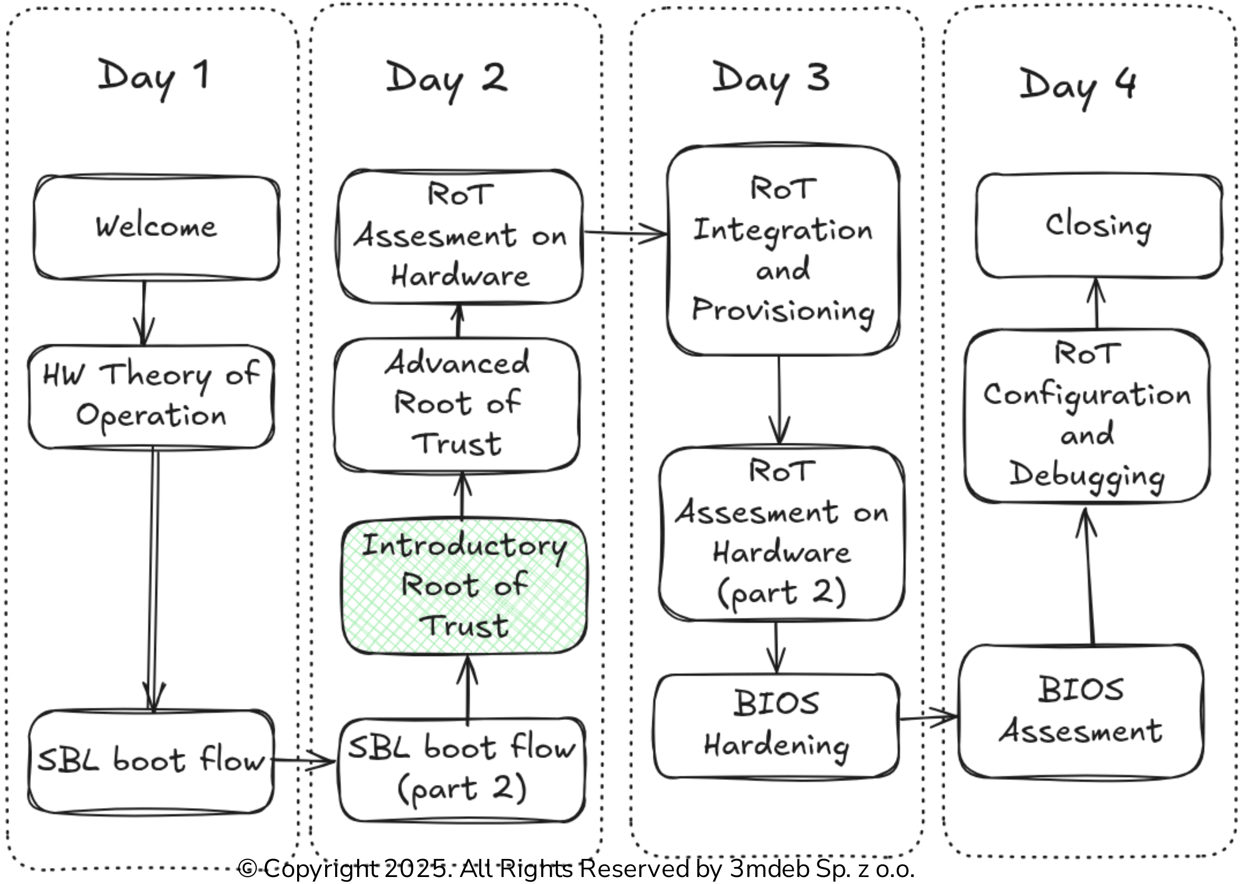
DS09SBL: Dasharo TrustRoot Training

Root of Trust and Chain of Trust Technologies (part 1)

Introductory Root of Trust and Chain of Trust

Where we are in the course



Day 1

Welcome

HW Theory of Operation

SBL boot flow

Day 2

SBL boot flow (part 2)

Introductory Root of Trust

Advanced Root of Trust

RoT Assesment on Hardware

Day 3

RoT Integration and Provisioning

RoT Assesment on Hardware (part 2)

BIOS Hardening

Day 4

BIOS Assesment

RoT Configuration and Debugging

Closing

Goals of the Presentation

In this presentation, we aim to:

- Understand Root of Trust and Chain of Trust Taxonomy and how it applies to Slim Bootloader running on Hardkernel Odroid-H4.

Recap

Recap

- Trust is **assured** reliance on the character, ability, **strength**, or truth of someone or something.

$$\text{Trust} \propto \text{Assurance of Strength} \propto 1 / \text{Skepticism}$$

Recap

- Trust is **assured** reliance on the character, ability, **strength**, or truth of someone or something.

$$\text{Trust} \propto \text{Assurance of Strength} \propto 1 / \text{Skepticism}$$

- System Integrity,

Recap

- Trust is **assured** reliance on the character, ability, **strength**, or truth of someone or something.

$$\text{Trust} \propto \text{Assurance of Strength} \propto 1 / \text{Skepticism}$$

- System Integrity,
- Security Mechanisms,

Recap

- Trust is **assured** reliance on the character, ability, **strength**, or truth of someone or something.

$$\text{Trust} \propto \text{Assurance of Strength} \propto 1 / \text{Skepticism}$$

- System Integrity,
- Security Mechanisms,
- Strength of Mechanism,

Recap

- Trust is **assured** reliance on the character, ability, **strength**, or truth of someone or something.

$$\text{Trust} \propto \text{Assurance of Strength} \propto 1\,/\,\text{Skepticism}$$

- System Integrity,
- Security Mechanisms,
- Strength of Mechanism,
- Software loading into memory,

Recap

- Trust is **assured** reliance on the character, ability, **strength**, or truth of someone or something.

$$\text{Trust} \propto \text{Assurance of Strength} \propto 1 / \text{Skepticism}$$

- System Integrity,
- Security Mechanisms,
- Strength of Mechanism,
- Software loading into memory,
- Software execution on hardware,

Recap

- Trust is **assured** reliance on the character, ability, **strength**, or truth of someone or something.

$$\text{Trust} \propto \text{Assurance of Strength} \propto 1 / \text{Skepticism}$$

- System Integrity,
- Security Mechanisms,
- Strength of Mechanism,
- Software loading into memory,
- Software execution on hardware,
- Load time integrity assessment (aka transitive trust aka chain of trust),

Recap

- Trust is **assured** reliance on the character, ability, **strength**, or truth of someone or something.

$$\text{Trust} \propto \text{Assurance of Strength} \propto 1 / \text{Skepticism}$$

- System Integrity,
- Security Mechanisms,
- Strength of Mechanism,
- Software loading into memory,
- Software execution on hardware,
- Load time integrity assessment (aka transitive trust aka chain of trust),
- Root of Trust.

Training Materials

In VM `$HOME/training_materials/hardware/intel`, you will find a couple of interesting documents that are publicly available but not always easy to find.

- Intel® Trusted Execution Technology (Intel® TXT)
  - `315168_TXT_MLE_DG_rev_017_4-5.pdf`
- Intel ® Converged Security and Management Engine (Intel® CSME) Security
  - `intel-csme-security-white-paper.pdf`

Root of Trust Taxonomies

- Roots of Trust by purpose
- Roots of Trust by establishment time
- Chains of Trust: verified boot and measured boot differences

Root of Trust Taxonomies

- Roots of Trust by purpose
- Roots of Trust by establishment time
- Chains of Trust: verified boot and measured boot differences

Root of Trust Taxonomies

- Roots of Trust by purpose
- Roots of Trust by establishment time
- Chains of Trust: verified boot and measured boot differences

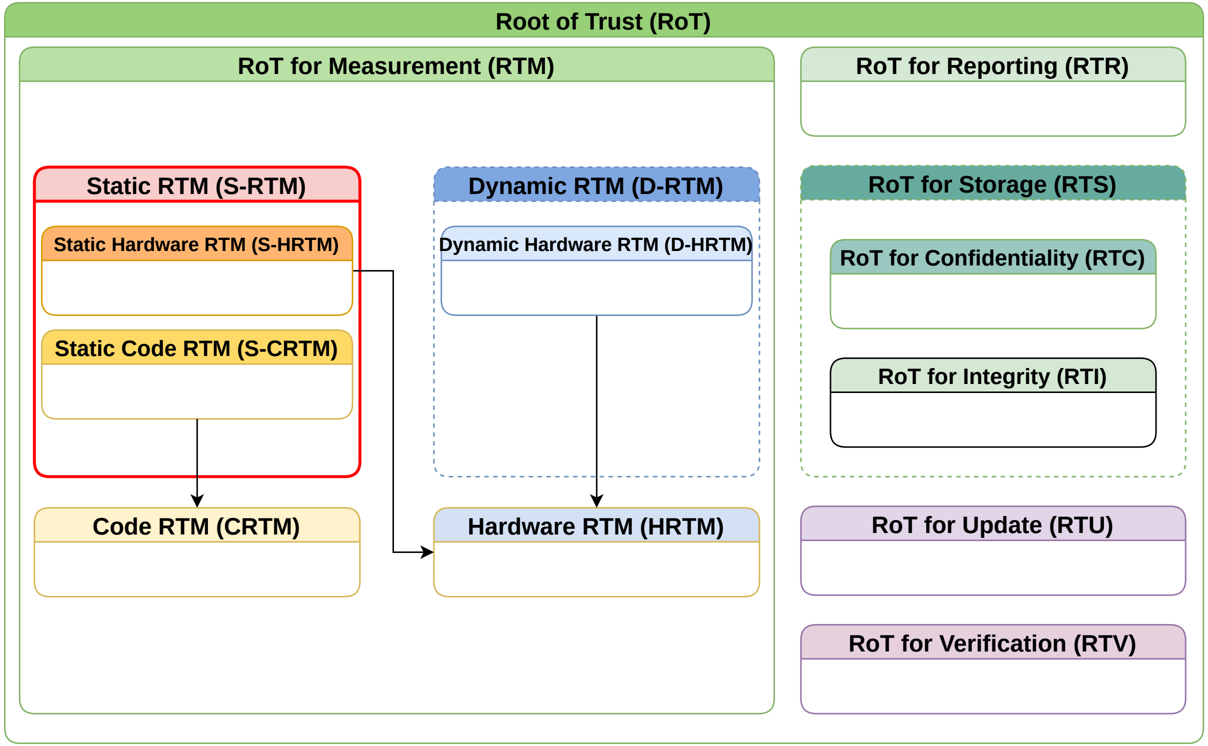
Root of Trust Taxonomies

- Roots of Trust by purpose
- Roots of Trust by establishment time
- Chains of Trust: verified boot and measured boot differences

