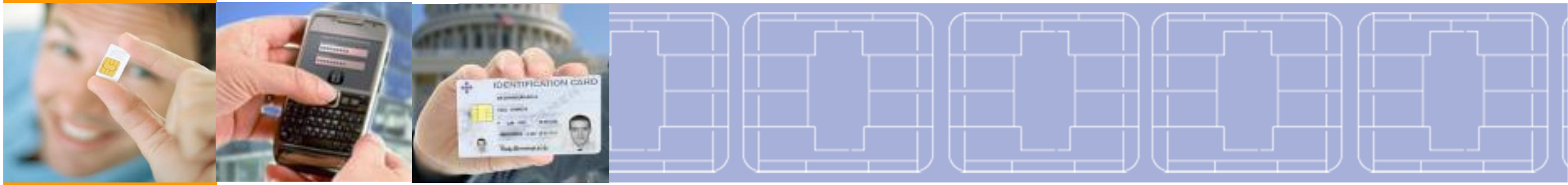
GLOBALPLATFORM™



Certification of the Trusted Execution Environment – one step ahead for secure mobile devices

GlobalPlatform Member Representatives:
Carolina Lavatelli, Trusted Labs
Hervé Sibert, ST Microelectronics

14th ICCC - Orlando, USA
September 10th 2013

@GlobalPlatform_

www.linkedin.com/company/globalplatform

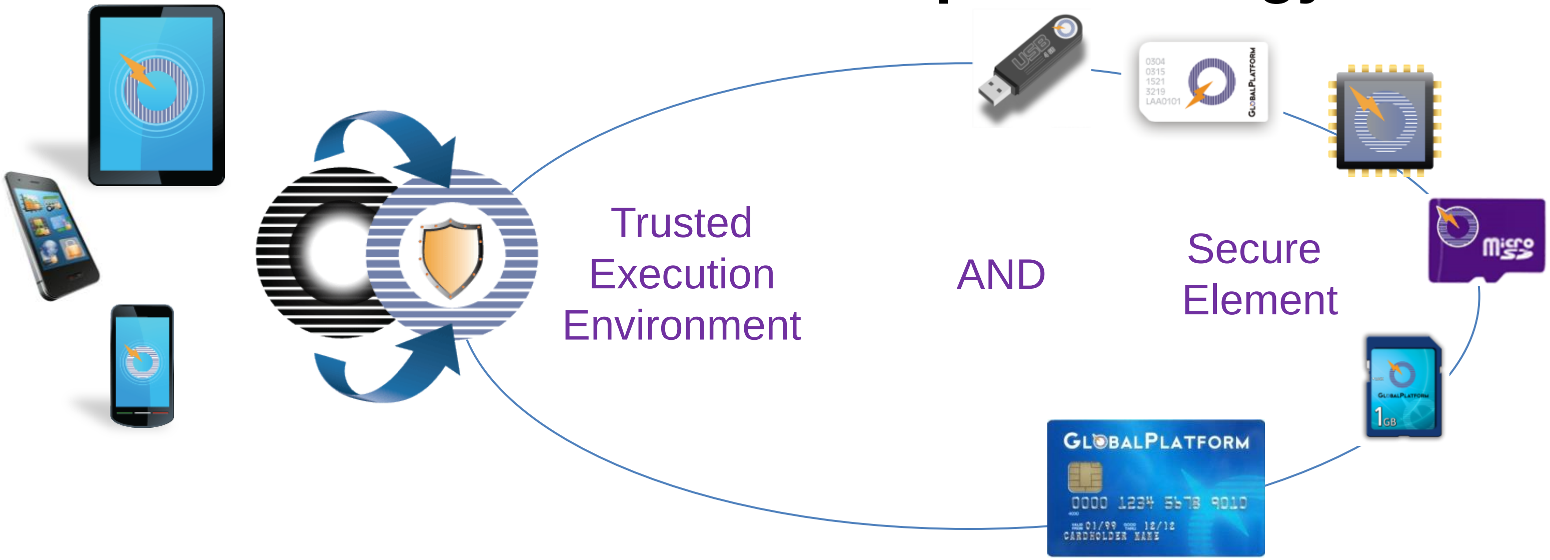
Agenda

- **Introduction**
  - GlobalPlatform positioning
  - Trusted execution environment (TEE) use cases, functionality and security properties
  - The choice of Common Criteria
- **Trusted Execution Environment Protection Profile (TEE PP)**
  - Target of Evaluation (TOE) boundary and security functionality
  - Threat model
  - Assets, security problem definition (SPD), objectives and SFR
  - TEE Evaluation Assurance Level (EAL)
- **Technical Communities (TC)**
  - The GlobalPlatform TC
  - The TEE PP roadmap
  - International TC: why and how?

Introduction

GlobalPlatform Positioning

GlobalPlatform is *the* standard for managing applications on secure chip technology



Trusted Execution Environment

AND

Secure Element

Across several market sectors and in converging sectors

TEE Use Cases

Smartphones, tablets, set-top boxes, automotive, etc.

Normal World

Secure World

Almost all recent mobile devices support TEE technology and the primary **commercial** usage today is DRM

Use cases

Content Protection

- IP streaming
- DRM…
- Key protection
- Content protection

Mobile Financial Services

- mBanking
- Online payment…
- User authentication
- Transaction validation

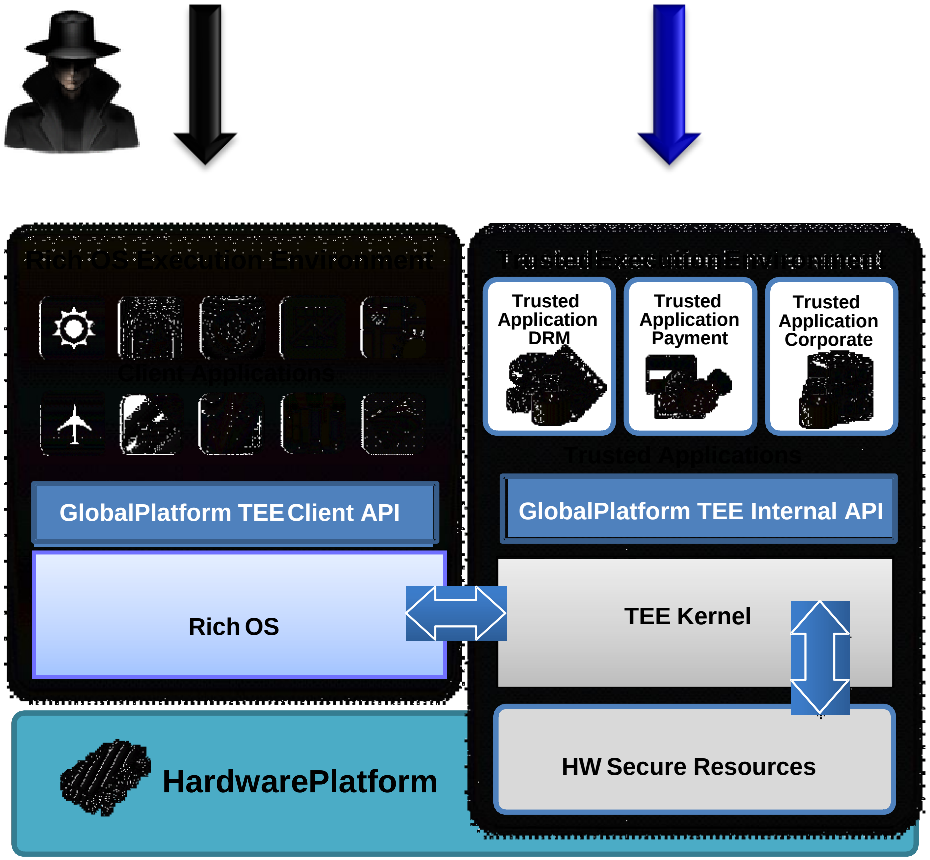
Corporate / Government

- Secure networking
- Secure email
- BYOD
- User authentication
- Data encryption

What is a TEE?

