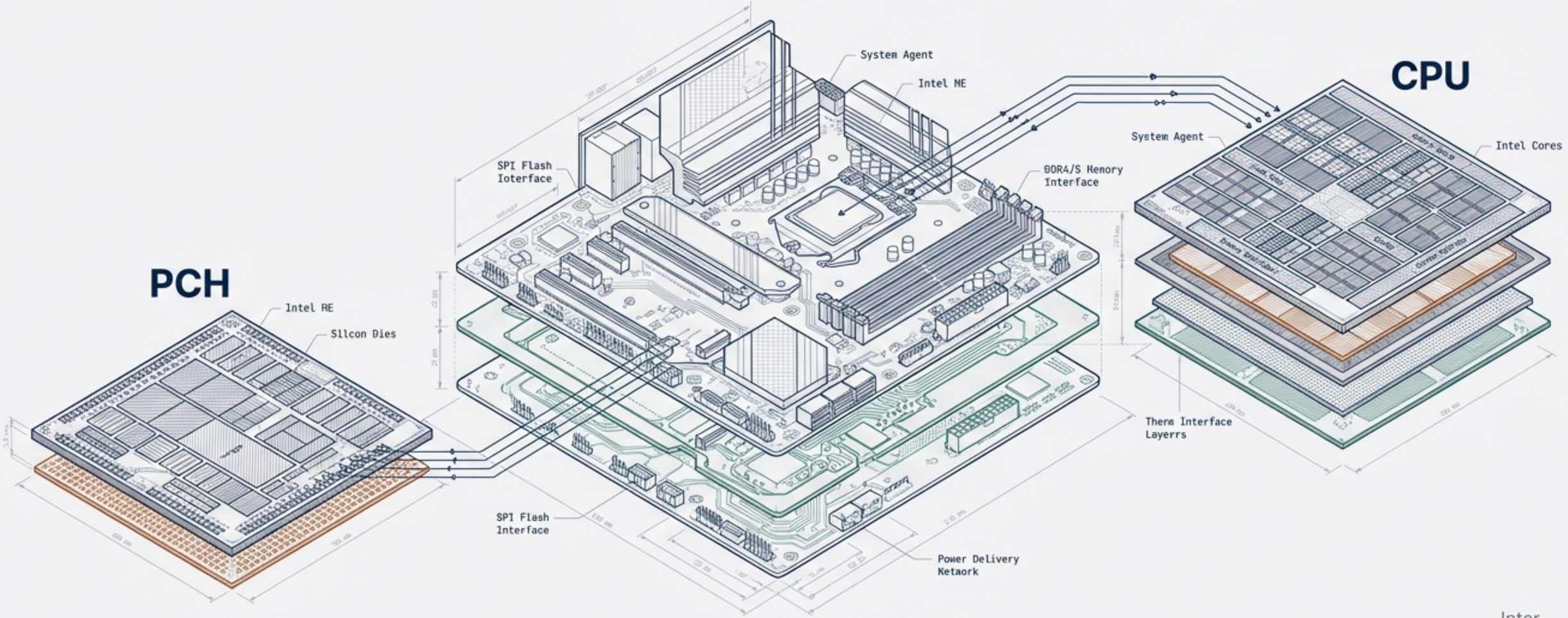
Intel Boot Guard: The Architecture of Trust

