👋 FOSDEM 2026 🎉

Open source firmware for high assurance confidential infrastructure

FOSDEM 2026 - Confidential Computing devroom

Michał Żygowski & Piotr Król

Kudos

- **Andrew Cooper** - XenServer, Xen maintainer
- **Demi Marie Obenour** - Spectrum OS
- **Paul Grimes** - AMD
- **Rich Persaud** - Platform Security Summit
- **Sid Hussmann** - CTO & Co-Founder, Gapfruit
- **Tim Ansell** - wafer.space
- **Zir Blazer** - Dasharo Community Top Contributor

whoami

Michał Żygowski

3mdeb Senior Firmware Engineer

- coreboot core developer
- Maintainer: Braswell, PC Engines, Protectli, MSI
- AMD OpenSIL contributor

🔑 `00B8 8FB2 5FD6 375B C5FF 195D 6B5B A214 D21F CEB2`

✉️ michal.zygowski@3mdeb.com

🐦 @_miczyg_ · 💻 GitHub

Piotr Król

3mdeb Founder

- Open-source firmware evangelist
- Conference speaker and organizer
- OpenSecurityTraining2 Instructor

🔑 `5468 873B 74F1 6315 2785 D2CC 67D4 F3E3 72CB C3A9`

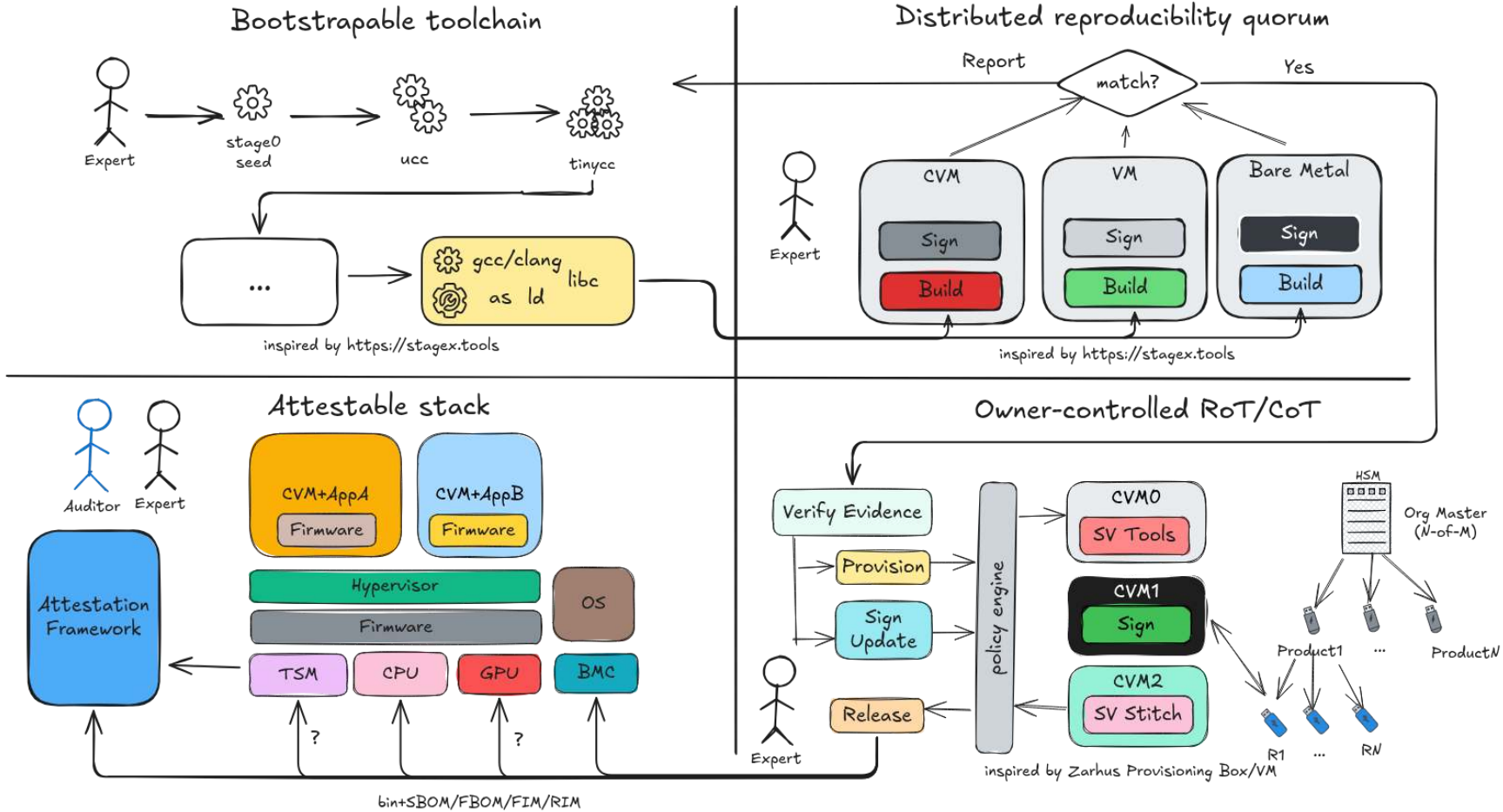
✉️ piotr.krol@3mdeb.com

🐦 @pietrushnic · 💻 GitHub

What We Will Cover

- Why do we need high assurance confidential infrastructure?
- High assurance architects have serious concerns about how responsibilities concentrate in various components of modern platforms
- Open-source firmware **complements** CC features to deliver together platform which helps grow open ecosystem in building such infrastructure
