Scott Johnson
Dominic Rizzo
Parthasarathy Ranganathan
Jon McCune
Richard Ho

Titan: enabling a transparent silicon root of trust for Cloud

Google Cloud

Talk outline

01

Motivation and problem statement

02

System View and Integration

03

Chip Architecture

04

Feature Deep Dives

05

Building a community: Open Titan?

Google Cloud

Motivation and architecture

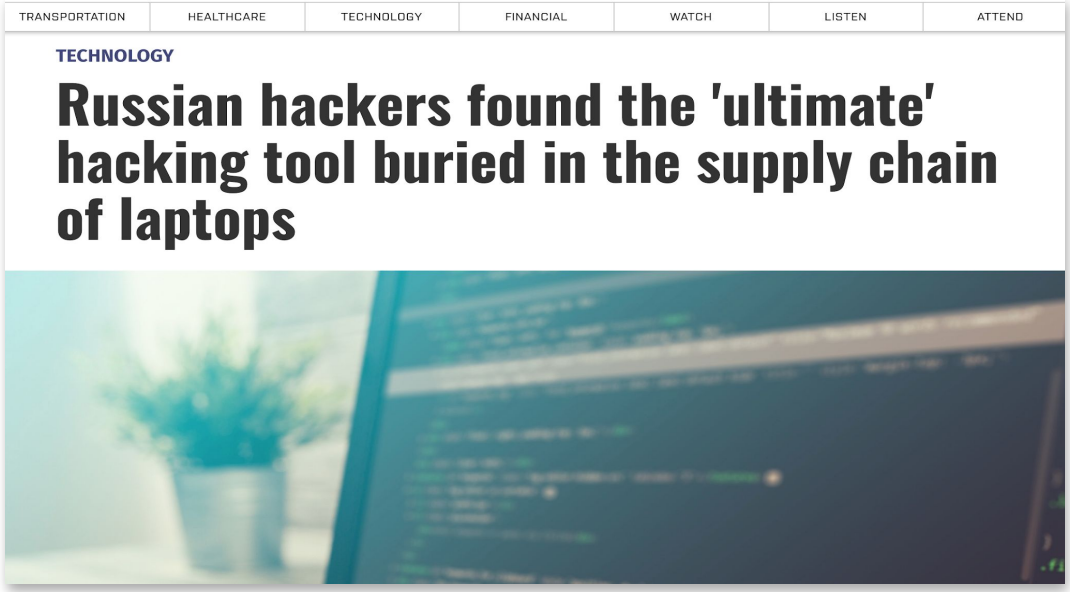
01

Google Cloud

The problem:

Google Cloud

Example 1:
How do we know it is our equipment?

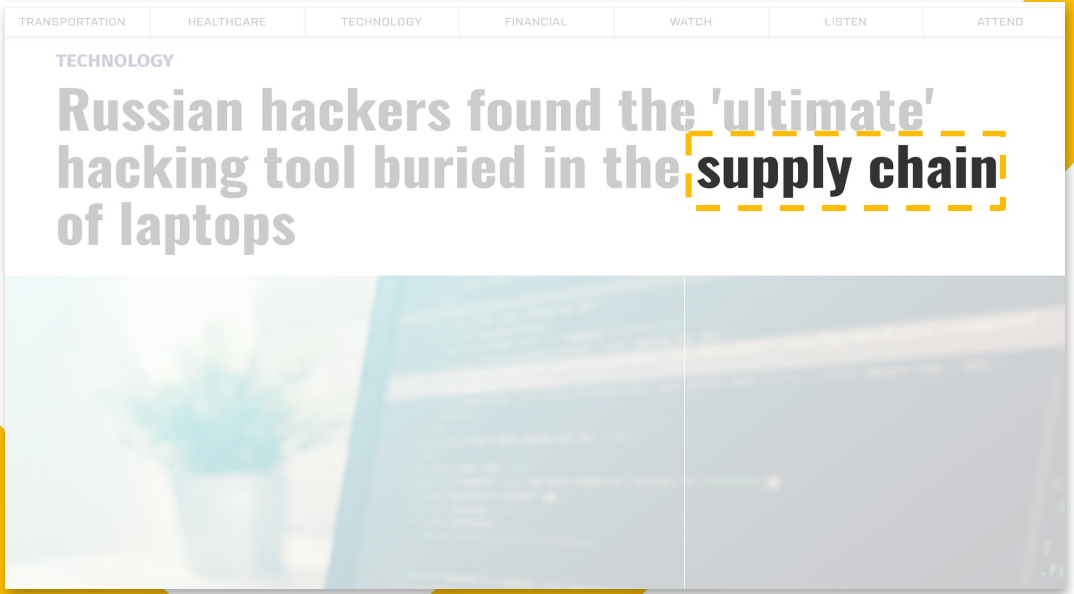

TRANSPORTATION | HEALTHCARE | TECHNOLOGY | FINANCIAL | WATCH | LISTEN | ATTEND

TECHNOLOGY

Russian hackers found the 'ultimate' hacking tool buried in the supply chain of laptops

Google Cloud

Solution:
Tag and verify every device



Google Cloud

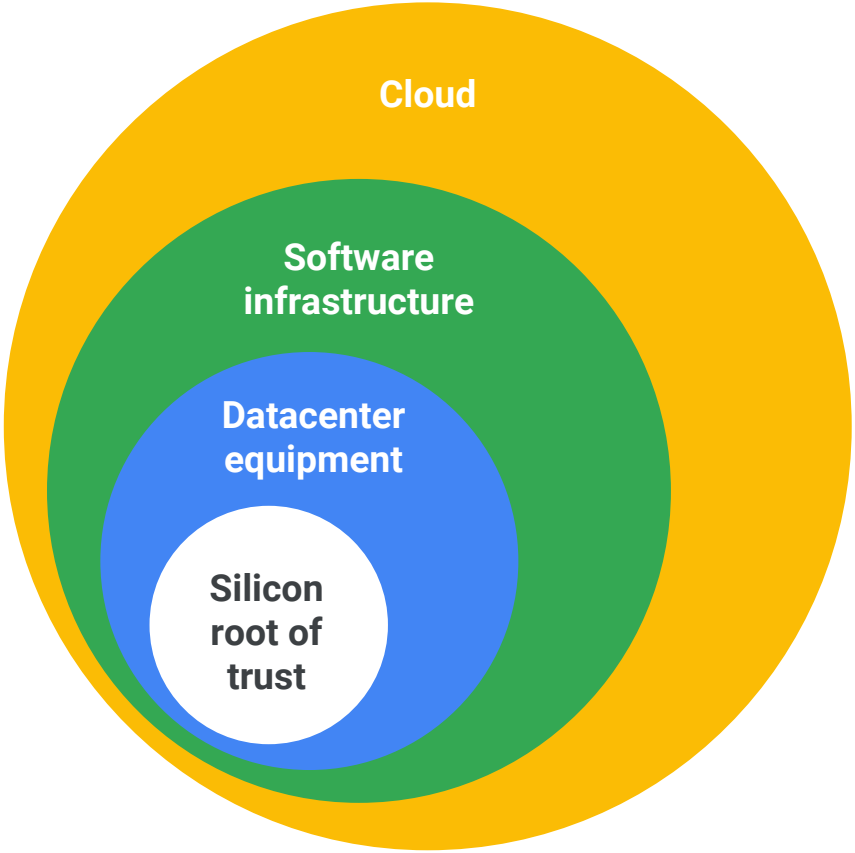
Example 2:
Can we trust our boot chain?

Google Cloud

Solution:
Sign and verify all boot code

Google Cloud

Conclusion:
We need a silicon root of trust



Google Cloud

Cloud security properties

Trusted Machine Identity

First Instruction Integrity

Tamper-evident logging

Trusted implementation

1 2 3 4

Every element in the datacenter should be securely identifiable: cryptographic attestation

Google Cloud

Cloud security properties

Trusted Machine Identity

First Instruction Integrity

Tamper-evident logging

Trusted implementation

1 2 3 4

The first code executed should be trusted: cryptographically signed and verified firmware, live monitored for protection

Google Cloud

Cloud security properties

Trusted Machine Identity

First Instruction Integrity

Tamper-evident logging

Trusted implementation

1 2 3 4

All activities in the datacenter should be monitored and logged in a tamper resistant manner

Google Cloud

Cloud security properties

1. Trusted Machine Identity
2. First Instruction Integrity
3. Tamper-evident logging
4. Trusted implementation

Own and/or verify every piece of the stack from transistors up to critical firmware

Google Cloud

Chip Requirements

1. Trusted Machine Identity
2. First Instruction Integrity
3. Tamper-evident logging
4. Trusted implementation

- On-chip verified boot
- Cryptographic identity & secure mfg
- Boot Firmware signature check + monitor
- Silicon physical security
- Transparent development, full-stack

