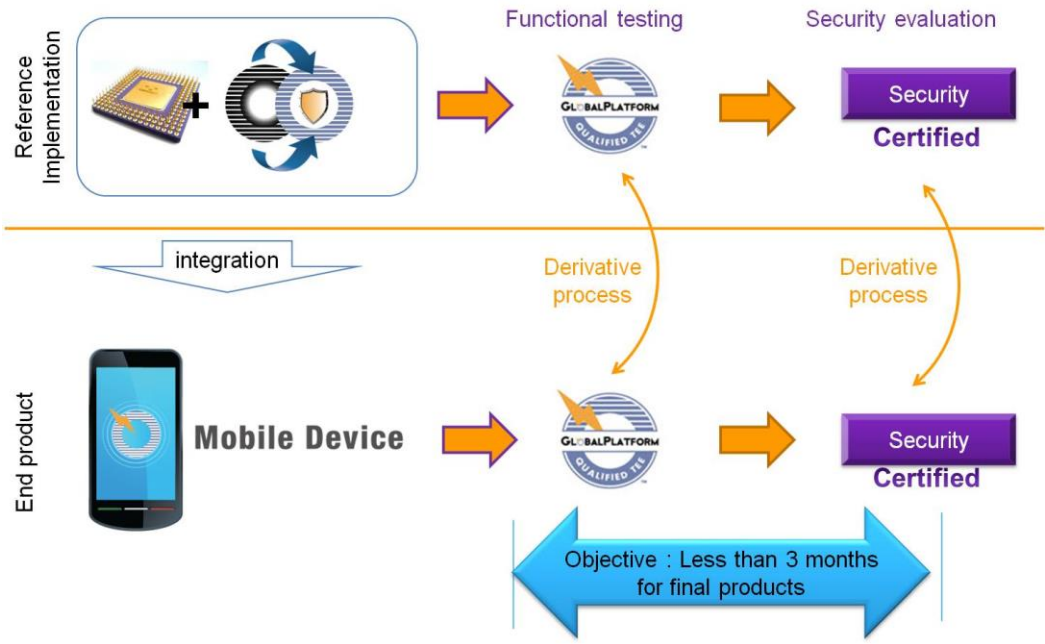
- Modular Protection Profile
  - The Protection Profile (PP) contains a core part, and optional modules
  - The PP does not specify some parts that are left to the security target, for example the instantiation of cryptographic security requirements as it can vary according to country, industry vertical…
  - Optional modules cover specific features
    - Existing modules: Controlled debug, Full rollback protection
    - Future modules such as a module for the protection of video path
- Complementary testing may be added (out of scope of GlobalPlatform protection profile)
  - integration of the certified components,
  - integration of the applicative part,
  - the provisioning of the keys,
  - the operation of the servers

  → many certifications of many kinds may coexist

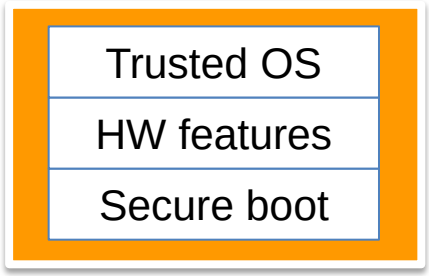
Evaluation Methodology

Reminder of the TEE certification initiative

- Multi market recognized certification scheme
  - Adapted to an heterogeneous set of market requirements
  - Facilitate procurement rules (e.g. Common Criteria based)
- Two phased process
  - Certification of the TEE in a reference board implementing the complete architecture
  - Second phase on the final device



