Computer System Security **CS3312**

# 计算机系统安全

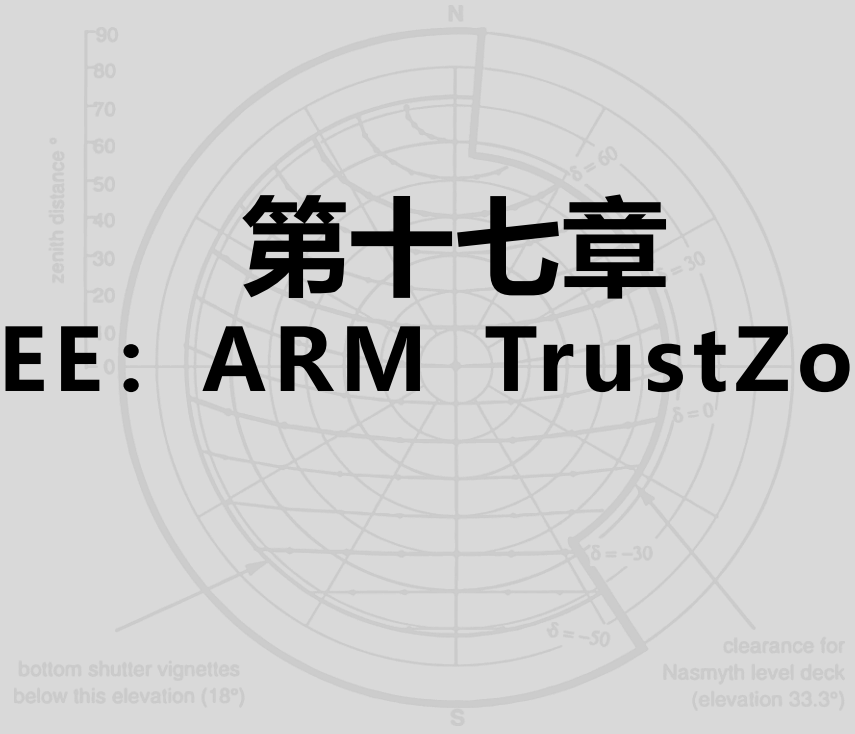
2024年 春季学期

主讲教师：张媛媛 副教授

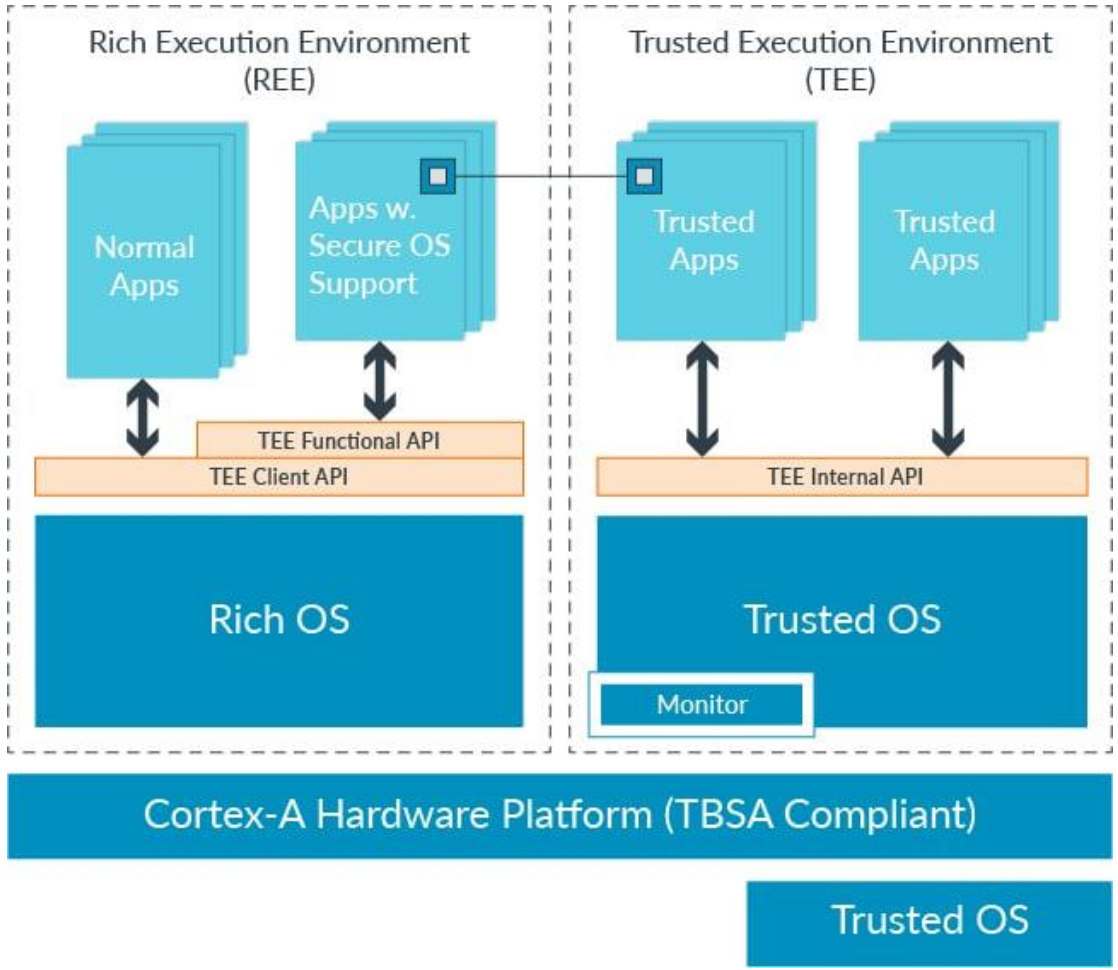
上海交通大学 计算机科学与技术系

# 第十七章

# TEE：ARM TrustZone



# OS隔离TEE的系统架构



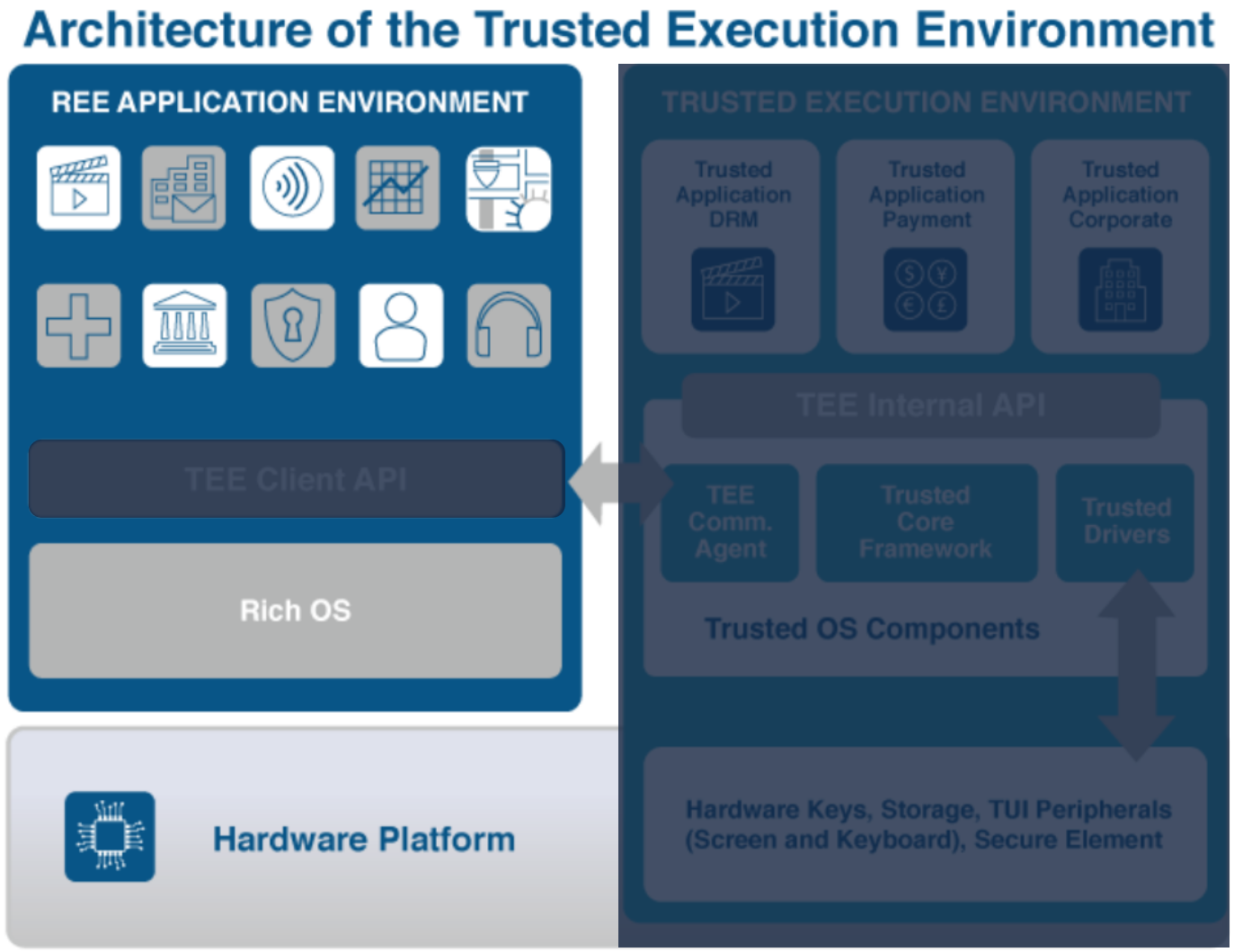

**The Rich OS** is an environment created for versatility and richness where device applications are executed.
It is open to third party download after the device is manufactured. Security is a concern here but is secondary to other issues. (aka, **REE**, **Normal World**, **NWd**)

**The Trusted OS** is an isolated environment that runs in parallel with the rich OS. (aka, **TEE**, **Secure World**, **SWd**)

The Trusted App