A Comparative Analysis of CSME vs. ACM Roles in Firmware Validation



Inter

Architecture Deep Dive & Documentation Correction

THE CORE QUESTION

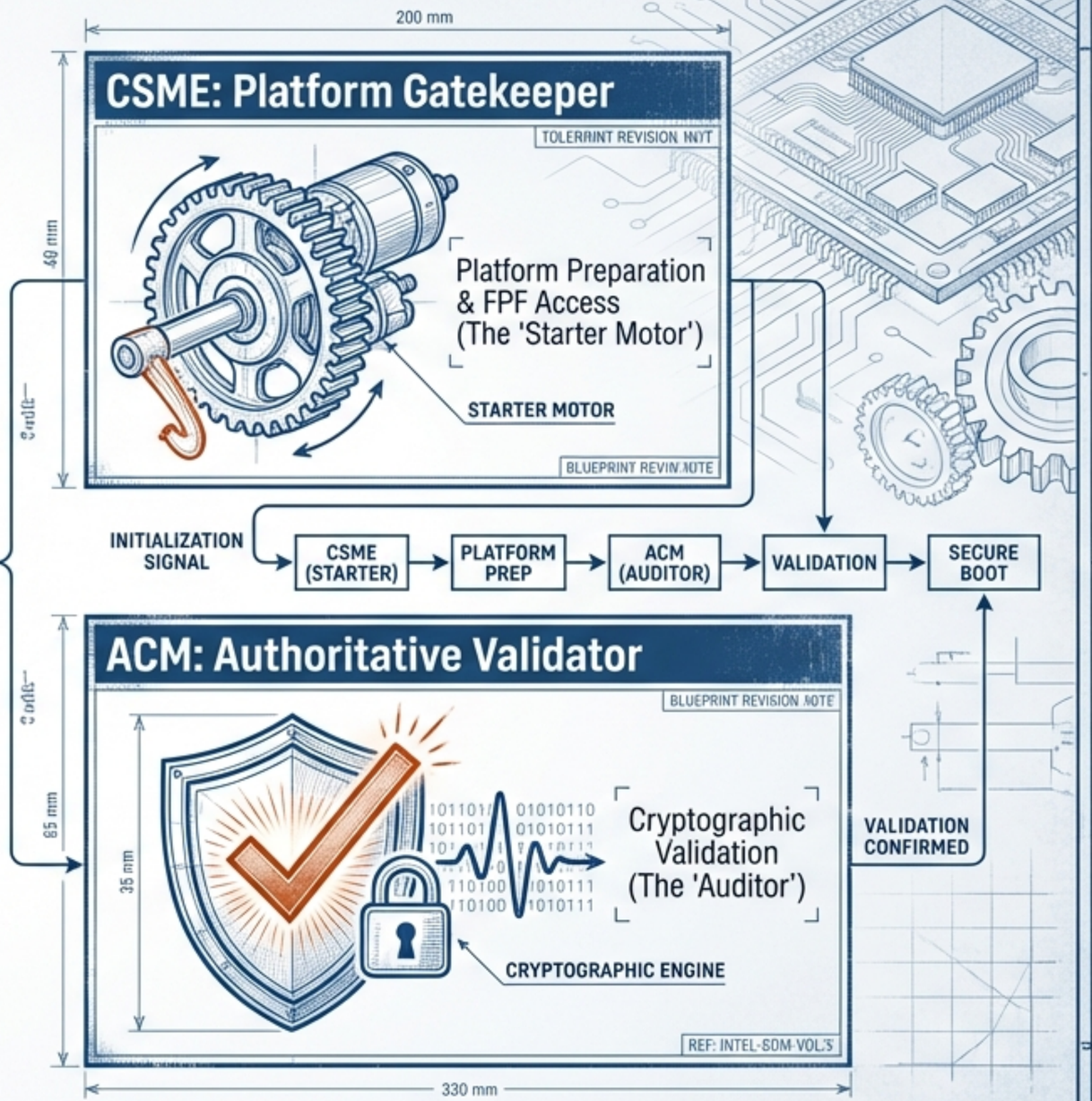
Does the CSME validate the Key and Boot Policy Manifests?

NO

REF: INTEL-SDM-VOL3-CHS

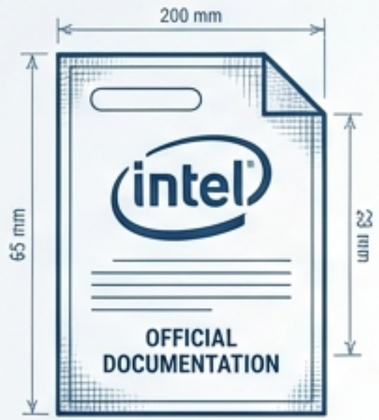
Official Intel documentation, TianoCore specifications, and architecture audits confirm that the ACM (Authenticated Code Module) is the sole authoritative validator of the manifest chain.

BLOCK DIAGRAM - ROLE SEPARATION



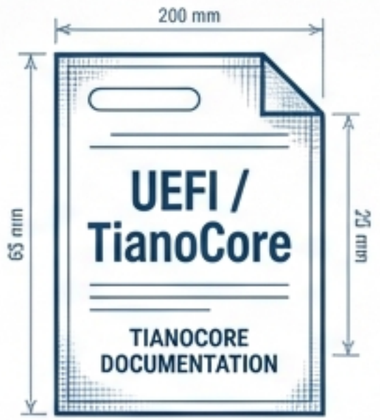
PROJECT:	DWG NO:	DATE:
INTEL ARCHITECTURE AUDIT	01A	2024.10.26

THE EVIDENCE: A THREE-SOURCE ANALYSIS



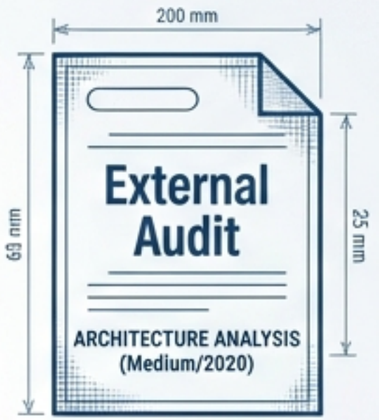
Quote:"The ACM loads and verifies the Boot Policy Manifest (BPM)."

Key Finding: Intel attributes execution/reset to CSME, but explicit validation to ACM.



