OWASP
Gothenburg Göteborg

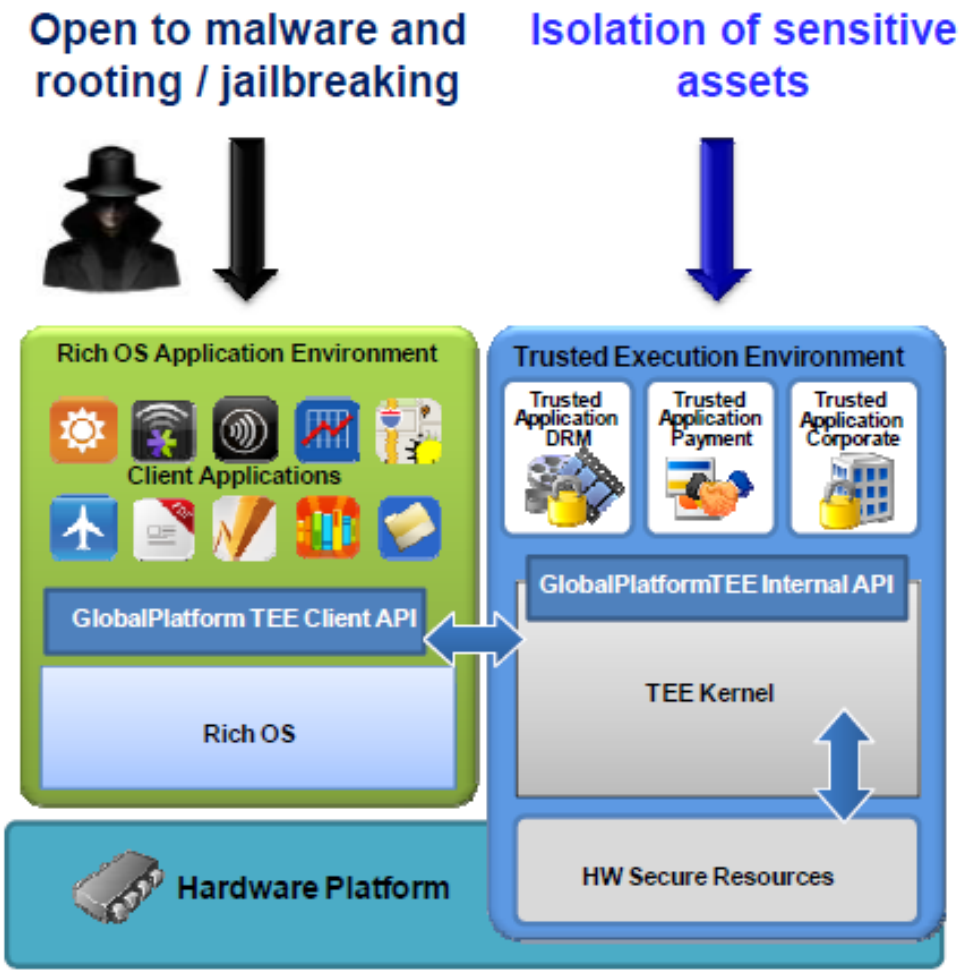
Trusted Execution Environment,
TrustZone and Mobile Security

OWASP Göteborg: Security Tapas, Oct-20, 2015

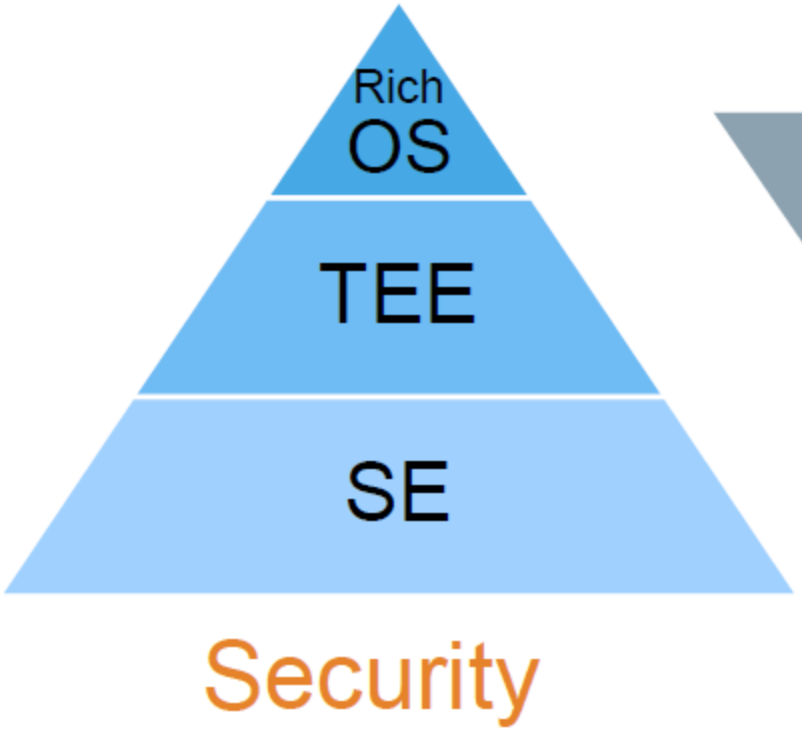
Peter Gullberg, Principal Engineer - Digital Banking, Gemalto

