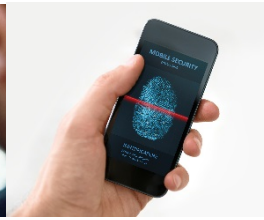



# GlobalPlatform

## *Common Criteria Protection Profile for Certifying the Security of the Trusted Execution Environment*

**18 May 2017**

**Hank Chavers**
**Technical Program Manager**

# GlobalPlatform Overview

# Securing Digital Services

GLOBALPLATFORM®

## GlobalPlatform: The Standard for Secure Digital Services and Devices

TRUSTED EXECUTION ENVIRONMENT

MESSAGING


SECURE ELEMENT

### Across several market sectors and in converging sectors

PREMIUM CONTENT

FINANCIAL

TELECOM

GOVERNMENT

AUTOMOTIVE

HEALTHCARE

RETAIL

TRANSIT

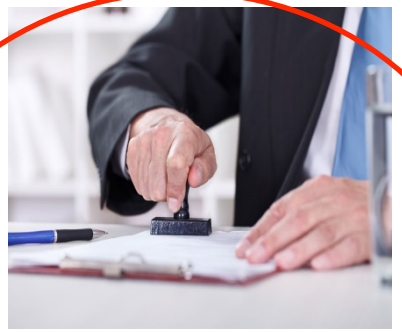
# Our Work Product

GLOBALPLATFORM®

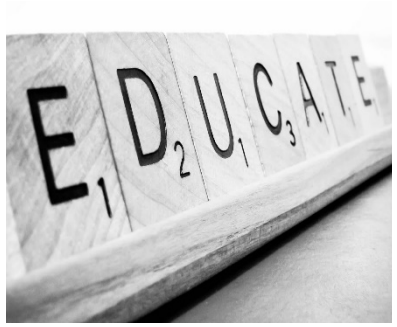

***Specifications***
Technical Industry Guidelines

***Configurations***
Guidelines Applied to Different Market Sectors


***Compliance***
Confirming Product Functionality to GlobalPlatform Technology



***Security Certification***
Streamlining Security Requirements & Testing




