Using Infineon OPTIGA™ TPM hardware and Mocana TrustPoint™ software for secured network equipment

By Steve Hanna, Senior Principal, Digital Security Solutions at Infineon Technologies and Dean Weber, CTO at Mocana

www.infineon.com

Contents

Abstract

Computers, servers and the people that operate them used to be the primary target of attackers. Today, because of increasing connectivity and dependence on networks, network equipment has become a frequent target for cyberattacks. As a result, unprotected routers, switches, firewalls, gateways and wireless access points provide a target for attackers.

The Trusted Computing Group's (TCG's) open document, "Guidance for Securing Network Equipment Using TCG Technology" describes how architects and designers can secure this equipment [1]. While the TCG documents provide the theory, additional effort is required to implement this protection. Using the techniques described in TCG documents, Infineon's OPTIGA™ Trusted Platform Module (TPM) hardware and Mocana TrustPoint™ software can provide enhanced security to protect network equipment. This white paper describes the next steps to implement the trust and security required for today's commercial, industrial and government networks.

Standards for trust

The Trusted Computing Group, an organization consisting of computing, networking, software and other security experts, has been developing open standards for nearly two decades. The foundation for the initial standards was based on a hardware element called a Trusted Platform Module (TPM). The TPM provides a hardware-based root of trust that is far more resistant to attacks than software-only approaches. Today, with the most recent TPM 2.0 specification, a TPM can take as many as five different forms but the most common form is a special-purpose hardware security chip.

TPMs and network equipment

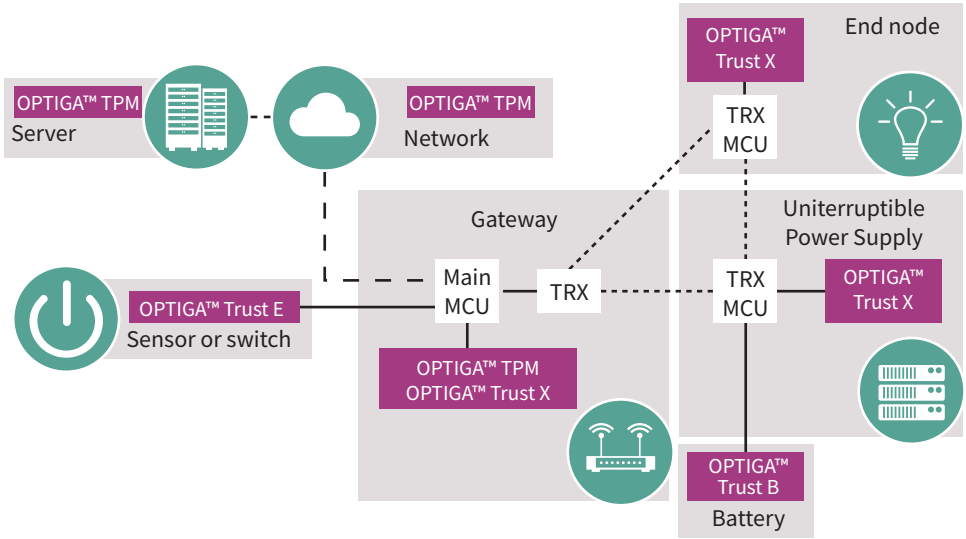
Released in 2016, TCG's TPM 2.0 has become an international standard (ISO/IEC 11889). Leading semiconductor suppliers, like Infineon, offer TPMs that conform to the TCG specification, so manufacturers and users can implement this trust in computers, storage equipment (self-encrypting drives), cloud services and networks - including network equipment. All TPMs support the same basic set of commands but there are subtle, and not so subtle, differences.

The Infineon OPTIGA™ TPM

Infineon offers a wide range of TPMs with various interfaces, temperature ranges and versions, depending on the needs of the customer. One of the most important differentiators for Infineon TPMs is the availability of dedicated products meeting the requirements of different applications such as consumer, industrial and automotive devices. The dedicated products differ with regards to quality level, lifetime and temperature range in order to meet the special requirements of the target applications.

