Securing Tomorrow's World: The Evolution of Hardware Root of Trust Security IP

Author

Frank Malloy
Marketing, Senior Director

Introduction

With the advent of AI, datacenter, high-performance computing (HPC), IoT, consumer, and automotive designs, security has become increasingly important. The need to protect sensitive data, systems, and operations from cyberattacks resulting in breaches, unauthorized access, theft, and other malicious activities has moved to the forefront.

In an increasingly connected world with devices ranging from computers and smartphones to IoT devices and advanced vehicles, a strong security foundation is critical for protection against various cyberthreats.

So, how do we keep our hardware and software systems secure from threats and attacks?

Security IP consists of specialized, dedicated hardware and software embedded in chip designs to ensure data integrity, confidentiality, and authentication. Security IP protects the intellectual property of chip manufacturers as well as enhancing the overall security of chips, including user/supplier data protection (e.g. AI models loaded onto the chip, end-user data processed by the chip, etc.), in applications ranging from consumer electronics to automotive systems to AI and HPC datacenters. In prioritizing IP security, designers mitigate potential risks, while maintaining competitive advantages, when building trust in their products within a rapidly evolving technological landscape.

The Root of Trust

A security IP Root of Trust (RoT) is a key foundational hardware component embedded within a chip that serves as the cornerstone for establishing trust in a system's security. The Root of Trust is responsible for ensuring that the system functions in a secure state, even in the presence of potential security threats.

The key benefits of the Root of Trust are to:

- Prevent unauthorized access
- Prevent IP theft
- Protect sensitive information
- Provide authentication towards other systems
- Protect integrity of software running on the device

The Root of Trust is designed to perform critical security functions to achieve the above benefits, including:

- **Secure boot.** Ensures a system's startup process is using trusted and verified firmware. It prevents malicious code from being executed.
- **Secure storage.** Creates a secure, protected area for storing critical and sensitive data. This includes cryptographic keys, credentials, and configuration settings.
- **Authentication and key management.** Verifies devices, software components, and users' identities. Critical to prevent unauthorized access and ensure that identities have not been compromised.
- **Cryptography.** Provides a secure environment for executing cryptographic operations such as encryption, decryption and the generation and verification of digital signatures.
- **Lifecycle Management.** Managing and provisioning of the product over its lifecycle (images, keys, etc.)
- **Side-Channel Countermeasures.** Countermeasures to prevent, eliminate or reduce information leakage that could be used by an attacker to compromise a system or device.
- **Host Processor Support.** Support for multiple hosts to securely offload security functions or acceleration of cryptographic operations.

A Root of Trust must be secure by design, as it is a fundamental security IP component which is inherently trusted and serves as the basis for all other security operations. It must be tamper-resistant to protect against malicious physical attacks, which are increasing and becoming more sophisticated.

The Ever-Changing Security Landscape

As the world becomes more increasingly connected and always-on, the threat of security attacks on everything from personal devices to data centers, to AI neural networks are increasing in both frequency and complexity.

In addition to the increase and sophistication of cyberattacks, the fast-changing hardware and software landscape demands ongoing modernization of security IP, most importantly the critical Root of Trust. Landscape changes include both growing and differing markets—each with its own security standards, protocols, and needs. In addition, different regions of the world each require different security standards or certificates.

Governments are increasingly advocating for a "security root of trust" in electronic devices to enhance cybersecurity and protect critical infrastructure, businesses, and individuals. Besides providing baseline security and mitigating cyberthreats, new regulations and standards (such as those in the EU and US) increasingly require strong device security to protect citizens' data and national interests. Many sectors, such as energy, healthcare, and transportation, rely on electronic devices. A compromised device in these sectors could have severe consequences. By ensuring devices are secure from the hardware up, governments aim to protect personal data and build consumer confidence in digital products and services.

As security and Root of Trust advances, many regions and markets have adopted their own standards and certification processes to validate the security of electronic devices and their root of trust implementations. Below is an example summary of markets and their respective certification standards and focus areas:

Market	Certification Body/Standard	Focus Area
International	Common Criteria (ISO/IEC 15408)	IT product security (multiple levels)
USA	NIST (FIPS 140-3), NIAP	Cryprography, general IT security
EU	EUCC, ENISA, DSI	Cybersecurity, trusted computing
UK	NCSC, CPA	Hardware/software product security
China	OSCCA	Cryptographic products
Japan	IPA	Common Criteria evaluation
Singapore	CSA	Local cybersecurity certification

As a result of these technological advancements and new challenges, the architecture of the Root of Trust must evolve.
Early implementations of Root of Trust were acting as a subordinate peripheral, responding to commands from the main processor (CPU or SoC). The host system controls when and how the Root of Trust is used. In this mode, The Root of Trust can only act when asked; it cannot initiate actions or enforce security policies independently.

Next generation Root of Trust implementations evolve from a subordinate architecture to a more active “master” or autonomous security controller, which can operate independently of the main processor, and monitor, enforce, and initiate security events proactively.

