Setting Hardware Root-of-Trust from Edge to Cloud, and How to Use it

Computer & Electronics Security Application Rendez-vous, 2022

Florent Chabaud
Chief Product Security Officer
16/11/2022

Trust is not Security

Years of debates: should you trust cryptography?

- Clipper Chip (1993)
- Trusted Computing Platform Alliance (1999)
- Trusted Computing Group (2003)
- Trusted Platform Module (2009)
- E. Snowden and other Leaks (2013-)

Root-of-Trust

An application of Kerckhoffs' second principle

- Minimize the data to protect from threats

- Everything can be public but secret keys
  - Same for private keys
- Everything can be changed but public keys

- Hardware makes sense to protect confidentiality and integrity (e.g. smart card)

Attestation Mechanism

Trusted Computing Base

- How can I trust hardware for protecting keys?
- Is it really “my” hardware?
- Attestation Mechanism principle allows a device to authenticate itself to a verifier

- Each device must have a Unique Device Secret (UDS) which characterizes the attester device.

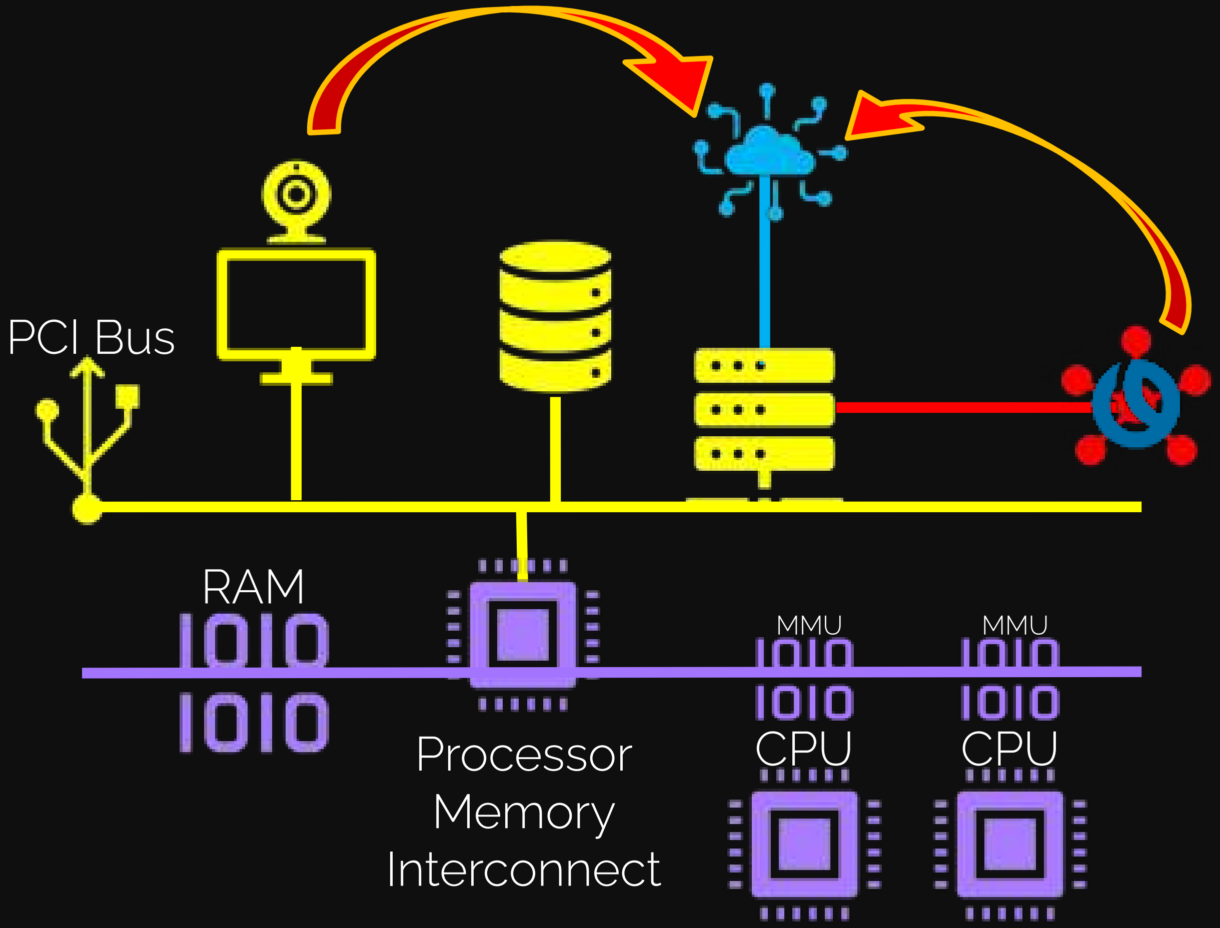
- A private authentication key unique to each device.
  - The key is immutable and certified by the provisioner.
- A private signature key unique to each device.
  - The key is updated and certified by the device owner