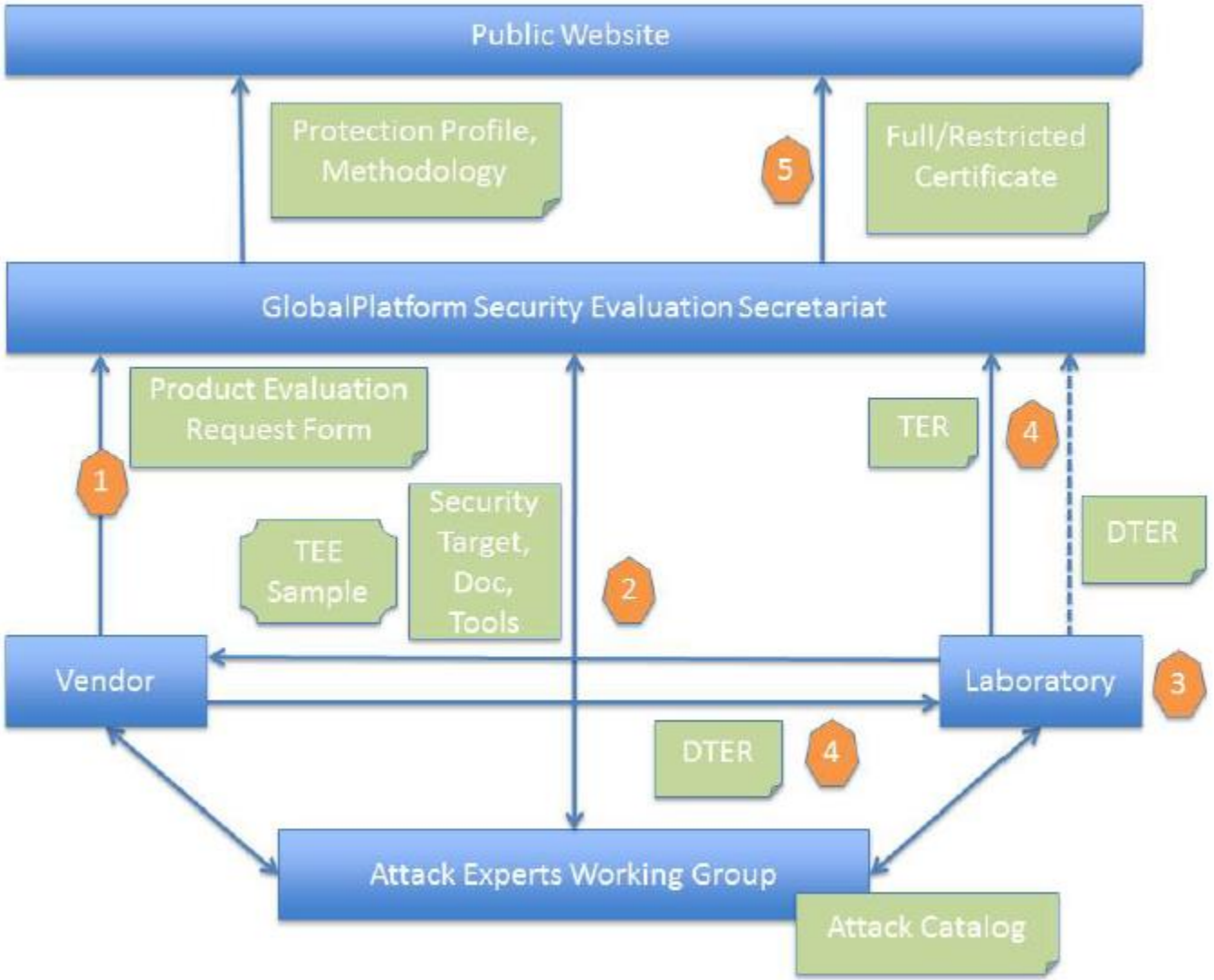
Evaluation scope



Process Flow

GLOBALPLATFORM®

Figure 5-1: GlobalPlatform TEE Certification Process Flow



Adapted to the mobile market

- The evaluation methodology apply on
  - Prototype
    - Example : a board with a TEE
    - This will allow a OEM to select already pre – validated TEE on chip set
  - Product
    - Example a set up box, smartphone
  - Derivative product
    - The delta evaluation will focus on modified part of the first evaluated scope.
    - A product derived from a certified product
    - A product embedding a certified prototype
- All Security certificate from GlobalPlatform or National Certification Body will be available in the GlobalPlatform public website.

GlobalPlatform TEE Security Evaluation (1/2)

- The objective of this methodology is to ensure that a GP Qualified TEE can be evaluated within 3 months time frame
  - Non compliant TEEs may be evaluated but the duration will not be within 3 months
- Evaluation methodology may apply on
  - Prototype
    - Example : a board with a TEE
  - Product
    - Example a set up box
  - Derivative product
    - A product derived from a certified

GlobalPlatform TEE Security Evaluation (2/2)

- Assurance approach
  - Documentation
    - Requires no specific documentation
    - Documentation used as source of information, not evaluated
  - Functional Testing
    - Evidences available to the lab if required
  - Penetration Testing
    - Same as CC: attacks up to 20 points have to be countered
- Evaluation duration
  - 3 months provided the TEE is GP compliant and source code is available
  - 1/3 design review
  - 2/3 penetration testing