Collectively, this evolution in the fast-moving security landscape demands a call to action to advance.

The Synopsys Modern, Evolving Root of Trust Solution

The Synopsys tRoot™ Fx Hardware Secure Modules (HSMs) are now in the 5th generation, evolving to meet the latest demands for secure hardware. Examples of newly added functionality include:

- **From firmware-based to more custom solutions:** tRoot customers can easily develop their own RoT firmware with help from the pre-packaged security libraries, which are provided as source code. This allows engineers to create the best hardware/firmware configuration considering the desired power, performance, area, and security level for their specific SoC needs, instead of a one-size-fits-all approach or a limited hardware solution space.
- **From a cryptographic accelerator to a trusted services off-load engine:** Where early versions of Root of Trust implementations were merely focused on offloading cryptographic operations to hardware, tRoot has evolved to become a much broader solution. Providing device makers with an enhanced software development kit (eSDK) and the ability to extend available solutions with their own embedded software on the programmable RoT. The eSDK provides higher-level security functionality such as key management, secure crypto, Crypto Manager, secure boot, secure access, secure debug, and private and shared secure storage.
- **From hosted (companion engine) to standalone (manager engine) with subordinate functionality:** With this enhanced capability, tRoot HSMs support multiple SoC scenarios. tRoot supports ROM-based host processors that boot first, then start the HSM and request secure boot or secure cryptographic functionality. tRoot HSMs also supports ROM-less host processor designs where the HSM will boot first and then provides a verified boot and/or application image for the host processor(s). Carrying flexibility further, tRoot HSM can provide full ROM-less solutions where no ROM on the SoC is required, as tRoot HSM can securely boots directly from embedded or external off-chip NVM.
- **From a packet encrypt/decrypt engine into a key manager for inline engines like (LP)DDR, Ethernet, PCIe, CXL, UAlink, UCIe, etc.:** HSMs provide packet based crypto engines, but with the latest interface performance requirements, inline crypto engines are required close to the interface engines. The role of HSMs changed for those interfaces into a key manager with key transport functionality. In this scenario, managing means: generation, provisioning, storage, policy validation, providing keys to the inline crypto engines, and revoking keys—all part of lifecycle management.

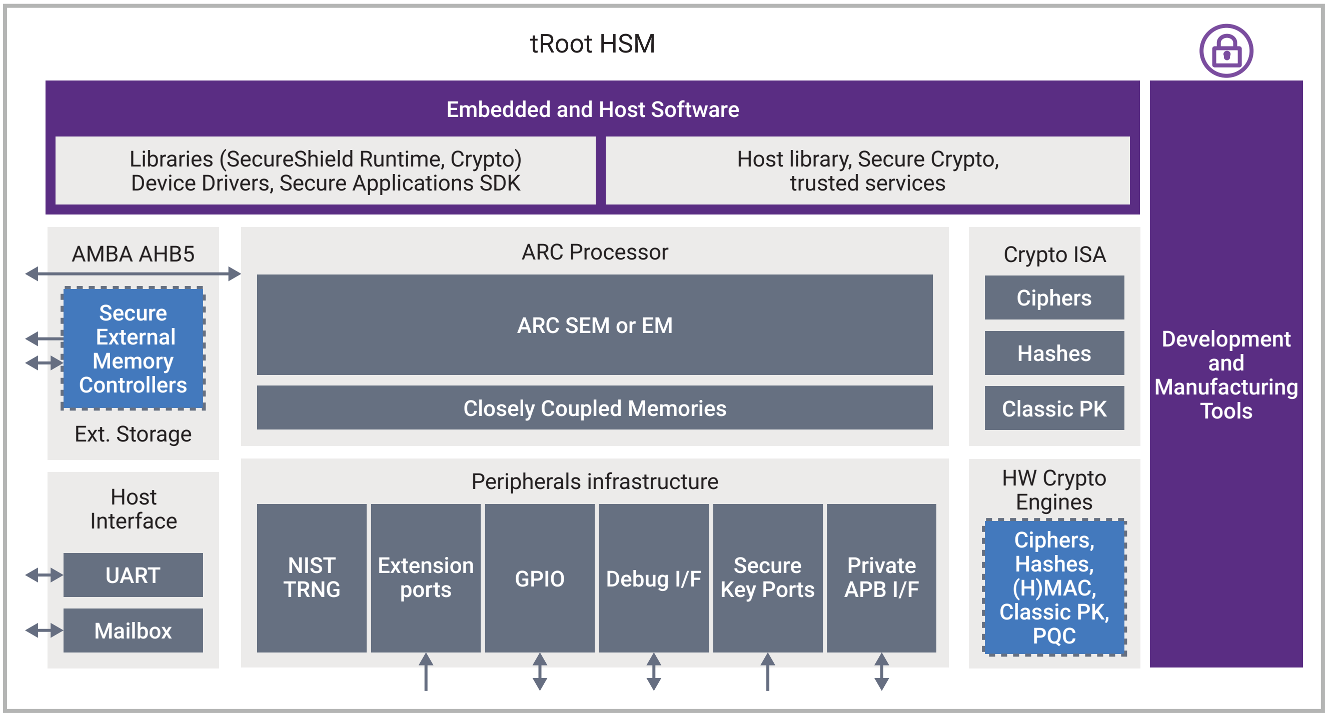
tRoot HSM
Embedded and Host Software
Libraries (SecureShield Runtime, Crypto) Device Drivers, Secure Applications SDK
Host library, Secure Crypto, trusted services
AMBA AHB5
Secure External Memory Controllers
Ext. Storage
ARC Processor
ARC SEM or EM
Closely Coupled Memories
Crypto ISA
Ciphers
Hashes
Classic PK
Development and Manufacturing Tools
Host Interface
UART
Mailbox
Peripherals infrastructure
NIST TRNG
Extension ports
GPIO
Debug I/F
Secure Key Ports
Private APB I/F
HW Crypto Engines
Ciphers, Hashes, (H)MAC, Classic PK, PQC

