

TEE技术与认证

A horizontal band featuring a microscopic view of a circuit board, showing two prominent, reflective spherical components.

泰尔终端实验室
国炜



1. TEE架构

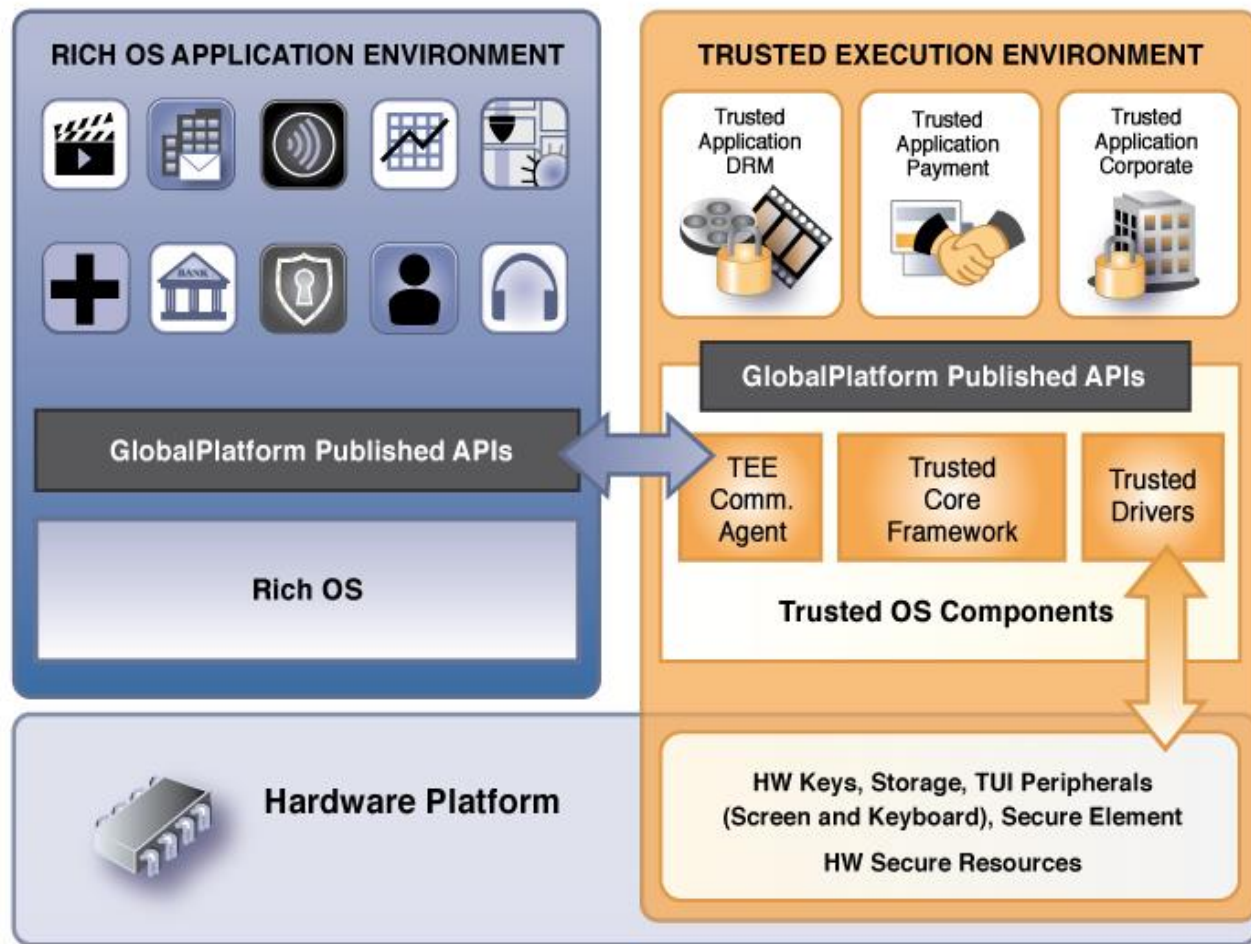
2. TEE的发展

3. GP TEE与国内标准进展

4. GP TEE认证

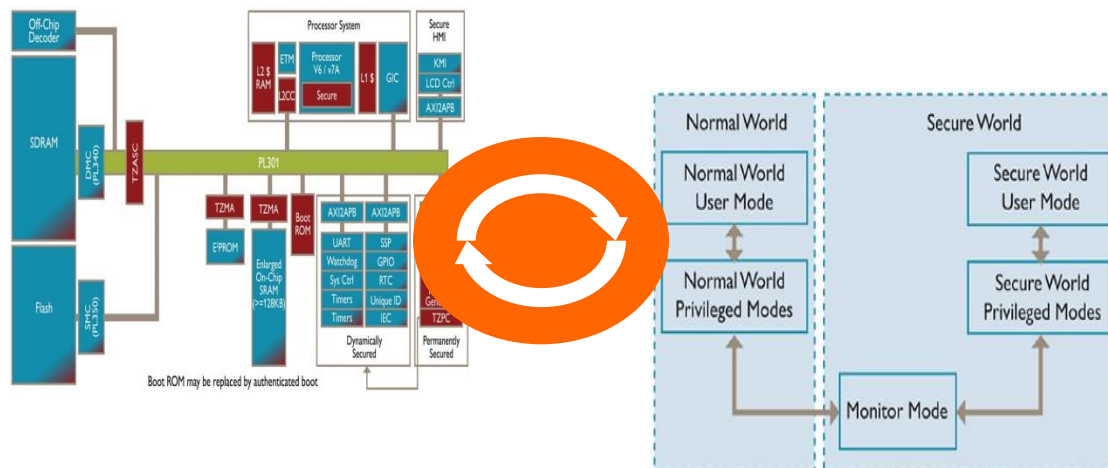


TEE架构



- ◆ TEE是与设备上的Rich OS（通常是Android等）并存的运行环境，且给Rich OS提供安全服务。
- ◆ TEE有其自身的执行空间，比Rich OS的安全级别更高，但是比起安全元素（SE，通常是智能卡）的安全性要低一些。
- ◆ TEE所能访问的软硬件资源是与Rich OS分离。

