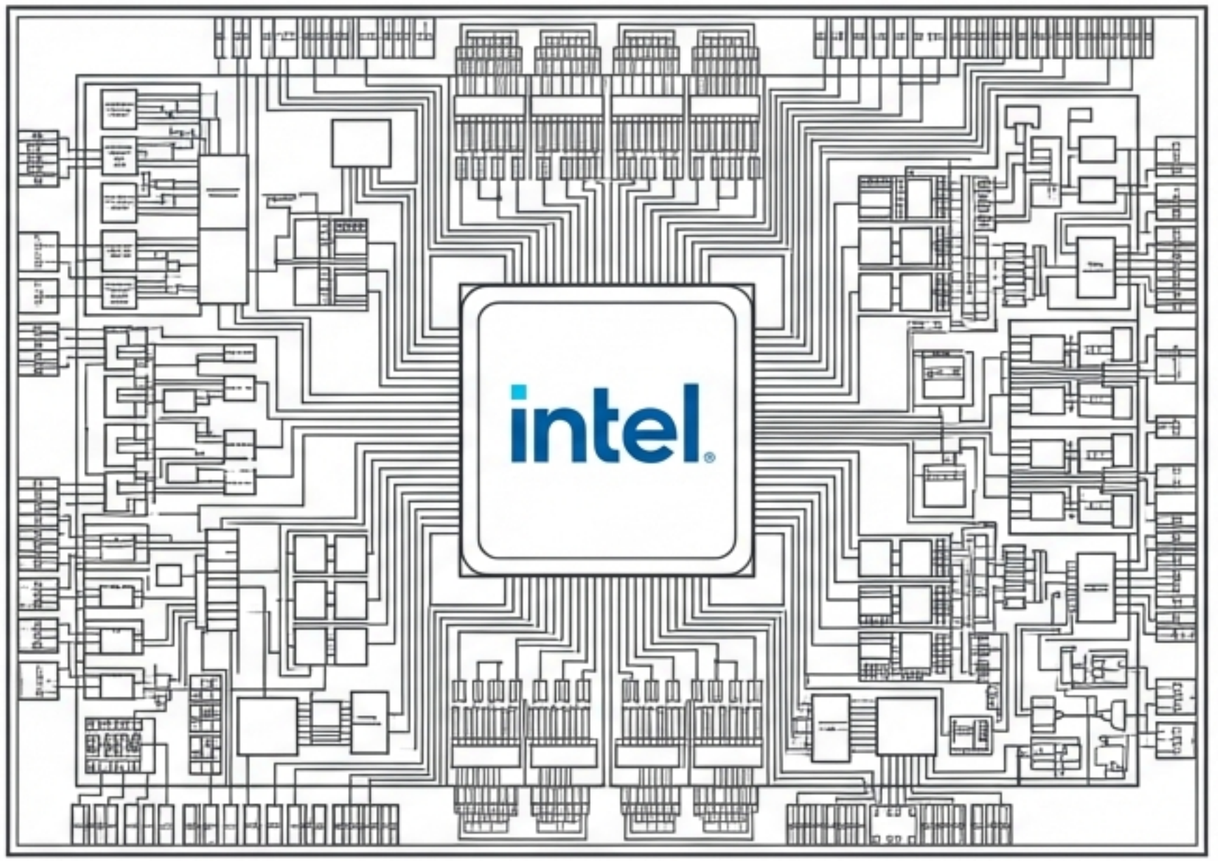


Intel® Converged Security and Management Engine (Intel® CSME)

Architecture, Security Design, and Defense-in-Depth

TECHNICAL WHITE PAPER OVERVIEW | COVERS CSME 14.0 (COMET LAKE) THROUGH 16.0 (ALDER LAKE)

