# Root-of-Trust Manufacturing

AMUSEC 2023

Florent Chabaud
Chief Product Security Officer
26 May 2023



an atos business

EVIDEN

An Atos business

- We're a **circa €5 billion revenue** Atos business that will become an independent company in late 2023.
- **A new digital scale-up** where brilliant minds come together to sustainably expand the possibilities of data and technology.
- We cover **6 segments:** Digital Transformation, Smart Platforms, Cloud, Advanced Computing, Digital Security and Net Zero.
- We're unique in being able to bring all these capabilities holistically for our clients with the **combination of our own IP and of the IP of our leading partners.**

**57,000** engineers and problem-solvers in 45 countries.

**Worldwide #1** in managed security services

**European #1** high-performance computing

**Visionary** In Public Cloud

**Leader** in Data & Analytics

Deep expertise in technology and data value chains: **2,100 patents, 50,000+ certifications**

# Trust is not Security

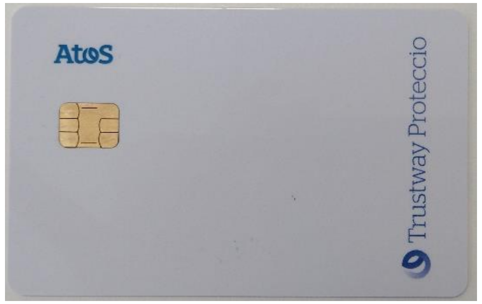
## Years of debates: should you trust cryptography?

- 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

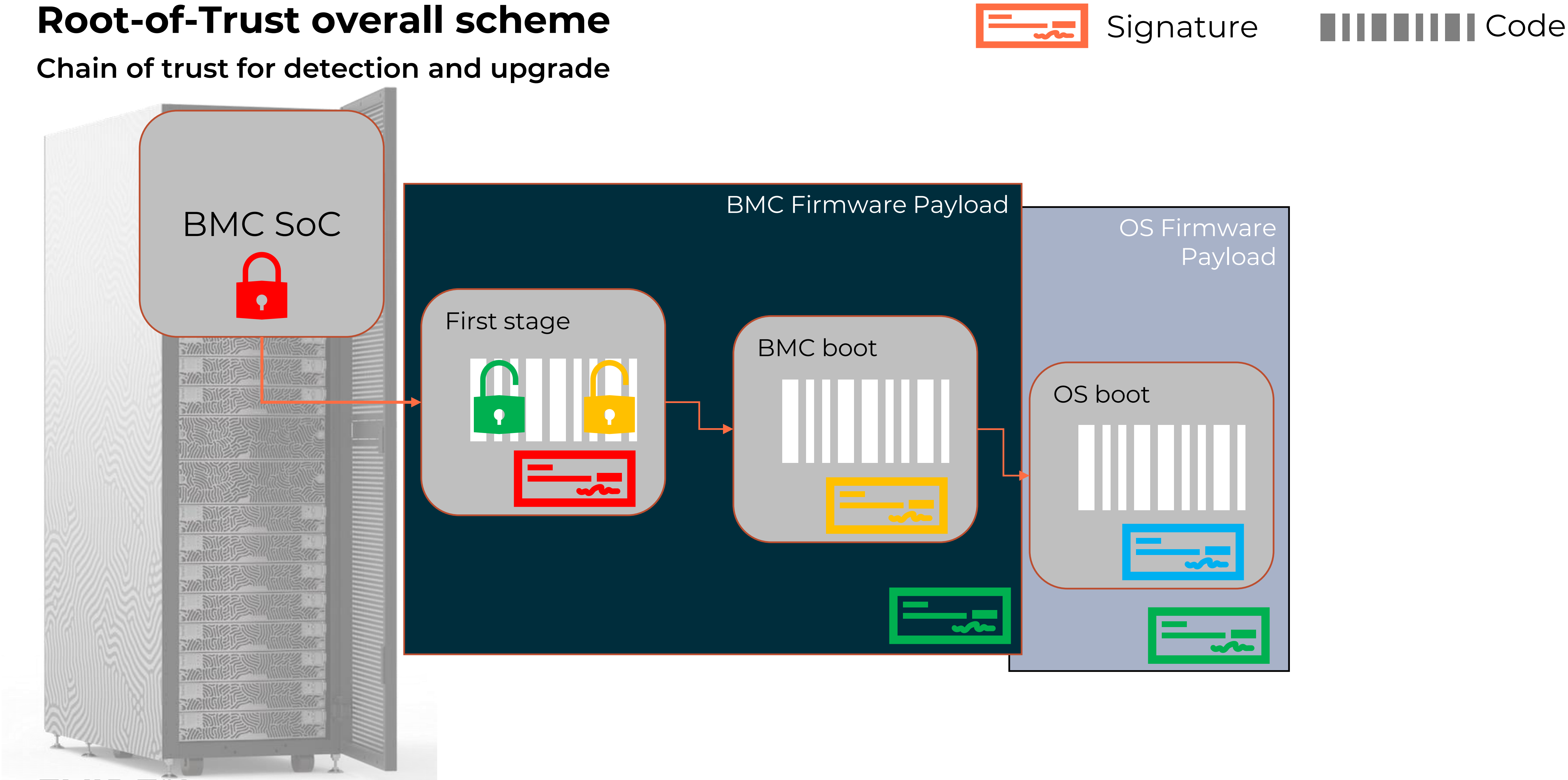
## An application of Kerckhoffs' second principle

