Cisco Trustworthy Technologies Data Sheet

Product Overview

Trustworthy solutions encompass Cisco's commitment to deliver products and solutions with multilayered security that protect against today's threats. Trustworthy technologies provide a foundation of security and resilience across Cisco's solutions portfolio. Trustworthy technologies such as image signing, secure boot, Cisco Trust Anchor module (TAm), and runtime defenses help ensure that the code running on Cisco hardware platforms is authentic, unmodified, and operating as intended. A hardware-level root of trust, unique device identity, and validation of all levels of software during startup establish a chain of trust for the system.

How Do Trustworthy Technologies Enhance the Security of Cisco Solutions?

Today's sophisticated cyberattacks increasingly seek to compromise the network infrastructure by attacking devices like routers and switches. By doing so, attackers can eavesdrop on sensitive communications, steal or manipulate data, and launch attacks against other parts of the network. This includes advanced persistent threats that modify the hardware or software of network devices. These threats can go unnoticed for months, or even years, inflicting devastating damage.

Cisco trustworthy technologies provide product assurance functionality as well as foundational security capabilities which enhance the security and resilience of Cisco solutions. To protect against device counterfeiting and malicious attacks on hardware and software, Cisco uses digitally-signed software images, hardware-anchored secure boot, Secure Unique Device Identifier (SUDI), and other trustworthy technologies to verify the authenticity and integrity of our solutions. Among other functions, trustworthy technologies run automated checks of hardware and software integrity and can shut down the boot process if compromise is detected. Cisco Trust Anchor module provides a Secure Unique Device Identifier, highly secure storage, a random bit generator, and secure key management. These added layers of security protect against counterfeit and software modification; enable secure, encrypted communications; and verify that Cisco network devices are operating as intended.

Why should you choose Cisco?

Cisco is deeply committed to security. Cisco trustworthy solutions start with security-focused development processes and standards-based technology and add security features which provide secure, resilient networking solutions. These security capabilities perform both system-critical functions and security functions, including proactive monitoring of the startup process.

Cisco works to continually enhance the security and resilience of our solutions. Verification of the authenticity and integrity of Cisco hardware and software platforms with trustworthy technologies such as secure boot of signed images and Trust Anchor module reduces risk and helps protect against today's threats.

Cisco has a dedicated team of engineers and security managers who work with Cisco product development teams to embed security across Cisco product lines. And Cisco uses the security expertise that we've gained defending our own global enterprise network to continually enhance the security of our business and our solutions.

Fundamental Concepts of Cisco Trustworthy Technologies

Image signing: Image signing is a two-step process for creating a unique digital signature for a given block of code. First, a hashing algorithm, similar to a checksum, is used to compute a hash value of the block of code. The hash is then encrypted with a Cisco private key, resulting in a digital signature that is attached to and delivered with the image. Signed images may be checked at runtime to verify that the software has not been modified.

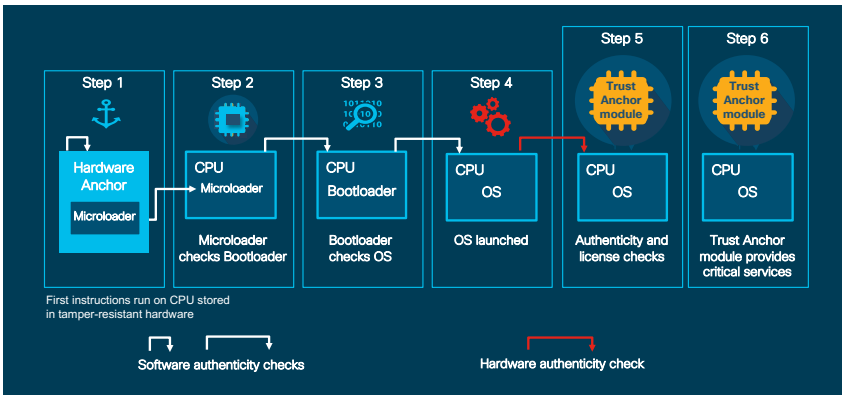
Secure boot: Cisco Secure Boot helps to ensure that the code that executes on Cisco hardware platforms is authentic and unmodified. Cisco hardware-anchored secure boot protects the microloader (the first piece of code that boots) in tamper-resistant hardware, establishing a root of trust that helps prevent Cisco network devices from executing tainted network software.