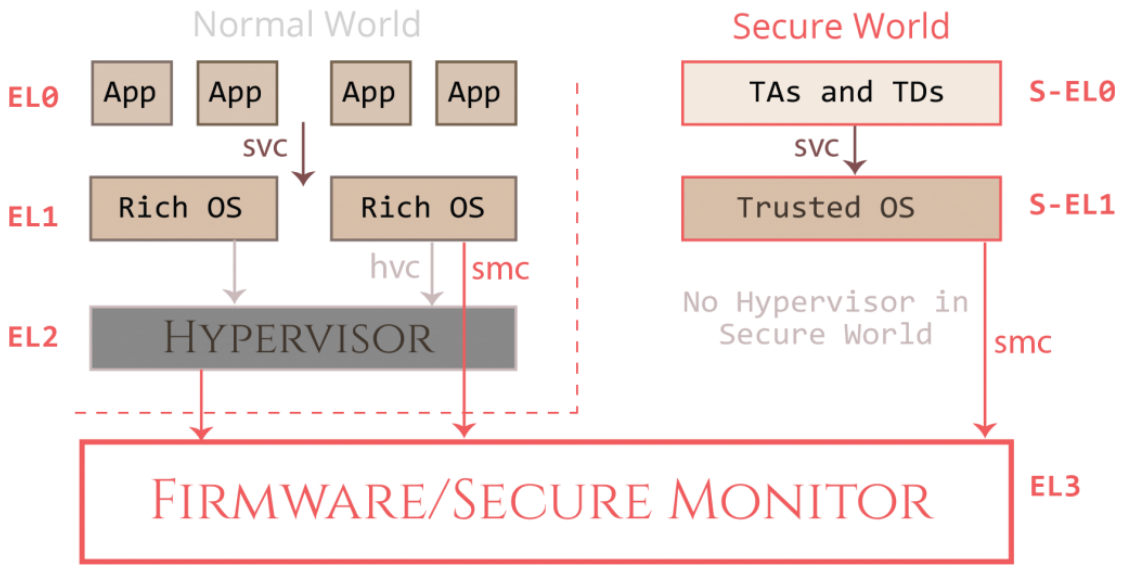
https://www.arm.com/ja/technologies/trustzone-for-cortex-a/tee-and-smc

# 一个典型的可信应用Trusted 的运行过程



# TEE中CPU的三种状态

- 用户模式：
  - 表明CPU当前正在执行普通的用户进程，特权级别最低
- 内核模式：
  - CPU正在执行操作系统的代码，特权级别较高，可访问低特权级别的代码和数据
- TEE 状态：
  - TrustZone 通过引入 CPU 可以运行的新“安全”模式来工作。在这种新模式下运行时，CPU 可以访问设备的所有硬件和内存。在非 TrustZone（“正常”）模式下运行时，只能访问一部分外围设备和特定范围的物理内存。 TEE 可以利用这项技术将自己的代码和数据放入这个“安全内存”中，从而防止任何在“正常模式”下运行的代码访问或修改它，即使该代码正在内核中运行。虽然内核无法访问 TEE 内存，但在 TEE 中运行的代码可以读取、修改和选择处理正常世界中的数据。




思考&讨论：信任根是什么？

# TEE 硬件架构 设计思路

**SCR寄存器**

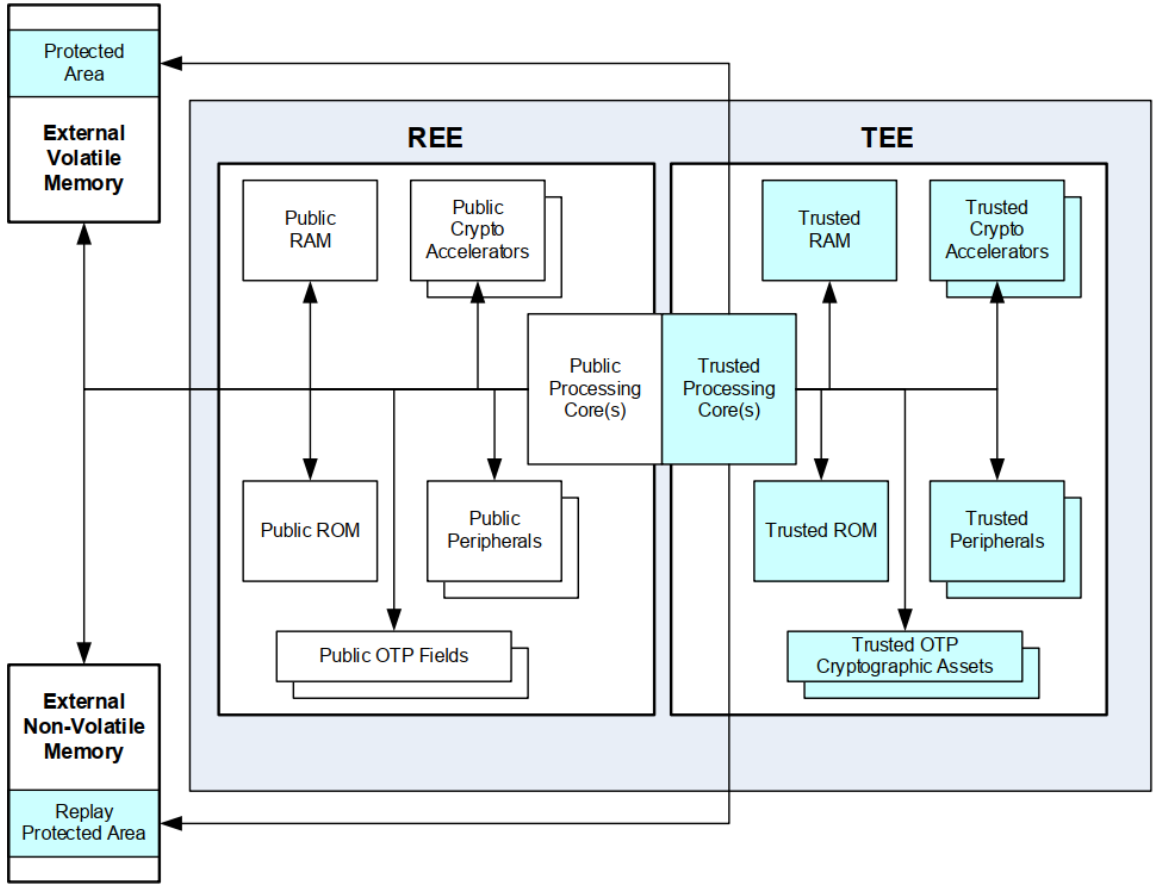
在硬件层面，CPU 通过 CP15（协处理器）中的安全配置寄存器 (SCR) 的 NS 位来确定它是在 SWd 还是 NWd 中运行。如果该位使能，则 CPU 在 NWd 中运行；否则它在 SWd 中运行。安全监视器确保该位不能被非安全程序写入，以保持 SWd 的完整性。