Quote: "The ACMs modules assume responsibility to verify OEM platform firmware."

Key Finding: Identifies ACM as the "Trust Point" (TP) for the entire chain.



Key Finding: Attributes the 4-step verification process (KM Public Key → KM Signature → BPM → IBB) → IBB) - Signature → ACM entirely to the ACM.

CONSENSUS: VALIDATION IS THE ACM'S RESPONSIBILITY.

N

PROJECT: INTEL ARCHITECTURE AUDIT | DWG NO: 01B | DATE: 2024.10.26

THE SOURCE OF CONFUSION: THE FPF FACTOR

THE MISUNDERSTANDING

BLUEPRINT REVISION NOTE

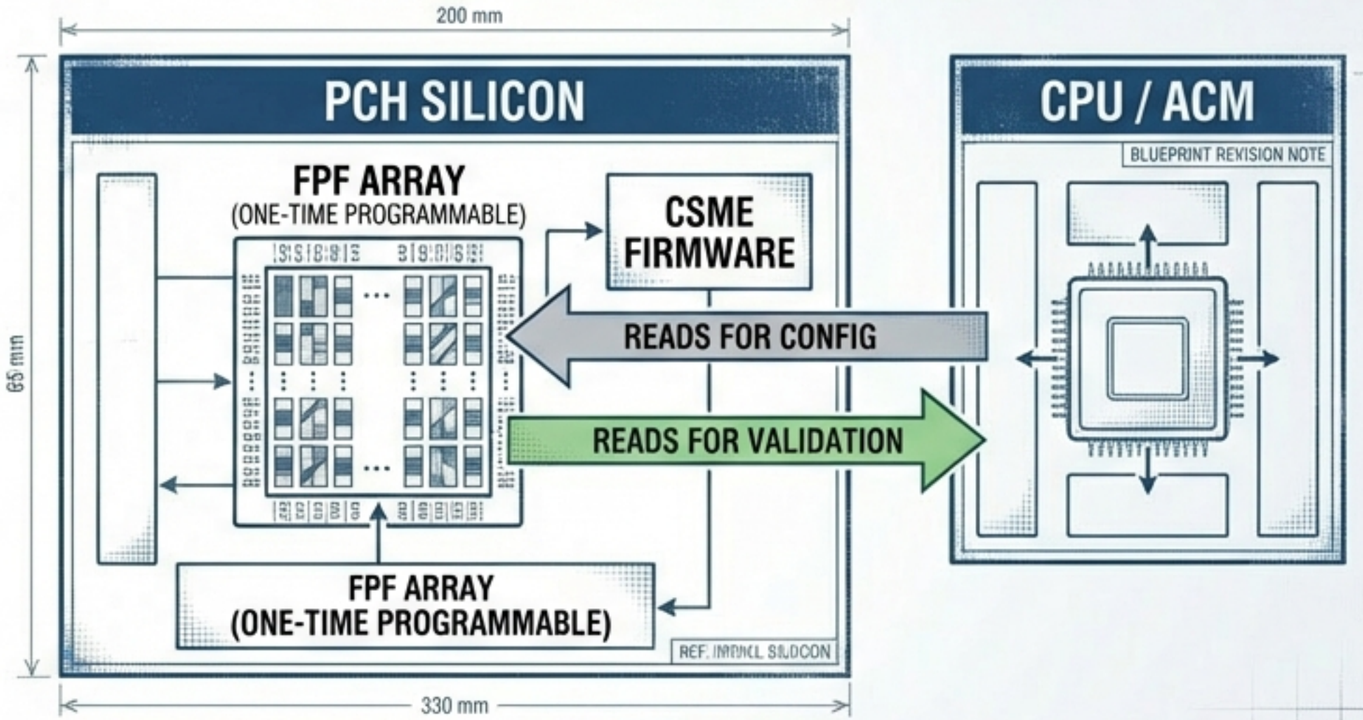
THE COMMON ASSUMPTION:
"FPF Fuses are located in the PCH. The PCH is the CSME's home. Therefore, CSME must own the validation."

THE TWIST: Just because fuses live in the PCH doesn't mean CSME is the one checking the ID.

