Global Platform®

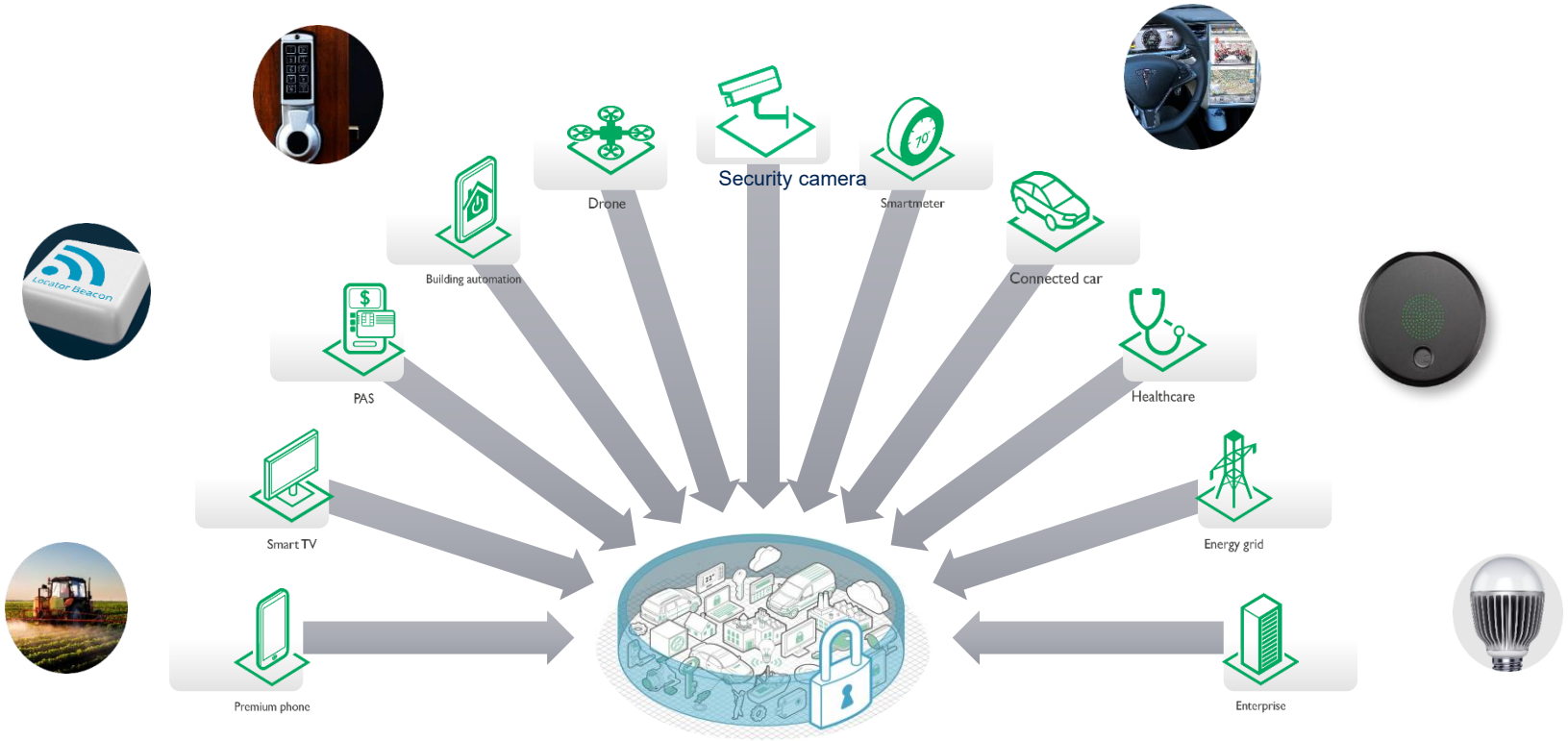
Root of trust and Chain of Trust

Gil Bernabeu, GlobalPlatform CTO

Robustness Against Malicious Attacks – IoT Everywhere

The three fundamental elements of security
- Confidentiality
- Integrity
- Availability

Others
- Non-Repudiation
- Authentication



And more …

Security: Threats, Attacks and Defenses

Threat Focus:

Hardware enforced defenses:

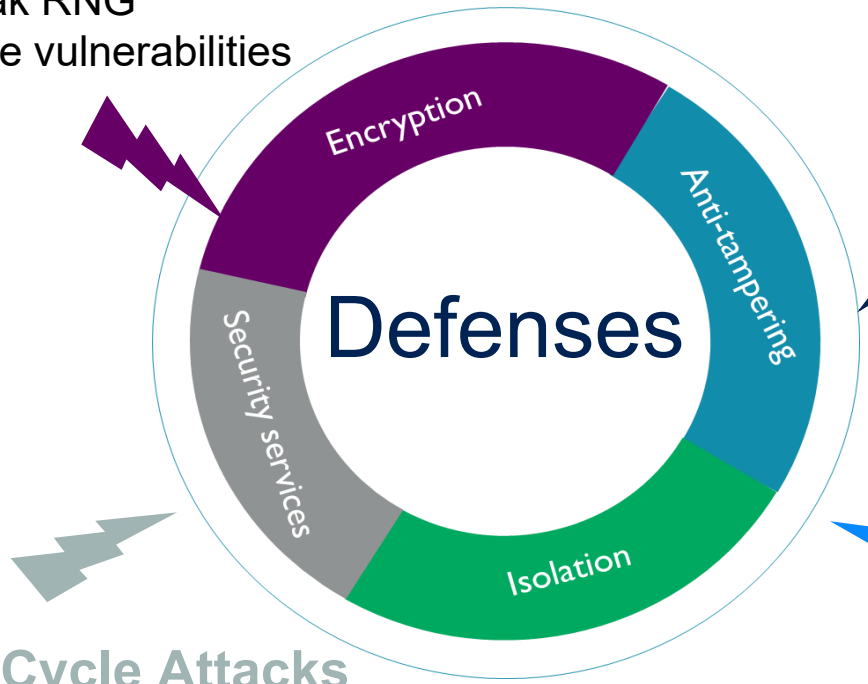
- Scalable software attacks
- Low cost hardware tampering
- Economically viable attacks