***Industry Education***
White Papers, Technical Documents & Seminars


***Industry Collaboration***
Workshops

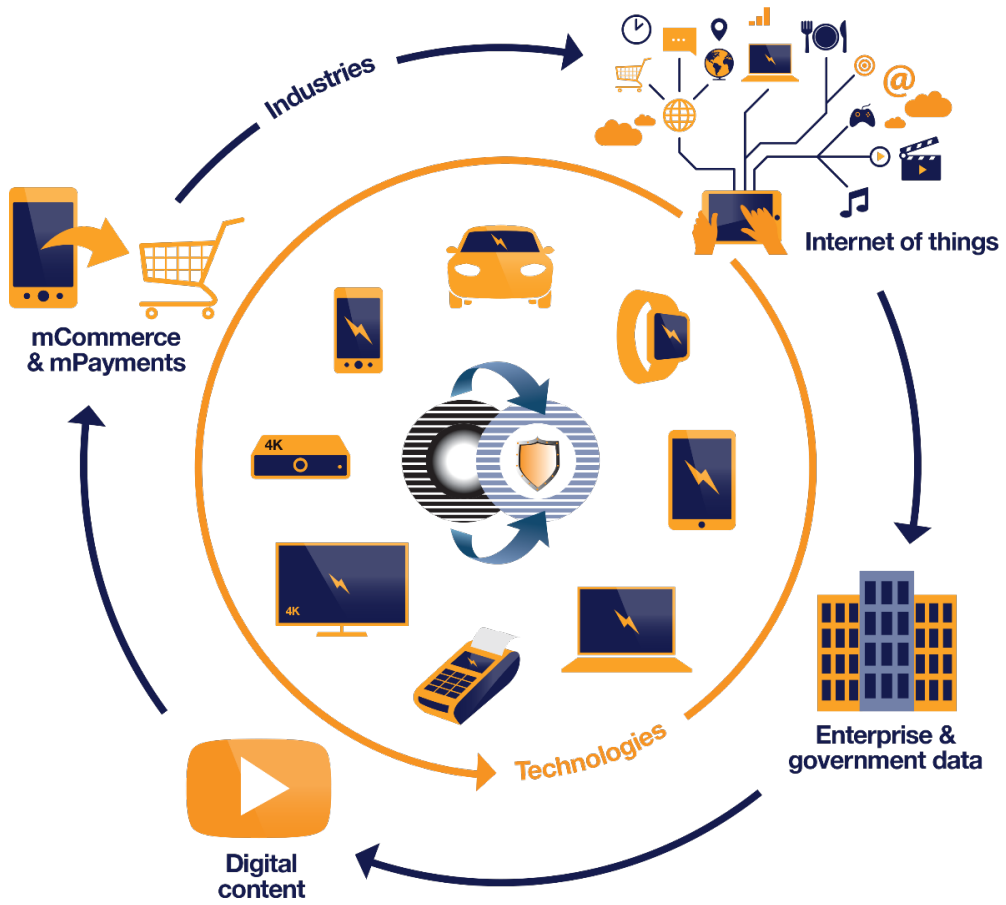
***Training***
Online & Instructor Led


***Developer Community***
Open Source Groups & Developer Workshops

# GlobalPlatform TEE Protection Profile

# GlobalPlatform TEE

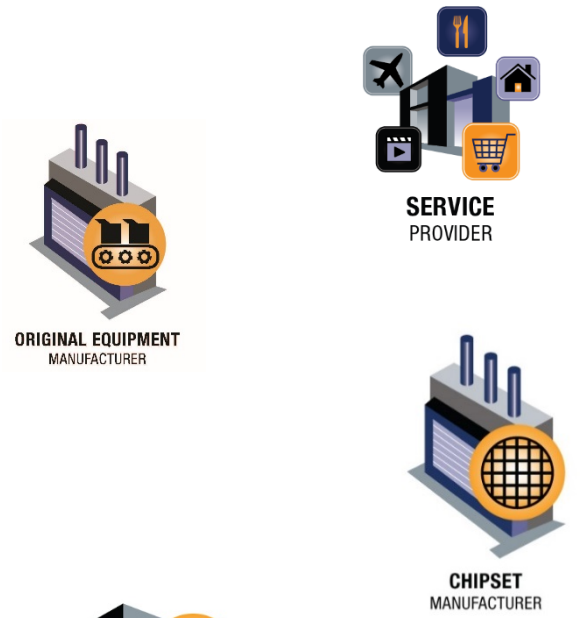
- GlobalPlatform defines a TEE as a secure area in the main processor in a smart phone (or any connected device)
- Ensures sensitive data is stored, processed, and protected in an isolated, trusted environment
- Offers isolated safe execution of authorized security software, known as 'trusted applications' which enables end-to-end security



# Addressing TEE Community Needs

GLOBALPLATFORM®

**GlobalPlatform members form a collaborative body…**

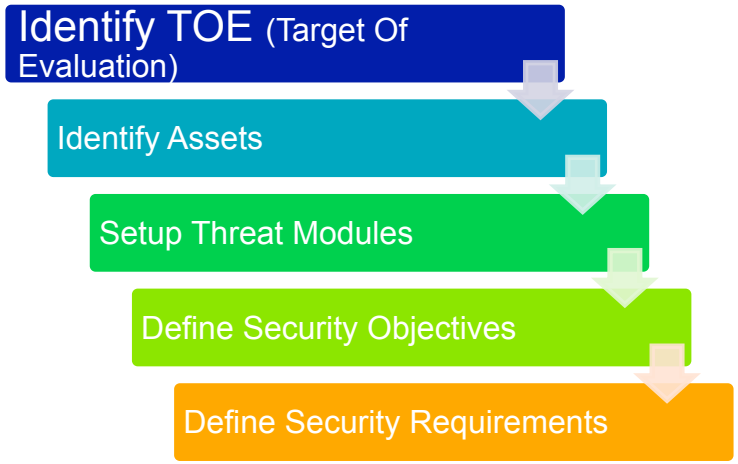



**…to address current and future requirements for the TEE Community**

- Specifications
- Functional Compliance Program
- TEE Protection Profile
- Security Certifications