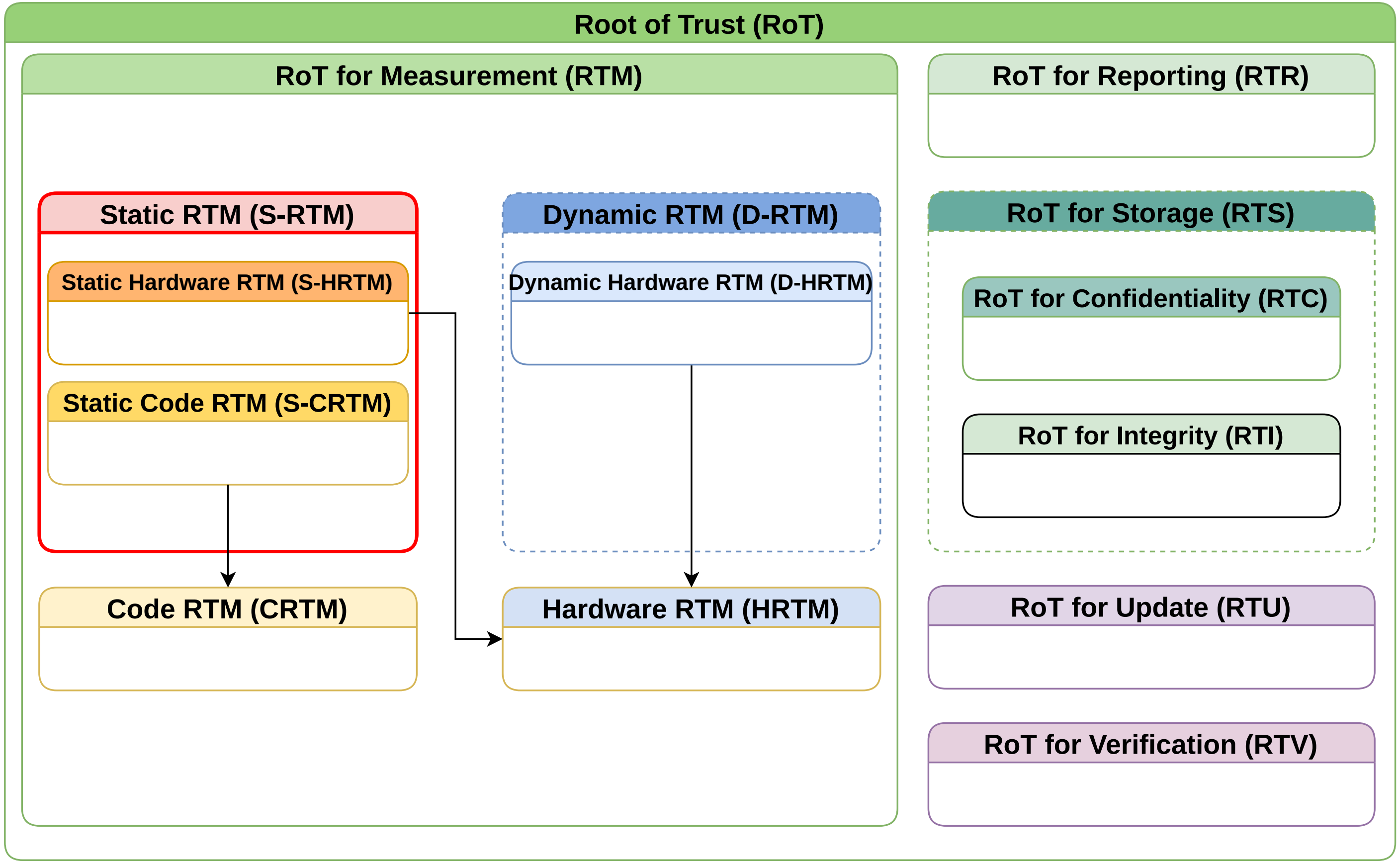
Root of Trust Taxonomies

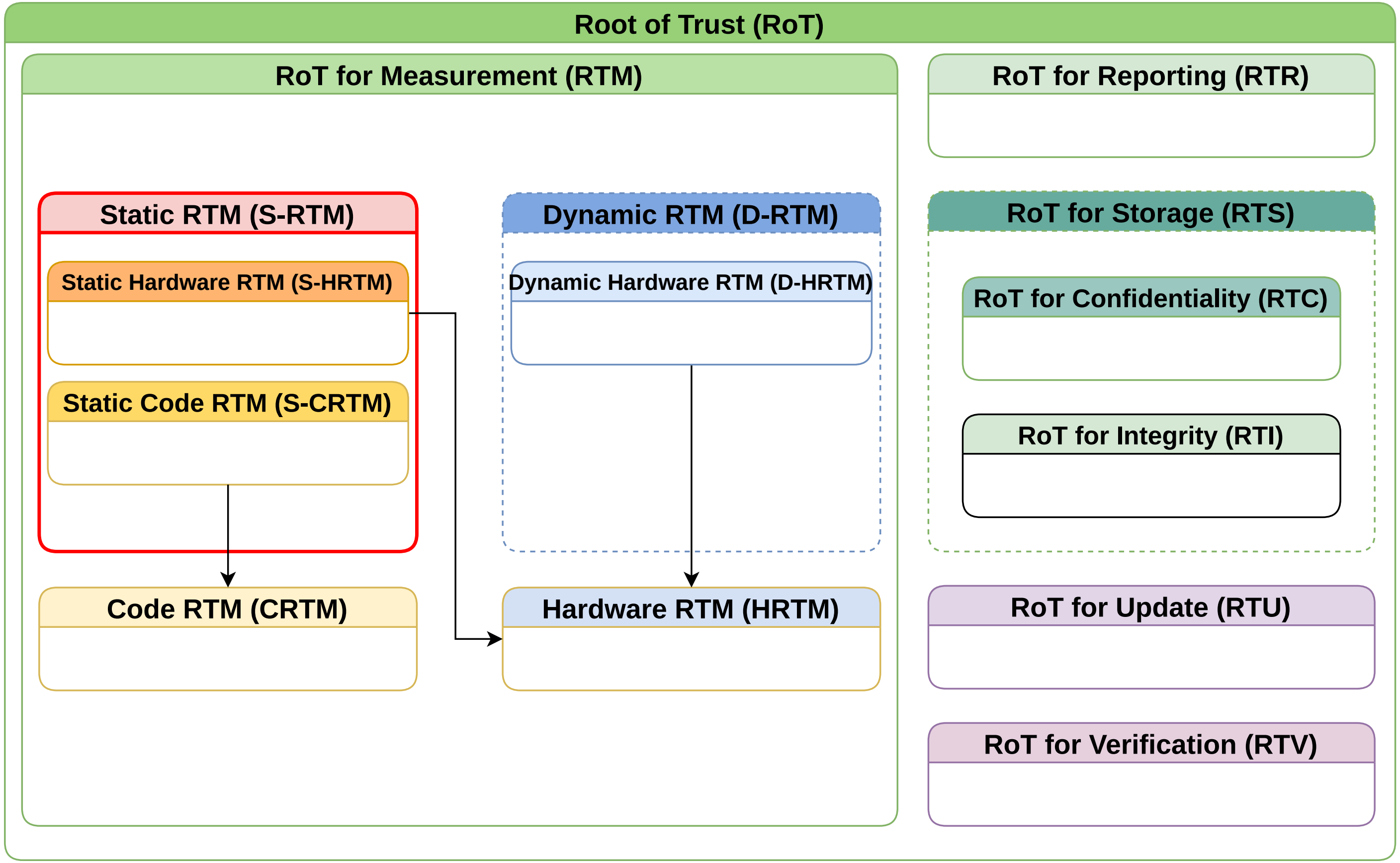
- Roots of Trust by purpose
- Roots of Trust by establishment time
- Chains of Trust: verified boot and measured boot differences