What is a device?

Why firmware is important?

- Typical host architecture
  - A bus to interconnect devices
  - A high speed interconnection for memory
- Two Memory Access modes
  - Indirect through CPUs
  - Direct through DMA

- For instance, NIC devices make extensive use of DMA
- What if their firmware is trapped or tainted?



What firmware?

Dozens of firmware!

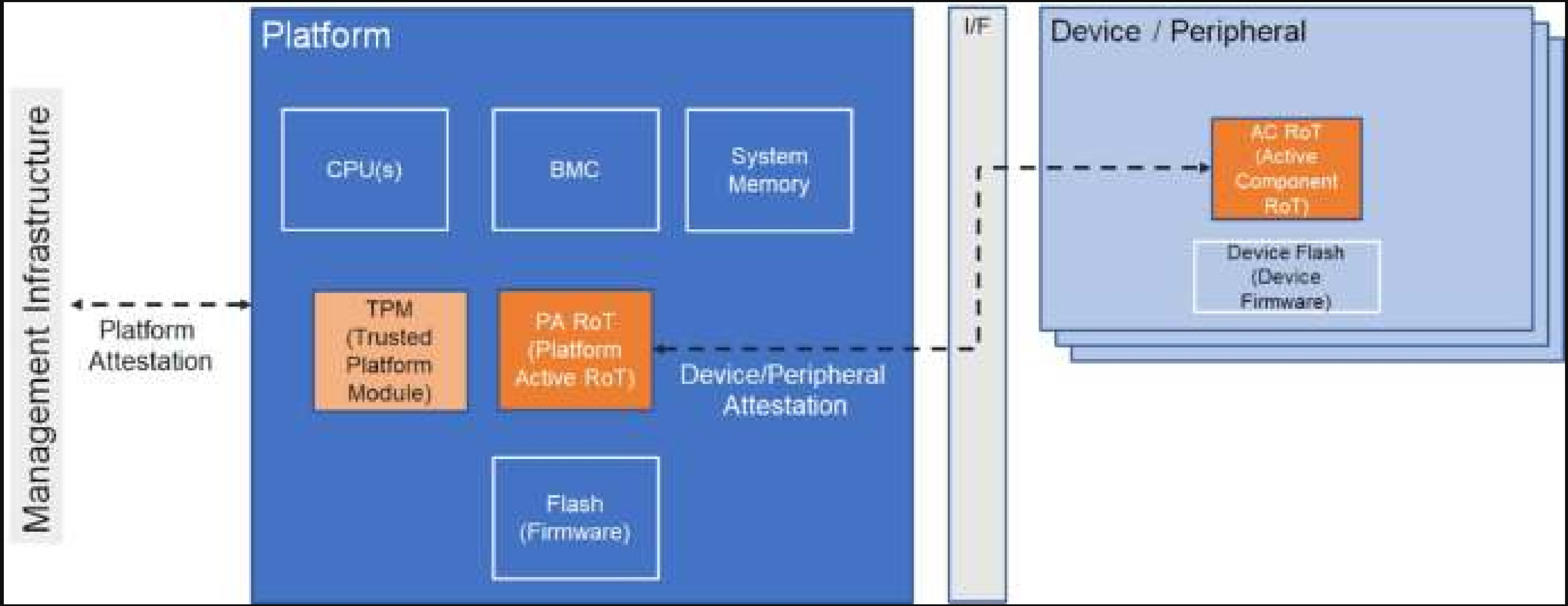
- Business context: Enterprise/EDGE Servers + HPC
  - Hardware is managed by a Baseboard Management Controller (BMC), Racks by RMC, Power by PMC, Hydro by HMC, etc.