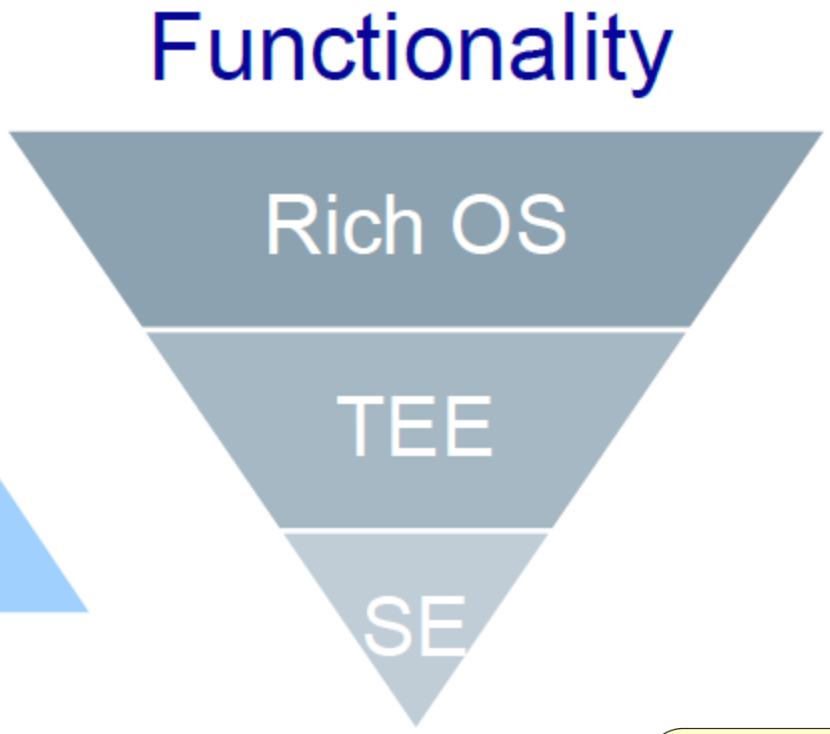
"TEE allows Applications to execute, process, protect and store sensitive data in an isolated, trusted environment."

Trusted Execution Environment (TEE)



- TEE provides **hardware-based isolation** from rich OS such as Android, Windows Phone and Symbian
- TEE runs on the **main device chipset**
- TEE has **privileged access** to device resources **(user interface, crypto accelerators, secure elements…).**





http://www.globalplatform.org/documents/GlobalPlatform_TEE_White_Paper_Feb2011.pdf