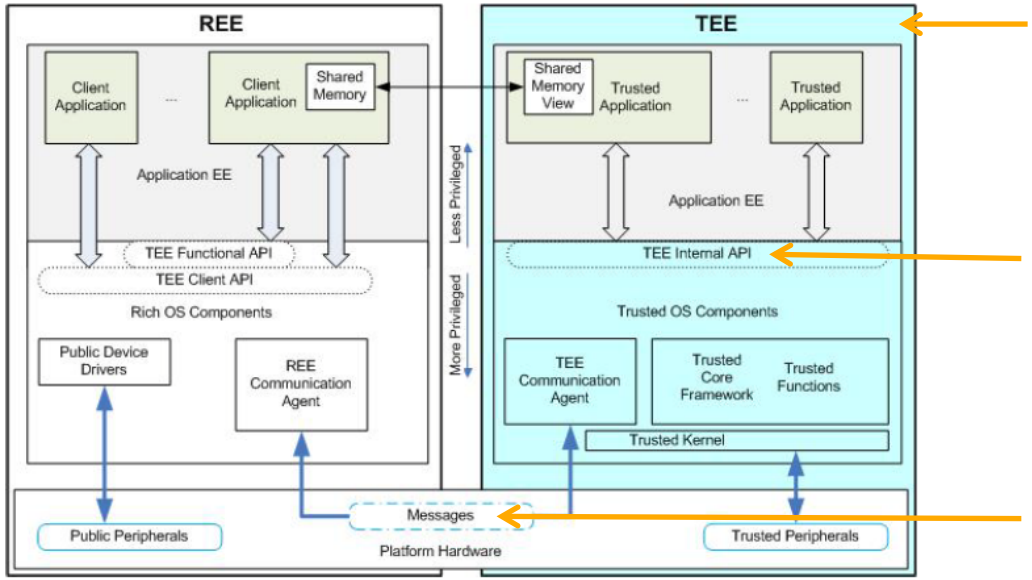
# TEE Protection Profile (TEE PP)

- Developed by the Security Working Group of the GlobalPlatform Device Committee
- Aiming at enabling mobile security services: content protection, rights management, corporate policies, payment, etc.
- GlobalPlatform TEE PP has been officially listed on the Common Criteria portal
- Certification scheme has been launched officially in June 2015
- GlobalPlatform TEE PP
  - specifies the typical threats the hardware and software of the TEE needs to withstand
  - details the security objectives that are to be met in order to counter these threats
  - specifies the security functional requirements that a TEE will have to comply with

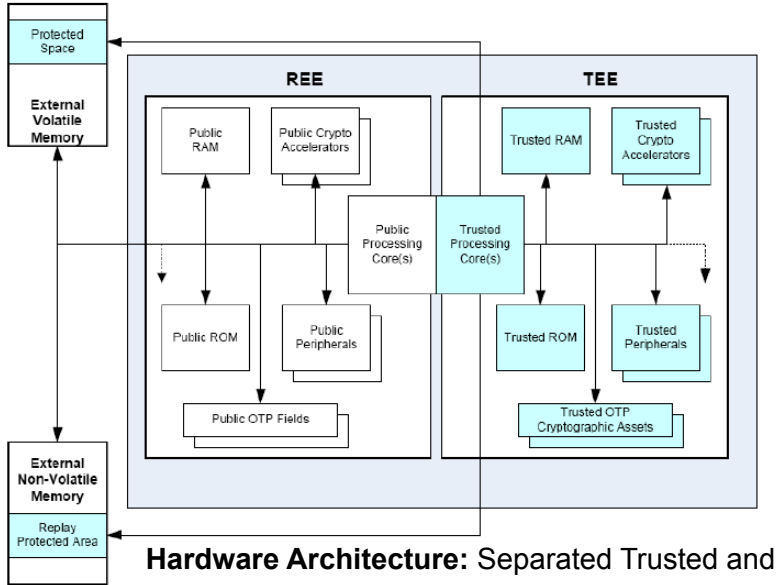


# TEE PP Scope

- TOE (Target Of Evaluation)
  - TOE comprises
    - Any 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
  - TOE does not comprise:
    - The Trusted Applications
    - The Rich Execution Environment
    - The Client Applications




