WHITE PAPER

Signed firmware, secure boot, and security of private keys

Cybersecurity features in Axis products

July 2020

AXIS COMMUNICATIONS

Table of Contents

1 Summary

This document describes some of the features available in Axis products that can mitigate cyber threats and counter specific types of attacks. The features are:

- signed firmware
- secure boot
- trusted platform module (TPM)
- Axis Edge Vault with Axis device ID.

The threats that are outlined include:

- firmware tampering
- supply-chain tampering
- extraction of private keys
- unauthorized device replacement.

1.1 Signed firmware

Signed firmware is implemented by the software vendor signing the firmware image with a private key. When a firmware has this signature attached to it, a device will validate the firmware before accepting to install it. If the device detects that the firmware integrity is compromised, the firmware upgrade will be rejected.

1.2 Secure boot

Secure boot is a boot process that consists of an unbroken chain of cryptographically validated software, starting in immutable memory (boot ROM). Being based on the use of signed firmware, secure boot ensures that a device can boot only with authorized firmware.

1.3 TPM

A TPM is a component which provides a set of cryptographic features suitable for protecting information from unauthorized access. Private keys are stored in the TPM and all cryptographic operations requiring the use of the private key are sent to the TPM to be processed. This ensures that the secret part of the certificate remains safe even in the event of a security breach. The TPM used in selected Axis products is certified to meet the requirements of FIPS 140-2.

1.4 Axis Edge Vault with Axis device ID

The new international standard IEEE 802.1AR describes a procedure for how to automate and secure the identification of a device over a network. In Axis products, these security measures are implemented by use of Axis Edge Vault and Axis device ID. Edge Vault can be used for cryptographic challenges operating on securely stored certificates. The private part of the certificates stay in Edge Vault even when it is being used. Axis device ID is securely and permanently stored in Edge Vault as a certificate signed by Axis root certificate and this enables a new level of device trust through the life cycle of the product.

2 Glossary

Certificate – In cryptography, a certificate is a signed document attesting origin and properties of a key pair. The certificate is signed by a Certificate Authority, CA, and if the system trusts the CA then it will also trust the certificates issued by it.

Certificate Authority, CA – the root of trust for a certificate chain. It is used to prove the authenticity and veracity of underlying certificates.

FIPS – Federal Information Processing Standards, standards for data encryption and data security issued in the US by NIST (National Institute of Standards and Technology).

Immutable ROM – to safely store the trusted public keys and the program that are used to compare signatures so that they can't be overwritten.

Provisioning – the process of preparing and equipping a device for the network. This involves delivering configuration data and policy settings to the device from a central point. The device is supplied with keys and certificates.

Public key cryptography – an asymmetric cryptography system where any person can encrypt a message using the receiver's *public key*, but only the receiver – using the *private key* – can decrypt the message. Can be used to both encrypt and sign messages.

TLS – Transport Layer Security, internet standard for protecting network traffic. TLS provides the S (for secure) in HTTPS.

3 Introduction

Axis follows industry best practices in managing and responding to security vulnerabilities in our products in order to minimize customer exposure to cyber risks. There is no way to guarantee that products and services are free from flaws that can be exploited for malicious attacks. This is not specific to Axis, but rather a general condition for all network devices. What Axis can guarantee, is that we always make a concerted effort at every possible stage in order to ensure that the least risk possible is associated with your Axis devices and services.

For more information about product security and discovered vulnerabilities, see *www.axis.com/support/product-security*. For more information about the measures you can take to reduce the risks of common threats, download Axis Hardening Guide from *www.axis.com/cybersecurity*.

This white paper presents some plausible cyberattacks and how they can be prevented in Axis products. It describes specifically how the features signed firmware and secure boot can prevent firmware tampering and supply-chain tampering. We also discuss the use of a trusted platform module (TPM) and Axis Edge Vault, which can both be used to secure private keys. Axis Edge Vault is used to securely store Axis device ID which enables a new level of device trust.