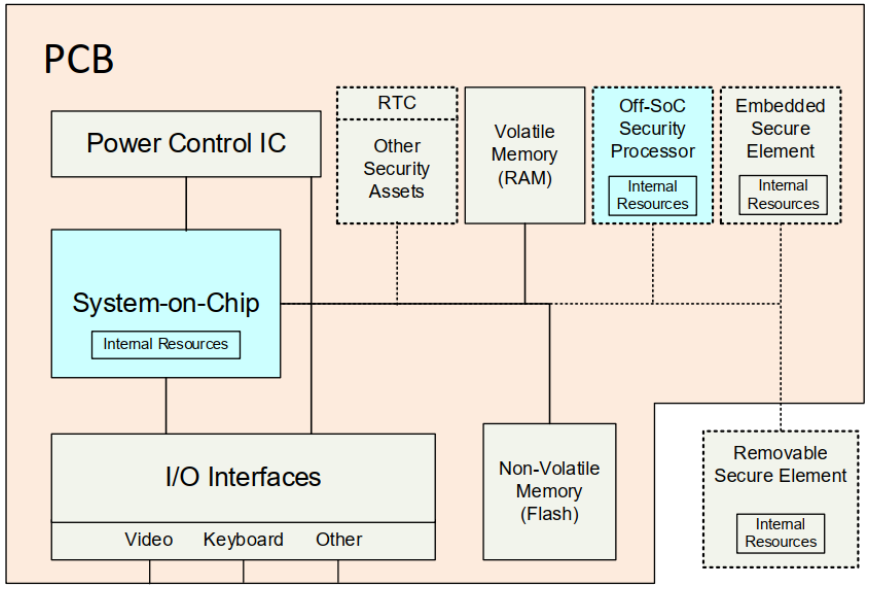
**通过系统总线保护外设访问**

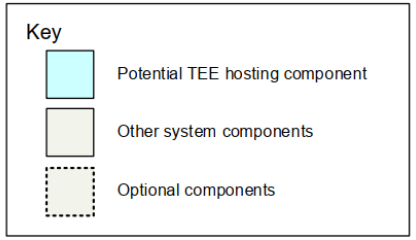
CPU 还可以将内存页面标记为受 TrustZone 保护（“安全”）或属于NWd（“非安全”）。页表条目 (PTE) 的 NS 位（第19个bit）确定该页是属于 SWd 还是 NWd 。该位决定在通过系统总线访问底层物理内存时是否设置了 AxPROT[1] 安全位，从而允许受 TrustZone 保护的操作系统和进程访问同一地址空间中受 TrustZone 保护的安全内存和 NWd 内存。当处理器在 TrustZone 模式之外运行时，内存访问总是忽略 NS 位；就像设置了 NS 位一样操作。

启用 TrustZone 的 AMBA3 AXI 总线结构中存在的硬件逻辑通过允许在总线传输期间将系统总线上的读写标记为“安全”或“非安全”来保护 SWd 资源不被 NWd 访问。当安全总线主机启动总线传输操作时，ARPROT[1] 或 AWPROT[1] 位确定传输是否应被视为安全或非安全事务。

# TEE 硬件架构



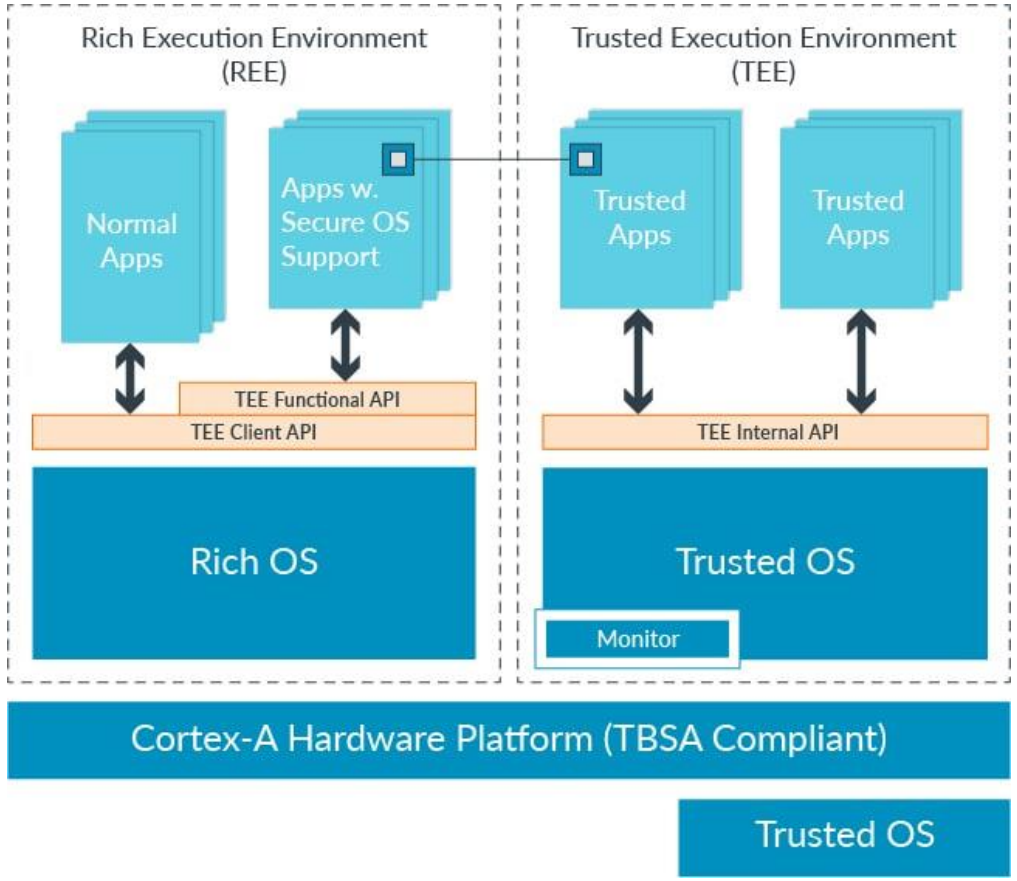




Internal resources:

Hardware components internal to a SoC such as internal RAM, ROM, or eFuse.