TEE的发展



- TEE的概念是基于ARM的TrustZone技术。
- TrustZone架构是ARM系统化设计，在处理器核和调试功能等方面都有充分的功能性和安全性考虑。



1. ARM develop Trustzone
2. TI OMAP m-shield hardware



BB5 security solution from NOKIA Symbian OS, TEE prototype



Advanced Trusted Environment OMTP



1. GP Device Committee
2. GP TEE Specification
3. GP TEE Compliance Program
4. GP TEE Security Certification



Development of TEE





GlobalPlatform介绍

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



TRUSTED EXECUTION
ENVIRONMENT



MESSAGING



SECURE ELEMENT

Across several market sectors and in converging sectors



PREMIUM
CONTENT



FINANCIAL



TELECOM



GOVERNMENT



AUTOMOTIVE



HEALTHCARE



RETAIL



TRANSIT

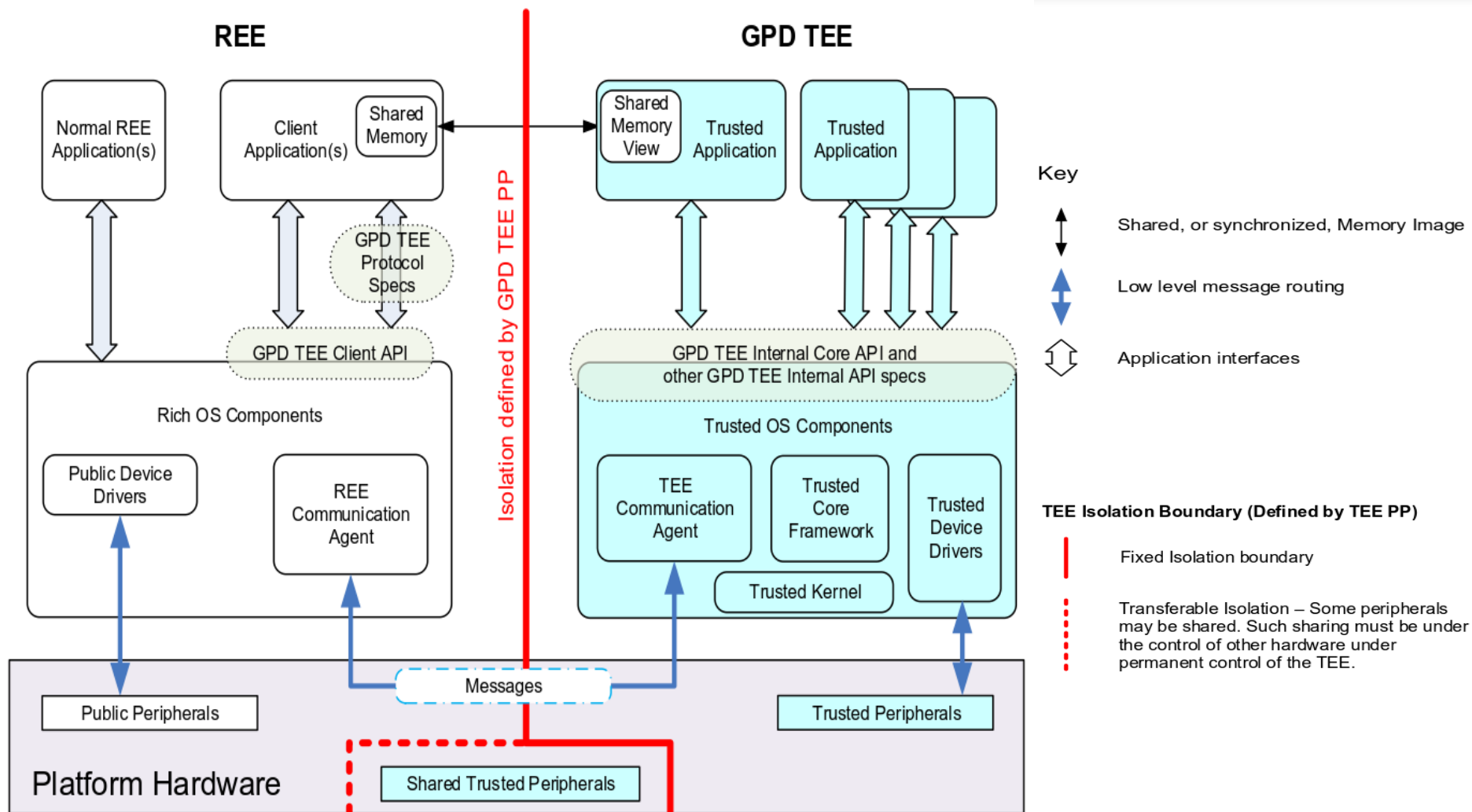