4 Firmware tamper detection

One possible attack vector that an adversary may try exploit after failing other attempts to breach the system, is to get the system owner to install altered applications, firmware, or other software modules. The altered software may include malicious code with a specific purpose. The common recommendation is to never install any software from a source that you do not fully trust. In a video system context there may be a "man in the middle" that could alter a device firmware and lure end users to install it. This is not an easy exercise and the adversary needs to be very skilled and determined. He needs an extremely detailed understanding of Axis firmware design and how the firmware operates in a device. Still, those adversaries may exist if the value of attacking a specific system is high enough. The common counter measure is for the software vendor to use signed firmware.

4.1 Firmware signing

Signed firmware is implemented by the software vendor signing the firmware image with a private key, which is held secret. When a firmware has this signature attached to it, a device will validate the firmware before accepting to install it. If the device detects that the firmware integrity is compromised, the firmware upgrade will be rejected.

The process of signing firmware is initiated through the computation of a cryptographic hash value. The value is then signed with the private key of a private/public key pair before the signature is attached to the firmware image.

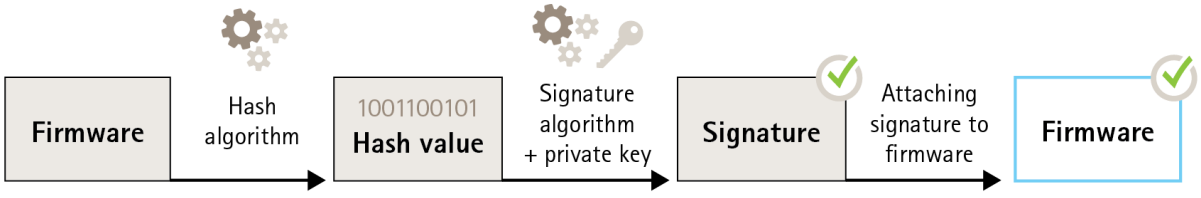

Figure 1. The process of signing firmware.

Before a firmware upgrade, the new firmware must be verified. To ensure that the new firmware is unmodified, the public key (which is included with the Axis product) is used to confirm that the hash value was indeed signed with the matching private key. By also computing the hash value of the firmware and comparing it to this validated hash value from the signature, the integrity of the firmware can be verified.

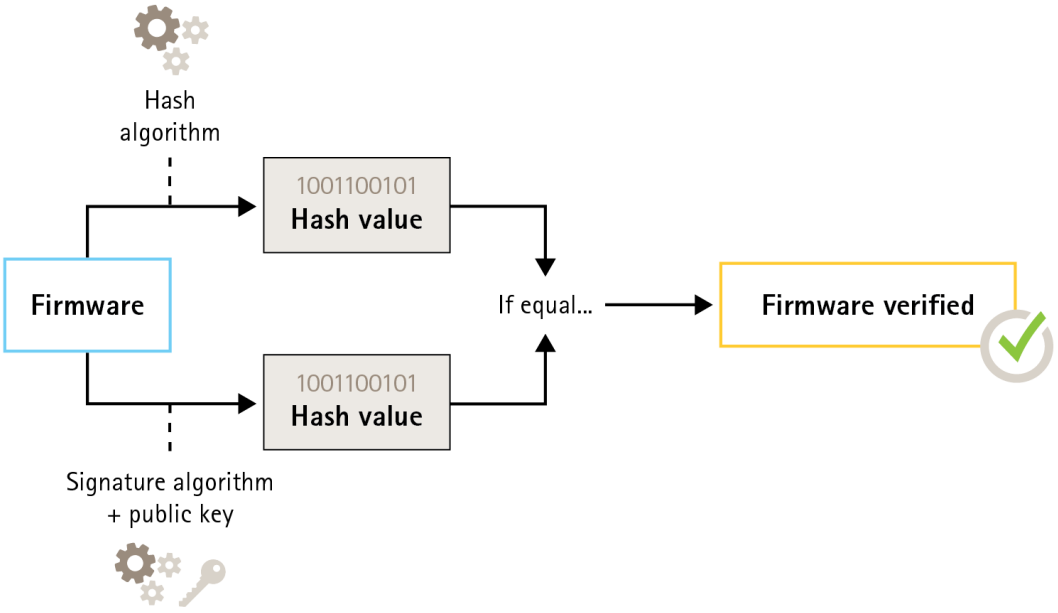

Figure 2. The process of verifying signed firmware.