The Silicon Fortress: An Isolated Subsystem

Definition

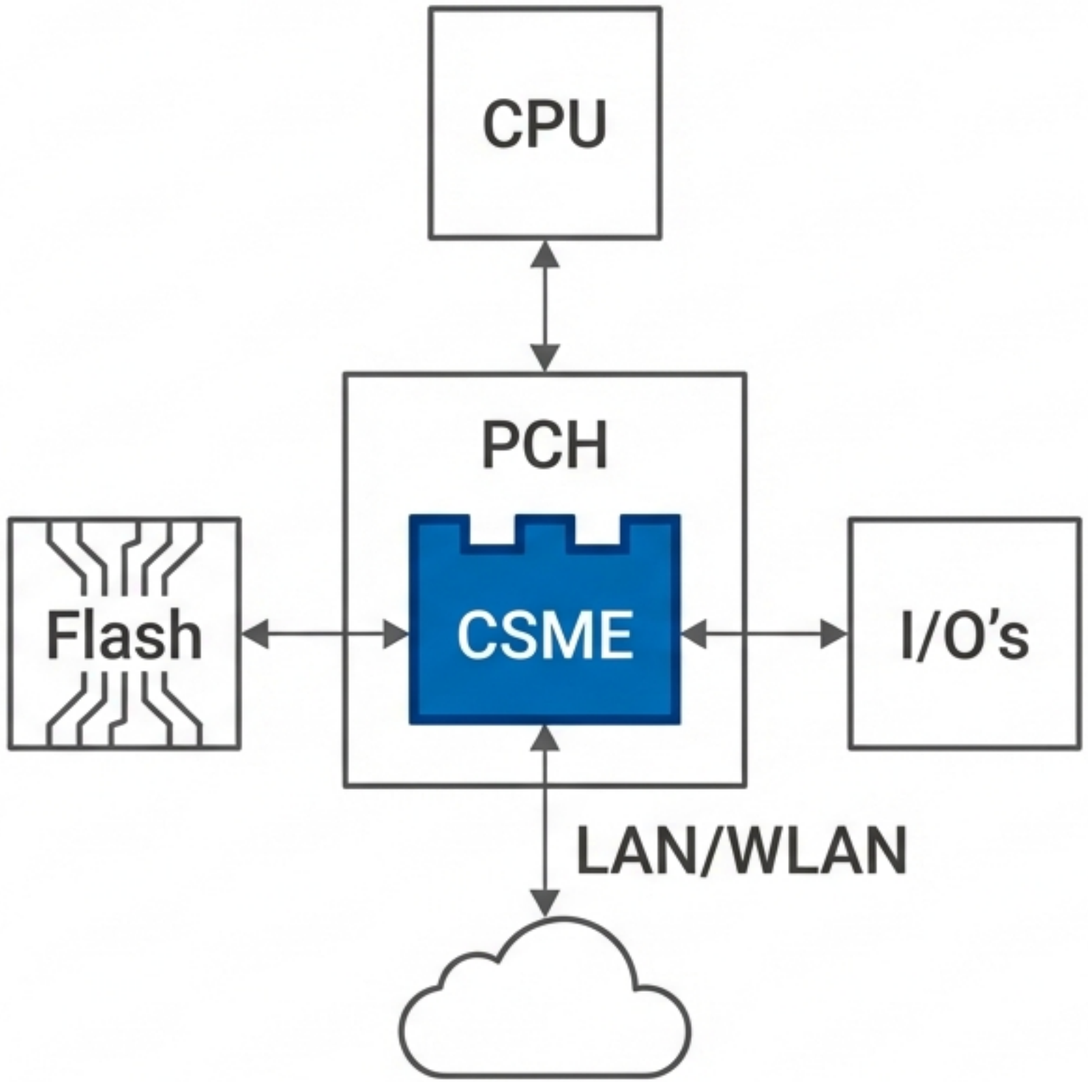
An embedded subsystem and PCIe device resident within the PCH.

Isolation

Operates independently from the Host CPU, BIOS, and OS. Maintains its own power states—alert even when the host sleeps.

Core Functions

1. **Silicon Initialization:** Clocks, GPIO, IP FW Authentication (PMC, Camera, Type C).
2. **Manageability**: Intel® Active Management Technology (AMT) for Out-of-Band access.
3. **Security**: Platform Root of Trust, Intel® PTT (TPM 2.0), Intel® Boot Guard.



Precision Engineering White Paper

Hardware Architecture & Isolation

SRAM / ROM (The Vault)

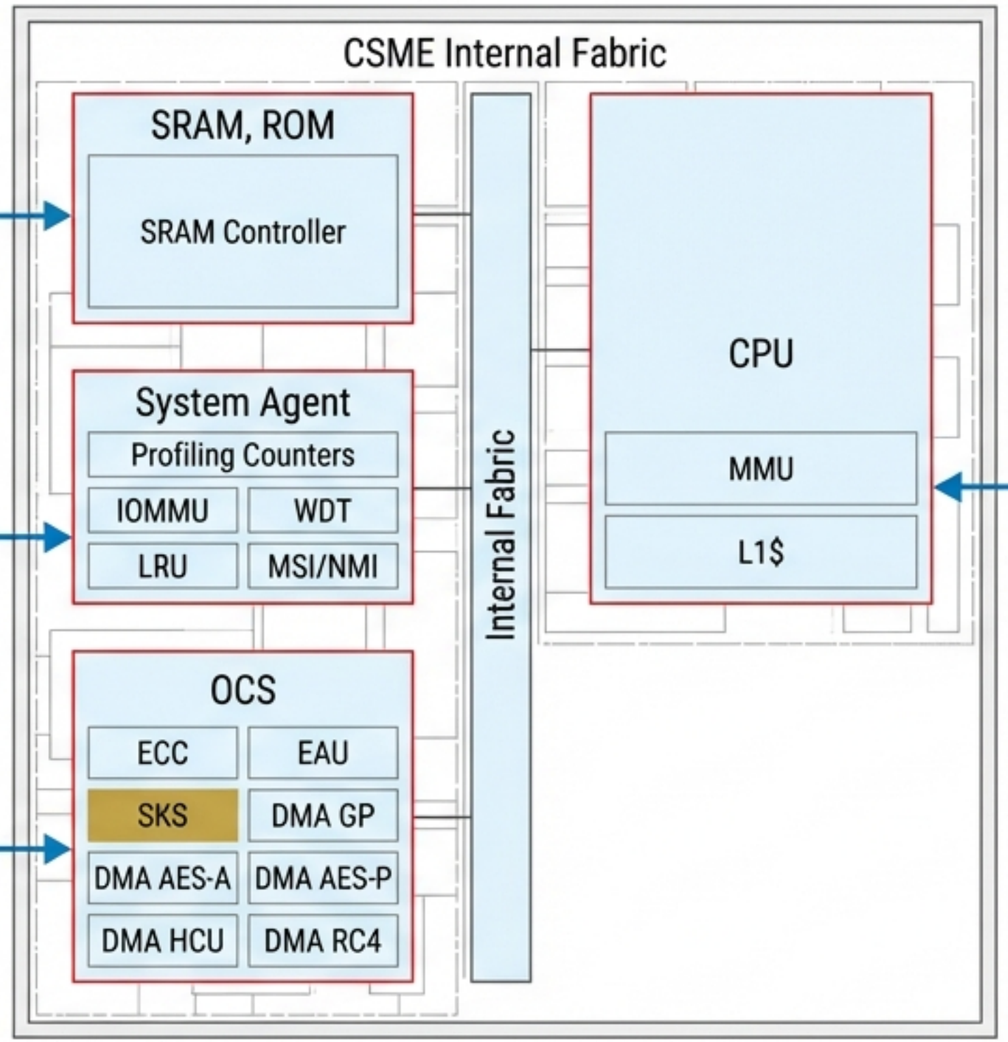
Internal SRAM (512KB – 1.9MB).
Physically isolated from host.
Cannot be probed via external interfaces.

