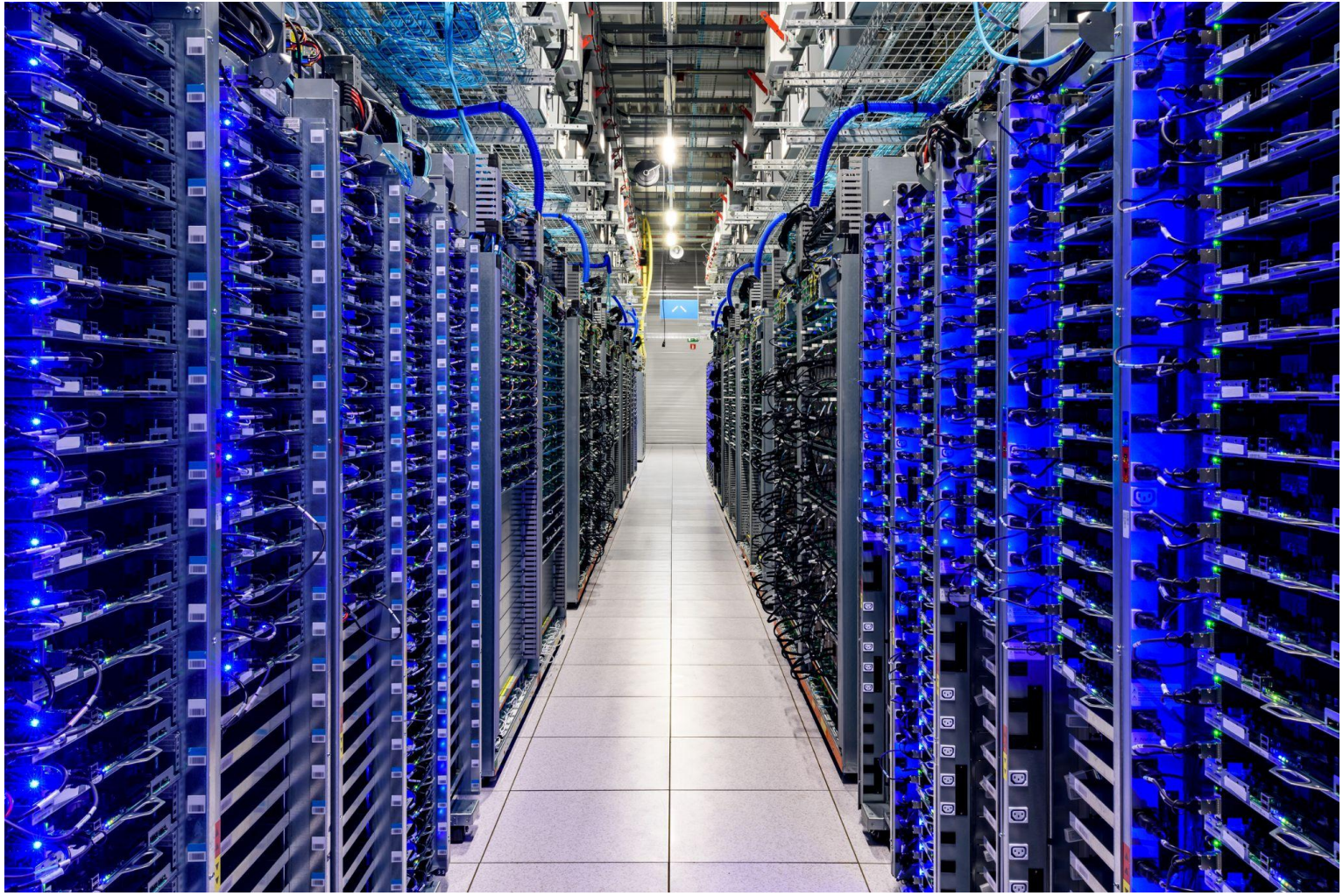
Silicon Root of Trust

Your Big Iron's Little Hero

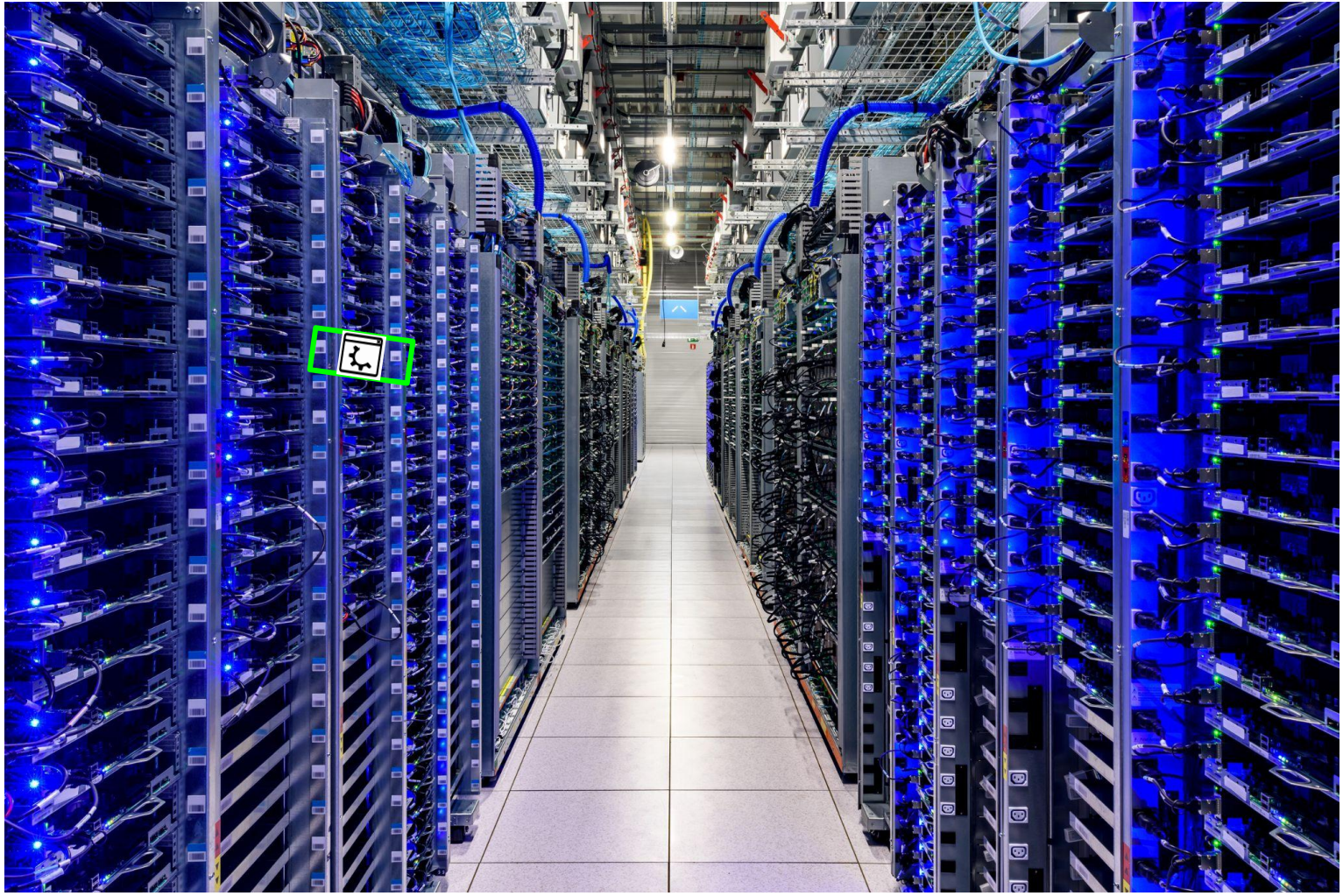
sameo@rivosinc.com - ER2023

Rivos

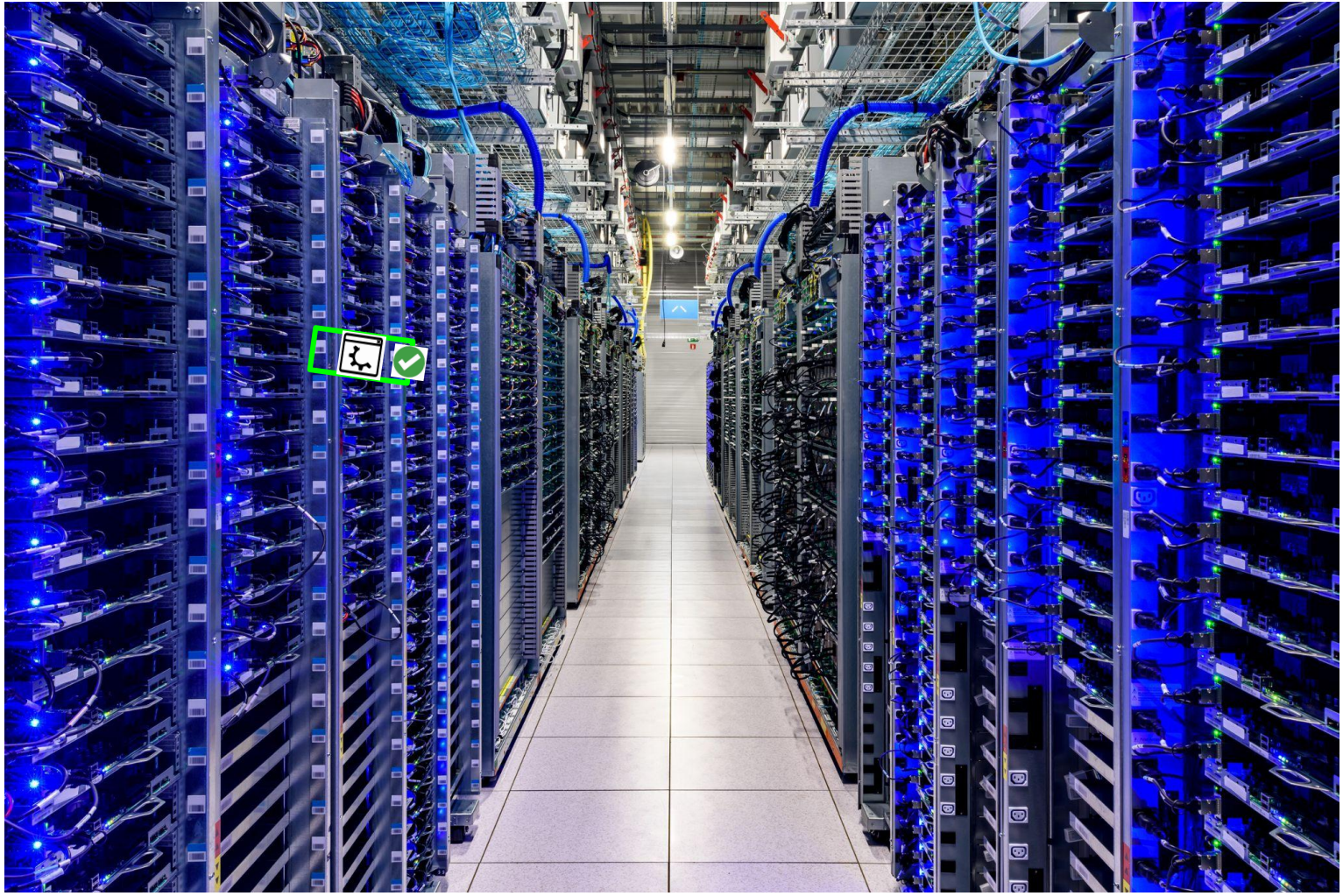


https://www.google.com/about/datacenters/gallery/#/tech1-st-ghislain-servers

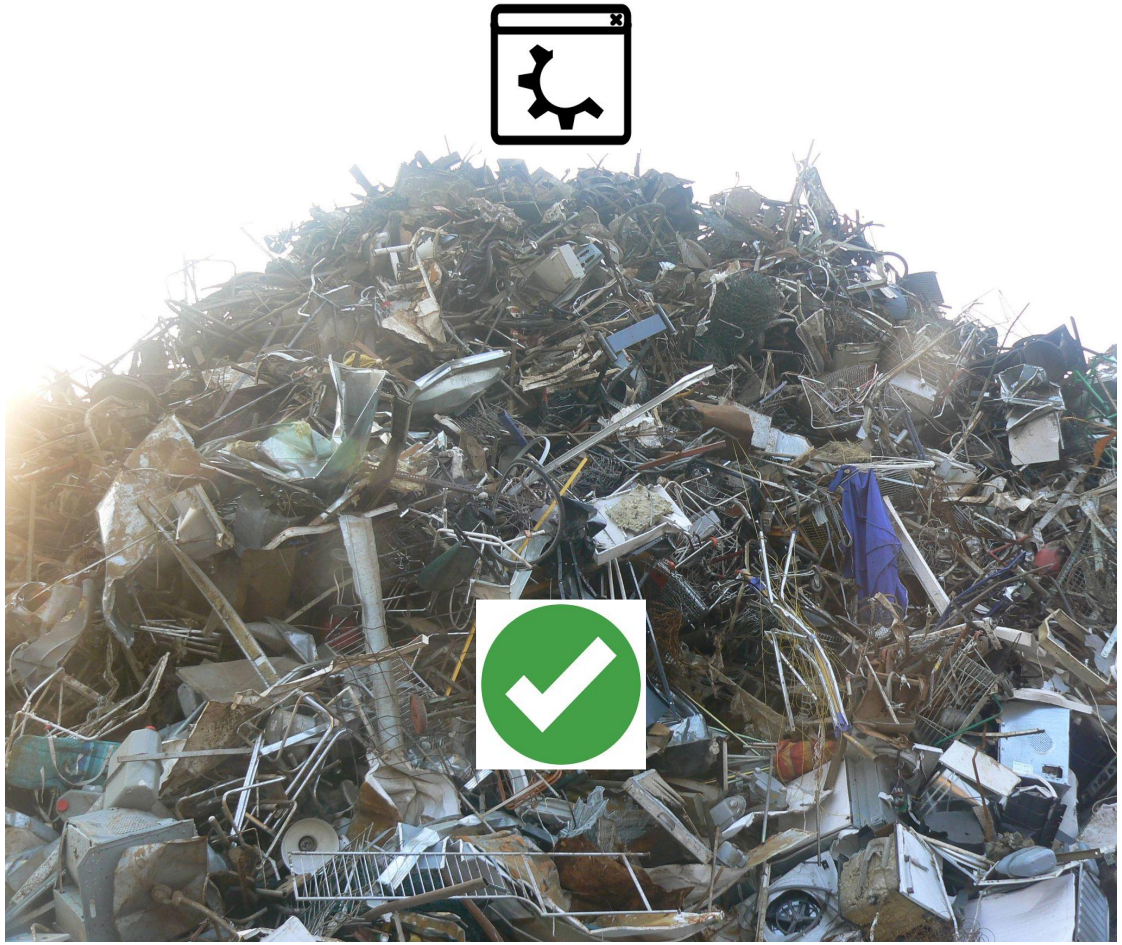
Rivos



Rivos



Rivos



Root of Trust

Root of Trust

"...a component that performs one or more security-specific functions, such as measurement, storage, reporting, verification, and/or update. " - TCG

Root of Trust