GlobalPlatform SES and Lab Accreditation

High level flow

GLOBALPLATFORM®

Functional qualification

Compliance SECRETARIAT

Security evaluation

or

CC Certification Body

GP Qualified TEST LABORATORY

GP - SES

Security Evaluation Secretariat

- SES will monitor by 4 processes:
  - The Scheme definition and its maintenance
    - Legal framework
    - Adaptation of the scheme when the PP or the evaluation methodology eveolves
    - Any other event that requires an update
  - The Laboratories accreditation
    - See next slide
  - The evaluation of the TEE product done by Evaluation Laboratories that leads to a issuance of a certificate
    - Application of the evaluation methodology and the scheme
  - Certificate issuance and maintenance

Lab selection process

- Initial selection (for one year)
  - GP Device committee participating member
  - At least one expert trained on GP TEE
  - Be accredited in a recognized certification framework such as ISO17025, CC, EMVco, PCI, Content protection schemes…
  - Proven financial accountability
  - Demonstrable experience of at least 3 years in security evaluations (software & hardware security testing)
  - First evaluation ready to start
- Renewal criteria (renewal is for a 2 years)
  - Verification of the above, plus
  - Active participation in labs and attack group meetings (attendance to at least 75% of all meetings , conf calls, plus active contributions)
  - Audit of evaluations and of the lab (access to details report)

Legal framework available

GLOBALPLATFORM®

How to Participate

For a laboratory to achieve GlobalPlatform accredited status, the organization must be a GlobalPlatform **Full Member** or **Participating Member** (participating in the Device Committee) in good standing.

Once membership is confirmed, security laboratories can apply to the Trusted Execution Environment (TEE) Security Evaluation Secretariat to initiate the **accreditation process**. The laboratory's processes will then be analyzed on-site to ensure that it is equipped to thoroughly evaluate a TEE product in line with the GlobalPlatform TEE Protection Profile.

In addition to the opportunity to contribute to this initiative, there are many other benefits to **becoming a GlobalPlatform member**.

Non-GlobalPlatform members wishing to purchase member documents such as Test Suites, please **visit our store**.

The legal and technical forms applicable to each type of qualification are provided below.

Participation Forms	Product Vendor	Laboratory
GlobalPlatform Security Evaluation Agreement	✓	
Exhibit B – GlobalPlatform Product Evaluation Request Form	✓	
GlobalPlatform Laboratory Accreditation Request Form		✓
GlobalPlatform Security Laboratory Relationship Agreement		✓

Collaboration with the technical community

GLOBALPLATFORM®

- Attack group has been created
- 1 representative and one alternate
- Open to National Certification Body

- NDA enforce the confidentiality of exchanges
- Information protected by PGP Keys

CHARTER

In accordance with GlobalPlatform's current Intellectual Property Rights (IPR) Policy, this Charter document establishes the parameters within which the below identified Task Force, Committee or Working Group shall operate.

Task Force/Committee/Working Group Name:

TEE Attack Expert Working Group

Submission Date:

10 October 2014

Effective Date:

16 December 2014

Licensing Mode:

RAND-Free

Purpose, Scope and Deliverables:

The objective of the GlobalPlatform ("GP") TEE Attack Expert Working Group ("WG") is to analyze known and recently discovered attacks to determine their relevance to TEE technology. The output of the WG will be updates to the TEE Protection Profile.

The GP Device Committee believes that this WG is unique, as compared to other GP WGs, and thus requires more specific rules and guidelines as provided below. Specifically, effective discussion of attacks requires a level of disclosure by participating organizations which goes beyond the level of disclosure required to secure interoperability, and which is above and beyond the normal expectations of participation in a standardization body. Additionally, there are official bodies that require the discussion of sensitive information, which may be useful in constructing a cyber-attack, to be discussed in closed mailing lists whose contents are encrypted. These factors justify certain participation guidelines and protection of information, as more fully described below.

Rules, if Applicable:

General rules

- Membership of the TEE Attack Expert WG is open to GP Member companies (1) allowed to participate to the GP Device Committee; (2) committed to collaborating and working cooperatively with, and providing constructive contribution to, GP; and (3) prepared to pool their expertise on TEE attacks with other GP members, subject to the guidelines below.