**Software Architecture** of a TEE-enable Device. Independent of any hardware architecture

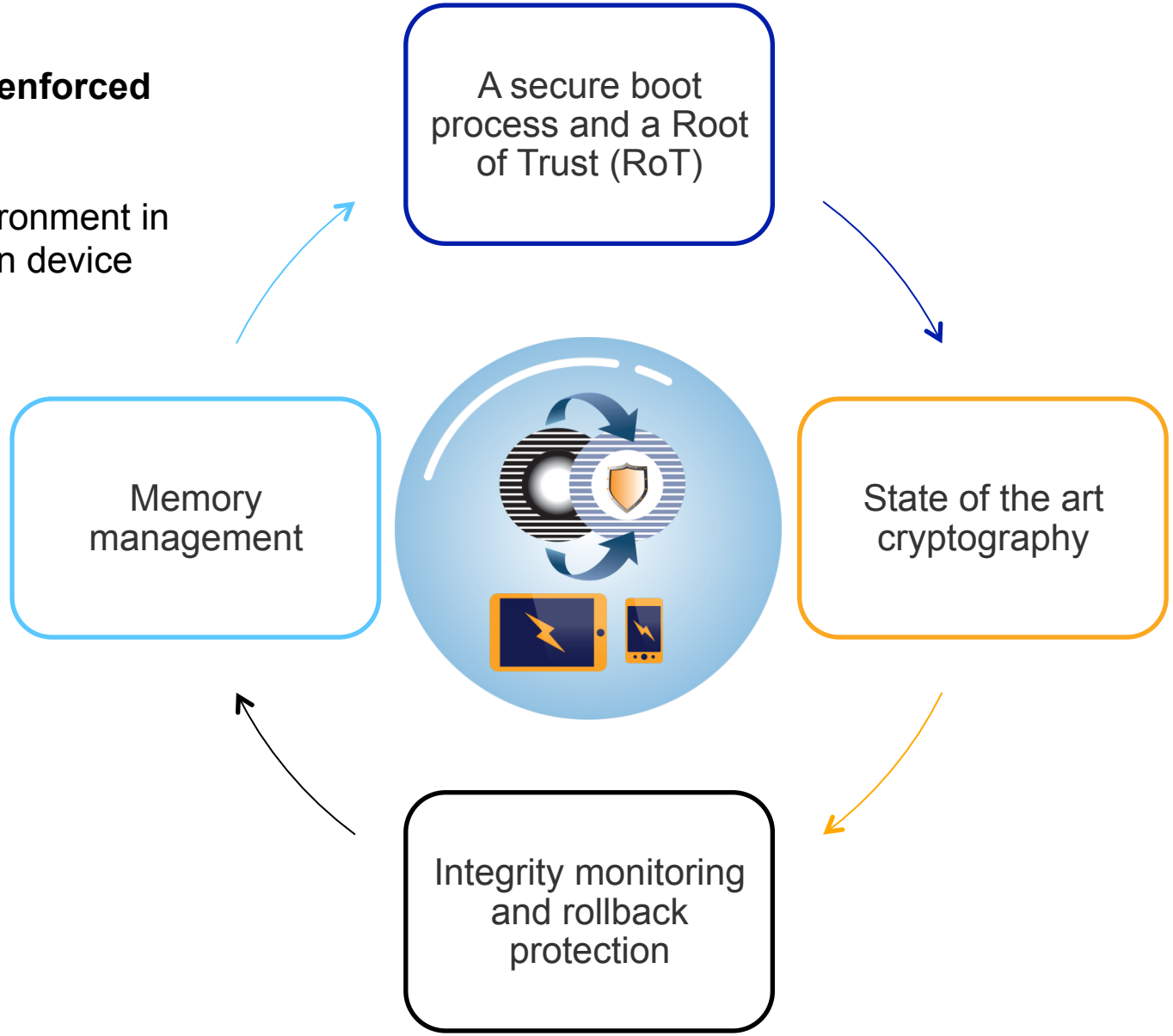



**Hardware Architecture:** Separated Trusted and Un-trusted Resources

# How to Create an Isolated Environment

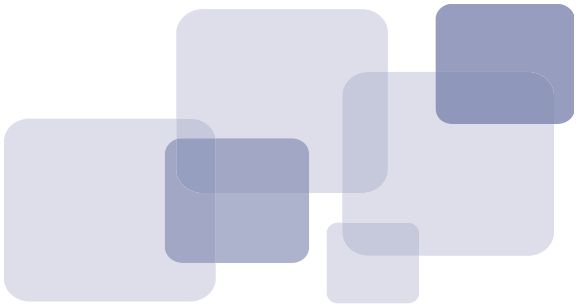
**Kernel-level hardware-enforced access control**