Communication Attacks

- Man In The Middle
- Weak RNG
- Code vulnerabilities

Physical Attacks

- Fault injection: clock or power glitch



Life Cycle Attacks

- Code downgrade
- Integrity vulnerabilities
- Factory oversupply

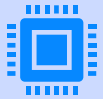
Software Attacks

- Buffer overflows
- Interrupts
- Malware

What is the Root of Trust (RoT)

and the Chain of Trust (CoT)?

Requirements for RoT



Specificities:

Consist of computing engine, code [and data and/or key(s)], all co-located on the same platform

Provides at least one security service

Small as possible to limit the attack surface

Properties:

Immutability

•Or mutability under authorization

Unique identifiable ownership

Ownership optionally transferable

A platform SHALL contain one and only one RoT, but a device embeds multiple platforms

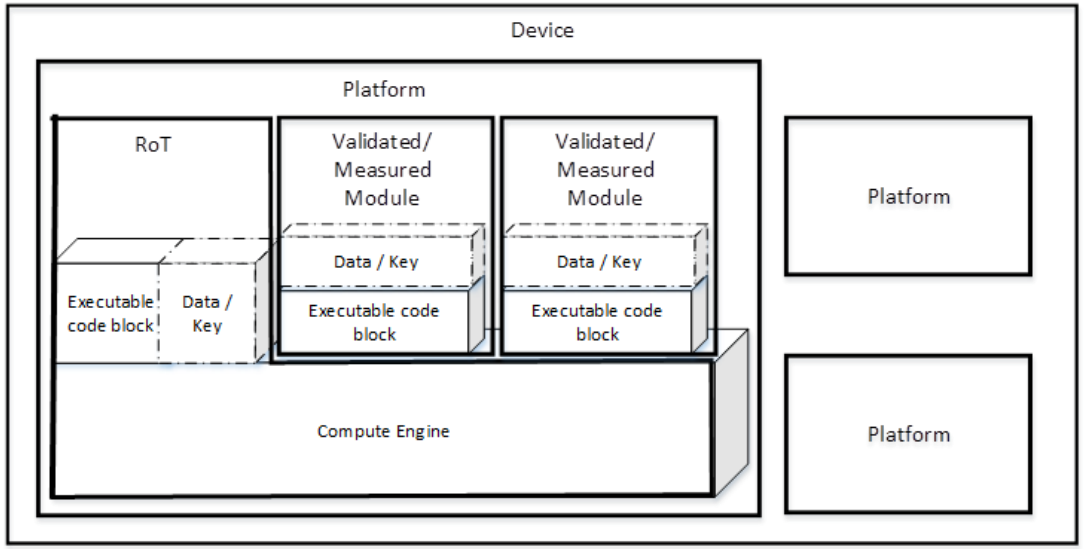
Suitable for certification

Non-Bootstrapped RoT

The RoT SHALL be:

The first code to execute on the platform

Created and provisioned during the manufacturing process



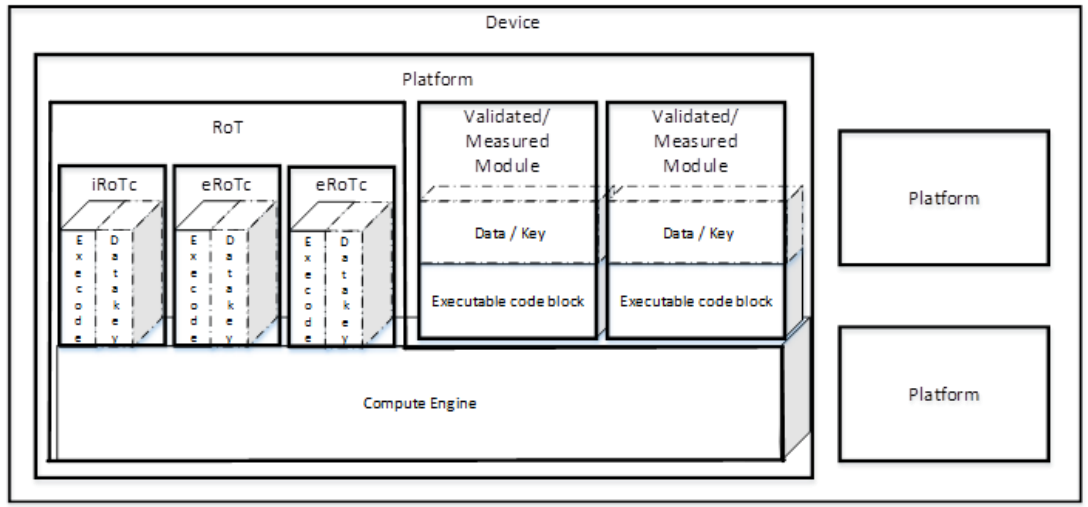
Bootstrapped RoT

The initial RoT SHALL be:

Unique on the platform

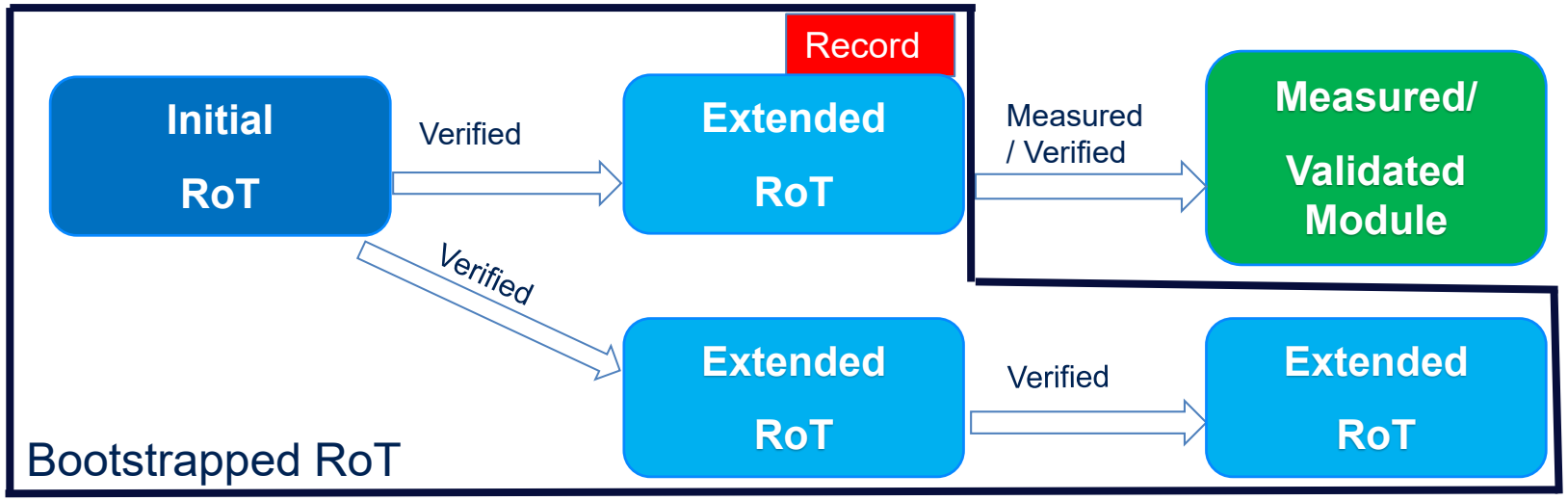
The first code to execute on the platform

Created and provisioned during the manufacturing process



A parent RoT component SHALL verify the integrity (code and data) of an extended RoT (without the possibility to preserve a reportable verification)

Example


Record
Initial
RoT
Verified
Extended
RoT
Measured
/ Verified
Measured/
Validated
Module
Verified
Extended
RoT
Verified
Extended
RoT
Bootstrapped RoT

RoT Security Services

RoT Security Services implement interface (API) allowing to exercise this capability

The interface SHALL provide the appropriate level of protection of the shielded locations to maintain

- The integrity of the contents
- The confidentiality of the contents when it is required

The RoT Security Services are

Authentication, Confidentiality, Identification, Integrity, Measurement, Authorization, Reporting, Update, Verification

Requirements for a Root Of Trust

Computing Engine and Core Data

Hardware, software and keys in the same location

Security Services

Provide one or more security services for the chain of trust

Certification

Shall be suitable for certification(i.e. a test lab is able to evaluate it

Unique identifiable ownership

A single identifiable owning entity

Mutability

Core and/or data are immutable. Or only the owner can control the mutability.

Ownership transfer

Shall be provided by the root of trust in case it exists

Secure Element a Root Of Trust

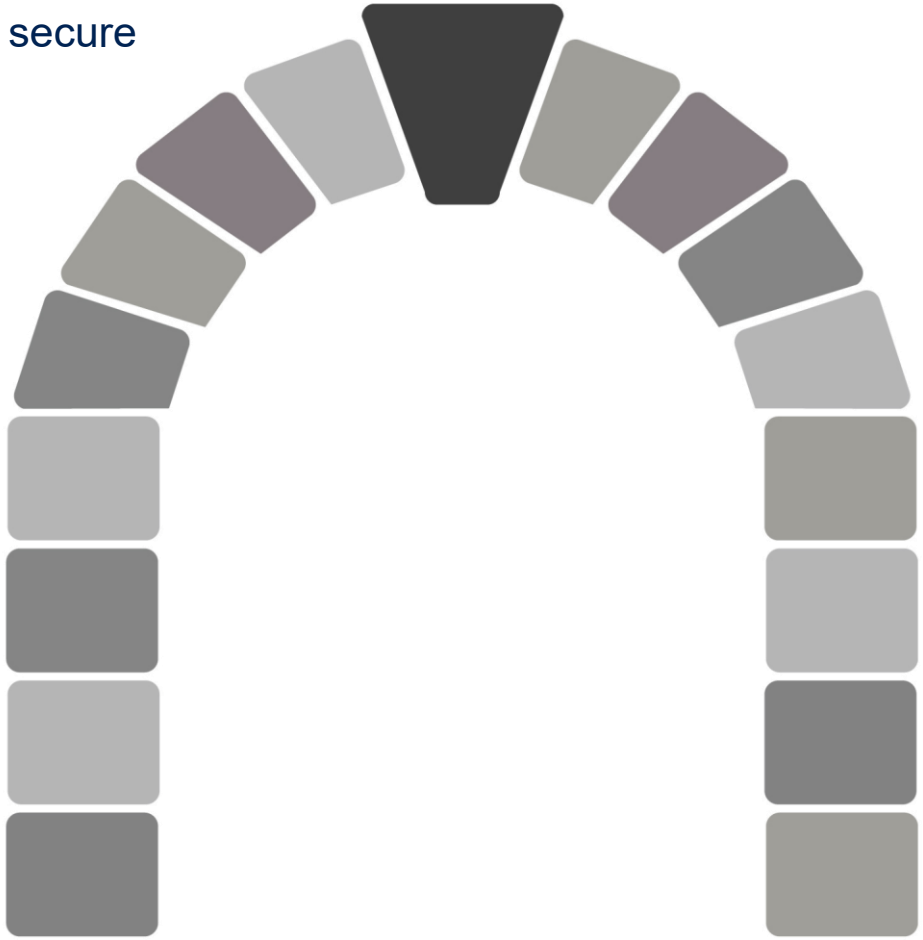
Like a building, Security needs a keystone to ensure the whole system is secure