GlobalPlatform and Content Protection

Sony Pictures' View of TEE

GLOBALPLATFORM®

TEE is part of the Response to Future Threats

- A trusted execution environment is a vital component
  - Movielabs' specification for Enhanced Content Protection for Next Generation Video specifies TEE and hardware root of trust
- Solutions are required for all classes of device
  - Mobile devices, set-top boxes, HDMI sticks, PCs, etc.
- Standardized trusted execution environments
  - Help all the stake holders
- Need to secure not just execution but the entire video path
  - Decryption to decode to re-encryption for the link to display

http://www.movielabs.com/ngvideo/index.html

How can we ensure a secure implementation?

Logo licensing and voluntary certification are not sufficient

Options include:
- Contractual, as before
- Trusted implementers
- 3rd party certification

Challenges:
- Defining robustness
- Identifying security providers and trusted implementers
- Scalability of the implementation infrastructure, e.g. certification

11

http://globalplatform.org/TEEevent/documents/GlobalPlatform_TEE_PresentationsOct2013.zip

How to Improve Things

- Common requirements
  - MovieLabs Enhanced Content Protection Specification: http://movielabs.com/ngvideo
    - Targeted at UHD/4K and early window
    - Requires hardware-based CP, e.g., TEE-based CP
  - GlobalPlatform Premium Content Requirements
- Common certification regimes
  - Need standardized protection profile and process definitions
  - Need regime(s) that stand outside of any format group

Motion Picture Laboratories, Inc.

Mapping of objectives to CP requirements (1/3)

GLOBALPLATFORM®

GP TEE PP Security Objective	Application to content protection schemes
O.CA_TA_IDENTIFICATION	Typically each content protection scheme will be installed in its own TA. This objective generally exceeds requirements of most CP schemes.
O.CRYPTOGRAPHY	CP TAs make use of available cryptographic functions in the TEE when available. Some CP schemes require unique functions not provided by standard cryptographic implementations. For performance reasons, some CP schemes require hardware cryptographic modules that operate as TEE-based peripherals.
O.DEVICE_ID	CP TAs make use of unique device IDs to derive keys bound to the device. Such keys are used to provide secure storage and similar functions.
O.INITIALIZATION	This objective applies to the TEE itself.
O.INSTANCE_TIME	Many CP TAs require monotonic time. In general, absolute time is not a requirement.
O.OPERATION	This objective applies to the TEE itself.

Mapping of objectives to CP requirements (2/3)

GLOBALPLATFORM®

GP TEE PP Security Objective	Application to content protection schemes
O.RNG	CP TAs use RNG functions to create ephemeral keys and protocol data, generate unique keys and key pairs.
O.RUNTIME_CONFIDENTIALITY	CP TAs are required to protect the confidentiality of secret data and in some cases algorithms during runtime.
O.RUNTIME_INTEGRITY	Runtime integrity enforces correct operation of TAs.
O.TA_ISOLATION	TAs must be isolated from each other.
O.TEE_DATA_PROTECTION	This objective applies to the TEE itself.
O.TEE_FIRMWARE_UPGRADE	This objective generally exceeds the requirements of most CP schemes.
O.TEE_ISOLATION	This objective applies to the TEE itself.
O.TRUSTED_STORAGE	TA CPs may make use of trusted storage to protect secret data of the scheme, its protocols and data.
O.ROLLBACK_PROTECTION	This objective generally exceeds the requirements of most CP schemes.
O.TA_PERSISTENT_TIME	This objective generally exceeds the requirements of most CP schemes.

Mapping of objectives to CP requirements (3/3)

GP TEE PP Security Objective	Application to content protection schemes
OE.DEBUG	This objective applies to the TEE itself, but fulfils a need to protect CP TAs from analysis, debugging and inspection.
OE.INTEGRATION_CONFIGURATION	This objective applies to the TEE itself.
OE.MANAGEMENT	This objective applies to the TEE itself.
OE.PROTECTION_AFTER_DELIVERY	Pre-installed CP TAs may have to account for the fact that the TEE is not fully provisioned until first use.
OE.ROLLBACK	Not needed if O.ROLLBACK_PROTECTION is implemented.
OE.SECRETS	CP TAs may rely on the TEE's implementation of this objective to provide secure provisioning and personalization.
OE.TA_DEVELOPMENT	CP TA developers must observe the guidelines provided by the TEE supplier.
OE.TEE_FIRMWARE_UPGRADE	This objective applies to the TEE itself.
OE.UNIQUE_DEVICE_ID	CP TAs may rely on the TEE's implementation of this objective to reliably derive unique secret data for their own purposes.