- Why home/SME environments matter:
  - Educational space for motivated engineers to build CC expertise
  - Open ecosystems thrive in home/SME as sovereign alternative
  - **Retail hardware, not cloud unobtanium** (RAMpocalypse pricing aside 💸)
- What we will show:
  - The firmware trust problem: who audits the foundation?
  - OpenSIL + coreboot on retail EPYC with SEV-SNP (live demo!)
  - Before/after: from proprietary to auditable stack

High Assurance Confidential Infrastructure 2026






Firmware

- **Era 1** (1975-1994): Proprietary
  - IBM BIOS → Phoenix
- **Era 2** (1994-2014): Openness
  - LinuxBIOS, U-Boot
- **Era 3** (2014+): Standardization
  - Intel FSP, openSIL, openSFI

Confidential Computing

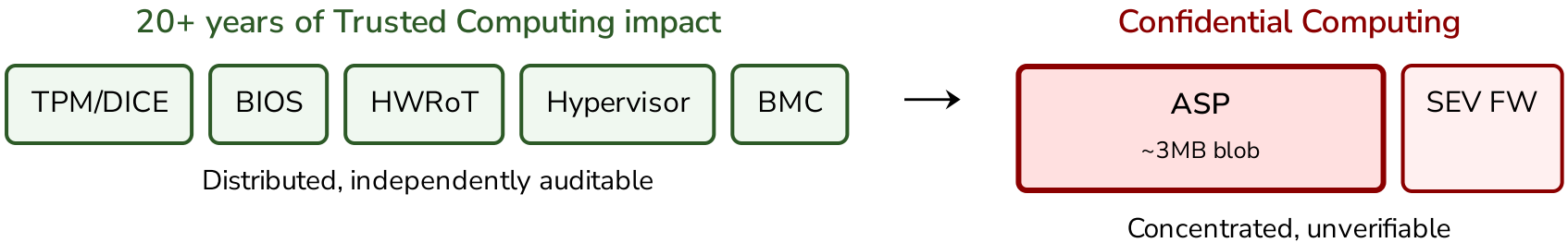
- **Era 1** (2015-2019): Proprietary
  - Intel SGX, AMD SEV
- **Era 2** (2019+): Opening Up
  - IBM PEF, Keystone, ARM CCA
- **Era 3** (2024+): Standardization
  - SEV-TIO, TDX, SPDM/IDE/TDISP

AMD SEV Evolution: A Decade of Iteration

Generation	Key Addition	Threat Addressed	CVEs
Naples (2017)	SME/SEV + SEV-ES	Cold boot, hypervisor introspection	n/a
Rome (2019)	GPA salting, ring buffer	Memory remapping attacks	n/a
Milan (2021)	SEV-SNP, RMP, attestation	Memory replay, integrity, aliasing	22
Genoa (2022)	SNP hardening, VLEK	SPL enforcement, CVE mitigation	28
Turin (2024+)	SEV-TIO (TDISP/SPDM)	Malicious PCIe/CXL devices	15+