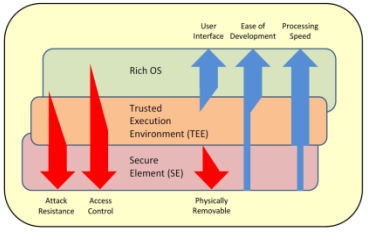


Figure 2 : Rich OS, TEE and SE Positioning

TEE - Use Cases

Content Protection

- IP streaming
- DRM
- Key protection
- Content protection

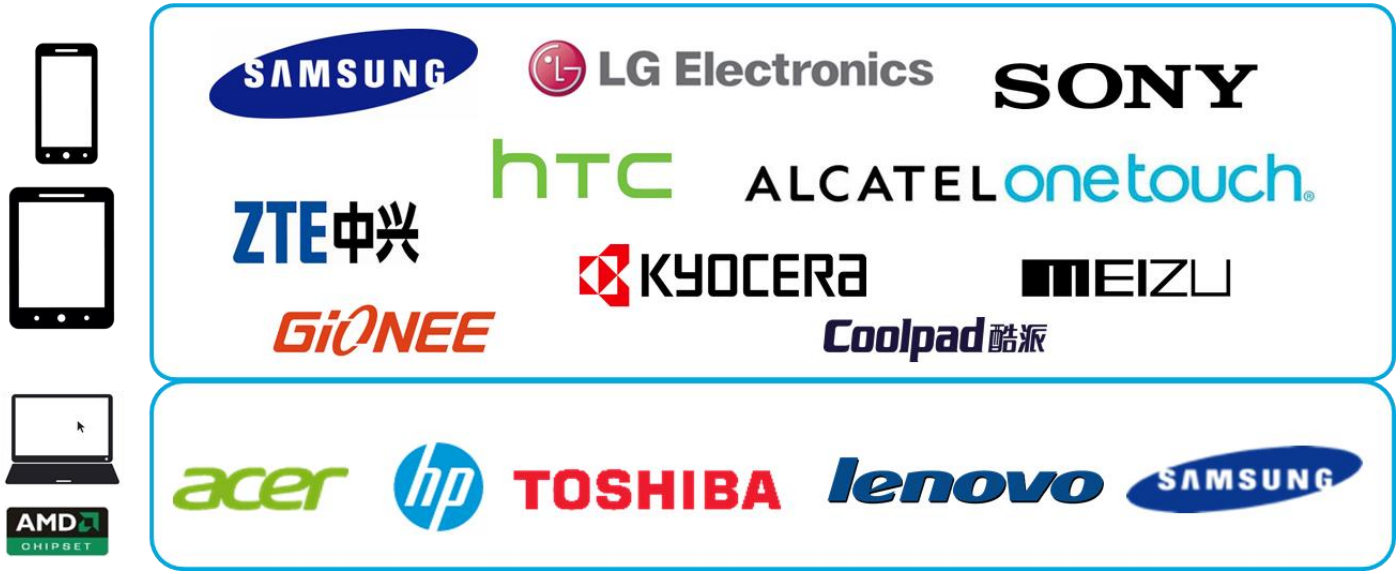
Mobile Financial Services

- mBanking
- Online payments
- User authentication
- Transaction validation

Corporate/government

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

Example of TEE enabled devices




Google Galaxy Nexus


Google Nexus 7


Samsung Galaxy S III


Samsung Galaxy Note II

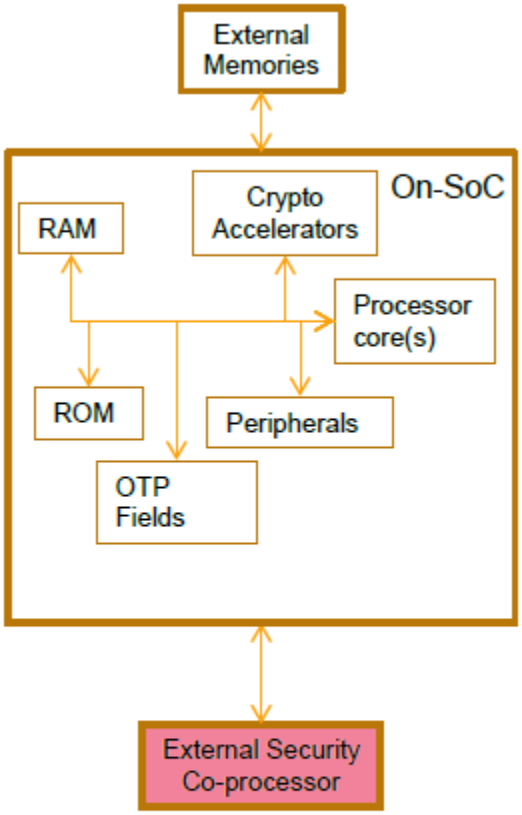

Amazon Kindle Fire HD


Motorola Razr HD

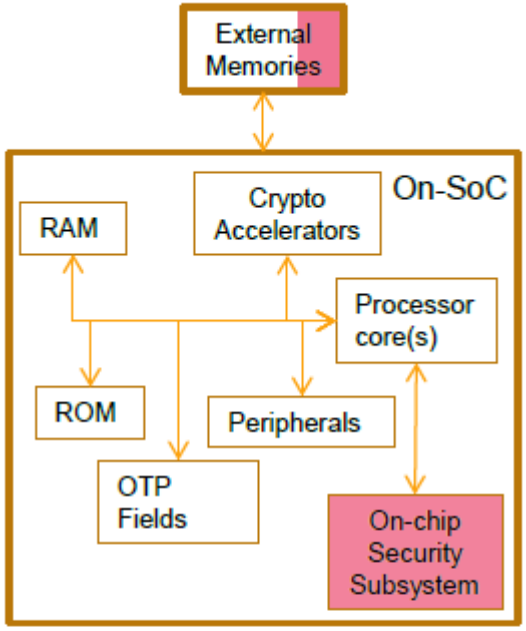

Samsung S4


Samsung S5

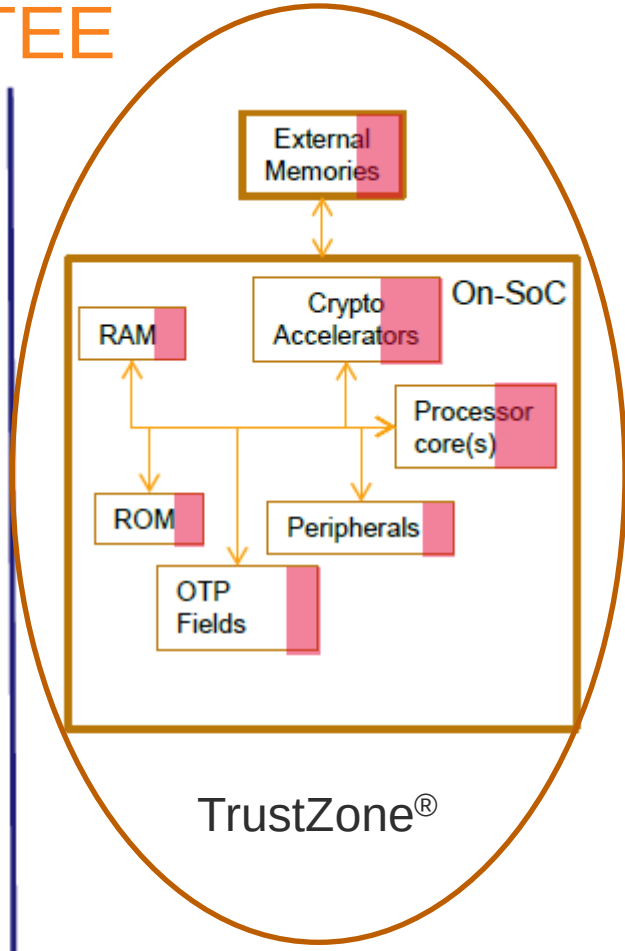
Architectural ways of achieving a TEE



External Secure Element



Embedded Secure Element



