Google's Leadership in Open Source Secure Silicon

Pioneering transparent, auditable, and collaborative hardware security implementations.

Caliptra

Caliptra: Root of Trust

openTitan

OpenTitan: Secure Element

RISC-V 協会 ALLIANCE JAPAN

Andrés Lagar-Cavillla, Distinguished Engineer, AI & Infrastructure Security, Google

RISC-V Day Tokyo 2025 Autumn, Dec 4th 2025

What We Will Discuss Today

- Introduction to Open Source Secure Silicon
- Caliptra: Root of Trust Caliptra
- OpenTitan: Secure Element opentitan
- The Role of RISC-V in Secure Silicon RISC-V 協会
- Collaborative Hardware Security
- Q&A

Why Open Source

- High quality peer reviewed implementations
- Ability to contribute by anybody
- Creates baseline implementations any company can use to deliver a product

Security Through Obscurity is not a good strategy.

Open Source in Software

- A proven method of delivery
- Entire software modules can be constructed in open source, with no hidden parts
- The success of Linux is a testament to the philosophy
- The success of OpenSSL is an example of high quality security modules through open source

OpenSSL

Google’s goals with open source

- High quality implementations
- A rising tide lifts all boats
- Security through transparency

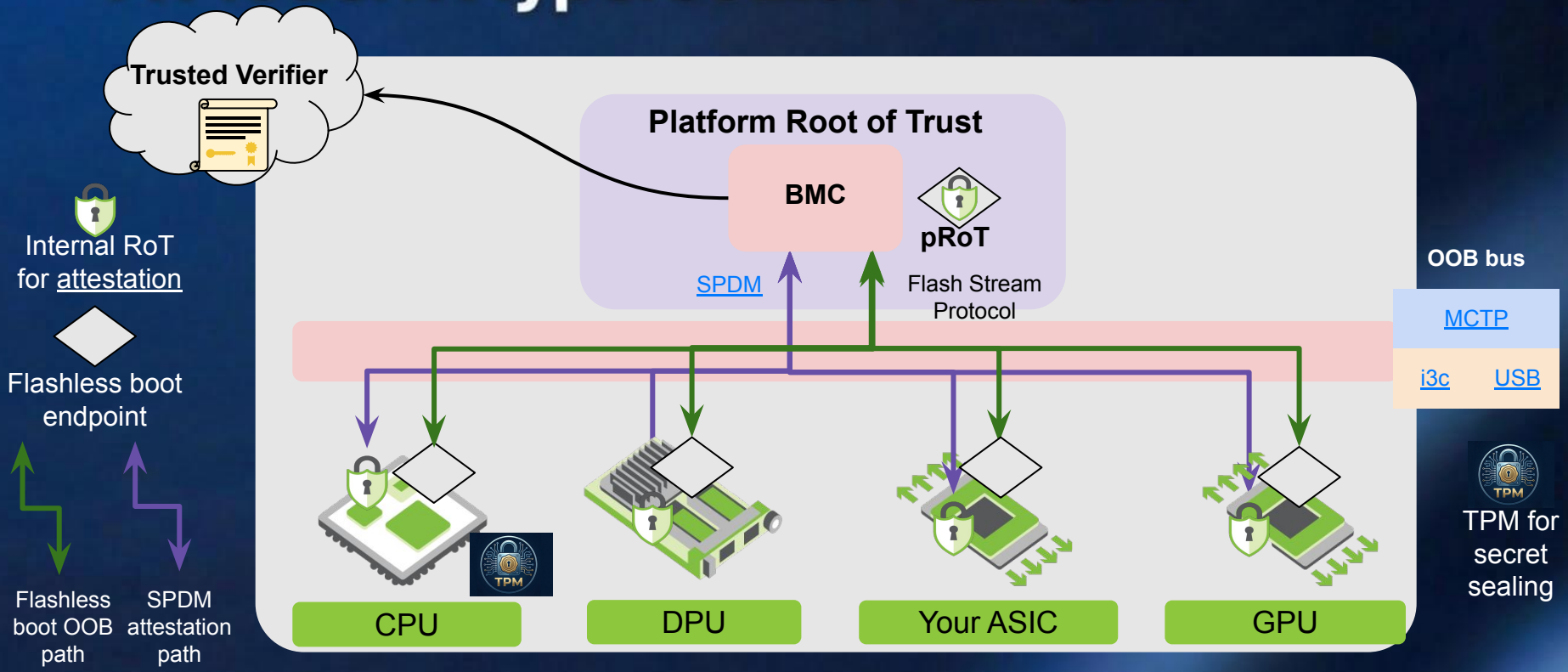
Why Silicon Security Matters

- Software is loaded by more software, until it's loaded by ROM
- It's turtles all the way down, to silicon
- Trust is anchored on the lowest layers and flows up the stack