The keystone ensures :

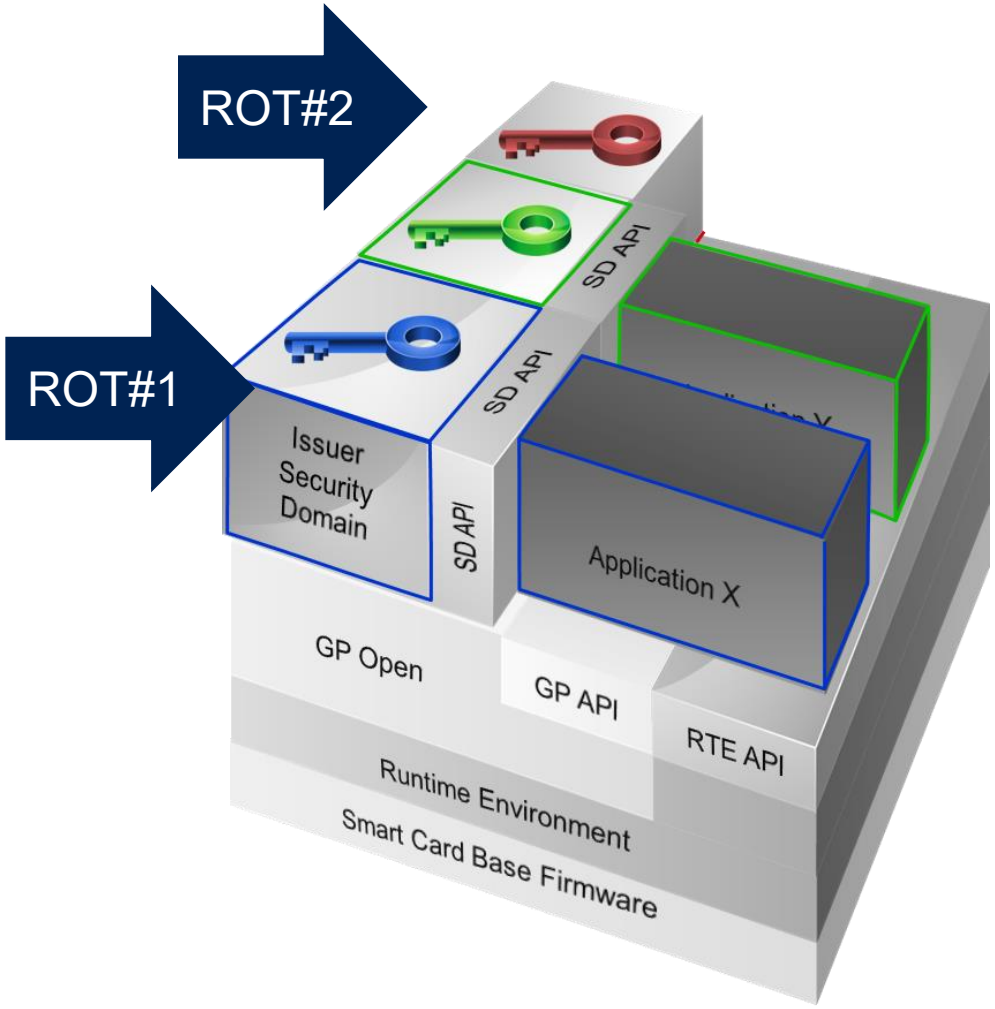
- The whole arch is standing
- The arch can support the building weight

An initial security seed (or root of trust) can that ensure :

- The whole platform is secure
- The system is secure



GlobalPlatform SE : Root(s) Of Trust



Hardware+soft+keys are on the same platform

Mutability
- SD code is immutable

ISD and CASD keys are mutable under Issuer control

Platform can be certified

The owner is the Issuer

Security services are provided

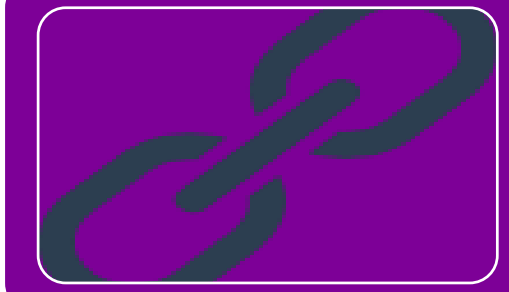
Requirement for GP Secure Elements

Manufacturing Process

- Shall be protected with procedures to protect the chip design, code and keys during fabrication
- If a CASD is present it shall be loaded during the manufacturing phase

Manufacturing Process Certification

- The platform shall be certified to prove the manufacturing process fits the security requirements



Chain of Trust

- All GP components shall implement a Chain of Trust for Confidentiality, Authentication and Integrity

eSIM part of the Device
The automotive case

SAE J3101: A Common Reference for Hardware Protected Security Environments

Basic characteristics

Establish trustworthiness

- device identity
- sealing
- attestation
- data integrity
- availability

Resilience to a wide range of attacks

- beyond software-only security mechanisms.

