Axis Edge Vault

March 2026

AXIS®
COMMUNICATIONS

Summary

Axis Edge Vault provides a hardware-based cybersecurity platform that safeguards the Axis device. It relies on a strong foundation of cryptographic computing modules (secure element and TPM) and SoC security (TEE and secure boot), combined with expertise in edge device security. Axis Edge Vault has its anchor point in the strong root of trust, established by *secure boot* together with *signed OS* ("OS" is for operating system). These features enable an unbroken chain of cryptographically validated software for the chain of trust that all secure operations depend on.

Axis devices with Edge Vault minimize customer exposure to cybersecurity risks by preventing eavesdropping and malicious extraction of sensitive information. Axis Edge Vault also enables the Axis device to be a trusted and reliable unit on the customer's network.

Axis Edge Vault cybersecurity platform

Cryptographic computing modules	Features	Use cases
• Secure element • TPM 2.0 • SoC security (TEE)	• Secure boot • Signed OS • Axis device ID • Secure keystore • Signed video • Encrypted file system	• Supply chain protection • Trusted device identity • Secure key storage • Video tampering detection

- **Supply chain protection**: Axis Edge Vault requires a secure foundation that acts as the root of trust. Without the help of secure boot and signed OS, the root of trust chain cannot be established. Secure boot, together with signed OS, provides an unbroken chain of cryptographically validated software, starting in immutable memory (boot ROM). Secure boot ensures that a device can boot only with signed OS, which prevents physical supply chain tampering. With signed OS, the device is also able to validate new device software before accepting to install it. If the device detects that the integrity is compromised or the device software is not signed by Axis, the upgrade will be rejected. This protects devices from software tampering.

- **Trusted device identity**: Being able to verify the origin of the device is key to establishing trust in the device identity. During production, devices with Axis Edge Vault are assigned a unique, factory-provisioned, and IEEE 802.1AR-compliant Axis device ID certificate. This works like a passport to prove the origin of the device. The device ID is securely and permanently stored in the secure keystore as a certificate signed by Axis root certificate. The device ID can be leveraged by the customer's IT infrastructure for automated secure device onboarding and secure device identification.

- **Secure key storage**: The secure keystore provides hardware-based, tamper-protected storage of cryptographic information. The secure keystore protects the Axis device ID, as well as customer-loaded cryptographic information, and prevents unauthorized access and malicious extraction in the event of a security breach.

- **Video tampering detection**: Signed video ensures that video evidence can be verified as untampered without proving the chain of custody of the video file. Each camera uses its unique video signing key, which is securely stored in the secure keystore, to add a signature into the video stream. When the video is played, *Axis signed media verifier* shows whether the video is intact. Signed video makes it possible to trace the video back to the camera origin and verifies that the video has not been tampered with after it left the camera.

Table of Contents

1   Introduction

Axis follows industry best practices in implementing security in our products. This is done to minimize customer exposure to cybersecurity risks and to make the Axis device a trusted unit on the customer's network.

Axis Edge Vault provides a hardware-based cybersecurity platform that safeguards the Axis device. It builds on a strong foundation of cryptographic computing modules (secure element and TPM) and SoC security (TEE and secure boot), combined with expertise in edge device security.

This white paper will outline the multi-layered approach of Axis edge device security, and present common risks and how they can be prevented. Axis Edge Vault requires a secure foundation that acts as the root of trust. Therefore, we will also look at supply chain security aspects of Axis devices and learn how signed OS (signed operating system) and secure boot are fundamental measures that counter software tampering and physical supply chain tampering.

At *www.axis.com/support/cybersecurity/resources* you can find more information about product security, discovered vulnerabilities, and the measures you can take to reduce the risks of common threats.

The last chapter of this white paper contains a glossary.

2   Supply chain protection

Axis Edge Vault requires a secure foundation that acts as the root of trust. Establishing the root of trust starts at the device's boot process. In Axis devices, the hardware-based mechanism *secure boot* verifies the operating system (AXIS OS) that the device is booting from. AXIS OS, in turn, is cryptographically signed using *signed OS* during the build process.

Secure boot and signed OS tie into each other. They ensure that the operating system or device software has not been tampered with (by anyone with physical access to the device) before the device is deployed and that, after deployment, the device cannot install compromised or non-code-signed software updates. Together, secure boot and signed OS create an unbroken chain of cryptographically validated software for the chain of trust that all secure operations depend on.

2.1 Secure boot

The secure boot mechanism is a boot process that consists of an unbroken chain of cryptographically validated software, starting in immutable memory (boot ROM). Secure boot makes sure that a device can boot only with authorized operating system.

The boot process is initiated by the boot ROM validating the bootloader. Secure boot then verifies, in real time, the embedded signatures for each software component that is loaded from the flash memory. The boot ROM serves as the root of trust, and the boot process continues only if 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.
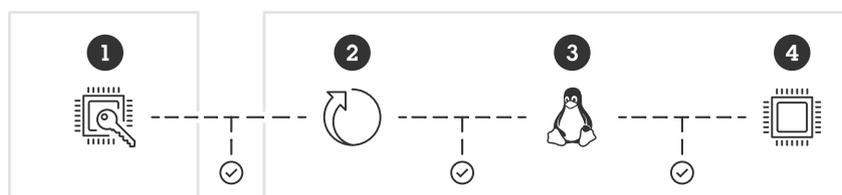
In the secure boot process, each part of the chain authenticates the next. This ultimately results in a verified root file system.

1   *Boot ROM (root of trust) on the SoC*
2   *Bootloader*
3   *Linux kernel*
4   *Root file system*

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 operating system in the flash memory is protected from being modified, while the configuration remains unprotected. Secure boot guarantees the correct state of the device, even after a factory default. But for secure boot to work, it must make sure that the boot verifies that the operating system is signed by Axis.

