SYNOPSYS®
Silicon to Software™

DesignWare tRoot Secure Hardware Root of Trust

Highlights

- Secure identification and authentication
- Secure communication
- Secure provisioning, storage and management of keys and other secrets
  - Hardware protected Device Unique Key and Platform Key – not accessible by trusted software
- Enables secure services deployment
- Secure in-field firmware updates
- Personalization
- Brand integrity protection
- Power management
- Secure boot
- Run-time integrity protection
- Anti-tampering anti-cloning. IP protection.
- Secure debug and testing
- Cryptographic cores and co-processors with virtualization support
- AMBA® AXI®/AHB® interfaces

Applications

- Embedded security
- Device identity
- Consumer electronics
- Industrial control
- Healthcare equipment
- Automotive
- Digital home
- Content protection

Overview

The highly secure DesignWare® tRoot™ Secure Hardware Root of Trust enables connected devices to securely and uniquely identify and authenticate themselves to create secure channels for remote device management and service deployment. tRoot's advanced design addresses complex threats by protecting the device and its data at boot time, run time and during the communication with other devices or the cloud. tRoot consistently addresses security throughout the device's lifecycle and it enables SoC designers with the most efficient combination of power, size and performance.

tRoot Secure Hardware Root of Trust

Synopsys' tRoot is a Secure Hardware Root of Trust that is suitable for consumer electronics and a variety of applications including the Internet of Things (IoT). tRoot provides the foundation of trust and security-critical functions required to identify, authenticate and protect connected devices and their communication with other devices against threats, and to enable new business opportunities through service deployment.

Depending on the application, tRoot can act as a slave (e.g. controlled by a host in a system), or as a master (e.g. operate in standalone mode).

Secure Boot, a primary security capability of tRoot, is used to bring up a device into a secure state and ensure that it runs only trusted firmware. For the secure boot process, tRoot can act as the master boot controller or as a peripheral for a host-driven secure boot where tRoot verifies host processor code base. By design, the secure code that runs in tRoot is run-time verifiable and therefore trusted.

For the host-driven secure boot case, when the device is first powered, tRoot uses secure code to verify the authenticity and integrity of the code base that will run on the host processor.

Upon successful authentication tRoot passes control to the system to continue with the boot process. Once the program memory has been established, tRoot continuously verifies the code base in the background.

Secure storage provides protection for the device's application data. tRoot provides a secure path to encrypt and decrypt the application data, preventing attackers from reading or modifying it. With this feature, data sets can only be decrypted on the local device (e.g. data sets are securely bound to the device and are protected by tRoot's internally generated keys).

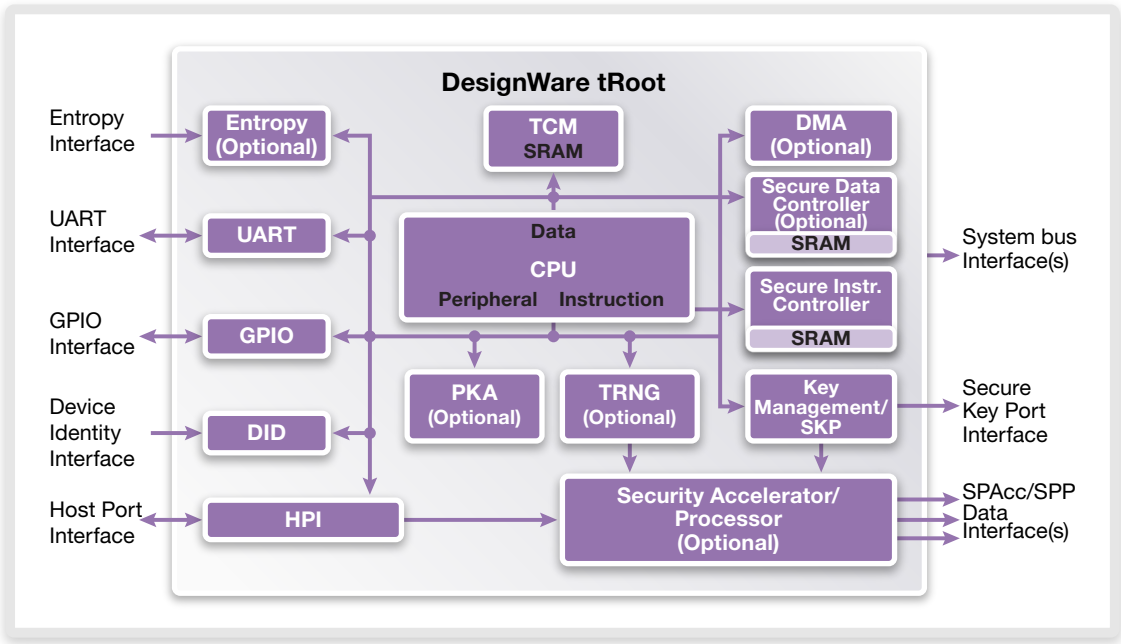

Figure 1: DesignWare tRoot Block Diagram

Device authentication is essential to ensure that one or more of the upstream and/or downstream devices communicating with the target device can be trusted. To ensure this trust, a mutually agreed upon authentication scheme is required. Synopsys' tRoot can ensure the integrity of various authentication protocols as well as ensure the confidentiality of shared secrets between devices.

Synopsys' tRoot can be implemented in a system without the need to lock memory resources as it can share memory resource already available in the system. Its unique architecture has the ability to effectively adjust to future security requirements and standards, and enable personalization of features, services and environments to create business growth and monetization in many markets, including the exploding IoT market. tRoot supports a whole range of additional features, from remote device and feature activation, secure key provisioning and management to secure communication, and secure in-field firmware updates.

tRoot Deliverables

- Synthesizable RTL
- Binary FW image(s)
- Configuration tools
- Host application library
- Verilog integration testbench and test vectors
- Integration test image(s)
- Sample simulation script
- Sample synthesis scripts and constraints captured in SDC format
- Documentation (hardware and system integration guides, software APIs)

About DesignWare IP

Synopsys is a leading provider of high-quality, silicon-proven IP solutions for SoC designs. The broad DesignWare IP portfolio includes logic libraries, embedded memories, embedded test, analog IP, wired interface IP, wireless interface IP, security IP, embedded processors, and subsystems. To accelerate prototyping, software development and integration of IP into SoCs, Synopsys' IP Accelerated initiative offers IP Prototyping Kits, IP Virtual Development Kits and IP subsystems. Synopsys' extensive investment in IP quality, comprehensive technical support and robust IP development methodology enables designers to reduce integration risk and accelerate time-to-market.

For more information on DesignWare IP, visit http://www.synopsys.com/designware. Follow us on Twitter at http://twitter.com/designware_ip.

SYNOPSYS®
Silicon to Software™

Synopsys, Inc. • 690 East Middlefield Road • Mountain View, CA 94043 • www.synopsys.com

11/15.rd.CS6721.