- BMC firmware
  - U-boot
  - BMC OS
- BMC Recovery firmware
- UEFI BIOS
- OS
- CPUs
  - Microcode
  - GPUs
- Devices
  - NIC
  - Disk
- FPGA/CPLD
  - 1, 2?... 9!

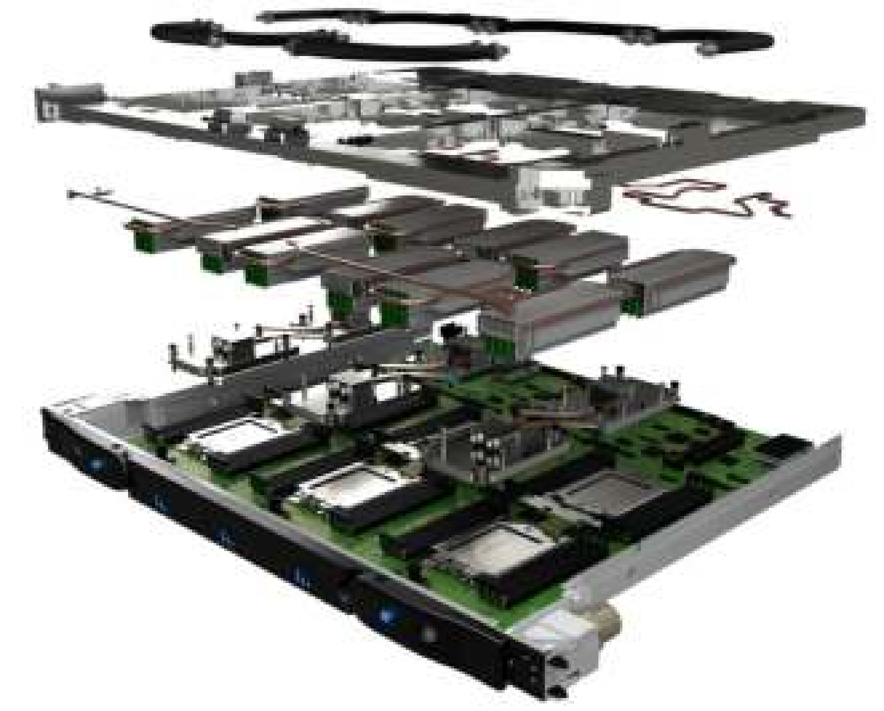
Sl#	Device Name	Device Type
1	MAIN FPGA	FPGA
2	IO FPGA	FPGA
3	PCPLD	CPLD
4	PFR CPLD	CPLD
5	MSM FPGA	FPGA
6	GPU CPLD0	CPLD
7	GPU CPLD1	CPLD
8	EDSFF CPLD 0	CPLD
9	EDSFF CPLD 1	CPLD

Open Compute Project

ARM, Meta, IBM, Intel, Nokia, Google, Microsoft, Dell, Hewlett Packard Enterprise, NVIDIA, Cisco, Lenovo and al…



The HPC challenge
Finding room for trust



- BullSequana X2410
  - 3 Compute nodes
  - 2 AMD Epyc Processors per node
- BullSequana XH2000
  - 32 blades per cabinet = 96 compute nodes
  - 30 cabinets = 5760 CPU
  - + management nodes, storage nodes, etc.