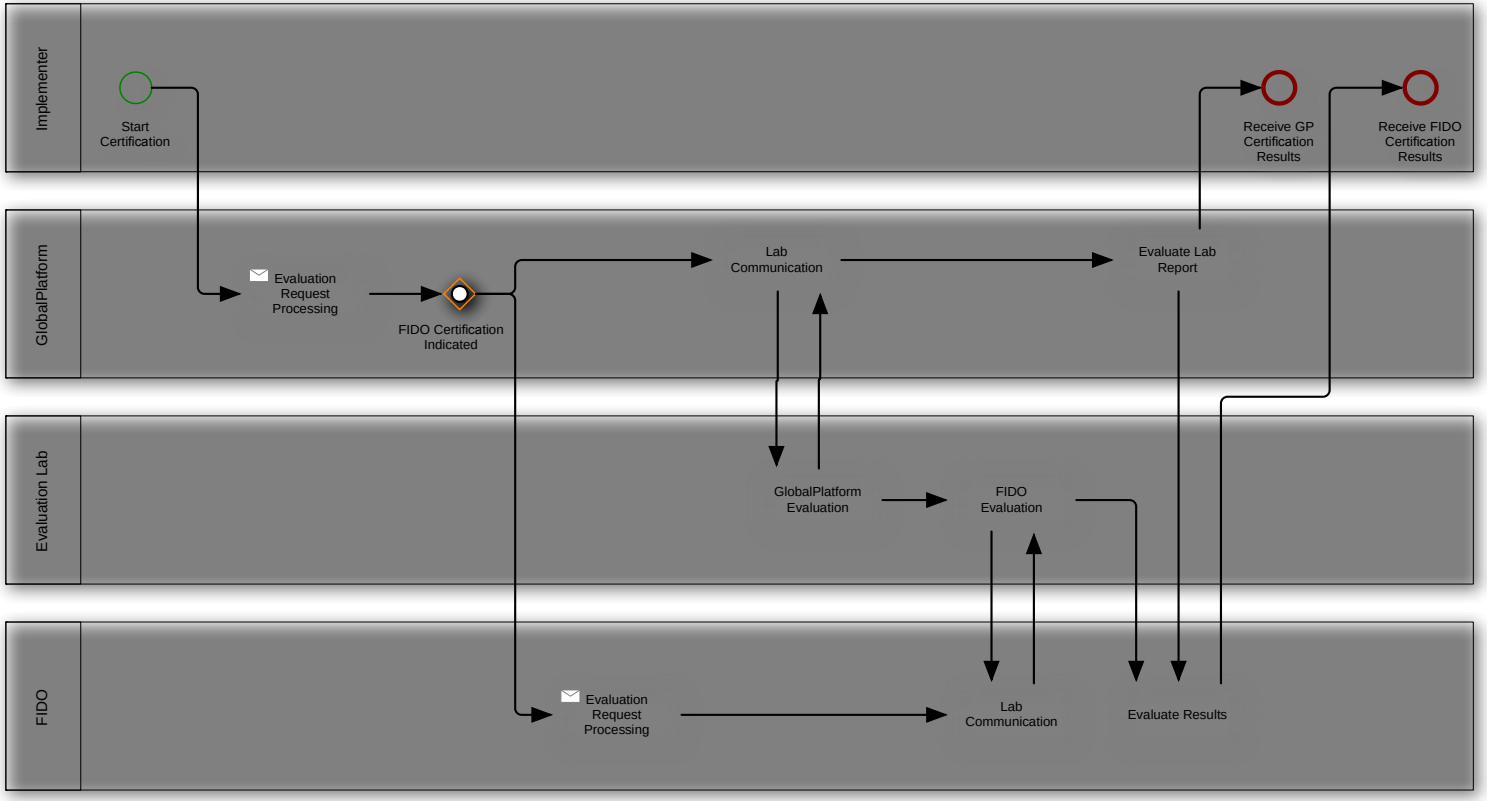
Threat Landscape

Threats	Mitigation	GlobalPlatform Positioning
Local attacker – discovery of attack	Increase Expertise and Cost required for Attack	Raises assurance bar for protection of decrypted Media playback on devices; Certification and Independent Evaluation for Hardware and Firmware implementation;
Packaging, Distribution and Replication of Attack;	Avoid use of Class secrets; Use of device binding; Experience degradation; Revocation;	Platform integrity, secure boot, Isolation between REE and between TAs prevents certain types of software attacks being replicated; In general TEE security features make it very costly to replicate attacks across devices;
Online distribution of pirated content	Forensic Watermarking, Legal means; System Renewal after Attack;	If TEE is not breached, provides a programmable security environment where updates can be provided in case of security breach.