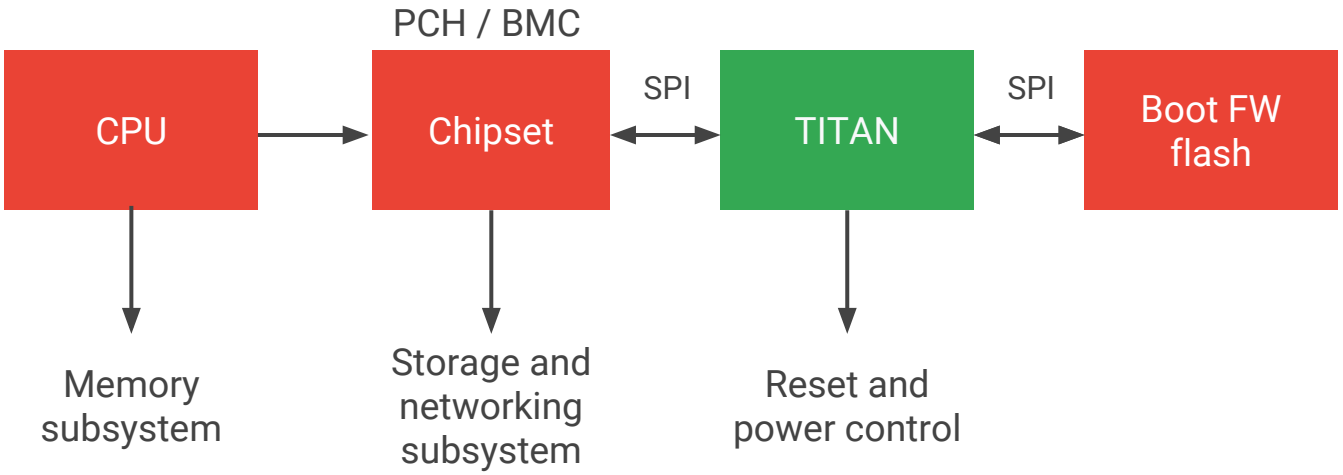
Google Cloud

System View and Integration

02

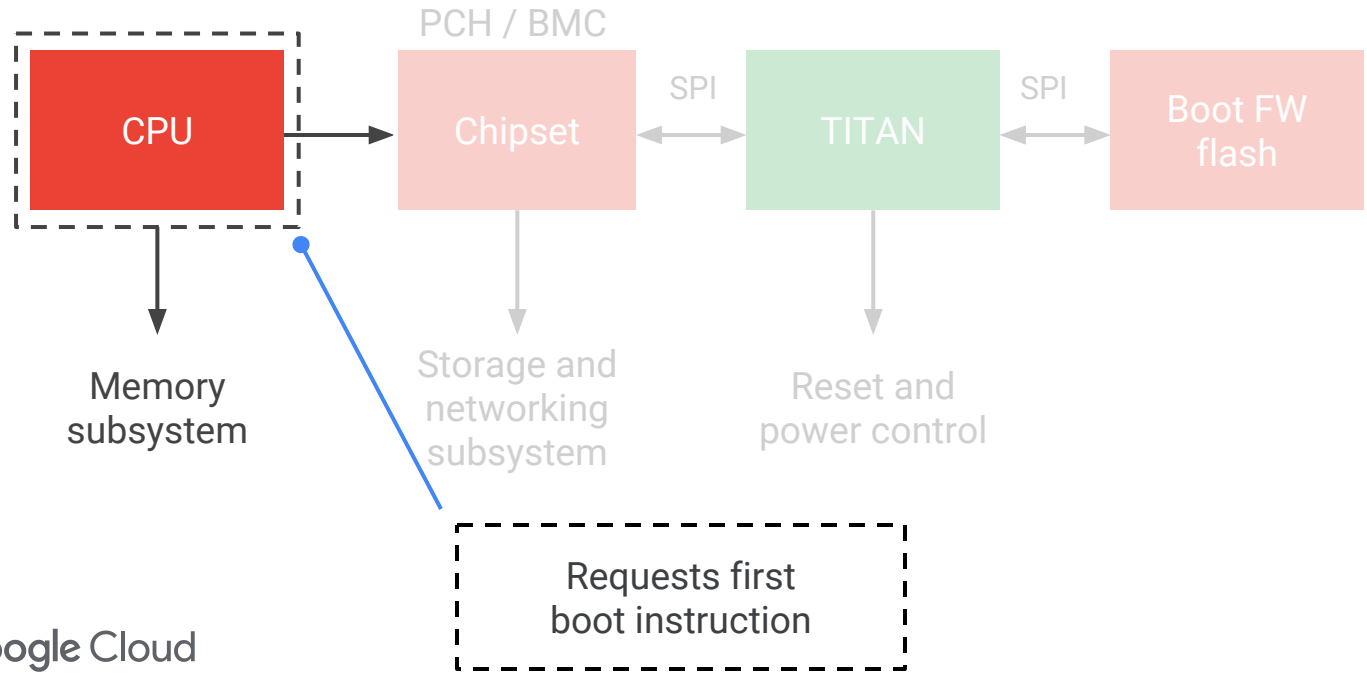
Google Cloud

Titan system integration



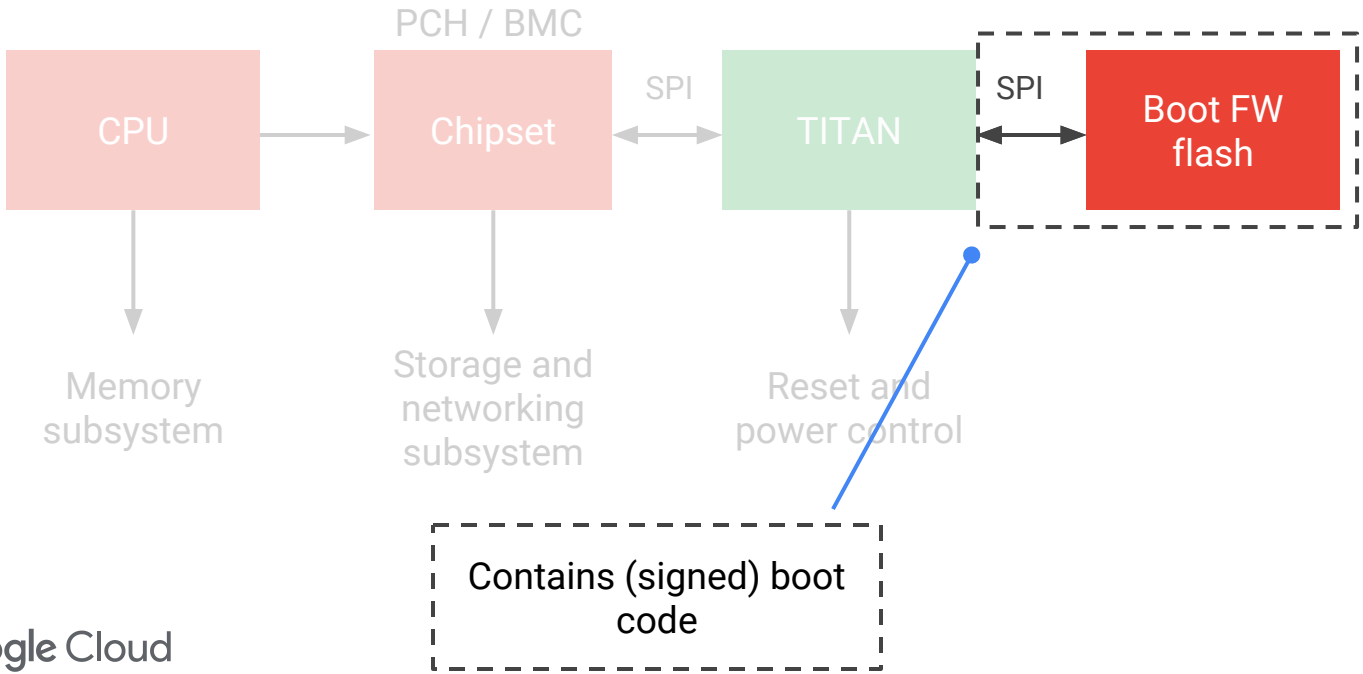
Google Cloud

Titan system integration



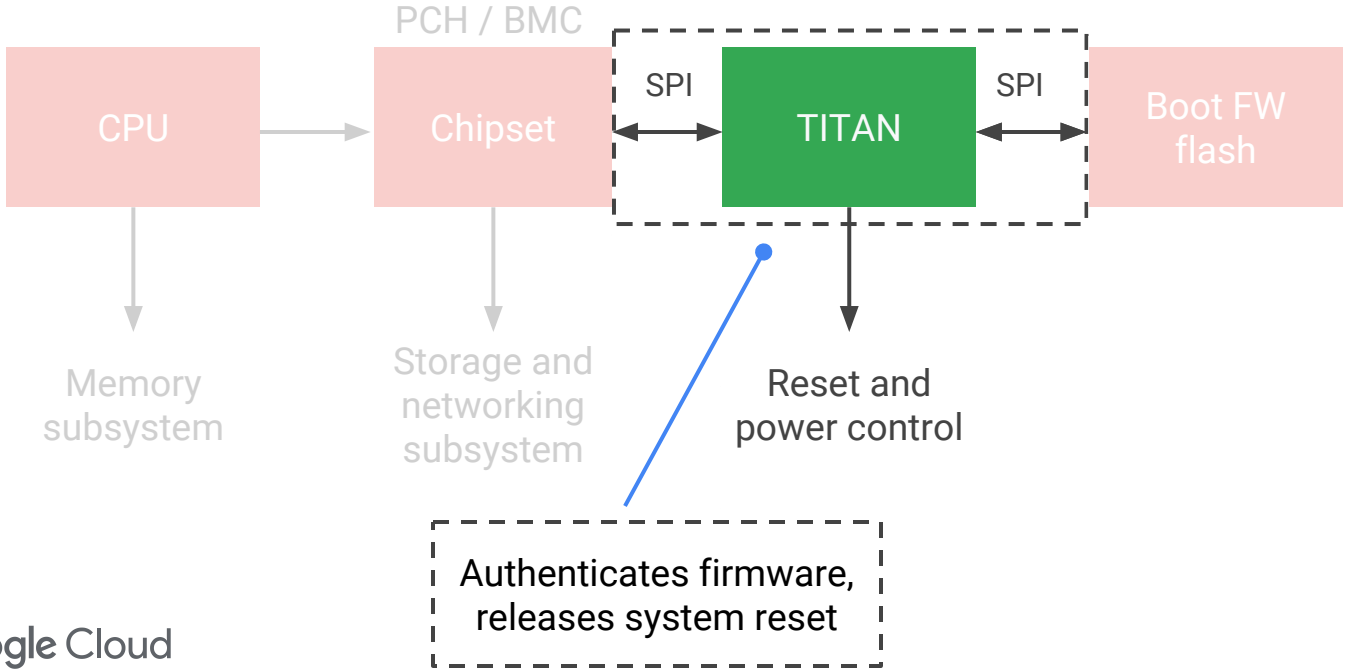
Google Cloud

Titan system integration