BullSequana Root-of-Trust Design

Why ATOS made a different choice

Sovereignty	Unknown hardware is difficult to trust.	Use well- known hardware
Flexibility	Need to address all kind of hardware (Edge to HPC) with different physical constraints	No additional hardware
Agility	Ability to add rapidly additional security features	Software based security
Agnostic	All our products to benefit of the same recoverability features whatever their CPU / GPU / HW	BMC is the RoT
Hardware security level	Leverage existing security hardware features to anchor security	Use ARM TrustZone

Components for BullSequana Trusted Computing Base

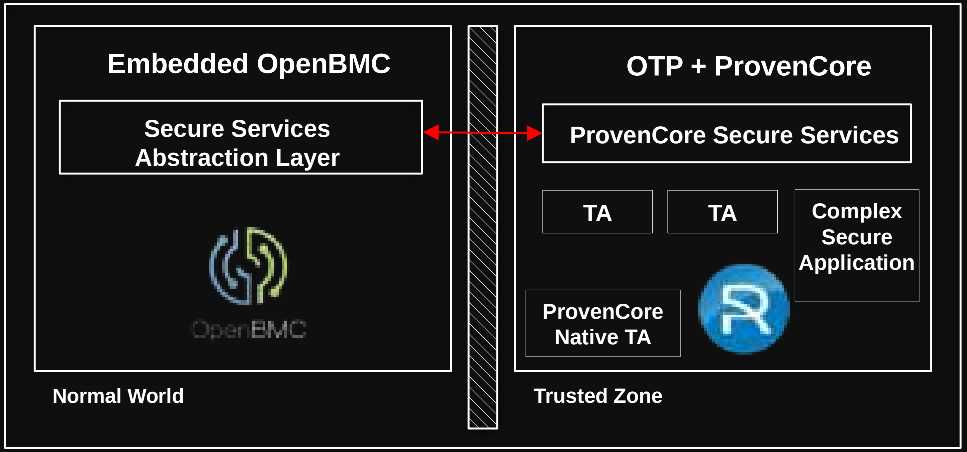
Certifiable at high level

- ARM OTP mechanism
  - Well-known security feature to anchor keys and secure configuration of the SoC ARM core
- ARM TrustZone
  - Simple and robust technology used in cell phones for years
- Secure OS (ProvenCore)
  - µOS whose security has been mathematically proven
  - Evaluation Assurance Level (EAL) 7 is the highest level of evaluation for Common Criteria
  - It means that the security properties are immune to ANY input presented to the OS