4.2 Signed firmware at Axis

Axis signed firmware is based on the industry-accepted RSA public-key encryption method. The private key is stored in a closely guarded location at Axis while the public key is embedded in Axis devices. The

integrity of the entire firmware image is assured by a signature of the image content. A primary signature verifies a number of secondary signatures, being verified while the image is unpacked.

5 Supply-chain tamper prevention

Firmware signing protects a device, in all future firmware updates, from installing a compromised firmware. But what if a man in the middle alters the device on its way between vendor and end user? An adversary that has physical access to the device during transit could perform an attack, such as compromising the boot partition of the device, bypassing firmware integrity checking in order to install an altered, malicious firmware before the device is deployed.

5.1 Secure boot

Secure boot is a boot process that consists of an unbroken chain of cryptographically validated software, starting in immutable memory (boot ROM). Being based on the use of signed firmware, secure boot ensures that a device can boot only with authorized firmware.

The boot process is initiated by the boot ROM validating the bootloader. Secure boot then verifies, in real-time, the embedded signatures for each block of firmware that is loaded from the flash memory. The boot ROM serves as the root of trust, and the boot process continues only as long as each signature is verified. Every part of the chain authenticates the next part, ultimately resulting in a verified Linux kernel and a verified root file system.

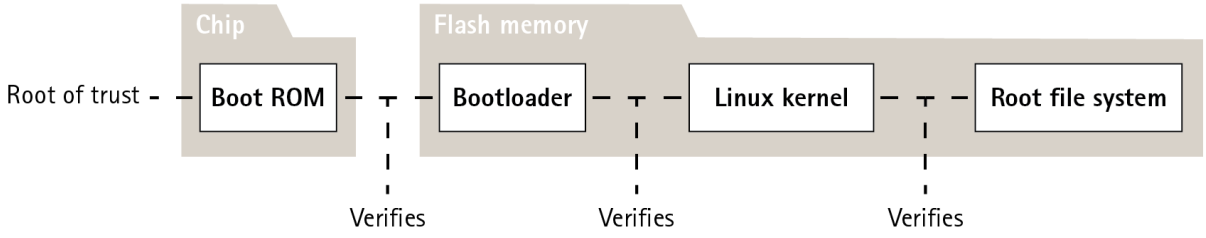

Figure 3. The secure boot process.

5.2 Axis secure boot

In many devices, it is important that the low-level functionality is impossible to alter. When other security mechanisms are built on top of the lower-level software, secure boot serves as a safe base layer that protects those mechanisms from being circumvented.

For a device with secure boot, the installed firmware in the flash memory is protected from being modified. The factory default image is protected, while the configuration remains unprotected. Secure boot guarantees that the Axis device is completely clean from possible malware after a factory default.

5.3 Secure boot and Custom Firmware Certificates

While secure boot makes the product safer, it does also reduce the flexibility with different firmware, making it more complicated to load any temporary firmware, such as test firmware or other custom firmware from Axis, into the product. However, Axis has implemented a mechanism that approves individual units to accept such non-production firmware. This firmware is signed in a different way, with approval by both the owner and Axis, and results in a Custom Firmware Certificate. When installed in the approved units, the certificate enables use of a custom firmware that can run only on the approved unit, based on its unique serial number and chip ID. Custom Firmware Certificates can be created only by Axis, since Axis holds the key to sign them.

6 Security of private keys

Axis devices support HTTPS (network encryption) and 802.1X (Network Access Control) which both use TLS (Transport Layer Security). The digital certificates of TLS use a public/private key pair. The private key is stored in the device while the public key is included in the certificate. Note that if neither HTTPS nor 802.1X is used, there are no keys to protect.