System Agent (The Gatekeeper)

Enforces access control.
Dedicated IOMMU polices DMA access to SRAM.

OCS (The Engine)

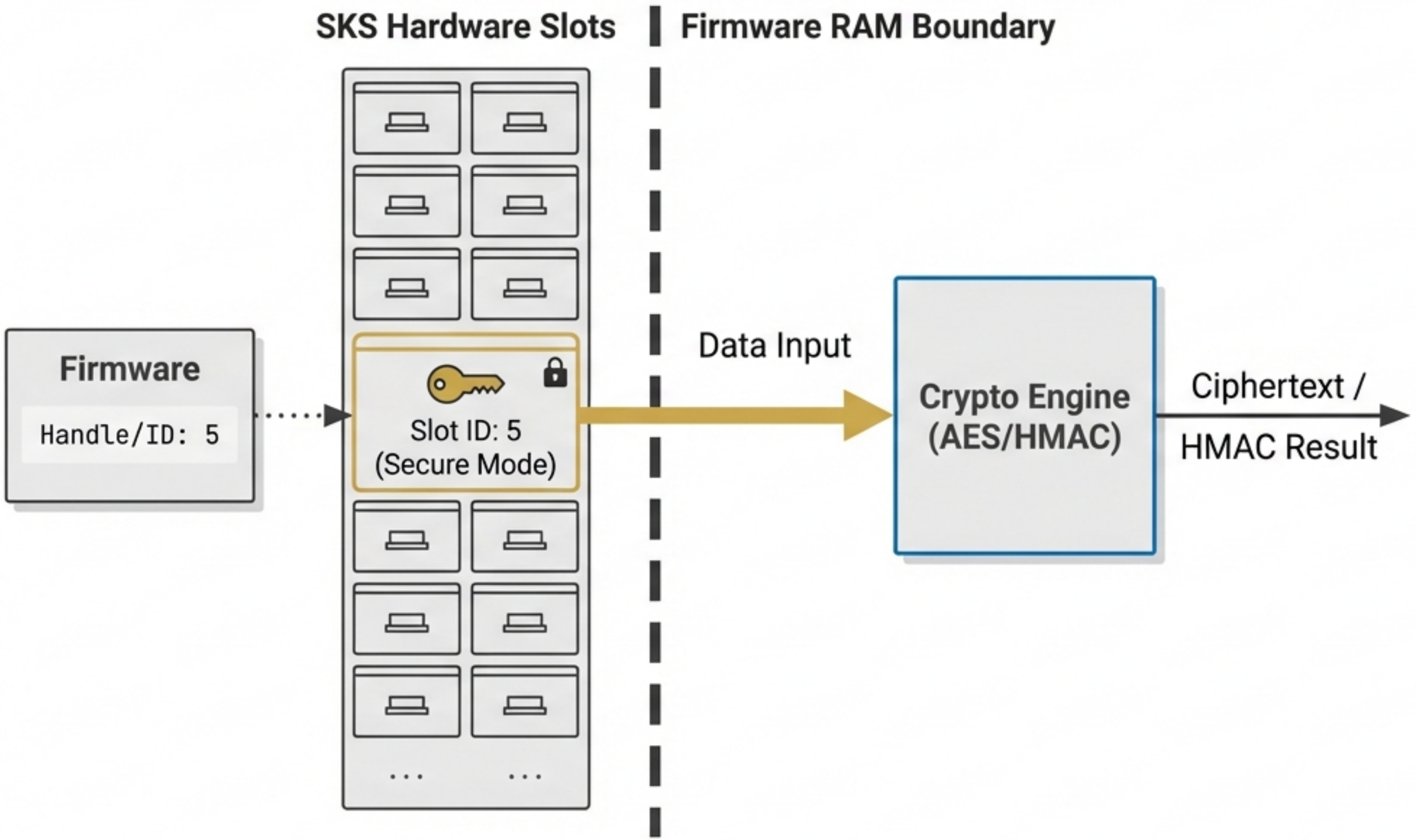
Offload & Cryptography Subsystem.
FIPS 140-2 Level 1 Certified.
Contains Secure Key Storage (SKS).



CPU (The Brain)

Dedicated 32-bit x86 processor (Intel 486 arch).
Ring 0/3 isolation.
CET support (Tiger Lake+).