- Minimize the  data to protect from threats
- Everything can be public but secret & private keys
- Everything can be changed but public keys
- Hardware makes sense to protect confidentiality and integrity (e.g. smart card)




# Root-of-Trust overall scheme

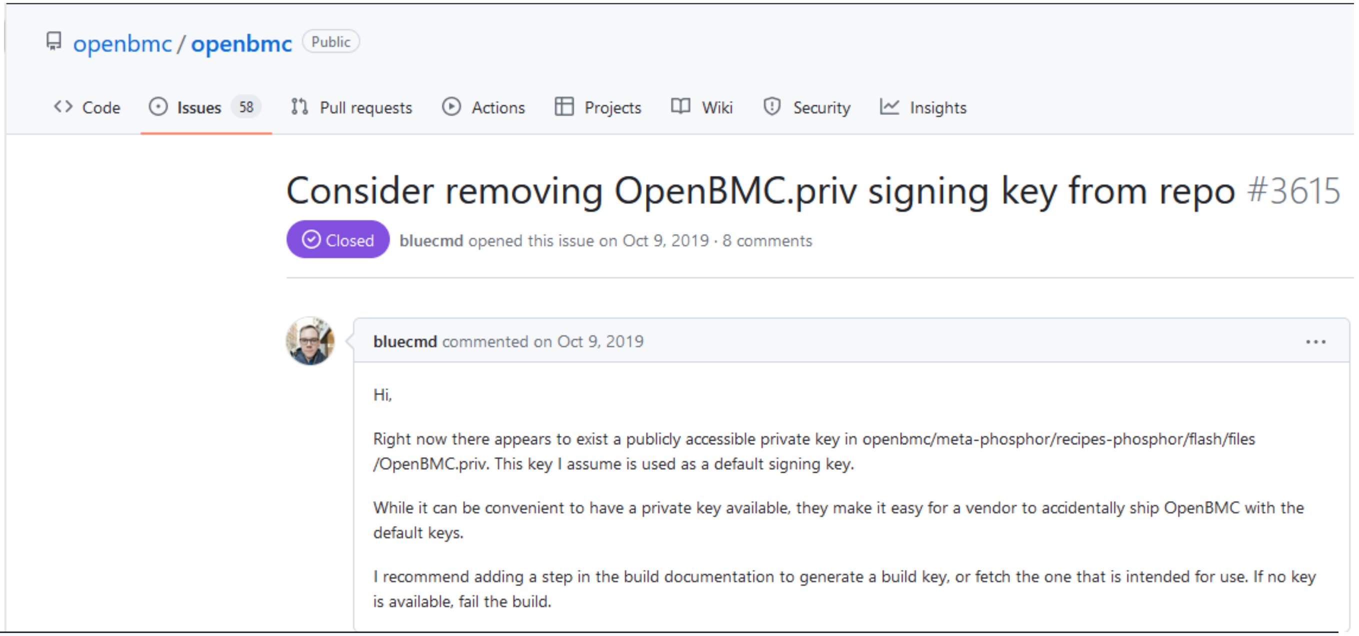
## Chain of trust for detection and upgrade