BLUEPRINT REVIN NOTE

65 mm

TECHNICAL REALITY DIAGRAM

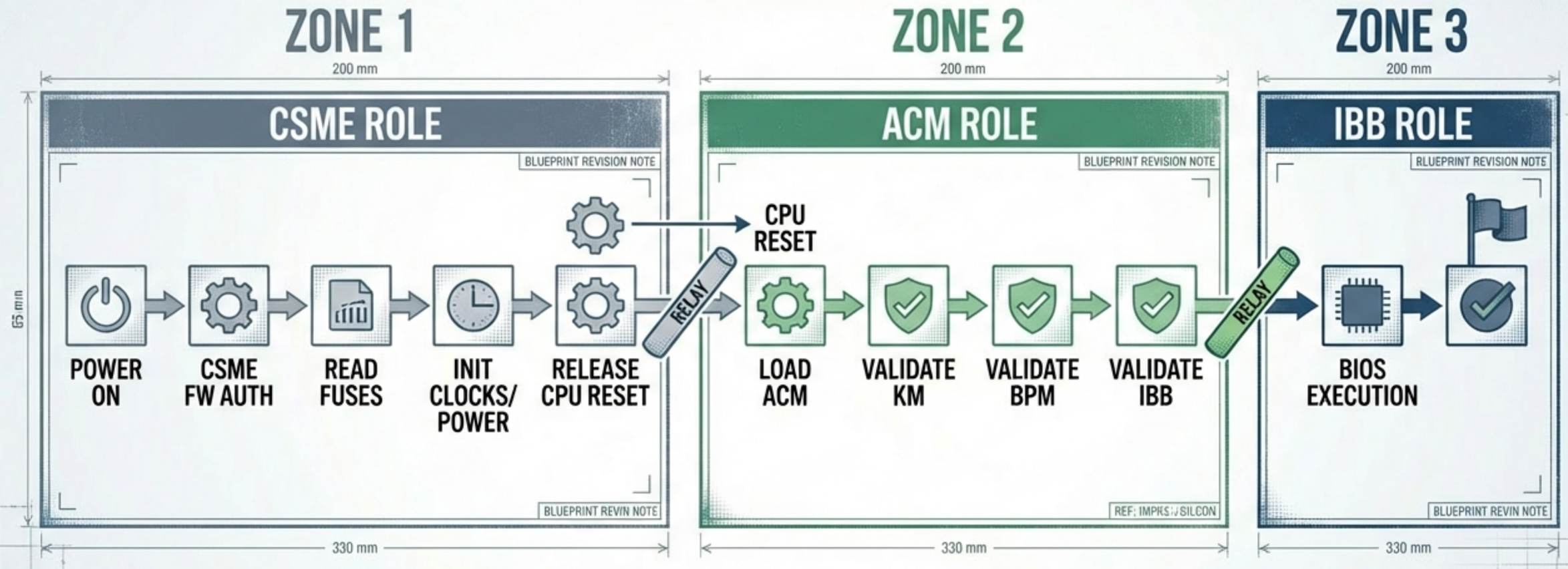


KEY INSIGHT: FPFs are a Shared Trust Anchor. They are hardware storage, not software logic. Both CSME and ACM can read them independently.

N

PROJECT: INTEL ARCHITECTURE AUDIT | DWG NO: 01C | DATE: 2024.10.26

THE TRUE BOOT FLOW: A RELAY RACE



CSME PREPARES THE TRACK. ACM RUNS THE RACE.