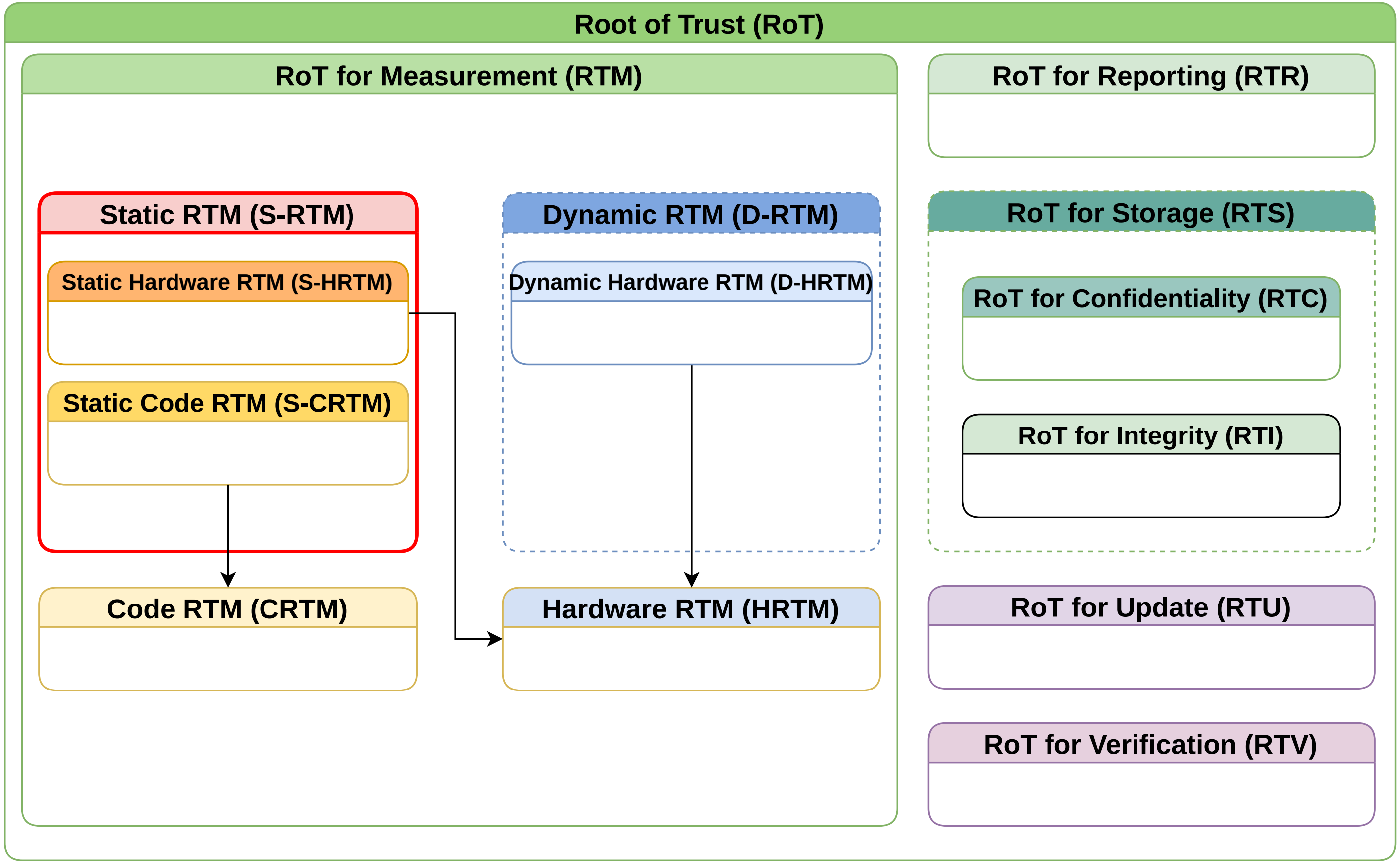
Roots of Trust by purpose

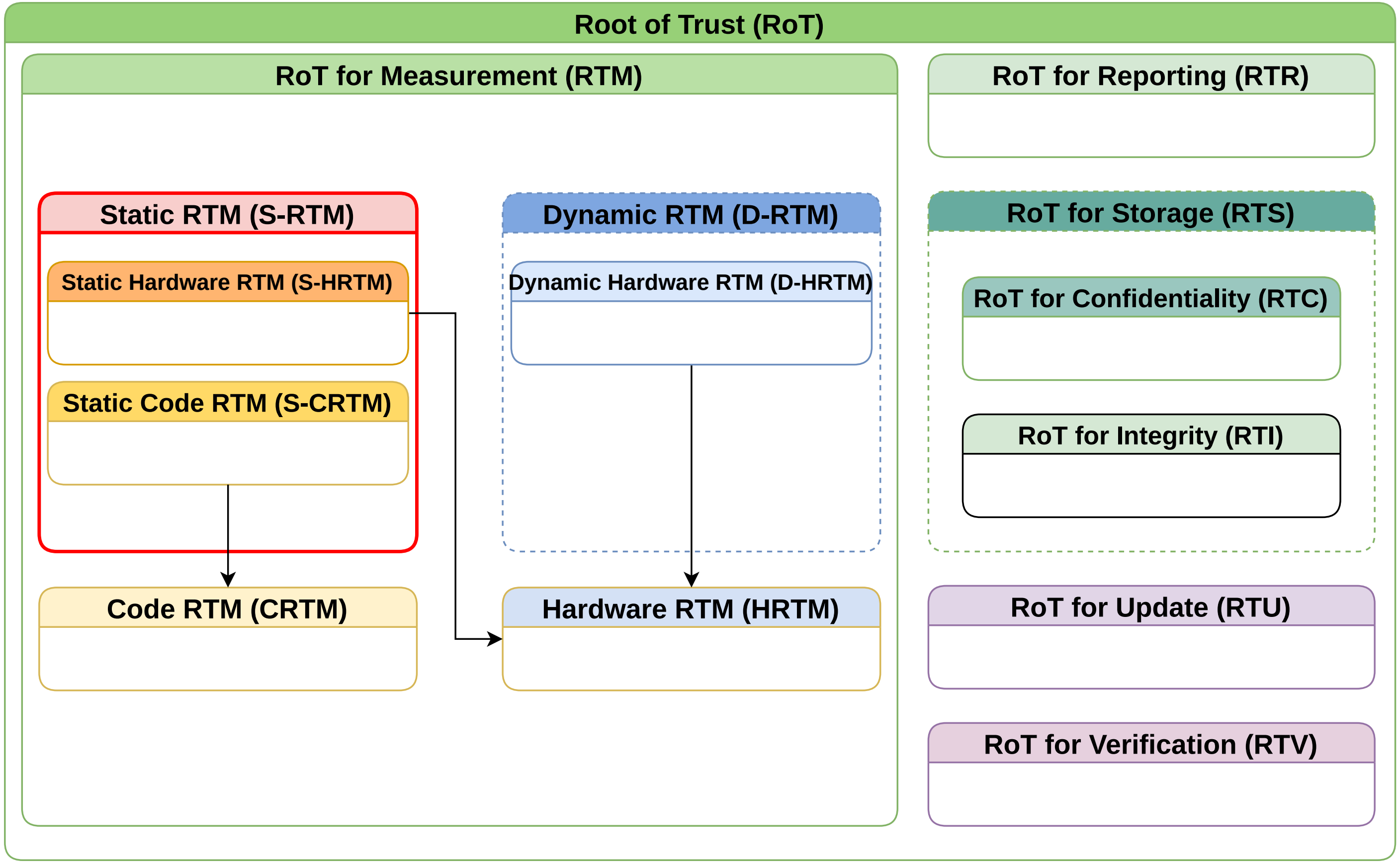


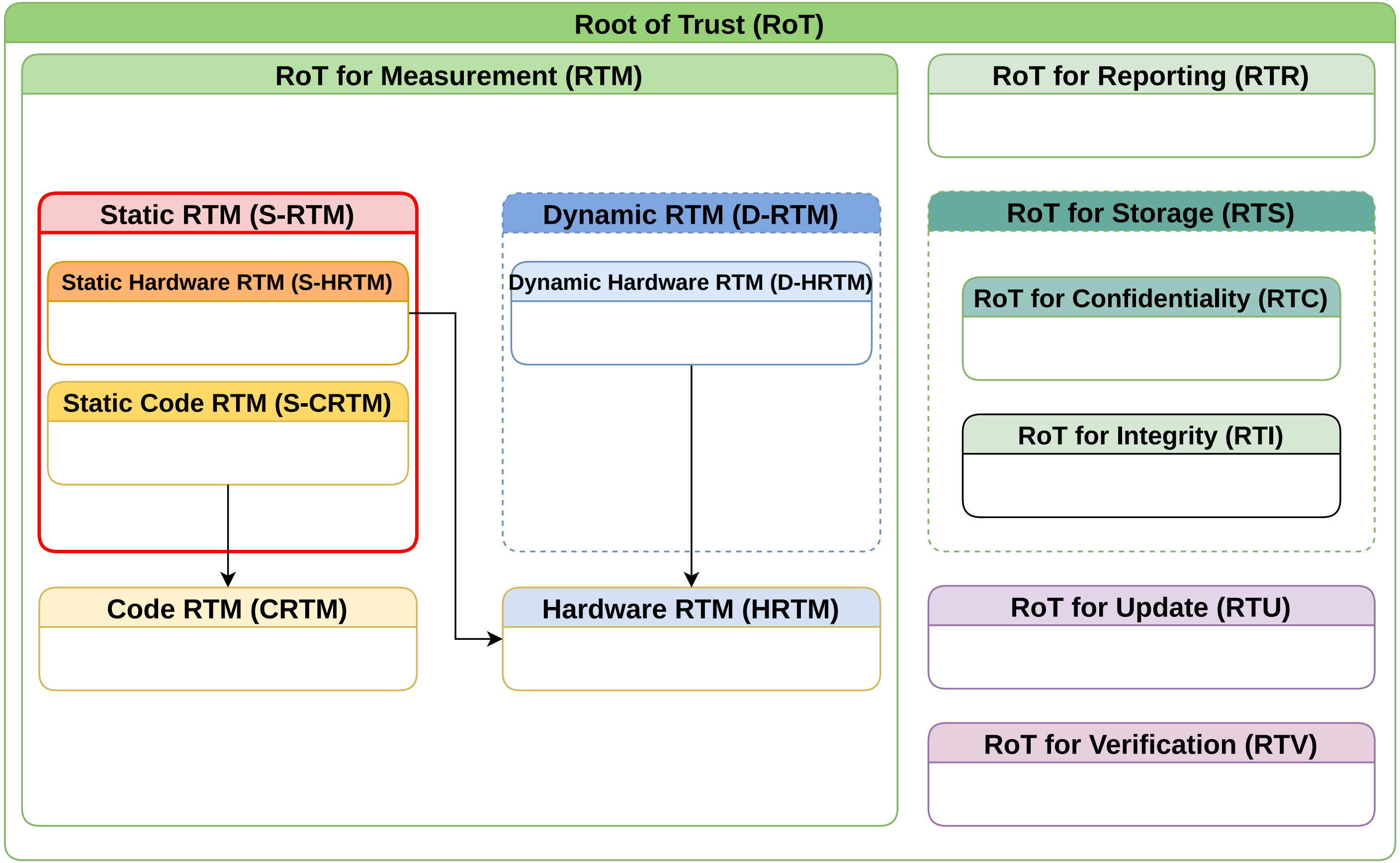
- TCG Specification Architecture Overview rev. 1.4, Section 4.2, Trusted Computing Group,
- Guidelines on hardware-rooted security in mobile devices (Draft), NIST Special Publication 800-164.
- GlobalPlatform Technology Root of Trust Definitions and Requirements Version 1.1

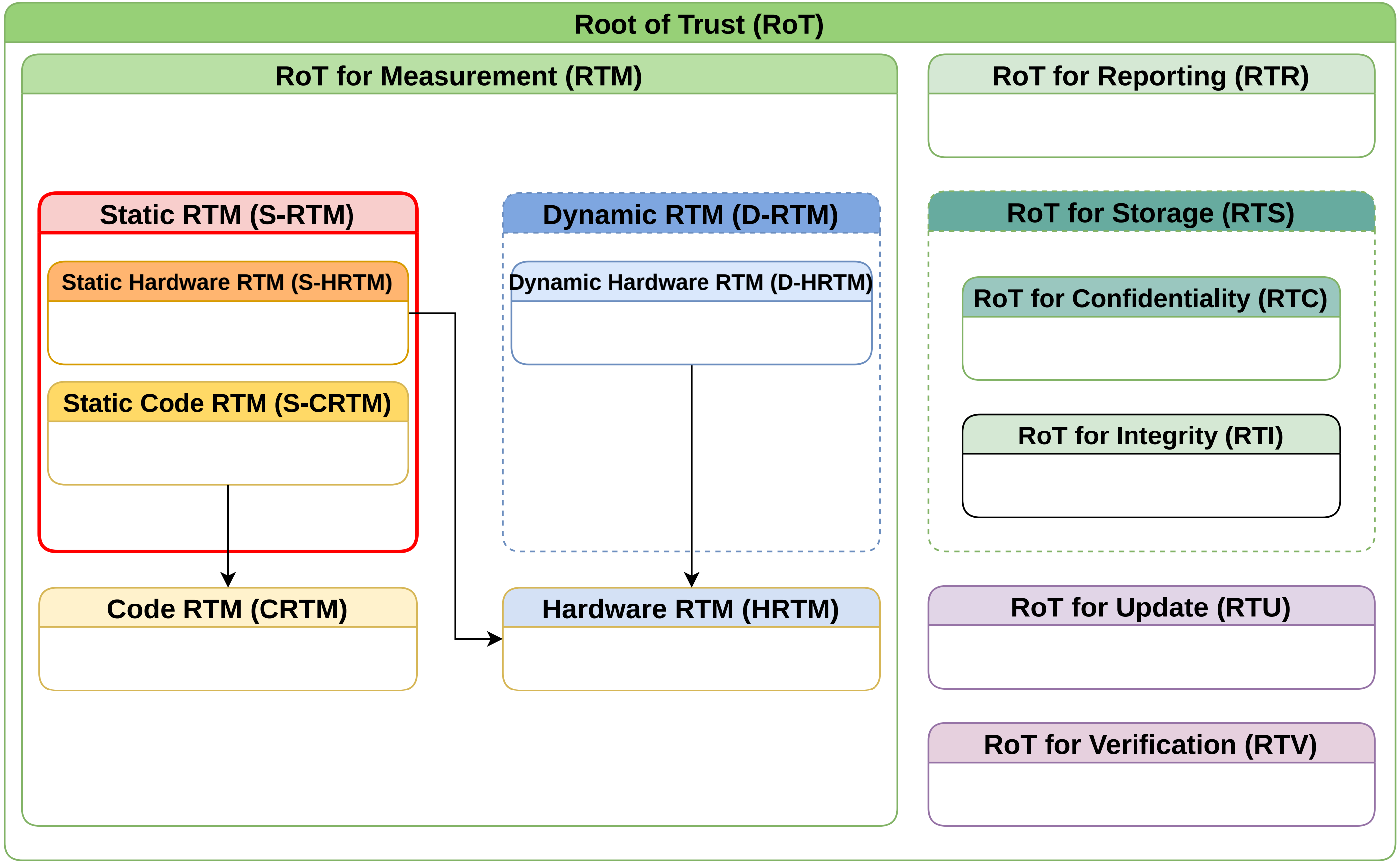

Root of Trust (RoT)
RoT for Measurement (RTM)
Static RTM (S-RTM)
Static Hardware RTM (S-HRTM)
Static Code RTM (S-CRTM)
Dynamic RTM (D-RTM)
Dynamic Hardware RTM (D-HRTM)
Code RTM (CRTM)
Hardware RTM (HRTM)
RoT for Reporting (RTR)
RoT for Storage (RTS)
RoT for Confidentiality (RTC)
RoT for Integrity (RTI)
RoT for Update (RTU)
RoT for Verification (RTV)