GlobalPlatform会员





GP TEE软件架构



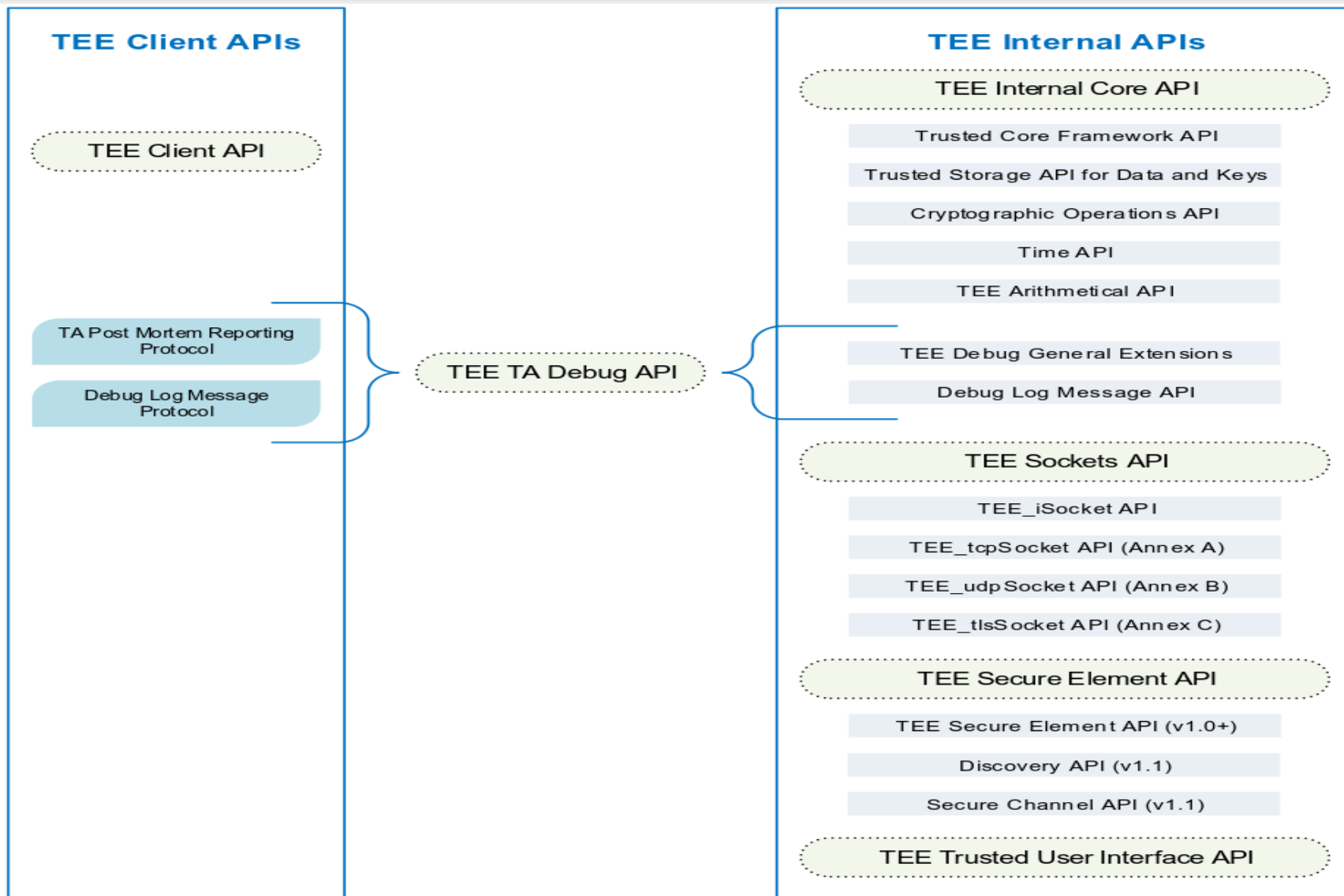


- 架构
 - TEE System Architecture v1.0
- TEE接入
 - TEE Client API Specification v1.0
- TA访问TEE功能API
 - TEE Internal Core API Specification v1.1
 - TEE Secure Element API Specification v1.1
 - Trusted User Interface API Specification v1.0
 - TEE TA Debug Specification v1.0
- 安全要求
 - TEE Protection Profile v1.2
- 认证
 - TEE Initial Configuration Test Suite v1.1.0
 - TEE Security Test Suite v1.0





GP TEE APIs 关系





GP TEE Client API

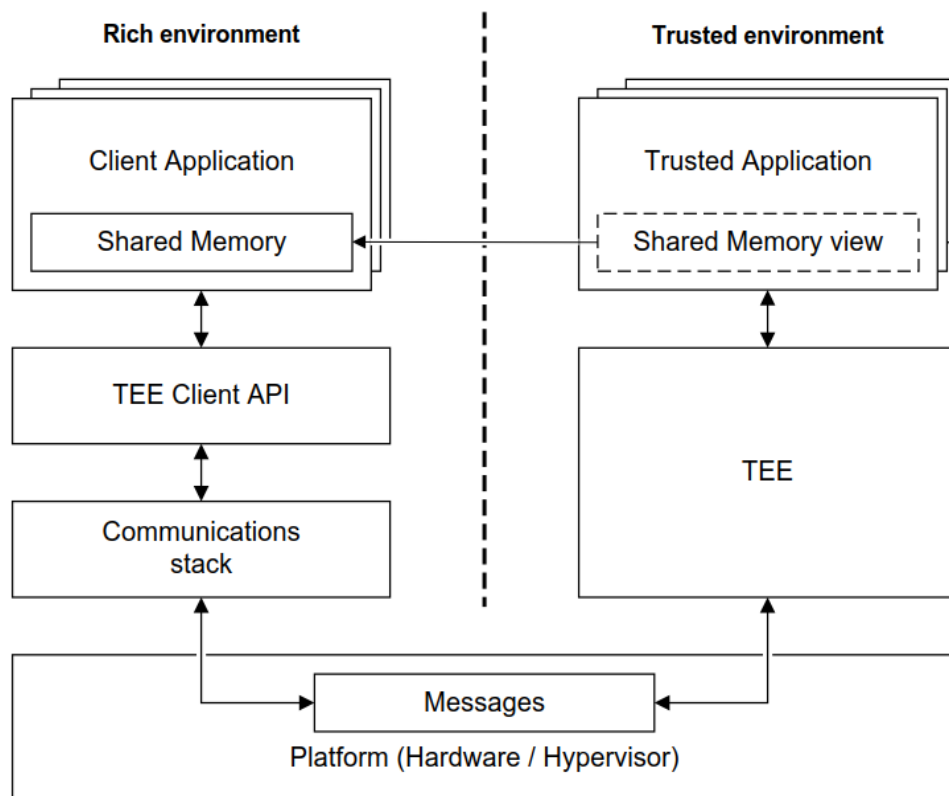


Figure 2-1: TEE Client API System Architecture

- 为客户端应用和可信应用提供通信功能。
- 与可信应用建立一个会话。
- 建立一个共享内存。
- 发送可信应用特有的命令激活TEE内的可信服务
- 关闭REE与TEE的通信。