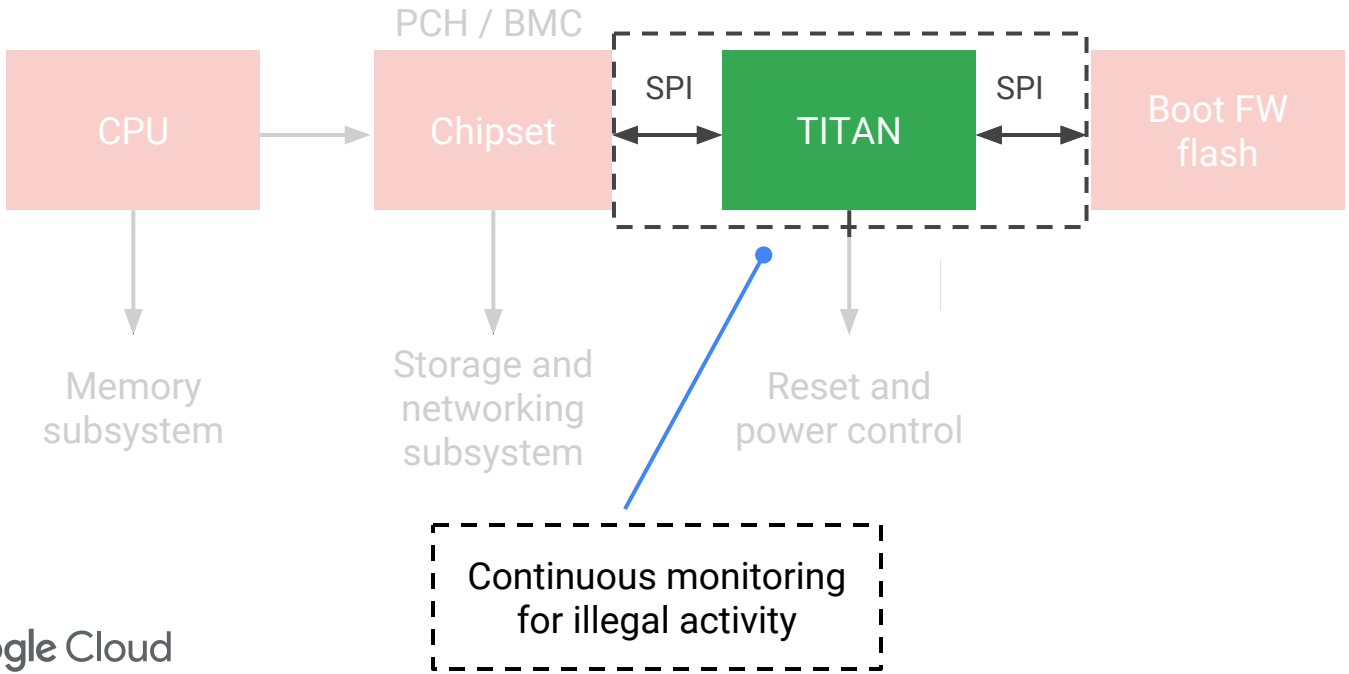
Google Cloud

Titan system integration



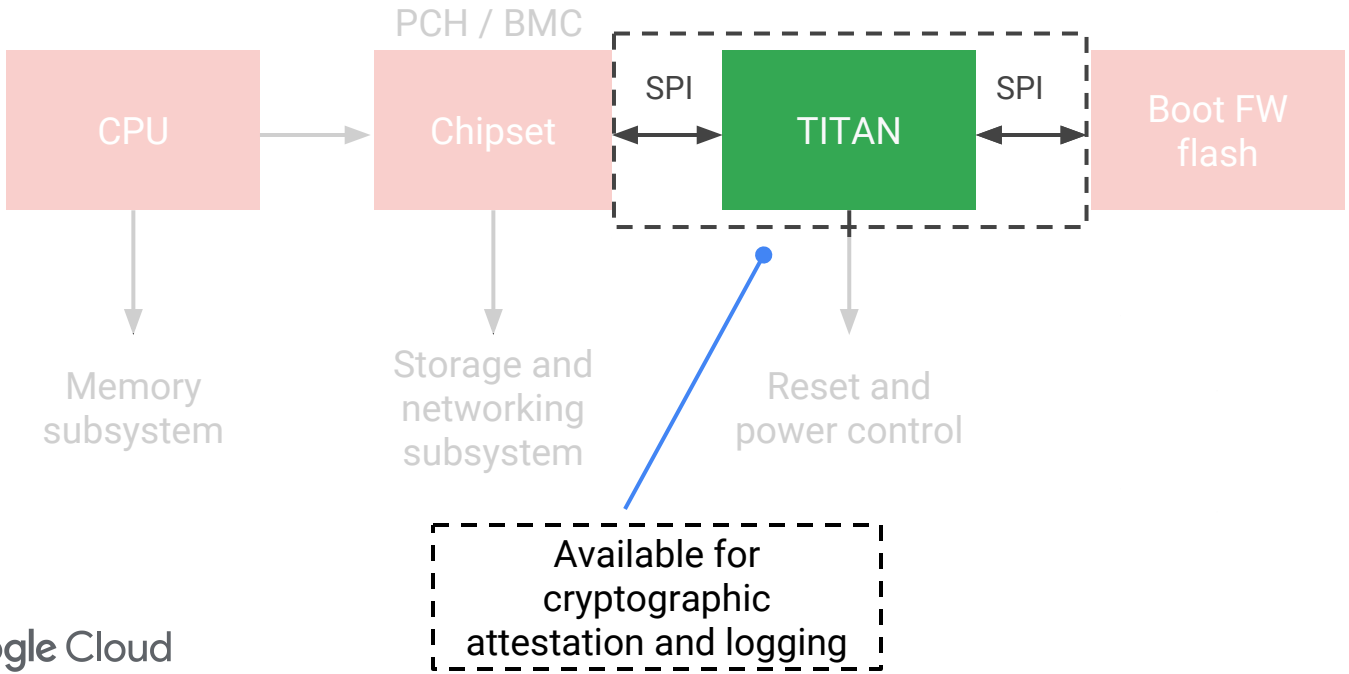
Google Cloud

Titan system integration



Google Cloud

Titan system integration



Google Cloud

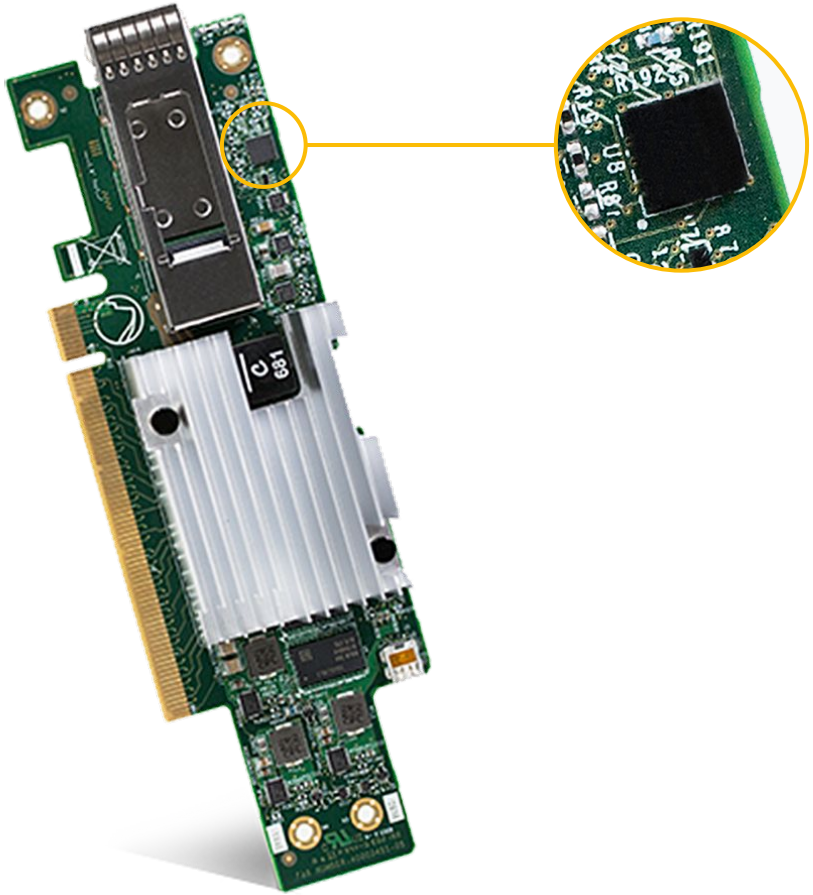
Chip architecture

03

Google Cloud

What
is Titan?