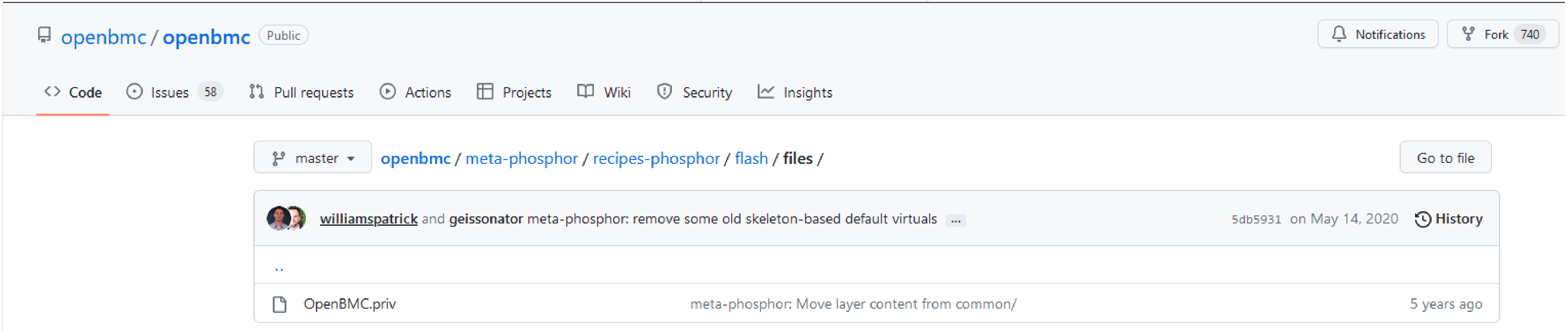


# The manufacturing problem

## Where is the key?

- Activating Secure Boot is super easy
- Assessing the verification feature is OK
- But:
  - How do you ensure the key integrity?
  - How do you handle compromise keys?
  - What about the signing feature security?