The Vault Mechanics: Secure Key Storage (SKS)

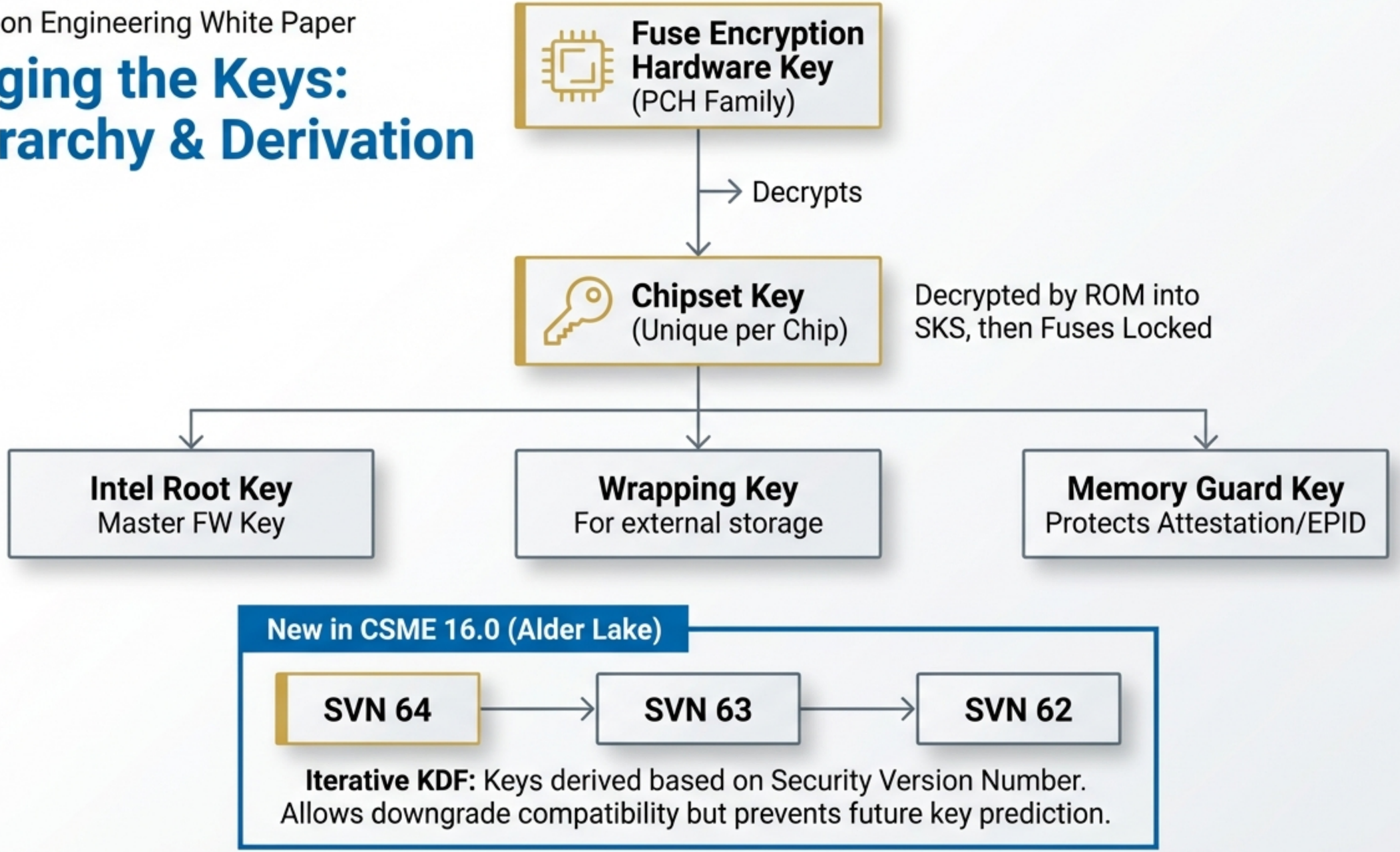


Slot Attributes

- **Secure Mode:** Result of crypto operations stays in hardware slots.
- **Privilege Level:** Hardware-enforced access control (Must meet OCS privilege).
- **Locked:** Cannot be overwritten until hardware reset.
- **Key Sizes:** Supports 128, 256, and 384 bits.

Precision Engineering White Paper

Forging the Keys: Hierarchy & Derivation



Awakening: The Boot Chain of Trust (Part I)

CSME ROM

Immutable Hardware Root of Trust

- Permanent, unpatchable silicon.
- **Initializes** CSME CPU (Protected Mode).
- Contains Hash of the Public Key.
- **ACTION:** Verifies & Loads RBE.