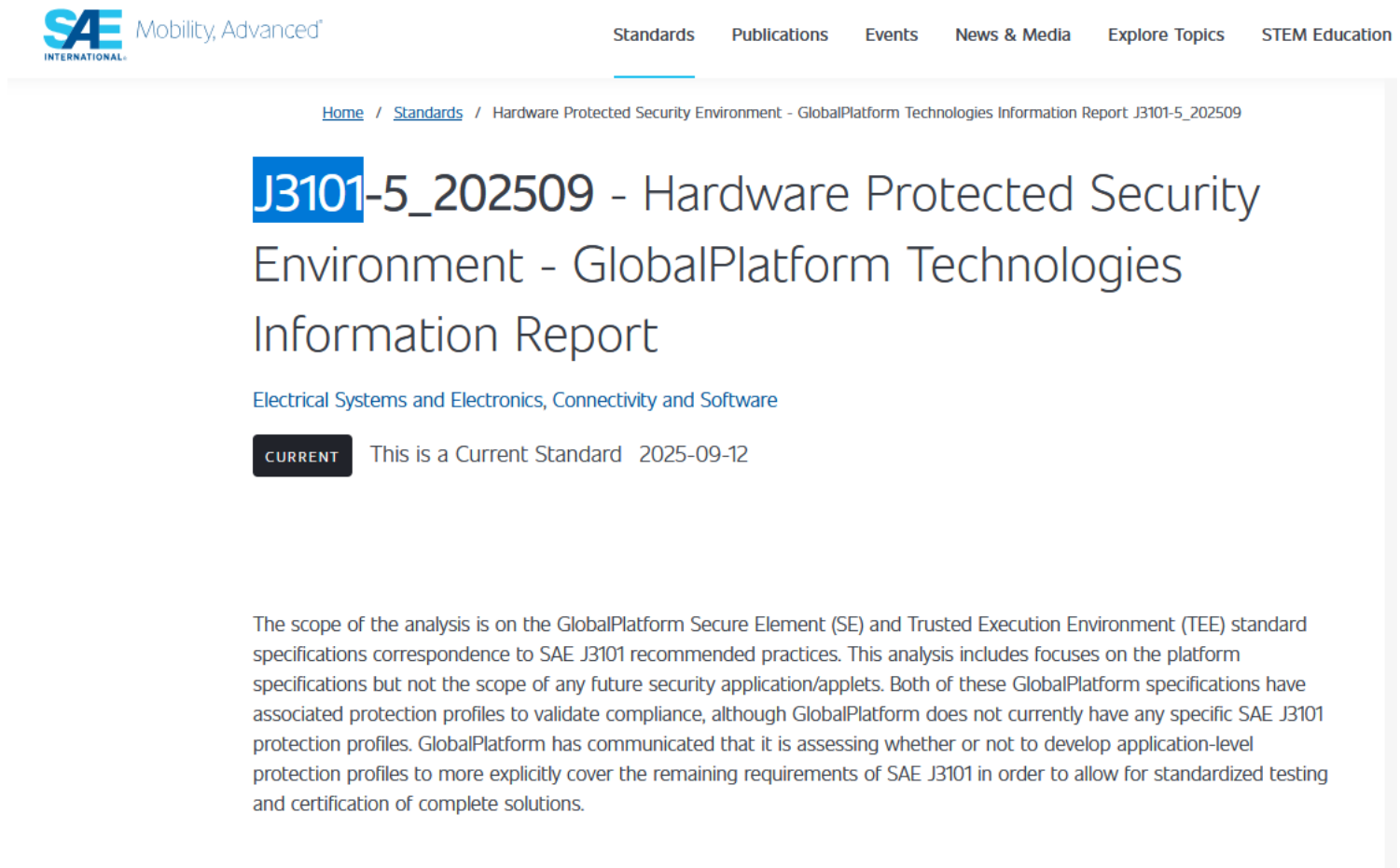
A hardware root of trust

- hardware-based security primitives
- for connected and highly automated or fully automated vehicles.

Requirements

Source: SAE, Surface Vehicle Recommended Practice, *Hardware-Protected Security for Ground Vehicles* (J3101™), Feb 2020. Issued 2020-02.