"...a component that performs one or more security-specific functions, such as measurement, storage, reporting, verification, and/or update. " - TCG

"A RoT is trusted always to behave in the expected manner, because its misbehavior cannot be detected..." - TCG

Root of Trust

"...a component that performs one or more security-specific functions, such as measurement, storage, reporting, verification, and/or update. " - TCG

"A RoT is trusted always to behave in the expected manner, because its misbehavior cannot be detected…" - TCG

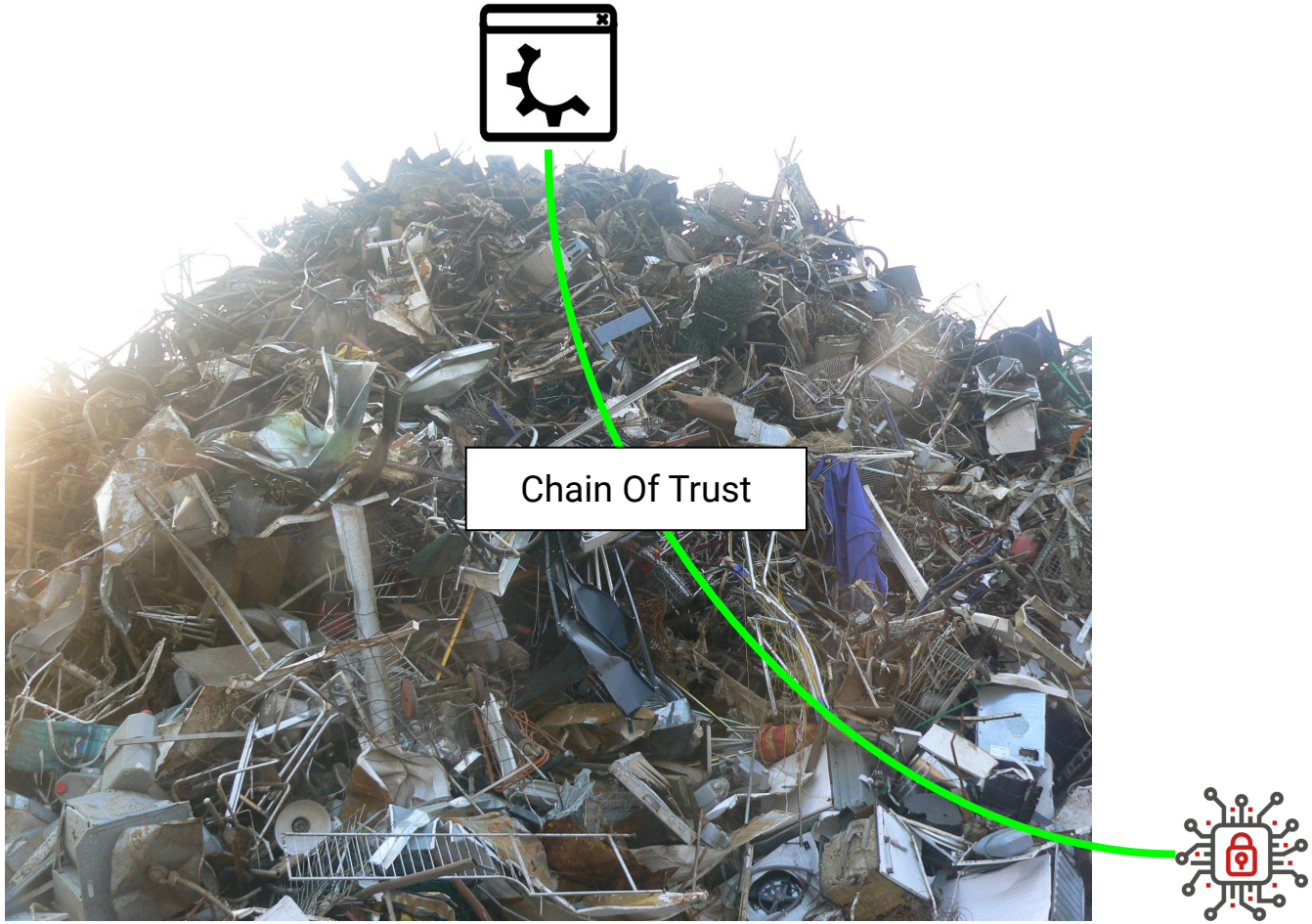
"A thing that has to be trustworthy for anything else on your computer to be trustworthy" - Matthew Garrett (mj59)

