RISC-V

ROOT-OF-TRUST SOLUTIONS

Trust is the value that makes our digital life secure. Semiconductors are the cells that fuel this life.

Because the reputation, the business and the success of service providers and device makers are at stake, they must be confident that their applications execute as intended, cannot be spied on, copied or altered. They also must be confident that their sensitive data cannot be extracted, modified, or intercepted, and their identity cannot be tampered with. Hence, there comes the need for hardware root-of-trust.

Security must be outlined at the start and be correct by design.

While modern cryptography is the pillar of digital security, equipping a microcontroller or a complex SoC to resist all inherent threats is yet another dimension involving rigorously architected layers of protections utilizing proven technologies.

Inside Secure Root-of-Trust

Inside Secure Root-of-Trust is a comprehensive platform security solution which protects the SoC, its identity, its secrets, its integrity and its operations. In the SoC, Inside Secure Root-of-Trust is the vault that guards your assets, a vault locked from the inside. The solution provides the hardware trust anchor, the cryptographic functions, the key management and derivation services, the APIs and the signing tool to secure the SoC and the ecosystem it belongs to.

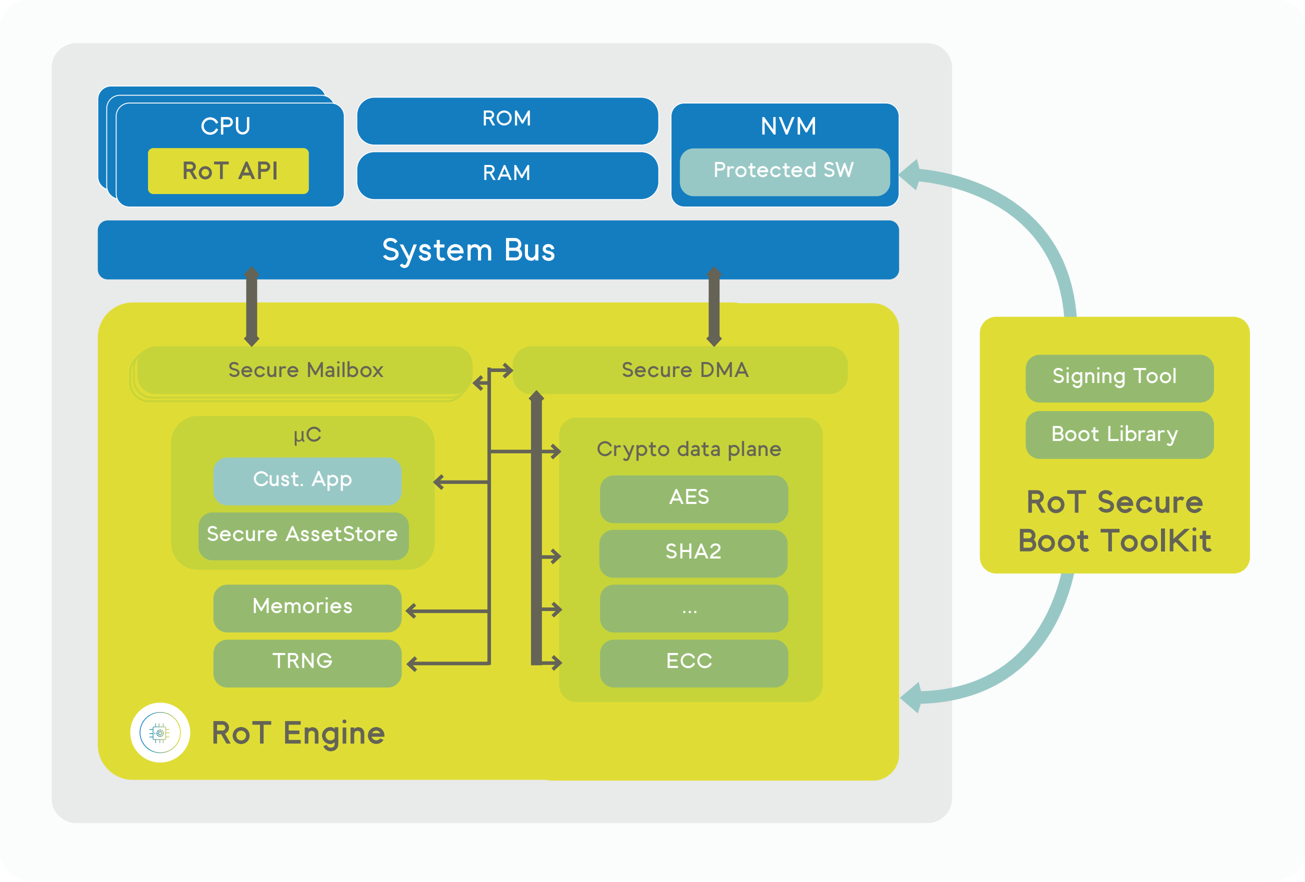
It provides the device with the capability to **securely boot, manage software update, execute software, control debug enablement, protect data, be authenticated, authenticate third parties and communicate**. The Root-of-Trust Engine is the ideal component to create an embedded HSM for IoT, automotive, datacenter and governmental applications within an optimized silicon footprint and power envelope.