Open to malware, rooting / jailbreaking

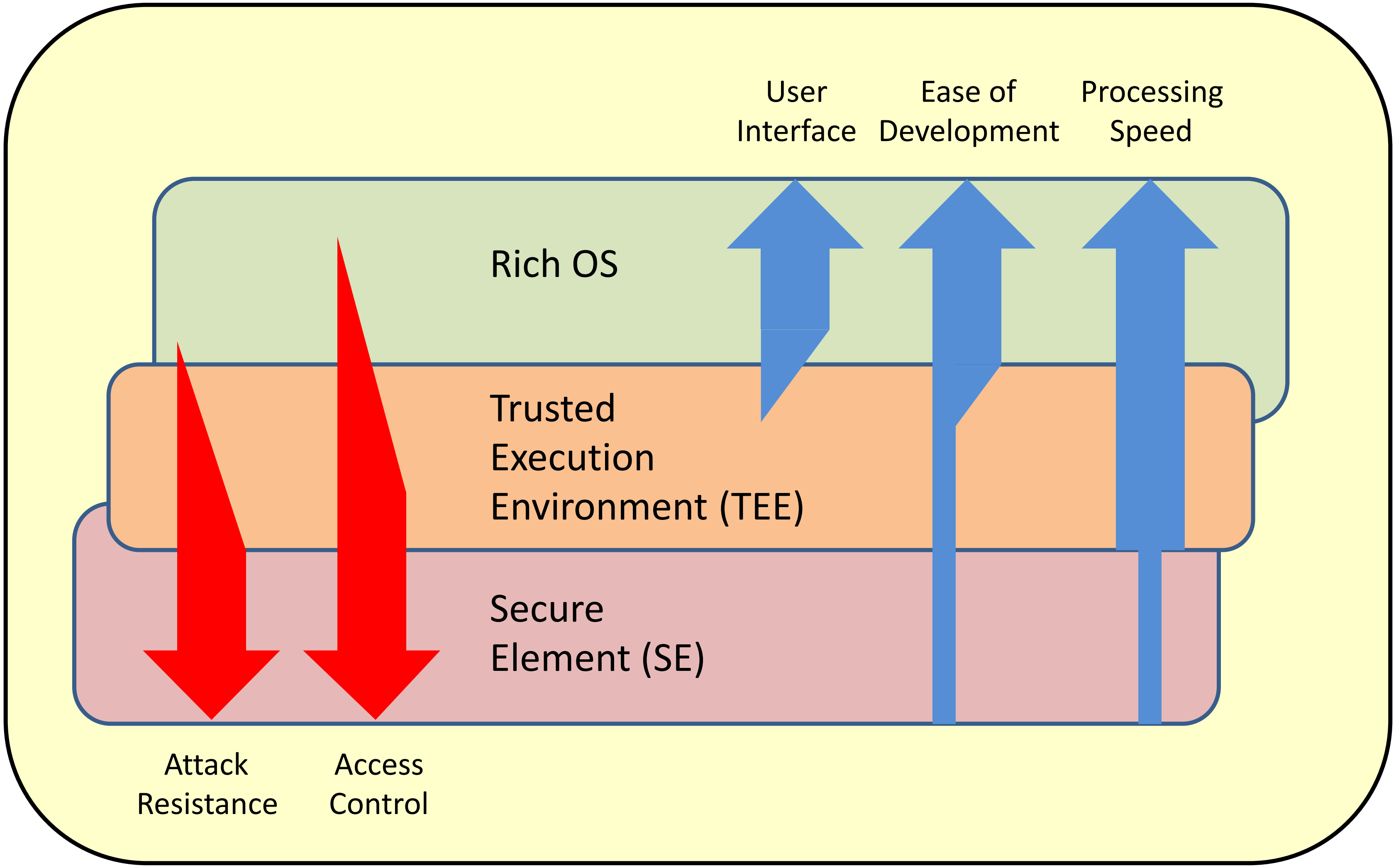
Isolation of sensitive assets and functionality



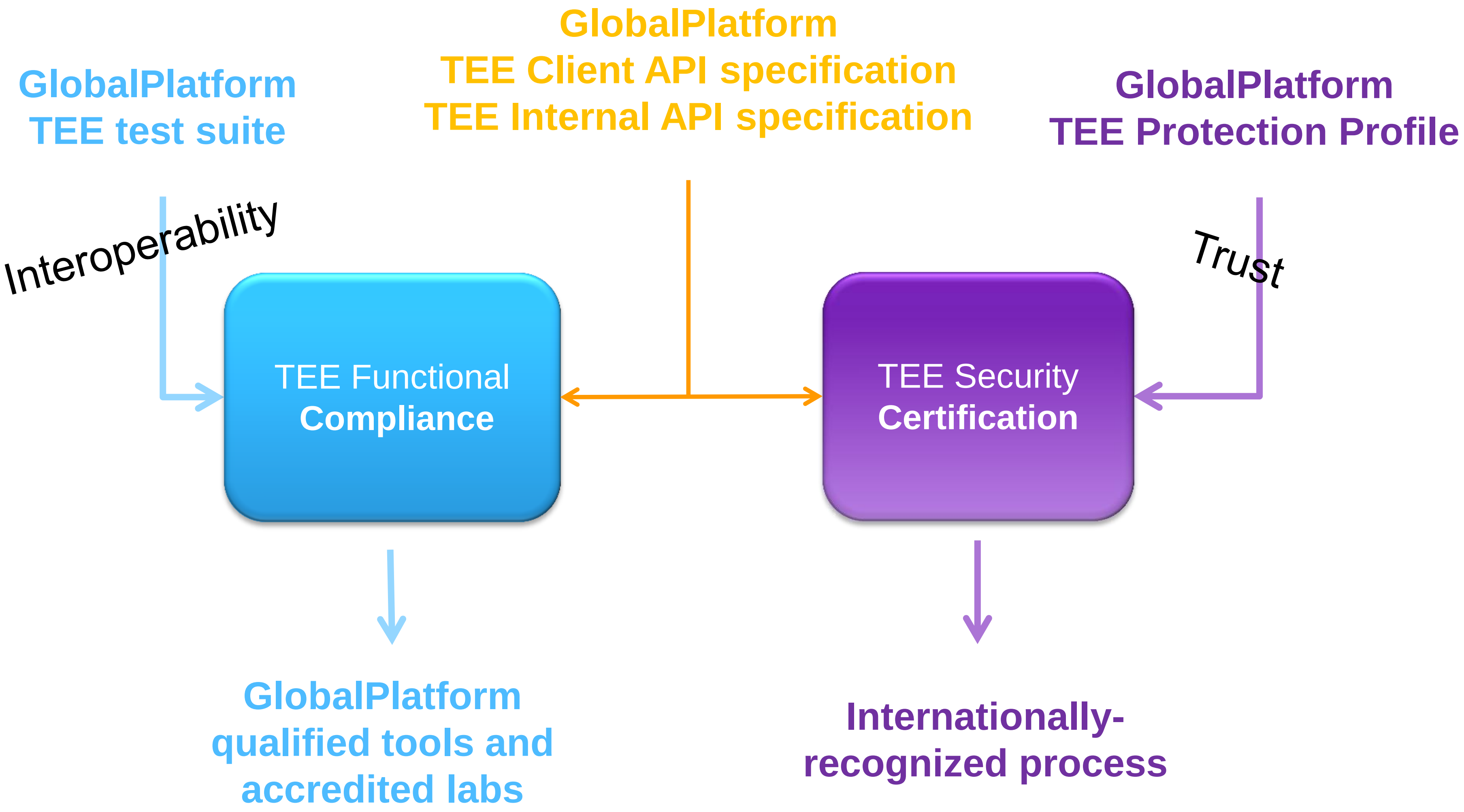
Rich OS Execution Environment
Client Applications
GlobalPlatform TEE Client API
Rich OS
Trusted Execution Environment
Trusted Application DRM
Trusted Application Payment
Trusted Application Corporate
Trusted Applications
GlobalPlatform TEE Internal API
TEE Kernel
HW Secure Resources
HardwarePlatform