Root of Trust

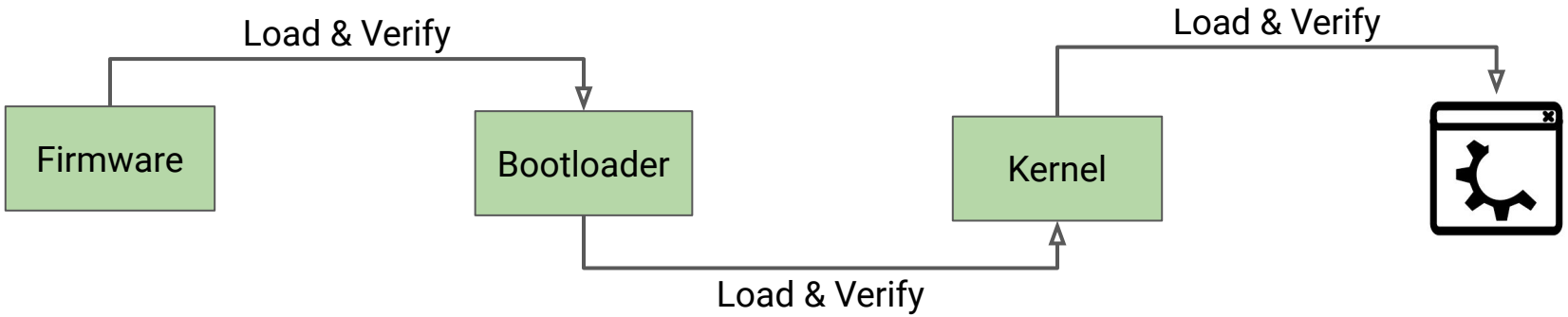
“...a component that performs one or more security-specific functions, such as measurement, storage, reporting, verification, and/or update. “ - TCG

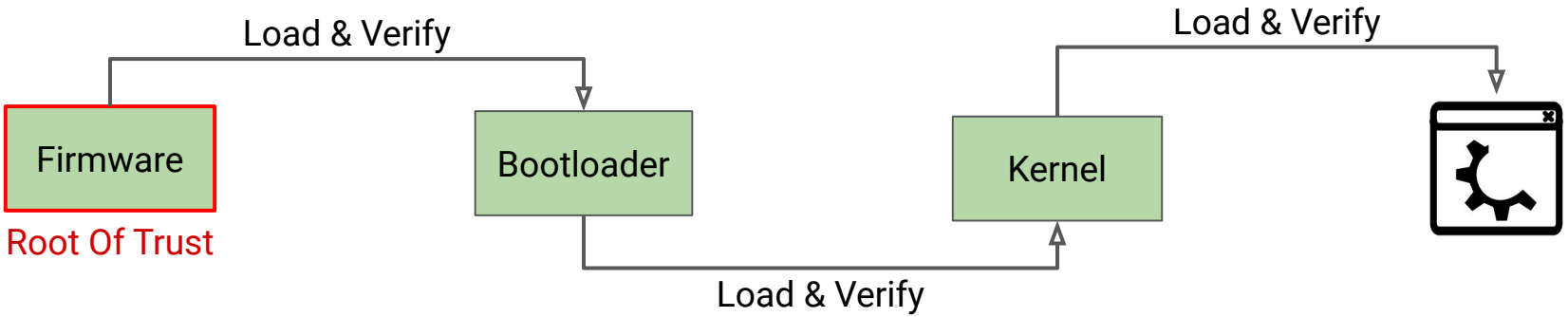
“A RoT is trusted always to behave in the expected manner, because its misbehavior cannot be detected…” - TCG

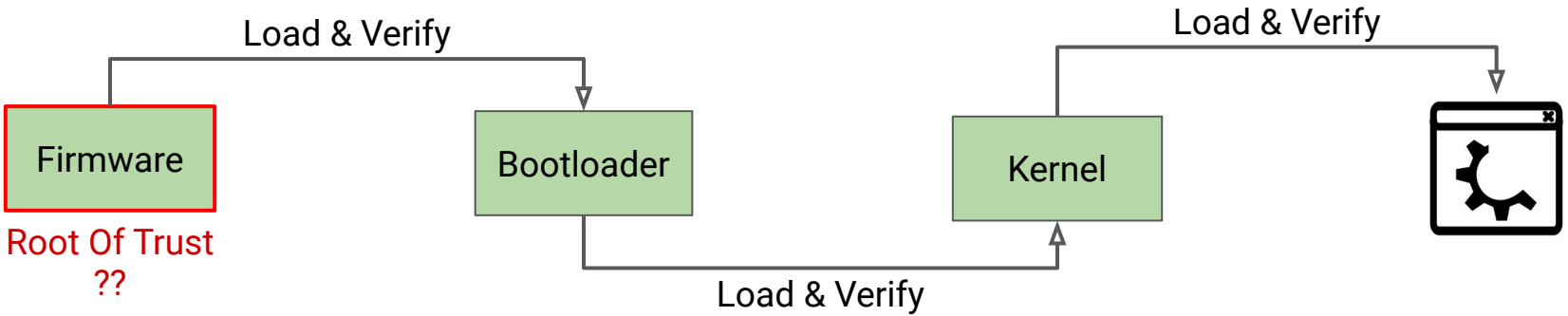
“A thing that has to be trustworthy for anything else on your computer to be trustworthy” - Matthew Garrett (mj59)