Silicon is Not Software –

there are limits to this journey and we need to keep pushing boundaries

A Modern Hyperscaler Platform



Google Platform using OpenTitan and Caliptra

Two Roots of Trust

Caliptra

Internal Root of Trust

- Used by SoCs to secure boot and cryptographically measure all firmware
- Gives SoCs a unique cryptographic identity
- Evolving to empower SoCs with key management for internal cryptography (such as in an SSD controller)

opentitan

Secure Element

- Has internal flash storage
- Can seal secrets, revoke secrets, rotate secrets almost infinitely
- Secrets are rollback and integrity protected
- Can be used as a TPM
- Can act as the root of recovery for a platform, because it can also control the firmware and reset for a managed BMC

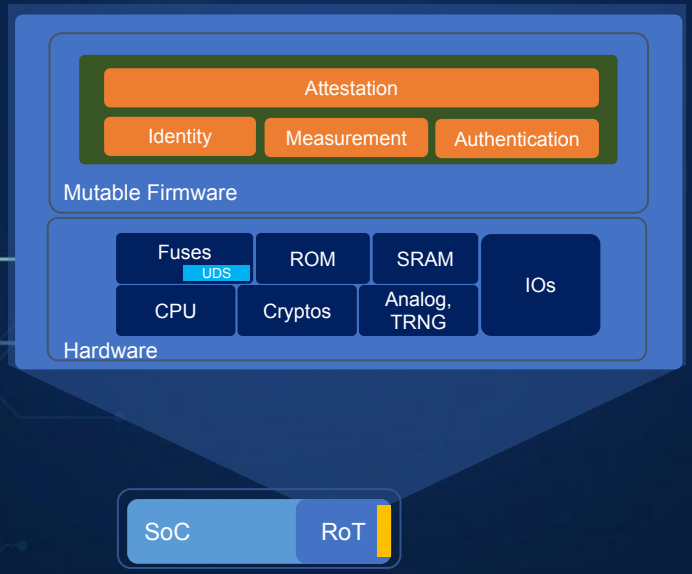
Why Both Roots of Trust in Open Source

Caliptra

opentitan

- Trust the Implementation, not the Standard
- Integrate rapidly, with low repetitive effort
- Coalesce a community of integrators into high quality Trust technology

Caliptra


Caliptra
Attestation
Identity
Measurement
Authentication
Mutable Firmware
Fuses
UDS
ROM
SRAM
IOs
CPU
Cryptos
Analog, TRNG
Hardware
SoC
RoT

What is Caliptra

Caliptra

- First thing out of reset in an SoC
- Reads fuses, forms unique chip identity
- Loads and measures firmware
- Creates a DICE context (DPE)
- Also extends PCRs
- Issues x.509 certificates

DICE = Device Identity Composition Engine
PCR = TPM Platform Configuration Registers

Why Caliptra

Caliptra

- Every SoC anchors trust independently
- Generates cryptographic attestation of the SoC state and firmware
- SoC application cores release from reset with cryptographic APIs and assets
- A DICE context, PCRs, a mailbox, cert chains
- locks debug state

Caliptra – a Journey Through Open Source Silicon

Caliptra

2021	Ideate the concept, enlist Microsoft and AMD
2022	Enlist Nvidia, create Caliptra Core, onboard to OCP and CHIPS Alliance
2023	Caliptra 1.0, github repos, community calls
2024	Caliptra 1.1, lock in integrations, CHIPS and project charter, trademark donation to Linux Foundation
2025	Formal Trademark criteria, Caliptra 2.0 and 2.1, public integrations
2026+	Caliptra 2.2 with USB support. Expand into client devices? Expand into UCIe?

Open Source Silicon is not the Same as Software

- Licensed “closed source” blocks are part of the solution: fuses, entropy sources, PHYs
- Verilator is great, but we need so many more verification tools
- Difficult to do synthesis without proprietary tools
- Every SoC is its own world: Caliptra upstream source is not a fit for per SoC quirks

You can define a sw library entirely in open source.
You can’t define a silicon block entirely in open source.