- TEE provides **hardware-based isolation** from rich operating systems (OS) such as Android
- TEE runs on the **main hardware platform and relies on hardware roots of trust (crypto keys and secure boot)**
- TEE has **privileged access** to device resources **(user interface, crypto accelerators, secure elements…)**

TEE Positioning



GlobalPlatform TEE Environment



GlobalPlatform
TEE test suite

GlobalPlatform
TEE Client API specification
TEE Internal API specification

GlobalPlatform
TEE Protection Profile

Interoperability

Trust

TEE Functional
Compliance

TEE Security
Certification

GlobalPlatform
qualified tools and
accredited labs

Internationally-
recognized process

Security Certification Program

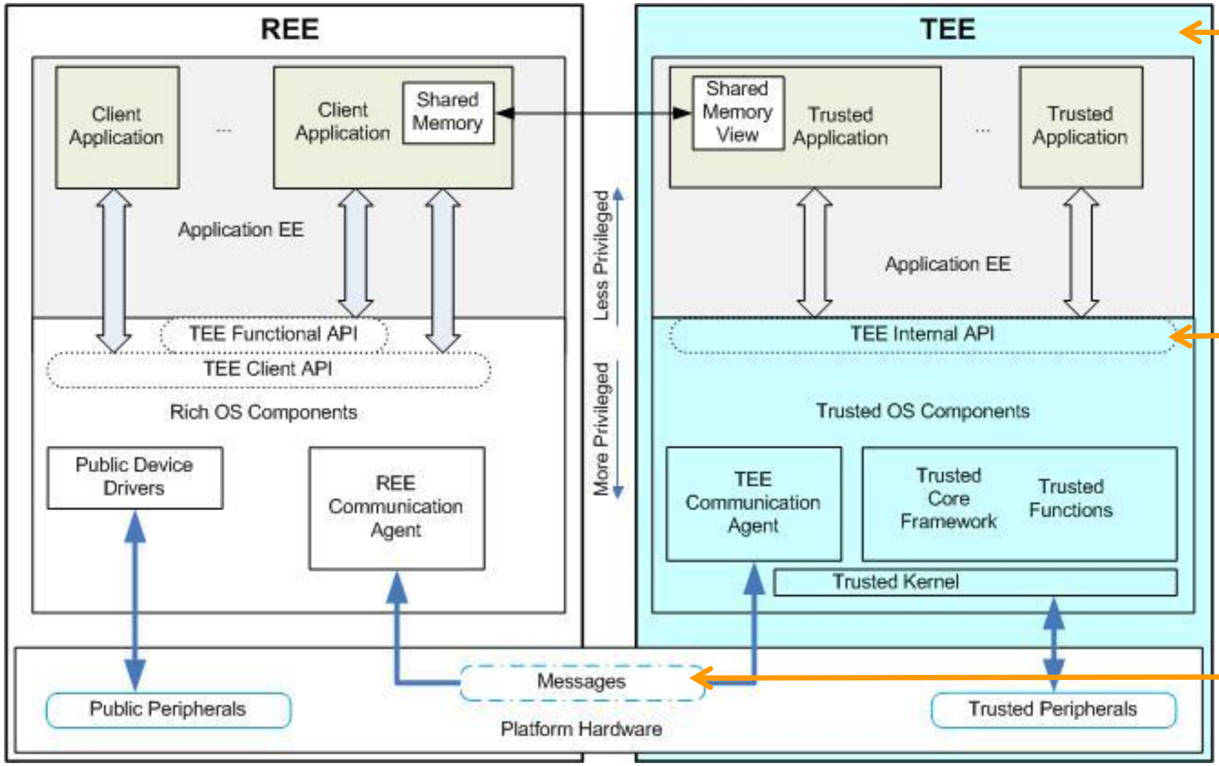
- Goals:
  - To ensure there is a means of evaluating TEE security by closing the certification gap with a pragmatic approach compatible with short device life-cycle
  - To provide security assurance to stakeholders (device manufacturers, service providers, regulators)
- The choice of Common Criteria methodology has been triggered by:
  - Proven framework for the statement of security requirements (through Protection Profiles) and evaluation methodology
  - Existent network of security accredited labs
  - International recognition
  - Applicability to the domain
  - Market acceptance

Trusted Execution Environment Protection Profile (TEE PP)

What is the security level of the TEE?

What are the security properties to be enforced?

The Target of Evaluation (TOE)



TOE (HW, FW, SW)

Boundary with Trusted Applications:

TEE Internal API

Boundary with Rich operating system (OS): Messaging interface

The TOE comprises:

- **Any hardware, firmware and software** used to provide the TEE security functionality
- The guidance for the secure usage of the TEE after delivery

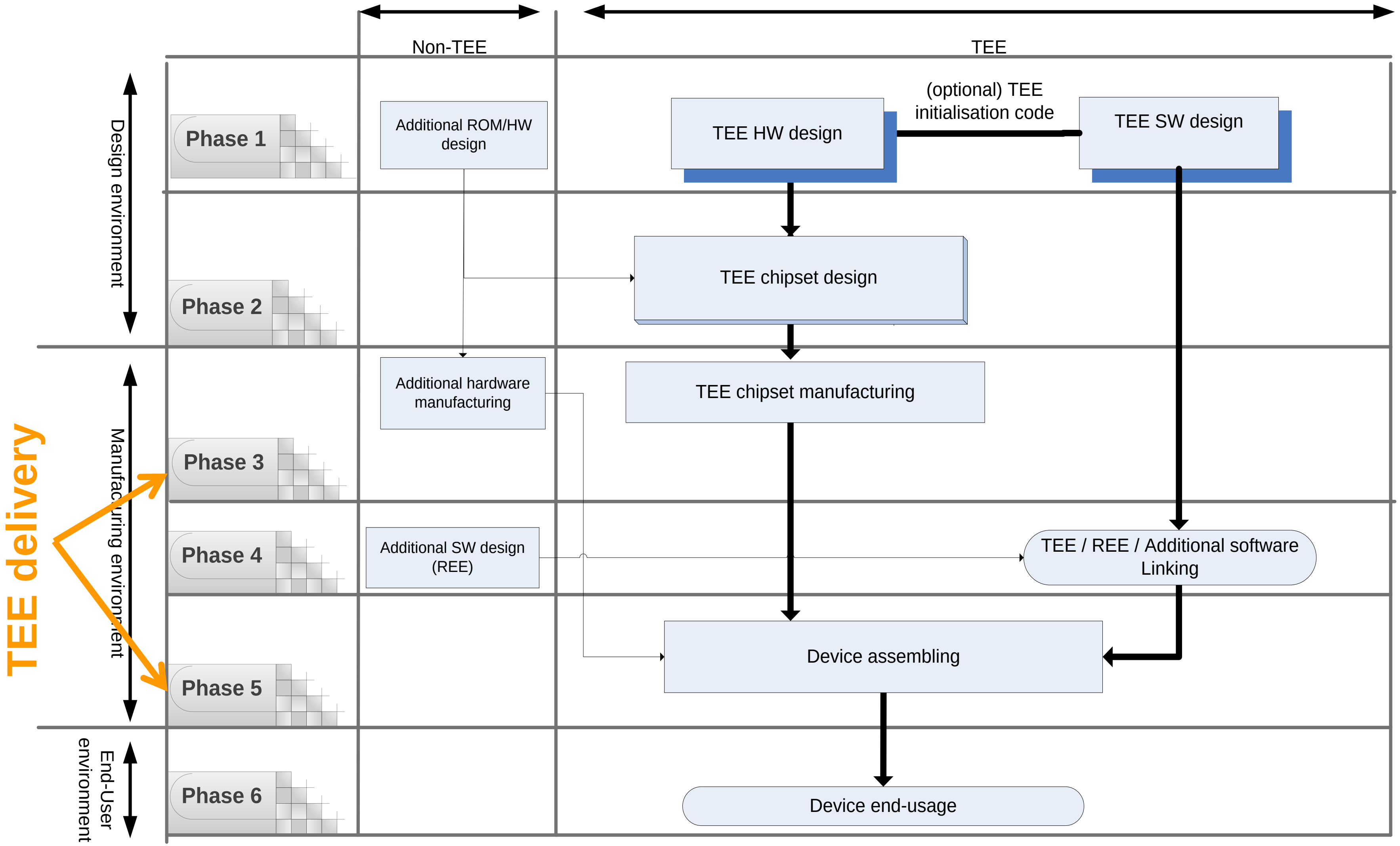
The TOE does not comprise:

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

TOE Security Functionality

- 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)
- Isolation of the TEE services, the TEE resources involved and all the TAs from the REE
- Isolation between TAs and isolation of the TEE from TAs
- Protected communication interface between CAs and TAs within the TEE, including communication endpoints in the TEE
- Trusted storage of TA and TEE data and keys, ensuring consistency, confidentiality, atomicity and binding to the TEE
- Correct execution of TA services
- Random number generator
- Cryptographic API including generation and derivation of keys and key pairs, support for cryptographic algorithms such as SHA-256, AES 128/256, T-DES, RSA 2048, etc.
- Monotonic TA instance time
- TEE firmware integrity up to modifications authorized by the upgrade policy (implementation-dependent)
- *Advanced TEE (rollback protection over resets)*
  - *Monotonic persistent time*
  - *Full integrity protection of TA data, code, keys and TEE data*

Device Lifecycle



Threat Model

- 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

Attack Potential

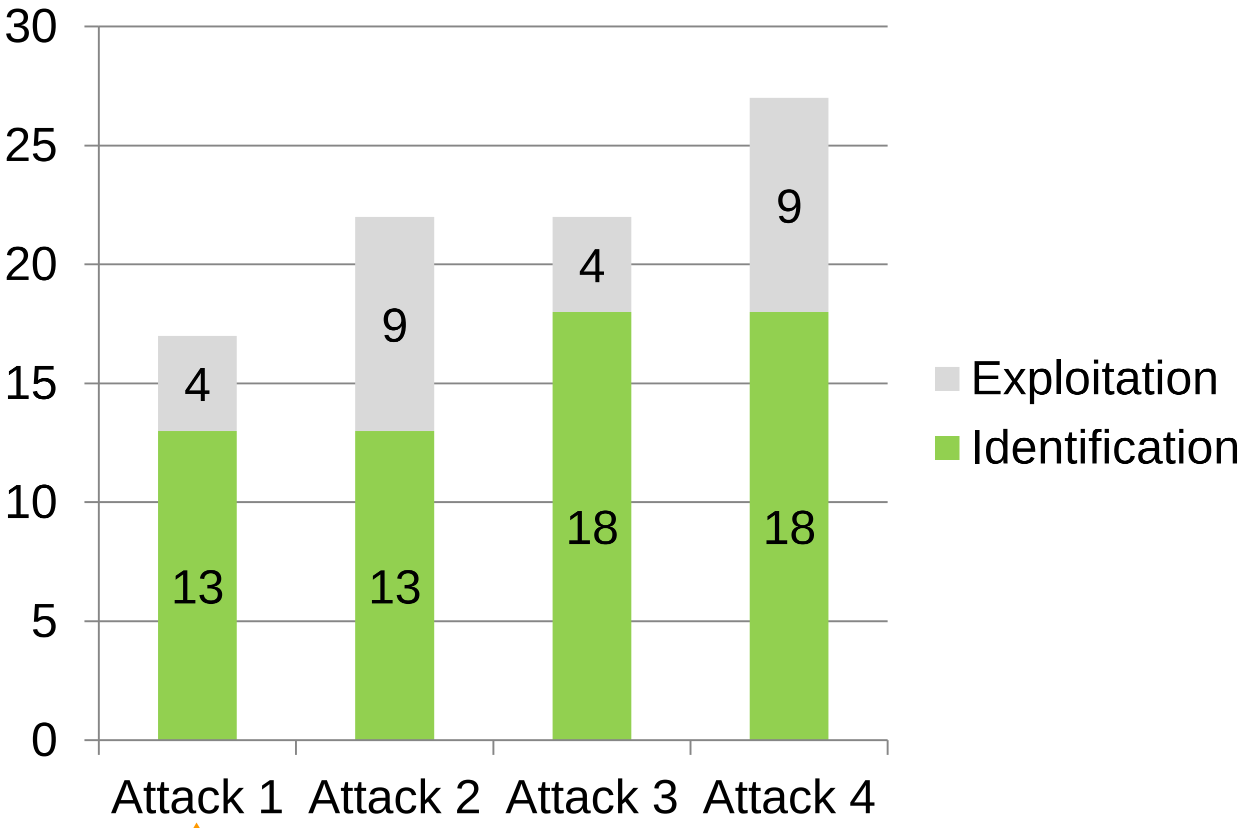
- The TEE PP provides:
  - The TEE attack quotation table for rating full attack paths from identification to exploitation
  - The description and quotation of four representative exploitation profiles
  - A list of illustrative attacks at identification phase