- Secure low-power microcontroller designed with cloud security as first-class consideration
- Not just a chip, but the supporting system and security architecture + manufacturing flow



Google Cloud

Why
make our own?

Implementation transparency

Complete ownership, auditability, build local expertise

Agility & velocity

Technology changes, new risk vectors arrive

No existing solutions

Vendor-agnosticity, custom features

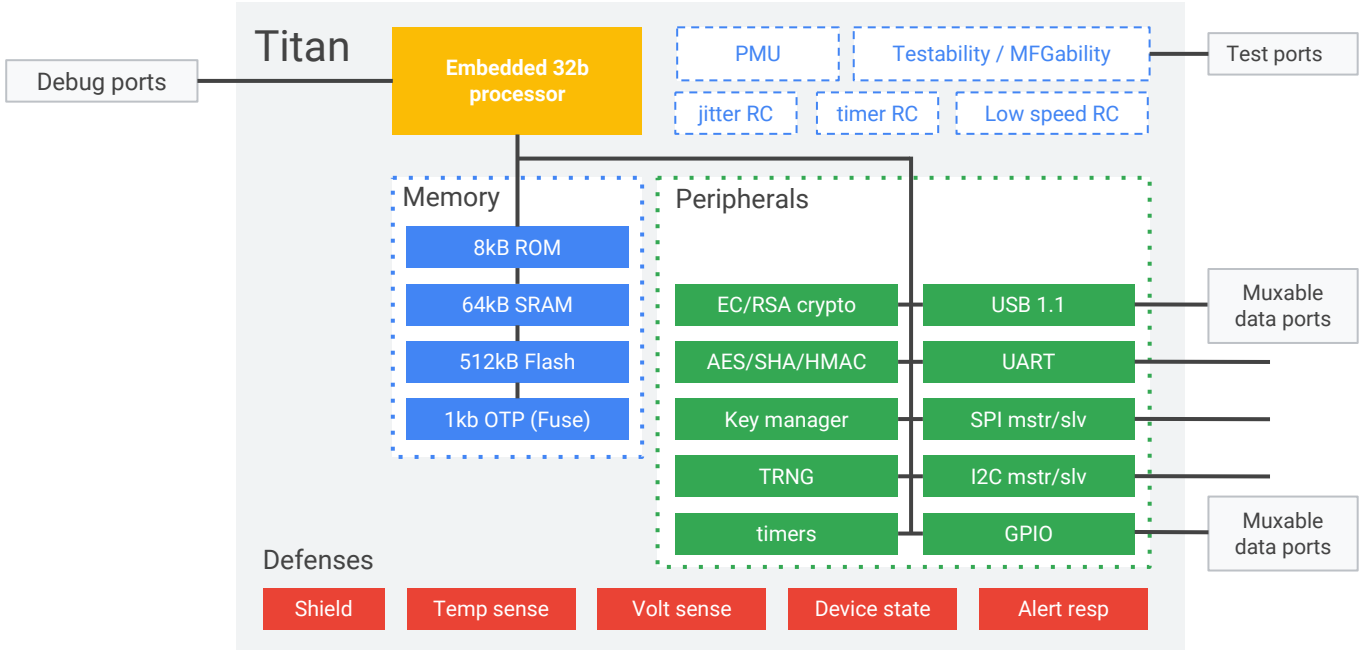
Google Cloud

Glossary: a quick security chip primer

AES	Symmetric (shared-key) crypto algorithm
alert	Security critical event
BIST	Built in self test
BL	Boot loader
CA	Certificate authority
device state	Temporal state in life cycle of device (test, production, return for test, end of life)
EC	Elliptic curve: modern crypto algorithm
HMAC	Hash message authentication code
I2C	Two-pin low-speed peripheral interface
key mgr	Management of key and secret storage

NMI	Non-maskable interrupt
OTP	One-time programmable (fuse) memory
PCH	Intel Platform Controller Hub
PMU	Power Management Unit
RC	Resistor/capacitor clock circuit
RSA	Circa 1980s crypto algorithm
RTC	Real Time Clock
SHA	Hashing algorithm
SPI	4+ pin peripheral interface
TRNG	True random number generator