CVE counts from AMD SEV firmware release notes analysis

The Firmware Trust Problem



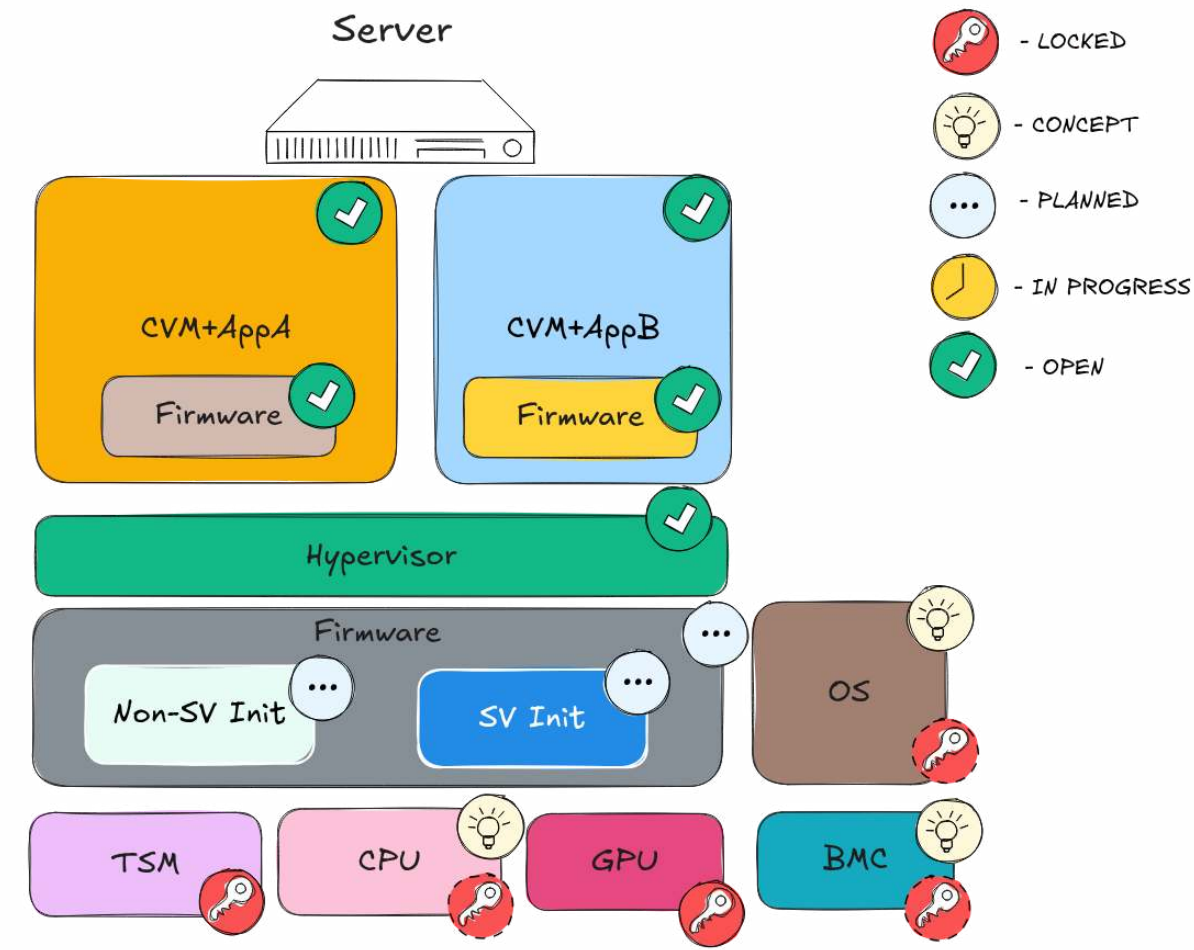
- Intel ME history proves single co-processor concentration is risky
- BIOS reached openness (coreboot, openSIL) - ASP remains opaque ~3MB blob
- Years of boot chain transparency work at risk for centralized single point of failure
- AMD co-founded Caliptra (open RoT) yet ASP contradicts its principles

"Great security compromised by other great ideas … starts to weaken its security posture … want to keep it very clean."

Bryan Kelly (Microsoft), Caliptra architect — OCP 2022

What We Built

State of HACI - FOSDEM'25



openSIL: Open Source Silicon Initialization

Approach	Source	Integration	Auditable
AGESA	Closed	UEFI-only	❌
Intel FSP	Binary blob	API mode (coreboot) / Dispatch (EDKII)	❌
openSIL	Full source	Static linking	✅