Inside Secure Silicon IPs

With more than 500 available configurations, **Inside Secure Silicon IP** is the largest silicon-proven security IP portfolio. Embedded in billions of devices spanning a wild range of applications such as High Speed Networking, Internet of Things, Automotive or Content Protection. Inside Secure Silicon IPs shorten time-to-market while reducing design cost.

INSIDE SECURE ROOT-OF-TRUST ENGINE AND PROGRAMMABLE ROOT-OF-TRUST ENGINE

Inside Secure Root-of-Trust Engine provides a rich set of symmetric, asymmetric, hashing and true random number generation (TRNG) services to the OS and applications running on the SoC. Its Secure Asset Store controls the use of keys and enforces authorization policies by identifying service requesters through a combination of hardware signaling and software identity. It gives developers peace of mind that secret data can never be visible to the OS or applications and that sensitive assets can never be extracted off-chip.



Inside Secure Programmable Root-of-Trust features a RISC-V 32-bit CPU and is delivered with its application development framework. It effectively enables developers to extend or customize the Secure Asset Store, the cryptographic algorithms or implement a custom key ladder. Embedded in the SoC, it hosts the platform most sensitive applications such as software update or provisioning components and it further secures TLS communications with the cloud.

The Programmable Engine can also authenticate the images and controls the boot of application CPUs to establish a chain of trust in the SoC.

Inside Secure Root-of-Trust Secure Boot Toolkit provides developers with the essential components for securing the SoC boot sequence. The signing tool formats and adds protection layers to the executables to ensure their integrity, authenticity and confidentiality. It ultimately generates the protected images. Developers integrate the Boot Library into the SoC boot loader, optionally adding anti-cloning and anti-rollback protections.

Differentiate through security; reduce your time to market.

Inside Secure Root-of-Trust Engine is the first FIPS-140-2 level 2 validated silicon IP (certificate #2272 – registered as VaultIP) that tightly combines a rich set of cryptographic services together with a Secure Asset Store within a clearly identifiable physical entity that minimizes the attack surface. Inside Secure customers can apply for incremental re-validation of their chip. While full FIPS-140-2 Level 2 validation typically takes a year to achieve, revalidation using the initial validation as a base allows for process efficiencies by both the laboratory and NIST and significantly reduces the time and cost.

BUILT-IN PROVISIONING AND DEVICE LIFECYCLE

Securing devices requires SoCs to be provisioned with assets such as unique identifiers, keys or certificates. This can be achieved at various stages in the device lifecycle: during the chip manufacturing, the device integration or in the field, and may be a multi-stop process. **Inside Secure Root-of-Trust Engine** provides built-in capabilities that facilitates the implementation of a secure provisioning scheme with policies configurable based on the device lifecycle.

While Consumer IoT, automotive, data centers, smart metering and other applications have all different set of requirements and because one size does not fit all, **Inside Secure Root-of-Trust Engine** is available in a wide range of configurations allowing for size-feature-performance trade-offs.

For instance, Chacha20 and Poly1305 support can be added on top of the commonly used AES and SHA2 algorithms. Bus interfaces can also be inter-changed for a smooth integration into the SoC architecture.

* TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

LAYERED DEFENSES

Beyond software attacks, connected devices may be subject to side channel attacks that exploit the power or electromagnetic signature generated by the **cryptographic operations** to extract key values. Furthermore, semi-invasive or invasive attacks can attempt to compromise the device behavior and secrets.

LICENSED
DPA
COUNTERMEASURES
TM

Inside Secure Root-of-Trust Engine optionally implements additional protection to defend against these classes of attacks. Inside Secure protected cryptographic engines are equipped with proven countermeasures that defeat side channel attacks.

Inside Secure Root-of-Trust Engine also optionally provides fault detection along with a configurable anti-tampering manager that implements the response policies.

Inside Secure Security Assessment Laboratory

Inside Secure Security Assessment Laboratory tests and evaluates secure hardware and software products capable of meeting the most demanding security standards such as FIPS-140-2 or Common Criteria (EAL5+). Inside Secure products use a range of advanced techniques to implement protection against a **wide range of threats** such as side channel leakage, reverse engineering, fault injection, and invasive attacks.

Security testing is a critical step to verify the implementation of these technologies and ensure that end products reach the required level of security protection. In some domains, evaluation of solutions is mandated to be carried out by **independent evaluation labs**. Over and above this, the Inside Secure Security Lab carries out a range of internal security testing to assess the security of our solutions, strengthen our products and accelerate our customers' time to market.

For further details on all of Inside's security solutions, visit www.insidesecure.com

Information in this document is not intended to be legally binding. Inside Secure products are sold subject to Inside Secure Terms & Conditions of Sale or the provisions of any agreements entered into and executed by Inside Secure and the customer. *The products described herein may be protected by one or more of the patents and/or patent applications listed in related datasheets, such document being available on request under specific conditions. Additional patents or patent applications may also apply depending on geographic regions.*