Titan specifications



Google Cloud

Titan specifications

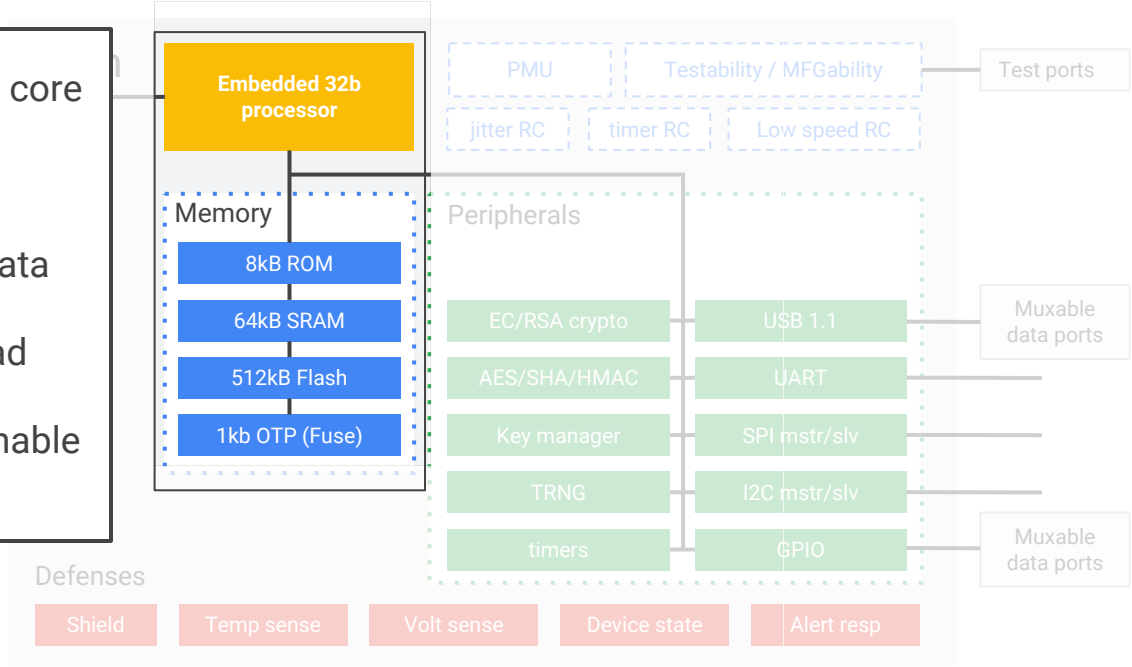
32b microcontroller core

Boot ROM

Flash for instr + data

SRAM scratchpad

One-time programmable fuses



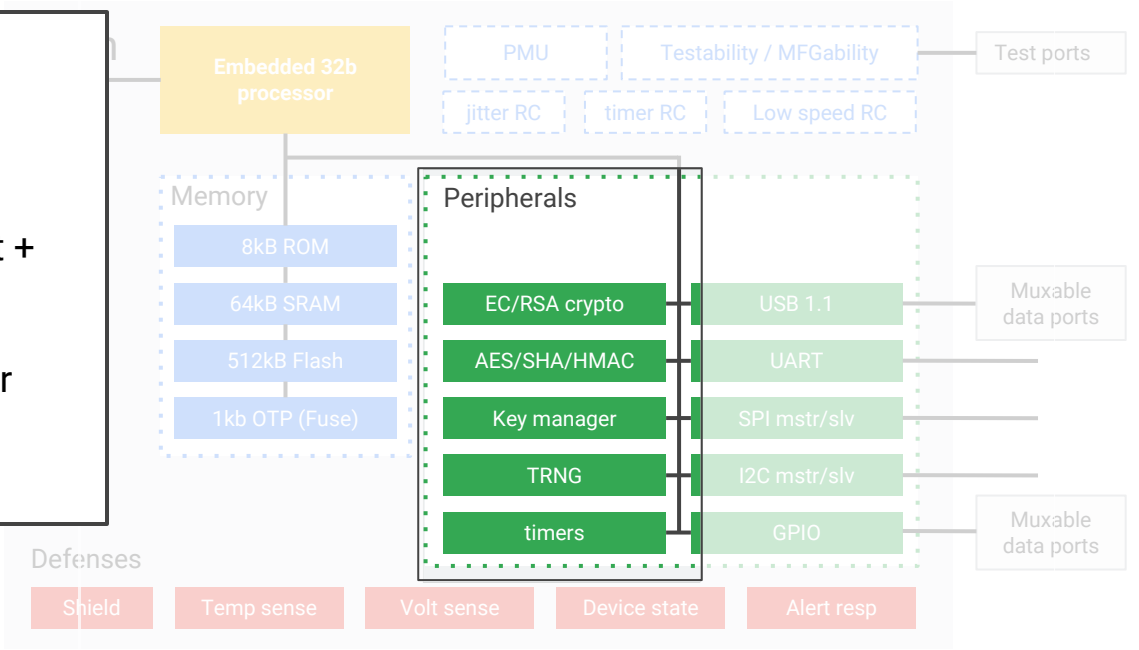
Google Cloud

Titan specifications

Cryptographic acceleration

Key management + storage

Random number generator



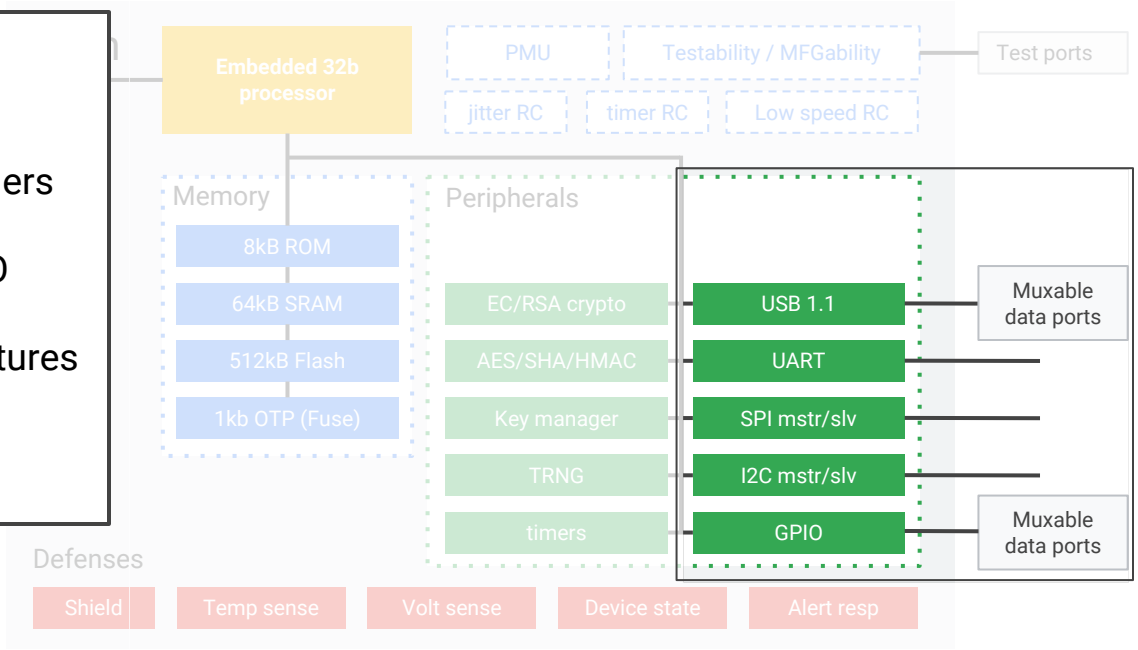
Google Cloud

Titan specifications

Peripheral controllers

Multipurpose IO

Custom Google features



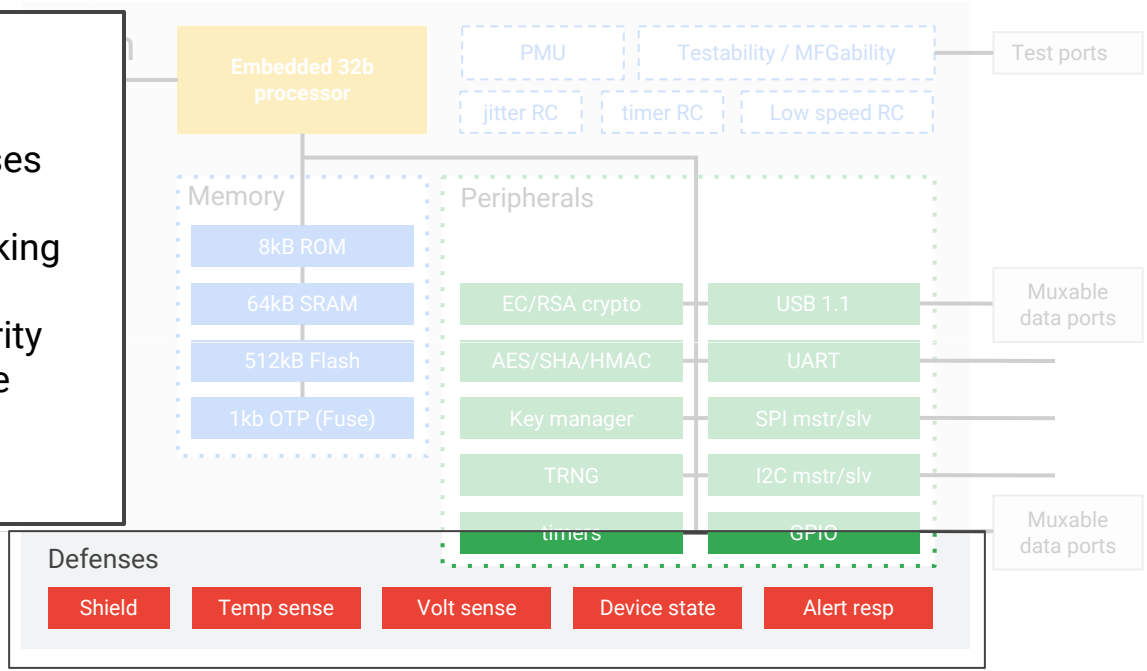
Google Cloud

Titan specifications

Physical defenses

Live status checking

Hardware security alert response



Google Cloud

Feature Deep Dives

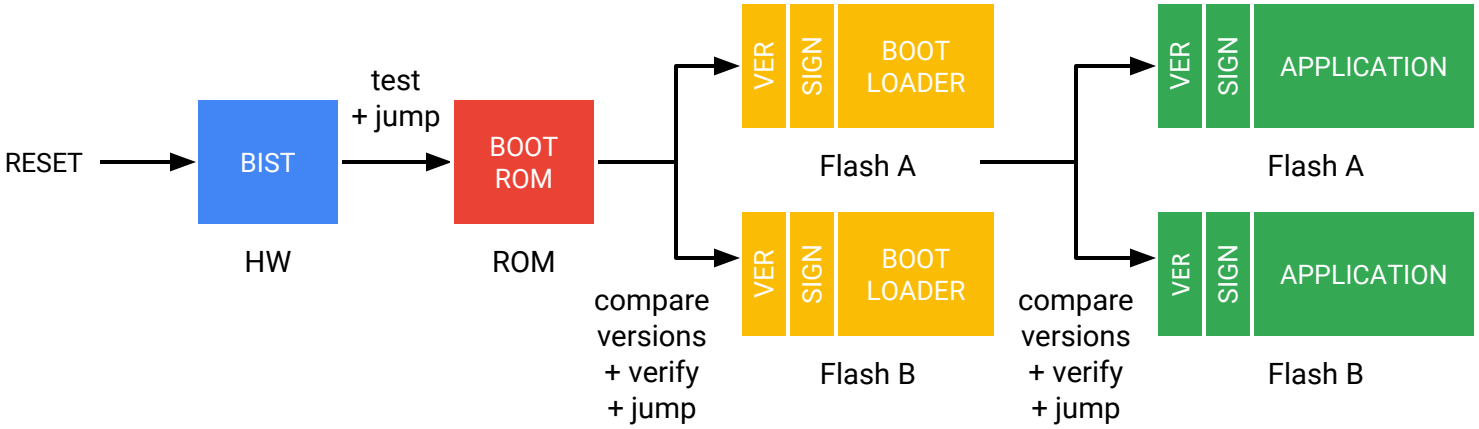
04

Google Cloud

Verified Boot

Google Cloud

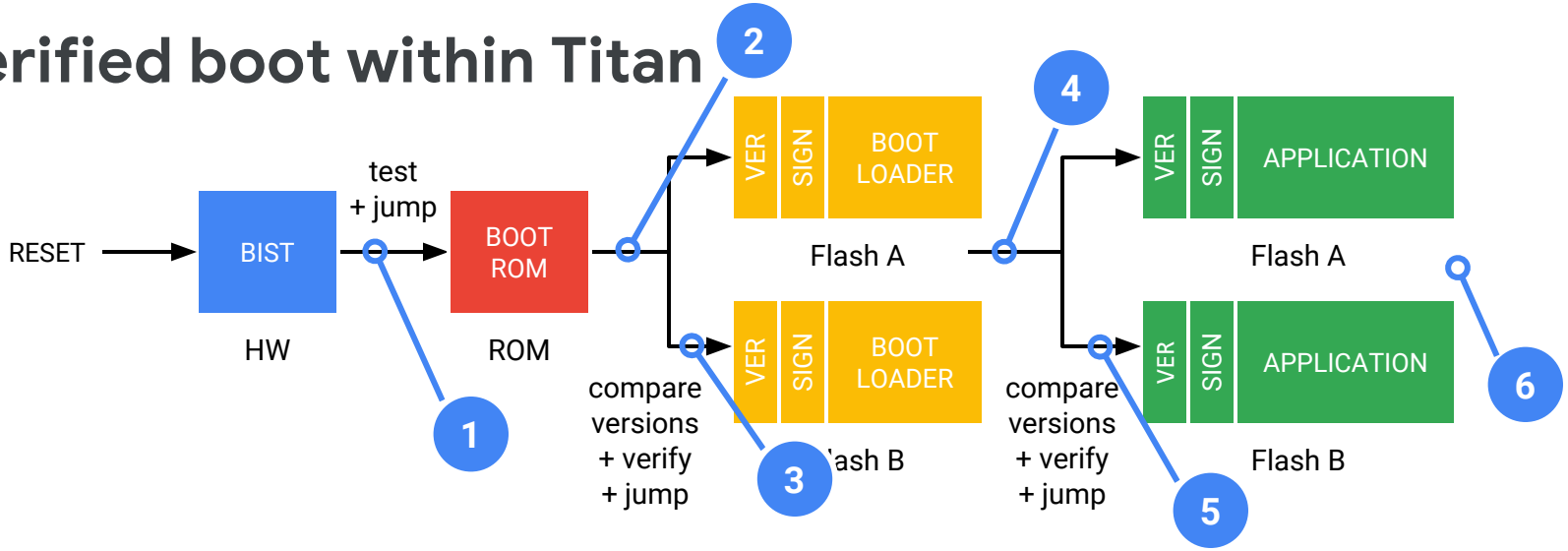
Verified boot within Titan



- Each stage verifies the next
- Earlier stages do security settings, lock out further access
- Permission levels drop at each stage, protecting critical control points
- Splitting flash code into banks allows two copies: live-updatable
- Code signing taken seriously; multiple key holders, offline logs, playbooks