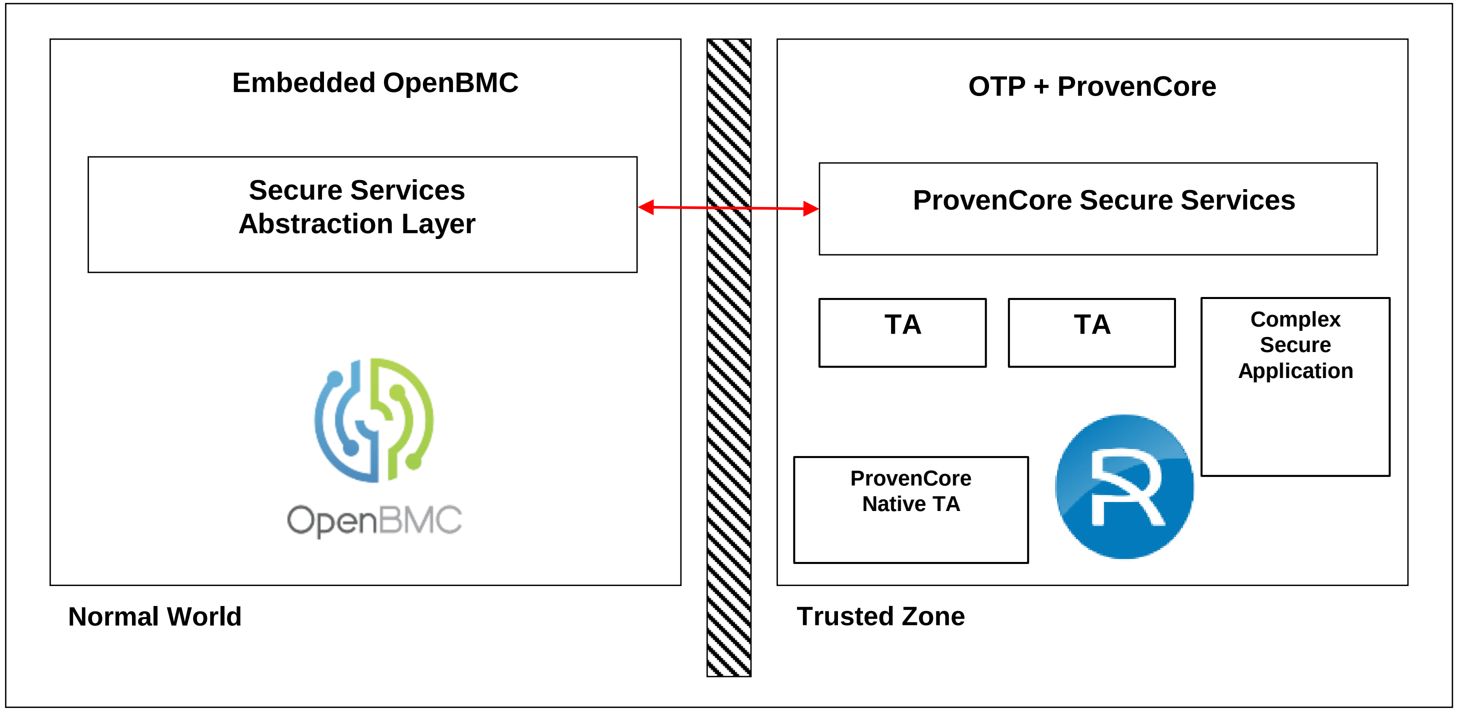



# Trusted Computing Base

## Trusted Execution Environment

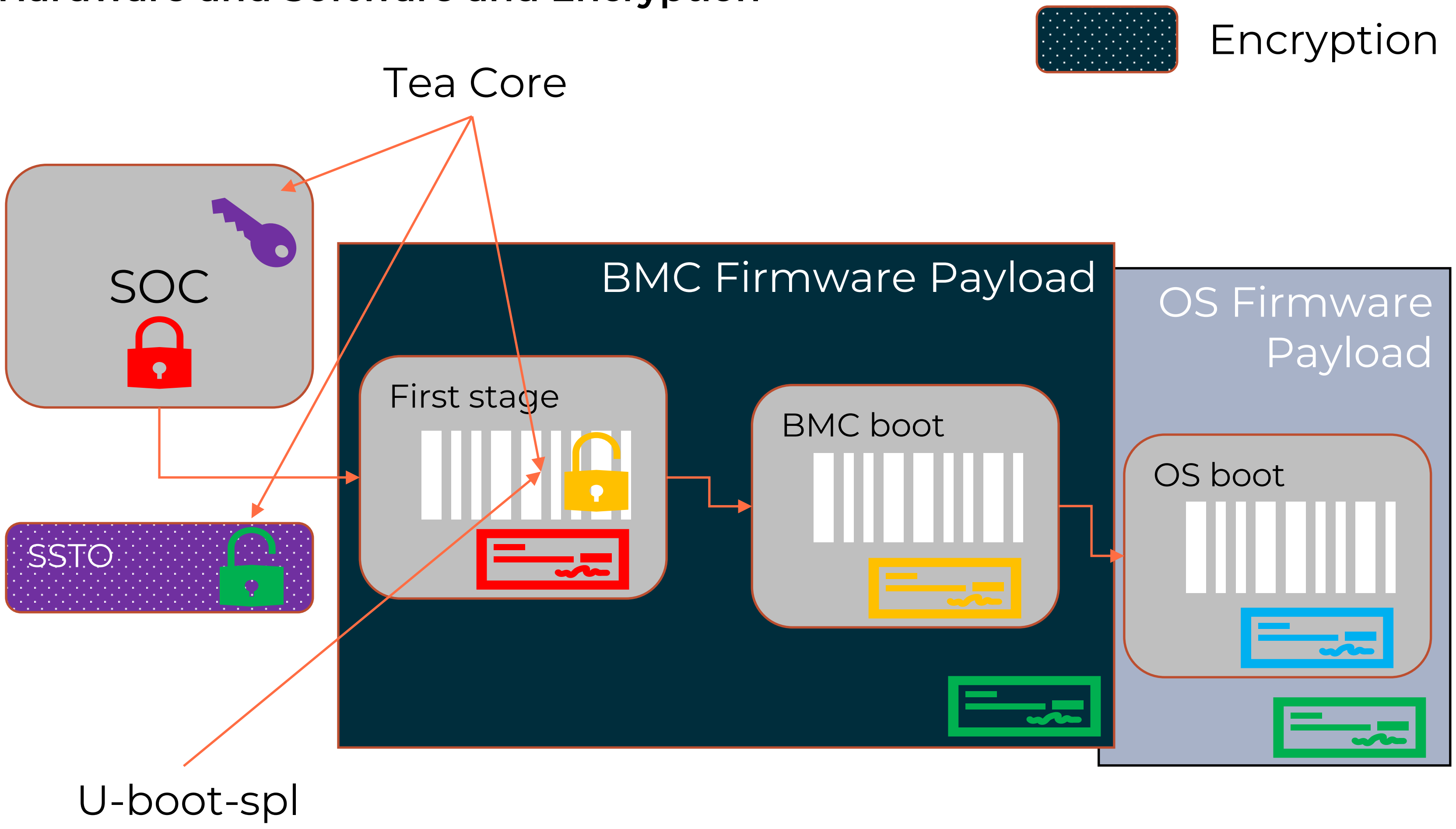
- **Chain-of-Trust for Detection - CTD (Secure boot)**
  - BMC FW boot / BIOS / OS boot
    - ARM CPU OTP provides HW Root of Trust
    - ProvenCore is launched as a second stage for boot. It stores keys securely.
    - ProvenCore double checks the initial boot stage of the host OS
- **Chain-of-Trust for Upgrade – CTU (Firmware Update)**
  - ProvenCore is the Root of Trust for any FW component update
  - Public CTU Key is hosted in an encrypted partition secured by SoC cryptoprocessor