Platform Firmware Resiliency

Initial level of PFR

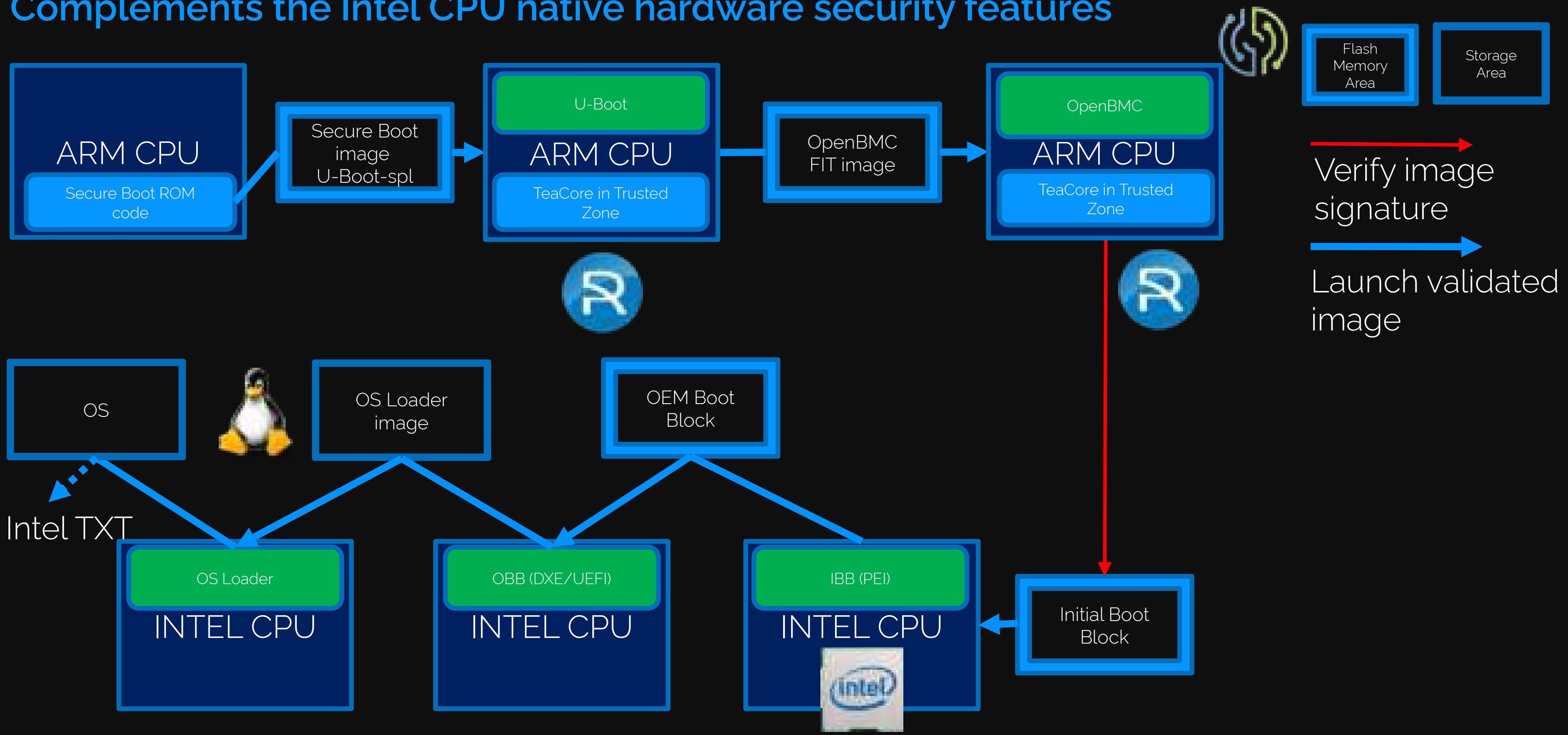
- Chain-of-Trust for Detection - CTD (Secure boot)
  - BMC FW boot / BIOS/OS boot
    - ARM CPU OTP provides HW Root of Trust
    - ProvenCore is launched as a second stage for boot. It stores keys securely.
    - ProvenCore double checks the initial boot stage of the host OS



- Chain-of-Trust for Upgrade – CTU (Firmware Update)
  - ProvenCore is the Root of Trust for any FW component update (BMC, CPLD, FPGA, BIOS)