Google Cloud

Verified boot within Titan



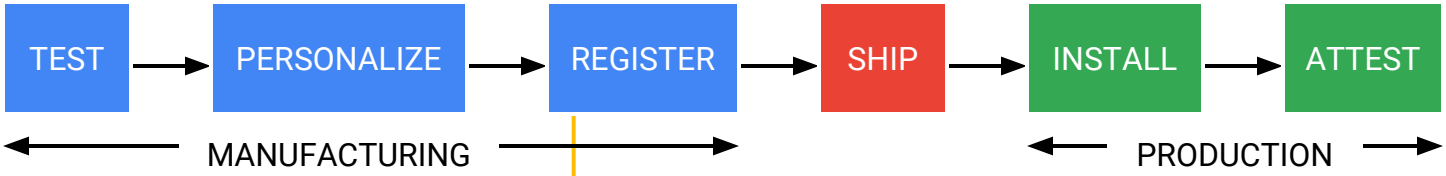
1. Test logic (LBIST) and ROM (MBIST); if fail ⇒ stay in reset; else jump to ROM
2. Compare bootloader (BL) versions A + B; choose most recent
3. Verify BL signature; if fail, retry with other BL; if fail, freeze
4. Compare firmware application (FW) versions A + B; choose most recent
5. Verify FW signature; if fail, retry with other FW; if fail, freeze
6. Execute successfully verified FW

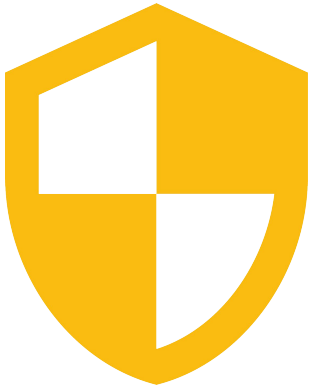
Google Cloud

Trusted identity

Google Cloud

Trusted chip identity



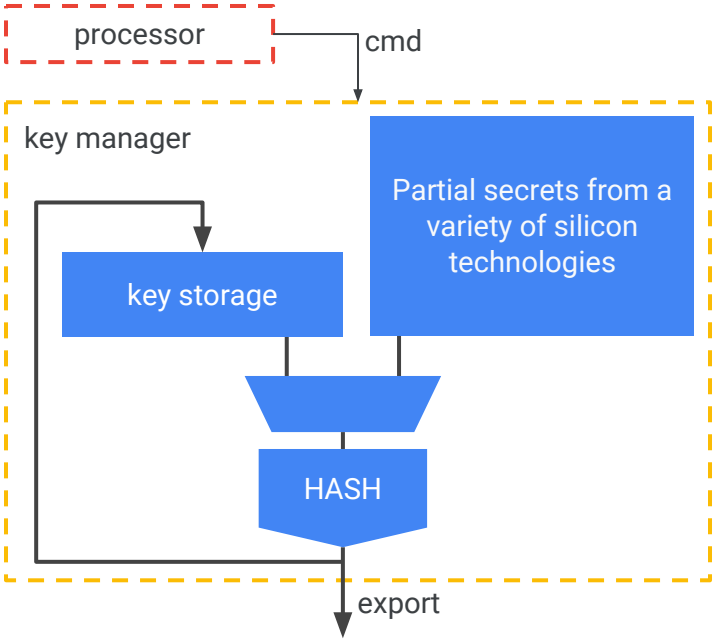


- Establish trust at manufacturing
- Each tested device uniquely identified (personalized)
  - Assigned a serial number, unique but not secret
  - Self-generates a cryptographically strong Identity Key
- Identity registered in off-site secure database
- Parts shipped, put onto datacenter devices for production
- Parts available for “attestation”, proof that they are ours

Google Cloud

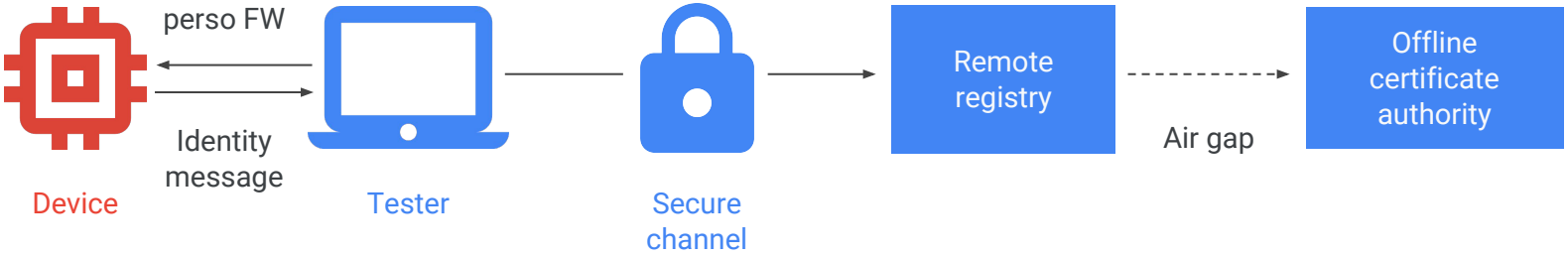
Key manager creates chip identity key

- Dedicated hardware execution
- Processor walks FSM commands
- Keys inaccessible to processor
- Identity = crypto_hash of partial secrets
  - Each comes from a different silicon technology
  - Requires attackers to defeat each
- Export enabled if FSM complete
- Export disabled after manufacture



Google Cloud

Trusted identity (registration)



- Personalization firmware loaded
- Chip creates identity message
- Identity exported to registry via secure channel
- Identities signed by offline certificate authority
- Certificate available for installation
- Identity available for later query

Google Cloud

Life cycle tracking using OTP Fuses

- After manufacturing, must continue to guarantee authenticity
- Define six stages, and what is enabled in each stage

  Raw: no features enabled, deters wafer theft

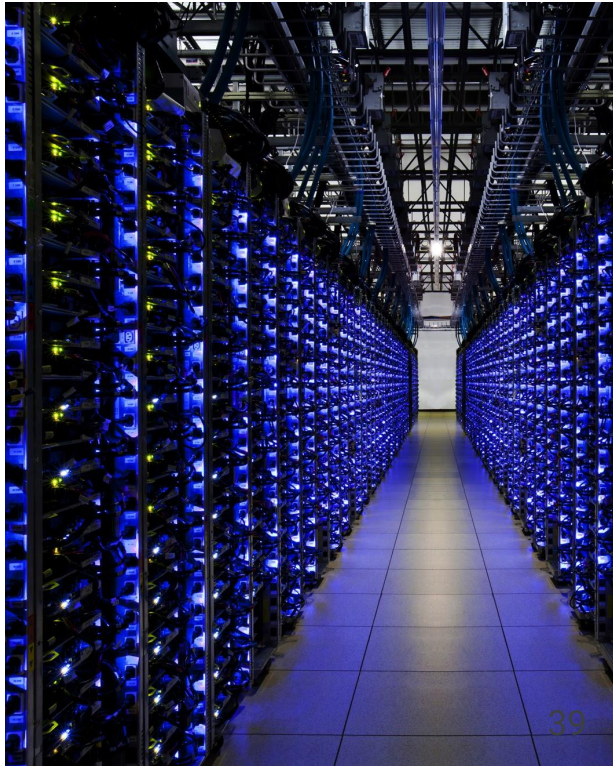
  Test: enable test features only, no production features

  Development: enable production-level features for lab bringup

  Production: final production features, no testability, unique keys

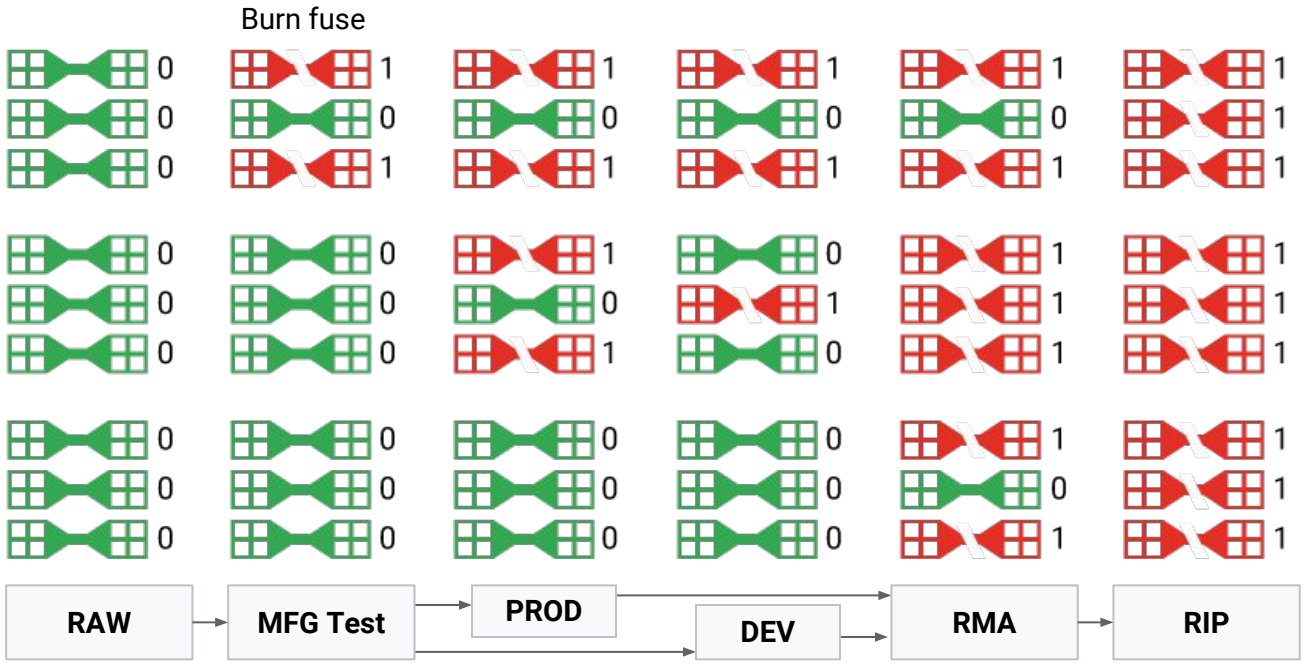
  RMA (return for test): re-enable testability, no more production