TeaCore



# Key integrity

## Hardware and Software and Encryption



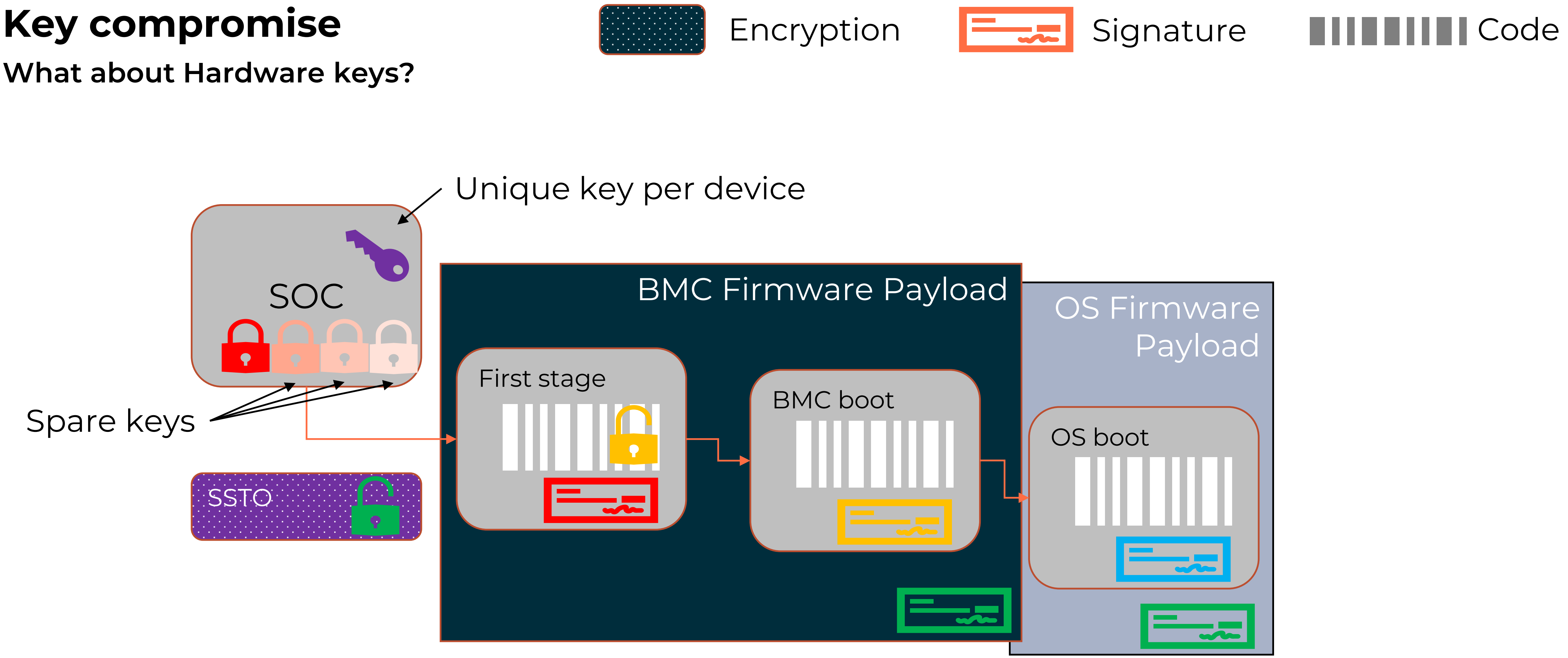

```
BSA2P0c03

U-Boot SPL 2019.04 (Mar 14 2023 - 11:51:32 +0000)
already initialized, Trying to boot from RAM
## Checking hash(es) for Image provencore ... sha256,rsa4096:K_Atos_CTD_PROD+ OK
## Checking hash(es) for Image uboot ... sha256,rsa4096:K_Atos_CTD_PROD+ OK
## Checking hash(es) for Image fdt ... sha256,rsa4096:K_Atos_CTD_PROD+ OK
Booting Provencore

Copyright (c) 2014-2022, ProvenRun S.A.S and/or its affiliates. All rights reserved.
ProvenCore  - version 85ca4a11a5b3 (0) / c3b37ae3bb6e (0)
Mar 10 2023 - 14:44:02 +0100
Cpu Cortex-A7 r0p5 midr:0x410fc075, revidr:0x1
Booted on core 0 in privileged mode.
```

```
## Loading kernel from FIT Image at 20600000 ...
   Using 'conf-openbmc_atos.dtb' configuration
   Verifying Hash Integrity ... sha256,rsa4096:K_Atos_CTD_PROD+ OK
   Trying 'kernel-1' kernel subimage
     Description:  Linux kernel
     Type:         Kernel Image
     Compression:  uncompressed
     Data Start:   0x206000ec
     Data Size:    4524104 Bytes = 4.3 MiB
     Architecture: ARM
     OS:           Linux
     Load Address: 0x80001000
     Entry Point:  0x80001000
     Hash algo:    sha256
     Hash value:   d689ab6270e1ed90d2b8c333bafdedb80ec28fffabb615f32af7658179d35a6d
   Verifying Hash Integrity ... sha256+ OK
## Loading ramdisk from FIT Image at 20600000 ...
   Using 'conf-openbmc_atos.dtb' configuration
   Verifying Hash Integrity ... sha256,rsa4096:K_Atos_CTD_PROD+ OK
   Trying 'ramdisk-1' ramdisk subimage
     Description:  obmc-phosphor-initramfs
     Type:         RAMDisk Image
     Compression:  uncompressed
     Data Start:   0x20a7901c
     Data Size:    1125340 Bytes = 1.1 MiB
     Architecture: ARM
     OS:           Linux
     Load Address: unavailable
     Entry Point:  unavailable
     Hash algo:    sha256
     Hash value:   090ce6afd3d4210c5c6ee9174b770176b87a2f61ca7f5f51a30c5309b8e0501c
   Verifying Hash Integrity ... sha256+ OK
## Loading fdt from FIT Image at 20600000 ...
   Using 'conf-openbmc_atos.dtb' configuration
   Verifying Hash Integrity ... sha256,rsa4096:K_Atos_CTD_PROD+ OK
   Trying 'fdt-openbmc_atos.dtb' fdt subimage
     Description:  Flattened Device Tree blob
     Type:         Flat Device Tree
     Compression:  uncompressed
     Data Start:   0x20a50a44
     Data Size:    165130 Bytes = 161.3 KiB
     Architecture: ARM
     Hash algo:    sha256
     Hash value:   ce567b944c3d2a043ec4734a109b1695e9c656bb3d71e3b28dfe0a224ce461d1
   Verifying Hash Integrity ... sha256+ OK
   Booting using the fdt blob at 0x20a50a44
   Loading Kernel Image ... OK
   Loading Ramdisk to 8feed000, end 8ffffbdc ... OK
   Loading Device Tree to 8fec1000, end 8fec509 ... OK
```