# TEE 软件架构

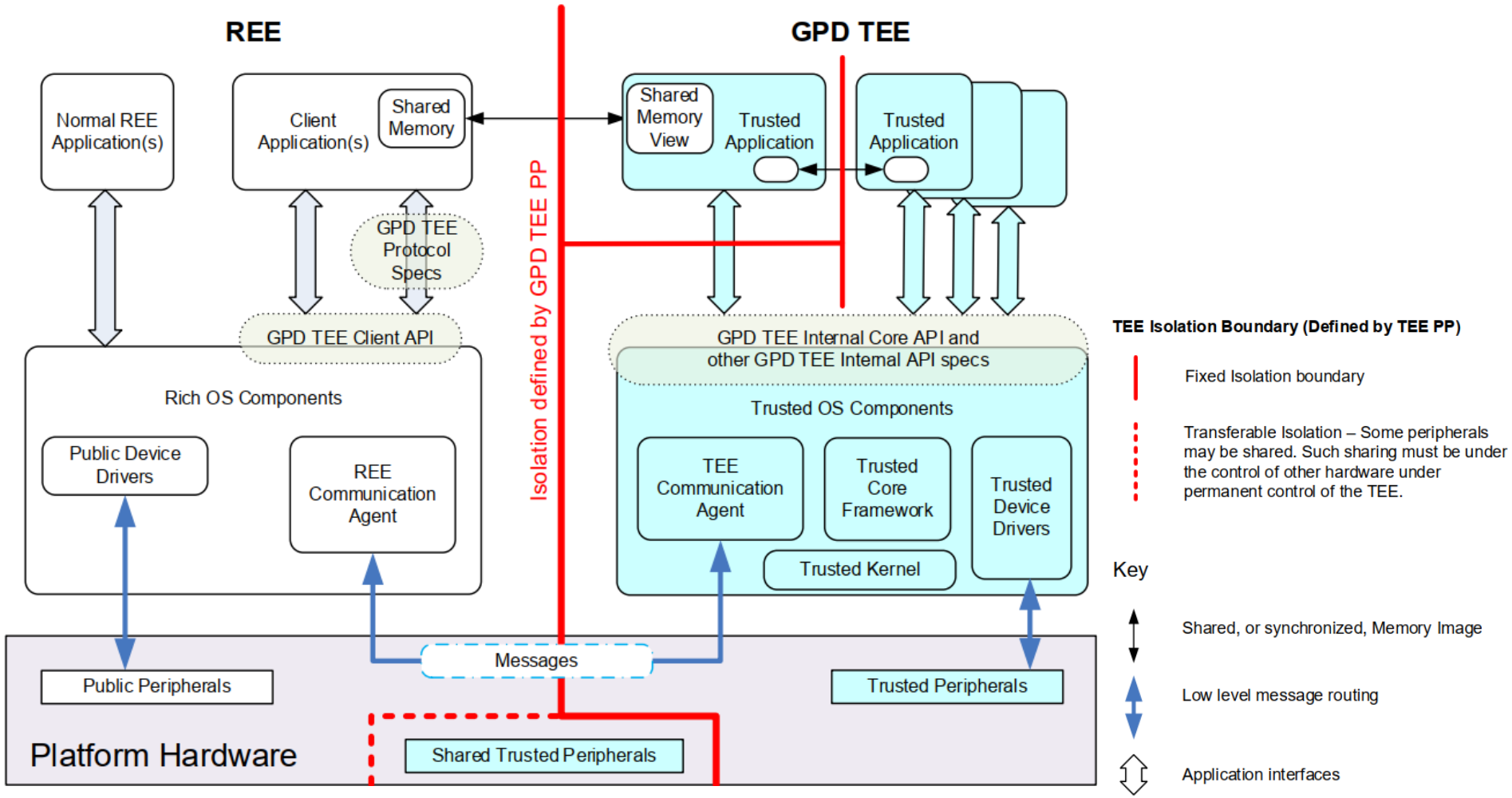



TEE的软件、硬件架构设计相辅相成。包含这几类软件：

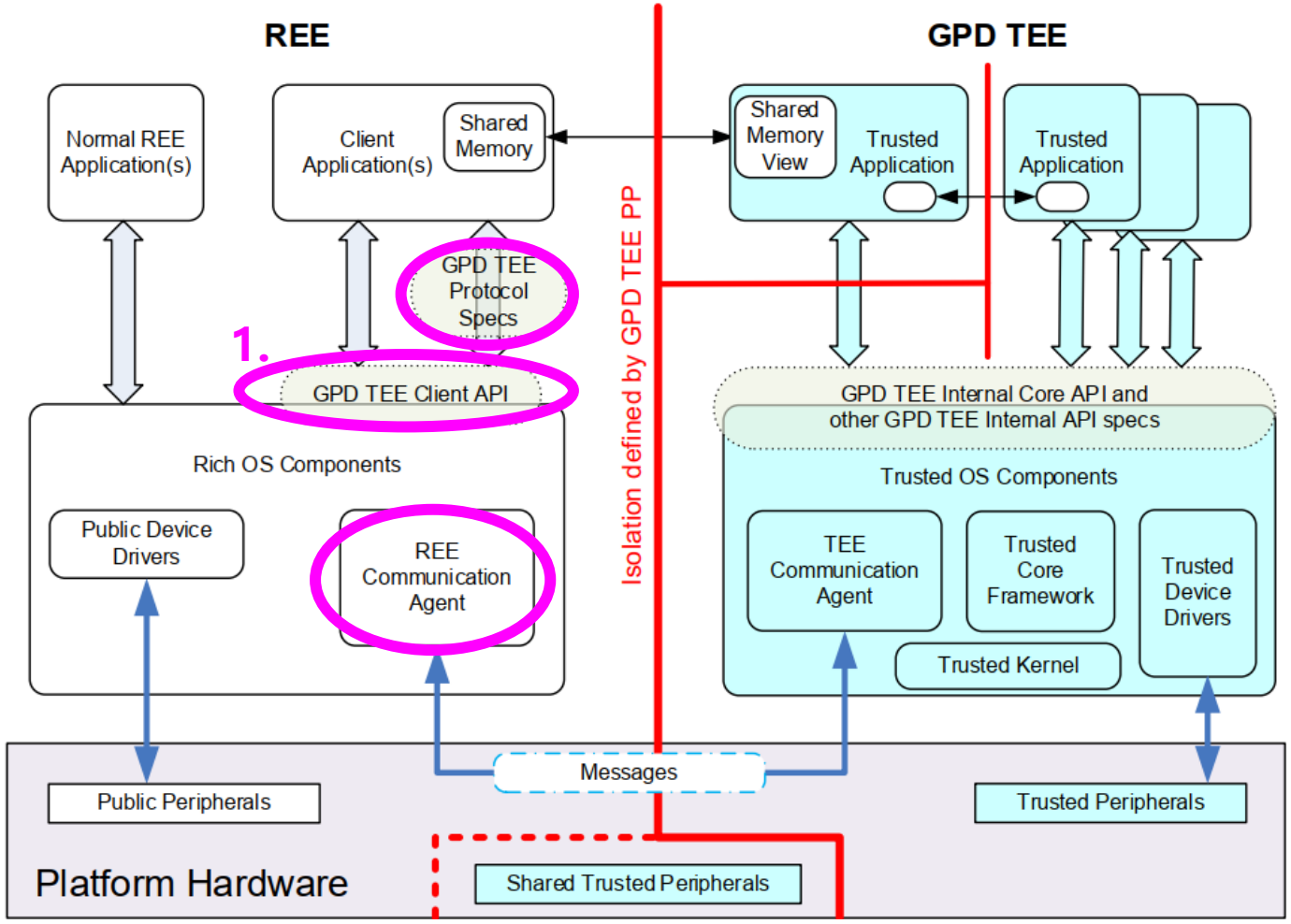
1. REE interfaces to the TEE
2. Trusted OS components
3. Trusted applications (TAs)
4. Shared memory
5. TA to TA communication

https://www.arm.com/ja/technologies/trustzone-for-cortex-a/tee-and-smc

# TEE 软件架构


REE
GPD TEE
Normal REE Application(s)
Client Application(s)
Shared Memory
Shared Memory View
Trusted Application
Trusted Application
GPD TEE Protocol Specs
GPD TEE Client API
GPD TEE Internal Core API and other GPD TEE Internal API specs
Isolation defined by GPD TEE PP
Rich OS Components
Trusted OS Components
Public Device Drivers
REE Communication Agent
TEE Communication Agent
Trusted Core Framework
Trusted Device Drivers
Trusted Kernel
Messages
Public Peripherals
Trusted Peripherals
Platform Hardware
Shared Trusted Peripherals
TEE Isolation Boundary (Defined by TEE PP)
Fixed Isolation boundary
Transferable Isolation – Some peripherals may be shared. Such sharing must be under the control of other hardware under permanent control of the TEE.
Key
Shared, or synchronized, Memory Image
Low level message routing
Application interfaces