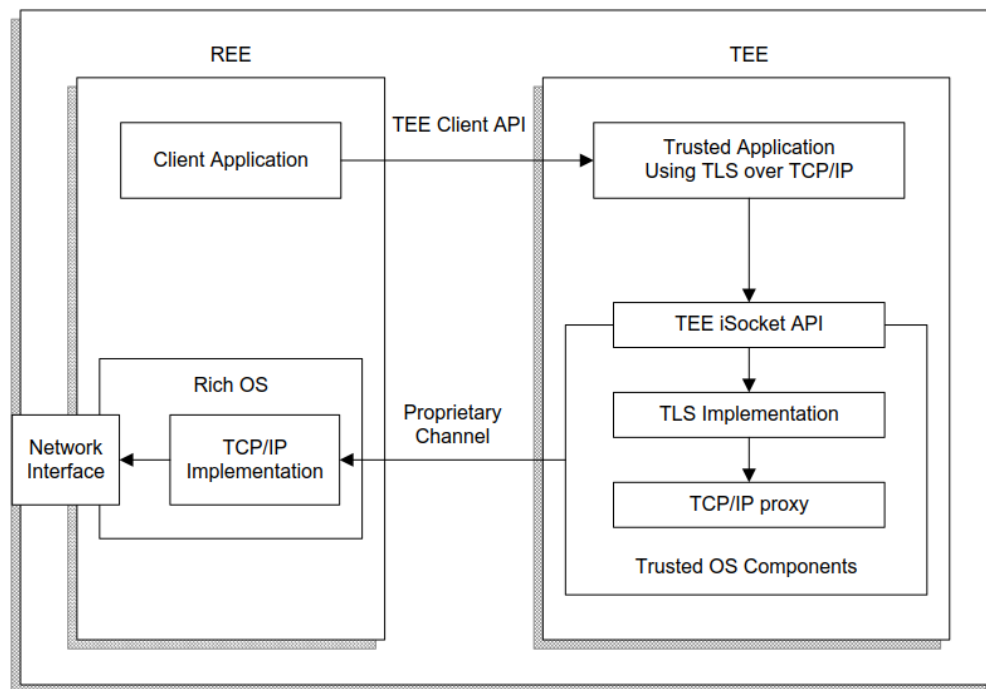
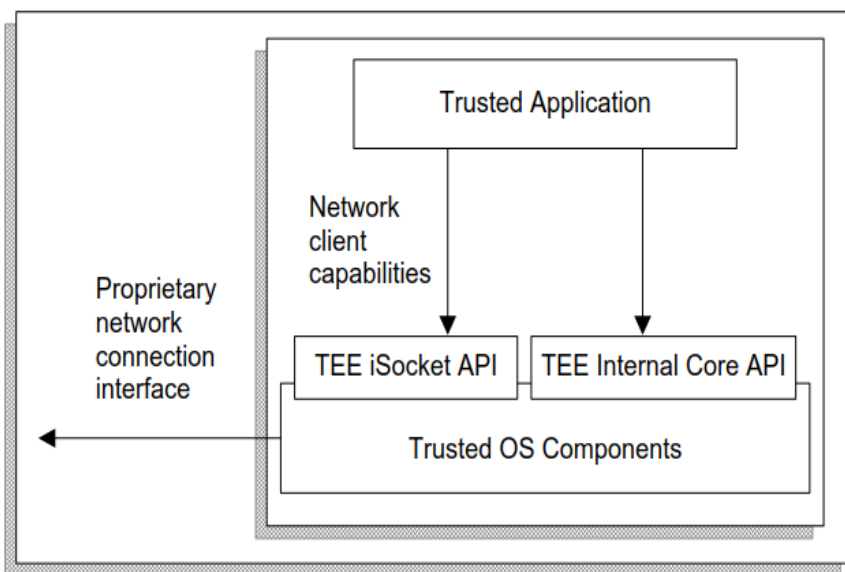
GP TEE Internal API

- 为可信应用提供可调用TEE能力的接口。
- TEE Internal Core API提供以下API接口能力子集：
 - ✓ Trusted Core Framework API: 提供调度、通信、存储管理和系统消息提取等功能接口；
 - ✓ Trusted Storage API: 为密钥和通用数据的安全存储提供功能接口；
 - ✓ Cryptographic API: 提供加密能力；
 - ✓ Time API: 为各种基于时间功能的任务（如DRM）提供支持；
 - ✓ TEE Arithmetical API: 为Cryptographic API所不包含的加密功能的产生提供原始的运算接口。