The Circle of Open Source Trust

- Google, Microsoft, AMD, Nvidia create Caliptra
- Generate the source, fund an ecosystem of contractors
- Bootstrap the community
- Create the trademark to defend quality and the community
- Donate the trademark to Linux Foundation
- Apply for a trademark grant, go through the process
- Learn from comments in reddit and hacker news :)

OpenTitan

opentitan

What is OpenTitan

The First Open Source Silicon Root of Trust (RoT)

Secure Element with Internal Flash Storage

Advanced Secret Management: Seal, revoke, and rotate secrets with rollback & integrity protection

Can function as a **Trusted Platform Module** (TPM)

Platform Root of Recovery: Controls firmware & resets for managed BMCs

Why OpenTitan

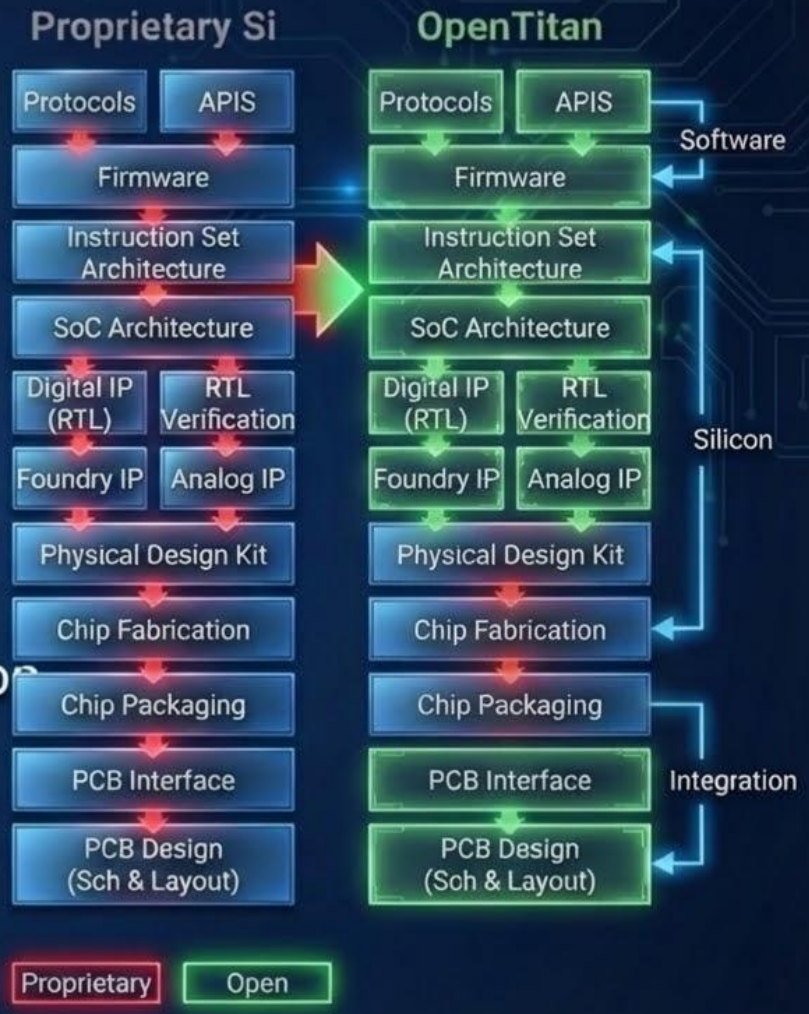
Can be used as secure storage, TPM, SPI Interposer, Platform Root of Trust.

Used in servers, laptops, phones, security keys, and more.

A stand-alone open source project → discrete chip → multiple packages → open source security in multiple markets

Open Silicon Stack

- Guiding principles: Transparency, High Quality, Flexibility
- Realistic, best-effort approach to open-source silicon design
- Design makes logical security guarantees, implementation relies on 3rd-party evaluation for physical security guarantees