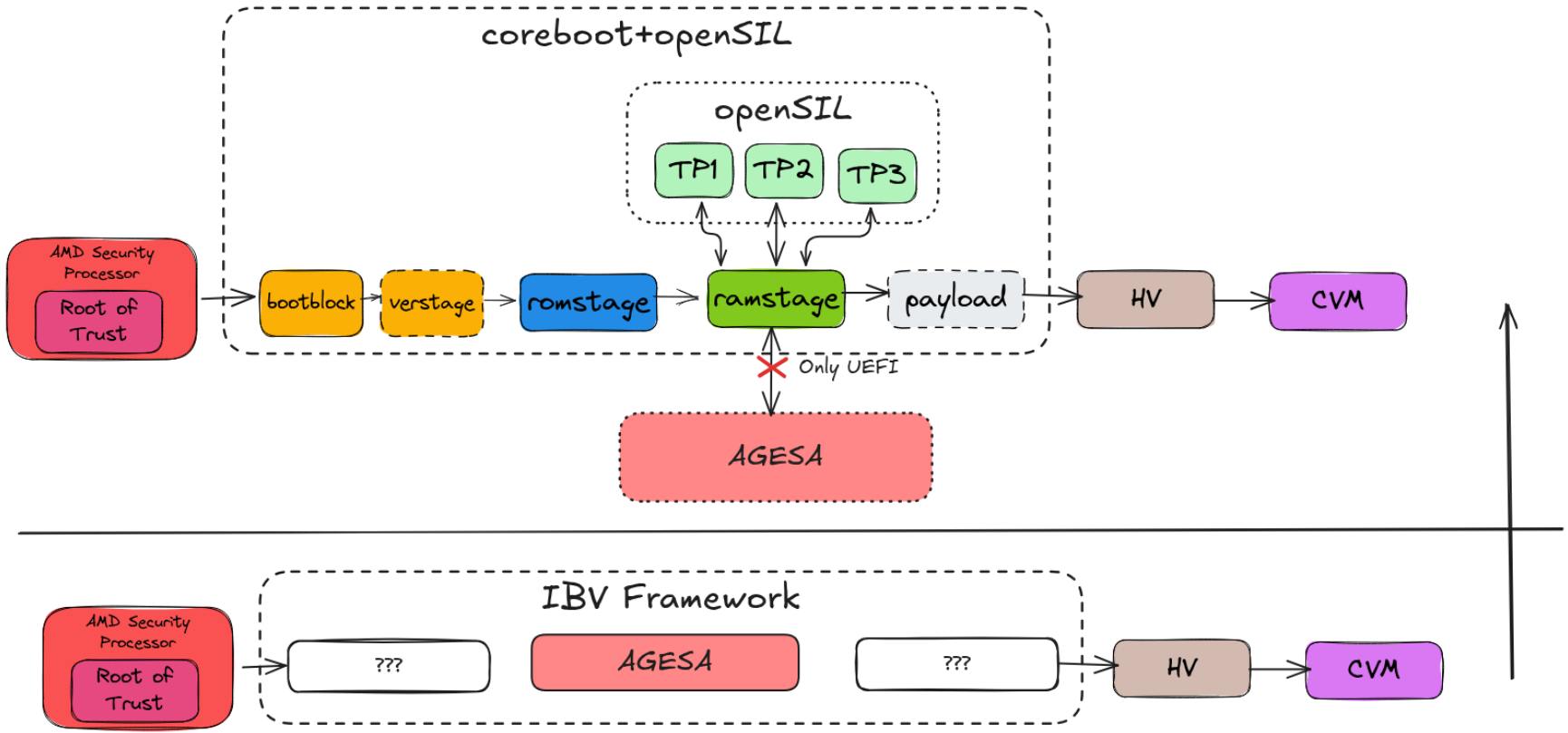
What OpenSIL opens:

- xSIM - Silicon Init (memory, CPU)
- xPRF - Platform Reference FW
- xUSL - Utilities & Services

What remains closed:

- ASP firmware (~3MB blob)
- SEV firmware
- ⚠️ *"ASP is outside the scope"*

> **OCP contribution (Sept 2025):** Spec v1.0 — industry standardization path



GIGABYTE MZ33-AR1

AMD EPYC 9005 Series (Turin) · 5th Gen · Up to 192 cores

Why this board?