Creates an isolated environment in a multi-environment open device

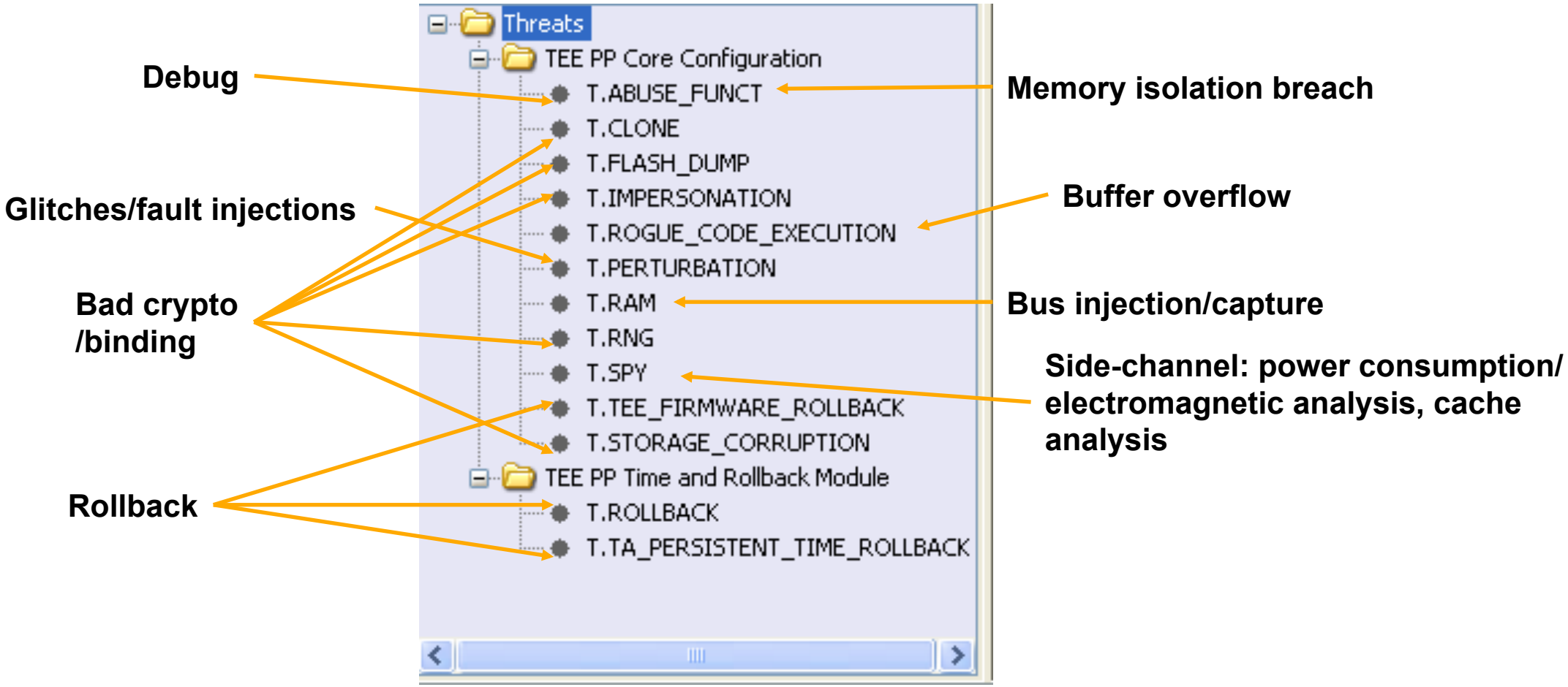


# Assets of the TEE Protection Profile

- TEE base-PP
  - TEE identification
  - RNG
  - Trusted Application code, data and keys
  - Trusted Application instance time
  - TEE runtime data, persistent data and firmware
  - TEE initialization code and data
  - TEE storage root of trust
- TEE Time and Rollback PP-Module
  - TA persistent time, data, keys and code
  - TEE data and rollback detection data
- TEE Debug PP-Module
  - TEE debug authentication key