Hash Verification

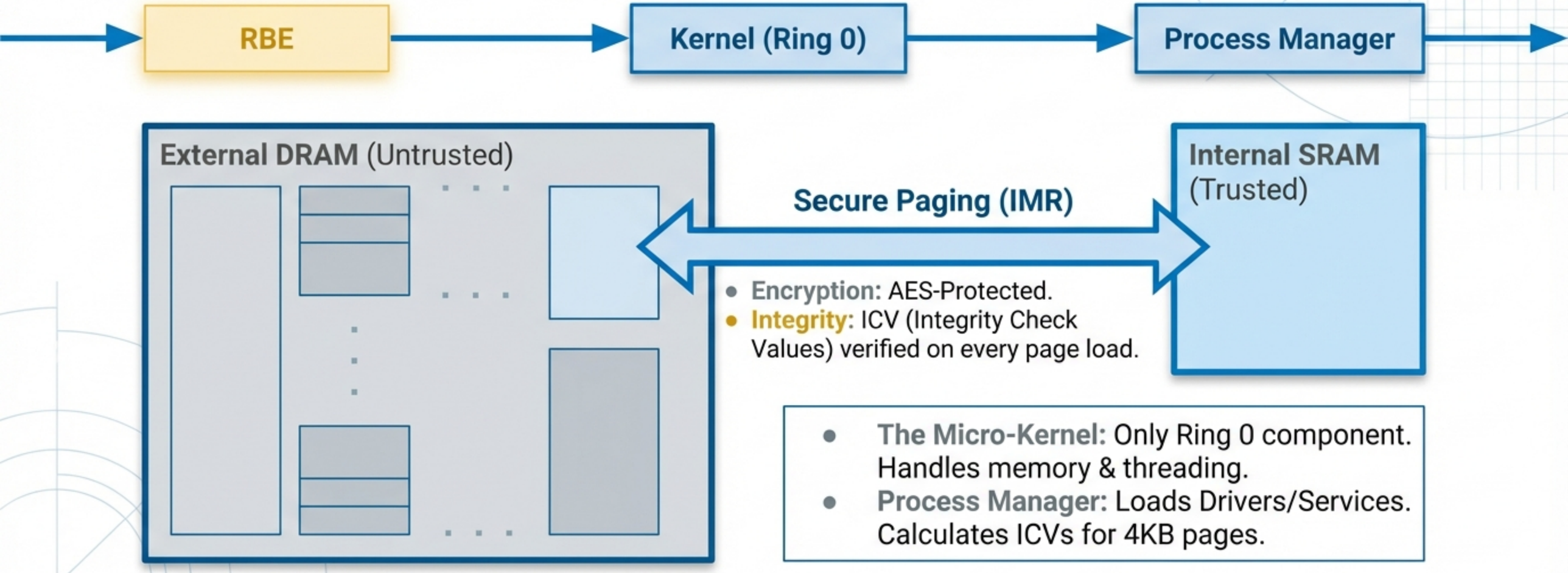
ROM Boot Extension (RBE)

The Bootloader

- **Integrity:** RSASSA-PSS 3072-bit Signature Check.
- **Version Control:** Anti-Rollback check against Fuses (FPF).
- **Silicon Enabling:** Authenticates Debug Tokens & Loads PMC Patch.