- First retail Turin board with coreboot+openSIL
- Retail server hardware
- Building on successful Genoa PoC
- AMD PSB unlikely provisioned
- OpenBMC potential (no ASPEED secure boot)

Implementation Journey

Funded by  — documented in 6 blog posts at blog.3mdeb.com

Month	Milestone	Blog Post
Aug	First serial output	Part 1: Initial porting
Sep	I/O initialization	Part 2: Blob analysis
Oct	PCIe working	Part 4: PCIe mapping
Nov	OS boots	Part 5: ACPI & bugfixes
Dec	Upstream ready	Part 6: Upstream & BMC

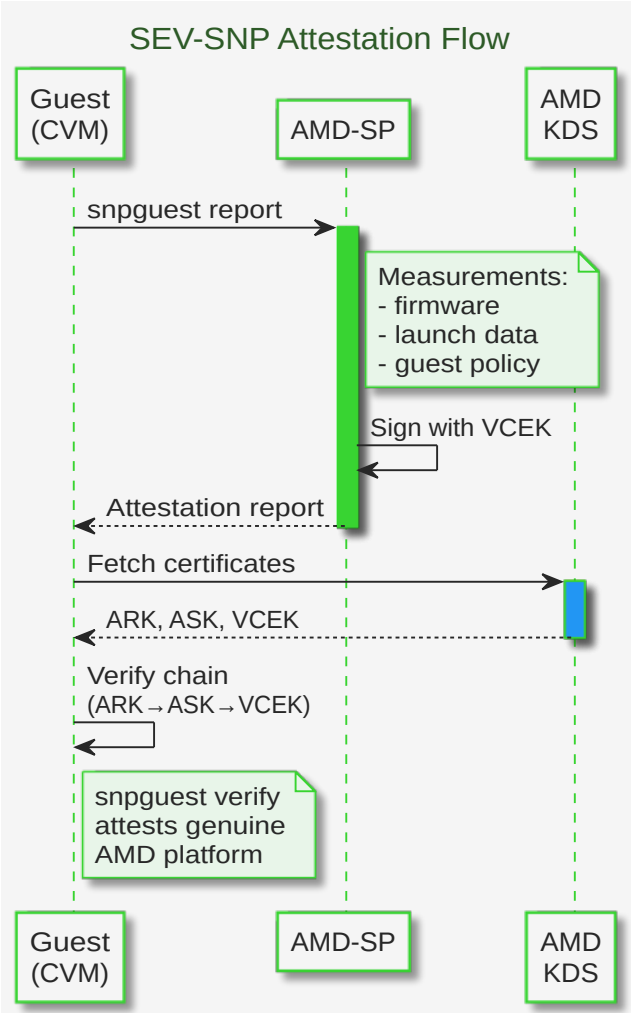
Statistics (w/o SEV-SNP): ~13k LOC · 84 coreboot patches · 7 openSIL PRs · ~3.7% of openSIL codebase

SEV-SNP on Open-Source Firmware

- First retail server board with open-source firmware + SEV-SNP
- No proprietary UEFI BIOS - only ASP blobs remain closed
- Changes pending upstream to coreboot mainline
- Enables cryptographic proof of platform state → attestation

Key Changes (~950 SLOC added):

Component	Change	Purpose
openSIL	PSP MMIO in NBIO init	Enable PSP mailbox for SEV
coreboot	RMP table reservation	Memory integrity protection
coreboot	SEV NVRAM data	PSP SEV initialization
coreboot	AP bring-up mods	Multi-core SEV support
coreboot	ASPT ACPI table	SEV platform info for OS



AMD KDS (Key Distribution Service):

- Public AMD service hosting certificate chain
- Provides ARK, ASK, and per-chip VCEK