Processor Secure Environment

TEE component

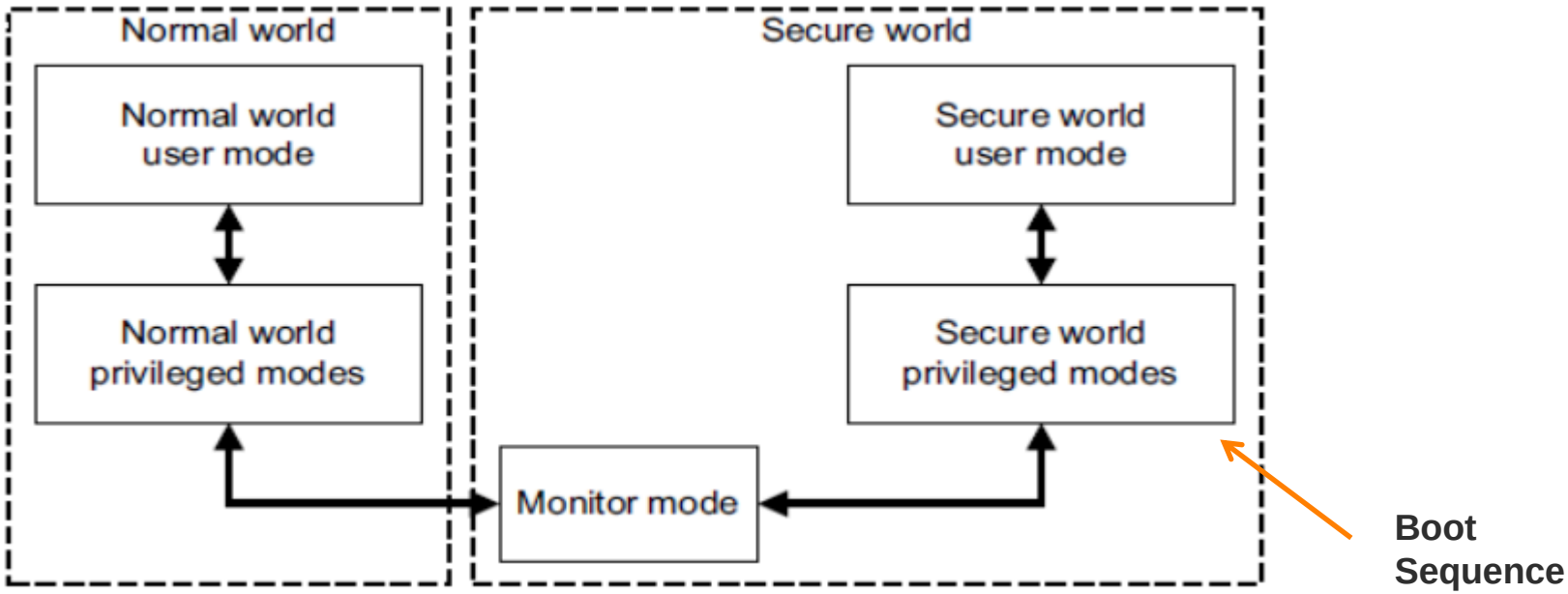
TrustZone®

ARM TrustZone

- TrustZone enables the development of separate environments
  - Rich Operating System - Normal domain
  - Trusted Execution - Secure domain
- Both domains have the same capabilities
  - Operate in a separate memory space
- Enables a single physical processor core to execute from both the Normal world and the Secure world
    - Normal world components cannot access secure world resources
- Cortex-A Processors

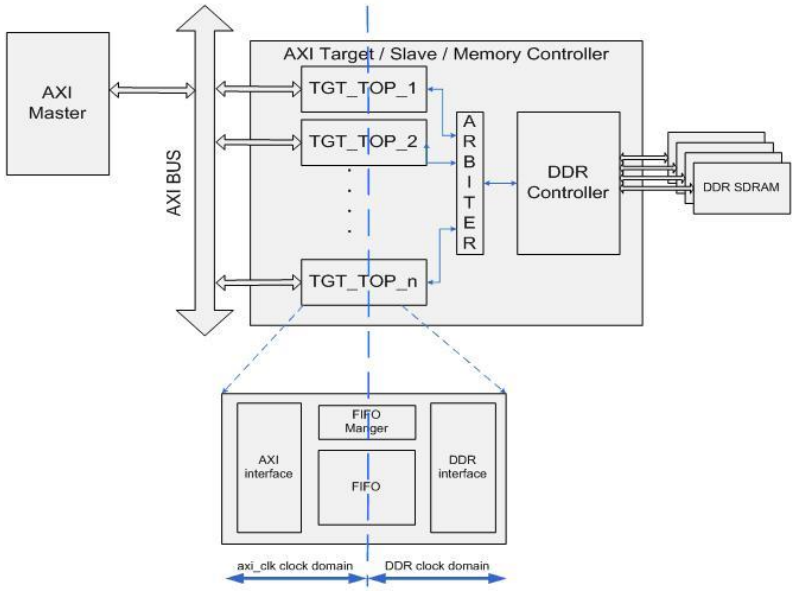
How TrustZone works

- Uses a “33rd bit”, signaling whether in secure mode
- This bit is also propagated outside the system on chip (SoC)
- Peripherals and memory are configured during startup which side to belong to (normal/secure)