- 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

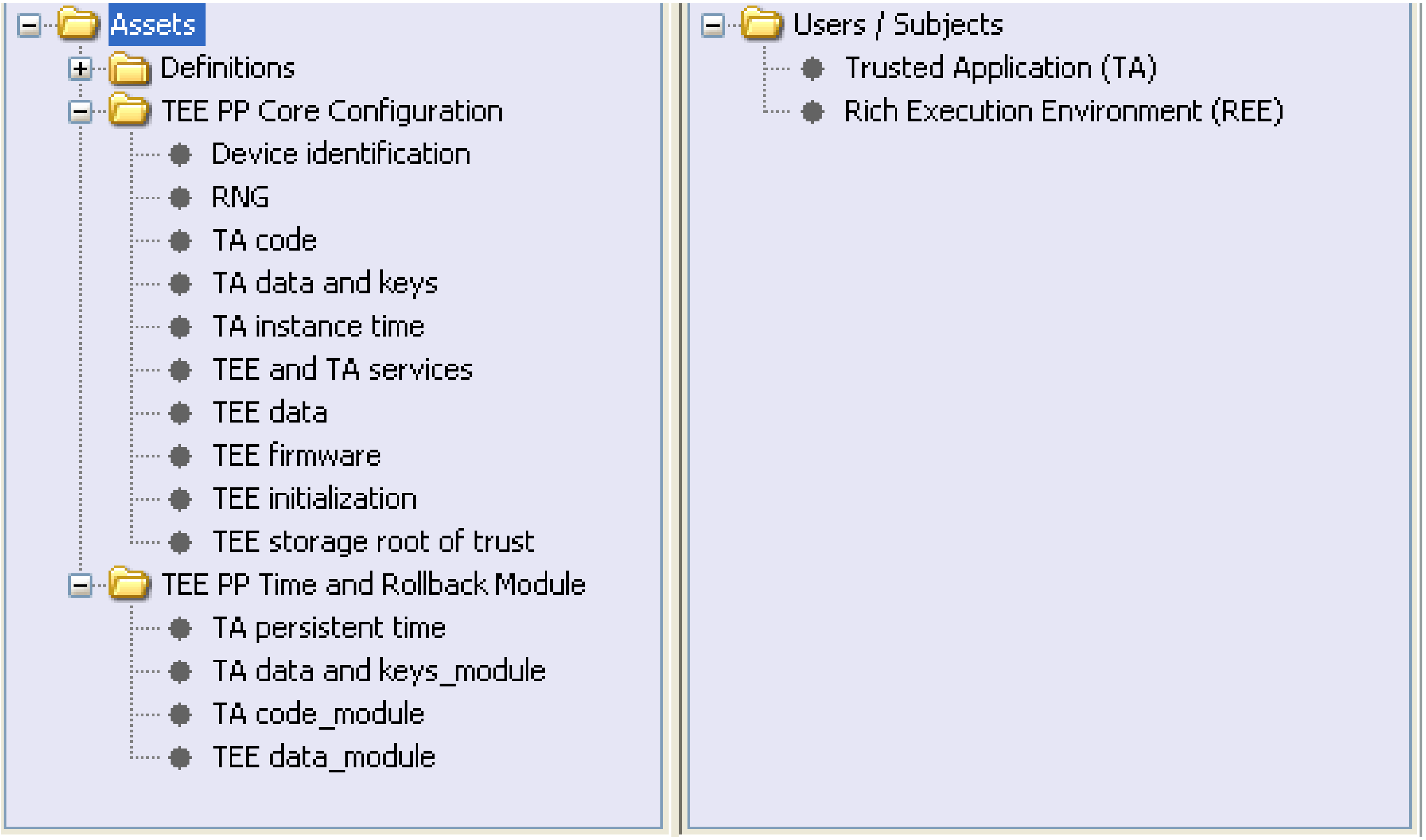
Enhanced-Basic



In scope

Discarded

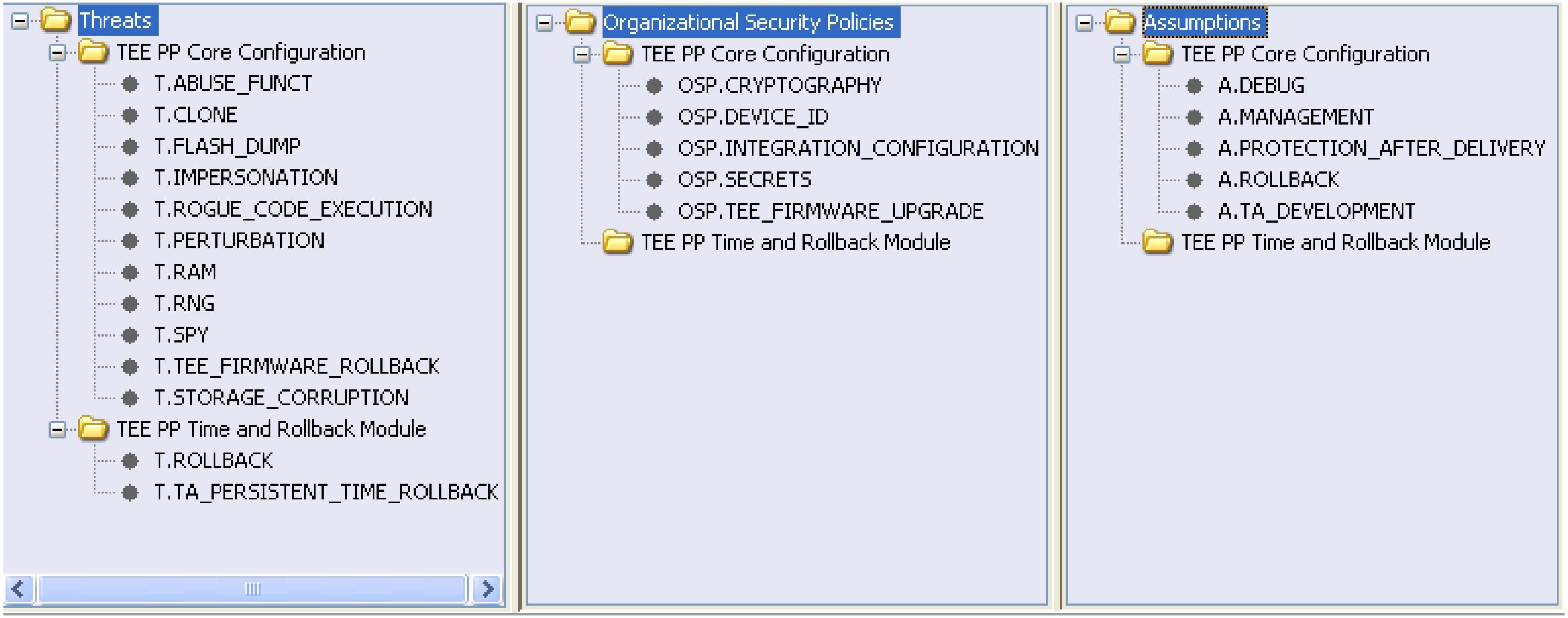
Assets and Users



- Assets
  - Definitions
  - TEE PP Core Configuration
    - Device identification
    - RNG
    - TA code
    - TA data and keys
    - TA instance time
    - TEE and TA services
    - TEE data
    - TEE firmware
    - TEE initialization
    - TEE storage root of trust
  - TEE PP Time and Rollback Module
    - TA persistent time
    - TA data and keys_module
    - TA code_module
    - TEE data_module

- Users / Subjects
  - Trusted Application (TA)
  - Rich Execution Environment (REE)