Root of Trust (RoT)
RoT for Measurement (RTM)
Static RTM (S-RTM)
Static Hardware RTM (S-HRTM)
Static Code RTM (S-CRTM)
Dynamic RTM (D-RTM)
Dynamic Hardware RTM (D-HRTM)
Code RTM (CRTM)
Hardware RTM (HRTM)
RoT for Reporting (RTR)
RoT for Storage (RTS)
RoT for Confidentiality (RTC)
RoT for Integrity (RTI)
RoT for Update (RTU)
RoT for Verification (RTV)


Root of Trust (RoT)
RoT for Measurement (RTM)
Static RTM (S-RTM)
Static Hardware RTM (S-HRTM)
Static Code RTM (S-CRTM)
Dynamic RTM (D-RTM)
Dynamic Hardware RTM (D-HRTM)
Code RTM (CRTM)
Hardware RTM (HRTM)
RoT for Reporting (RTR)
RoT for Storage (RTS)
RoT for Confidentiality (RTC)
RoT for Integrity (RTI)
RoT for Update (RTU)
RoT for Verification (RTV)


Root of Trust (RoT)
RoT for Measurement (RTM)
Static RTM (S-RTM)
Static Hardware RTM (S-HRTM)
Static Code RTM (S-CRTM)
Dynamic RTM (D-RTM)
Dynamic Hardware RTM (D-HRTM)
Code RTM (CRTM)
Hardware RTM (HRTM)
RoT for Reporting (RTR)
RoT for Storage (RTS)
RoT for Confidentiality (RTC)
RoT for Integrity (RTI)
RoT for Update (RTU)
RoT for Verification (RTV)


Root of Trust (RoT)
RoT for Measurement (RTM)
Static RTM (S-RTM)
Static Hardware RTM (S-HRTM)
Static Code RTM (S-CRTM)
Dynamic RTM (D-RTM)
Dynamic Hardware RTM (D-HRTM)
Code RTM (CRTM)
Hardware RTM (HRTM)
RoT for Reporting (RTR)
RoT for Storage (RTS)
RoT for Confidentiality (RTC)
RoT for Integrity (RTI)
RoT for Update (RTU)
RoT for Verification (RTV)



Root of Trust (RoT)

RoT for Measurement (RTM)

Static RTM (S-RTM)

Static Hardware RTM (S-HRTM)

Static Code RTM (S-CRTM)

Dynamic RTM (D-RTM)

Dynamic Hardware RTM (D-HRTM)

Code RTM (CRTM)

Hardware RTM (HRTM)

RoT for Reporting (RTR)

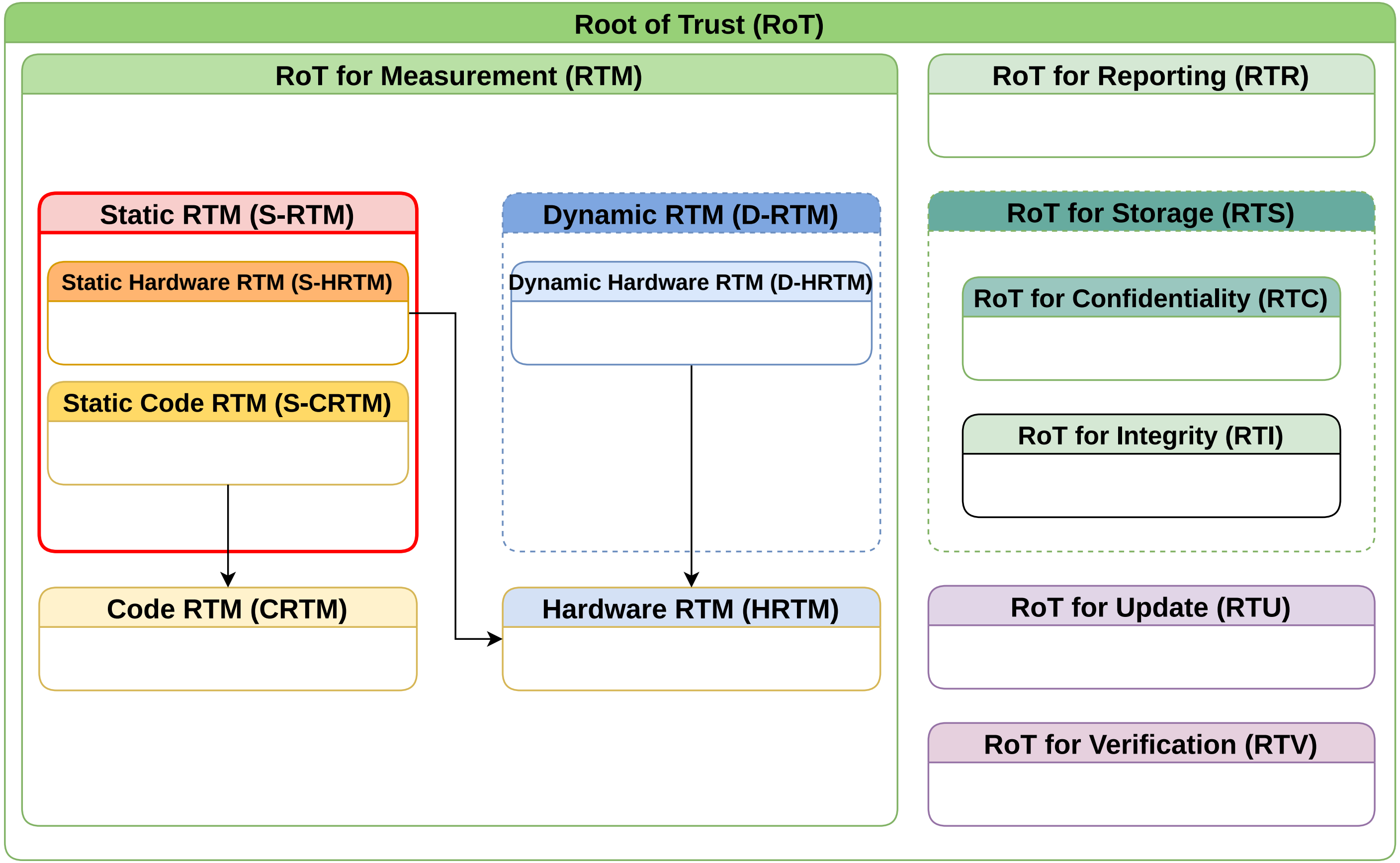
RoT for Storage (RTS)

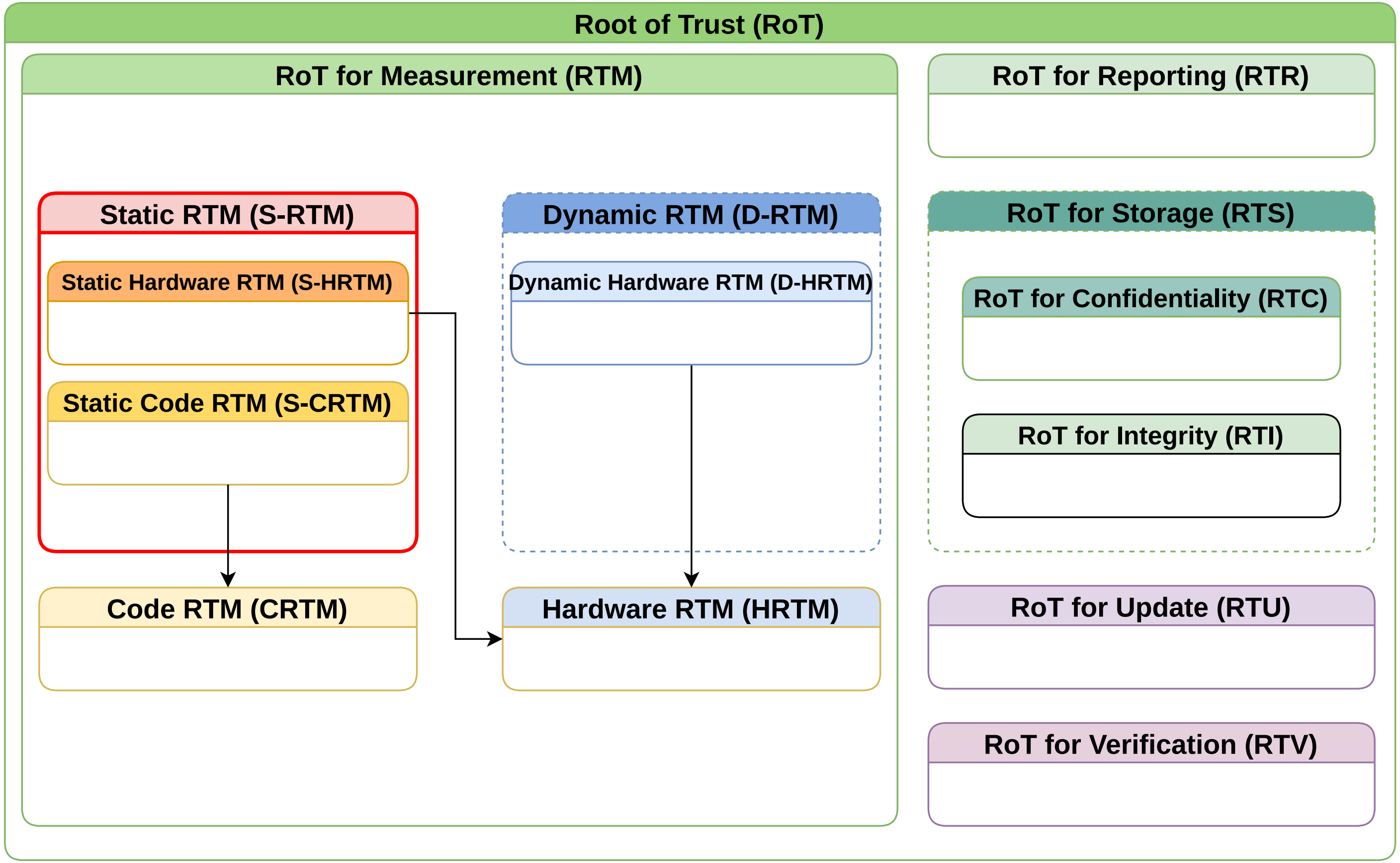
RoT for Confidentiality (RTC)