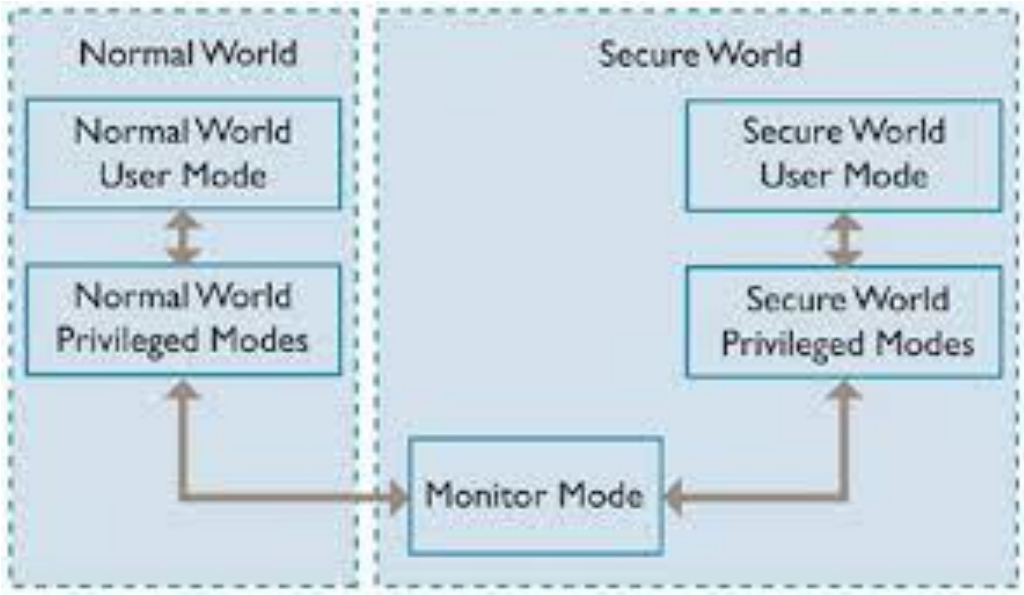
ARM TrustZone: Non Secure bit

- The memory is split in Secure and Non-secure regions
- Non-secure (NS) bit
  - Determines if the program execution is in the Secure or Non-secure world
- AMBA AXI bus propagates the NS bit
- Shared memory between two worlds
- Possible to secure peripherals
  - Screen, crypto blocks
  - Protected against software attacks