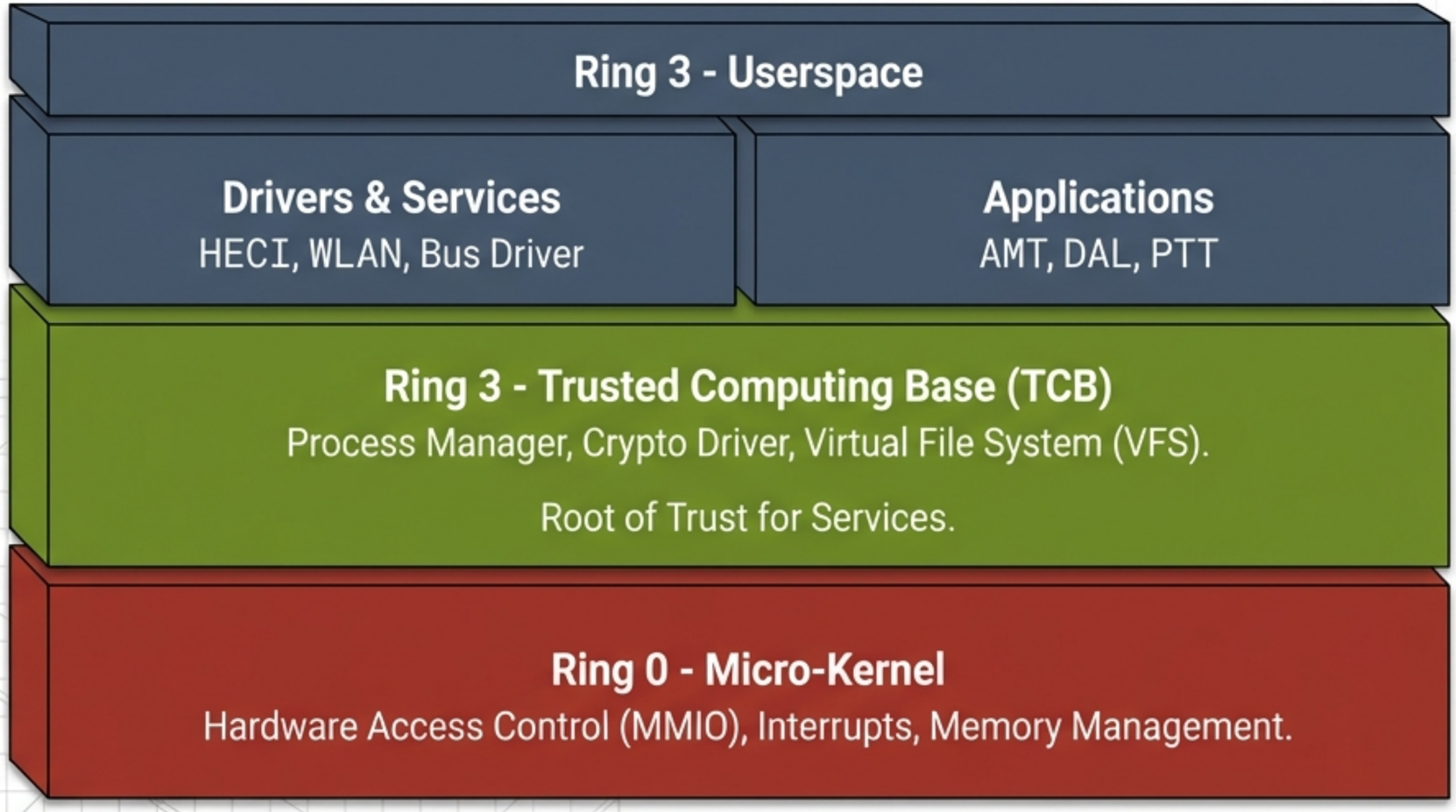
Precision Engineering White Paper

Establishing Consciousness: The Boot Chain (Part II)



Precision Engineering White Paper

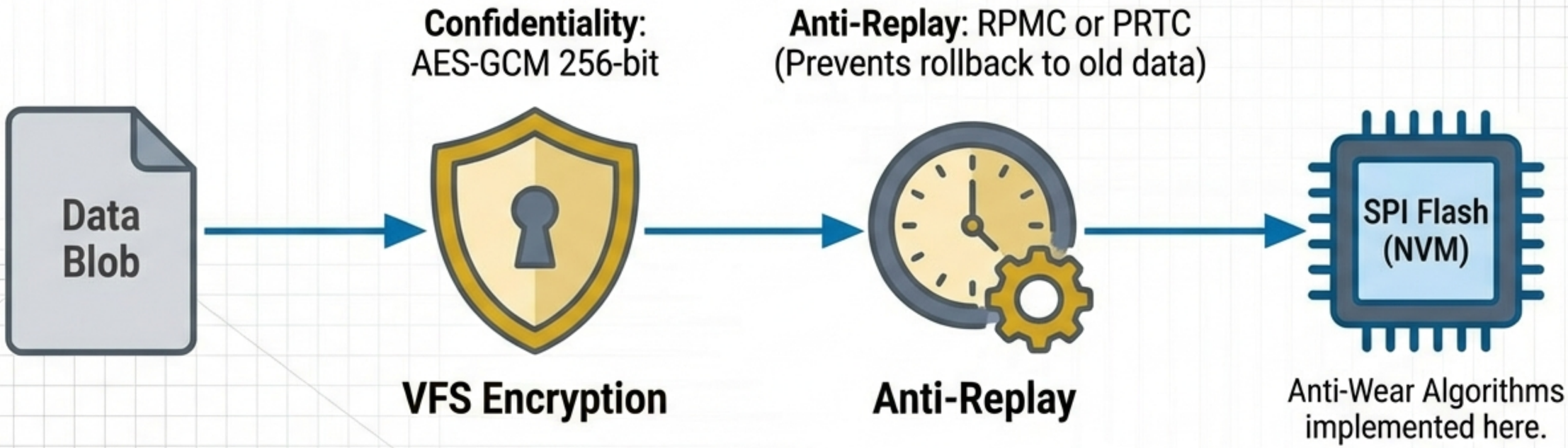
The Operating System Architecture



Least Privilege Design

Minix-based micro-kernel. Static permission tables define exactly which driver can access which hardware.

Managing Assets: The Virtual File System (VFS)



The Challenge: External Flash storage is accessible and untrusted.

The Solution: VFS ensures CSME applications never write directly to flash. All data is wrapped in confidentiality and integrity protections before leaving the enclave.

Applications & Capabilities

Intel® AMT

Active Management Technology. Out-of-band management (KVM, Remote Power) independent of OS state.

Intel® PTT

Platform Trust Technology. Firmware-based TPM 2.0 implementation. Supports BitLocker & Secure Boot.