Security Problem Definition

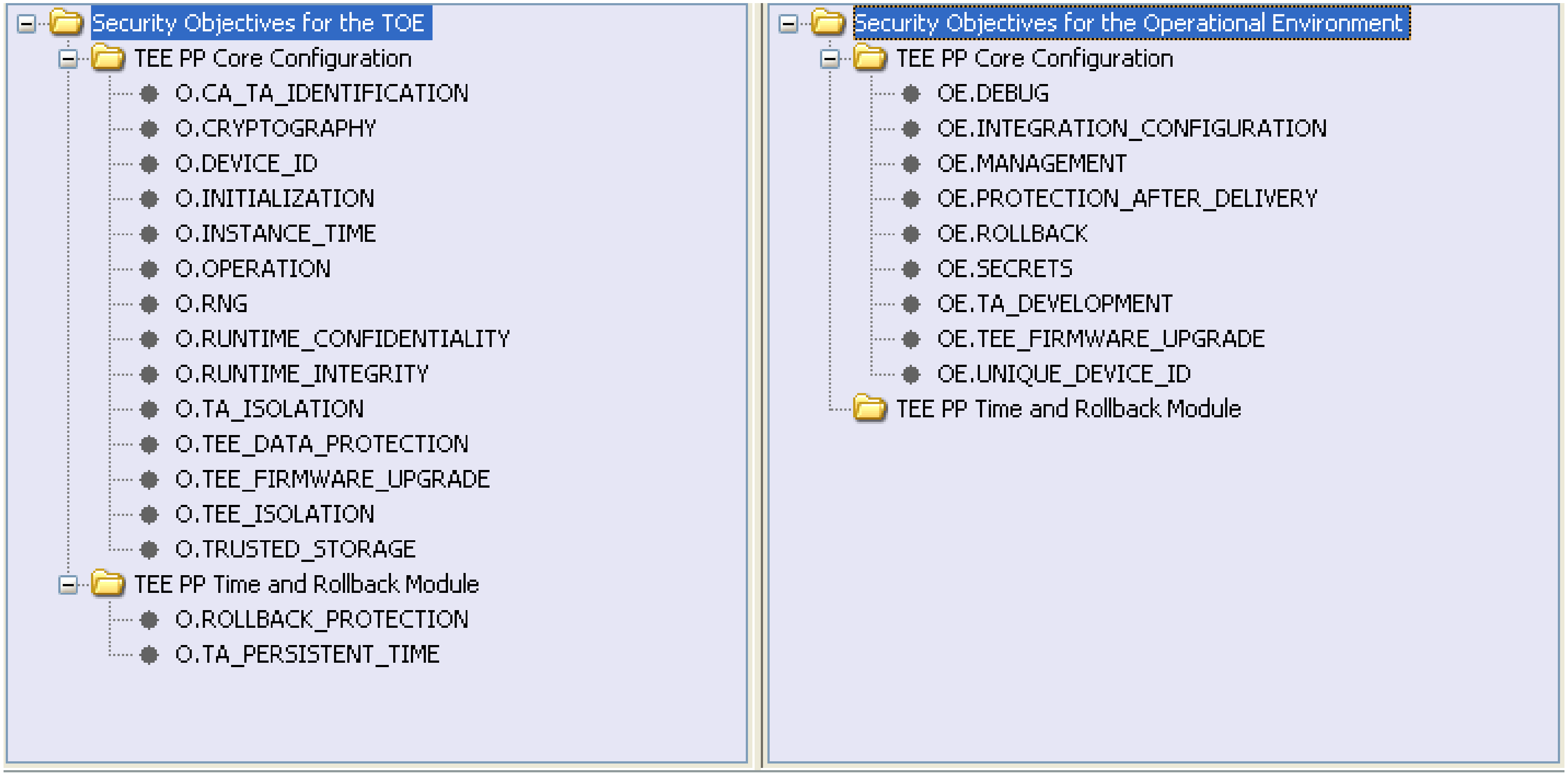


- Threats
  - TEE PP Core Configuration
    - T.ABUSE_FUNCT
    - T.CLONE
    - T.FLASH_DUMP
    - T.IMPERSONATION
    - T.ROGUE_CODE_EXECUTION
    - T.PERTURBATION
    - T.RAM
    - T.RNG
    - T.SPY
    - T.TEE_FIRMWARE_ROLLBACK
    - T.STORAGE_CORRUPTION
  - TEE PP Time and Rollback Module
    - T.ROLLBACK
    - T.TA_PERSISTENT_TIME_ROLLBACK

- Organizational Security Policies
  - TEE PP Core Configuration
    - OSP.CRYPTOGRAPHY
    - OSP.DEVICE_ID
    - OSP.INTEGRATION_CONFIGURATION
    - OSP.SECRETS
    - OSP.TEE_FIRMWARE_UPGRADE
  - TEE PP Time and Rollback Module

- Assumptions
  - TEE PP Core Configuration
    - A.DEBUG
    - A.MANAGEMENT
    - A.PROTECTION_AFTER_DELIVERY
    - A.ROLLBACK
    - A.TA_DEVELOPMENT
  - TEE PP Time and Rollback Module

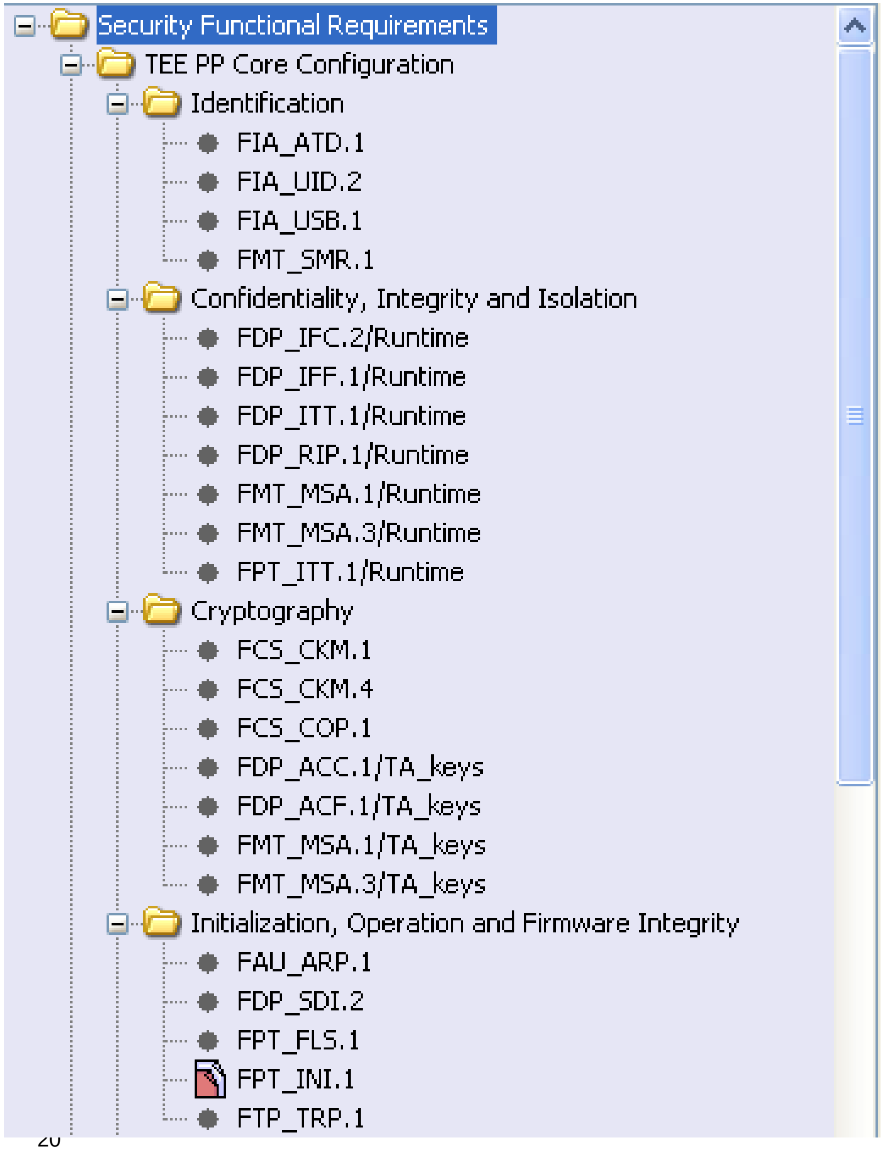
Security Objectives



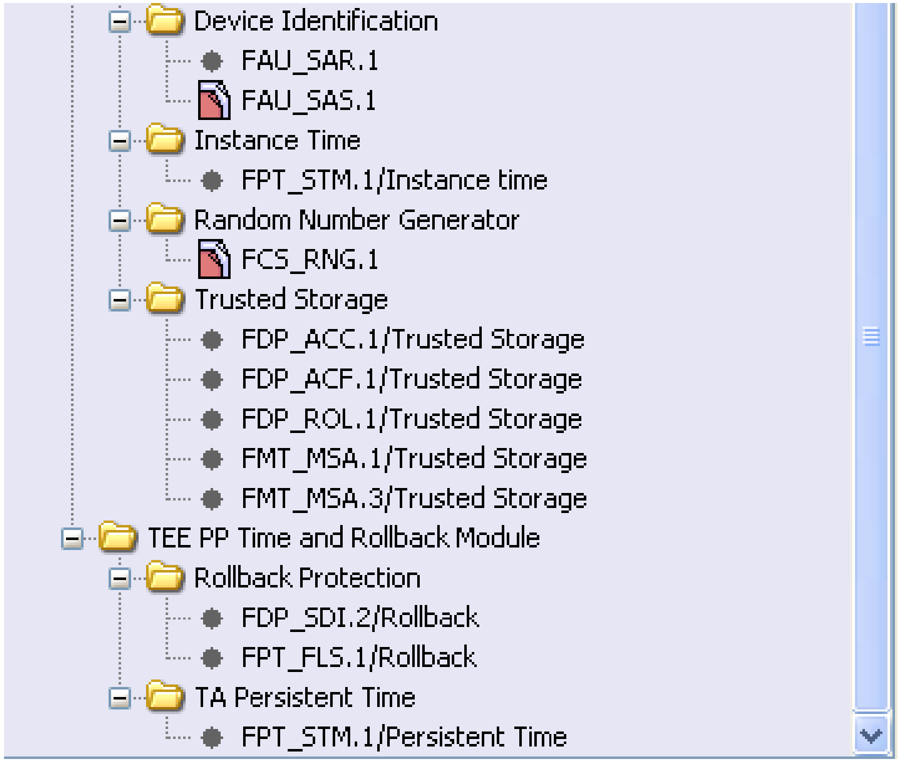
- Security Objectives for the TOE
  - TEE PP Core Configuration
    - O.CA_TA_IDENTIFICATION
    - O.CRYPTOGRAPHY
    - O.DEVICE_ID
    - O.INITIALIZATION
    - O.INSTANCE_TIME
    - O.OPERATION
    - O.RNG
    - O.RUNTIME_CONFIDENTIALITY
    - O.RUNTIME_INTEGRITY
    - O.TA_ISOLATION
    - O.TEE_DATA_PROTECTION
    - O.TEE_FIRMWARE_UPGRADE
    - O.TEE_ISOLATION
    - O.TRUSTED_STORAGE
  - TEE PP Time and Rollback Module
    - O.ROLLBACK_PROTECTION
    - O.TA_PERSISTENT_TIME