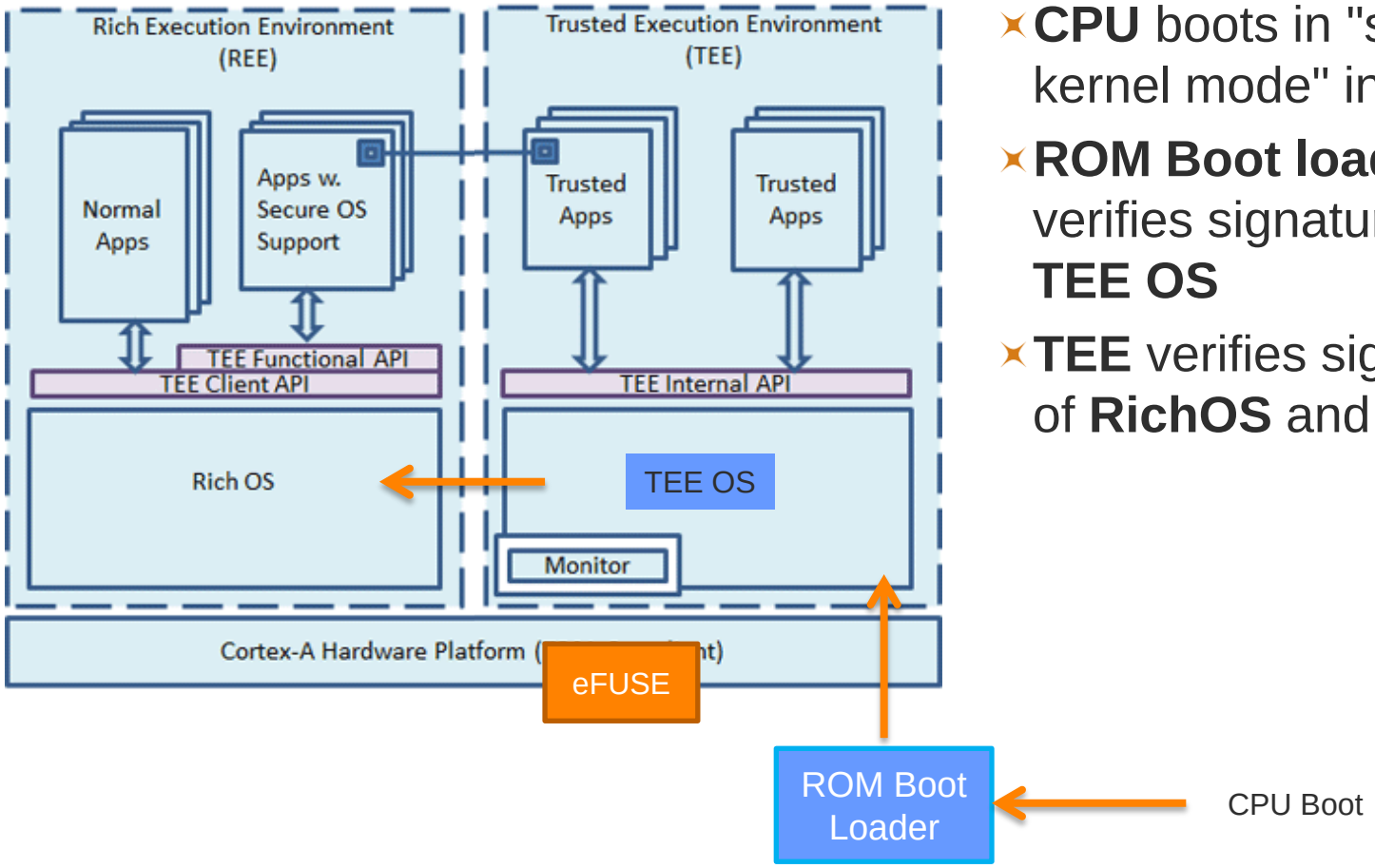


ARM TrustZone: transition management

- Switch between normal and secure domain
- Monitor
  - Gatekeeper that controls migration between Normal and Secure world
- In normal world, have both user mode and privileges mode. Same for Secure world
  - Secure device drivers typically run in user mode
  - Cannot switch the NS bit in user mode
- Secure Monitor Call
  - SMC



Secure Boot - typical scenario



- **CPU** boots in "secure kernel mode" in **ROM**
- **ROM Boot loader** verifies signature of **TEE OS**
- **TEE** verifies signature of **RichOS** and starts it