Figure 1: Synopsys tRoot™ Fx HSM High-Level Diagram

PQC-Based Cryptography

Cryptography is a fundamental and critical capability for a root of trust solution. RSA and Elliptic Curve Crypto (ECC) are widely used algorithms for securing digital communications, authentication, and establishing trust (e.g., in root of trust solutions). Their security relies on mathematical problems (integer factorization for RSA, discrete logarithm for ECC) that are currently infeasible for classical computers to solve in a reasonable time. Quantum computers, when sufficiently advanced, could use algorithms like Shor's algorithm to efficiently solve these problems, rendering RSA and ECC insecure. This means encrypted data (when shared secret keys have been agreed using RSA or ECC based communication algorithms), digital signatures, and certificates could be compromised if intercepted and decrypted by future quantum computers.

The Synopsys tRoot solution employs post-quantum cryptography (PQC) algorithms designed to be secure against attacks from both classical and quantum computers. Through a hybrid approach of combining classic and PQC algorithms, tRoot maintains compatibility with today's cryptography and remains secure when quantum computers become available, providing a future-proof solution.

Scalable performance

The tRoot HSM family offers a well-defined security boundary for a complete, drop-in security solution with extensibility and flexibility that enable designers to tune the HSM to their exact requirements with the most efficient combination of security, power, area and performance. In configurations where dedicated cryptographic accelerators are available, they will be used because of their speed and security advantages. In implementations that are area critical, gate count can be reduced by choosing a configuration without dedicated crypto accelerators and use of software implementations with or without Crypto ISA support. This scalability of tRoot is unique in the market and provides hybrid solutions in between the full hardware and the full software approach that make use of instruction set extensions of the embedded secure processor.

NVM-Based Boot Support

A device's boot process typically begins by executing code directly from Read-Only Memory (ROM). ROM is typically immutable after manufacturing—its contents cannot be changed or updated. Because of this, it is a highly secure and tamper-resistant foundation for the root of trust. However, if vulnerabilities or bugs are discovered, the ROM code cannot be patched or updated.

The 5th generation tRoot implements a non-volatile memory (NVM) boot using eXecute in place (XIP) technology. NVM can be updated post-manufacturing, allowing code and data to be changed as needed. Security patches, feature upgrades, and bug fixes can be applied to NVM, enhancing device lifecycle management.

SoC Plug and Play

tRoot HSMs are designed to easily integrate into SoCs and provide robust hardware-enforced protection while maintaining a high level of performance through cryptographic acceleration. They provide a Trusted Execution Environment (TEE) to protect sensitive information and processing, and implement security-critical functions such as secure boot, storage, debug, anti-tampering and key management required throughout the device's lifecycle.

The Synopsys tRoot HSMs provide SoCs with a unique identity that cannot be tampered with and extends the trust of that identity to other internal and external entities in the SoC, with security functions in a trusted environment but also as a companion to a host processor.

The Secure Instruction and Data Controllers provide protected access and runtime tamper detection in non-secure (embedded or off-chip) memories for code and data privacy protection without the need for a dedicated secure memory. In addition, they reduce system complexity and cost by allowing tRoot's firmware to reside in any non-secure memory space.

Scalability

tRoot's unique architecture can effectively adapt to future security requirements and standards as it utilizes multiple scalable extension interfaces both in hardware and software.

These complete, standalone products and capabilities provide a secure hardware enclave with firmware components and tools, allowing designers to quickly configure and integrate a security solution without requiring the expertise to write security software.

Summary

We are in an era of pervasive intelligence. With the rise of the number and types of interconnected devices, from smartphones and laptops to datacenter servers, AI/ML chips, IoT devices, autonomous vehicles, and medical devices, the vulnerability to cyberattacks and threats is greater than ever, creating new opportunities for cybercriminals to exploit hardware vulnerabilities.

This evolution of interconnected, always-on devices demands that security IP—especially Root of Trust—evolve to meet ever-changing and advancing security requirements.

The 5th generation of Synopsys tRoot Hardware Secure Modules meet these major demands with an evolving, modern, and scalable solution.