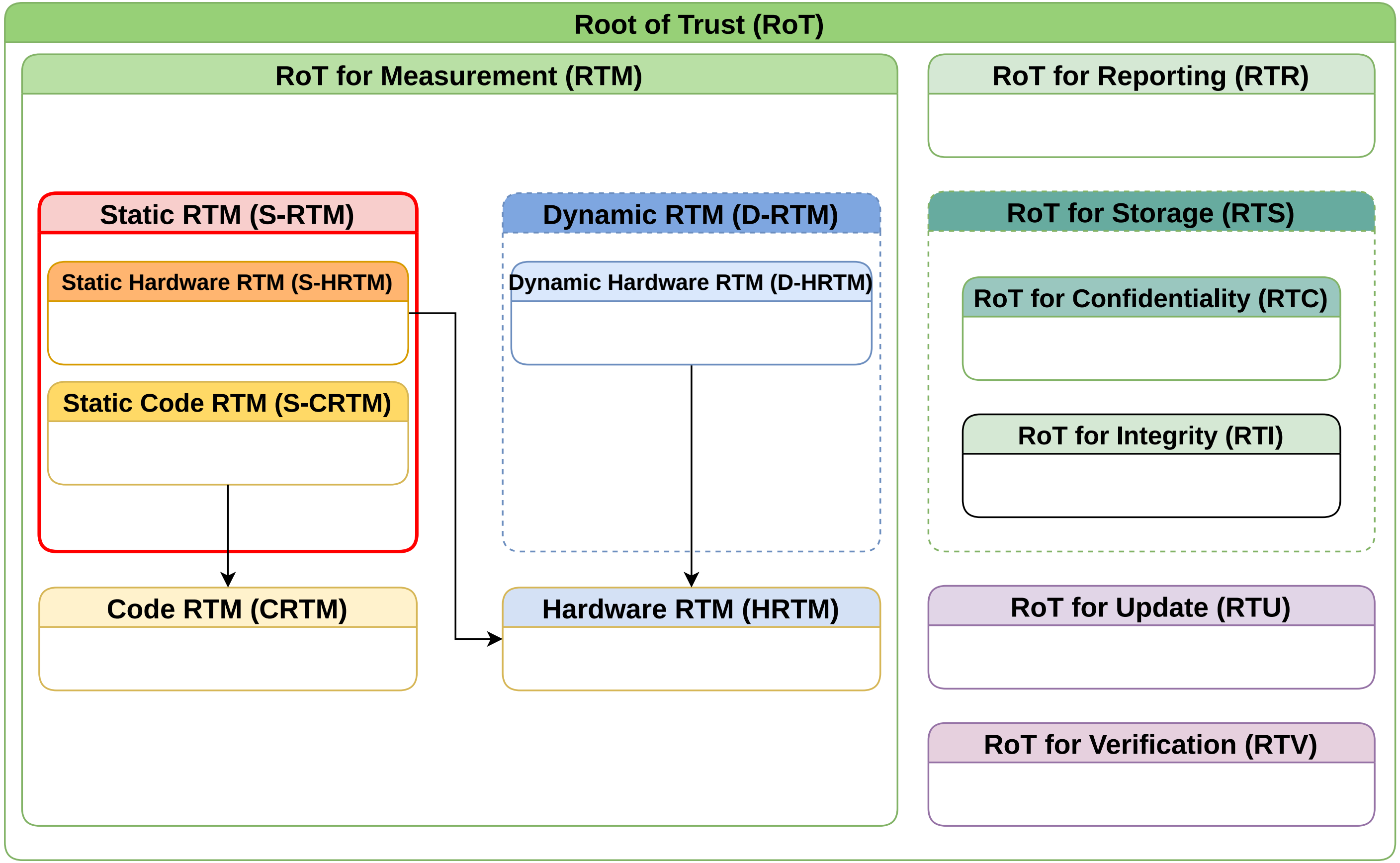
RoT for Integrity (RTI)

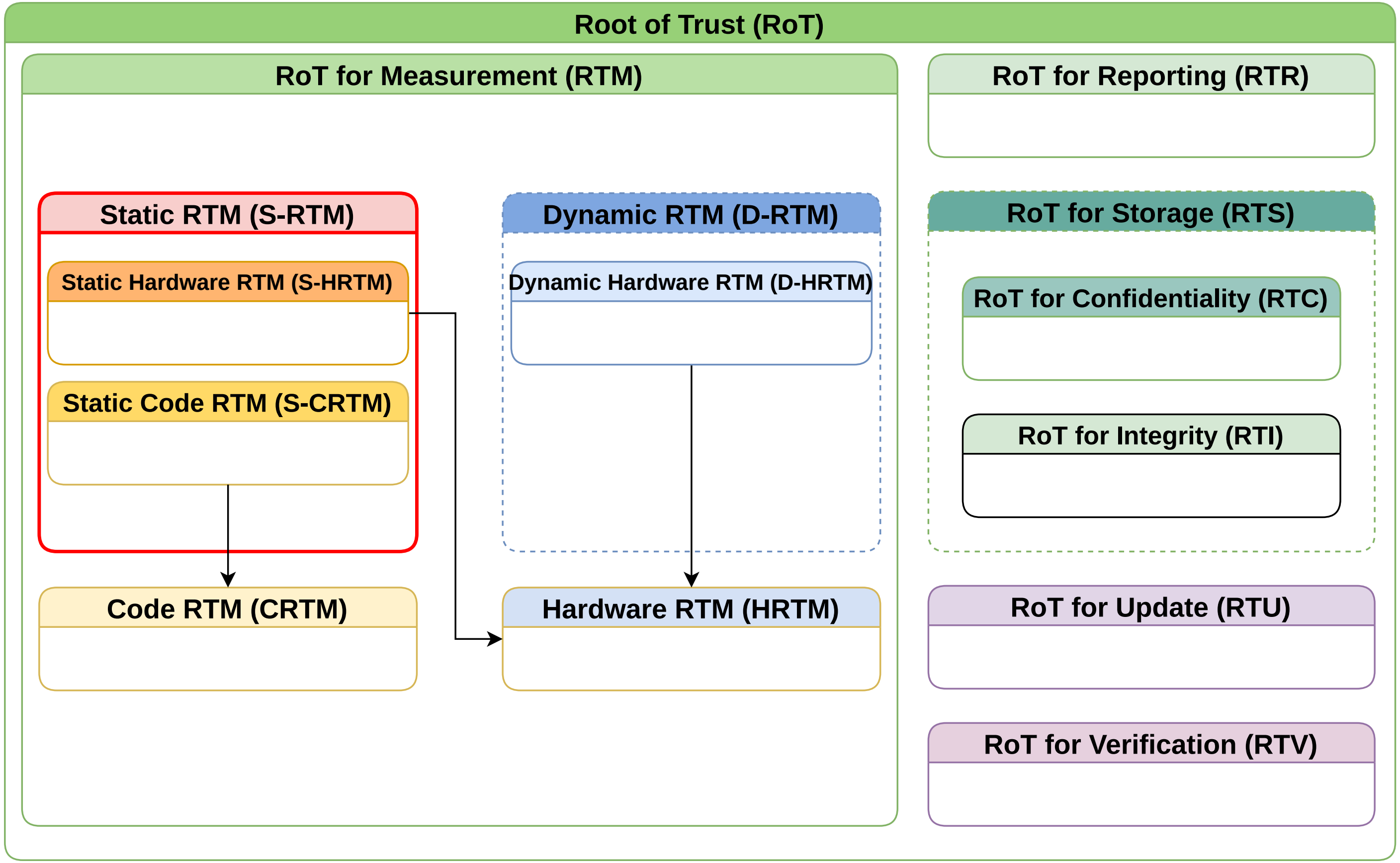
RoT for Update (RTU)

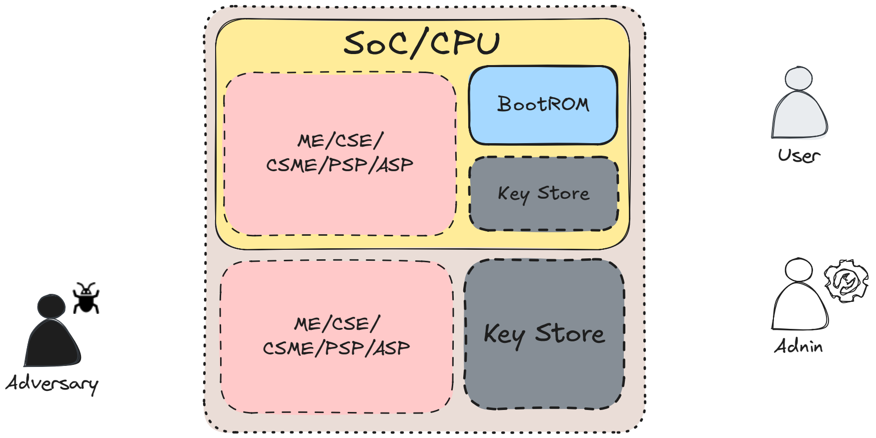
RoT for Verification (RTV)


Root of Trust (RoT)
RoT for Measurement (RTM)
Static RTM (S-RTM)
Static Hardware RTM (S-HRTM)
Static Code RTM (S-CRTM)
Dynamic RTM (D-RTM)
Dynamic Hardware RTM (D-HRTM)
Code RTM (CRTM)
Hardware RTM (HRTM)
RoT for Reporting (RTR)
RoT for Storage (RTS)
RoT for Confidentiality (RTC)
RoT for Integrity (RTI)
RoT for Update (RTU)
RoT for Verification (RTV)


Root of Trust (RoT)
RoT for Measurement (RTM)
RoT for Reporting (RTR)
Static RTM (S-RTM)
Static Hardware RTM (S-HRTM)
Static Code RTM (S-CRTM)
Dynamic RTM (D-RTM)
Dynamic Hardware RTM (D-HRTM)
RoT for Storage (RTS)
RoT for Confidentiality (RTC)
RoT for Integrity (RTI)
Code RTM (CRTM)
Hardware RTM (HRTM)
RoT for Update (RTU)
RoT for Verification (RTV)


Root of Trust (RoT)
RoT for Measurement (RTM)
Static RTM (S-RTM)
Static Hardware RTM (S-HRTM)
Static Code RTM (S-CRTM)
Dynamic RTM (D-RTM)
Dynamic Hardware RTM (D-HRTM)
Code RTM (CRTM)
Hardware RTM (HRTM)
RoT for Reporting (RTR)
RoT for Storage (RTS)
RoT for Confidentiality (RTC)
RoT for Integrity (RTI)
RoT for Update (RTU)
RoT for Verification (RTV)


Root of Trust (RoT)
RoT for Measurement (RTM)
Static RTM (S-RTM)
Static Hardware RTM (S-HRTM)
Static Code RTM (S-CRTM)
Dynamic RTM (D-RTM)
Dynamic Hardware RTM (D-HRTM)
Code RTM (CRTM)
Hardware RTM (HRTM)
RoT for Reporting (RTR)
RoT for Storage (RTS)
RoT for Confidentiality (RTC)
RoT for Integrity (RTI)
RoT for Update (RTU)
RoT for Verification (RTV)