# TEE 软件架构

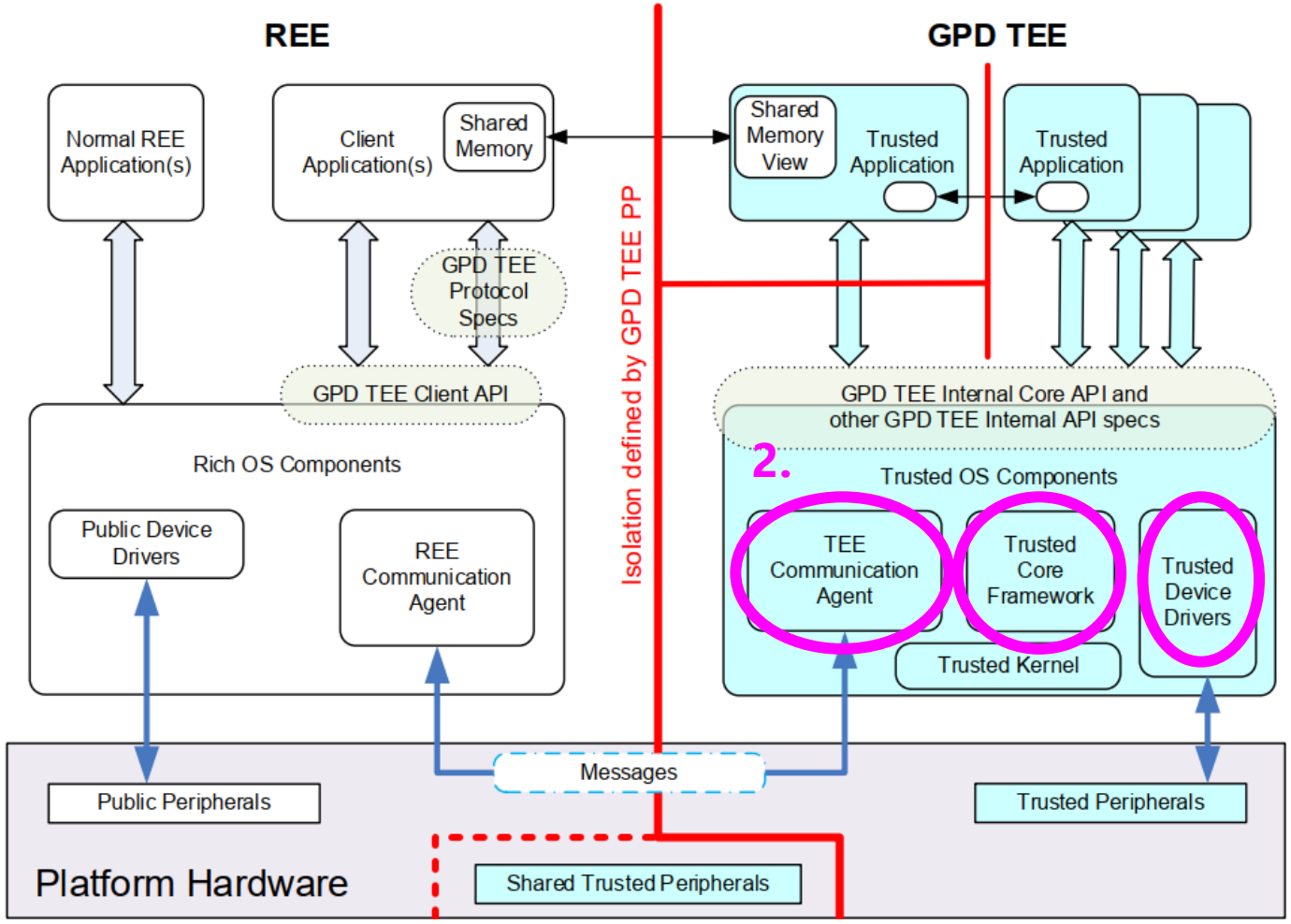



1. **REE interfaces to the TEE**
2. Trusted OS components
3. Trusted applications (TAs)
4. Shared memory
5. TA to TA communication

在 REE 中，该架构标识了一个可选的协议规范层、一个 API 和一个支持通信代理（从上到下）：

- REE 中公开的 TEE 协议规范层为客户端应用程序提供了一组更高级别的 API 来访问某些 TEE 服务。
- TEE 客户端 API 是一个低级通信接口，旨在使运行在富操作系统中的客户端应用程序能够访问并与运行在受信任执行环境中的受信任应用程序交换数据。
- REE 通信代理为客户端应用程序和可信应用程序之间的消息传递提供 REE 支持。

# TEE 软件架构



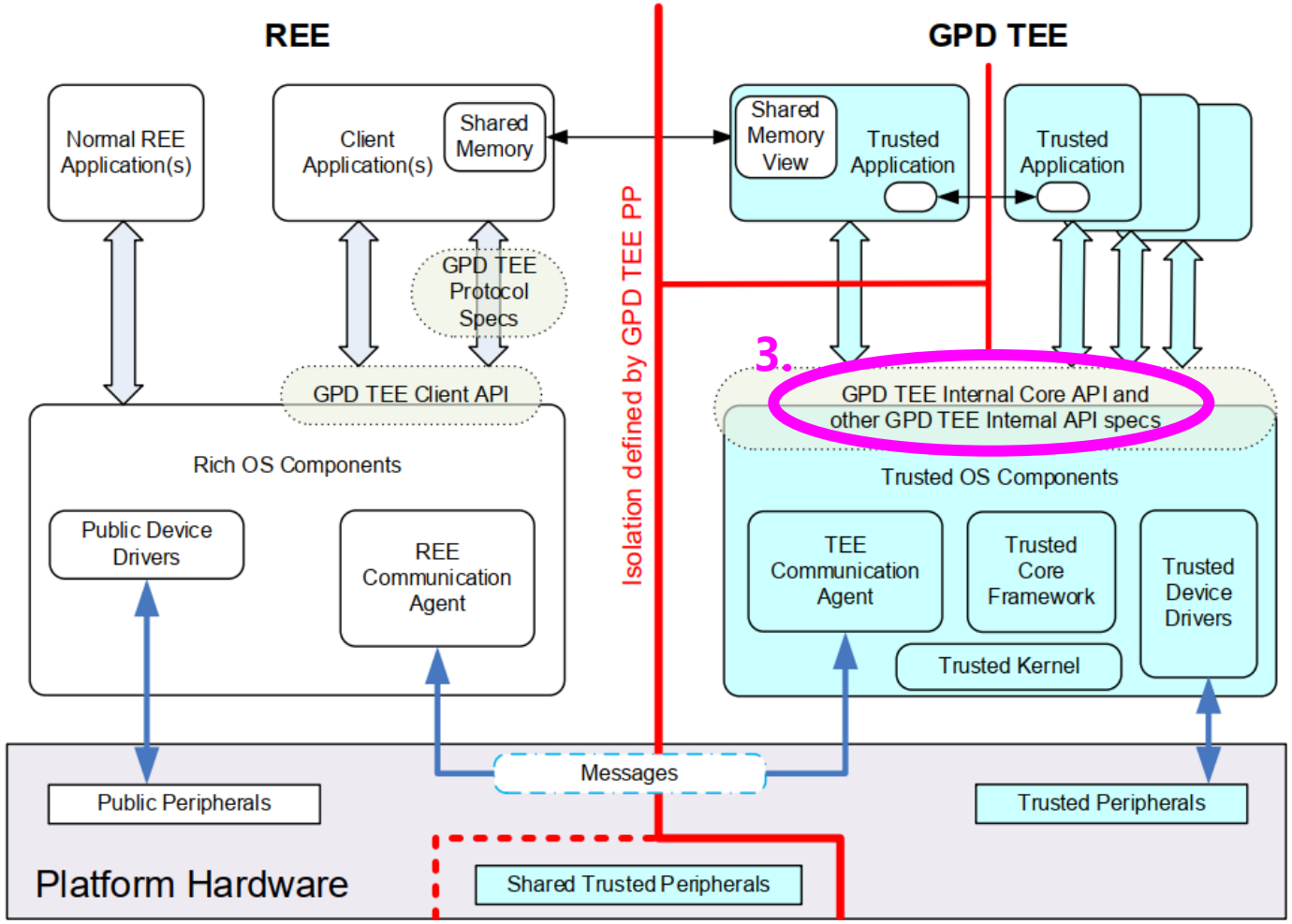

1. REE interfaces to the TEE
2. **Trusted OS components**
3. Trusted applications (TAs)
4. Shared memory
5. TA to TA communication

在 TEE 中，该架构确定了两类不同的软件：受信任的操作系统组件提供的托管代码，以及在该代码之上运行的受信任的应用程序。

可信操作系统组件包括（从左到右）：

- TEE 通信代理是可信操作系统组件的一个特例。它与它的对等体 REE 通信代理一起工作，在 CA 和 TA 之间安全地传输消息。
- 为可信应用程序提供操作系统功能的可信核心框架。 可信核心框架是 TEE 内部核心 API 的一部分。
- 可信设备驱动程序，为专用于 TEE 的可信外围设备提供通信接口。
  - 可信应用程序和可信核心框架使用可信内核提供的调度和其他操作系统管理功能。

# TEE 软件架构




1. REE interfaces to the TEE
2. Trusted OS components
3. **Trusted applications (TAs)**
4. Shared memory
5. TA to TA communication