For people who build network equipment, it is especially important to have extended temperature range and extended product lifetime because a router or other network equipment mounted in an outside location may experience temperature extremes and replacing it could pose problems. Additionally all OPTIGA™ TPMs are tested against the TPM test suites to achieve highly compatible operation and interoperability.

Infineon OPTIGA™ TPMs have been certified to Common Criteria Evaluation Assurance Level (CC EAL) 4+. They include 6 KB of user-accessible non-volatile memory, as well as Elliptic Curve Cryptography (ECC-256) and RSA2K encryption, with the private key stored in secured hardware. As shown in Figure 1, Infineon also offers OPTIGA™ products with other security feature sets (Trust B, E, X and P) that can be used to address a variety of system trust requirements.



Note: TRX indicates communications function

Figure 1. Infineon provides a variety of OPTIGA™ microcontrollers (MCUs) for different applications in networks, servers and connected devices.

Additional Infineon TPM differentiation comes from expert support based on direct TCG specification involvement, a global network of trained support engineers and more than a dozen different technology partners, of which Mocana is one. Customers with engineering activity in locations such as India, Taiwan, and other global locations will find local experts to help with problems that could occur, where Infineon can address the hardware aspects and Mocana can handle the software aspects.

TCG network equipment guidance

With TCG's TPM 2.0 specification providing the hardware foundation, TCG's Network Equipment Sub Group developed "Guidance for Securing Network Equipment Using TCG Technology" to address the rapidly expanding network threat posed by unprotected routers, switches, firewalls, gateways and wireless access points. This specification defines prime use cases, including access, identity and attestation for integrity (health check), as well as eight others and explains how each works. In addition, the guidance identifies building blocks and makes technology recommendations regarding the use cases, providing in-depth information for how each use case can be implemented.

Mocana solution: TrustPoint™ on-device security software stack and TrustCenter™ device security services

With TCG's Network Equipment Guidance document defining the common architecture, Mocana's TrustPoint™ on-device security software and TrustCenter™ security management platform provide the enabling tools to protect network devices by using the integrated cryptographic features in the TPM. Supporting TCG's TPM 2.0 specifications, Mocana TrustPoint™ provides source code, binaries, sample code, and a simple set of application programming interfaces (APIs) for developers to leverage TPM capabilities to build trusted solutions. Key features of Mocana endpoint security software support for TPM 2.0 include:

- Mocana transport protocol stack (Transport Layer Security (TLS), Secure Shell (SSH) and Internet Protocol Security (IPsec)) integrated with TPM keys
- Applications running on native (bare metal) platforms can use TPM via local mode of execution
- Applications running in a container (for example Docker or LXC) or virtual machine (VM) environment can access a TPM via remote mode of execution
- Support for Certified Migratable Key (CMK) functionality to migrate TPM keys
- Support for platform attestation with TPM quote
- Support for hardware, firmware or even virtual TPMs that are TCG compliant

As shown in Figure 2, trusted device identification derived from a hardware or firmware-based TPM Root of Trust provides identity proofing for digital authentication that meets NIST 800-63B Authentication Assurance Level (AAL) 3, the highest level of this authentication assurance. In addition, this level of verification supports Proof of Possession of a secret for both Certificate Management over CMS (CMC) and the Enrollment of Secure Transport (EST). Integrated with Mocana TrustCenter™ services, this enables automated secured device enrollment based on multi-factor trusted artifacts.