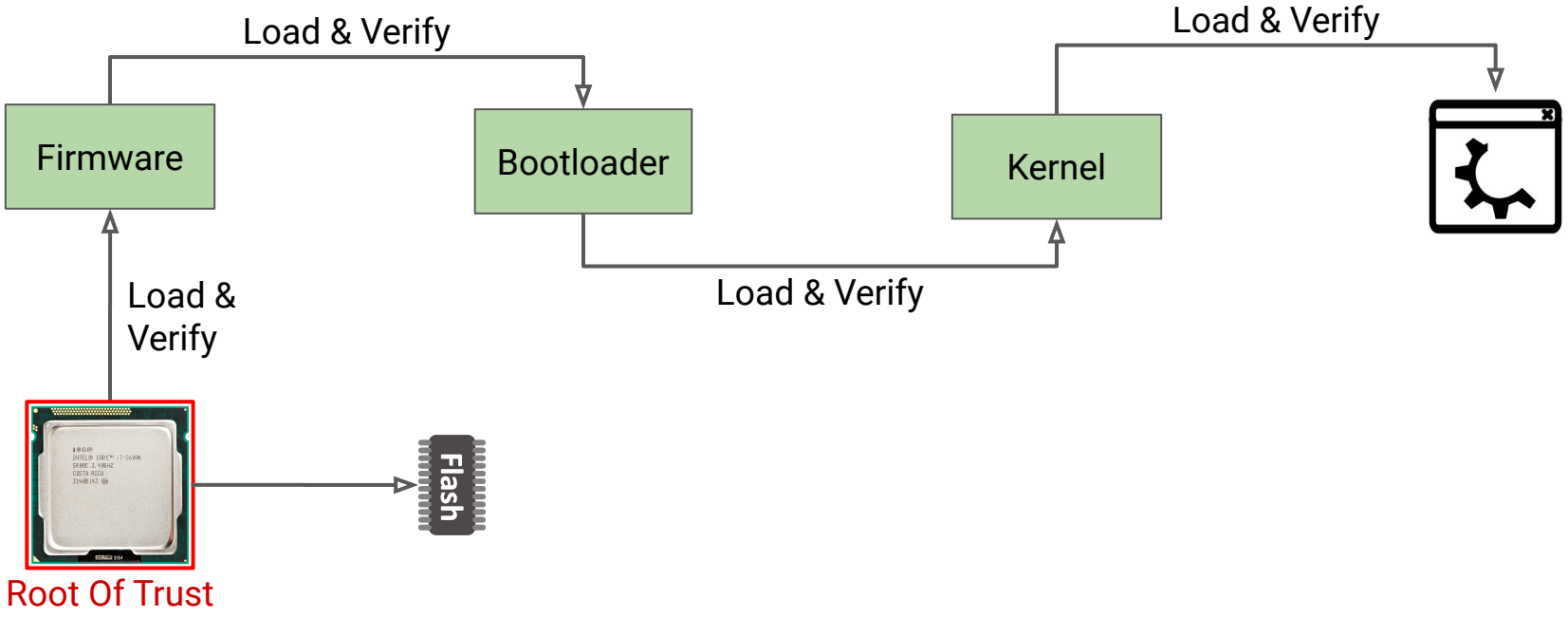


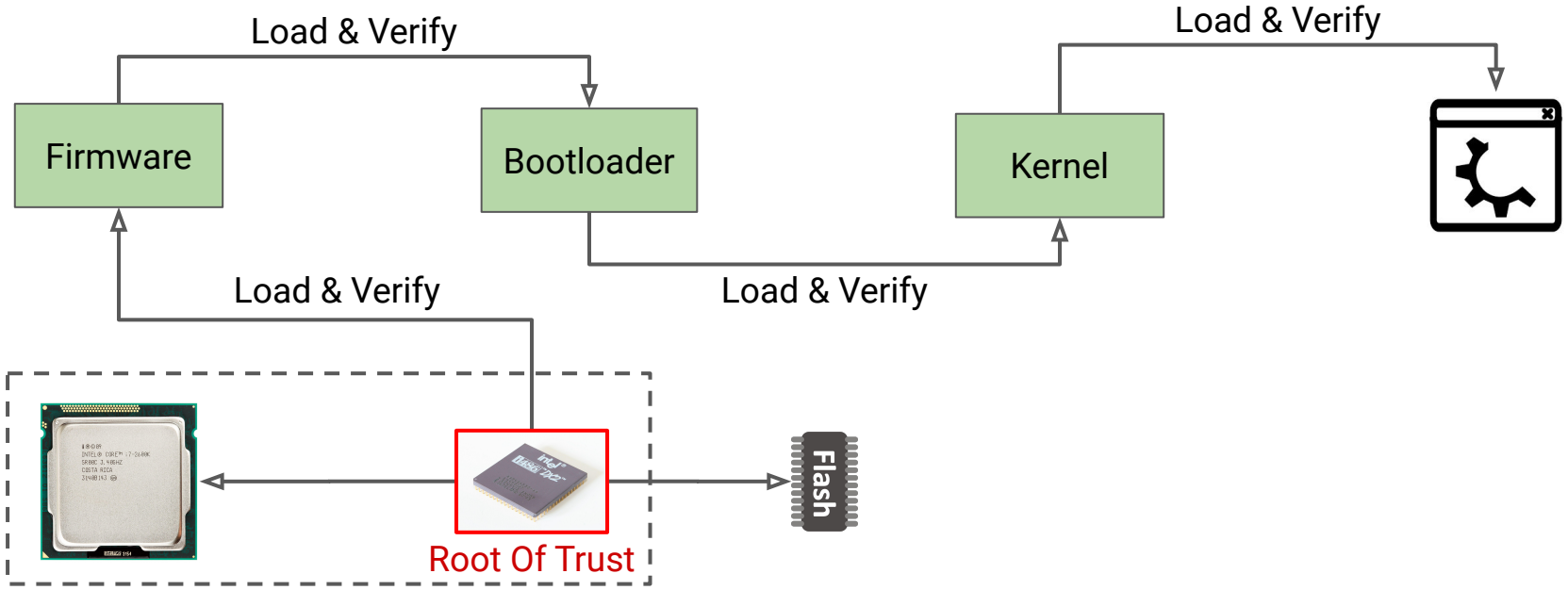
Rivos

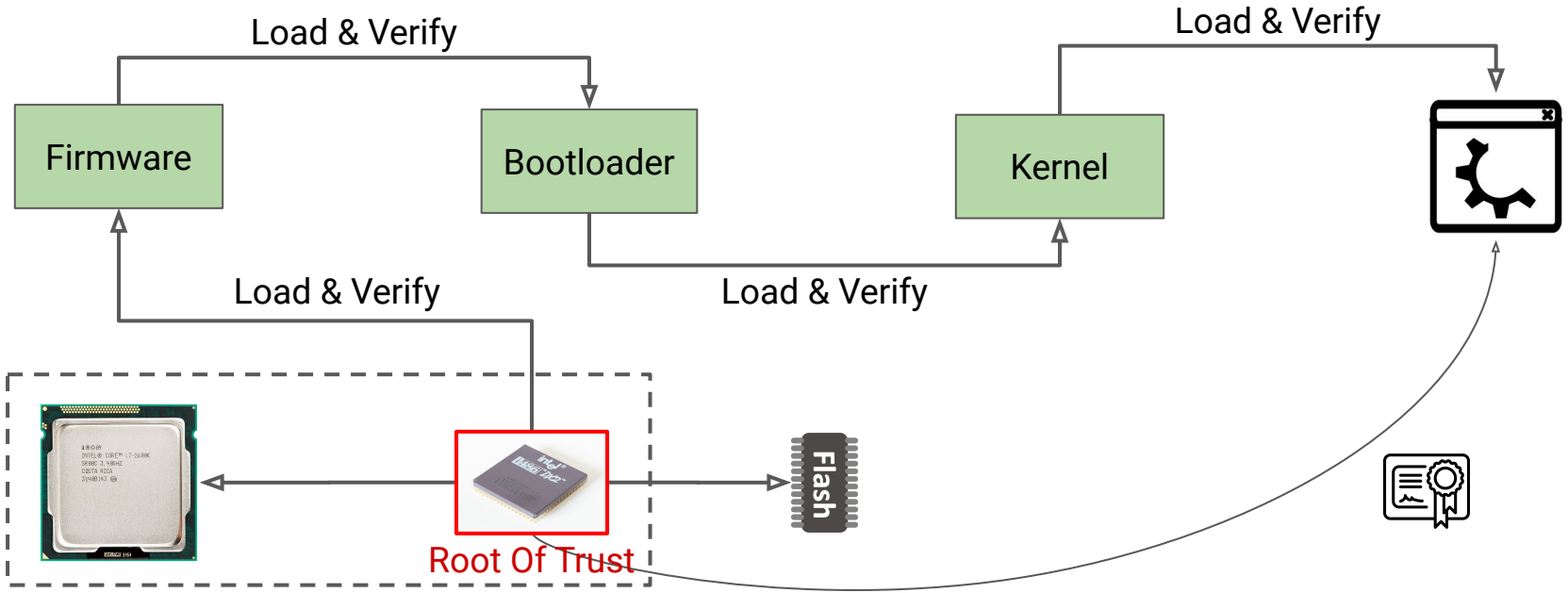

Load & Verify
Load & Verify
Firmware
Bootloader
Kernel
Load & Verify

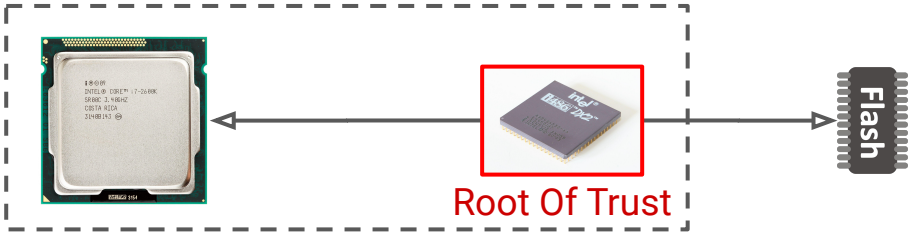

Load & Verify
Load & Verify
Firmware
Bootloader
Kernel
Root Of Trust
Load & Verify


Load & Verify
Load & Verify
Firmware
Bootloader
Kernel
Root Of Trust
??
Load & Verify









Manufacturing Flows

Platform Attestation

Authenticated Debug

(UEFI) Secure Boot

Firmware Update

Power-on Reset

A Trustworthy Root Of Trust

Manages the platform flows for

- Boot, security, manufacturing, update and debug

Most of the cloud security is built on those tiny 32-bit SoCs

- Running closed source C and assembly ROMs
- Manufactured from proprietary hardware designs
- Unknown testing and validation coverage

A Trustworthy Root Of Trust

Manages the platform flows for

- Boot, security, manufacturing, update and debug

Most of the cloud security is built on those tiny, 32-bit SoCs

- Running closed source C and assembly ROMs
- Manufactured from proprietary hardware designs
- Unknown testing and validation coverage

Why should I trust it more than I trust the platform CPU?

- Or than an open source, simple (Rust) firmware?
- https://cve.mitre.org/cgi-bin/cvekey.cgi?**keyword=Intel+Management+Engine**

Open Source Hardware RoTs

“Given enough eyeballs, all bugs are shallow” **- Linus Law**

Open source hardware design

- RTL, Design Validation (DV), Documentation, Software (ROM) and tools

Transparent, open and trustworthy development process

- Leading to more secure RoTs

Two main projects

- Caliptra (ChipsAlliance)
- OpenTitan (lowRISC)

