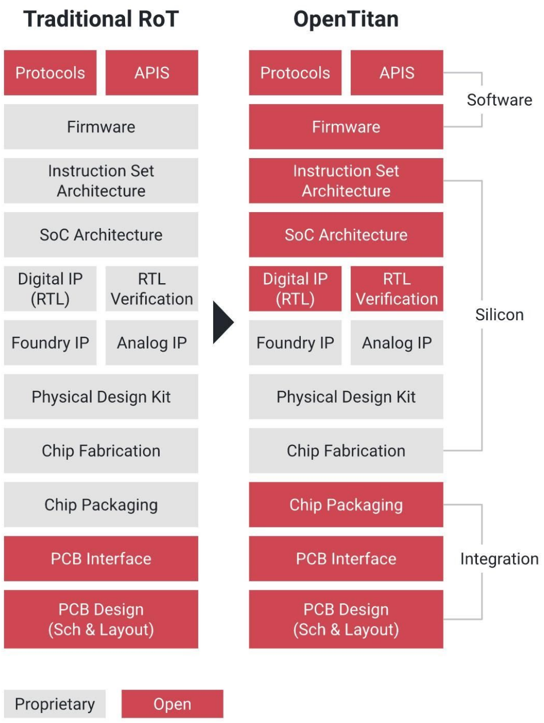
opentitan

OpenTitan is the first open source project building a transparent, high-quality silicon root of trust (RoT) design. The project uses a successful collaborative engineering model pioneered by lowRISC in partnership with Google and other commercial and academic partners.



Traditional RoT	OpenTitan	
🟥 Protocols · 🟥 APIS	🟥 Protocols · 🟥 APIS	Software
▨ Firmware	🟥 Firmware	
▨ Instruction Set Architecture	🟥 Instruction Set Architecture	Silicon
▨ SoC Architecture	🟥 SoC Architecture	
▨ Digital IP (RTL) · ▨ RTL Verification	🟥 Digital IP (RTL) · 🟥 RTL Verification	
▨ Foundry IP · ▨ Analog IP	▨ Foundry IP · ▨ Analog IP	
▨ Physical Design Kit	▨ Physical Design Kit	
▨ Chip Fabrication	▨ Chip Fabrication	
▨ Chip Packaging	🟥 Chip Packaging	Integration
🟥 PCB Interface	🟥 PCB Interface	
🟥 PCB Design (Sch & Layout)	🟥 PCB Design (Sch & Layout)	

▨ Proprietary 🟥 Open

Transparent Anyone can inspect, evaluate, and contribute to OpenTitan’s design and documentation to help build a more transparent, trustworthy silicon RoT for all.

High quality OpenTitan is building and maintaining a high-quality logically-secure silicon design, including reference firmware, verification collateral, and technical documentation.

Flexible Adopters can reduce costs and reach more customers by using a vendor- and platform-agnostic silicon RoT design that can be integrated into data center servers, storage devices, peripherals, and other hardware.

Security begins with secure infrastructure. To increase confidence in the security and integrity of the infrastructure, we need to anchor our trust at the foundation - in a special-purpose chip. OpenTitan will deliver a high-quality RoT design and integration guidelines for use in data center servers, storage, peripherals, and more. Open sourcing the silicon design makes it more transparent, trustworthy, and ultimately, secure.

Founding partners

lowRISC

ETH zürich

G+D
Mobile Security

Google

nuvoTon

Western Digital.

Interested in participating in the project? Contact us at get-involved@opentitan.org

OpenTitan is administered by lowRISC.
Find out more at www.opentitan.org

lowRISC

Anchoring trust in silicon

The silicon RoT helps ensure the hardware infrastructure and software that runs on it remain in their intended, trustworthy state by verifying critical system components boot securely with authorized and verifiable code. It helps to:

- Ensure that a server or a device boots with the correct firmware and hasn't been infected by a low-level malware.
- Provide a cryptographically unique machine identity so an operator can verify that a server or a device is legitimate.
- Protect secrets like encryption keys in a tamper-resistant way even for people with physical access (e.g., while a server or a device is being shipped).
- Provide authoritative, tamper-evident audit records, and other runtime security services.

OpenTitan can be used to secure the integrity of servers, network cards, client devices (e.g., laptops, phones), routers, IoT devices, autonomous vehicles, 4G/5G basestations and more.

Find out more at www.opentitan.org

Check out the source on GitHub: github.com/lowRISC/opentitan

Features

1. Independently managed
   OpenTitan is stewarded by lowRISC, a not-for-profit company that uses collaborative engineering to develop and maintain open source silicon designs and tools for the long term.
2. Open source
   OpenTitan is an open source project with technical contributors from leading not-for-profit, academic, and commercial organizations.
3. Security through transparency
   As an open source project, OpenTitan enables the larger community to proactively audit, evaluate, and improve the security properties of the design.
4. High-quality IP from experienced teams
   OpenTitan is developed by engineers and researchers from ETH Zürich, G+D Mobile Security, Google, lowRISC, Nuvoton Technology, and Western Digital. Our community brings ideas and expertise from a variety of perspectives.
5. Modern architecture
   OpenTitan is designed to serve as the system root of trust by actively mediating access to the first-stage boot firmware. It is built upon the quality constructs and security principles used to create Google's Titan chips.
6. Vendor- and platform-agnostic
   Because it is not proprietary to a specific vendor or platform, OpenTitan can be integrated with data center servers, peripherals, storage devices, and other hardware, helping reduce deployment costs.

OpenTitan is administered by lowRISC.
Find out more at www.opentitan.org