GP TEE Socket API

- 为TA与网络其它节点通信提供一个通用的类接口。
- 使TA具有网络客户端能力。
- 为降低系统的复杂性，将安全协议与纯粹的传输协议分离。



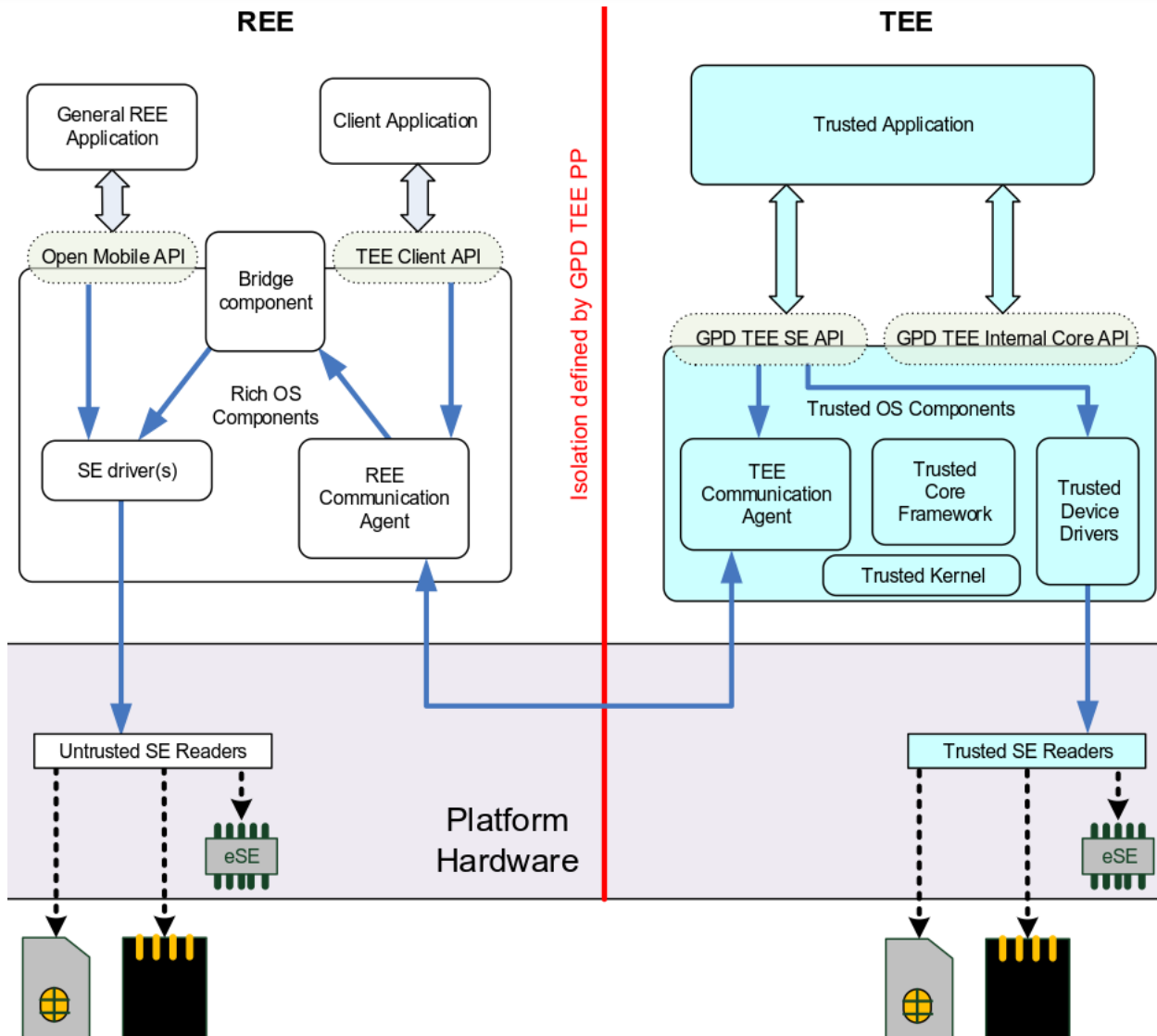


GP TEE TA Debug API

- 为支持TA开发以及TEE Internal API一致性测试提供接口。
- 事后报告（Post Mortem Reporting）为TEE提供向客户端报告TA的最终状态。
- 调试日志消息（Debug Log Message）服务为TA提供报告简单的调试信息。



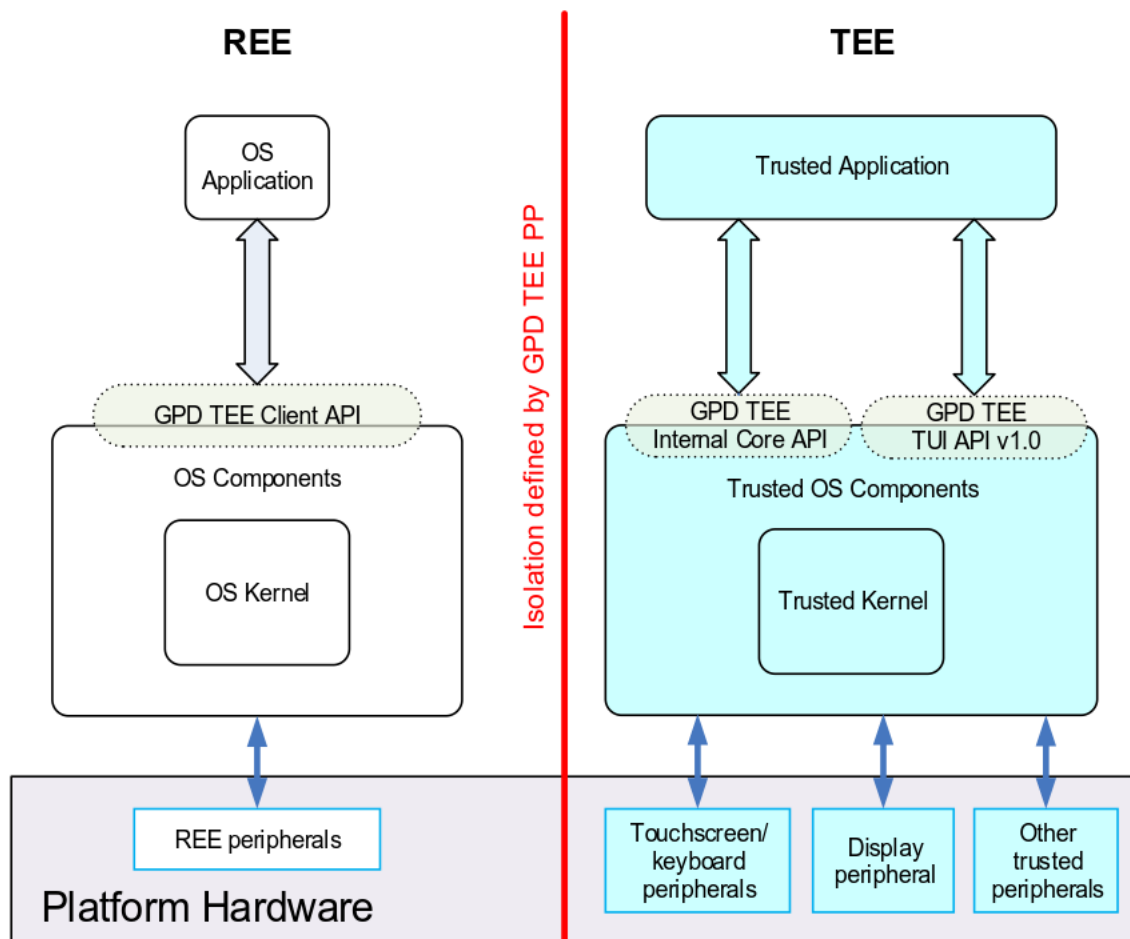
GP TEE SE API



- TA可不通过REE与SE相互通信。
- TA需要通过REE与SE相互通信。这种场景下，建议使用安全通道来防止REE的攻击。



GP TEE Trusted User Interface API



- 安全显示：显示给用户的信息不能够被REE中的软件或者非授权的TA接入、修改、提取。
- 安全输入：用户输入的信息不能够被REE中的软件或者非授权的TA导出和修改。
- 安全指示：向用户指示当前显示屏的安全状态。



中国通信标准化协会

China Communications Standards Association

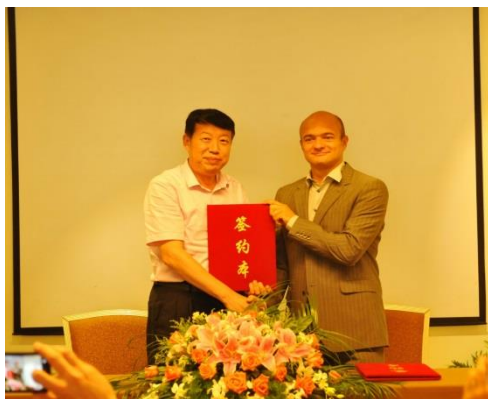
Trusted Execution Environment (TEE) 标准:

- YD/T 2844.1-2015 移动终端可信环境技术要求 第1部分: 总体
- YD/T 2844.2-2015 移动终端可信环境技术要求 第2部分: 可信执行环境
- YD/T 2844.3-2015 移动终端可信环境技术要求 第3部分: 安全存储
- YD/T 2844.4-2015 移动终端可信环境技术要求 第4部分: 操作系统的安全保护
- YD/T 2844.5-2016 移动终端可信环境技术要求 第5部分: 与输入输出设备的安全交互
- YD/T 2844.6-2016 移动终端可信环境技术要求 第6部分: 与SE的安全交互



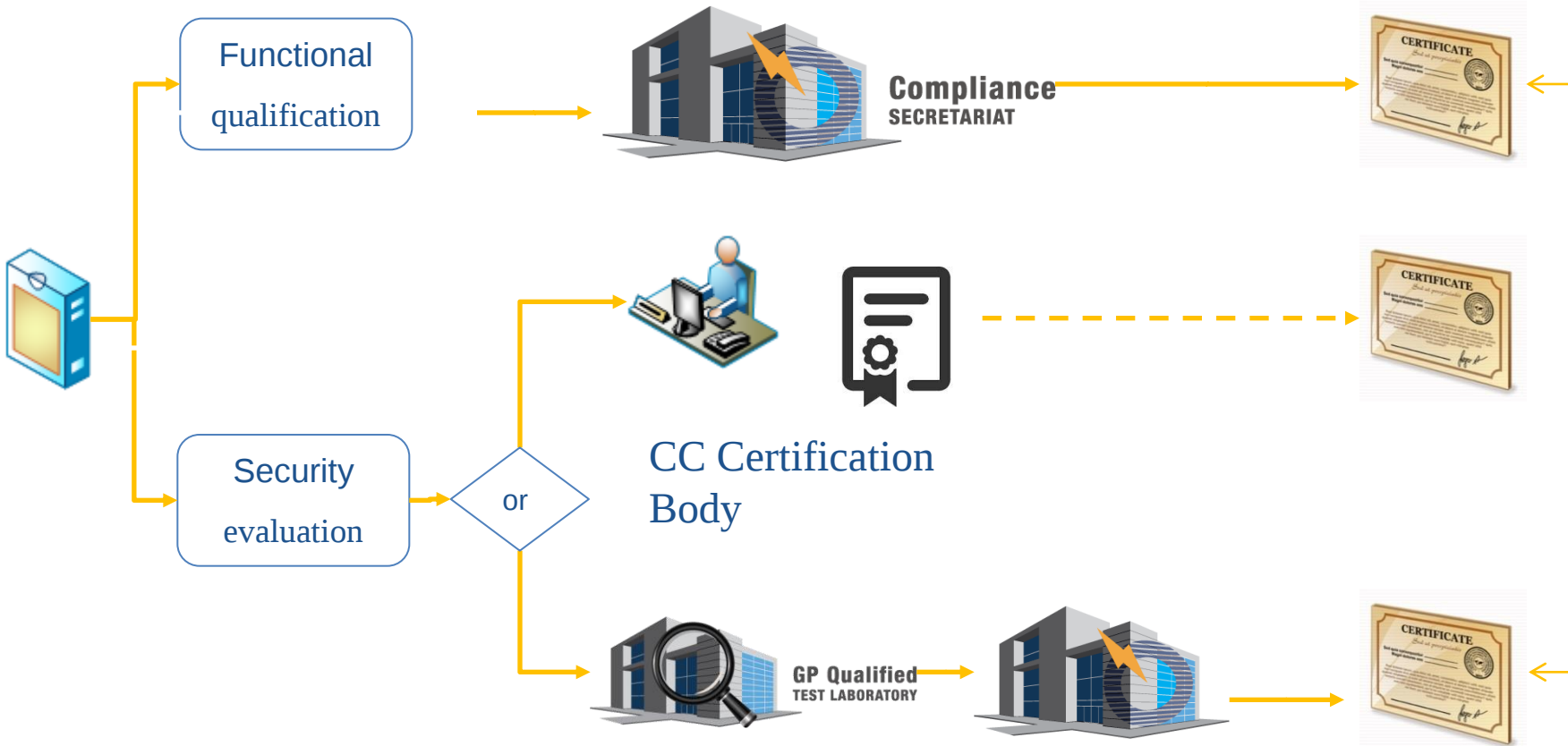
Trusted Execution Environment (TEE) 标准:

- TAF-WG4-AS0003-V1.0.0 基于UICC的TEE初始化技术要求
- TAF-WG4-AS0005-V1.0.0 TEE Client API技术要求 (Java版)
- TAF-WG4-AS0006-V1.0.0 TEE Internal API技术要求 (Java版)
- TAF-WG4-AS0007-V1.0.0 Trust UI API技术要求 (Java版)
- TAF-WG4-AS0001-V1.0.0 基于TEE的指纹识别技术要求
- TAF-WG4-AS0002-V1.0.0 基于TEE的指纹识别测试方法





GP TEE 认证



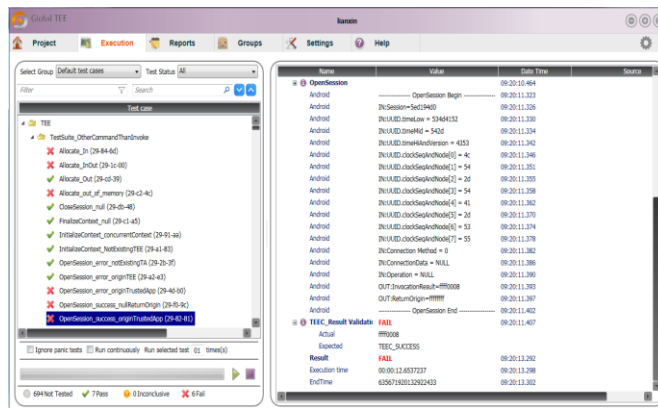


The image shows the front cover of a technical specification document. At the top, the 'GLOBALPLATFORM' logo is centered in a bold, sans-serif font. Below the logo is a horizontal line. Underneath the line, the title 'GlobalPlatform Trusted Technology' is written in a smaller font, followed by 'TEE Client API Specification' in a larger, bold font. Below the title, the version 'Version 1.0' is indicated. Further down, the text 'Public Release' is followed by the date 'July 2010' and the document reference 'Document Reference: TEE_CAPI_001'. At the bottom of the cover, there is a decorative graphic consisting of a blue and green globe-like shape on the left, transitioning into a horizontal band of green and blue wavy lines.