An adversary could try to extract the private key and the certificate from the device and install them on an attacking computer. In the case of HTTPS, that private key could be used to eavesdrop encrypted network traffic between the device and the VMS. Or, if spoofing the network, the attacking computer could get access to the VMS by pretending to be a legitimate device. In the case of 802.1X, the adversary could use the private key to gain access to an 802.1X-protected network, posing as a trusted device.

Certificates and private keys are generally stored in a device's file system, protected by the account access policy and used in the normal computing environment. In most cases this is sufficient since the account is not easily compromised. Note that certificates can be revoked if a compromise is suspected, making the private key useless.

Some end users of critical systems may experience an increased risk of determined and skilled adversaries that try to breach the device to extract the private key. A trusted platform module (TPM) stores the key in such a way that it is close to impossible to extract it, even when the device is compromised.

6.1 Safe key storage with a TPM (trusted platform module)

A TPM is a component which provides a certain set of cryptographic features suitable for protecting information from unauthorized access. The private key is stored in the TPM and never leaves the TPM. All cryptographic operations requiring the use of the private key are sent to the TPM to be processed. This ensures that the secret part of the certificate never leaves the secure environment within the TPM and remains safe even in the event of a security breach.

6.2 FIPS 140-2 certification

For some products and use cases, it may be a regulatory requirement to use a TPM for protecting information, sometimes in combination with a requirement of FIPS 140-2 compliance. FIPS (Federal Information Processing Standard) 140-2 is an information security standard for cryptographic modules, issued in the US by NIST (National Institute of Standards and Technology).

Validation by a NIST-certified test laboratory assures that the module system and the cryptography of the module are correctly implemented. In short, the certification requires description, specification,

and verification of the cryptographic module, approved algorithms, approved modes of operation, and power-up tests.

More details about the certification requirements of FIPS 140-2 can be found at the NIST website *https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards*

6.2.1 Certified TPM in Axis products

The TPM used in selected Axis products is certified to meet the requirements of FIPS 140-2. More specifically, it is certified to Security Level 2 of the standard, which means that the TPM also fulfills requirements for role-based authorization and tamper evidence, among other requirements.

7 IEEE 802.1AR - device verification with Axis device ID

A person buying an Axis network device can perform a manual examination before starting to use it. By visually inspecting the product and using prior knowledge about the look and feel of Axis products, the customer can feel convinced that the product really does originate from Axis. However, that type of inspection can only be done by a person with physical access to the product. So, when you communicate with a non-provisioned product over a network, how can you be sure that you are communicating with the correct unit? That the device hasn't been unauthorizedly replaced? Neither networked equipment nor software on servers can perform a physical inspection. As a security measure, it has been common to first interact with a new product over a closed network, where the unit can be provisioned safely.