EVIDEN

# Key compromise

## What about Hardware keys?

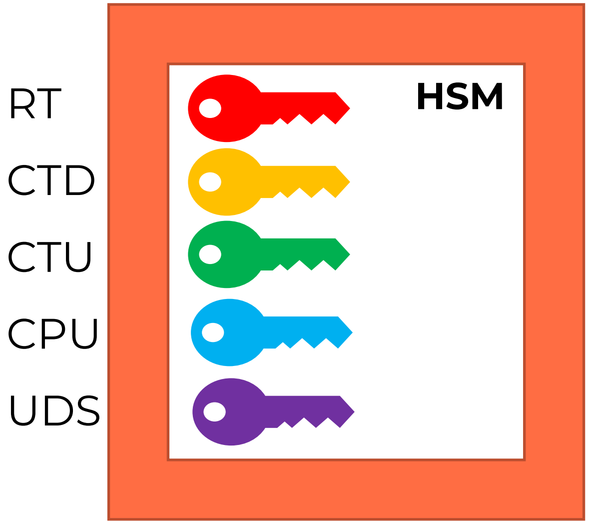


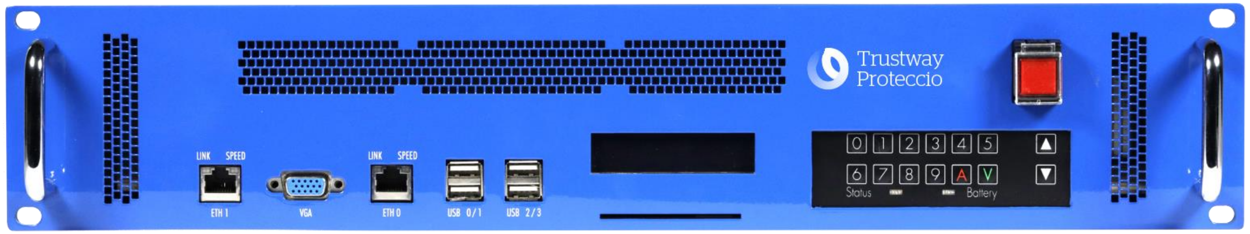
# Signing feature security

## All private keys stored in HSM

- Atos Trustway Proteccio is certified by ANSSI
- Backup Shamir Scheme protects CIA of keys
- DEV vs. PROD to ease development

| 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 |



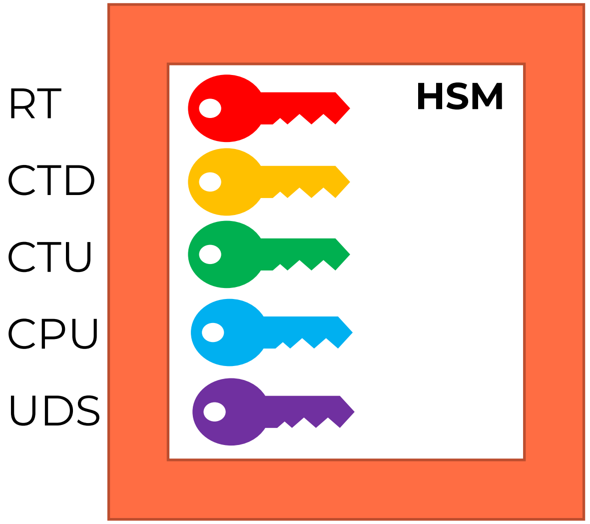

# Signing feature security

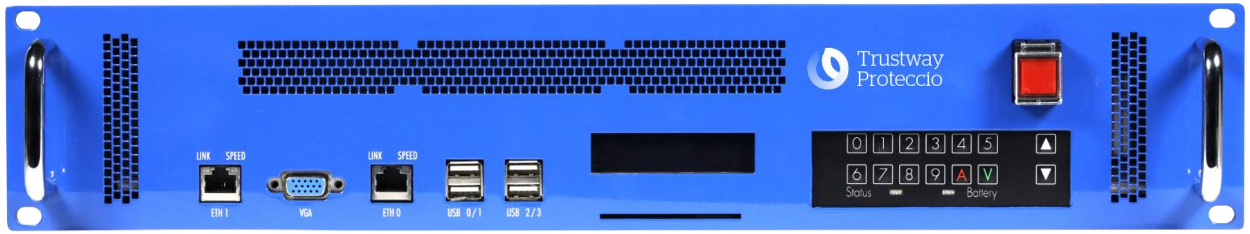
## All private keys stored in HSM

- Atos Trustway Proteccio is certified by ANSSI
- Backup Shamir Scheme protects CIA of keys
- DEV vs. PROD to ease development

| 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~~ Automated |
| SPARE RoT | 3 out of 6 on 2 sites | From backup only |