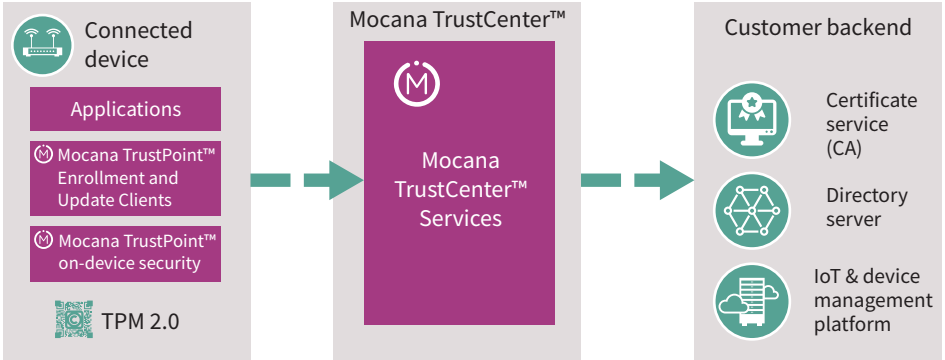


Figure 2. Mocana's TrustCenter™ platform and TrustPoint™ on-device software simplify the use of the TPM's many capabilities.

Network equipment vulnerability

Routers and other network equipment need to be more secured using trusted hardware for a variety of reasons. Possibly one of the more surprising aspects is that some equipment manufacturers already use Mocana software and have a TPM in their equipment but they do not take advantage of its capabilities. A better understanding of the problem and the solution can change this.

Existing network equipment is not inherently trustworthy for many reasons. There are many documented cases of network equipment that arrives at the customer's premises already compromised – the problem caused somewhere in the supply chain. This can occur because it was tampered within transit, it is counterfeit or has grey market (counterfeit) content or it is equipment that was resold and had already been infected. Countless counterfeit routers and other equipment available that are indistinguishable from the real thing were reported [2]. Through the use of a TPM, users can be confident that the product is what it claims to be and verify the version of firmware and software installed on it.

To prevent supply chain compromises, the U.S. has issued guidance on supply chain security for both federal and non-federal systems and organizations [3][4]. While these documents address computer equipment in general, they also include specific information about routers, firewalls, and intrusion detection systems to prevent these systems from being compromised.

Once in service, attacks specifically aimed at subverting the integrity of firmware in routers, switches and firewalls, normally among the trusted components in enterprise networks, can cause them to convey data insecurely. The compromised firmware of a router, switch or firewall, allows the attacker into the middle of all sorts of sensitive conversations and data communications. More than just eavesdropping, the intruder can also change the conversation, often without detection.

For example, when a laptop boots up, it communicates with the Dynamic Host Configuration Protocol (DHCP) server, get its internet protocol (IP) address with the Domain Name System (DNS) server address and then tries to contact other computers on the network to download firmware and software updates or to access email. If a connected router or switch has been compromised, the attacker can redirect those queries to the attacker's computer(s) at their servers and act as a man in the middle. In addition, they can deliver maliciously crafted messages to take over the computer and install a keystroke logger or other types of malware.

There are even greater threats. In today's sophisticated ships, submarines, shore or aircraft systems, a substantial amount of switching and routing can occur. Therefore, the concern for governments' agencies goes beyond counterfeit man-in-the-middle attacks; it involves the ability of an adversary to disrupt such systems at a critical moment. Commercial enterprises and industrial organizations are also frequent targets for attackers. Any of the 16 critical infrastructures vital to security, national economic security, national public health or safety are fair game [5].

Industrial control systems today are often based on Transmission Control Protocol/Internet Protocol (TCP/IP) over Ethernet or legacy networks, such as the Modbus, but still have switches and routers. Legacy equipment that is not properly secured poses the greatest problem. Attacking the switch or router is a sophisticated way of silently attacking the industrial control system (ICS) or power supplies associated with these systems. Some of the larger ICS and power supply manufacturers have found that their system has been totally compromised with grey market content that looks identical and is indistinguishable, visually and electrically, from the specified content. Only an in-depth analysis of the functions associated with the platform reveals the hostile code that can wreak havoc. Often considered safety aspects in an industrial network, ICS and power supplies can damage or stop the functions of industrial networks when they are sidelined, generating a classic control systems failure caused by illegal access.