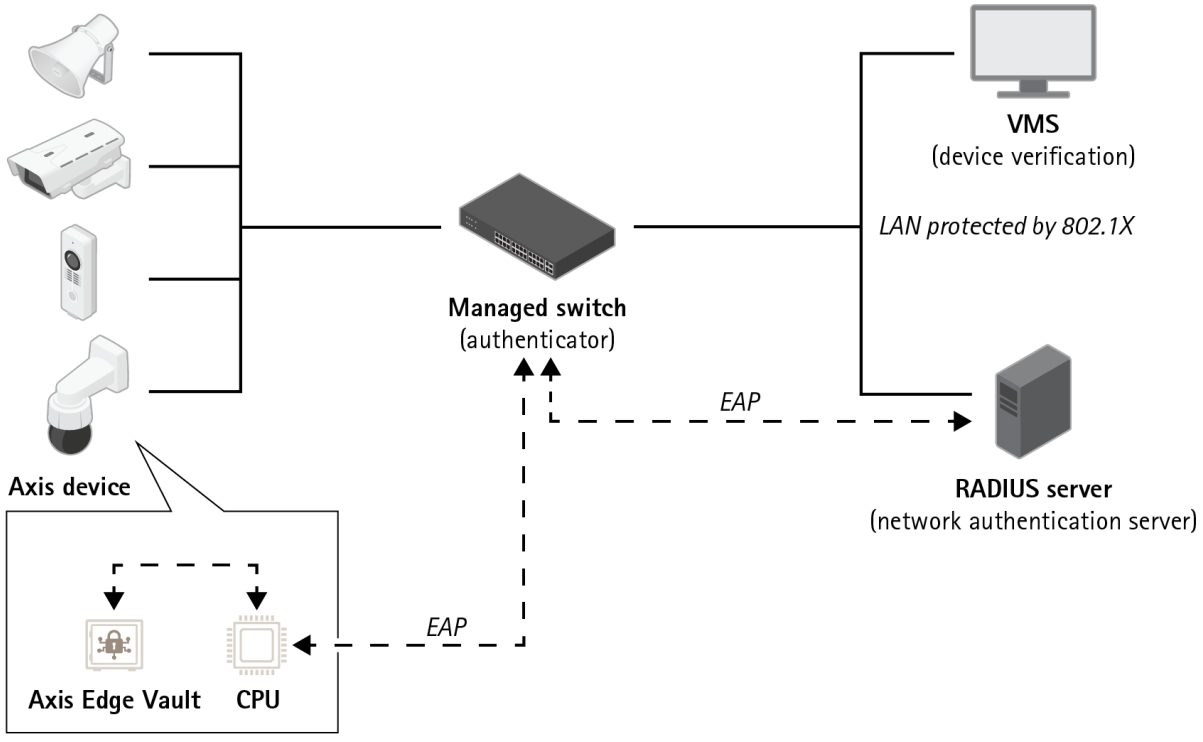

Figure 4. Customers may instruct their authentication server to automatically accept purchased Axis products on to the network using device serial numbers and Axis device ID.

The new international standard IEEE 802.1AR (*https://1.ieee802.org/security/802-1ar/*) defines a method for how to automate and secure the identification of a device over a network. If the communication is forwarded into an embedded secure module, the unit can return a trustworthy identification response according to the standard.