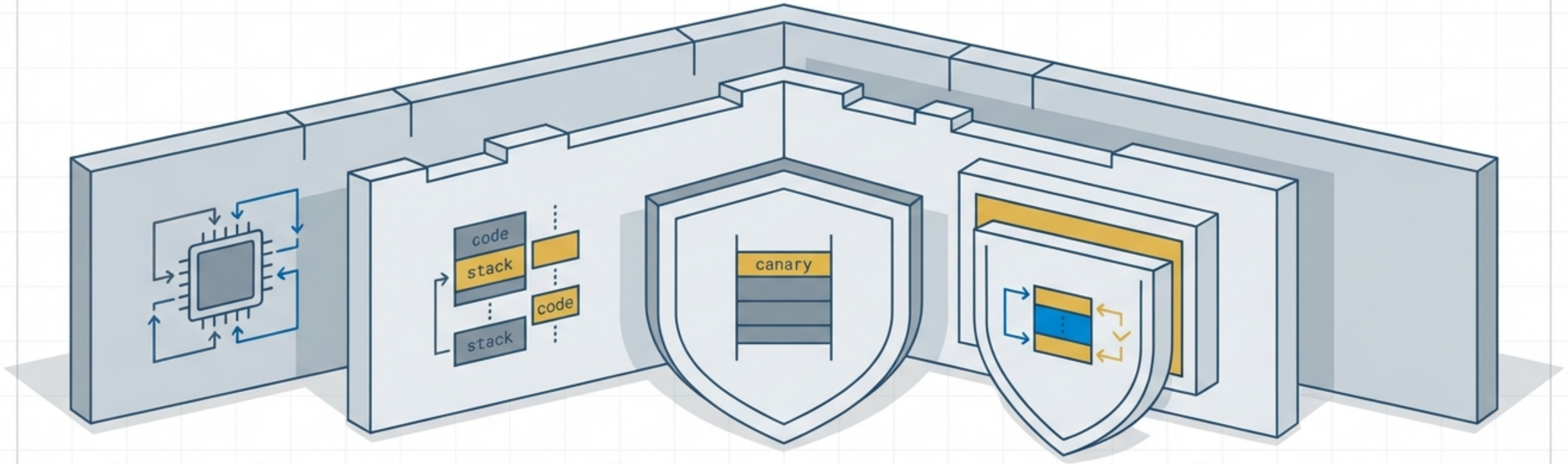
Intel® Boot Guard

Hardware-based Boot Integrity. Authenticates System BIOS using policies burned into PCH Fuses.

Intel® DAL

Dynamic Application Loader. A secure, sandboxed execution environment for trusted applets.

Active Defense: Anti-Exploitation Techniques



1. CET (Control-Flow Enforcement)

Hardware-assisted protection (Tiger Lake+). **Shadow Stacks** & **Indirect-Branch Tracking** prevent ROP/JOP attacks.

2. ASLR / DASLR

Address Space Layout Randomization.
Randomizes Code, Stack, and Heap layout per boot. Makes target addresses unpredictable.

3. Canaries

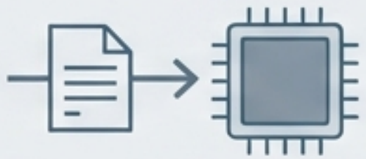
Stack Protectors.
Random values placed on stack. **XORed** with return addresses to detect overflows.

4. Data Fortify

(CSME 16.0+)
Runtime boundary checks for linear copy operations (memcpy/strcpy).

Resilience: Updates & Anti-Rollback (ARB)

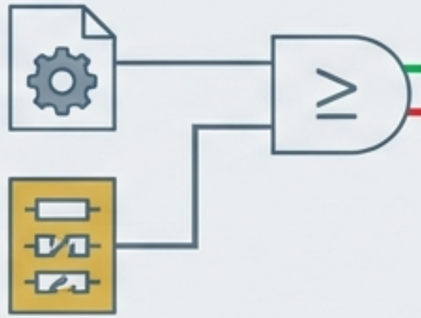
STEP 1: THE UPDATE



Firmware Update delivered via HECI. Fault-tolerant process.

STEP 2: THE CHECK (THE RATCHET)

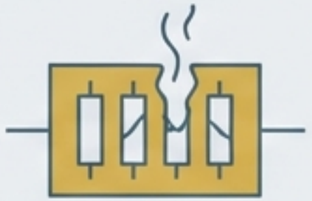
Compare FW SVN (Security Version Number) vs. FPF (Fuse) SVN.



FW SVN ≥ Fuse SVN -> **BOOT ALLOWED**

FW SVN < Fuse SVN -> **BOOT DENIED (Rollback Attempt)**

STEP 3: THE LOCK



On successful boot of new SVN:

Burn Fuses to match new SVN.

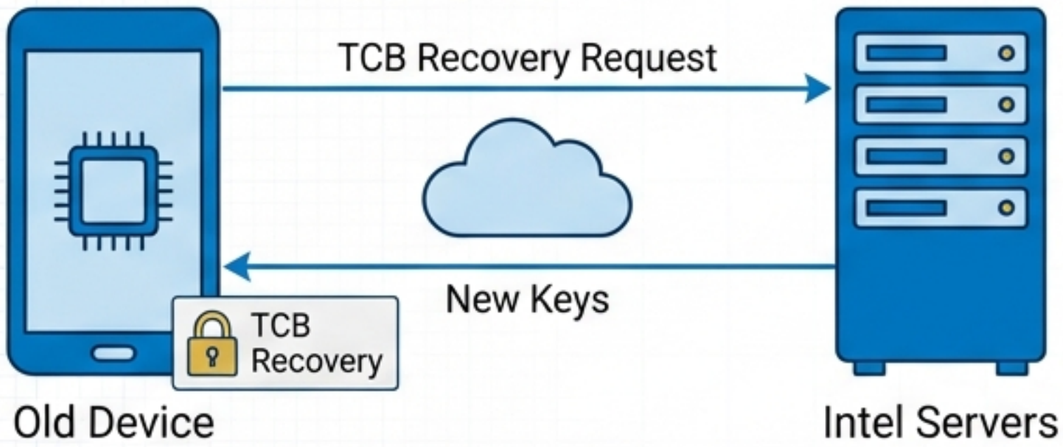
Downgrade is now physically impossible.

Intel® FVC:

Hardware-enforced version control prevents attackers from downgrading the system to exploit vulnerability patches.