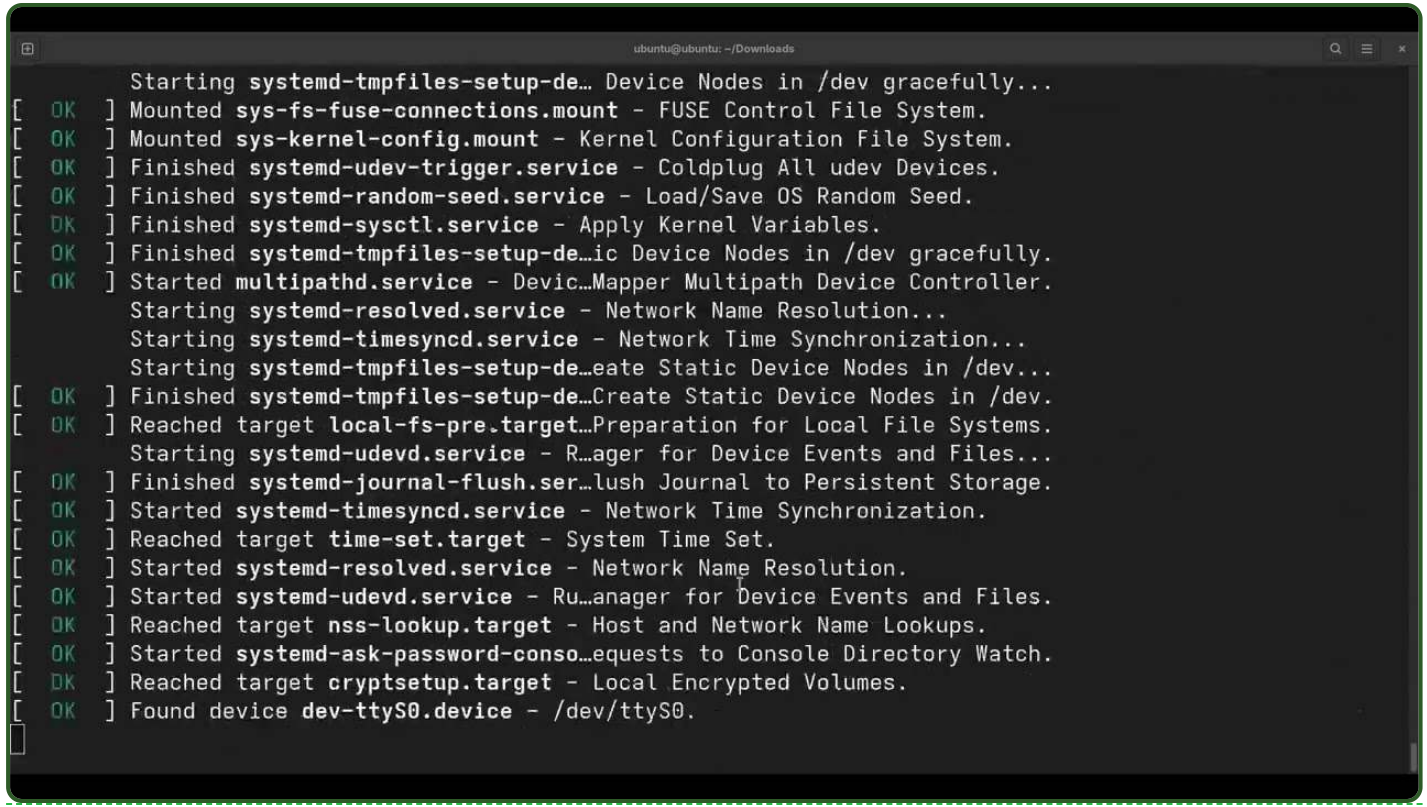
Certificate Chain:

- **ARK** - AMD Root Key (self-signed)
- **ASK** - AMD SEV Key (signed by ARK)
- **VCEK** - per-chip key (signed by ASK)