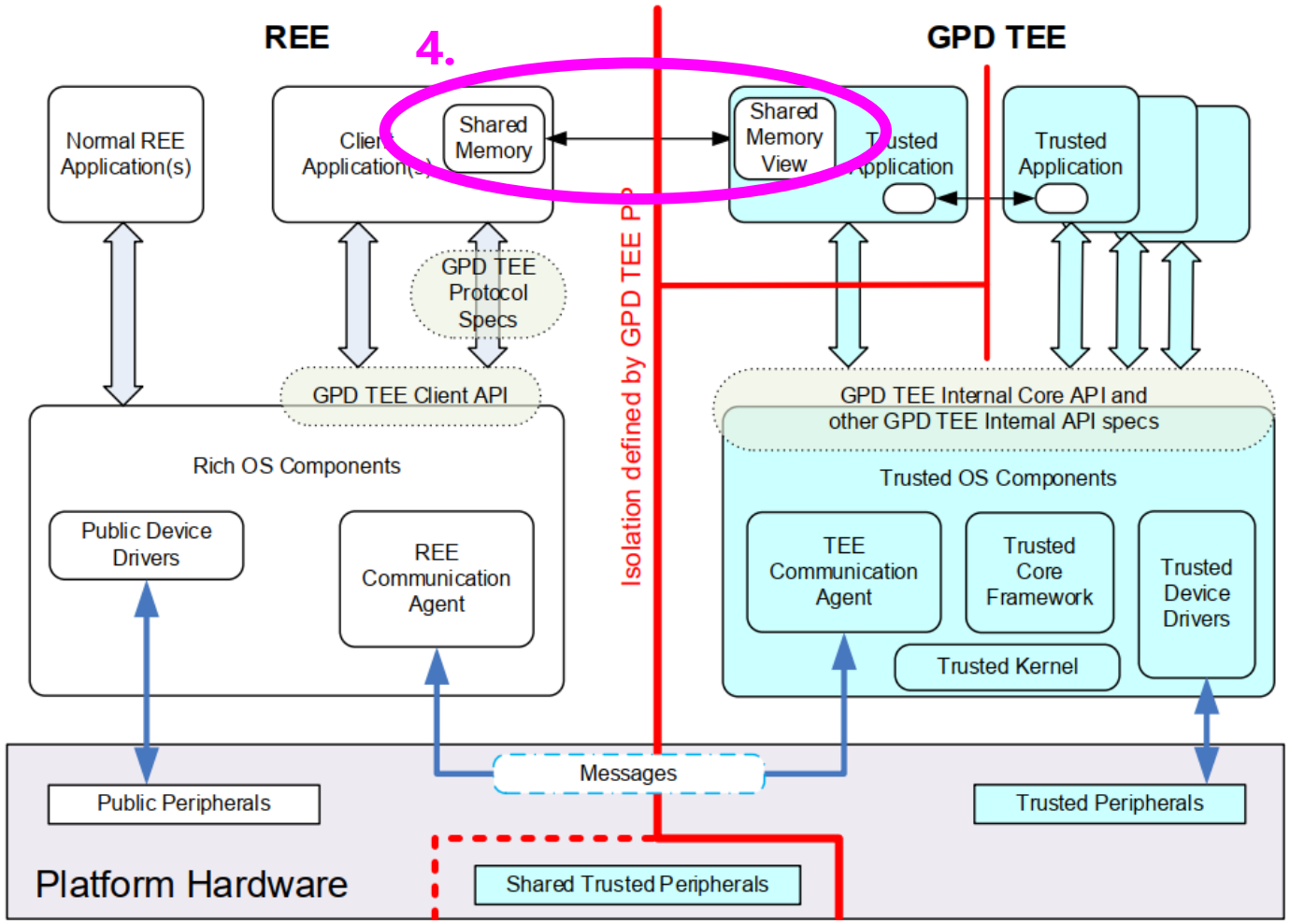
受信任的应用程序通过受信任的操作系统组件公开的 API 与系统的其余部分进行通信。

- TEE 内部 API 定义了 TEE 的基本软件功能。
- 可以定义其他非 GlobalPlatform 内部 API 以支持接口以进一步实现专有功能。

当客户端应用程序与可信应用程序创建会话时，它会连接到该可信应用程序的一个实例。

可信应用程序实例具有与所有其他可信应用程序实例的物理内存地址空间分开的物理内存地址空间。

# TEE 软件架构



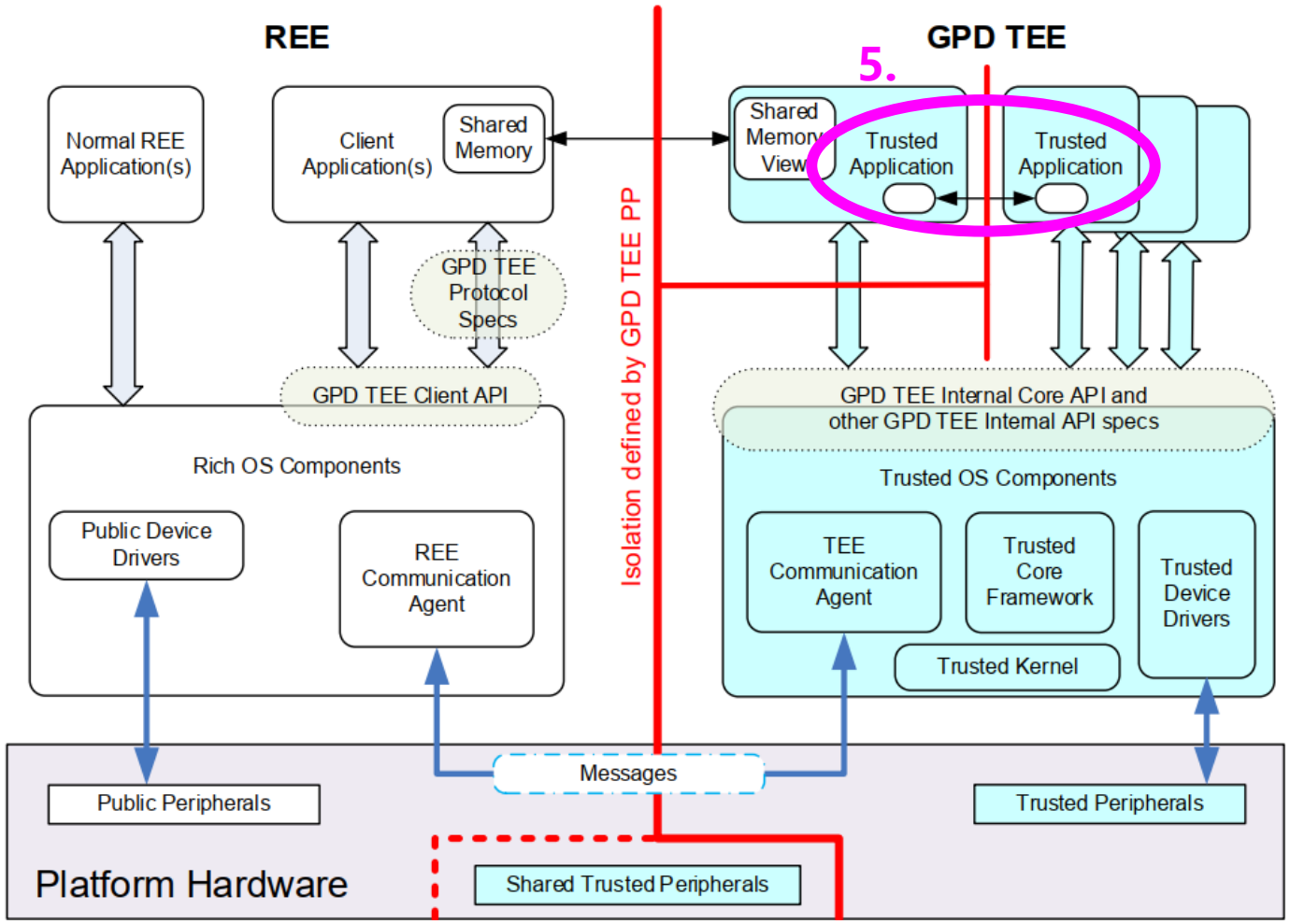

1. REE interfaces to the TEE
2. Trusted OS components
3. Trusted applications (TAs)
4. **Shared memory**
5. TA to TA communication