Securing network equipment

TCG's Network Equipment Guidance addresses the problems described in the last section and more.
The document describes 11 different use cases:

- Device identity*
- Secured zero touch provisioning
- Securing secrets
- Protection of configuration data
- Remote device management*
- Software inventory
- Attestation of integrity for network devices (health check)*
- Composite networking devices
- Integrity-protected logs
- Entropy generation
- Deprovisioning

This document will focus on some of the most critical use cases, as indicated with an asterisk above.
For information on the other use cases, the reader is referred to the TCG document.

Device identity

Working together, Infineon and Mocana address device identity and the other use cases with TPM technology to provide the storage as well as operational mechanisms associated with obtaining and using endorsement keys to create a trust chain. Figure 3 shows keys and credentials for networking equipment. The three layers of identity, one for the TPM, one for the platform (IDevID) and one for the local identity (LDevID) are used to confirm that the equipment was properly manufactured, was installed at a particular location/facility, and is authorized by its owner.

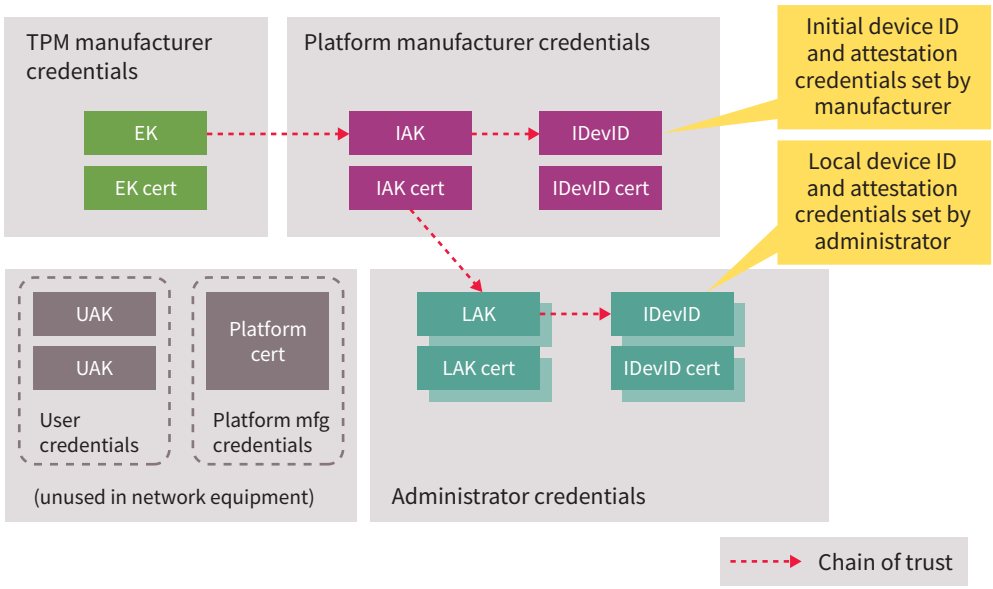


Figure 3. TPMs protect keys and credentials in network equipment.

Within the TPM, the endorsement key (EK) and EK certificate are installed by Infineon in every OPTIGA™ TPM. Every OPTIGA™ TPM shipped by Infineon comes with an individual endorsement private key, an individual endorsement public key, and an individual EK certificate signed by Infineon, so this chain of trust can be followed to confirm that the TPM is valid.

Next, the platform manufacturer credentials vouch for the installation of a specific TPM in a particular type of router or switch, perhaps even with a serial number. These credentials include the initial attestation key (IAK) and the initial device identification (IDevID). When the equipment is delivered to the customer, an administrator can but is not required to install company credentials such as a local device identity (LDevID), a local attestation key (LAK) and corresponding certificates.