Chain of trust: A chain of trust exists when the integrity of each element of code on a system is validated before that piece of code is allowed to run. A chain of trust starts with a root of trust element. The root of trust validates the next element in the chain (usually firmware) before it is allowed to start, and so on. Through the use of signing and trusted elements, a chain of trust can be created which boots the system securely and validates the integrity of Cisco software. See Figure 1.

Trust Anchor module (TAm): This proprietary, tamper-resistant chip is found in many Cisco products and features nonvolatile secure storage, Secure Unique Device Identifier, and crypto services, including random number generation (RNG), secure storage, key management, and crypto services to the running OS and applications.

Runtime defenses (RTD): Runtime defenses target injection attacks of malicious code into running software. Cisco runtime defenses include Address Space Layout Randomization (ASLR), Built-in Object Size Checking (BOSC), and X-space. Runtime defenses are complementary.

Figure 1. Hardware-Anchored Secure Boot and TAm Verify Hardware and Software Integrity



Common Questions

How do I know that my hardware and software are genuine Cisco and that my system software has not been modified before or during boot up?

Trustworthy technologies give customers the confidence that the product is genuine Cisco. Cisco Secure Boot protects the boot code in hardware and uses a check of digitally-signed images to verify that only genuine, unmodified code boots on a Cisco device. The SUDI in the Trust Anchor module provides verification that the hardware is genuine Cisco.

How do you know that your device has implemented Cisco's trustworthy technologies?

Trustworthy technologies are available today in many Cisco solutions. Our product teams design security technologies into their products based on the use case of the device. These capabilities are available in many Cisco routing, switching, wireless, server, and security products today, and we are designing them into additional platforms. We constantly review and adapt Cisco product security requirements as the threat landscape evolves. Cisco is committed to advanced security research and continues to innovate and develop new trustworthy technologies, which we implement as they become available. Please contact your account manager or sales engineer for your device's security profile.

What's the risk of not implementing Cisco trustworthy technologies?

The lack of a hardware-anchored root of trust has resulted in known hacks. Third parties can tamper with BIOS, boot loader, or ROM monitor (ROMMON) boot code to load modified software images; bypass hardware, authenticity, and licensing checks; or perform additional functions with malicious intent. Tampered code can also result in data manipulation, data theft, and can provide a platform to launch attacks, including denial of service (DoS). Cisco trustworthy technologies help close these potential security gaps.

Cisco also works with our suppliers as well as our manufacturing and distribution partners to address supply chain risks through our Value Chain Security program. This program takes a multi-layered approach to security that uses physical security practices, logical security processes, and security technology to address taint, counterfeit, and misuse of intellectual property. Our comprehensive program continually assesses, monitors, and improves security across the entire lifecycle of our solutions. We consistently strive to enhance security and earn the trust of our customers.

Immutable Identity—SUDI

The Secure Unique Device Identifier, or SUDI, is an X.509v3 certificate which maintains the product identifier and serial number. The identity is implemented at manufacturing and is chained to a publicly identifiable root certificate authority. The SUDI can be used as an unchangeable identity for configuration, security, auditing, and management.

The SUDI credential in the Trust Anchor module can be either RSA or Elliptic Curve Digital Signature Algorithm (ECDSA) based. The SUDI certificate, the associated key pair, and its entire certificate chain are stored in the tamper-resistant Trust Anchor module chip. Furthermore, the key pair is cryptographically-bound to a specific Trust Anchor chip and the private key is never exported. This feature makes cloning or spoofing the identity information virtually impossible.

Data-at-Rest Encryption and Decryption Functions Using Secure Keys

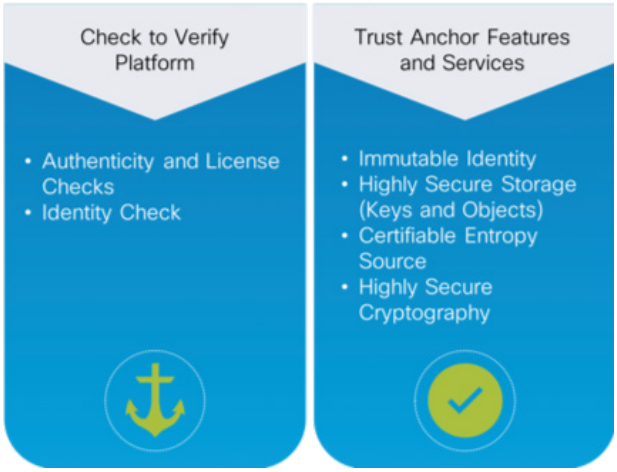
The Cisco Trust Anchor can also generate key pairs that can be used for customer-controlled certificates commonly called locally significant certificates (LSCs or local device identity (LDevID) certificates.