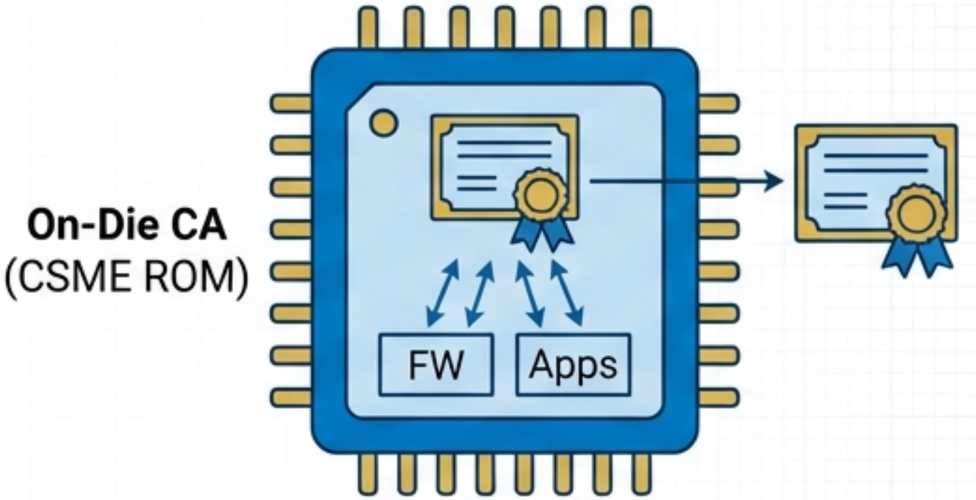
Identity & Attestation: Evolution of Trust

Legacy: Intel® EPID



- Anonymous Group Signatures.
- Privacy-focused.
- **Dependency**: Requires connection to Intel Servers for Re-Keying.

Modern: On-Die CA (CSME 15.0+)



- **On-Die Certificate Authority**.
- CSME ROM acts as the CA.
- Issues x509v3 certificates to FW & Apps internally.
- **Benefit:** TCB Recovery is local. No external server dependency for key generation.

The Human Element: Manufacturing & Validation

End-of-Manufacturing (EoM)

Mandatory Locking:

- Burn FPFs (OEM Key Hash).
- Lock Debug Ports.
- Lock SPI Flash Descriptor.

Flexible EoM (CSME 16.0) allows split-stage locking.

Validation Technologies

Process & Hardening:

- **Fuzzing:** AFL Coverage-guided fuzzing on real silicon.
- **ASAN:** Address Sanitization for memory error detection.
- **Red Teaming:** Offensive security research and manual penetration testing.

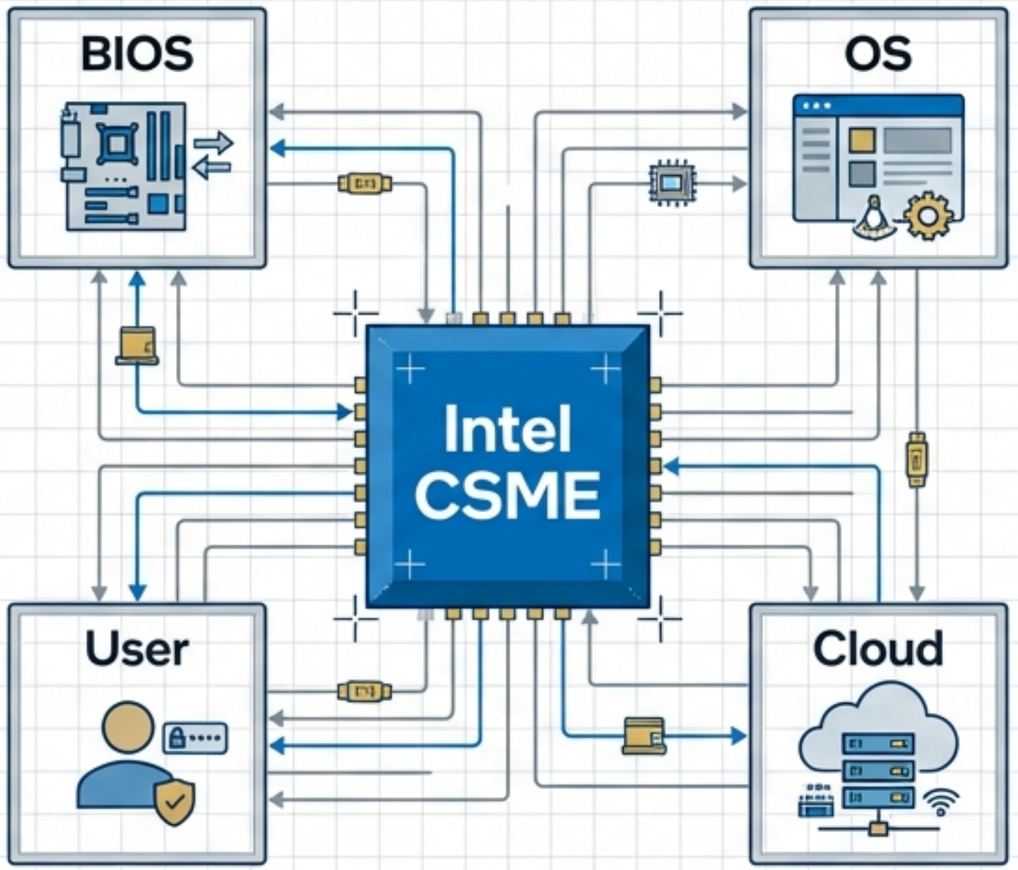
The Converged Advantage

Foundation:

- Hardware Root of Trust for the modern platform.

Convergence:

- Unifies Manageability (AMT) and Security (PTT) in one isolated subsystem.



Resilience:

- Self-healing capabilities with Anti-Rollback and TCB Recovery.

Defense-in-Depth:

- Layered protection from Fuses to Runtime Memory Defense.

> **“Trusted execution begins before the OS loads.”**