N

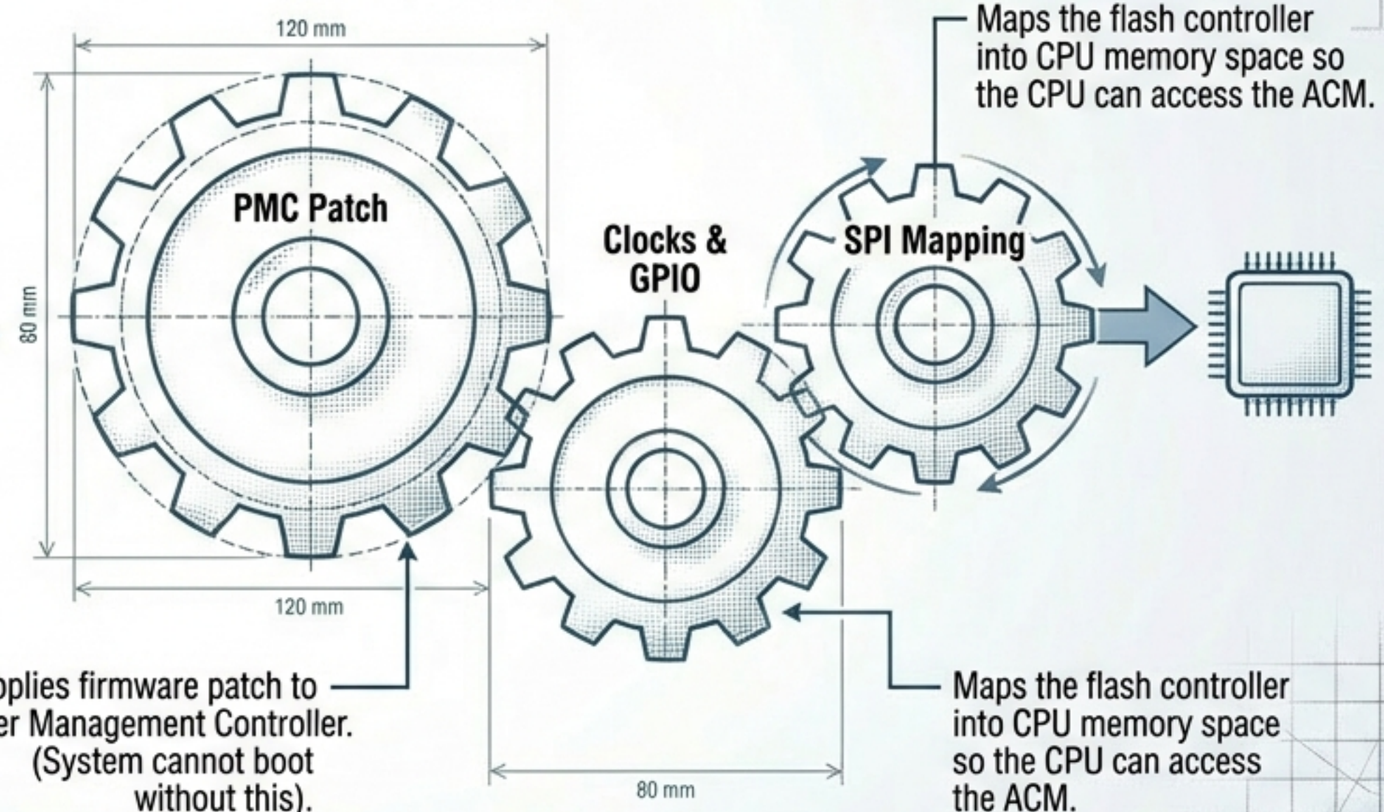
PROJECT: INTEL ARCHITECTURE AUDIT | DWG NO: 010 | DATE: 2024.10.26

CSME ROLE: THE 'STARTER MOTOR'

CONTEXT

The CPU is physically incapable of executing instructions until CSME prepares the ground.