- ## 授权实验室

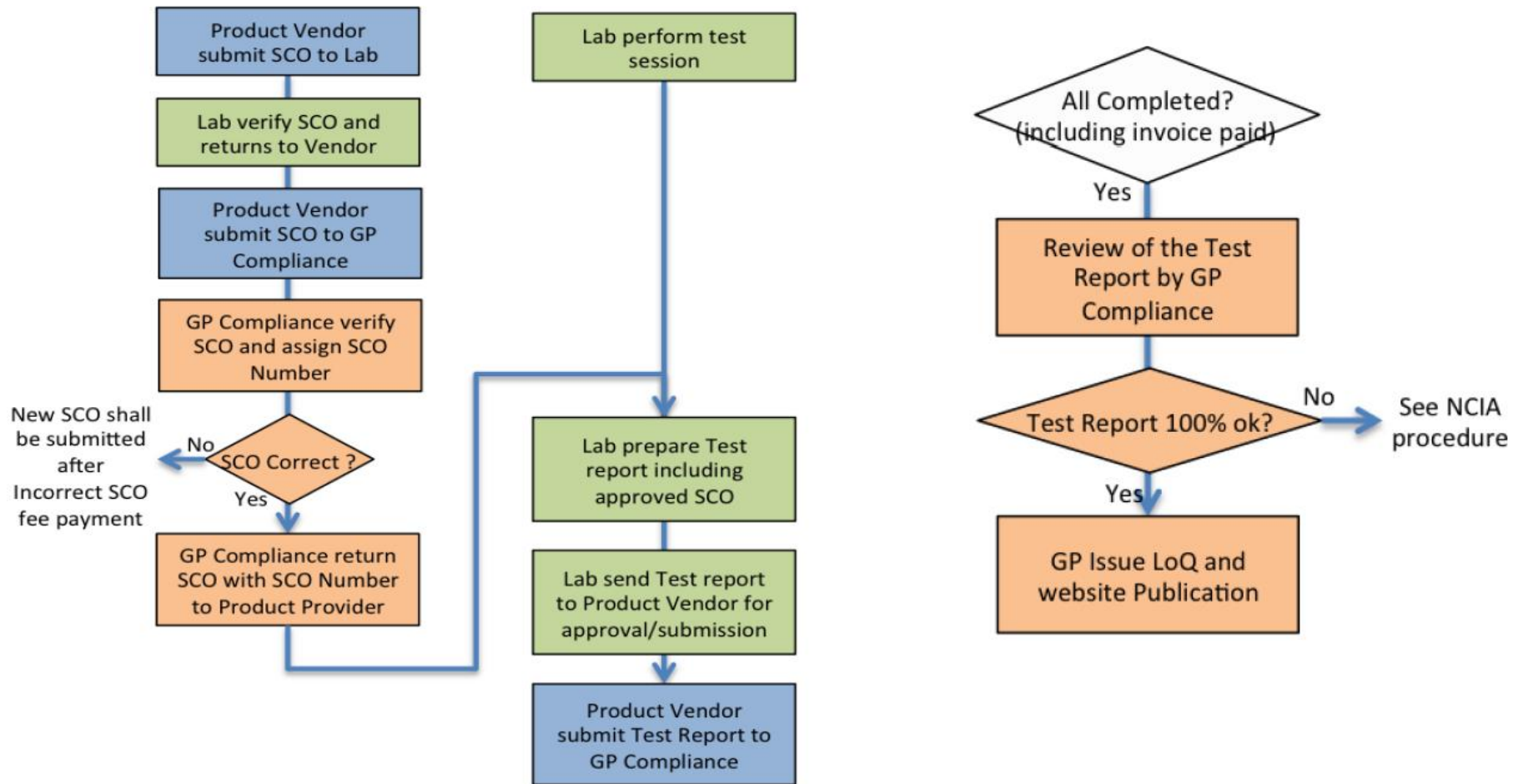


- ❑ Adaptation Layer for GP TEE Internal API v1.1.0
- ❑ TEE Client API (38 NB)
- ❑ Crypto (242 NB)
- ❑ Data Storage (187 NB)
- ❑ Time Arithmetical (174 NB)
- ❑ TEE Trusted Core Framework (66NB)
- ❑ TTAs
- ❑ All features are mandatory





GP TEE 一致性认证流程



SCO: Supported Configuration Options

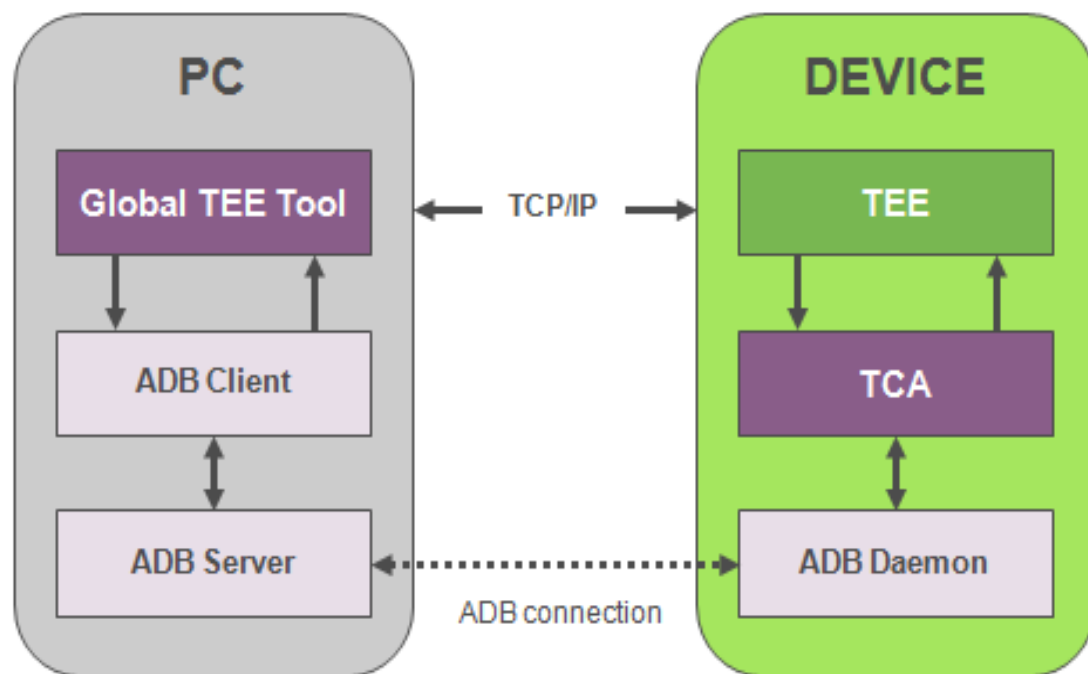
LoQ: Letter of Qualification

CAR: Compliance Assessment Report

NCIA: Non Conformance Investigation Assessment



GP TEE 一致性测试



– 测试覆盖:

- ✓ 客户端API
- ✓ TEE内部API
- ✓ 可信框架
- ✓ 时间和算术
- ✓ 数据存储
- ✓ 加密

– 由于测试软件和TEE厂家对数据结构定义的差异性，在测试过程中可能会产生崩库，因此需要使用TEE厂家自己的tee_client_api.h文件以及libtee.so文件重新编译生成APK。



GP TEE 安全认证架构

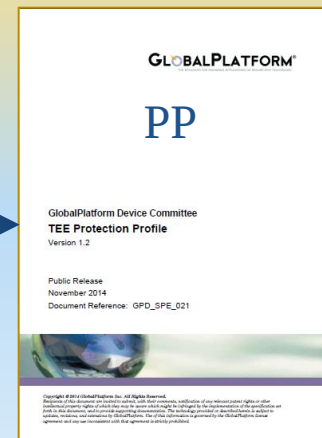
TEE Attack WG

TEE Security WG

TEE Lab WG

Security Evaluation Secretariat

Attack
list



Methodology

GlobalPlatform Device Committee
TEE Protection Profile
Version 1.2

Public Release
November 2014
Document Reference: GPD_SPE_021

test
list

Security
target

Process

GlobalPlatform Device Committee
TEE Protection Profile
Version 1.2

Public Release
November 2014
Document Reference: GPD_SPE_021

Lab &
Product
vendor
Contracts

Board

Board

Board



GP TEE PP接受官方认证

Media & Resource Center > Press Releases

- > Press Releases
- > Industry Events
- > FAQs
- > White Papers & Guides
- > Audio / Video
- > Newsletters
- > Industry Interviews
- > Executive Profiles

The GlobalPlatform Trusted Execution Environment Protection Profile is Officially Certified Against Common Criteria

Product vendors are now able to undertake formal security evaluations for TEE products

4 February 2015 – The Common Criteria portal has officially listed the GlobalPlatform Trusted Execution Environment (TEE) Protection Profile (PP) on its [website](#), under the Trusted Computing category. This important milestone means that industries using TEE technology to deliver services such as premium content and mobile wallets, or enterprises and governments establishing secure mobility solutions, can now formally request that TEE products are certified against this security framework.

GlobalPlatform presented its TEE Protection Profile to Common Criteria for certification via [Agence Nationale de la Sécurité des Systèmes d'Information \(ANSSI\)](#).

The GlobalPlatform TEE PP specifies the typical threats the hardware and software of the TEE – a secure area that resides in the main processor of a mobile device and ensures that sensitive data is stored, processed and protected in a secure environment – needs to withstand. It also details the security objectives that are to be met in order to counter these threats and the security functional requirements that a TEE will have to comply with. A security assurance level of EAL2+ has been selected; the focus is on vulnerabilities that are subject to widespread, software-based exploitation.

Vincent Strubel, spokesperson from ANSSI, comments: "It is important to remember that organizations expect all the services that they wish to deploy, especially those offering mobility of users and their access to sensitive information, to operate in a secure way. The TEE – regardless of manufacturer – must meet the requirements of a range of service

If you are a media representative, analyst or conference organizer and have a query regarding GlobalPlatform, please contact [iseepr](#).

Tel: +44 (0) 1943 468007
[Email iseepr](#)



GP TEE安全认证机制

The screenshot shows the GlobalPlatform website's TEE Certification Scheme page. The header includes the GlobalPlatform logo and navigation links: Home, Member Login, Become a Member, Store, Search, and Contact Us. Below the header are social media icons for Twitter, LinkedIn, and YouTube. A secondary navigation bar lists: specifications, compliance, certification, membership, about us, markets, media & resource center, and training. The main content area features a large heading 'TEE Certification Scheme' and a grid of images showing a hand holding a blue card, a mobile phone, and server racks. A sidebar on the left contains a list of links: Evaluated Products, Accredited Laboratory Services, How to Participate, and Industry Benefits of the Scheme. The main text area has a sub-heading 'TEE Certification Scheme' followed by two paragraphs of text.

GLOBALPLATFORM®

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

specifications compliance certification membership about us markets media & resource center training

TEE Certification Scheme

TEE Certification Scheme

- > Evaluated Products
- > Accredited Laboratory Services
- > How to Participate
- > Industry Benefits of the Scheme

TEE Certification Scheme

GlobalPlatform is committed to ensuring a standardized level of security for e has developed an open and thoroughly evaluated trusted execution environ evaluated products.

The GlobalPlatform TEE Certification Scheme, managed by its TEE Security conformance of their TEE products to the organization's [TEE Protection Profile](#)

Website live!

Press release

GlobalPlatform Launches TEE Security Evaluation Secretariat to Accelerate Deployment of Certified Trusted Execution Environment Products

Products will be evaluated for conformance to the TEE Protection Profile through GlobalPlatform's TEE Certification Scheme

23 June 2015 – In a move that will accelerate the deployment of certified Trusted Execution Environment (TEE)* products and promote a globally interoperable mobile ecosystem, GlobalPlatform has announced that it is launching a TEE Security Evaluation Secretariat to manage its TEE Certification Scheme. Under the scheme, providers of TEE products will be able to submit their products to the new GlobalPlatform secretariat for independent evaluation of their conformance to the organization's TEE Protection Profile.

The TEE Protection Profile, which has been certified against Common Criteria under its Trusted Computing category, specifies the typical threats the hardware and software of the TEE needs to withstand. It also details the security objectives that are to be met in order to counter these threats and the security functional requirements that a TEE will have to comply with. A positive evaluation of conformance to this security framework, through GlobalPlatform's Certification Scheme, will indicate that a TEE product meets an international security baseline. The scheme will enable service providers to confidently and effectively manage risk, by ensuring that there is a consistent level of security across connected devices.

Thank You!

国 炜
guowei1@caict.ac.cn