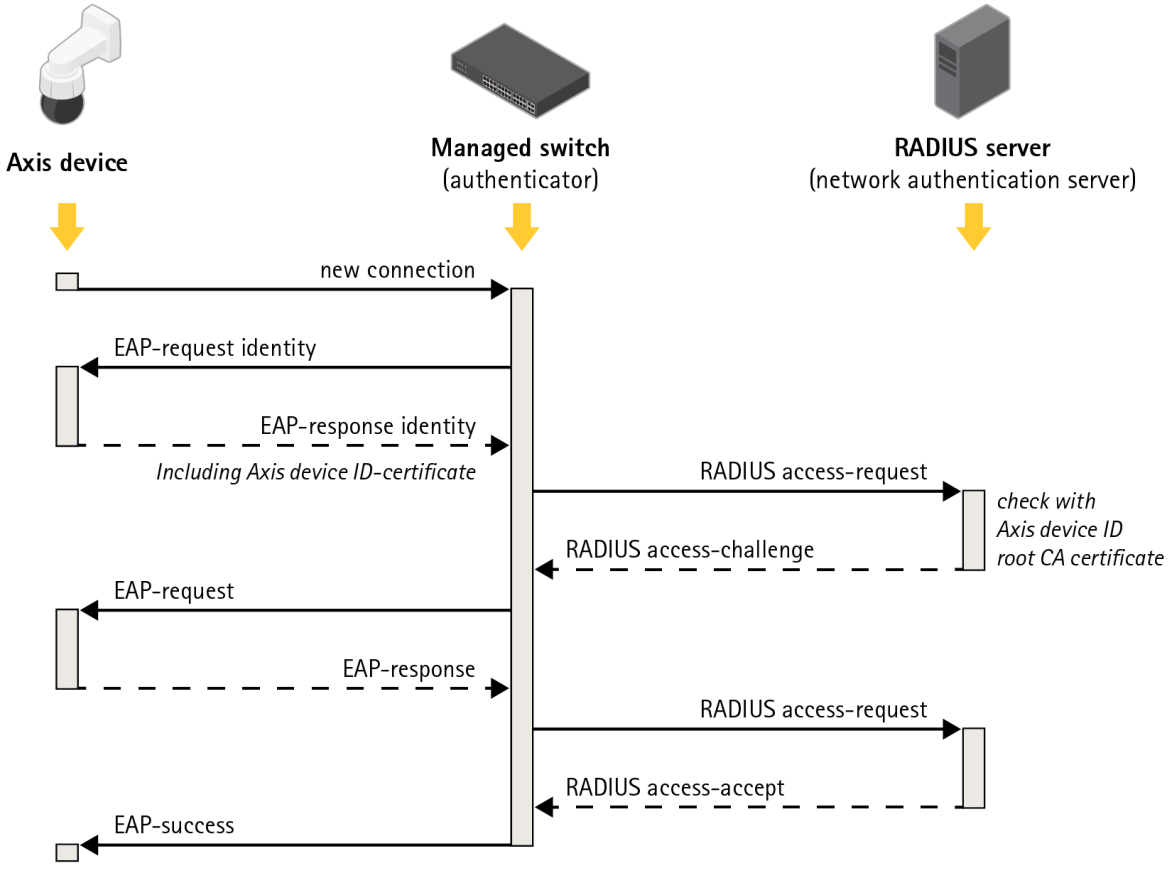

Figure 5. IEEE 802.1AR defines a method for how to identify a device over a network by following a protocol sending Extensible Authentication Protocol requests (AEP) to the switch that use Remote Authentication Dial-In User Service (RADIUS) - requests to grant access.

In Axis products, these security measures are implemented by use of Axis Edge Vault and Axis device ID. Axis Edge Vault is a secure module in which Axis device ID, a collection of certificates to verify device identification, is installed. These features provide your network with cryptographically verifiable proof that a specific unit was produced by Axis and that the network connection to the unit is indeed served by that very unit.

A device with Axis device ID has been provisioned in the factory (with keys and certificates). This provisioning can later be used by a customer to further provision the device in the field with other keys and/or certificates allowing it to access some of the customer's network resources.

By identifying the unit with Axis device ID, the time for deployment of devices can be reduced, since less work needs to be done with the device before installing and configuring for it on the intended network. Another benefit is that Axis device ID, apart from providing an additional, built-in source of trust, also provides a means to keep track of devices in a large system.

7.1 Axis Edge Vault

Axis Edge Vault is a secure cryptographic compute module in form of a chip mounted on the PCB inside the product. Edge Vault has the possibility to securely store certificates and can be used for cryptographic operations on securely stored certificates.

Certificates that are stored in Edge Vault don't need to leave it in order to be used by the device. They stay securely in Edge Vault even when they are being used, since the cryptographic hardware that operates on the key is installed on the same physical chip.

7.2 Axis device ID

During production of each Axis network device unit a "digital passport" called Axis device ID is securely installed in the unit's Axis Edge Vault. This identity is unique for each unit and is designed to prove the origin of the device. Axis device ID is a collection of certificates that is used in the cryptographic operation part of the module to sign challenges presented by the embedded product firmware to Edge Vault. The response from this operation is sent back to the receiver that can use Axis public keys to validate the authentication of the response.