TEE 的一个特点是它能够使 CA 和 TA 通过访问 TEE 和 REE 均可访问的内存区域快速有效地通信大量数据。

API 设计允许此功能由通信代理作为内存副本或直接共享内存来实现。

必须注意使用共享内存的安全方面，因为客户端应用程序或受信任的应用程序可能会与其他方在该内存上操作时异步修改内存内容。

# TEE 软件架构



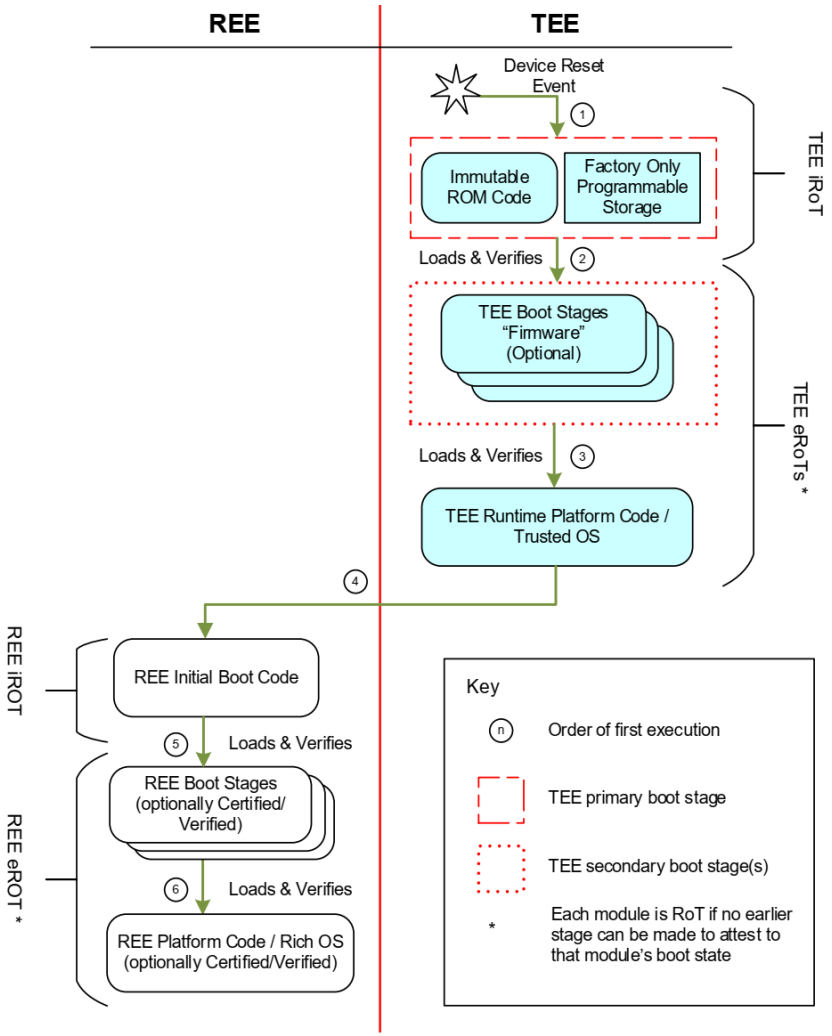

1. REE interfaces to the TEE
2. Trusted OS components
3. Trusted applications (TAs)
4. Shared memory
5. **TA to TA communication**

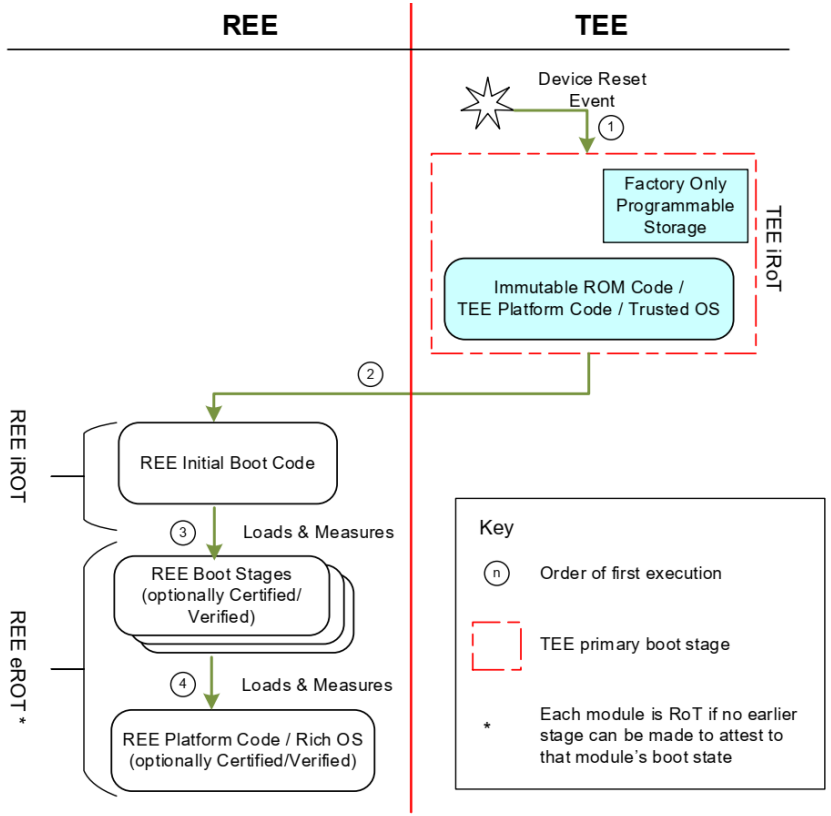
一个 TA 可以与另一个 TA 通信。 这使用了 CA 与 TA 通信所使用的相同过程，但可信赖的指示符允许接收 TA 确保通信没有暴露在 TEE 之外。

这简化了确定是否信任通信内容以及与内容相关联的元数据（例如主叫 TA 的身份）的问题。

由于这种信任关系，同一设备中另一个 TEE 中的 TA 被视为基于 REE 的 CA，因为接收 TA 的 TEE 没有理由信任调用 TA 的 TEE。

# TEE 的启动过程




可信根包括iRoT和eRoT。
iRoT是初始化可信根，是设备厂商在终端制造时植入的，用于系统的安全启动、平台镜像文件执行时的验证等等。
eRoT是增强可信根，是设备在运行阶段生成的,由iRoT来验证生成eRoT镜像的可信，eRoT的生成是安全认证、安全验证、更新下载授权等业务场景的需要而存在的。

# TEE的标准化工作

- OMTP standard – hosted by **GSMA**
  - Open Mobile Terminal Platform (OMTP) first defined TEE in their "Advanced Trusted Environment: OMTP TR1" standard
  - Work on the OMTP standards ended in mid 2010 when the group transitioned into the Wholesale Applications Community (WAC).

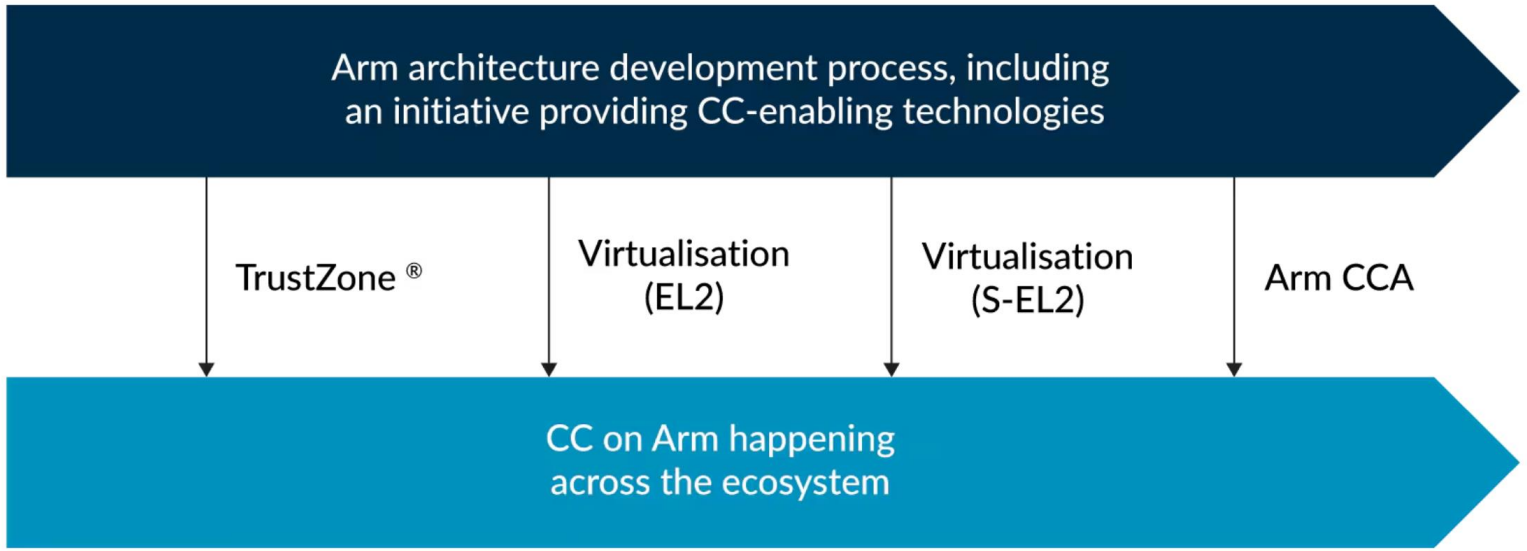
- de facto standard – hosted by **GlobalPlatform**
  - Commercial TEE solutions base on ARM TrustZone
  - Conformed to OMTP TR1 standard
  - GPD TEE