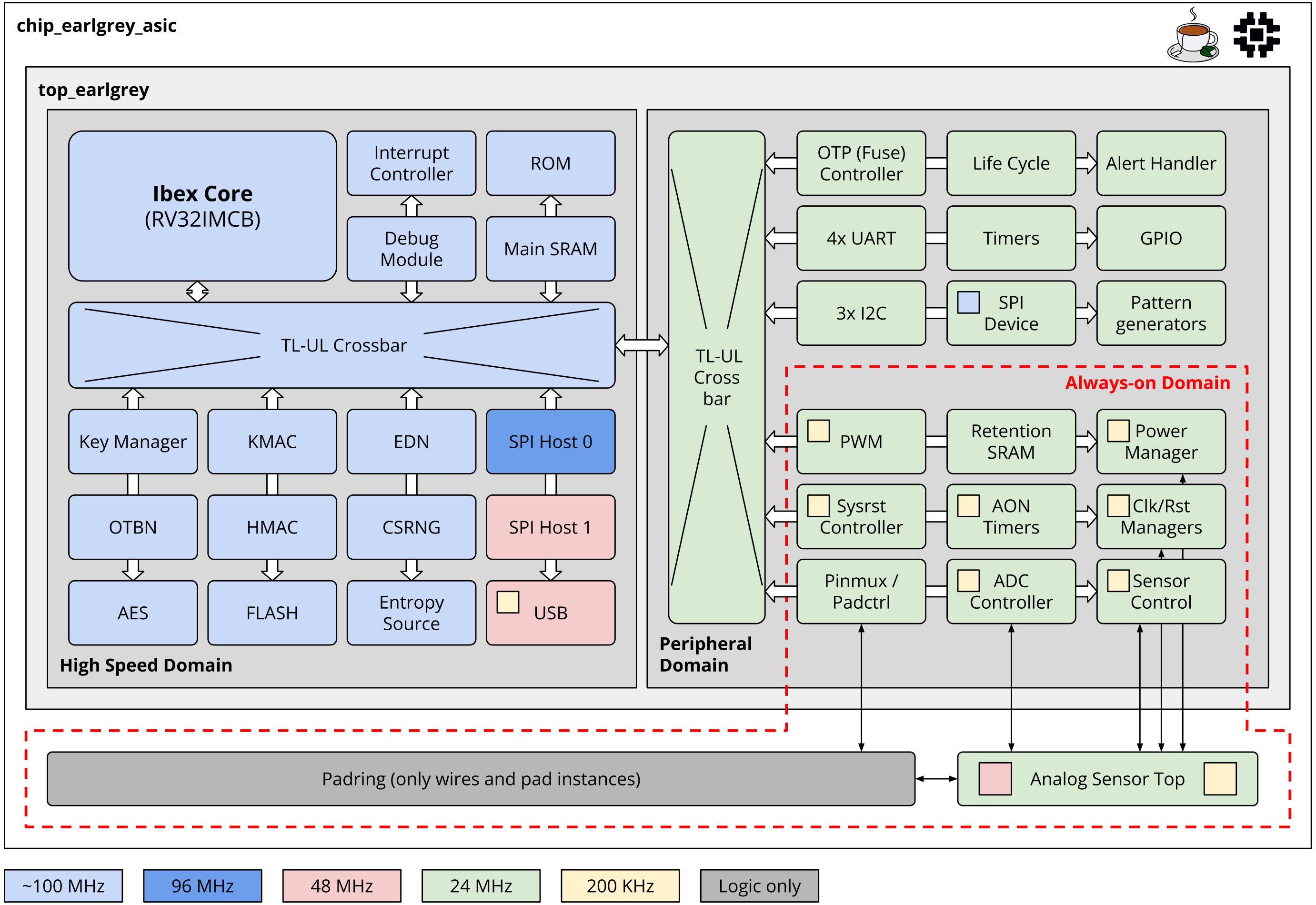
> **Quote**
>
> It executes the signature verification algorithm and has access to a key store that includes the public key needed to verify a signature. This key store may be stored internally by the RTV, or it may rely on an RTS to protect and maintain the key store.

source: *NIST SP800-164*

opentitan

- OpenTitan is an open-source project creating reference designs and integration guidelines for RoT chips
- Partners include Google, lowRISC, ETH Zurich, G+D Mobile Security, Nuvoton and Western Digital
- It aims to make silicon RoT technology more possible and more secure by creating open-source designs.
- Derived from Google Titan technology.
- BYORoT (Bring Your Own Root of Trust) approach.

source: OpenTitan - open sourcing transparent, trustworthy, and secure silicon



chip_earlgrey_asic

top_earlgrey

Ibex Core
(RV32IMCB)

Interrupt Controller

ROM

Debug Module

Main SRAM

TL-UL Crossbar

Key Manager

KMAC

EDN

SPI Host 0

OTBN

HMAC

CSRNG

SPI Host 1

AES

FLASH

Entropy Source

USB

High Speed Domain

TL-UL Cross bar

OTP (Fuse) Controller

Life Cycle

Alert Handler

4x UART

Timers

GPIO

3x I2C

SPI Device

Pattern generators

Always-on Domain

PWM

Retention SRAM

Power Manager

Sysrst Controller

AON Timers

Clk/Rst Managers

Pinmux / Padctrl

ADC Controller

Sensor Control

Peripheral Domain

Padring (only wires and pad instances)

Analog Sensor Top

~100 MHz

96 MHz

48 MHz

24 MHz

200 KHz

Logic only

Caliptra

- Caliptra consists of IP and firmware for an integrated Root of Trust block.
- Caliptra targets datacenter-class SoCs like CPUs, GPUs, DPUs, and TPUs. It is the specification, silicon logic, ROM, and firmware for implementing a Root of Trust for Measurement (RTM) block inside an SoC. A Caliptra integration provides the SoC with Identity, Measured Boot and Attestation capabilities.
- Caliptra’s source code is available on GitHub under the CHIPS Alliance Project, which is under the wings of Linux Foundation.
  - It is Apache-2.0 licensed.
- Founded by Microsoft, Google and AMD.

Caliptra

- Caliptra consists of IP and firmware for an integrated Root of Trust block.
- Caliptra targets datacenter-class SoCs like CPUs, GPUs, DPUs, and TPUs. It is the specification, silicon logic, ROM, and firmware for implementing a Root of Trust for Measurement (RTM) block inside an SoC. A Caliptra integration provides the SoC with Identity, Measured Boot and Attestation capabilities.
- Caliptra's source code is available on GitHub under the CHIPS Alliance Project, which is under the wings of Linux Foundation.
  - It is Apache-2.0 licensed.
- Founded by Microsoft, Google and AMD.

Caliptra

- Caliptra consists of IP and firmware for an integrated Root of Trust block.
- Caliptra targets datacenter-class SoCs like CPUs, GPUs, DPUs, and TPUs. It is the specification, silicon logic, ROM, and firmware for implementing a Root of Trust for Measurement (RTM) block inside an SoC. A Caliptra integration provides the SoC with Identity, Measured Boot and Attestation capabilities.
- Caliptra's source code is available on GitHub under the CHIPS Alliance Project, which is under the wings of Linux Foundation.
  - It is Apache-2.0 licensed.
- Founded by Microsoft, Google and AMD.

Caliptra

- Caliptra consists of IP and firmware for an integrated Root of Trust block.
- Caliptra targets datacenter-class SoCs like CPUs, GPUs, DPUs, and TPUs. It is the specification, silicon logic, ROM, and firmware for implementing a Root of Trust for Measurement (RTM) block inside an SoC. A Caliptra integration provides the SoC with Identity, Measured Boot and Attestation capabilities.
- Caliptra's source code is available on GitHub under the CHIPS Alliance Project, which is under the wings of Linux Foundation.
  - It is Apache-2.0 licensed.
- Founded by Microsoft, Google and AMD.

Caliptra

- Caliptra consists of IP and firmware for an integrated Root of Trust block.
- Caliptra targets datacenter-class SoCs like CPUs, GPUs, DPUs, and TPUs. It is the specification, silicon logic, ROM, and firmware for implementing a Root of Trust for Measurement (RTM) block inside an SoC. A Caliptra integration provides the SoC with Identity, Measured Boot and Attestation capabilities.
- Caliptra’s source code is available on GitHub under the CHIPS Alliance Project, which is under the wings of Linux Foundation.
  - It is Apache-2.0 licensed.
- Founded by Microsoft, Google and AMD.

- Root of Trust for Measurement
  - The open-source implementation of Caliptra drives transparency into the RTM and measurement mechanism that anchors hardware attestation.
  - Exposes a "TCG DICE-as-a-Service".
- Root of Trust for Identity
  - Responsibility:
    - boot the SoC,
    - measure the mutable code it loads,
    - measure and control mutation of non-volatile configuration bits,
    - report measurements with signed attestations rooted in unique per-asset cryptographic entropy,

Quote

Often we see[...] great security[...] compromised by other great ideas for mgmt and other things[...] starts to weaken its security posture[...] want to keep Caliptra very clean via OSS firmware transparency

Bryan Kelly

source: Caliptra: A Datacenter System on a Chip (SOC) Root of Trust (RoT)

Quiz

Quiz

What does RTM mean?

Quiz

What does RTM mean?

- Root of Trust for Measurement

Quiz

What does RTM mean?

- Root of Trust for Measurement

What does RTV mean?

Quiz

What does RTM mean?

- Root of Trust for Measurement

What does RTV mean?

- Root of Trust for Verification

Quiz

What does RTM mean?

- Root of Trust for Measurement

What does RTV mean?

- Root of Trust for Verification

What root of trust Intel Boot Guard implements?

Quiz

What does RTM mean?

- Root of Trust for Measurement

What does RTV mean?

- Root of Trust for Verification

What root of trust Intel Boot Guard implements?

- Root of Trust for Verification and Static Code Root of Trust for Measurement.

Quiz

What does RTM mean?

- Root of Trust for Measurement

What does RTV mean?

- Root of Trust for Verification

What root of trust Intel Boot Guard implements?

- Root of Trust for Verification and Static Code Root of Trust for Measurement.

What are the benefits of RoT implementation like OpenTitan or OCP Caliptra?

Quiz

What does RTM mean?

- Root of Trust for Measurement

What does RTV mean?

- Root of Trust for Verification

What root of trust Intel Boot Guard implements?

- Root of Trust for Verification and Static Code Root of Trust for Measurement.

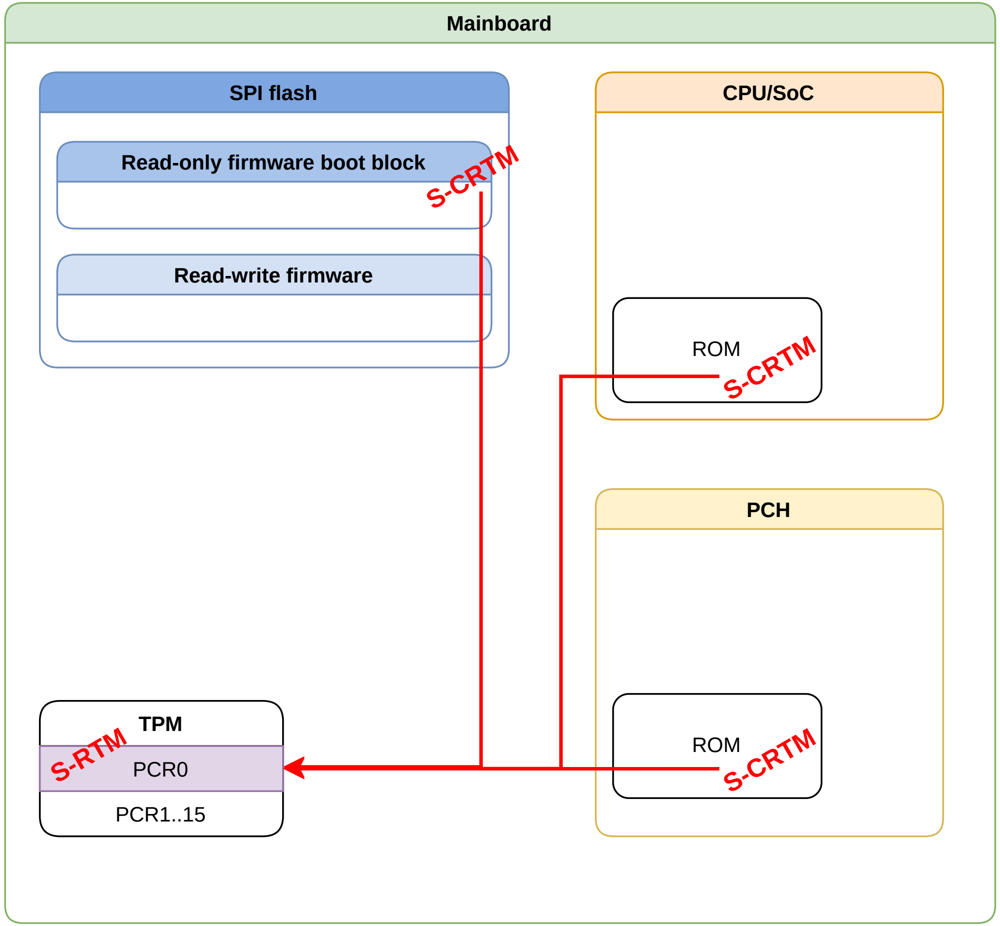
What are the benefits of RoT implementation like OpenTitan or OCP Caliptra?