Customer identity functions supported by the Trust Anchor include:

- Retrieval of LDevID RSA public keys
- Authentication with a Certificate Authority (CA) before LSC enrollment
- Zero-touch provisioning authentication
- Secure boot posture assessment

The SUDI can be used for asymmetric key operations such as encryption, decryption, signing, and verifying that allow passage of the data to be operated upon. This capability makes remote authentication of a device possible. It enables accurate, consistent, and electronic identification of Cisco products for asset management, provisioning, version visibility, service entitlement, quality feedback, and inventory management. (See Figure 2.)

Figure 2. SUDI Immutable Device Identity



Highly Secure Storage

The Cisco Trust Anchor module provides highly secure storage for keys, passwords, customer credentials, and other critical security information for the device. One of its advantages is the ability to store private encryption keys and passwords for even greater security. Allocating secure storage outside the Trust Anchor module is also possible.

Random Number Generation and Entropy Source

Strong random number generation (RNG) is at the core of encryption, while weak RNG can undermine the entire encryption system. Random number generators play a key role in creating cryptographic keys, in establishing highly secure communications between users and websites, and in resetting passwords for email accounts. Without assured randomness, an attacker can predict what the system will generate and undermine the algorithm. The Cisco Trust Anchor module is compliant with NIST specifications and provides a NIST SP 800-90A and B certifiable RNG that extracts entropy from a true random source within the Trust Anchor.

Feature	Description	Benefits
Trustworthy technologies	An evolving range of security technologies designed into Cisco Networking devices that protect against counterfeit and software modification and verify that Cisco products are operating as intended. Trustworthy technologies include image signing, secure boot, and runtime defenses in addition to security capabilities in the Trust Anchor module such as Random Number Generation (RNG) and crypto support, secure storage, and Secure Unique Device Identifier (SUDI).	• Verifies that hardware is genuine Cisco • Protects against counterfeit and software modification • Supports secure, encrypted communications • Helps to enable device authentication and zero-touch provisioning, reduces to deployment costs
Image signing	Image signing is a two-step process for creating a unique digital signature for a given block of code. First, a hashing algorithm, similar to a checksum, is used to compute a hash value of the block of code. The hash is then encrypted with a Cisco private key, resulting in a digital signature that is attached to and delivered with the image. Signed images may be checked at runtime to verify that the software has not been modified.	Cryptographically signed images: • Help ensure that the firmware, Basic Input Output System (BIOS), and other software are authentic and unmodified • Provided a critical check so only genuine, unmodified software can boot on a Cisco device • Effectively mitigate persistent attacks
Secure boot	Cisco Secure Boot helps to ensure that the code that executes on Cisco hardware platforms is authentic and unmodified. Cisco hardware-anchored secure boot protects the microloader (the first piece of code that boots) in tamper-resistant hardware, establishing a root of trust that helps prevent Cisco network devices from executing tainted network software.	• Automated check of software integrity at boot-up • Monitors the startup process and can shut down the boot process if it detects a compromise • Helps to ensure that only genuine, unmodified software boots on a Cisco platform
Trust Anchor module (TAm)	This proprietary, tamper-resistant chip is found in many Cisco products and features non-volatile secure storage, SUDI, and crypto services, including RNG, key store, and crypto engine.	• X.509 SUDI certificate installed at manufacturing provides a unique device identity • SUDI helps to enable anti-counterfeit checks, along with authentication and remote provisioning • Secure, on-board storage • RNG/crypto services support secure communications
Hardware authenticity check	A process that uses the X.509 SUDI certificate installed in the Trust Anchor module to verify that Cisco hardware is authentic (manufactured by Cisco). The hardware authenticity check runs only after the secure boot process has been completed and the software has been verified to be trusted.	• Verifies hardware authenticity • Protects against counterfeit
Runtime defenses	Runtime defenses target injection attacks of malicious code into running software, Cisco runtime defenses include Address Space Layout Randomization (ASLR), Built-in Object Size Checking (BOSC), and X-space Runtime defenses are complementary.	• Makes it harder or impossible for attackers to exploit vulnerabilities in running software • Runtime defenses are complementary; you can implement these individually or deploy several runtime defenses together