THE MECHANISM



N

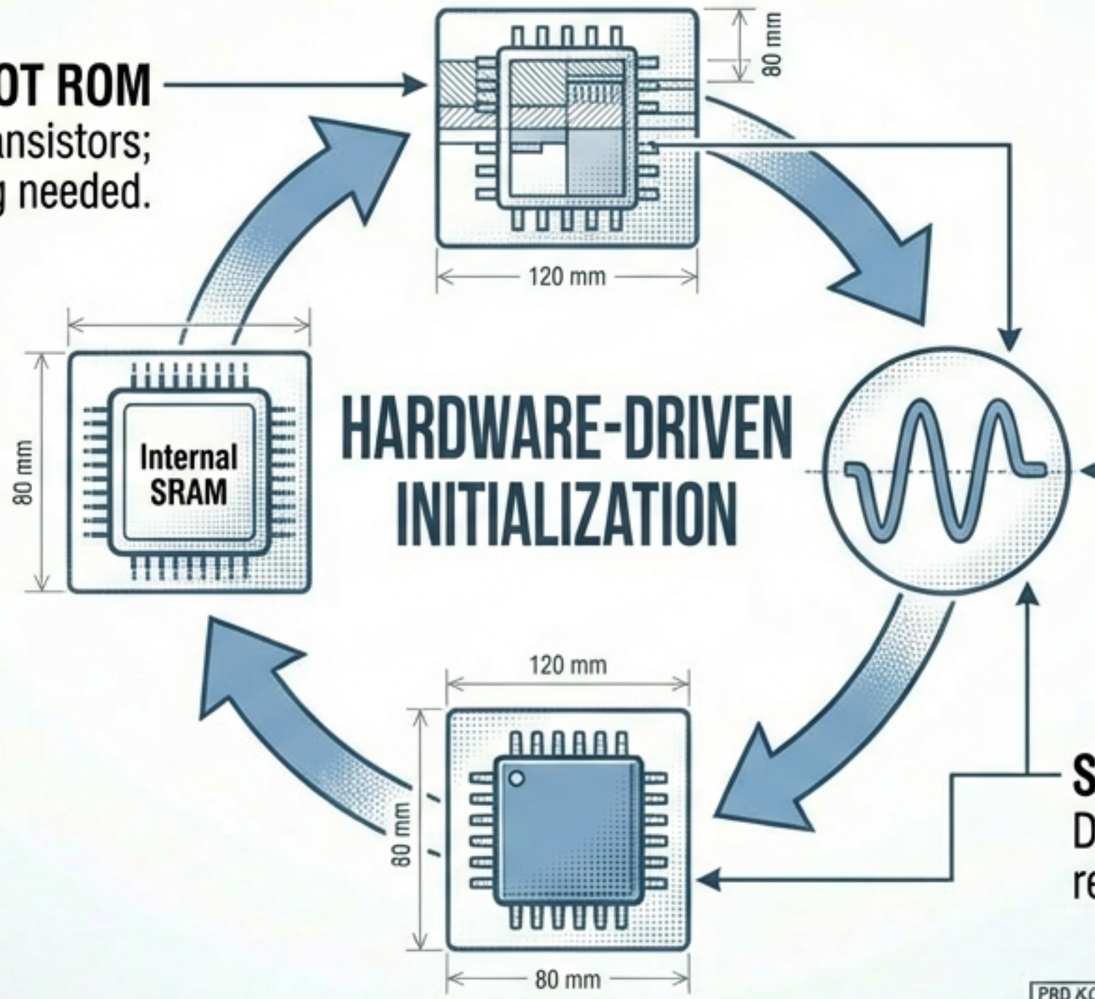
PROJECT:	DWG NO:	DATE:
INTEL ARCHITECTURE AUDIT	010	2024.10.26

SOLVING THE ‘CHICKEN AND EGG’ PROBLEM

How does CSME start if the Flash Controller isn’t initialized?

HARDWIRED BOOT ROM
Built into silicon transistors; no loading needed.

SRAM LOAD
Firmware loaded for execution.



HARDWARE DMA REQUEST
ROM invokes Direct Memory Access without software drivers.

SPI FLASH READ
Default hardware state reads firmware.

N