With these certificates and credentials, the customer can easily verify that this router or switch came from a specific supplier, has a specific model number and serial number, and is the actual piece of equipment purchased for use within the customer's particular facility, so it can be trusted. This might contrast to another product from the same supplier that could be a second-hand version with unknown history and therefore no basis for trust. Through the TCG specifications, the three layers of identity (the TPM, the platform and the local owner/operator) tie together to provide a chain of trust and chain of custody that gives the user confidence in the provenance of the device.

The ability to uniquely establish device identity solves other problems. For example, many pieces of networking gear employ the outmoded user name and password authentication technique. In fact, many devices include a preinstalled default username and password. Eliminating those default artifacts is sometimes difficult because they are used for administrative configuration. Moving to unique cryptographic identities enables mutual authentication and secured communications for all connections. For more examples, see the sidebar at the end of this page titled "Addressing additional identity issues".

While provisioning these credentials sounds rather straightforward, it is typically far more difficult to do because the traditional certificate tools that are given as a function of either certification authorities (CAs) or in Hardware Security Modules (HSMs) are not well understood nor are they easy to use. In contrast, they are easy to implement with Mocana software. Taking advantage of the broad set of key generation and key operations with TPM 2.0, Mocana software supports Storage and Endorsement hierarchies as well as RSA and ECC keys. Furthermore, Mocana's software can use the TPM-generated key pairs to provision digital certificates to determine the integrity of containers, applications, data and communications.

Addressing additional identity issues

In the chain of trust, transfer of ownership poses challenges. A brand new piece of equipment assembled by one company could be sold to another that installs that equipment into an end product, perhaps an aircraft, that is installed on backplane with its own certificate on the airframe - all of these are transfer of ownership functions. Currently, there isn't a good way to effectively validate the transfer function between those elements without using certificates and cryptography signing and endorsement. Device identity keys and certificates correct that situation.

In contrast to personal computers, with network equipment there are no users with unique keys and credentials on whose behalf the equipment is operating. The network equipment itself has its own identity or identities and they may validate others, but there is no user that it is specifically operating for. However, there are many use cases even without the concept of a keyboard user where additional certificates are used in a trust stream for specialized functions, such as reporting analytics, implementing read-only functions, and the separation of read-only from read-write functions on a local platform. Those can be multi-level, where one group of users might be able to update the firmware, while another group of users might be able to update the operating environment and a third group of users might be able to update some of the applications space functions or configuration functions.

There are other uses of multi-tiered certificates in use in the trust chain to add significant value to the overall trustworthiness of the platform. In this case, the platform authenticates an external user. It is not the key of the external user but the certificate of the external user or administrator that is part of a handshake. That is why within the constellation of credentials, the most essential ones are the ones highlighted in Figure 3. These credentials are those that allow the platform to authenticate itself to others or to perform an attestation to others not so much the ones it uses to authenticate some external party.

Remote device management

Network equipment is typically managed remotely either with a command line, with a GUI (Graphic User Interface), or with automation such as SDN (Software-Defined Networking). The most fundamental security aspect of this management is authentication and secured communications. Fortunately, the Mocana software and Infineon TPM hardware provide the ability to setup secured communications using not just the prevalent TLS (Transport Layer Security) protocol but also with SSH (Secure Shell), IPsec (Internet Protocol Security) and with other protocols as well. Sessions created with the Mocana software are authenticated and even encrypted using the device identities that are installed in the platform.

Once authentication and secured communication with the device are established, remote management of the device can be conducted over the secured protocol. Many other security operations can also be performed such as verifying that the device is not counterfeit, that it is the device that is supposed to be installed at this location, and that it has not been tampered with (using remote attestation, the next use case).

Remote attestation

Remote attestation allows a device to attest to (vouch for) the software it is running so that a remote party can verify this attestation. As shown in Figure 4, Mocana's endpoint security software and Infineon's TPM enable a remote "verifier" (a specialized service) to determine the level of trust in the integrity of a device or of a containerized application running on a device (platform).