Rivos

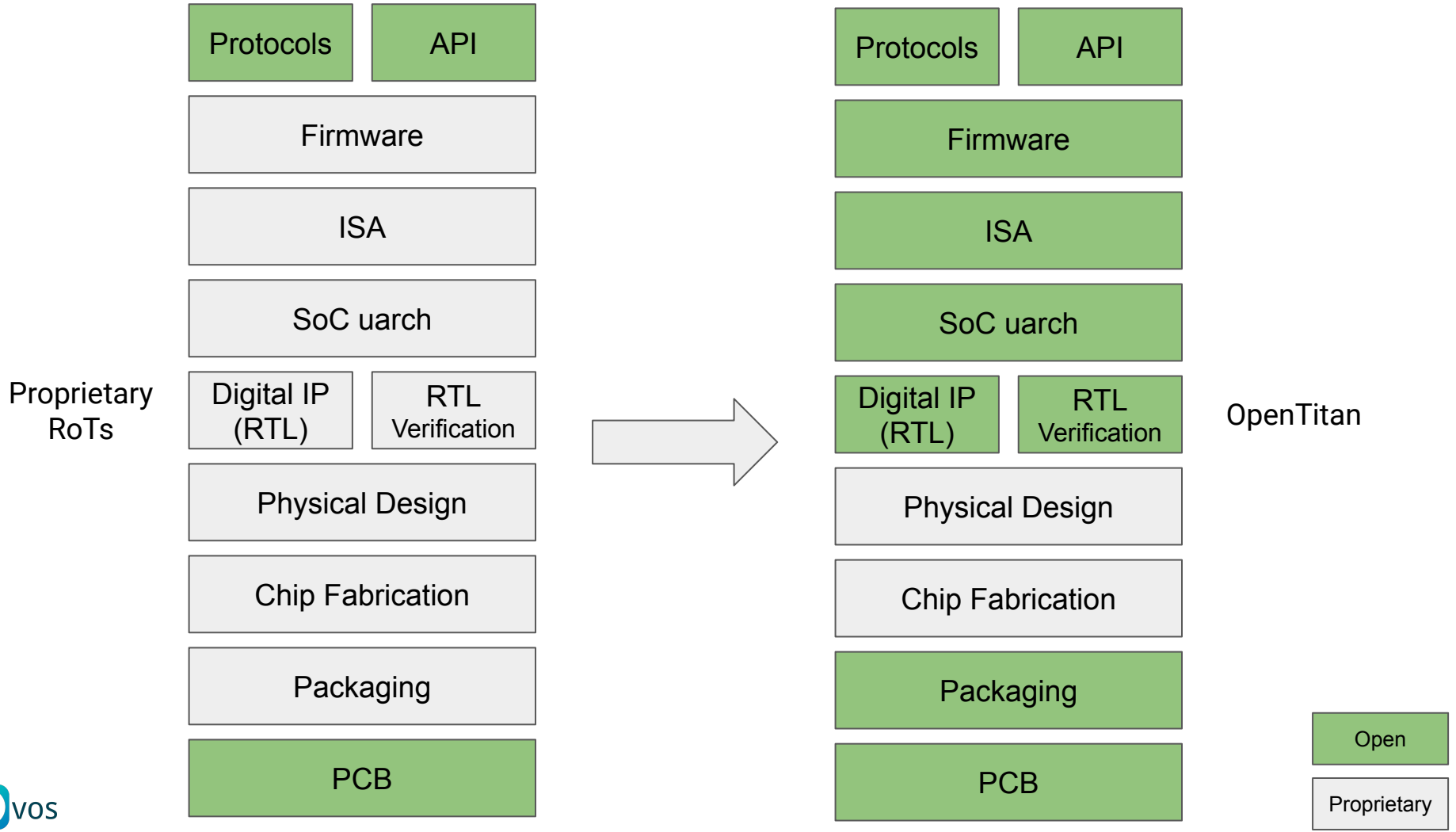
OpenTitan

Largest open source hardware project

Google Titan != OpenTitan

OpenTitan is entirely written from scratch

“Transparent, high-quality reference design for silicon RoTs”


Protocols
API
Firmware
ISA
SoC uarch
Digital IP (RTL)
RTL Verification
Physical Design
Chip Fabrication
Packaging
PCB
Proprietary RoTs
Protocols
API
Firmware
ISA
SoC uarch
Digital IP (RTL)
RTL Verification
Physical Design
Chip Fabrication
Packaging
PCB
OpenTitan
Open
Proprietary
Rivos

Open Hardware. For Real

A good open source citizen

- Pull requests and reviews (RTL, SW, FW, etc.)
- Testing and documentation required (Including Design Verification - DV)
- Systematic and thorough CI
- Enforced coding style
- Apache 2 licensed by default (exceptions allowed)
- Open governance

HW, SW, DV and documentation developed together

- Strictly defined and tracked development stages
- No IP block without DV, SW library and (autogenerated) documentation

Security Focus

Any critical asset must be protected with security countermeasures

- **Assets: Keys, token, memory, signal, registers, etc**
- **Countermeasures: Shadow regs, sparse FSMs, Multiple bits encoding, etc**

All peripherals can define security alerts (interrupt-ish)

All bus transaction are integrity protected

All memories are scrambled

All keys are protected from SW and from the SoC Core

Comportable IP Blocks

IP blocks that behave

Compliance

- Between IP blocks
- With the top level design

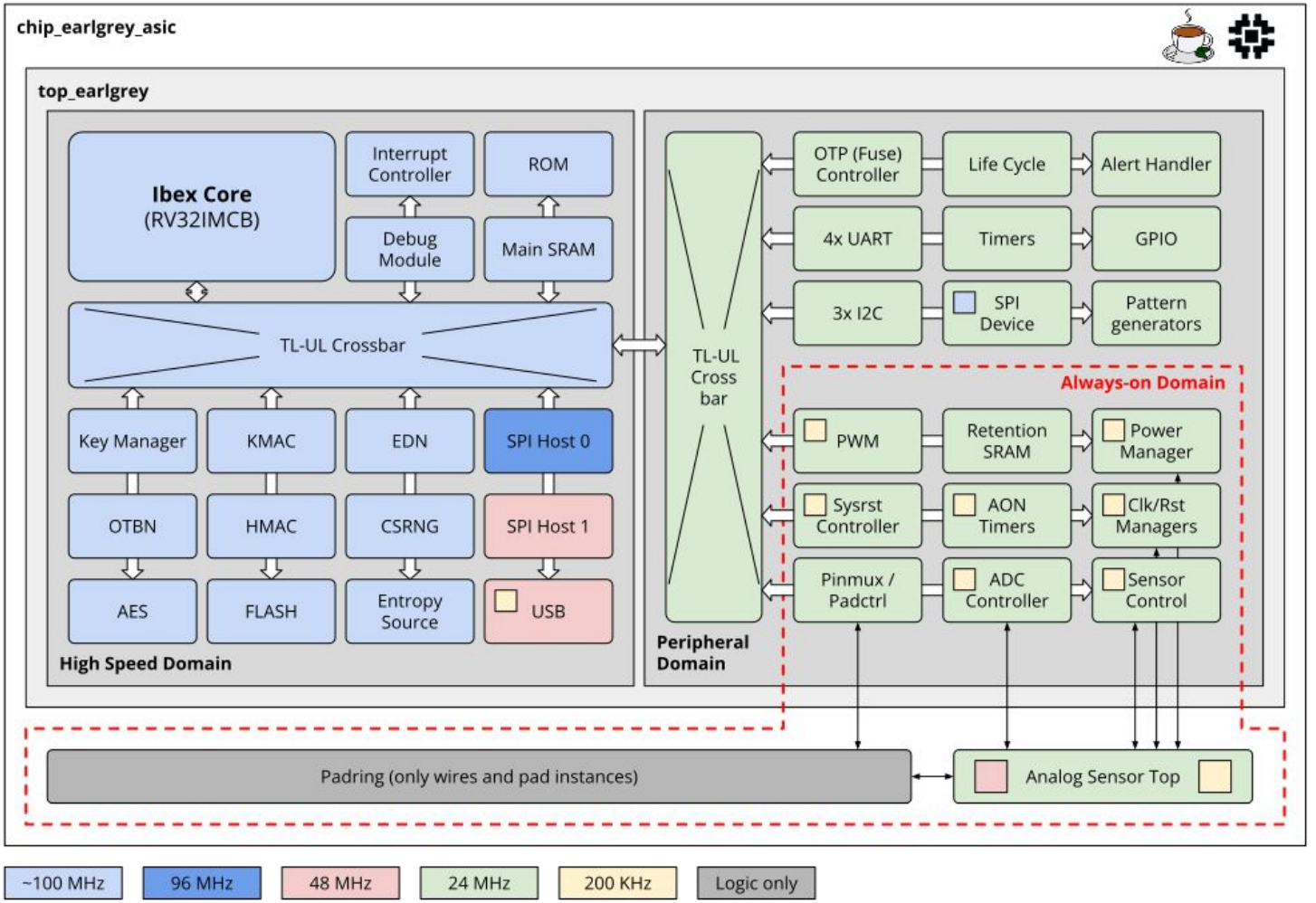
Each IP block is described through a comportability configuration file

- Clocks, buses, interrupts, alerts, security countermeasures, registers, etc

Plug & play IP blocks

RTL, documentation and C/Rust header files autogeneration

OpenTitan Discrete (a.k.a. Earlgrey)