GlobalPlatform and FIDO

FIDO - GlobalPlatform Collaboration

- Ease product vendors life by creating a **One Step Certification** process for TEE+FIDO
- High level process may be explained as follows:



Extension of the TEE Evaluation Methodology

GLOBALPLATFORM®

TEE PP and Evaluation Methodology

FIDO Security Requirements

fido alliance | simpler stronger authentication

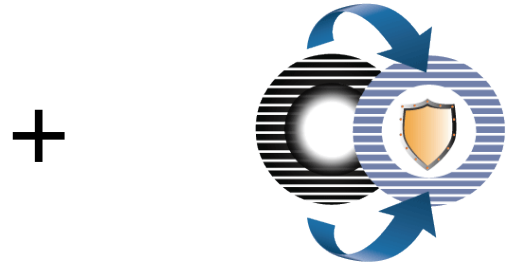
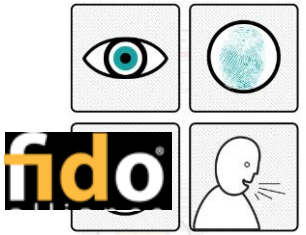
FIDO Evaluation on TEE

Lab Requirements For Accreditation

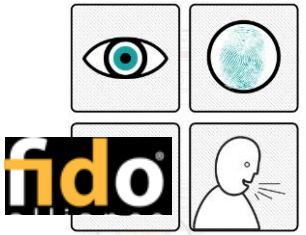
Add FIDO requirements (if any)

GP TEE Lab

Scope




Already Certified SE


Visit our website at www.globalplatform.org

GLOBALPLATFORM®

GLOBALPLATFORM®

Home | Member Login | Become a Member | Store | Search | Contact Us

specifications compliance certification membership about us media & resource center training 中文内容 jobs

The Standard for Managing Applications on Secure Chip Technology

Download the Latest Specs

> Card
> Device
> Systems
> Specs under public review

Become a Member

> Influence specifications development
> Enhance your global industry positioning
> Build industry relationships

Join Now >

Made Simple Guides

GlobalPlatform has launched a series of guides that aim to explain in simple terms the technology developments that it is working on and how these will benefit the industry.
Read More >

Technical Priorities

> Identity Task Force
> Internet-Of-Things Task Force
> Japan Task Force
> Mobile Task Force
> Premium Content Task Force
> Security Task Force
> Card Committee
> Device Committee
> Systems Committee

Enter Email Address

OK

I want to receive specification updates

GlobalPlatform News

> 12 Apr 16 - GlobalPlatform Agrees Memorandum of Understanding with Car Connectivity Consortium
> 06 Apr 16 - Executive Director Newsletter
> 04 Apr 16 - GlobalPlatform Welcomes New Participating Member Beijing Beanpod Technology
> 01 Mar 16 - Shenzhen Excelsecu Data Technology Co., Ltd. Joins GlobalPlatform
> More news

Global Events & Discounts

Recent Updates/Latest Content

GlobalPlatform is requesting SEs in SO ID-1 or UICC format for developing and testing purposes. Interested parties, please **share your proposals** by 30 June 2016.

The call for papers for the 2016 TEE Conference is now open! **Submit your speaker proposal now** to discuss payments, IoT, premium content protection, certification and more. Also, here's highlights from the 2015 event:

- 4th Annual Trusted Execution Environment (TEE) Seminar
- Thursday, 13 October 2016 in Santa Clara, California, USA
- Pre-Seminar TEE Specifications Training, Tuesday, 11 October and Wednesday, 12 October
- Post-Seminar TEE Application Developers Workshop, Friday, 14 October
- GlobalPlatform Presents: The Trusted Execution Environment (TEE): Connected Device Security for Today and Tomorrow

GLOBALPLATFORM™

THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

GlobalPlatform Presents:

THE TRUSTED EXECUTION ENVIRONMENT (TEE):

NEXT GENERATION MOBILE SECURITY FOR TODAY AND TOMORROW

Thank you!