- Security Objectives for the Operational Environment
  - TEE PP Core Configuration
    - OE.DEBUG
    - OE.INTEGRATION_CONFIGURATION
    - OE.MANAGEMENT
    - OE.PROTECTION_AFTER_DELIVERY
    - OE.ROLLBACK
    - OE.SECRETS
    - OE.TA_DEVELOPMENT
    - OE.TEE_FIRMWARE_UPGRADE
    - OE.UNIQUE_DEVICE_ID
  - TEE PP Time and Rollback Module

Security Functional Requirements Overview



- Security Functional Requirements
  - TEE PP Core Configuration
    - Identification
      - FIA_ATD.1
      - FIA_UID.2
      - FIA_USB.1
      - FMT_SMR.1
    - Confidentiality, Integrity and Isolation
      - FDP_IFC.2/Runtime
      - FDP_IFF.1/Runtime
      - FDP_ITT.1/Runtime
      - FDP_RIP.1/Runtime
      - FMT_MSA.1/Runtime
      - FMT_MSA.3/Runtime
      - FPT_ITT.1/Runtime
    - Cryptography
      - FCS_CKM.1
      - FCS_CKM.4
      - FCS_COP.1
      - FDP_ACC.1/TA_keys
      - FDP_ACF.1/TA_keys
      - FMT_MSA.1/TA_keys
      - FMT_MSA.3/TA_keys
    - Initialization, Operation and Firmware Integrity
      - FAU_ARP.1
      - FDP_SDI.2
      - FPT_FLS.1
      - FPT_INI.1
      - FTP_TRP.1



- Device Identification
  - FAU_SAR.1
  - FAU_SAS.1
- Instance Time
  - FPT_STM.1/Instance time
- Random Number Generator
  - FCS_RNG.1
- Trusted Storage
  - FDP_ACC.1/Trusted Storage
  - FDP_ACF.1/Trusted Storage
  - FDP_ROL.1/Trusted Storage
  - FMT_MSA.1/Trusted Storage
  - FMT_MSA.3/Trusted Storage
- TEE PP Time and Rollback Module
  - Rollback Protection
    - FDP_SDI.2/Rollback
    - FPT_FLS.1/Rollback
  - TA Persistent Time
    - FPT_STM.1/Persistent Time

TEE EAL

- EAL2+ where AVA_VAN.2 is refined with **enhanced-basic attack potential:** same attack potential as EAL4, i.e. attacks ranging up to 20 pts. are countered
- EAL2 chosen because of the complexity of higher EAL rules when applied to application processor design
- AVA_VAN.3 not included because access to the full implementation might be difficult (dependency on ADV_IMP.1).

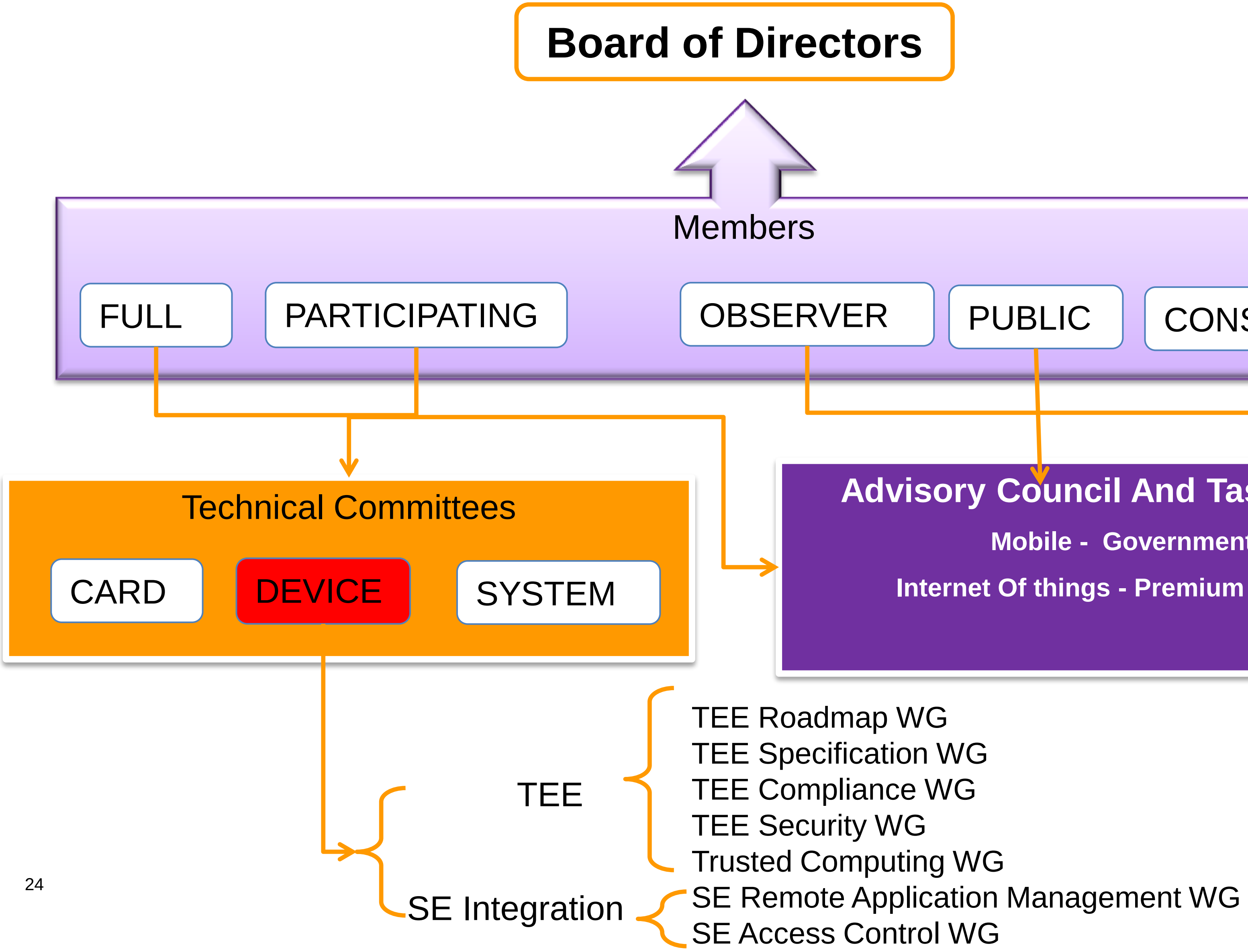
Range of values*	TOE resistant to attackers with attack potential of
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Future Work

- Extend the TEE platform certification to:
  - Trusted user interface (TUI)
  - Remote administration
  - Content protection
- Device certification
- TAs certification