SAE's Vehicle Electrical System Security Committee – Publication of J3101-5

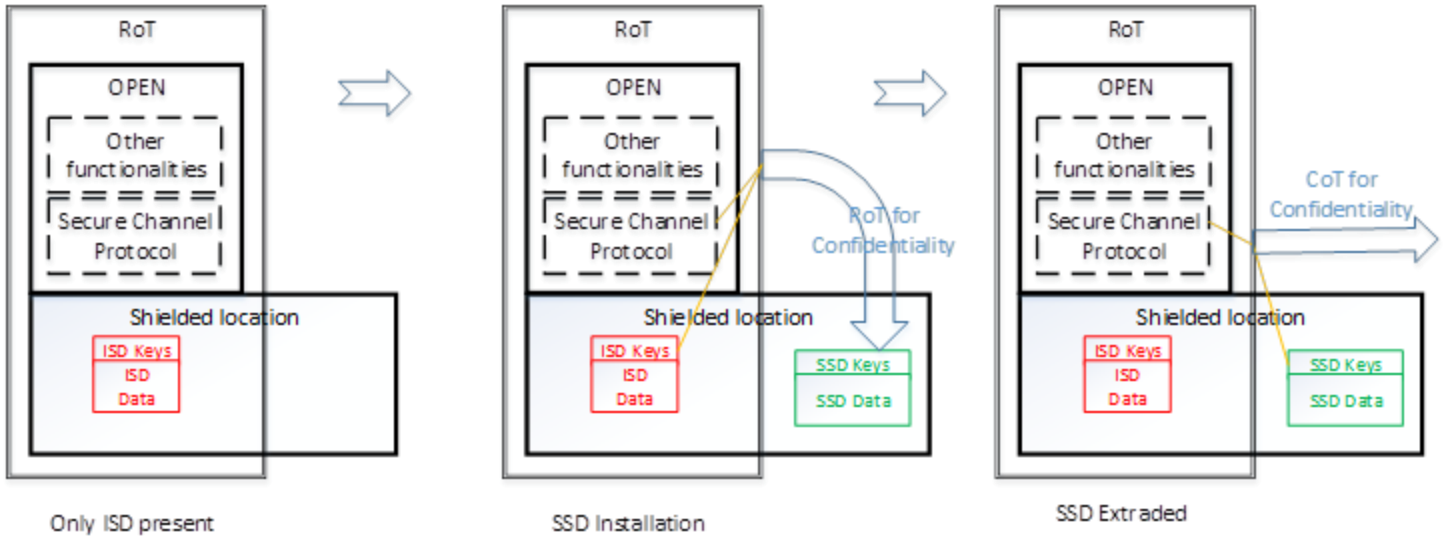


Trust Relationships

4 relationships described

- Bootstrapped RoT
- Chain of Trust (CoT)
  - Anchor in a non-bootstrapped RoT
  - Anchor in a bootstrapped RoT
- CoT of Confidentiality
- Intrinsic Trust

CoT Confidentiality

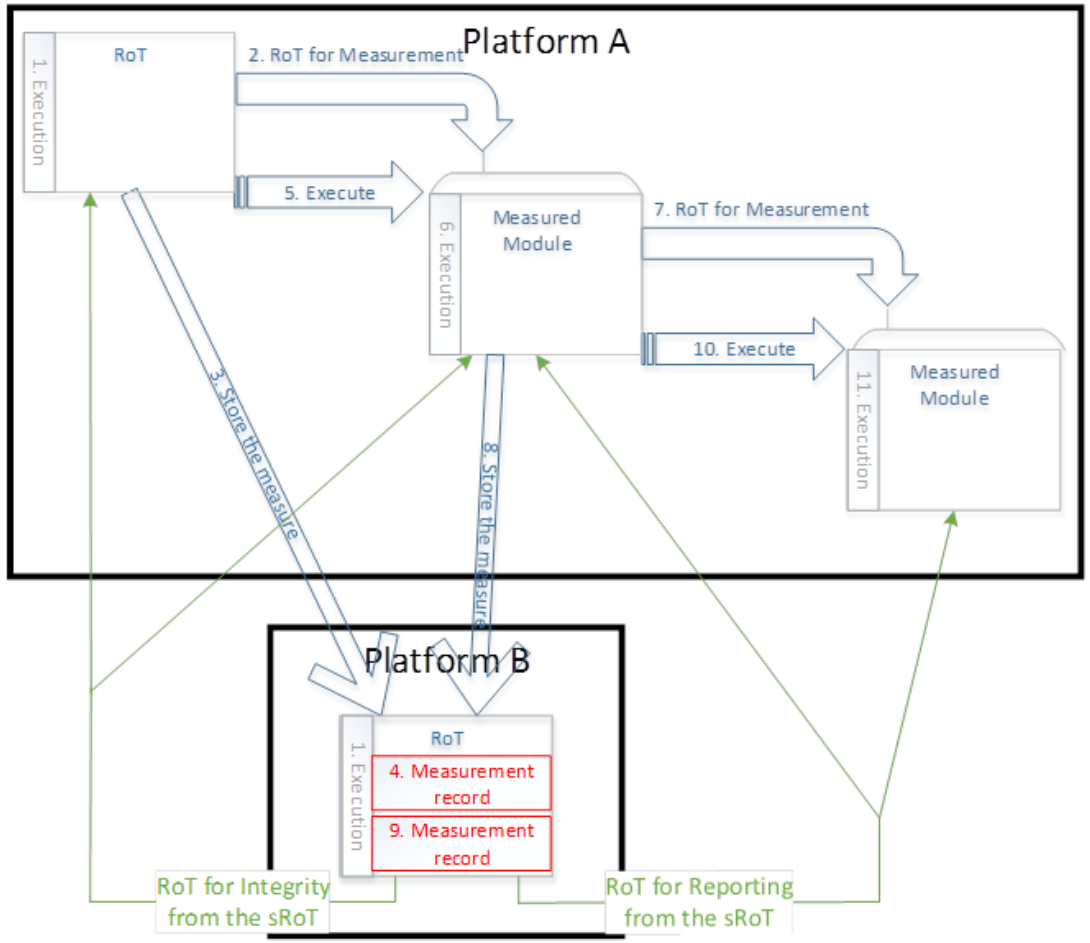


CoT for Confidentiality when new SSD is instantiated.