  RIP: after RMA or mfg failure, permanently disable device
- Burnable fuses track life cycle from manufacturing to production
- Each stage transition a one-way street



Google Cloud

Life cycle tracking using OTP Fuses



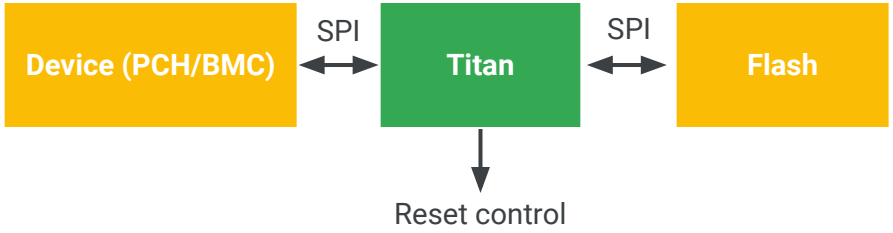
Google Cloud

First instruction integrity

Google Cloud

First instruction integrity

- Titan interposes on SPI, between host and system firmware Flash
- At system reset, does signature check of FW
  - Signature OK ⇒ enables system
  - Signature fail ⇒ alerts of failure
- Live monitoring
  - Snoops SPI for illegal activity
  - Unauthorized actions converted to harmless commands

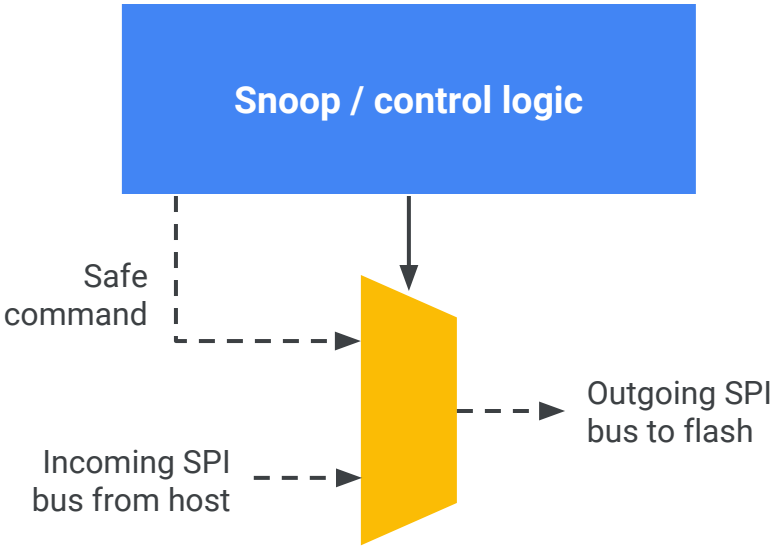


Google Cloud

SPI interposition

The challenges of SPI interposition

- Vendor agnostic requires flexibility
- SPI does not have flow control
- Passthrough latency must be minimized
- Chip & board timing a challenge
- Can affect boot latency



Physical and tamper-resistant security

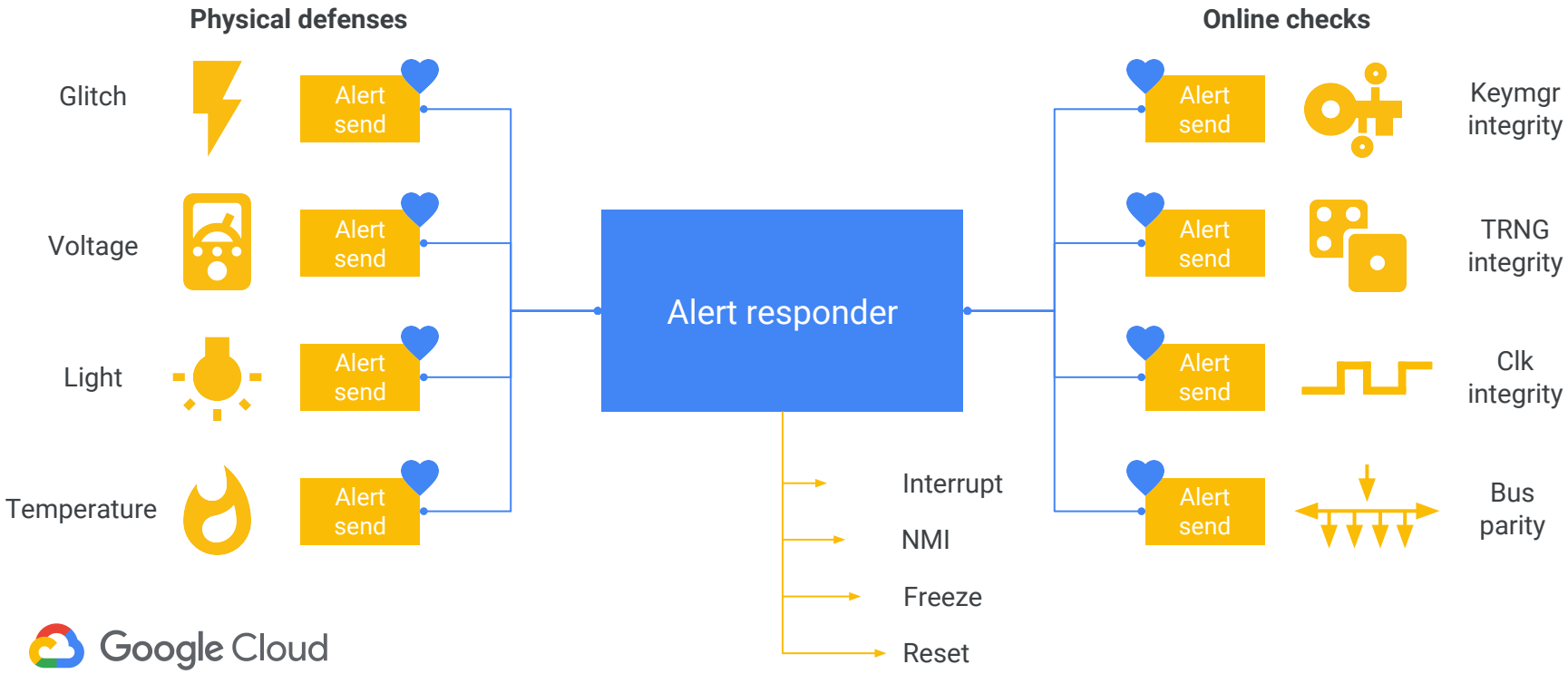
Google Cloud

Physical security & countermeasures

Anti-glitch / anti-tamper mechanisms

- Attack detection (glitch, laser, thermal, voltage)
- Fuse, key storage, clock, and memory integrity checks
- Memory and bus scrambling and protection
- Register — and memory-range address protection and locking
- TRNG entropy monitoring
- Boot-time and live-status checks

Physical security & countermeasures

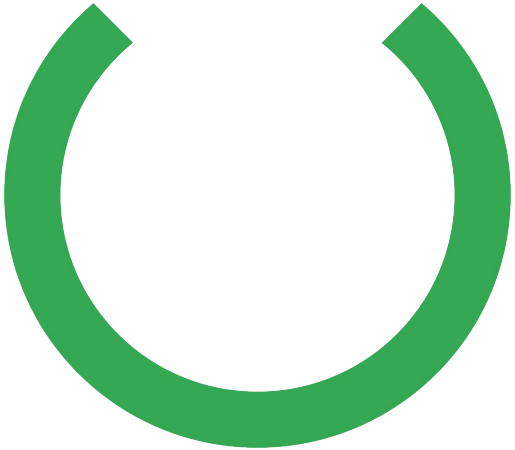


Google Cloud

Open Titan

Google Cloud

Moving from Titan to Open Titan



Google Cloud

Thesis

The functional security mechanisms, provenance and digital implementation are commodities and thus good candidates for open sourcing