Technical Communities (TCs)

GlobalPlatform and its Device Committee



Board of Directors

Members

FULL

PARTICIPATING

OBSERVER

PUBLIC

CONSULTANT

Technical Committees

CARD

DEVICE

SYSTEM

Advisory Council And Task Forces

Mobile - Government

Internet Of things - Premium Content

TEE

- TEE Roadmap WG
- TEE Specification WG
- TEE Compliance WG
- TEE Security WG
- Trusted Computing WG

SE Integration

- SE Remote Application Management WG
- SE Access Control WG

GlobalPlatform Members

AMD · AMERICAN EXPRESS · ARM · athena Smartcard · at&t · BlackBerry · BROADCOM

COMPRION · Clear2Pay · ERICSSON · FeliCa Networks · FIME · Galitt

gemalto security to be free · Giesecke & Devrient · Good · HID · infineon · inside SECURE · MasterCard Worldwide

NAGRA KUDELSKI · NTT · NVIDIA · NXP founded by Philips · OBERTHUR TECHNOLOGIES · ORACLE · orange

QUALCOMM · RENESAS Everywhere you imagine. · ROGERS · SAFRAN Morpho · SAMSUNG · SOLACIA

Sprint · ST · Trusted Labs · TRUSTONIC · UL · verizon wireless · VISA

Applus · BARNES INTERNATIONAL · DNP · FINGERPRINTS · LG · TÜV SÜD Japan · iCTK

secunet IT security beyond expectations · SK C&C · TELUS · TEXAS INSTRUMENTS · TOSHIBA · VALID

ABnote · aconite · BARCLAYS · BellID · i-FREE · CB · CESG · consult hyperion securing tomorrow's transactions · UnionPay 银联 中国银联 China UnionPay · CROCUS Technology Blossoming future · CRYPTOMATHIC www.cryptomathic.com · Datang Microelectronics

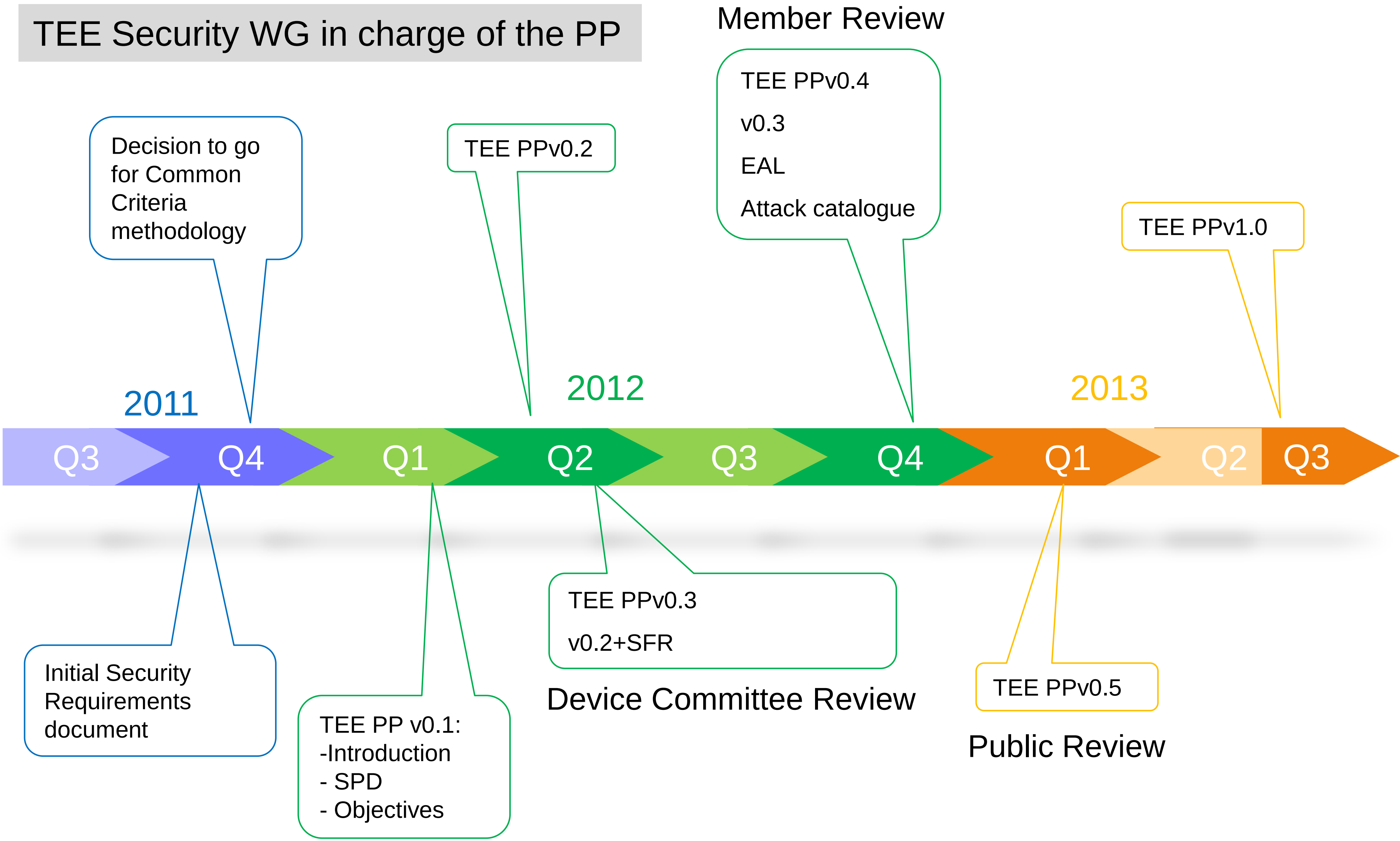
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA · DatacardGroup · DISCOVER · Discretix trust • embedded · DYNAMICS · 东信和平 EASTCOMPEACE · Elliptic · EQUENS · FEITIAN WE BUILD SECURITY · 財金資訊股份有限公司 FINANCIAL INFORMATION SERVICE CO., LTD. · 恒宝股份 HENGBAO CO., LTD. · HITACHI Inspire the Next

HUAWEI · intercede · irdeto · ISIS · JCB Good times start here. · kona i · LG CNS · MARVELL · monetech · NEC · NEXTENDIS · Plastic Card

Posteitaliane · Proxama · Real Casa de la Moneda Fábrica Nacional de Moneda y Timbre · Redsýs · SafePay systems · SAMSUNG · SAMSUNG SDS · sequent · 上海柯斯 SHANGHAI COS · 上海华虹集成电路有限责任公司 Shanghai Huahong Integrated Circuit Co.,Ltd · 上海复旦微电子集团股份有限公司 Shanghai Fudan Microelectronics Group Company Limited

Secure Platforms Technology SP-Tek · THALES · THATER & SCHWIER CONSULTING · TIANYU · TOPPAN · TOPPAN FORMS · UBIVELOX · validity · Vellhi · Watchdata · wave · XROMB

The Roadmap of the GlobalPlatform TC for TEE PP



TEE Security WG in charge of the PP

Initial Security Requirements document

Decision to go for Common Criteria methodology

TEE PP v0.1:
-Introduction
- SPD
- Objectives

TEE PPv0.2

TEE PPv0.3

v0.2+SFR

Device Committee Review

Member Review

TEE PPv0.4

v0.3

EAL

Attack catalogue

TEE PPv0.5

Public Review

TEE PPv1.0

International TC

- GlobalPlatform has started discussions with the industry to create a Common Criteria International Technical Community with the aim of simplifying the deployment of TAs.

- Why?
  - To avoid de-fragmentation: one TEE evaluation methodology
  - To promote the largest mutual recognition
  - To benefit from the largest expertise

- How?
  - Prepare a proposal for the Common Criteria Management Board
  - Invite CC certification schemes to join GlobalPlatform initiatives

Thank you