Chain-of-Trust for Detection

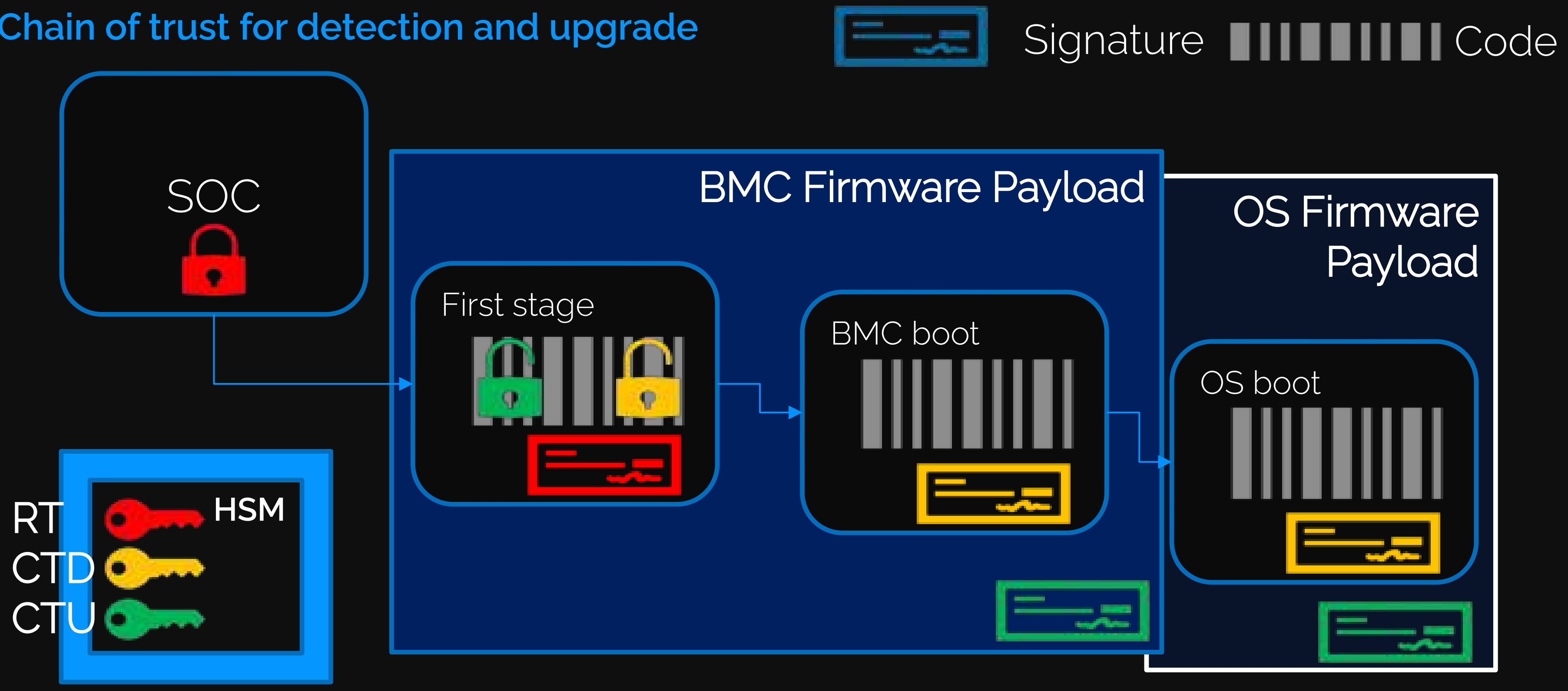
Complements the Intel CPU native hardware security features