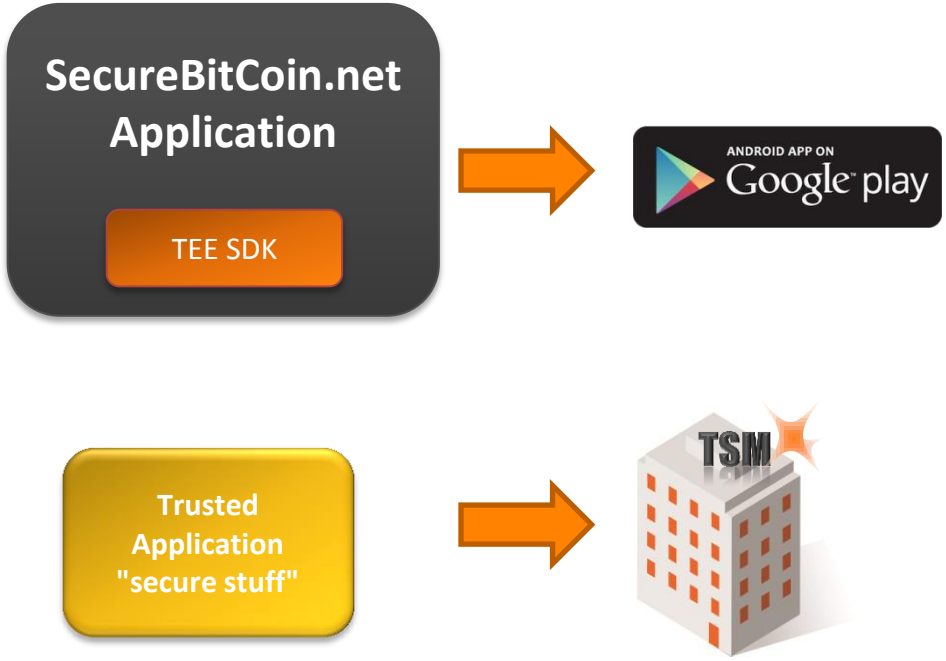
Example on use case

securebitcoin.net

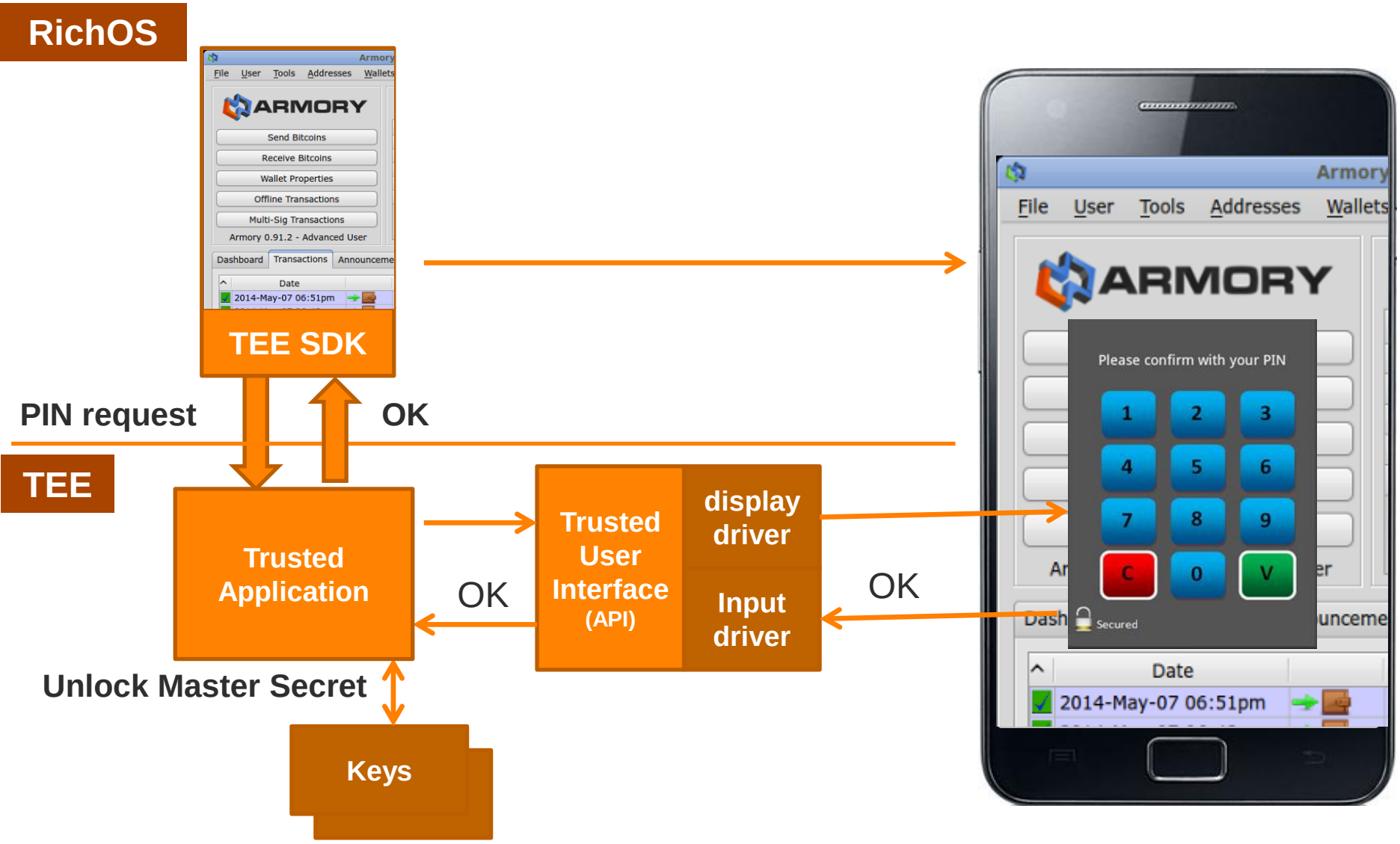
BitCoin - example

SecureBitCoin.net

- Secure management of Master Secret
- PIN-entry to access the Master Secret
- Use secure crypto provided by TEE
- Master Secret is kept secure at all time
- Malware cannot steal data, or modify transactions