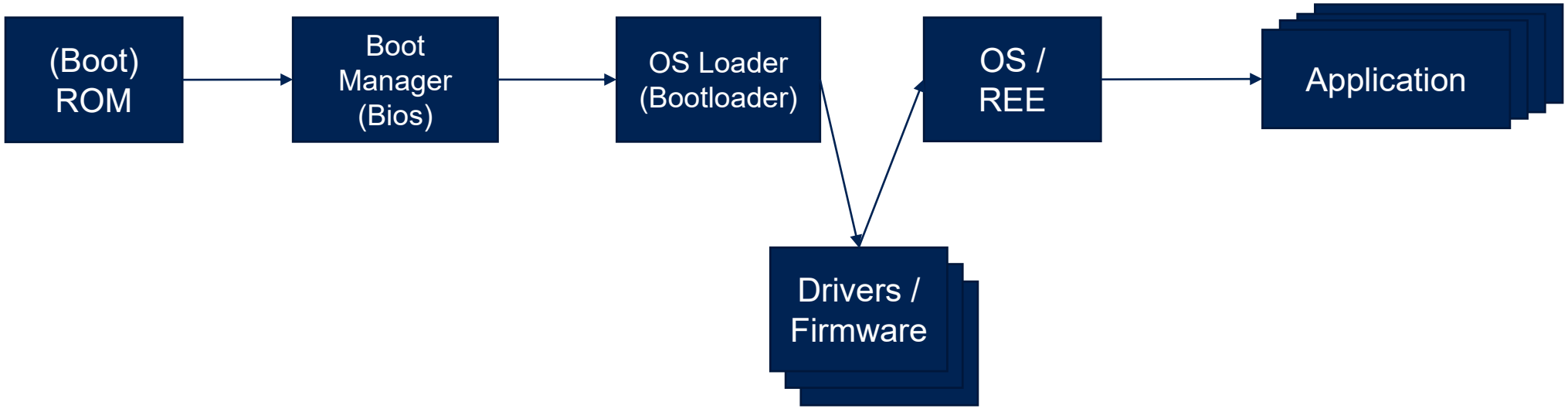
Intrinsic Trust

Relation between two platforms offering RoT functionality where one platform

provides RoT Security Services to another platform.



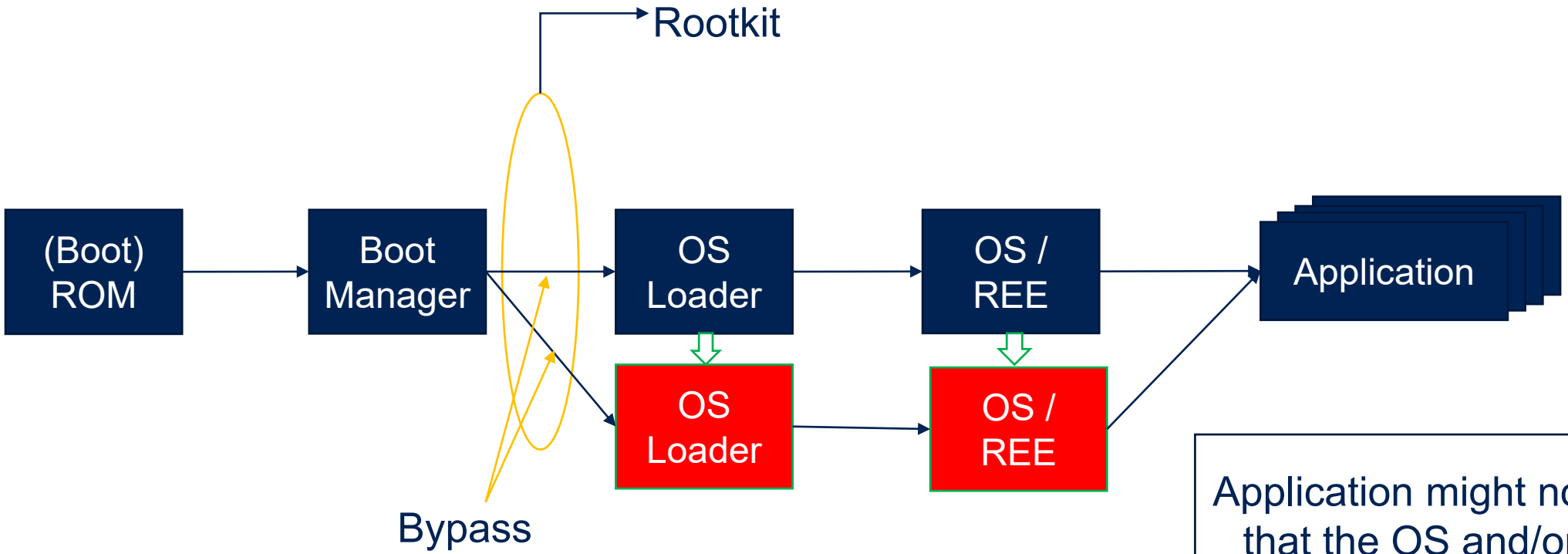
Boot Implementation Example



Rootkit Attack Example

In addition to the malware/virus that may run in the Device OS, a new type of attack

- Rootkit (or bootkit) which starts the OS in a compromised state or replace/change the original operating system with a “rogue” OS