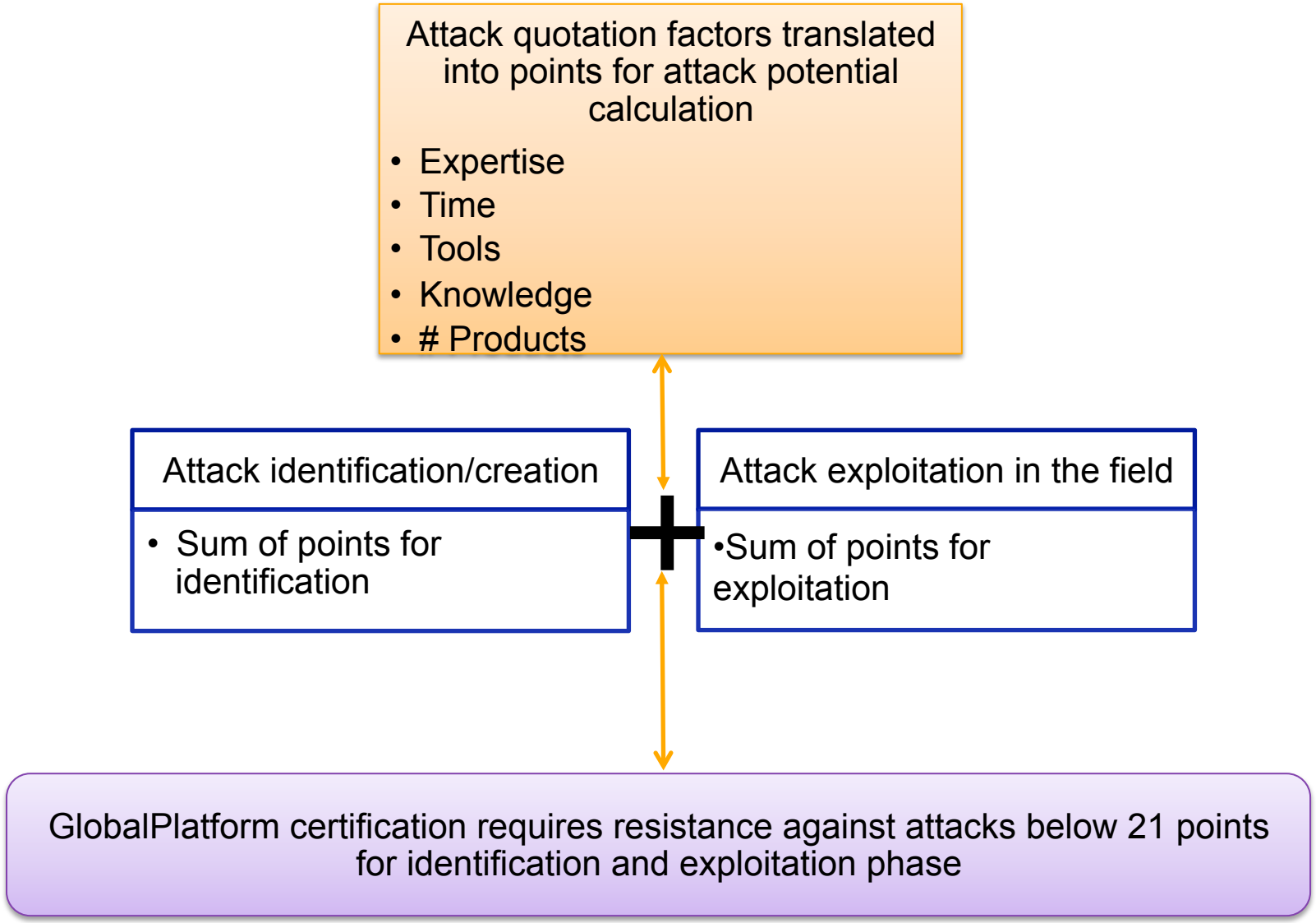
# Threats


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/fault injections
Bad crypto /binding
Rollback
Memory isolation breach
Buffer overflow
Bus injection/capture
Side-channel: power consumption/ electromagnetic analysis, cache analysis

# From Threats to Security Objectives and Security Requirements: An Example


| | | |
|---|---|---|
| **T.RAM**: attacker recovers RAM content, disclosing runtime data which potentially allows him to interfere with TEE code and data | **O. INITIALIZATION**: TEE shall be started through a secure initialization process | **FPT_FLS.1, FPT_INI.1, FCS_COP.1** |
| | **O.RUNTIME_CONFIDENTIALITY**: TEE shall ensure that confidential TEE runtime data and TA data & keys are protected against | **FDP_IFC.2/Runtime, FDP_IFF.1/Runtime, FDP.ITT.1/ Runtime, FDP_RIP.1/Runtime, FPT_ITT.1/Runtime** |
| | **O.RUNTIME_INTEGRITY**: TEE shall ensure that the TEE firmware, the TEE runtime data, the TA code and the TA data and keys are protected against unauthorized modification at runtime when stored in volatile memory | **FDP_IFC.2/Runtime, FDP_IFF.1/Runtime, FDP.ITT.1/ Runtime, FPT_ITT.1/Runtime, FDP_SDI.2** |
| | **O.TA_ISOLATION**: The TEE shall isolate the TAs from each other | **FDP_ACC.1/Trusted Storage, FDP_ACF.1/Trusted Storage, FDP_IFC.2/Runtime, FDP_IFF.1/Runtime; FMT_MSA.1/Trusted Storage, FMT_MSA.3/Trusted Storage; FMT_SMF.1, FCS_COP.1, FPT_FLS.1** |
| | **O.TEE_ISOLATION**: The TEE shall prevent the REE and the TAs from accessing the TEE own execution and storage space and resources | **FDP_IFC.2/Runtime, FDP_IFF.1/Runtime;** |