- Openness, state of the art modern design, pave path for industry standardization of RoT.

Roots of Trust by establishment time

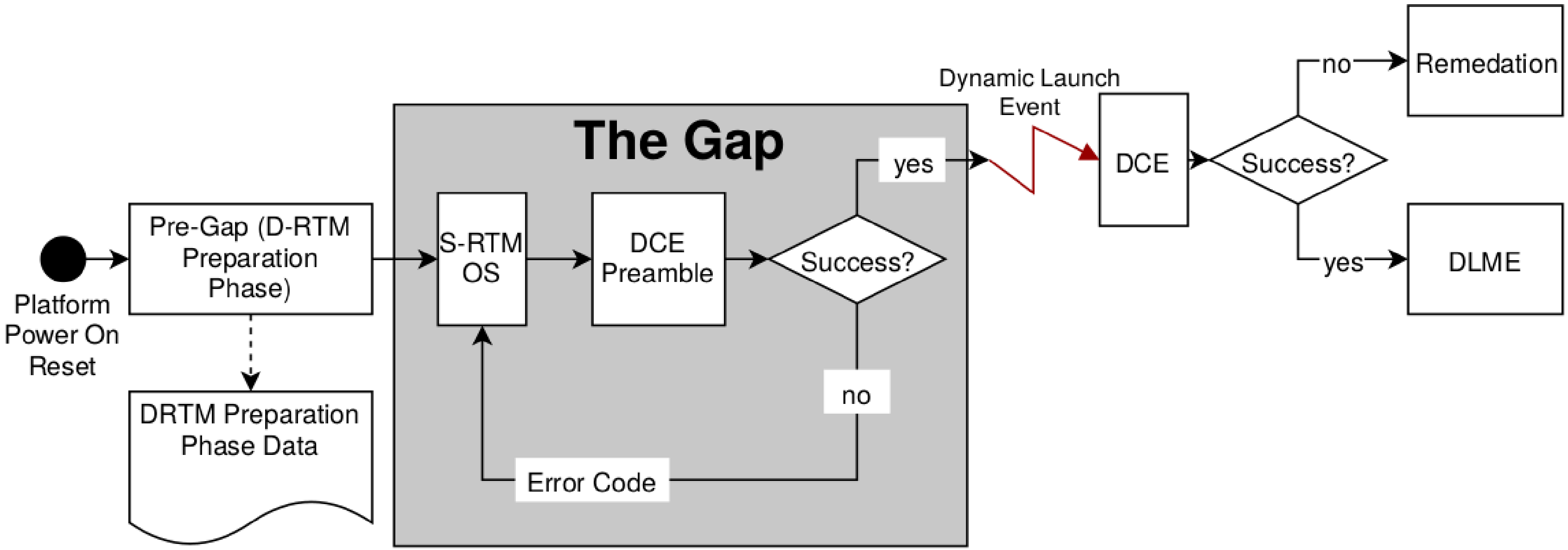
S-RTM

- **Static Root of Trust for Measurement** - established at a fixed point in time typically, platform reset
  - it can be implemented as code or as hardware
  - is the mechanism mutable or immutable?
- S-RTM is as good as code/hardware making initial measurement
- Initial measurement protection (Silicon Vendor Security Technologies):
  - Intel Boot Guard, AMD HVB/PSB, NXP HAB, Rockchip Secure Boot etc.
- Local attestation: coreboot+TrustedGRUB2, Dasharo+LUKS2, Microsoft BitLocker
- Problems
  - requires a reboot to re-establish trust
  - requires NDA with SV and skilled personnel to protect initial measurement
  - most hardware vendors do not implement it correctly
  - not standardized measurement information (event log)
  - complexity: over 20 keys involved (~5 just for Intel Boot Guard)


Mainboard
SPI flash
Read-only firmware boot block
S-CRTM
Read-write firmware
CPU/SoC
ROM
S-CRTM
PCH
ROM
S-CRTM
TPM
S-RTM
PCR0
PCR1..15

Dynamic Root of Trust for Measurement

- **Dynamic Root of Trust for Measurement** - established at an arbitrary point in time through a dedicated mechanism (e.g. CPU instruction)
  - it can be implemented as code or as hardware
- It was standardized according to the TCG D-RTM Architecture specification.
- Currently, most active development related to the implementation of D-RTM technology in FOSS is TrenchBoot.
  - TrenchBoot goal is to upstream support for D-RTM for all FOSS relevant projects, starting with Linux kernel, GRUB2 bootloader, Xen, there is even some preliminary work on coreboot.
- Microsoft leverage D-RTM technology under System Guard.
- There are multiple hardware specific standards discussing and publications discussing D-RTM:
  - Intel® Trusted Execution Technology (Intel® TXT)
  - Intel Software Developers Manual - chapter 7
  - AMD Architecture Programmer’s Manual - chapter 15.27
  - DRTM Architecture for Arm



source: TCG D-RTM Architecture

How that applies to our use case?

- We should always start analysis from CPU microarchitecture we trying to secure.
- Microarchitecture documentation should define platform on which it can be integrated, what defines security properties and potential mechanisms which can be used.
- Our target platform is Intel Alder Lake N, but following applies to all modern Intel-based platforms.
    - Intel Boot Guard serves as Root of Trust for Verification (RTV) as well as Static Code Root of Trust for Measurement (S-CRTM).
    - Intel Boot Guard is not related or dependent on firmware stack, but its properties may align better of worse with some implementations.
    - Intel Boot Guard implementations differ slightly between microarchitectures (number eFuse slots, ability to transfer ownership, tooling).
    - Intel Boot Guard is responsible for validation of Initial Boot Block (IBB), further chain of trust (transitive trust) continuation depends on firmware stack.

Chain of Trust

Chain of Trust Taxonomy

- Based on function:
  - Chain of Trust for Detection (CTD)
  - Chain of Trust for Recovery (CTRec)
  - Chain of Trust for Update (CTU)
- Based on method of transitive trust:
  - Measured Boot (integrity)
  - Verified Boot (authenticity, integrity)

Chain of Trust Taxonomy

- Based on function:
  - Chain of Trust for Detection (CTD)
  - Chain of Trust for Recovery (CTRec)
  - Chain of Trust for Update (CTU)
- Based on method of transitive trust:
  - Measured Boot (integrity)
  - Verified Boot (authenticity, integrity)

Chain of Trust Taxonomy

- Based on function:
    - Chain of Trust for Detection (CTD)
    - Chain of Trust for Recovery (CTRec)
    - Chain of Trust for Update (CTU)
- Based on method of transitive trust:
    - Measured Boot (integrity)
    - Verified Boot (authenticity, integrity)

Chain of Trust Taxonomy

- Based on function:
  - Chain of Trust for Detection (CTD)
  - Chain of Trust for Recovery (CTRec)
  - Chain of Trust for Update (CTU)
- Based on method of transitive trust:
  - Measured Boot (integrity)
  - Verified Boot (authenticity, integrity)

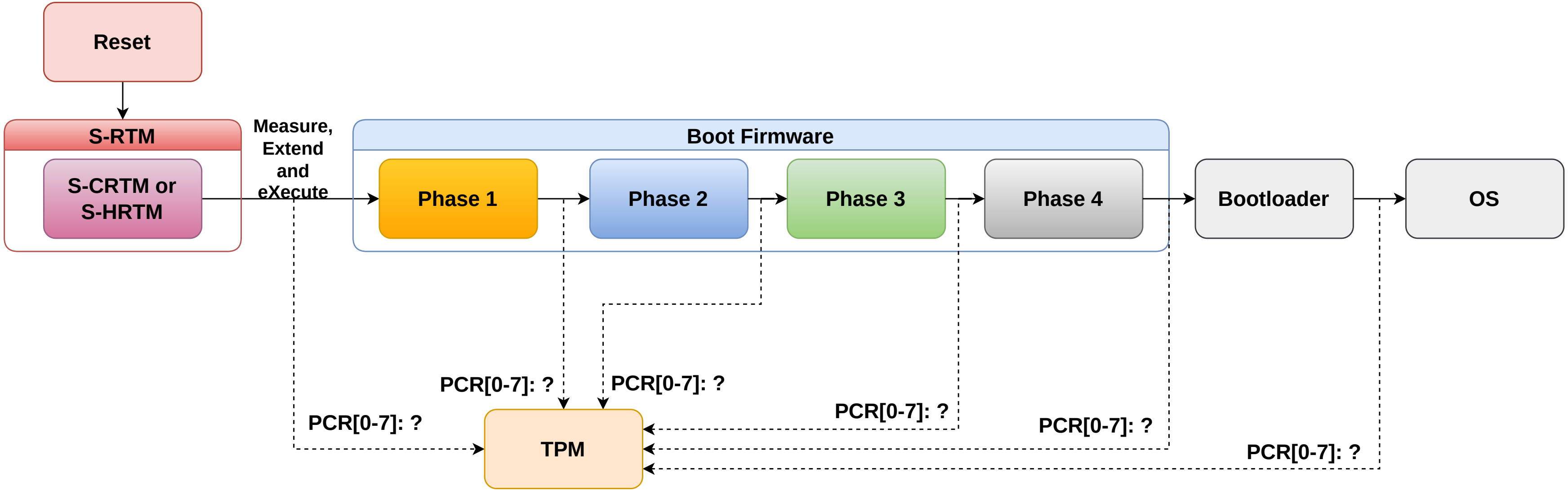
Chain of Trust Taxonomy

- Based on function:
  - Chain of Trust for Detection (CTD)
  - Chain of Trust for Recovery (CTRec)
  - Chain of Trust for Update (CTU)
- Based on method of transitive trust:
  - Measured Boot (integrity)
  - Verified Boot (authenticity, integrity)

Chain of Trust Taxonomy

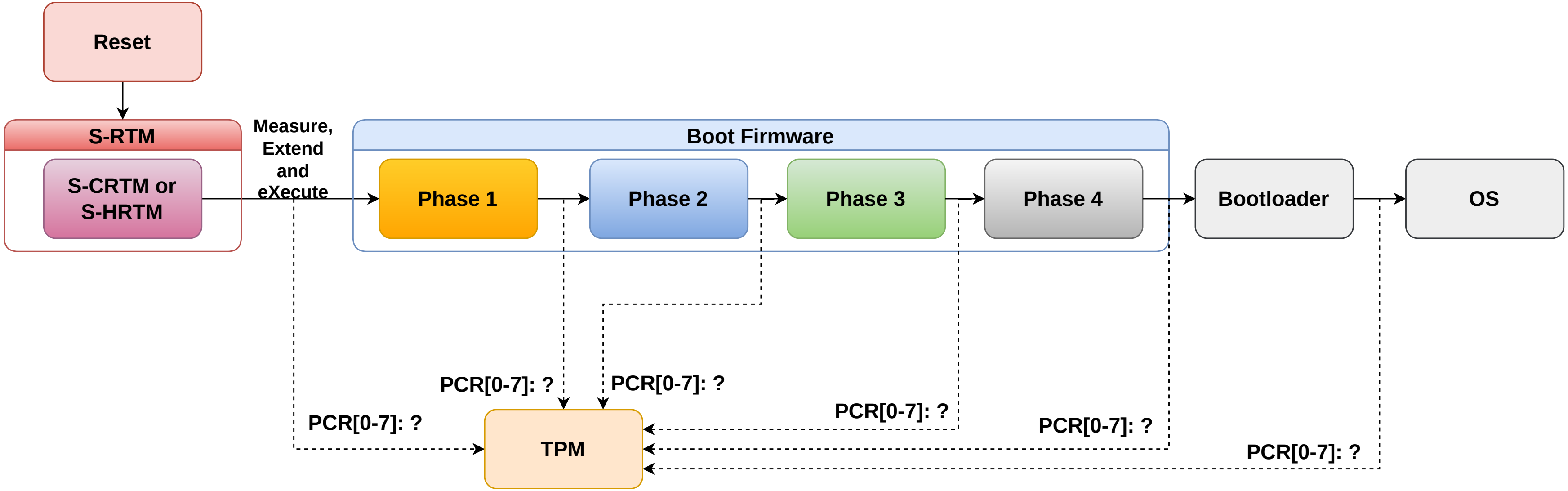
- Based on function:
  - Chain of Trust for Detection (CTD)
  - Chain of Trust for Recovery (CTRec)
  - Chain of Trust for Update (CTU)
- Based on method of transitive trust:
  - Measured Boot (integrity)
  - Verified Boot (authenticity, integrity)

How Measured Boot works?