Application might not detect that the OS and/or steps before are compromised

Countermeasure from the RootKit : Secure boot

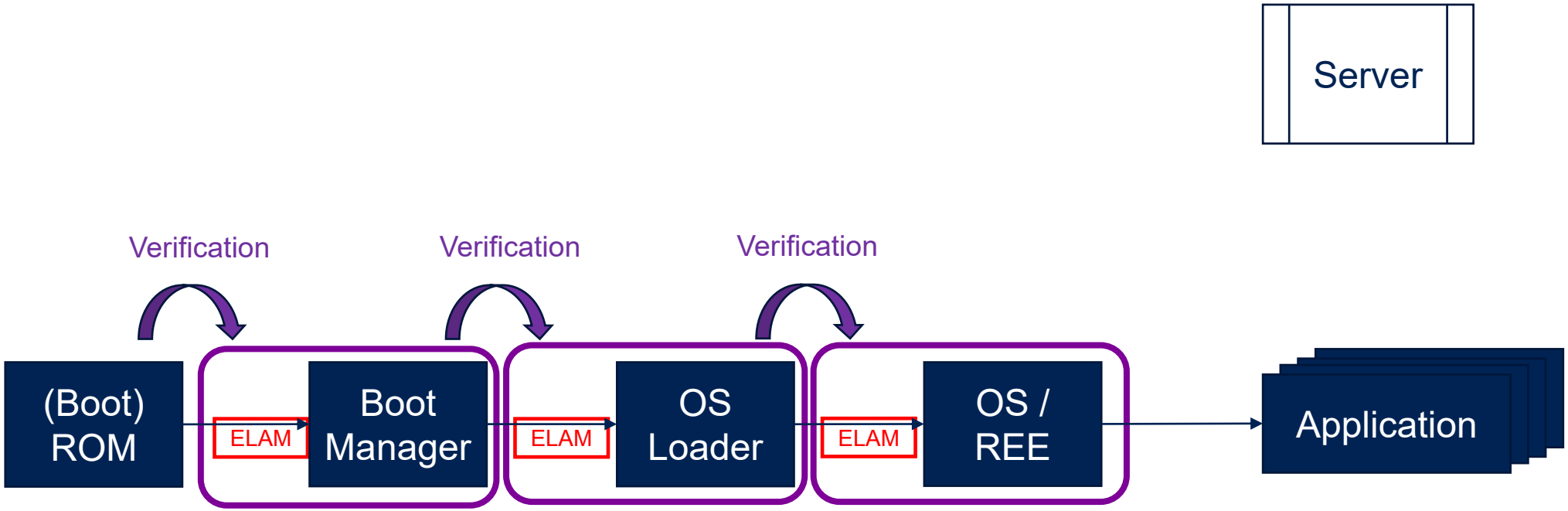
Type of boot processes

- **Trusted boot:** the integrity of every component of the startup process is checked before the OS is started, it may use:
  - **Early Launch Anti-Malware (ELAM):** Test all components before they load and prevents unapproved component from loading
    - If the test succeeds, the boot process goes on
    - If the test fails, the boot process is halted
- **Validated boot:** All modules loaded and executed are tested against a similar approval process as ELAM above. All results are logged for future access. The difference with Trusted Boot is that the boot process does not stop if a test result is negative, it may use:
  - **Measured Boot:** Firmware logs the boot process checking operations

Attestation (Software / Remote)

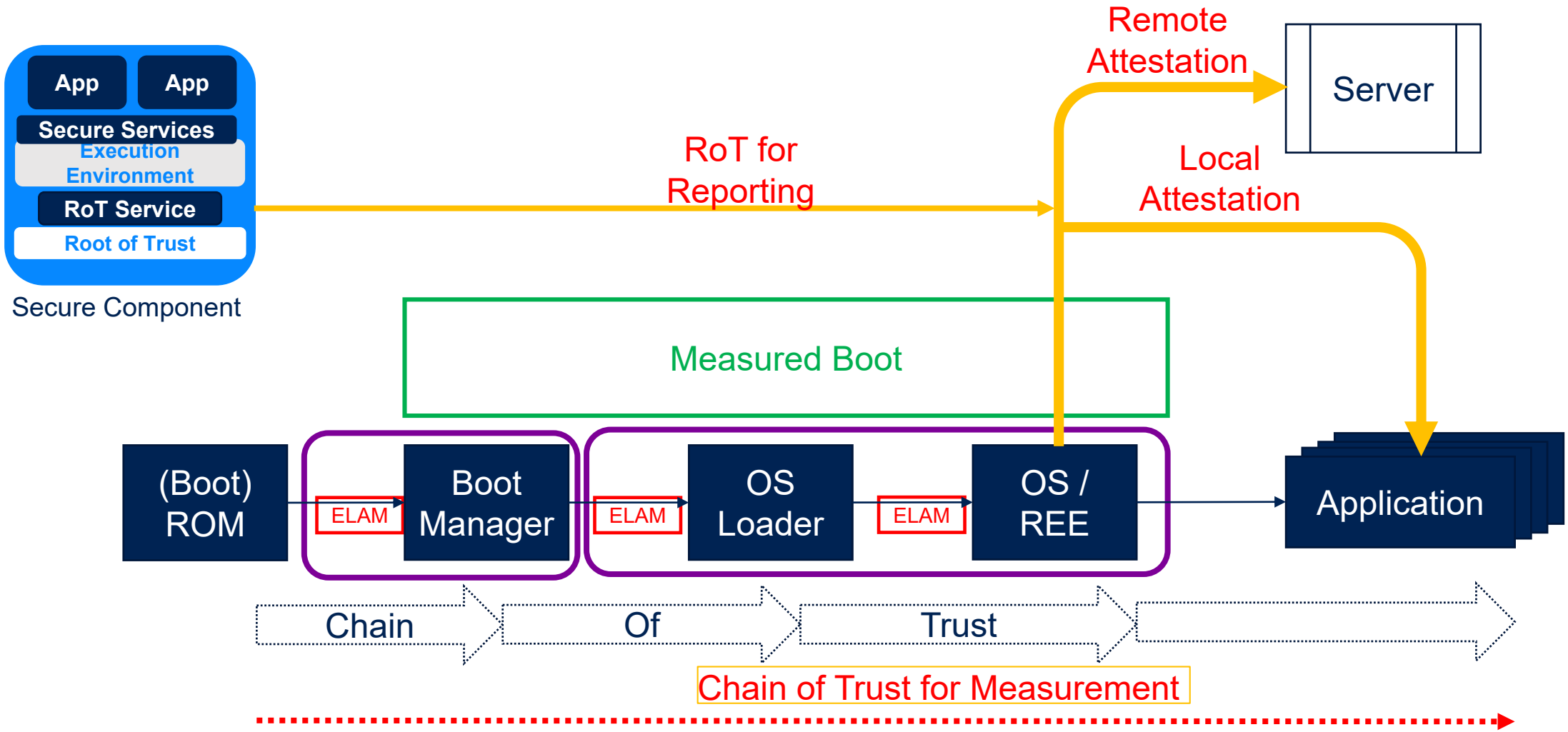
- The OS is able to send the ELAM tests to another local or remote entity for the assessment of the Device's health.

ELAM Implementation Example



Trusted Boot

Implementation Example 3



Global Platform®

Securing the digital future

→globalplatform.org