Attestation Report:

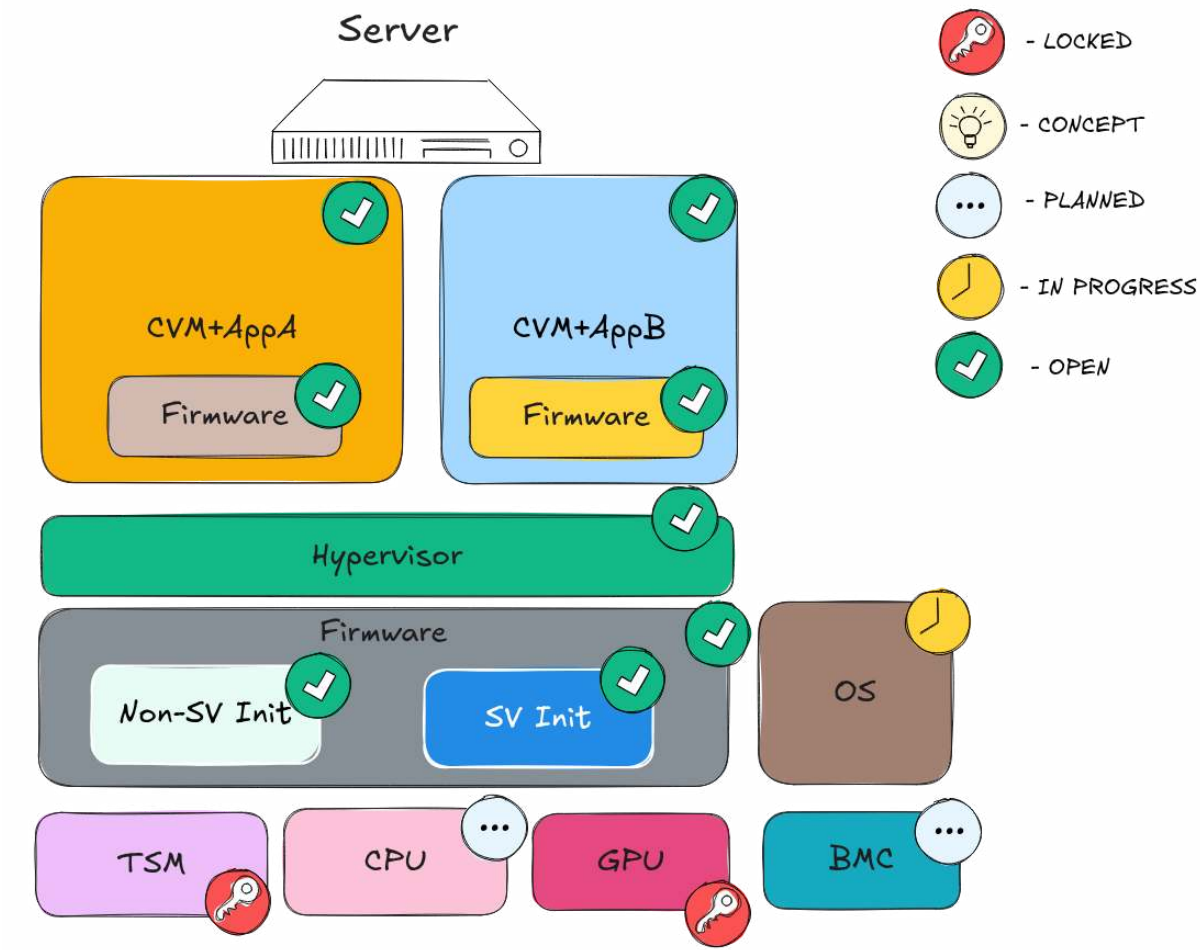
- TCB versions, guest measurements
- Platform info & policy
- Signed by chip-unique VCEK