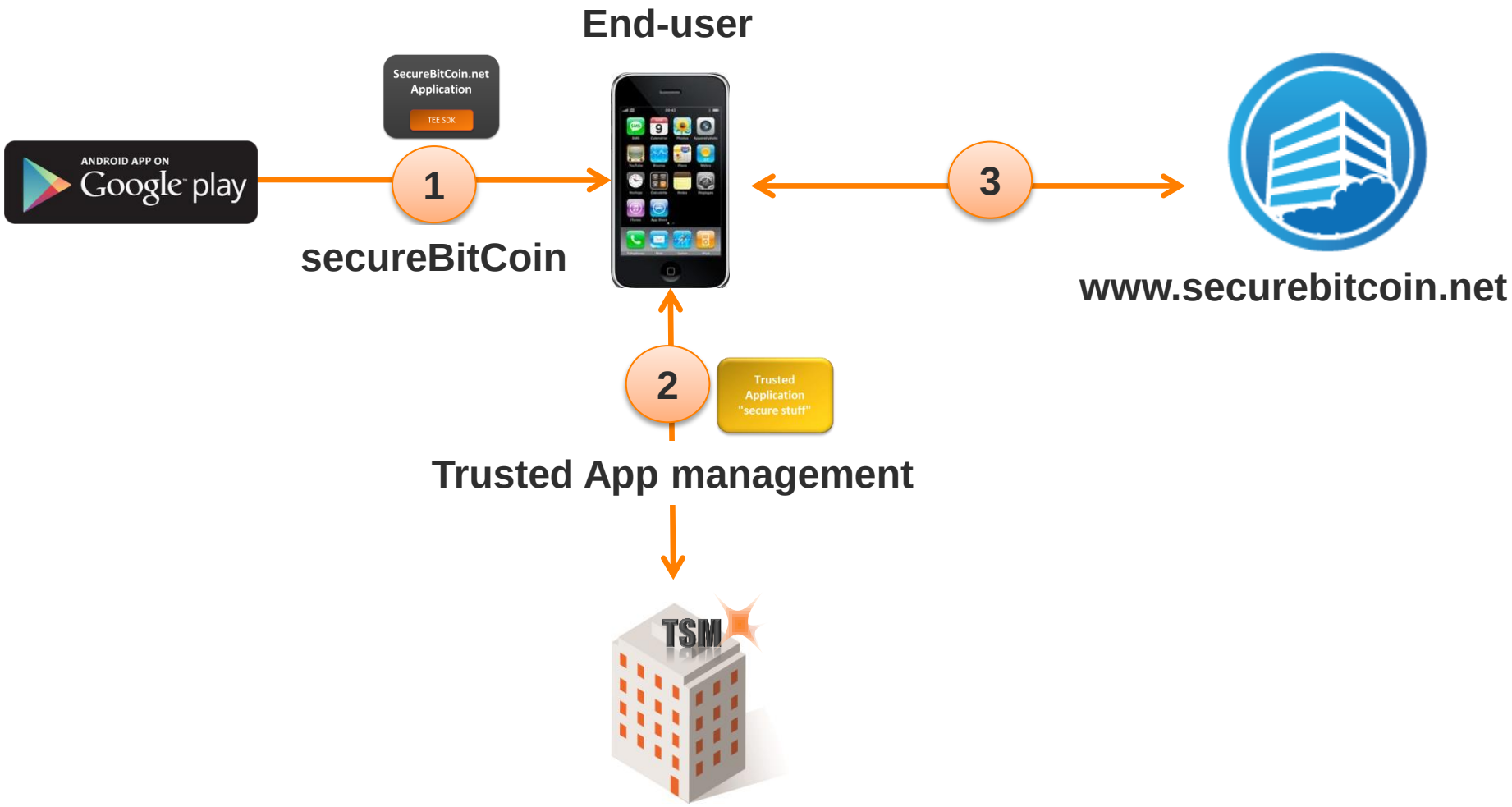


Trusted User Interface



App Deployment

"secure BitCoin" App



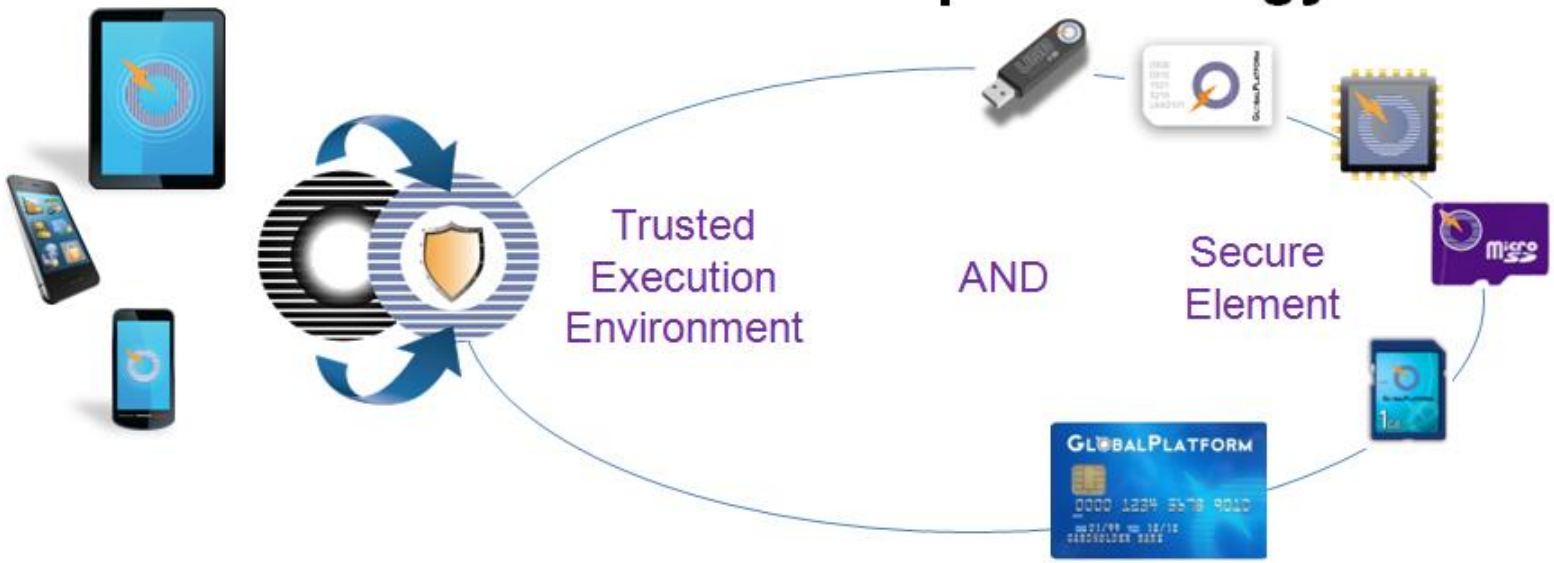
Thank you

Global Platform

GlobalPlatform Positioning

GLOBALPLATFORM™

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



Across several market sectors and in converging sectors

TEE Standardization Principles

GLOBALPLATFORM™

- Overall objective: promote TEE ecosystem
  - Have interoperable TEEs across silicon vendors and devices
  - Have one single set of APIs for service providers whatever the silicon vendors and devices
  - Have standardized way to administrate the TEE
- Technology agnostic
- Resistant to
  - any software attack (remote and local)
  - basic hardware attacks (local)
    - debug interface, firmware tampering, …
- TEE programming environment
  - Native-based (C-based)
  - Isolation between Trusted Applications