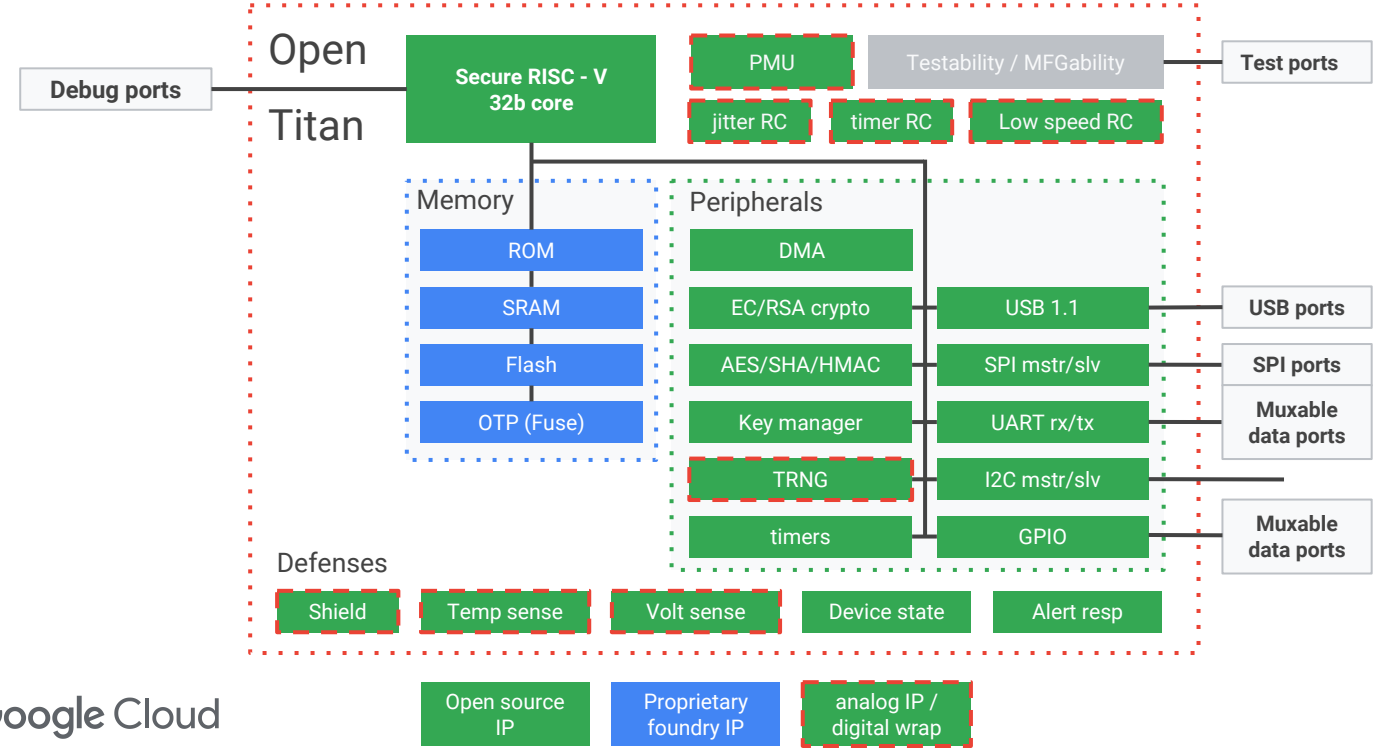
Evidence

Credible open ISAs, our RTL repositories, standard crypto primitives

Outcome

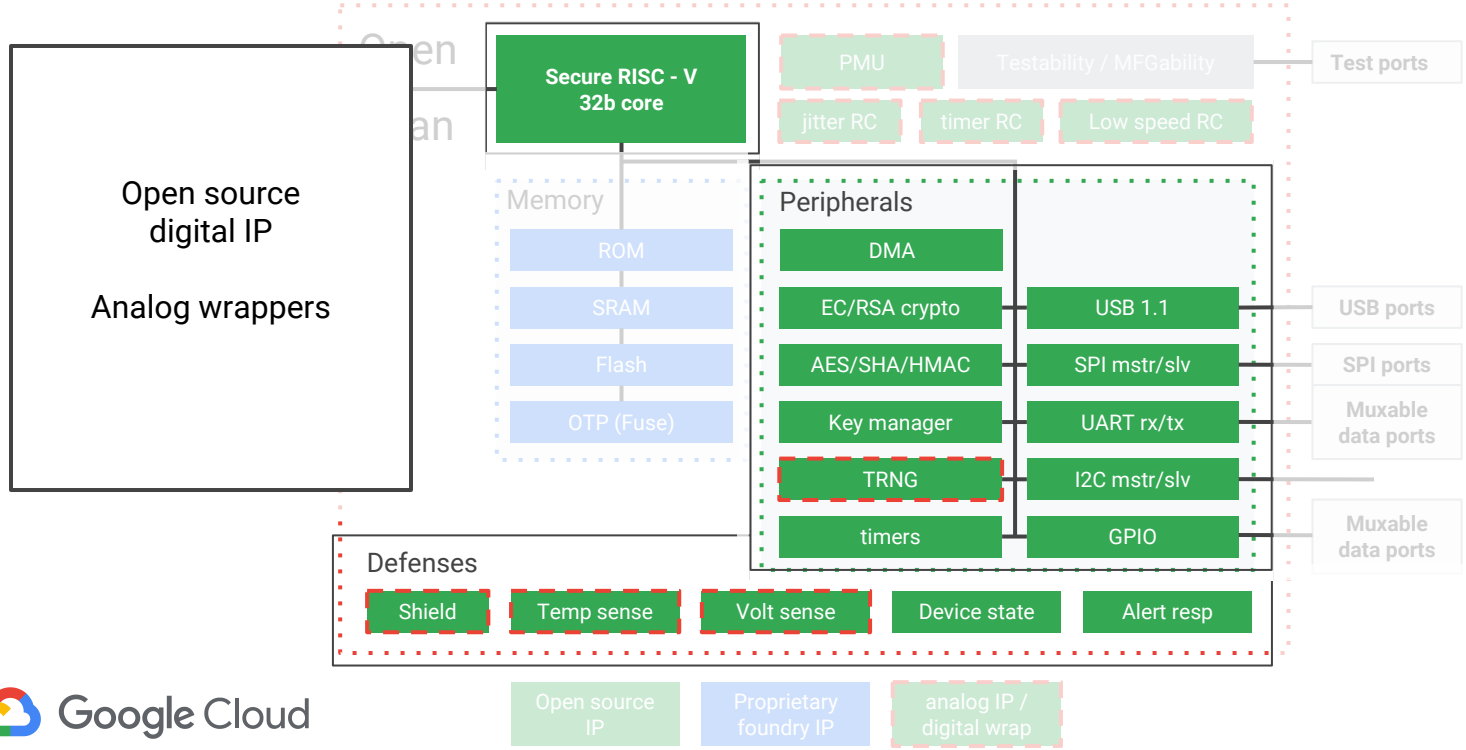
An open, transparent implementation of a secure cloud root of trust

What would Open Titan look like?



Google Cloud

What would Open Titan look like?

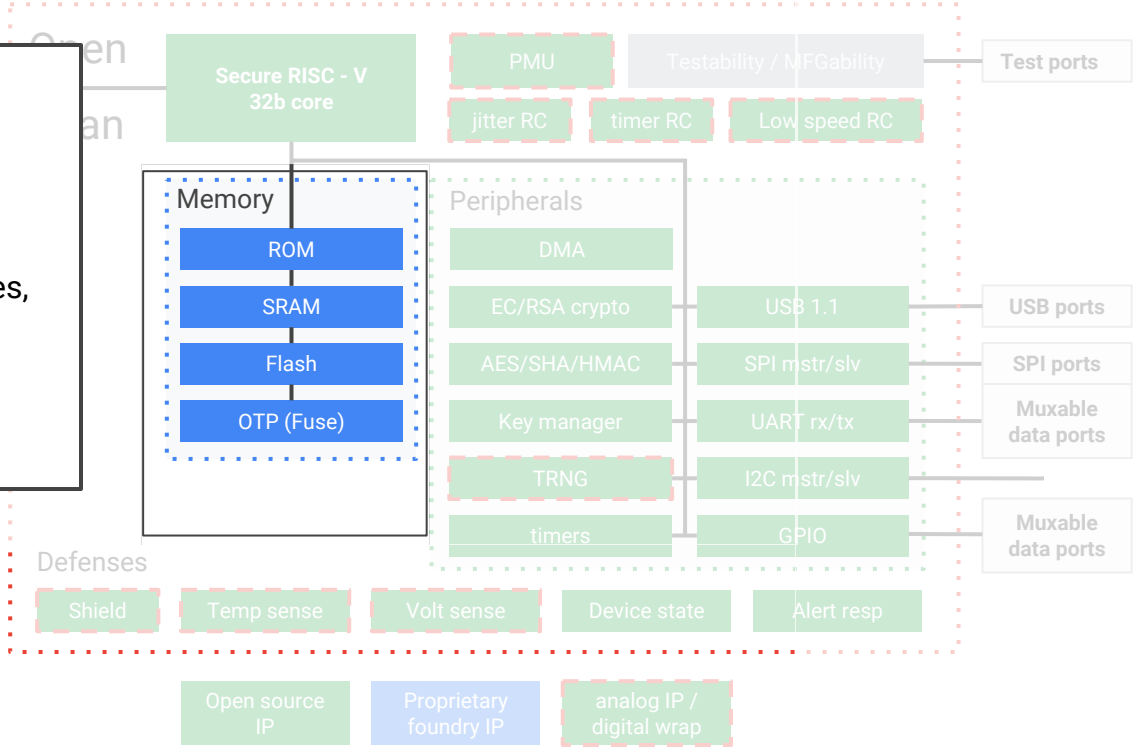


Google Cloud

What would Open Titan look like?

Required vendor collateral:

STDCELL, memories, pads, etc.



Google Cloud

Silicon Transparency Working Group

Questions

For additional information
https://cloudplatform.googleblog.com/2017/08/Titan-in-depth-security-in-plaintext.html

Google Cloud

That’s a wrap