Demo: SEV-SNP on Open-Source Firmware

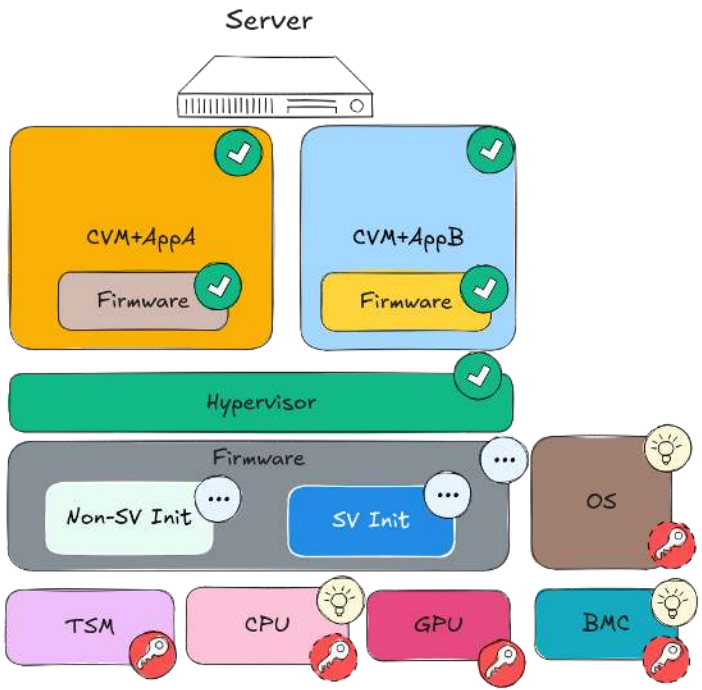


Watch: youtube.com/watch?v=dy_sCNIXEBY

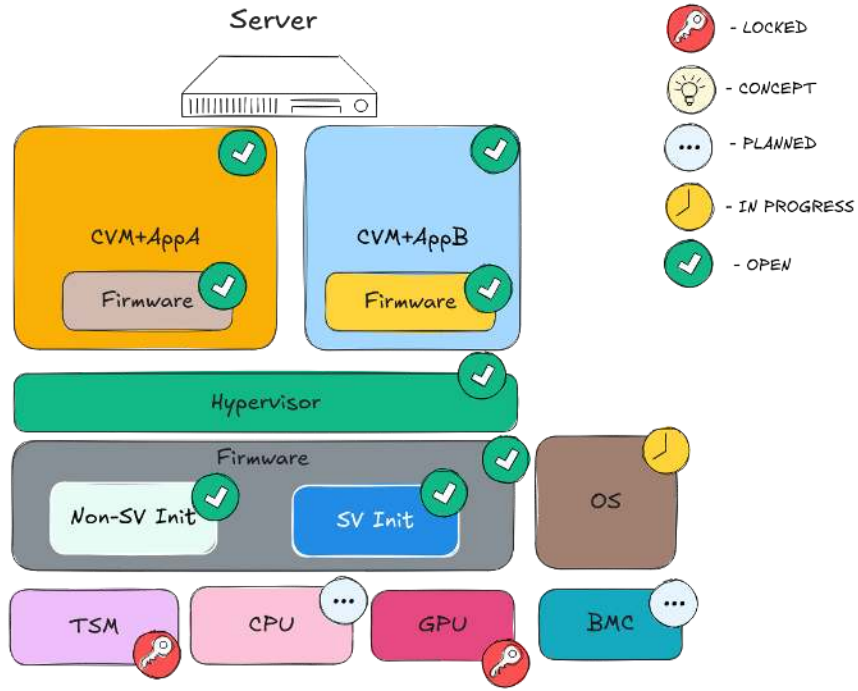
State of HACI - FOSDEM'26



State of HACI - FOSDEM'25



State of HACI - FOSDEM'26



Roadmap: Open-Source Firmware for Confidential Computing

Q1/Q2 2026

- Upstream to coreboot mainline
- Dasharo for Gigabyte MZ33-AR1
  (signed, reproducible, validated)
- Community testing & feedback

→

Q3/Q4 2026

- SEV-TIO (GPU/accelerators)
- TDISP/IDE/SPDM integration
- OpenBMC for MZ33-AR1
- OpenSFI participation

→

2027

- Intel TDX support
- ARM CCA (TF-A/TF-RMM)
- Universal attestation
- Cross-vendor CC ecosystem

Goal: Auditable firmware foundation for all confidential computing platforms

Join us for talks, workshops, and real-world boot security — bsmconf.com

Questions?

Backup Slides

The Trust Paradox

The accepted mindset:

> *"We cannot do anything about firmware. Let the vendor be responsible."*

But history proves otherwise: Proprietary BIOS → coreboot+FSP → coreboot+openSIL → openSFI (future)

The responsibility shift:

Component	Trend
CPU BIOS	Responsibilities moving → ASP
Hypervisor	Responsibilities moving → SEV firmware
OS	Cooperates with silicon vendor, extends trust primitives

Historical pattern: OS complained about BIOS, then hypervisor...

When will OS start questioning silicon vendor firmware?

AMD SEV-SNP Architecture

- **Memory encryption**: AES-128, per-VM keys, C-bit page control
- **RMP**: Hardware-enforced page ownership (prevents remapping attacks)
- **Attestation**: Cryptographic proof of VM launch state

What's in the TCB?

Component	Role	Open?
ASP	Key mgmt, attestation	❌ ~3MB blob
CPU BIOS*	HW init, ASP communication	✅ coreboot+OpenSIL
Hypervisor	VM management	✅ KVM/QEMU, Xen

*AMD nomenclature for system firmware. CPU BIOS openness is our key contribution.

Firmware History: A Lesson for CC?

Era 1: Proprietary (1975-1994)

- Gary Kildall: BIOS for CP/M
- IBM monopoly
- Phoenix clean room → AMI, Award

→

Era 2: Openness (1994-2014)

- IEEE-1275 Open Firmware
- LinuxBIOS, U-Boot (1999)
- AGESA in coreboot

→

Era 3: Standardization (2014+)

- Intel FSP modularization
- AMD openSIL (source open)
- OCP openSFI (2025)

Pattern: Proprietary → Openness → Standardization → *IP shifts to new proprietary component*

Research: Supply Chain Proof

Vulnerability Spectrum Analysis

Analyze CC stack to provide evidence for supply chain claims:

- **Turin SEV firmware release notes** - compare with other platforms
- **AMD Product Security**: https://www.amd.com/en/resources/product-security.html
- **Hypervisor CVEs** - KVM, Xen XSAs
- **Linux kernel SEV-related issues**

Goal: Create chart showing vulnerability distribution by component and which parts are auditable vs black boxes.

Backup: Security Analysis Tools

Platform	Tool	Purpose
AMD PSP	PSPTool	Extract, analyze PSP firmware
AMD SEV	AMD-ASPFW	PSP SEV FW source (Genoa)
Intel ME	MEAnalyzer	Parse ME firmware

Backup: Systemd CC Integration

- **systemd 255+**: Measured boot, UKI with PCR measurements
- **systemd-creds**: TPM2-bound secrets for services
- **systemd-cryptenroll**: LUKS with TPM2 policies