# Attack Criteria



# GlobalPlatform TEE Security Certification Program

# Market-Driven Scheme

- A certification process that takes into account the reality of TEE Products' life cycle
  - (Families of products) Initial and derived certificates
  - (Reuse) SoC and Device certification
- An evaluation methodology that focuses on the robustness of the security features
  - **3-month evaluation** of GlobalPlatform compliant products with source code
  - 100-day evaluation : 1/3 analysis, 2/3 testing
  - Delta evaluation process
  - Can be applied to con-compliant products supporting a secure enclave
- Risk management support to TEE Users / Service Providers
  - Residual vulnerability impact analysis
  - Full and Restricted certificates
- Developers & Verticals friendly
  - A platform-level certification reusable across verticals and form-factors
  - Extensible function-based certification, e.g. Media Content Protection, Biometric Systems
- Collaboration Effort across market and region
  - Standardization: FIDO, TAF, IFA, CC Certification Body (National CB), ISO/IEC JTC 1/SC 27, and ITC DSC
  - Working with Hollywood Studios

# TEE Security Certification Scheme

GLOBALPLATFORM®

## -- Fully Operational --

**Technical Community**
TEE & Security Experts
Laboratories
Developers
Integrators

→ TEE Protection Profile

Evaluation Methodology

PP Modules Under Development
(Secure Media Path, Trusted UI, Biometric API, SE API)