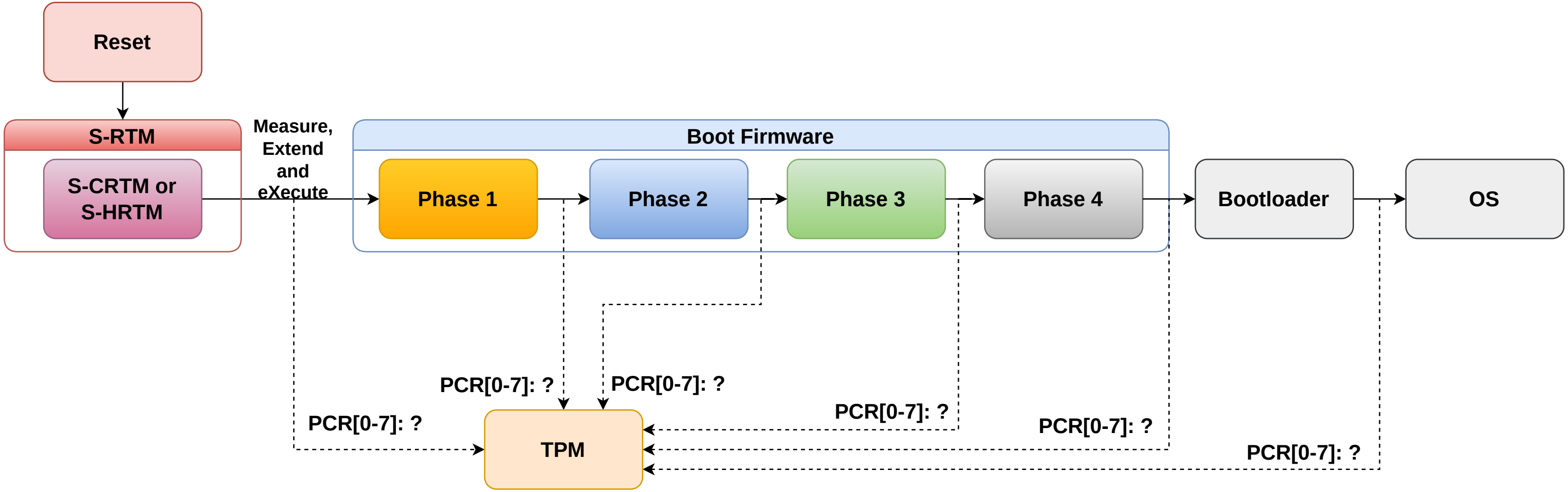
- **Measured Boot** - is boot process during which transitive trust was performed and chain of trust (chain of integrity measurements) was established.

How Measured Boot works?



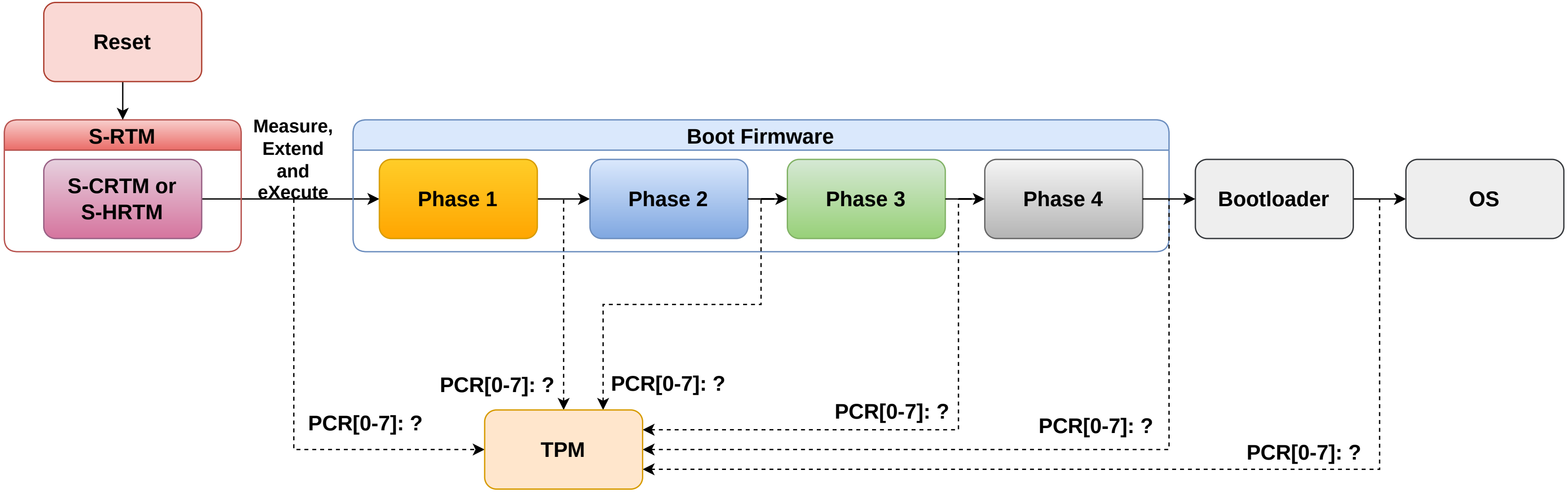
- **Measured Boot** - is boot process during which transitive trust was performed and chain of trust (chain of integrity measurements) was established.

How Measured Boot works?



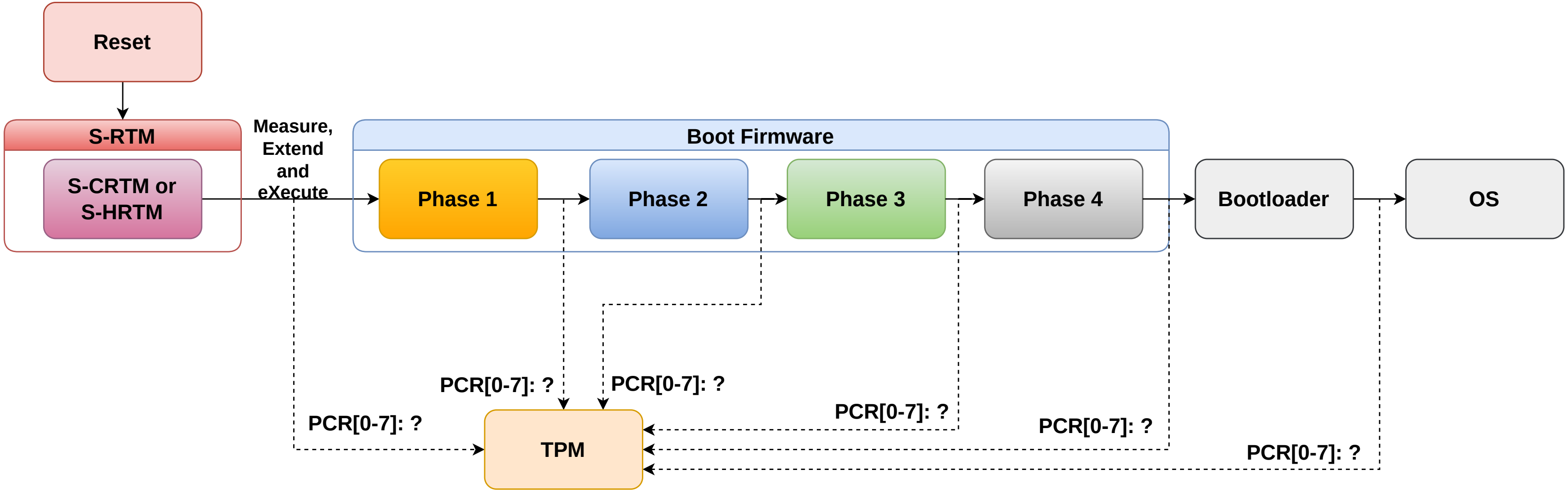
- **Measured Boot** - is boot process during which transitive trust was performed and chain of trust (chain of integrity measurements) was established.

How Measured Boot works?



- **Measured Boot** - is boot process during which transitive trust was performed and chain of trust (chain of integrity measurements) was established.

How Measured Boot works?



- **Measured Boot** - is boot process during which transitive trust was performed and chain of trust (chain of integrity measurements) was established.

How to protect S-RTM?

- It depends on the mechanism delivered by the platform and/or silicon vendor.
- Verified Boot-like technologies with strong RoT (Intel Boot Guard, AMD Hardware Validated Boot, NXP High Assurance Boot, etc.)
- How hard is it to sign firmware and fuse/provision platform?
  - it really depends on the vendor,
- What we can do with all those measurements in TPM?
  - local attestation - secret unsealing,
  - remote attestation,
- Maybe Measured Boot and S-RTM don’t make sense, and Verified Boot is the one to rely on?
  - ownership transfer,
  - vendor lock-in,
  - closed, centralized authority vs open, decentralized community,

Quiz

Quiz

What are the 5 types of Chain of Trust?

Quiz

What are the 5 types of Chain of Trust?

- CTD
- CTRec
- CTU
- Measured Boot
- Verified Boot

Quiz

What are the 5 types of Chain of Trust?

- CTD
- CTRec
- CTU
- Measured Boot
- Verified Boot

Where are the measurements typically stored?

Quiz

What are the 5 types of Chain of Trust?

- CTD
- CTRec
- CTU
- Measured Boot
- Verified Boot

Where are the measurements typically stored?

- In TPM PCR registers

Quiz

What are the 5 types of Chain of Trust?

- CTD
- CTRec
- CTU
- Measured Boot
- Verified Boot

Where are the measurements typically stored?

- In TPM PCR registers

Which measurement is the most important and why?

Quiz

What are the 5 types of Chain of Trust?

- CTD
- CTRec
- CTU
- Measured Boot
- Verified Boot

Where are the measurements typically stored?

- In TPM PCR registers

Which measurement is the most important and why?

- First, because based on it the whole chain is formed.

Quiz

Quiz

What are the technologies to protect the first measurement?

Quiz

What are the technologies to protect the first measurement?

- Intel Boot Guard, AMD Hardware Validated Boot, NXP High Assured Boot, SPI read-only protection.

Conclusion

In this lecture, we learned about the following:

- What are the taxonomies of Root of Trust and Chain of Trust technologies.
- Where in those taxonomies Intel Alder Lake (e.g. Intel N97) and other modern Intel hardware is placed with its security properties.
- Basics of Measured Boot works and for what it can be used.

This information will provide us with a solid foundation for understanding:

- Root of Trust Assessment, Integration and Provisioning.
- Deep diver into Slim Bootloader implementation of Verified Boot and Measured Boot.

Q&A