Rivos

Ibex - OpenTitan Core

A simple, verified, production-ready RV32 core

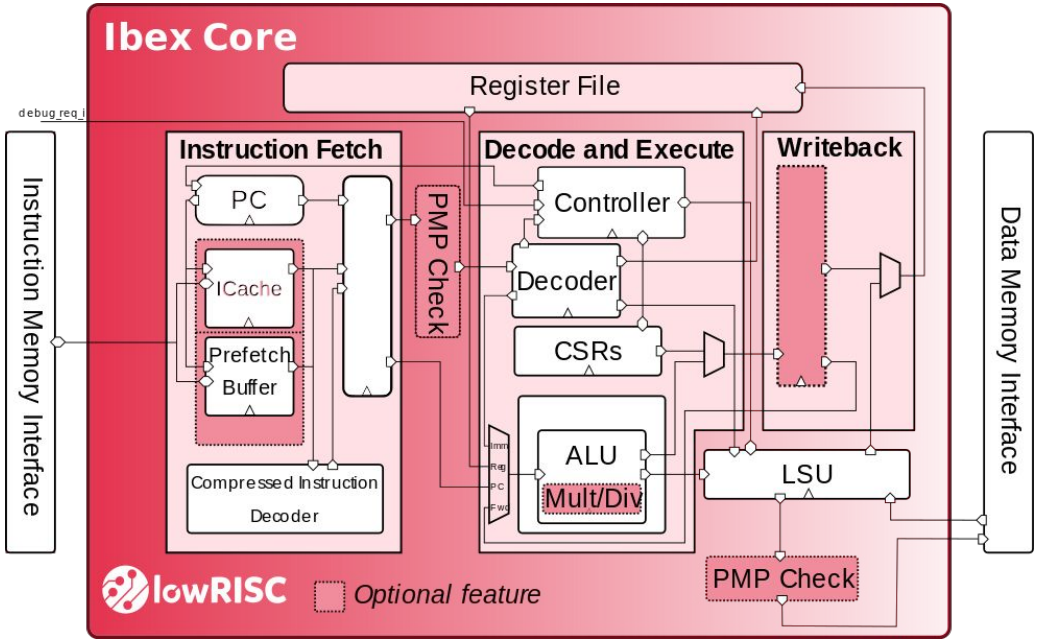
Open source as well

3 stages pipeline

Branch prediction is optional

Two lock-step cores in OpenTitan

Enhanced physical memory protection (ePMP)

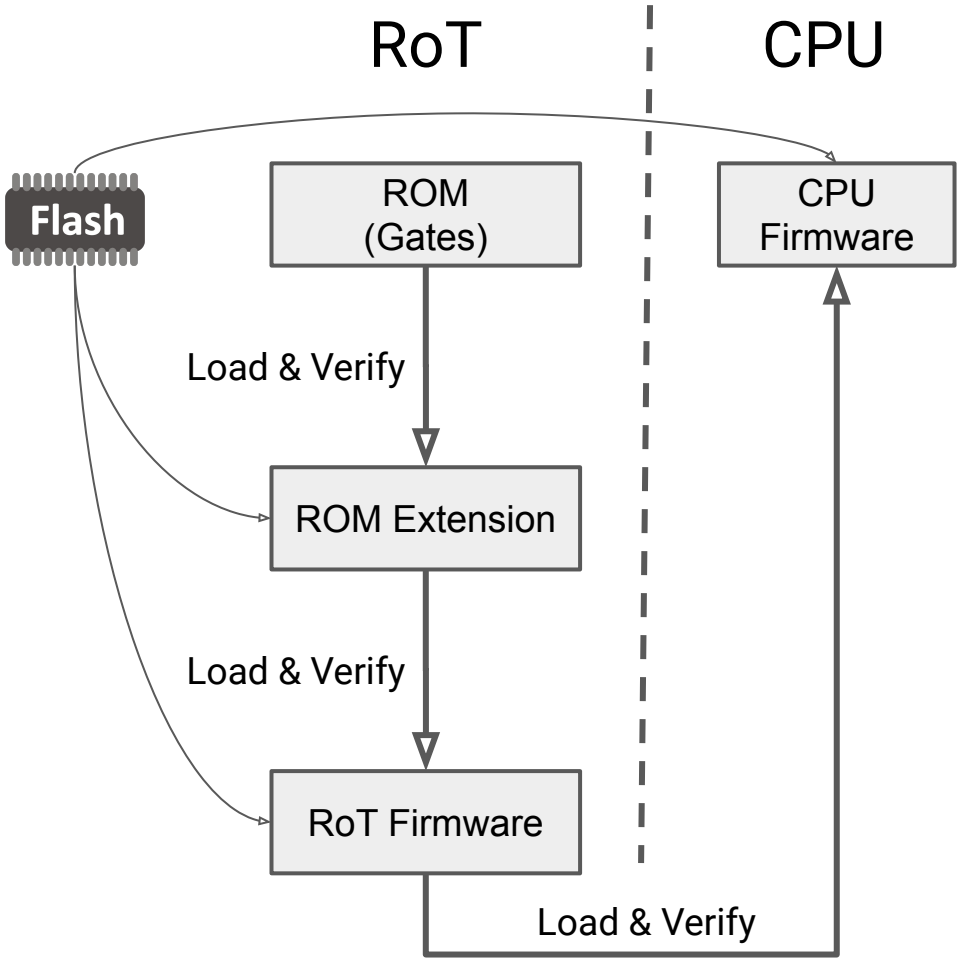


Software. Firmware. ROM

3-stage secure boot

1. **ROM**
   a. In-gates, immutable. “Simple” C and asm
2. **ROM Extension**
   a. First mutable code. Extends the ROM
3. **RoT Firmware**
   a. Device owner (e.g. OEM) code
   b. Hubris, Zephyr, etc
   c. Resident firmware, provides RoT services