The remote attestation process proceeds as follows. The software on the device is measured with a cryptographic hash. These measurements are extended into Platform Configuration Registers (PCRs) in the TPM, where they are stored securely. When the remote party wishes to obtain an attestation, it sends a challenge to the device. The software on the device sends this challenge to the TPM, which produces a "quote" – a copy of the challenge and the current PCR values, signed by an Attestation Identity Key (AIK) held by the TPM. The quote is sent back to the server along with an AIK certificate issued by a trusted CA and an integrity log listing the software loaded on the device. The verifier can verify all these things to determine whether the software on the device is acceptable. A related technology known as "sealing" can be used for local attestation. And device configuration can be verified in the same manner.

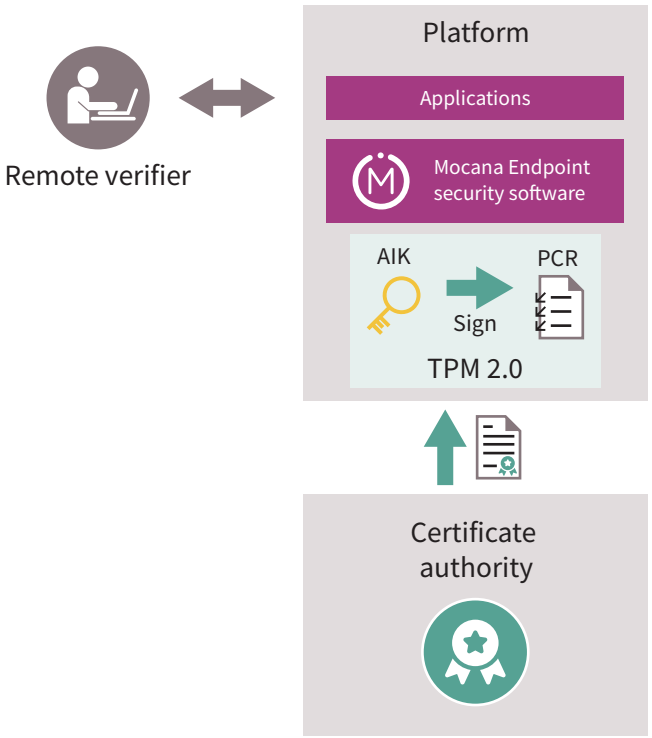


Figure 4. Using the remote attestation capabilities of TPM 2.0, Mocana endpoint security software establishes the trustworthiness of containerized applications.

Summary: A combined solution for the highest security and trust

With unprotected network equipment providing new targets for attackers, preventing those types of attacks needs to be high on the must do list of information technology (IT), network and security experts as well as many levels of enterprise management.

The consequences of inaction are too great. In contrast, implementing standardized protection is made much easier based on the combined efforts of Infineon and Mocana.

Infineon's certified OPTIGA™ TPM MCUs provide networks, servers and connected devices with state-of-the-art hardware security, working with Mocana's TrustPoint™ on-device security software and TrustCenter™ security management platform to provide the enabling tools that protect network devices by using the integrated cryptographic features in the TPM.

Together, the combination of Infineon OPTIGA™ TPM hardware and Mocana TrustPoint™ software provide enhanced security tools that protect vital network equipment, with a global network of expert engineers to provide direct local hardware and software support.

Backed by Trusted Computing Group standards, Infineon and Mocana provide an easily implementable trust and security solution to handle network security threats directly. This makes it possible for a variety of enterprises and infrastructure to avoid persistent, subtle infections and counteract a vast variety of attacks

OPTIGA™ is a trademark of Infineon. Mocana TrustCenter™ and TrustPoint™ are trademarks of Mocana.

References

[1] https://trustedcomputinggroup.org/resource/tcg-guidance-securing-network-equipment/

[2] https://www.infoworld.com/article/2653167/fbi-worried-as-dod-sold-counterfeit-cisco-gear.html

[3] SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-161/final

[4] SP 800-171 Rev. 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

[5] https://www.dhs.gov/critical-infrastructure-sectors