Atos

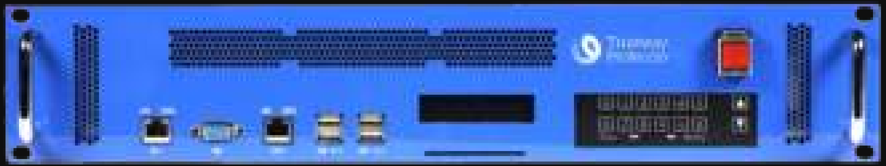
Root-of-Trust overall scheme

Chain of trust for detection and upgrade



Certified HSM appliance

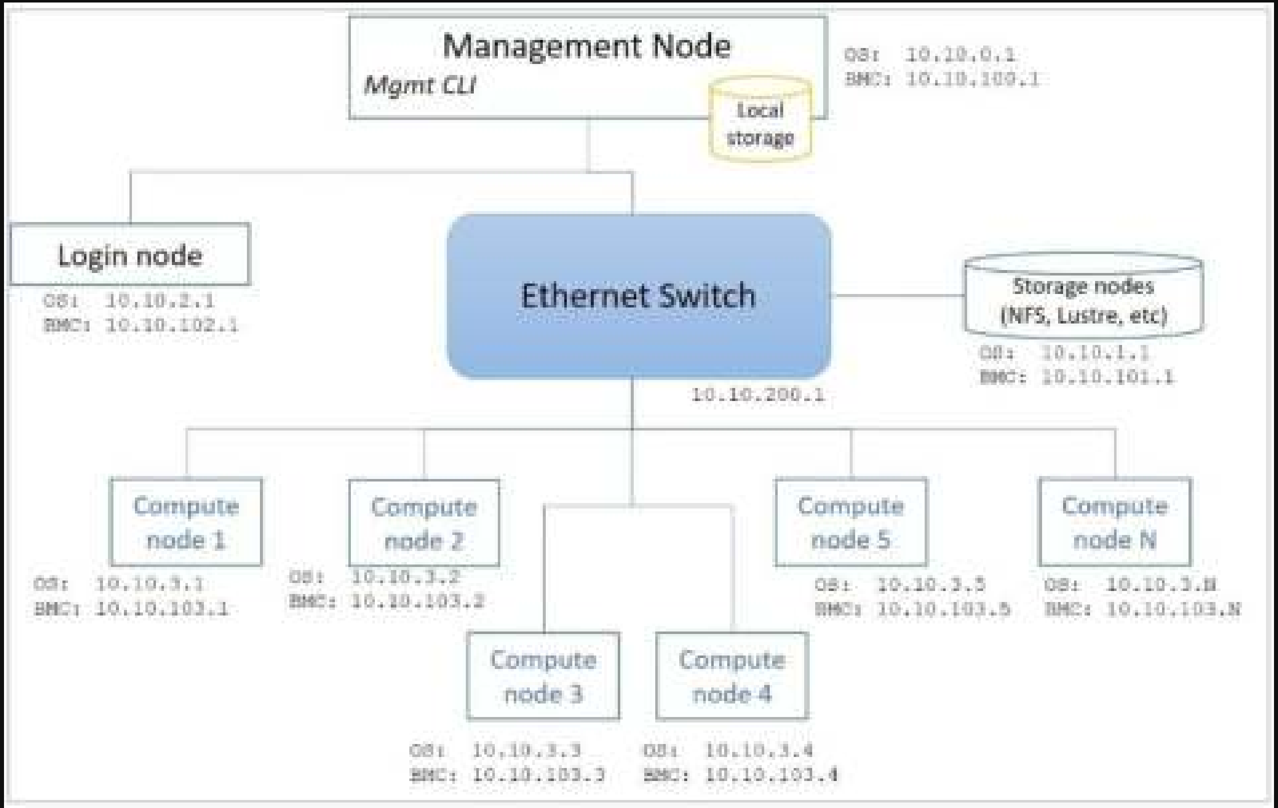
Trustway Proteccio by Atos



Keys	Backup Shamir Scheme	Usage
DEV	1 out of 3	Automated
PROD CoT	3 out of 6 on 2 sites	Automated
PROD RoT	3 out of 6 on 2 sites	CIK: 1 out of 3
SPARE RoT	3 out of 6 on 2 sites	From backup only

Atos

Addressing the HPC challenge
Using Trusted Execution Architecture (TEA) in each BMC



- All 2000+ nodes have a BMC with TEA
- We have the eggs; we can build the chicken!
- We can build a shared secret known to the TEAs
- And use it to protect internal communications

Conclusion

And envisioned next steps

- Next generation of BullSequana servers from Edge to Cloud and HPC will embed a Trusted Execution Architecture

- Trust in Atos' TEA is founded on:
  1. Public cryptographic root-of-trust keys anchored in silicon.
  2. Private keys protected by an RGS certified Atos Trustway Proteccio HSM.
  3. The well-known ARM TrustZone technology embedded in the existing BMC component of our platforms.
  4. The hardened operating system TeaCore developed by ProvenRun on Atos specification and based on their formally proven and EAL7 certified operating system ProvenCore

- Initial security features implemented:
  1. Secure Boot (Chain-of-Trust for Detection)
  2. Firmware update (Chain-of-Trust for Upgrade)

- Envisioned next steps
  - Internal and third-party security assessment
  - Leverage the benefit from a Trusted Execution Environment to develop additional security features (e.g., TPMfw)
  - Adapt CTD to other CPUs such as EPI's chips
  - Take in account hybrid architectures mixing devices from different vendors

Atos

Thank you!

For more information please contact:
M +33 675 084 850
florent.chabaud@atos.net