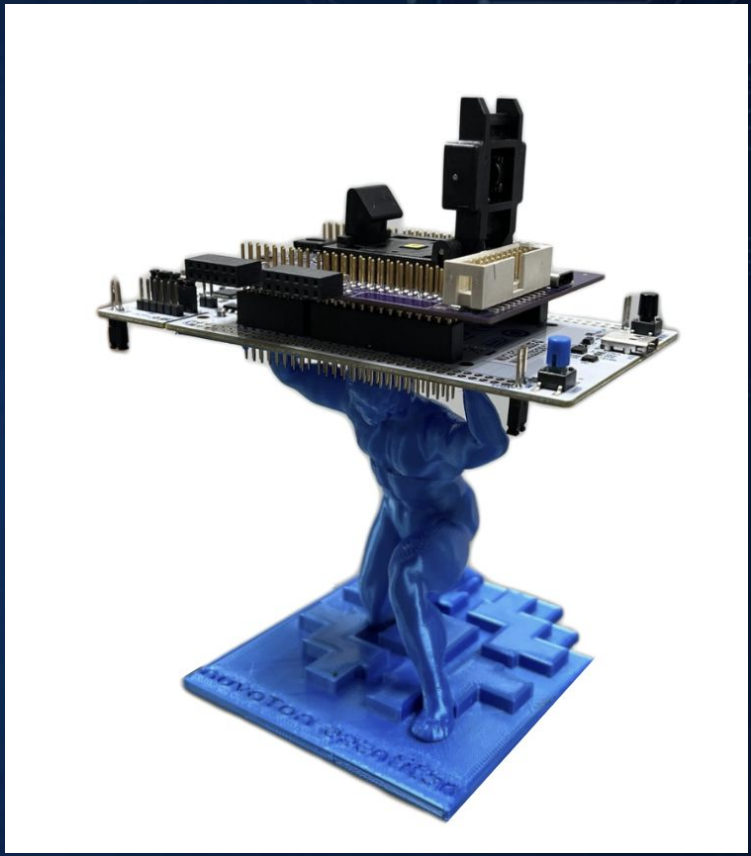
OpenTitan – A Journey Through Open Source Silicon

OpenTitan

- 2018 — Vision boot strapped
- 2019 — lowRISC enlisted
- 2020 — Furious development
- 2021 — Nuvoton enlisted
  Operational Committee to drive integrations
- 2023 — Pivot the project to execute externally
- 2024 — It Lives!
- 2025 — GA platforms committed
- 2026 — $ Production GA

Earl Grey

- Taped out Q2 2025
- Production Ready
- GA in 2026 and 2027 products



Benefits and Challenges of Open Source Silicon

Benefits

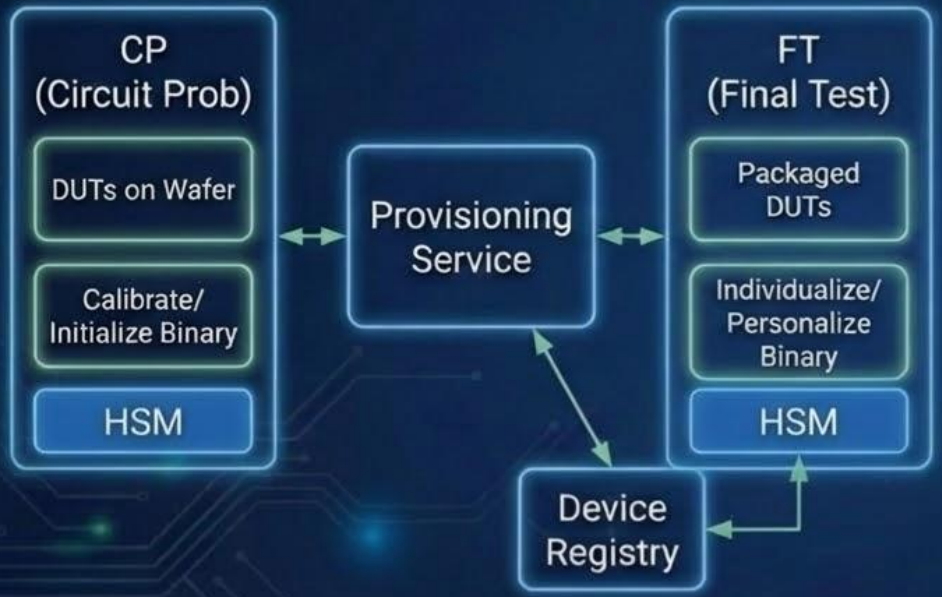
- OpenTitan has generated multiple reusable high quality blocks, many used in Caliptra.

Challenges

- In addition to proprietary blocks, the value of the silicon is rooted in its unique identity, which needs to be provisioned in a proprietary process.