PROJECT	DWG NO.	DATE
INTEL ARCHITECTURE AUDIT	010	2024.10.26

ACM ROLE: THE AUTHORITATIVE AUDITOR

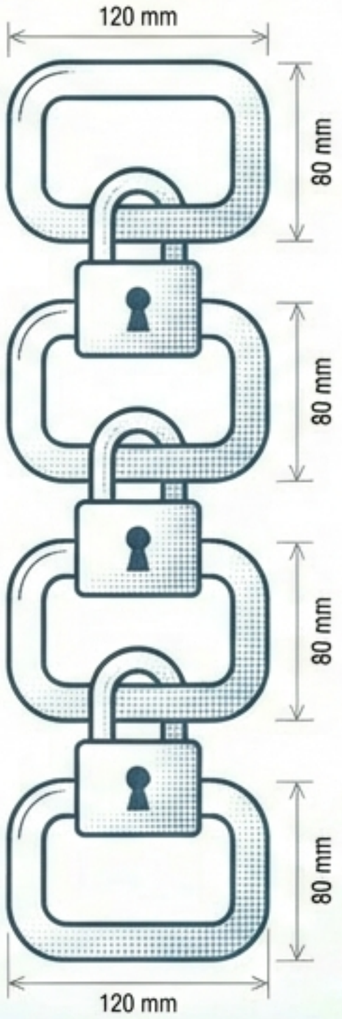
The Hardware-Enforced Verification Chain

1. KM Public Key
Verified against BP.KEY hash in FPF fuses.

2. KM Signature
Establishes trust in OEM root.

3. Boot Policy Manifest (BPM)
Verified using the now-trusted public key from KM.

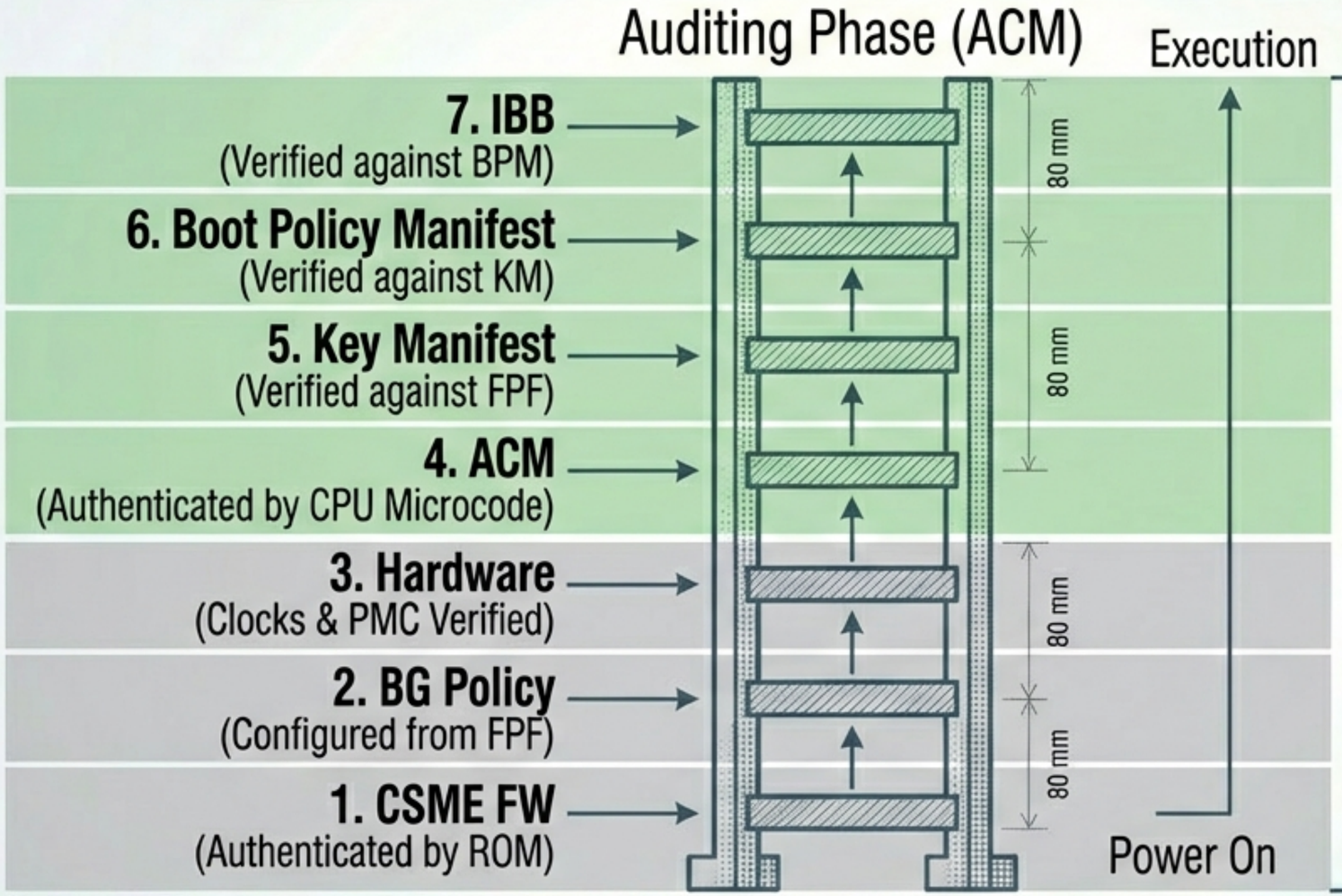
4. Initial Boot Block (IBB)
Hashes verified against the trusted BPM.