Bound to the Key Manager stages



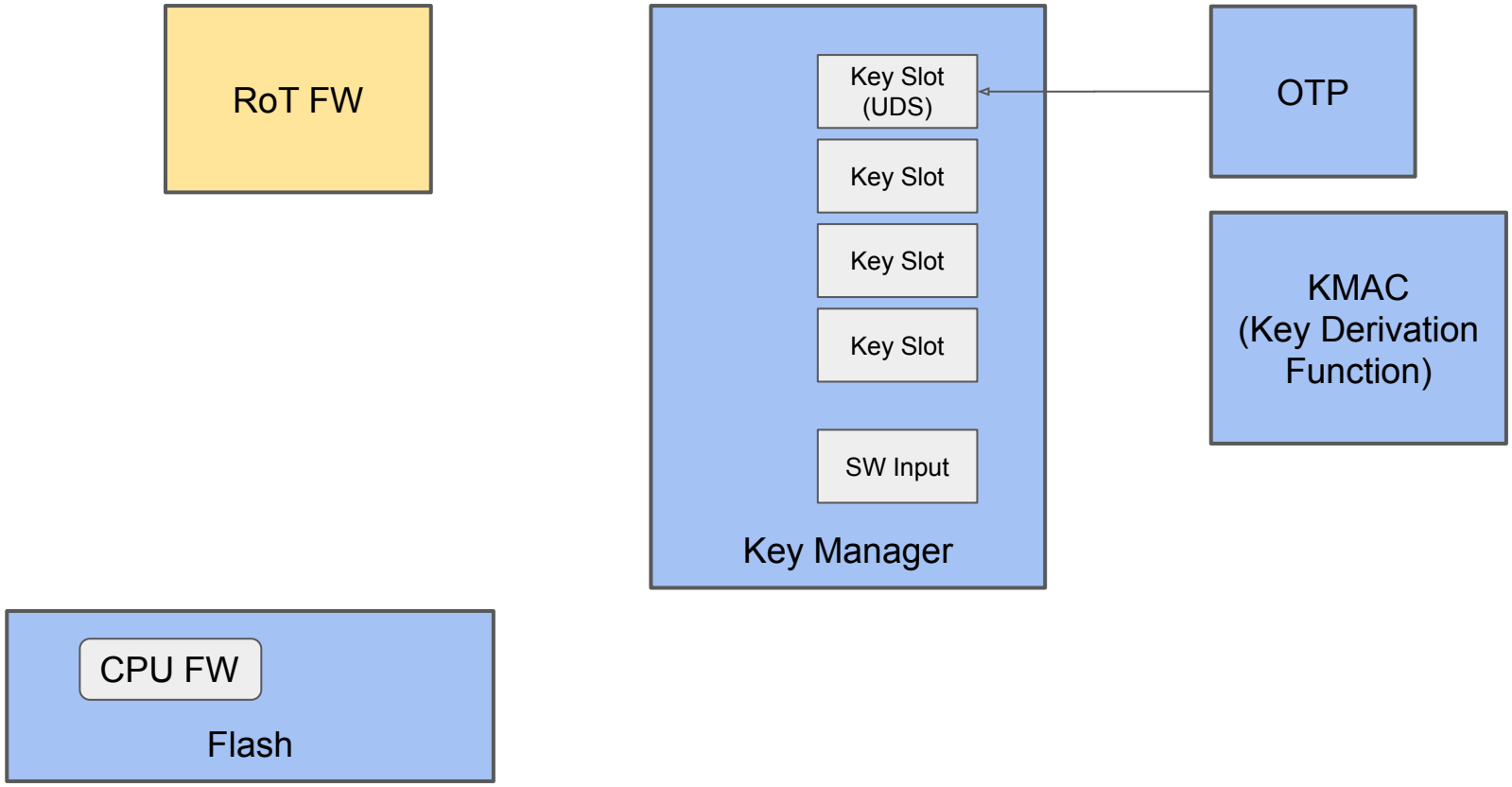
OpenTitan Device Software

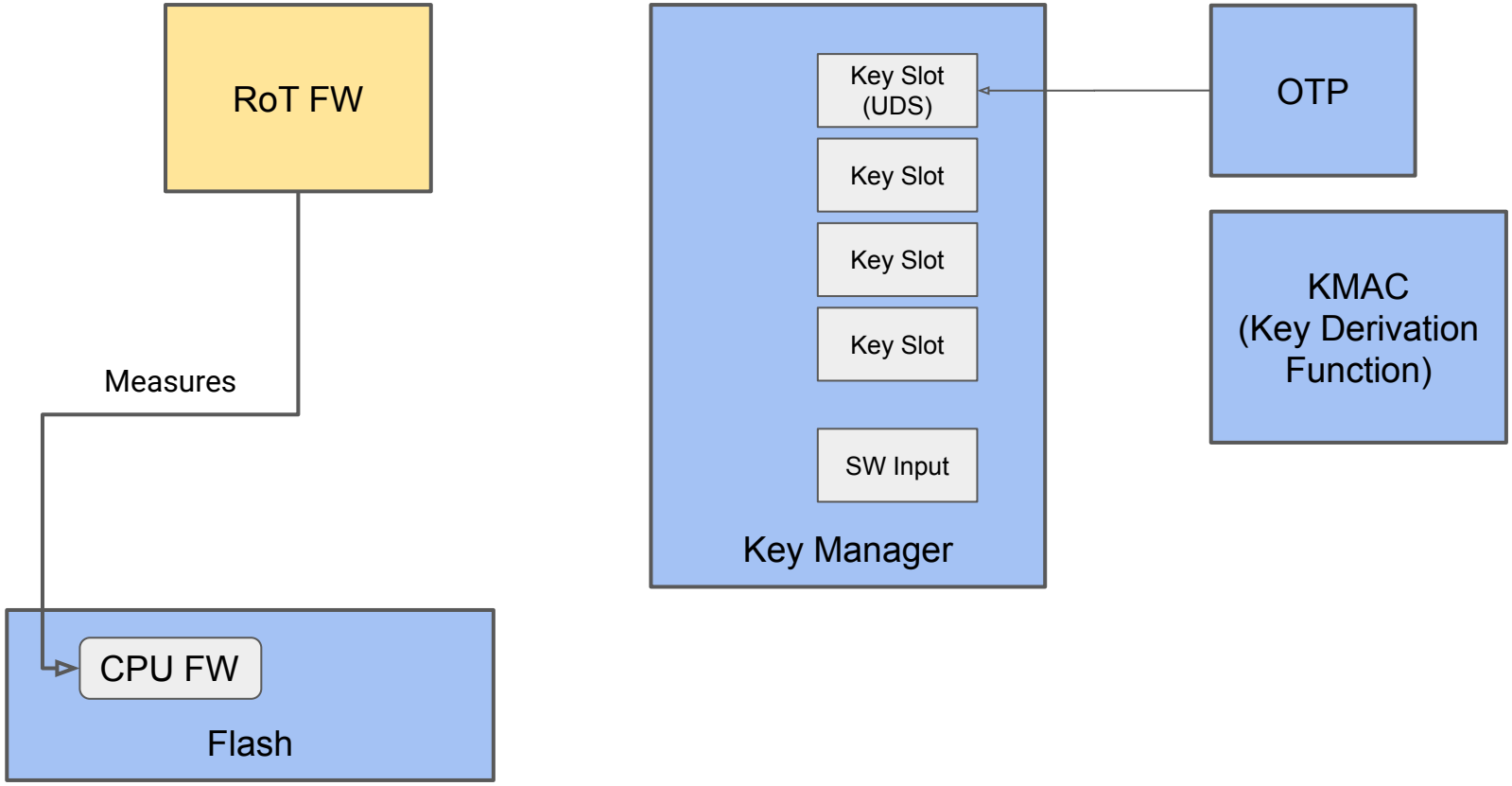
ROM and ROM extension

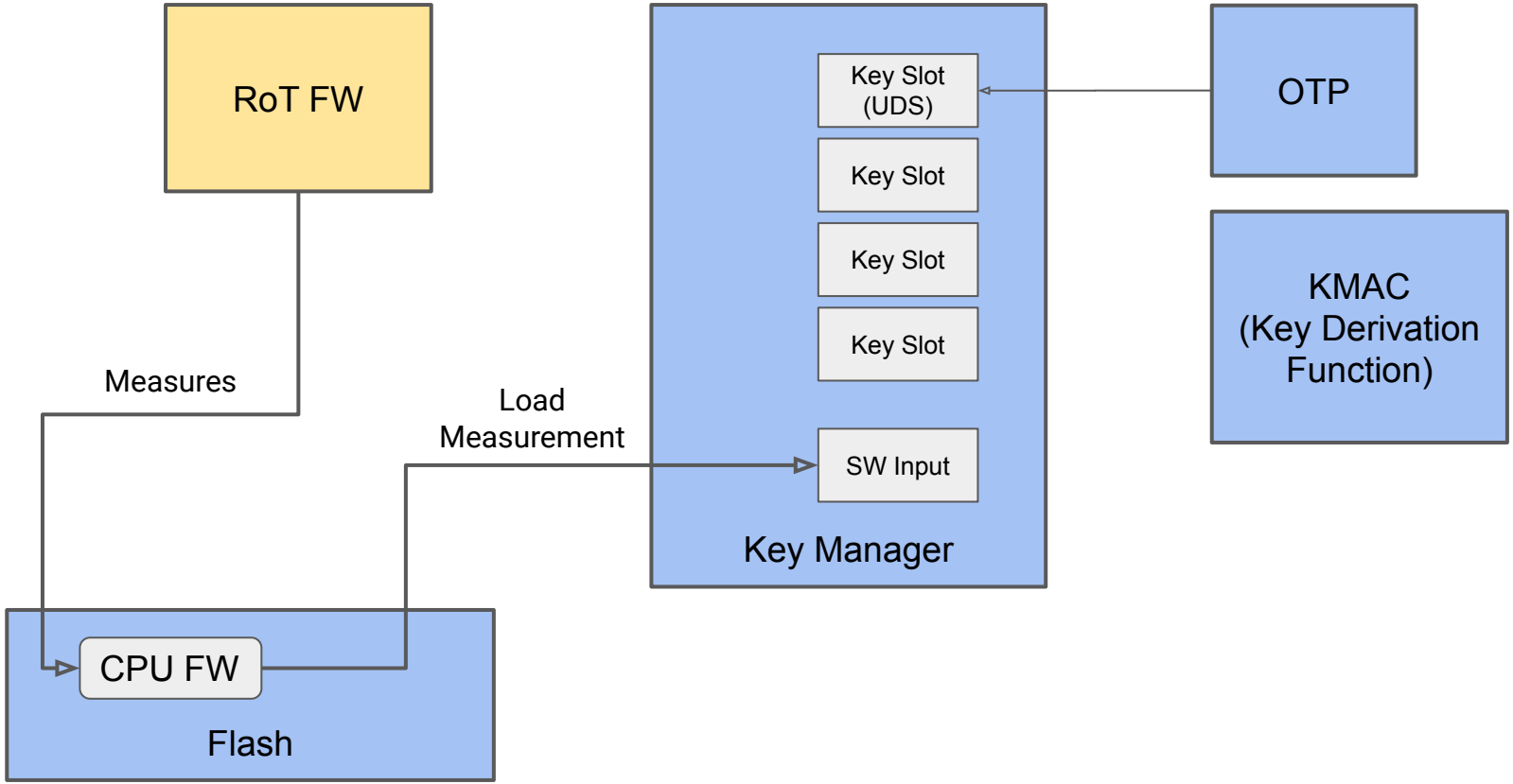
- Open source reference code
- Peripheral drivers
- C and assembly code for booting the actual firmware
- ROM is the real Root of Trust