# ARM CCA

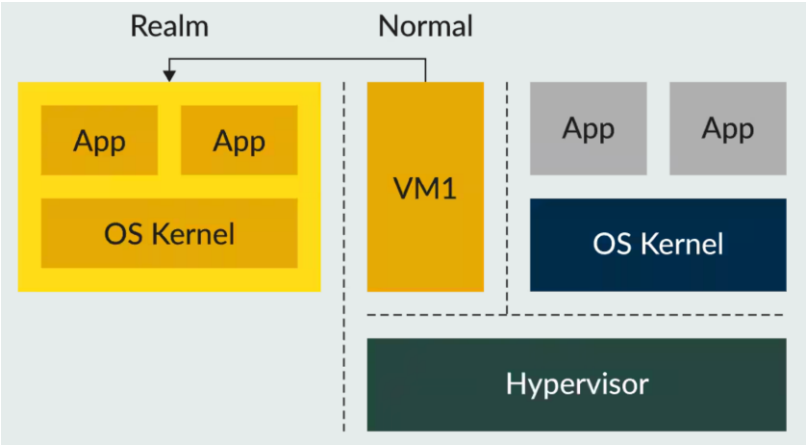
## Confidential Computing: A New Model of Trust on the Arm Architecture

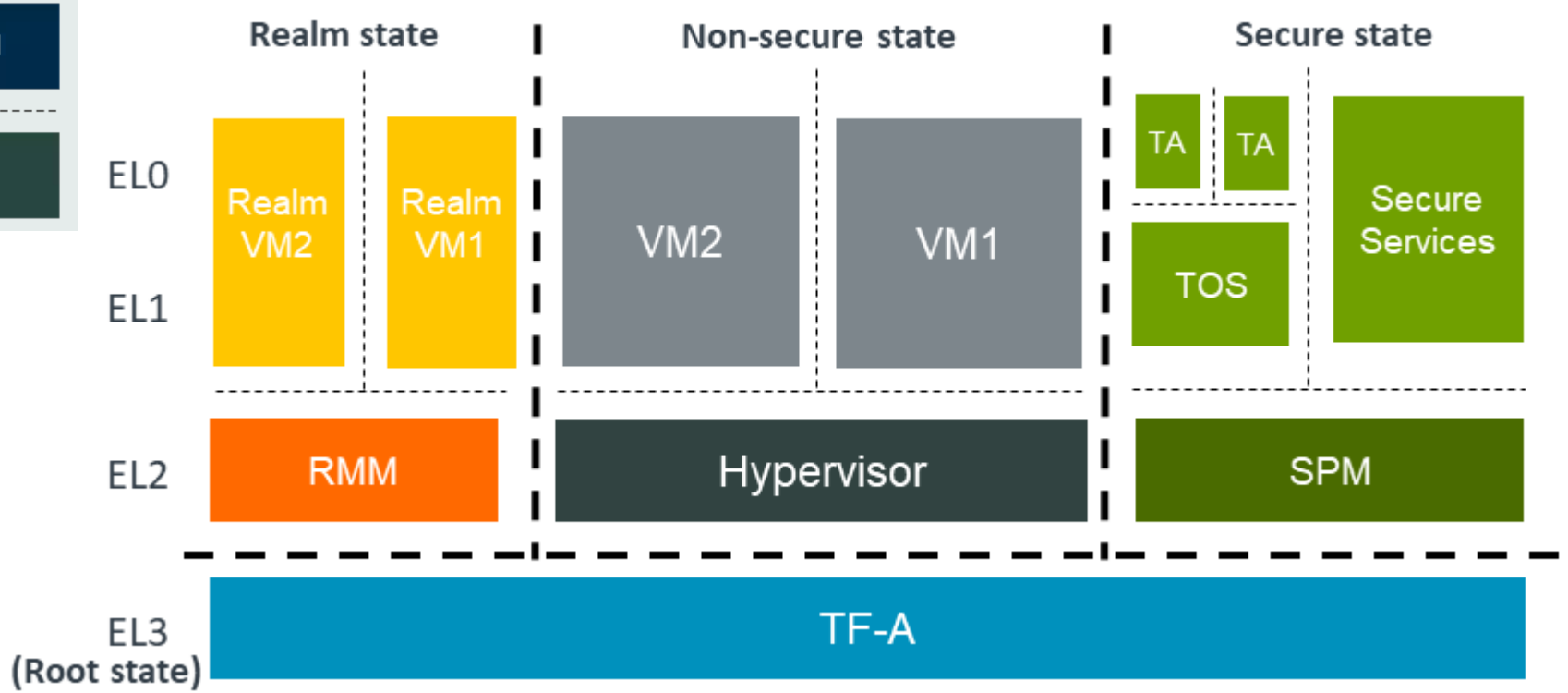
Computing has become a distributed utility where computing sessions can run on any platform that meets the required security policy, making the ability to trust the computing utility infrastructure crucial to ensure confidence in the security and privacy of information. This model is a prime target for cybercriminals, intent on stealing data and code.

Confidential compute is a broad term for technologies that reduce the need to trust a computing infrastructure, such as the need for processes to trust operating system (OS) kernels and the need for virtual machines to trust hypervisors. While threats span all industry sectors, the Arm architecture is unique in the breadth of form factors and markets where it is used and our partners are actively innovating and delivering confidential computing using existing Armv8-A devices.



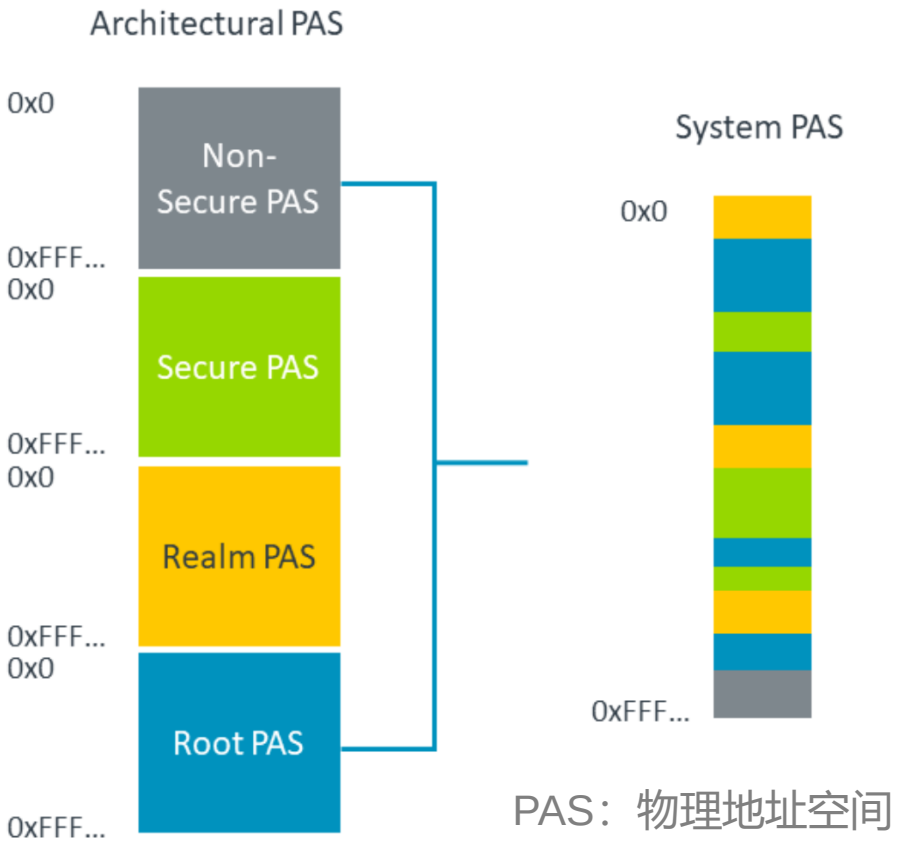

Arm CCA builds on the strong security foundations of TrustZone and introduces the concept of dynamically created Realms to be both evolutionary and revolutionary.




[Arm Confidential Compute Architecture – Arm®]

# ARM CCA 不同类型物理地址分布




PAS：物理地址空间

不同类型间的可访问性

| 空间类型 | Non-secure | Secure | Realm | Root |
|---|---|---|---|---|
| Non-secure | √ | x | x | x |
| Secure | √ | √ | x | x |
| Realm | √ | x | √ | x |
| Root | √ | √ | √ | √ |

# 本章要点

- ARM TrustZone
  - 软硬件架构
  - 启动机制
- ARM CCA
  - 与机密计算概念混合后的TEE