Isolated, Hardware-Enforced Checkpoint in AC RAM.

PRODUCT: INTEL ARCHITECTURE AUDIT | DWG NO. 010 | DATE: 2024.10.26

The Seven Checkpoints of Trust

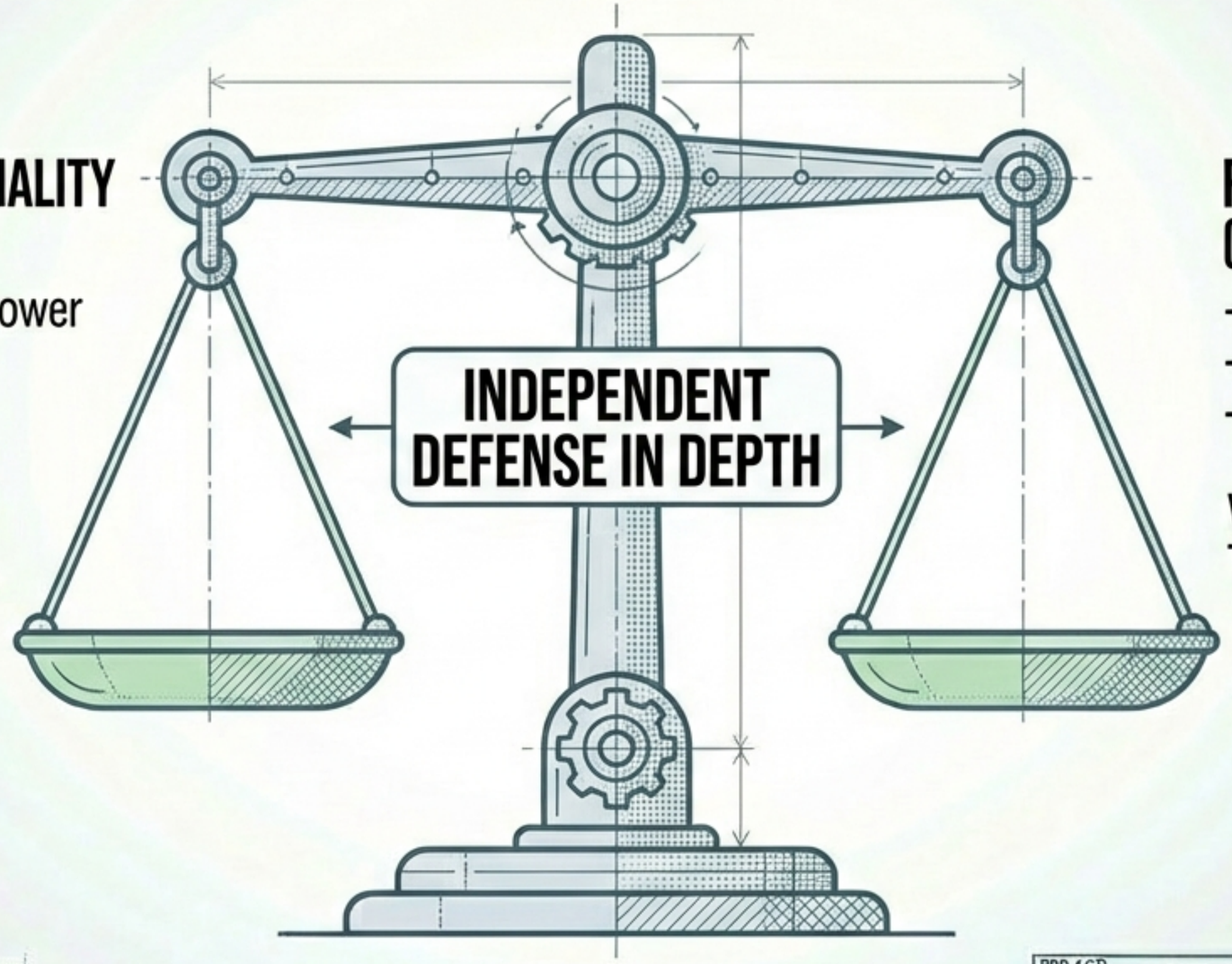


COMPLEMENTARY ROLES, NOT REDUNDANT

PLATFORM FUNCTIONALITY (CSME)

- Initializes Clocks & Power
- Releases CPU Reset
- Enforces Policy

Without CSME:
The Platform is Dead.



FIRMWARE TRUST (ACM)

- Validates Cryptography
- Root of Trust Anchor
- Checks Bios Integrity

Without ACM:
The Platform is Untrusted.

PRD ACT	DWG NO.	DATE
INTEL ARCHITECTURE AUDIT	010	2024.10.26

Analogy: The Secure Building

The Facility Manager (CSME)

Unlocks main doors.
Turns on lights and HVAC.
Checks safety systems.
Result: The building is functional.

The Security Guard (ACM)

Stands at High-Security Zone entrance.
Independently checks ID badges.
Verifies against trusted list.
Result: Only authorized code enters.

SUMMARY OF RESPONSIBILITIES

FEATURE	CSME (CONVERGED SECURITY)	ACM (AUTHENTICATED CODE MODULE)
Initialization	Active / Primary (Clocks, Power)	None
FPF Fuses	Programs & Reads (Shared)	Reads Independently (Shared)
KM / BPM Validation	None	Authoritative Validator
Execution Environment	PCH Processor	Isolated AC RAM
Security Model	Platform Gatekeeper	Chain of Trust Root

PRD ACT: INTEL ARCHITECTURE AUDIT | DWG NO: 016 | DATE: 2024.10.26

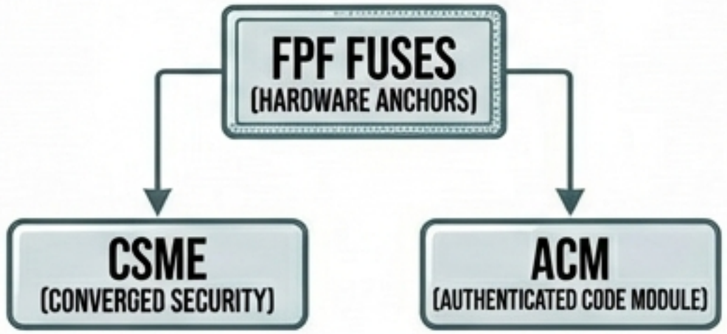
FINAL TAKEAWAYS

1. CORRECTED FLOW

CSME prepares the platform; **ACM** validates the manifests.

2. SHARED ANCHOR

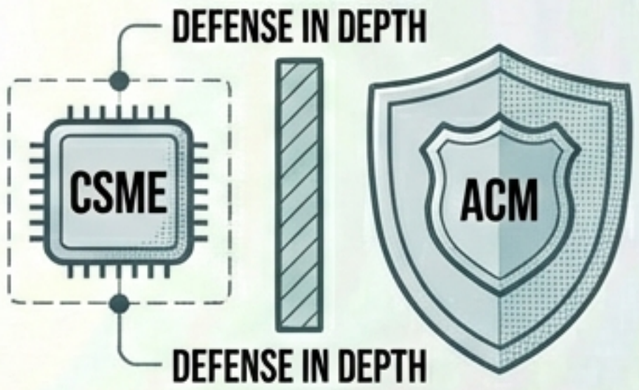
FPF Fuses are hardware anchors shared by both. They are not “owned” by CSME software.



FPF Fuses are hardware anchors shared by both. They are not “owned” by CSME software.

3. DEFENSE IN DEPTH

The architecture relies on the independence of these two components.



The architecture relies on the independence of these two components.

“Precision in documentation defines the security architecture. The ACM is the authoritative validator.”

PROJECT INTEL ARCHITECTURE AUDIT | ORIGINATOR 003 | DATE 2024.10.26