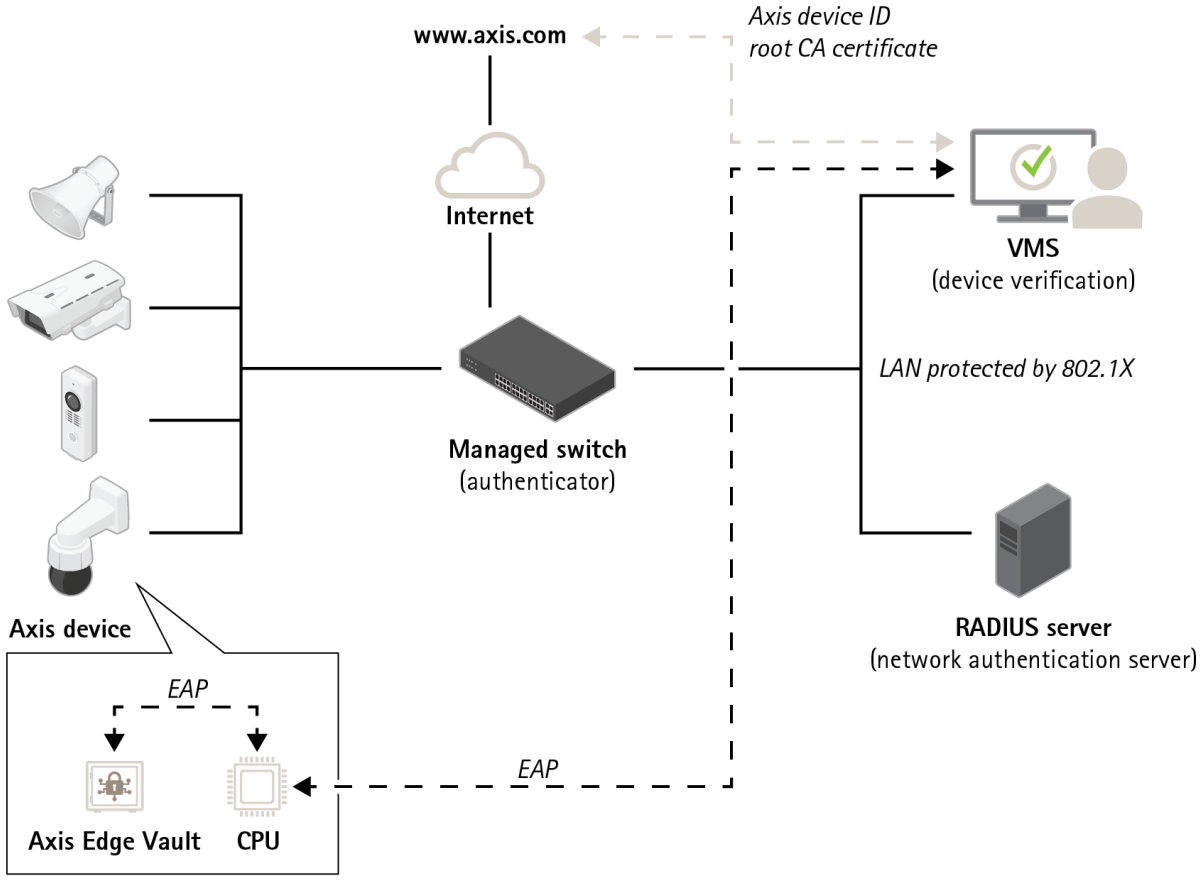

Figure 6. Software applications in other parts of the system can use the Axis device ID and cryptographic operations to verify whom it's communicating with. The Axis device ID was verified by the public Axis device ID Root CA certificate from axis.com.

7.2.1 Certificate hierarchies

A certificate is a small piece of data combining a public key and metadata describing the key along with a signature from the issuer attesting the validity of the certificate.

A certificate hierarchy is a way to prove the provenance of the certificate. Let's consider an analogy between Axis device ID and a passport. If you have a passport, your country's government provides assurance that you are in fact the person that the passport claims you to be. In a similar way, all Axis device ID certificates are endorsed by an Axis device ID Root CA Certificate. Just like a customs agent trusts your country's government to have correctly issued your passport, a network security system trusts the Axis device ID Root CA Certificate to have correctly verified a network-connected unit's Axis certificate.