Security Functional Test Plan
Attack Methods

**GP Security Evaluation Secretariat**

→ TEE Certification Process

Lab Accreditation Guidelines

Lab & Vendor Agreements

**Laboratories**
ISO 17025

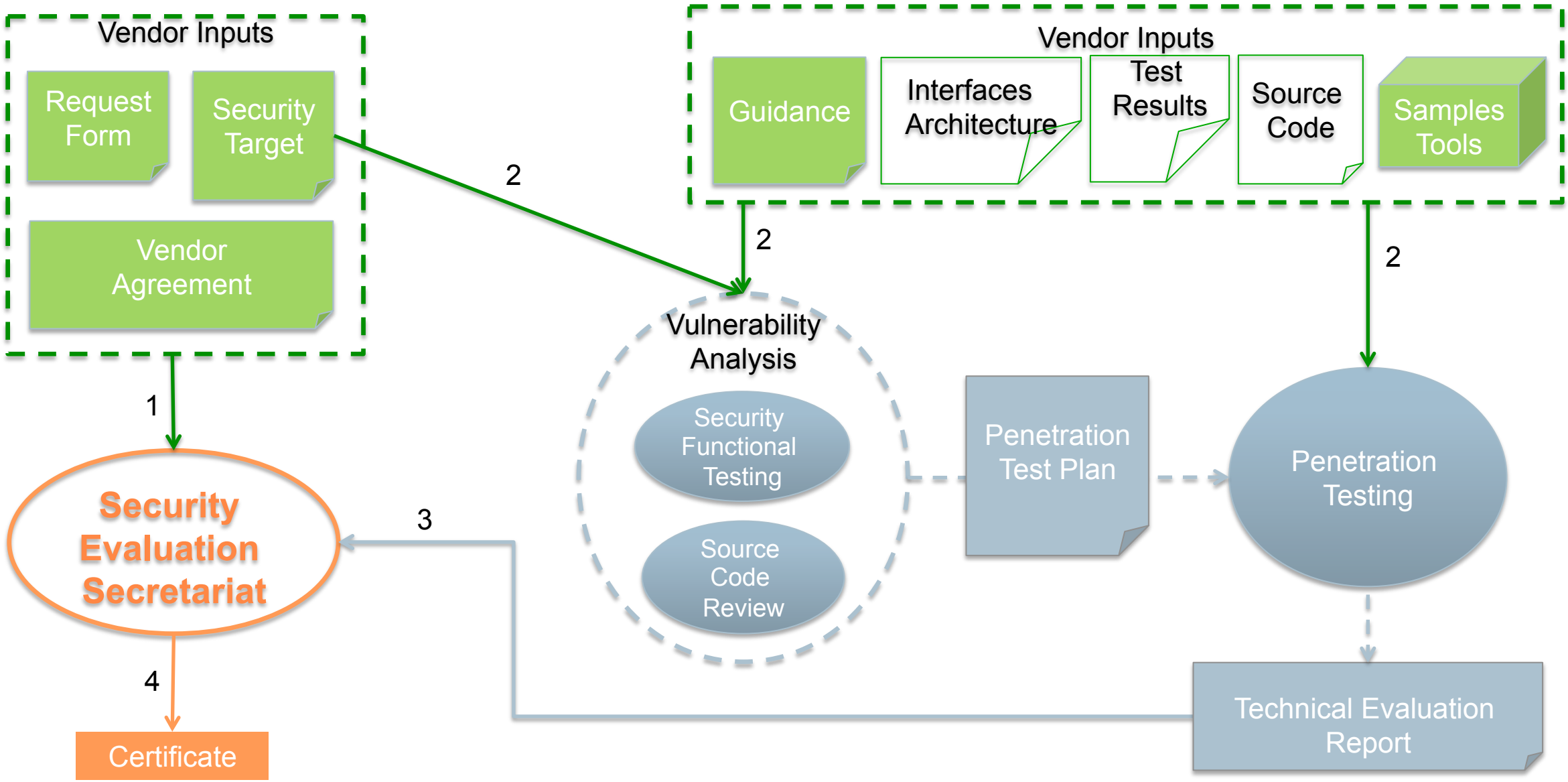
→

**Accredited**
Applus
Riscure
Thales

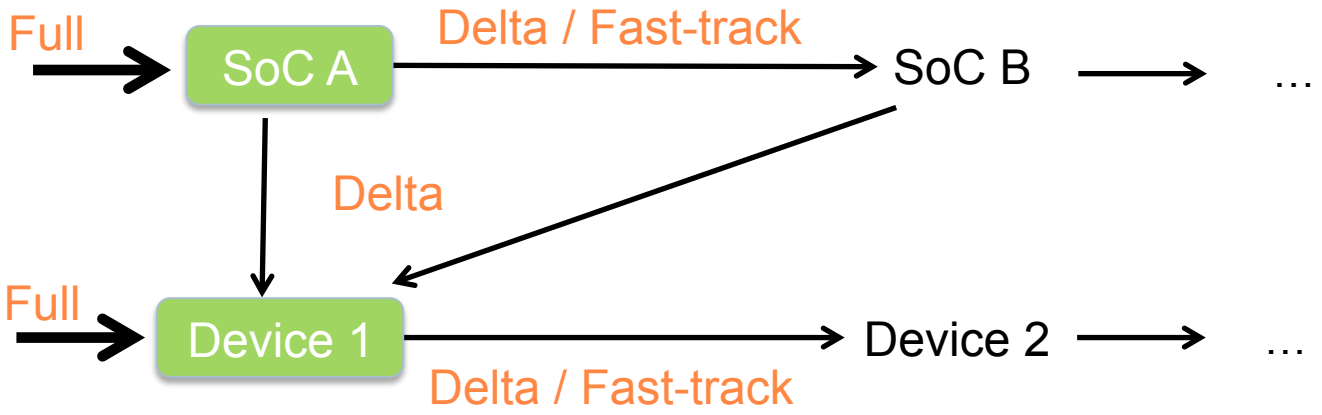
**Pre-Accredited**
Brightsight
DPLS
Trusted Labs
UL

# Evaluation and Certification Process

GLOBALPLATFORM®



# Full, Delta and Fast-track Evaluation




Fast-track

(same type of TOE): list of changes that do not require lab analysis

Delta evaluation

(same type of TOE): examples of TOE changes that can be evaluated locally

(from SoC to Device): examples of SoC changes and Device features that can be evaluated locally

# Stakeholders Benefits

GLOBALPLATFORM®

**Service providers** can develop a service once and deploy everywhere, which enables universal and consistent risk management strategy

**Chipset manufacturers / OEMs** prove the security of products to internationally recognized standard

**National certification** bodies can connect with experts in the field to set regional standards

**Industries bodies** can incorporate into their requirements, streamlining product testing

**Security labs** have the opportunity to play an active role in the evolution of TEE security

# Thank you!