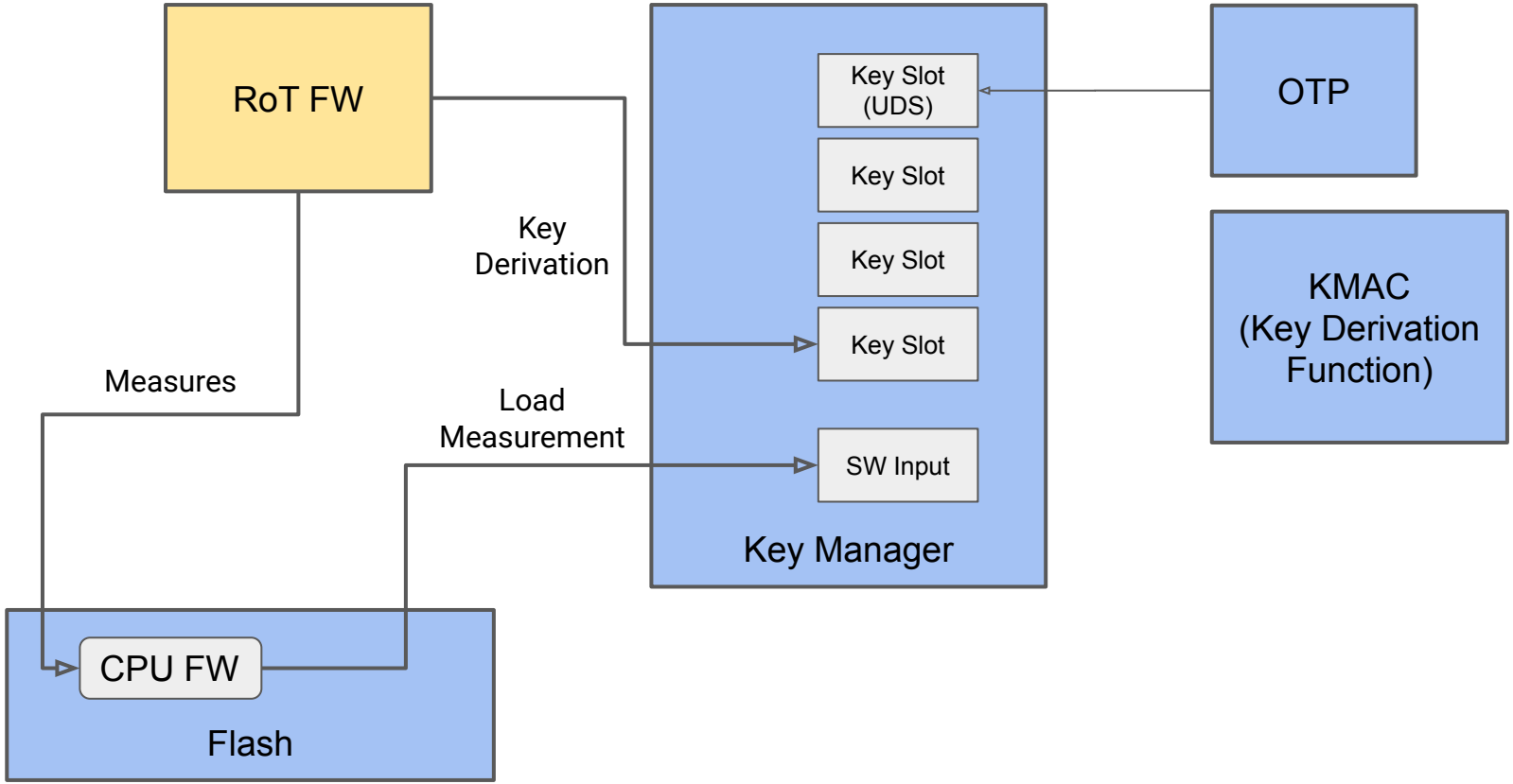
RoT Firmware

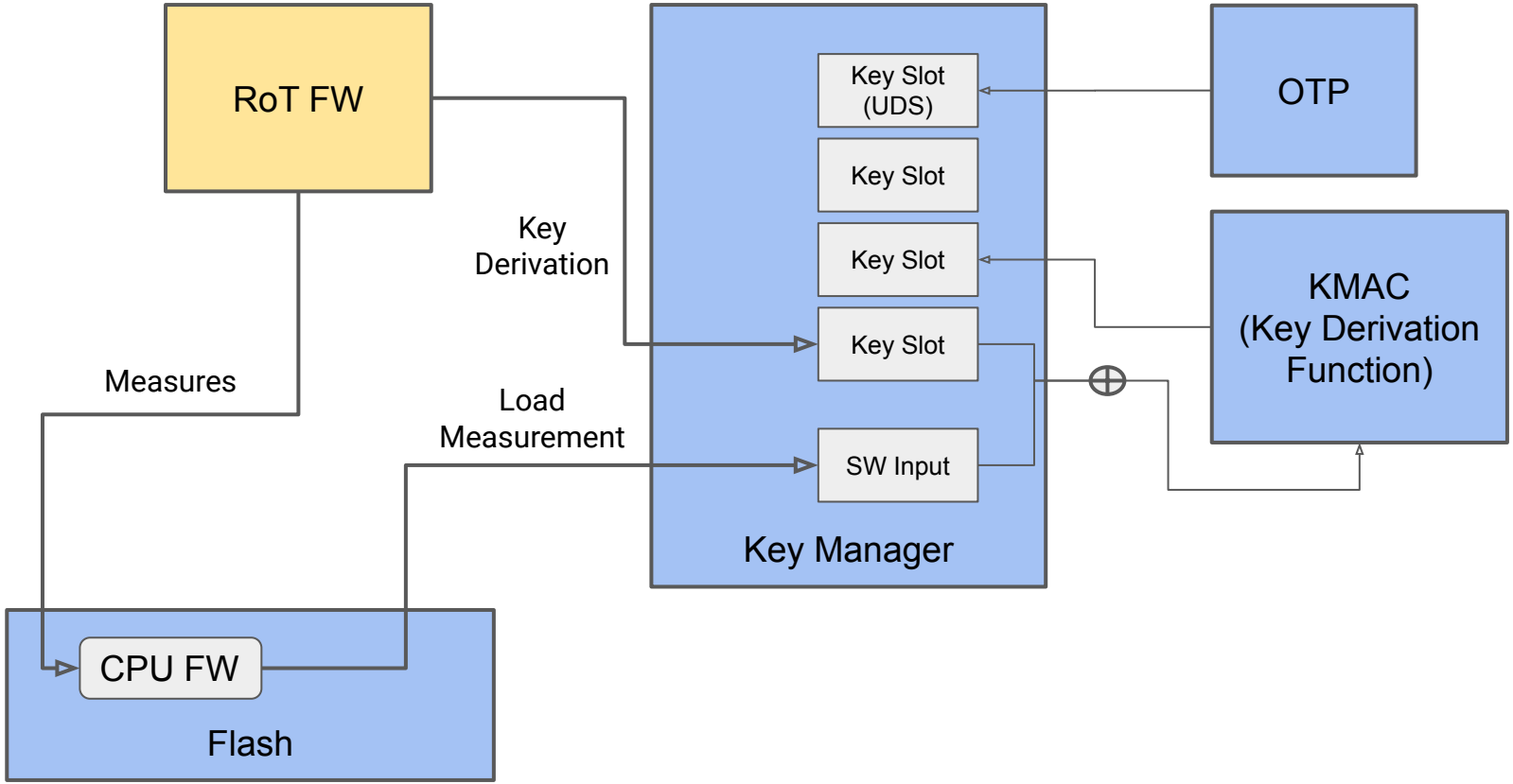
- Full OS, not provided


RoT FW
Key Slot
(UDS)
Key Slot
Key Slot
Key Slot
SW Input
Key Manager
OTP
KMAC
(Key Derivation
Function)
CPU FW
Flash


RoT FW
Measures
CPU FW
Flash
Key Slot (UDS)
Key Slot
Key Slot
Key Slot
SW Input
Key Manager
OTP
KMAC (Key Derivation Function)


RoT FW
Key Slot (UDS)
Key Slot
Key Slot
Key Slot
OTP
KMAC (Key Derivation Function)
Measures
Load Measurement
SW Input
Key Manager
CPU FW
Flash


RoT FW
Key Slot (UDS)
Key Slot
Key Slot
Key Slot
OTP
KMAC (Key Derivation Function)
Key Derivation
Measures
Load Measurement
SW Input
Key Manager
CPU FW
Flash


RoT FW
Key Derivation
Measures
Load Measurement
Key Slot (UDS)
Key Slot
Key Slot
Key Slot
SW Input
Key Manager
OTP
KMAC (Key Derivation Function)
CPU FW
Flash

Key Manager

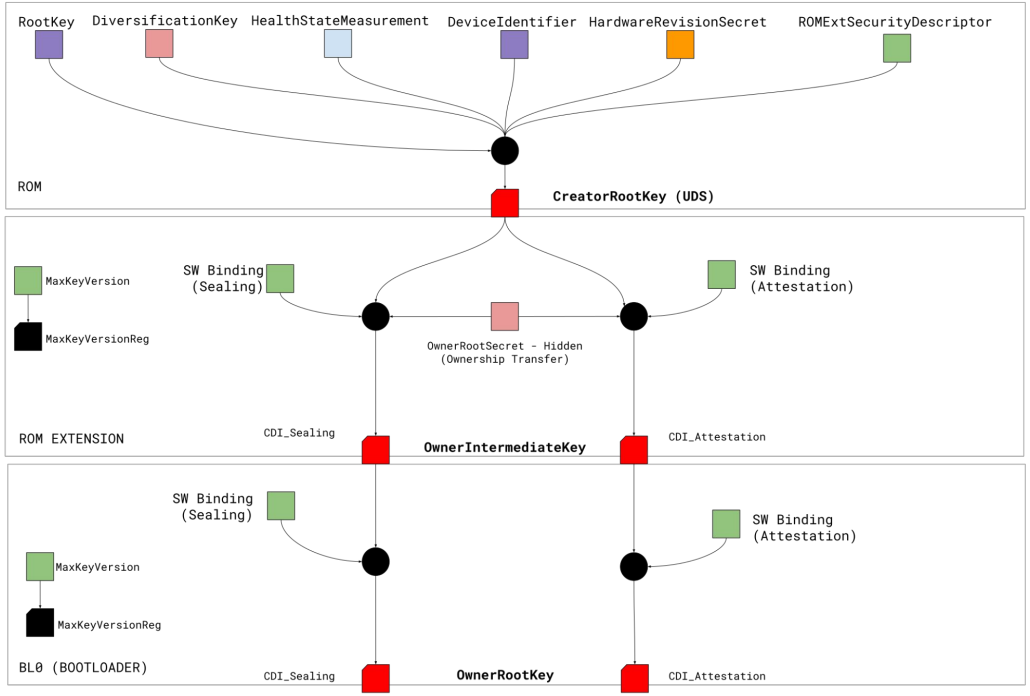
Hardware support for DICE implementation

RoT Firmware is the DPE

Each boot stage:

- **Gets a signed certificate chain from its parent**
- **Measures the next stage**
- **Adds measurement to the chain**

RoT Firmware provides attestation report



Takeaways

Security is hard. It's easier with open source hardware

Open source hardware RoTs can make the cloud a less scary place

OpenTitan is truly an open source hardware project

Participate

- **https://github.com/lowRISC/opentitan**
- **FPGA**
- **https://github.com/lowRISC/qemu**