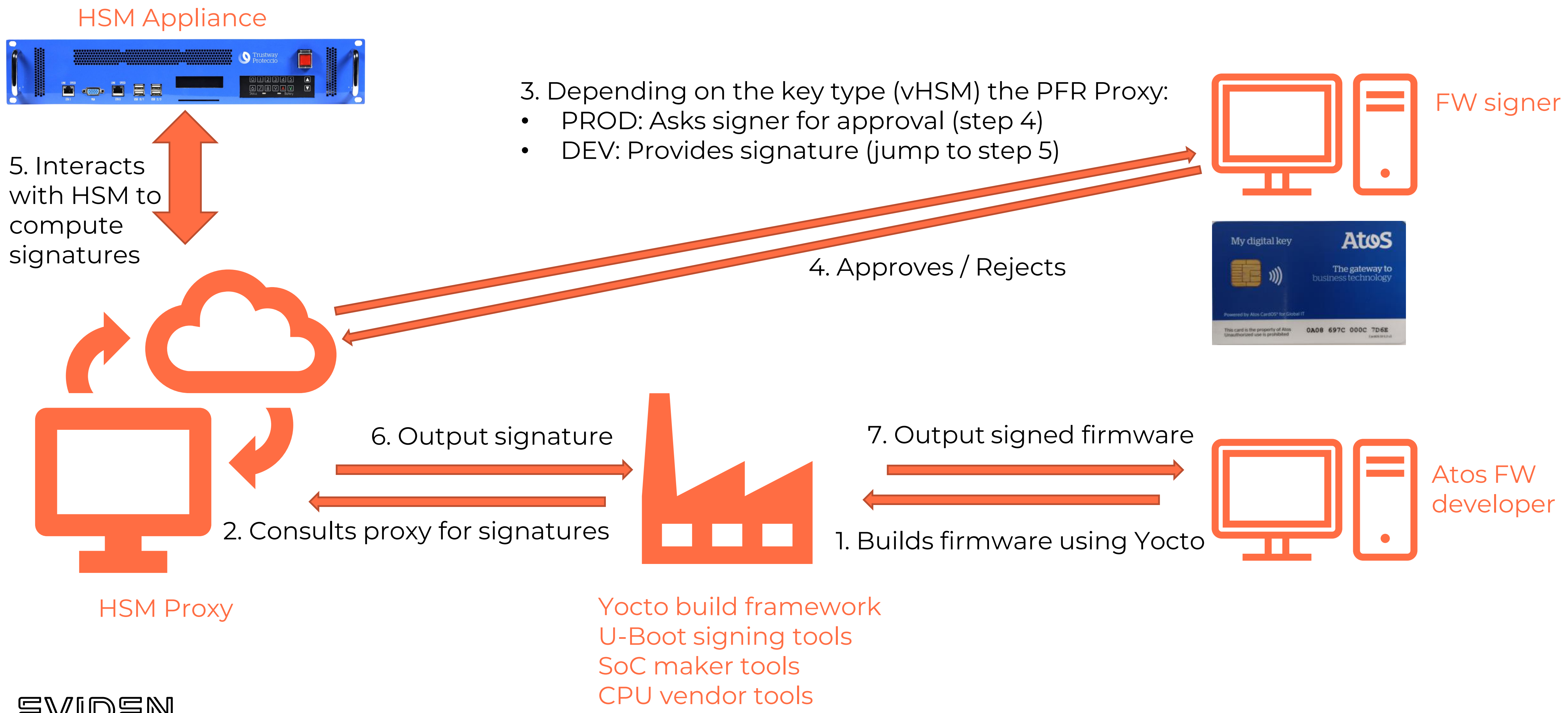
**Where is the pin?**



# Firmware approval framework

## How to control the signature process



# Conclusion

## This is just the beginning

**Trusted Execution Architecture in new Eviden servers**

- Implementing Root-of-Trust is not just a cryptographic matter
- Designing processes is as important as implementation
- Development and Manufacturing phases must be carefully designed

**Initial Security Features**

- Secure Boot (Chain-of-Trust for Detection)
- Firmware update (Chain-of-Trust for Upgrade)

**Trust in Eviden's TEA has strong foundations**

- Root-of-trust keys anchored in silicon.
- Private keys protected by an HSM Trustway Proteccio.
- ARM TrustZone embedded in the existing BMC
- Hardened µOS TeaCore developed by ProvenRun

**Envisioned next steps**

- Leverage the benefit from a TEE for additional security features
- Adapt CTD to other CPUs such as EPI's chips
- Hybrid architectures mixing devices from different vendors

# Questions

## Follow our Journey

**Follow us at**
www.twitter.com/EvidenLive
www.linkedin.com/Eviden
www.Instagram.com/EvidenLive
https://www.youtube.com/@Evidenlive

## Visit our Website

**Visit** www.eviden.com

For more information, please contact:

Florent.Chabaud@eviden.com