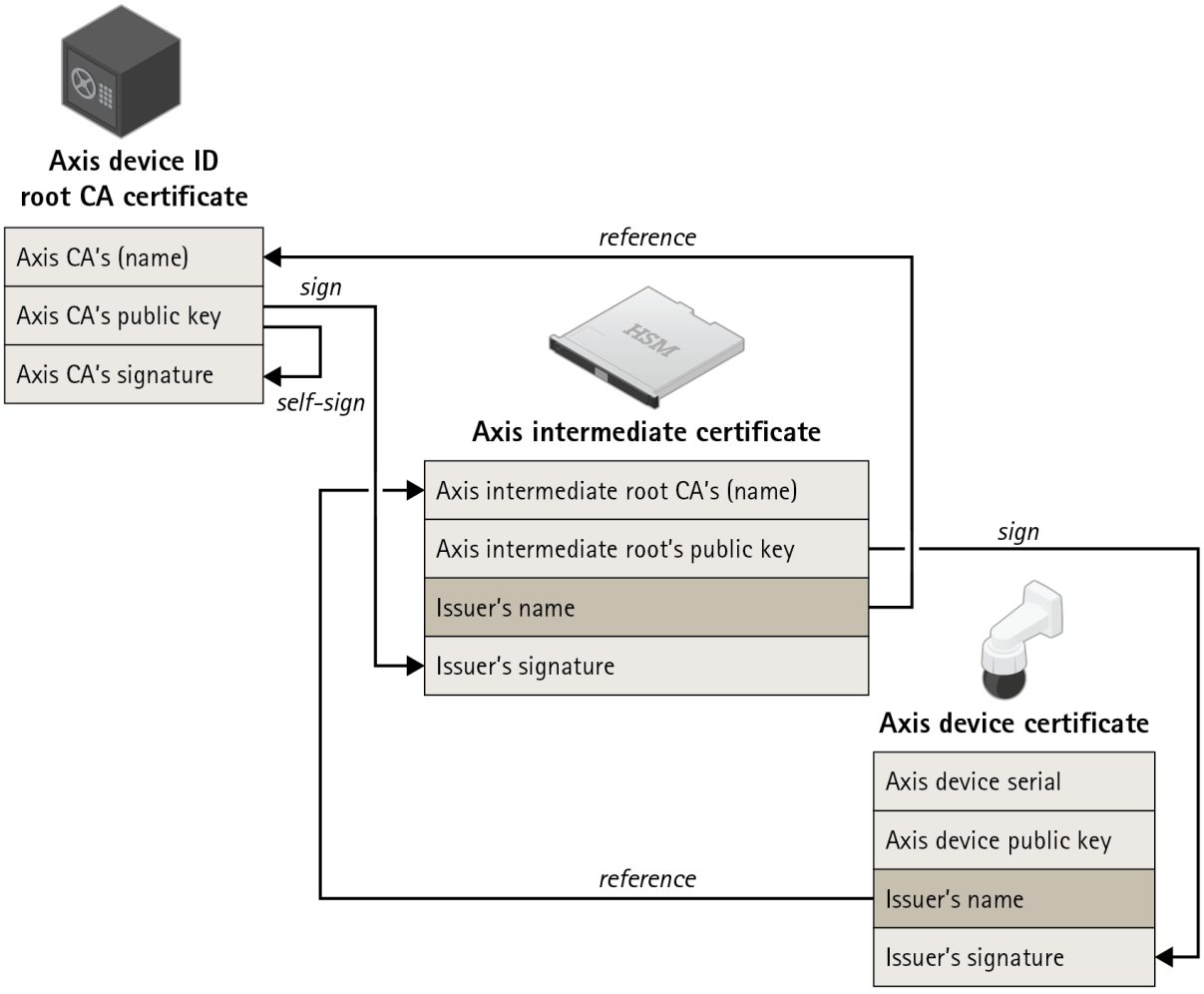

Figure 7. Axis device ID, which is a certificate incorporating the serial number of the product, is signed by an intermediate certificate which was signed by the Axis root certificate. Since the Axis root certificate is very valuable and need to be stored in a safe, the intermediate certificate is needed during provisioning in the factory.

T10154694/EN/M1.8/2007

About Axis Communications

Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axis offers products and services for video surveillance and analytics, access control, and audio systems.

Axis has more than 3,500 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Axis was founded in 1984 and has its headquarters in Lund, Sweden.

For more information about Axis, please visit our website *axis.com*.