Open Source Provisioning Infrastructure

OpenTitan



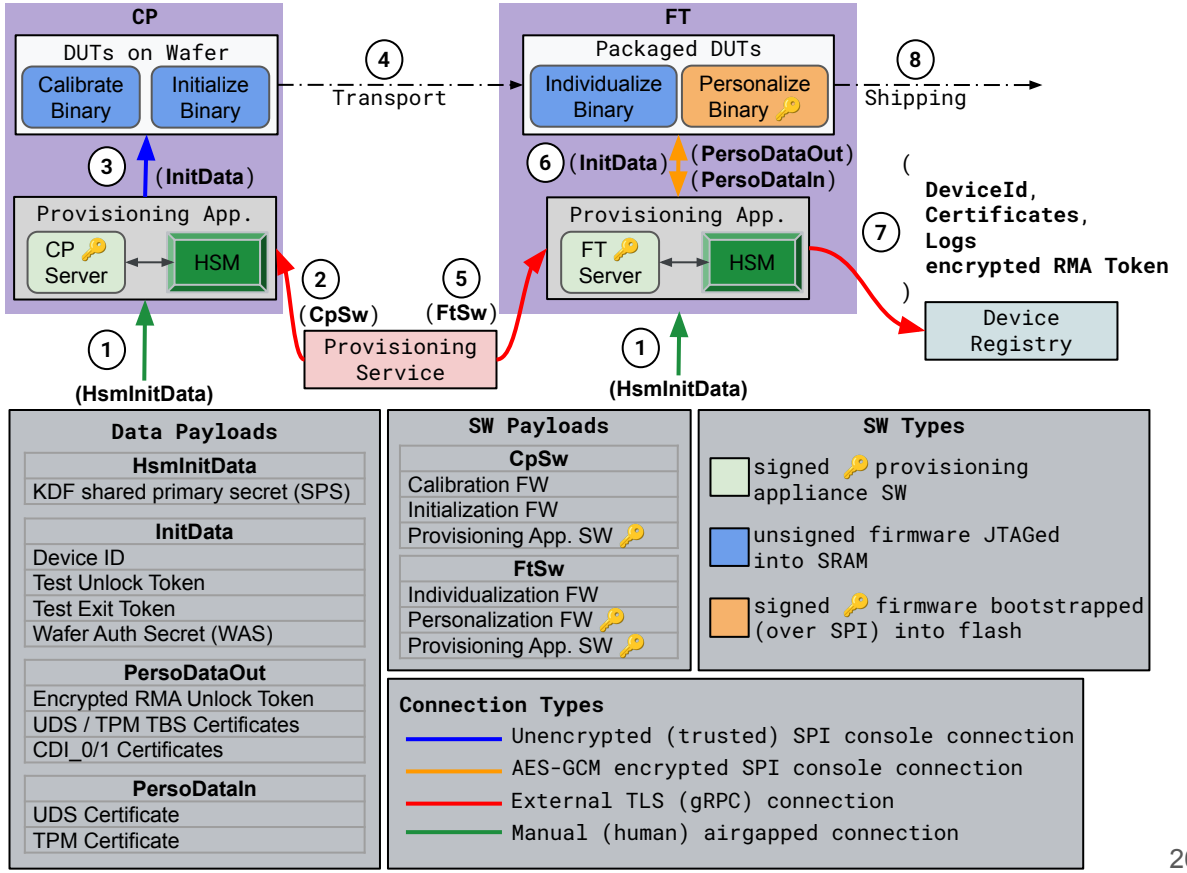
- Secure & Transparent Lifecycle Management
- Wafer & Packaged Device Support
- Cryptographic Initialization & Personalization
- Based on github.com/lowRISC/opentitan-provisioning

github.com/lowRISC/opentitan-provisioning

Open Source Provisioning Infrastructure

- CP (Circuit Prob)
  - Where
    - OSAT (ASE)
    - MSSR compliant facility
  - Two (unsigned) binaries run:
    - calibration
    - initialization
- FT (Final Test)
  - Where
    - OSAT (ASE)
    - MSSR compliant facility
  - Two binaries run
    - individualization (unsigned)
    - personalization (signed 🔑)

github.com/lowRISC/opentitan-provisioning



Demo Time

The Role of RISC-V in Secure Open Source Silicon

RISC-V Cores for the Win

Veer EL2

Ibex

Veer vs Ibex

	Veer	Ibex
Performance	Higher clock frequency (4-stage)	Lower max clock frequency (2-stage)
Security	Lacking initial security features. New features: PMP, DCLS.	Many security features: • Security outputs • Data Independent Timing • Dummy Instruction Insertion • Bus integrity checking • Register file ECC • Register file write enable glitch detection • Icache ECC • Hardened PC • Shadow CSRs • Dual Core Lockstep
VA	Unsupported	Unsupported
S mode	Unsupported	Unsupported

RISC-V Powers Open Source Security

- The engine for open source silicon security
- Diversity of CPUs for different scenarios
- Looking forward to more Control Flow Integrity RISC-V ISA implementations in these cores

Collaborative Hardware Security

- Phenomenal open source traction
- Need more open source tools for verification, synthesis, that commercial chip shops are willing to believe in
- Need more CFI coverage in RISC-V open implementations
- Need open source ecosystem companies to steer trademark license applications, provide quality support packages.

Thank You

Q&A