2.2 Signed OS

Axis signed OS involves Axis code-signing the device software image with a private key that is kept secret. At device startup, the secure boot of an Axis device will check that the device software is signed. If the device detects that the integrity of the device software is compromised, the device will not run. When upgrading the device software, the device's existing signed AXIS OS will automatically check that the new AXIS OS is also signed. If not, the upgrade will be rejected.

The process of code-signing OS 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 AXIS OS image.
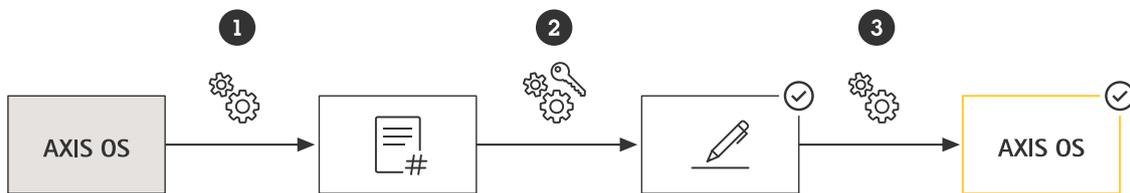
The process of code-signing OS.

1   *A cryptographic hash value for AXIS OS is created.*
2   *The signature is created by combining the hash and the private key.*
3   *The signature is added to the AXIS OS version and binary.*

Before an upgrade, the authenticity of the new software update must be verified. To ensure this, 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 and comparing it to this validated hash value from the signature, the integrity can be verified. The boot process of the Axis devices would be aborted if the signature is invalid or the AXIS OS image has been tampered with.
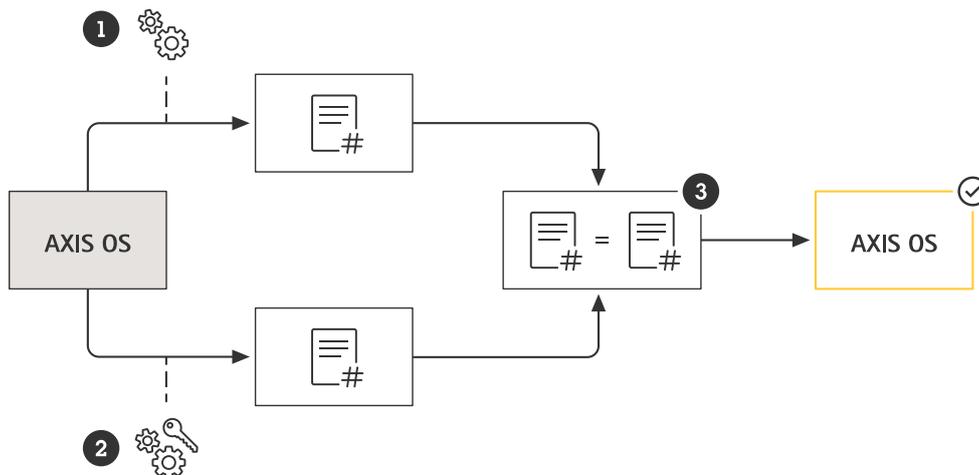
The process of verifying signed OS.

1   *Computing the hash value of AXIS OS*
2   *Using the public key to confirm hash value from signature*

3   Only if the results match, the signature is successfully verified.

Axis signed OS 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 software image is assured by a signature. A primary signature verifies several secondary signatures, being verified while the image is unpacked.

For test and custom builds, Axis has implemented a mechanism that approves individual devices to accept non-production images. This image is code-signed using a key dedicated for that purpose, with approval by both the owner and Axis, and results in a custom signature. When installed in the approved devices, the certificate enables the use of a custom image that can run only on the approved device, based on its unique serial number and chip ID. Custom certificates can be created only by Axis since Axis holds the key to sign them.

3   Trusted device identity

In modern zero-trust security networks ("never trust, always verify"), the ability to verify the origin of the device, its authenticity, and its connections is a foundational need. A network device can verify its integrity and authenticity in a way that is similar to showing your passport to authorities at the airport for identity verification.

3.1 Secure device identification with Axis device ID

The international standard *IEEE 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 cryptographic computing module, the device can return a trustworthy identification response according to the standard. This trustworthy response can be used by the network infrastructure to allow for automated and secure onboarding of the device into a provisional network for initial device configuration and software updates.

To comply with IEEE 802.1AR, we manufacture most of our devices with device-unique and factory-provisioned Axis device ID certificate (IEEE 802.1AR Initial device identifier, IDevID). The Axis device ID is securely stored in the tamper-protected secure keystore, provided through a cryptographic computing module on the device itself. This identity is unique for each Axis device and is designed to prove the origin of the device.
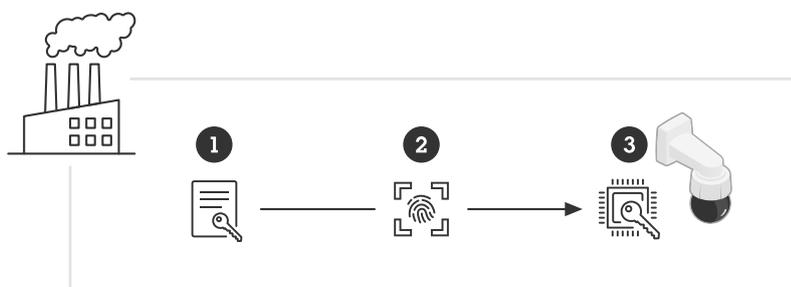
During the manufacturing process of a device, the unique Axis device ID (2) is stored in the device's secure keystore (3).

1   *Axis device ID key infrastructure (PKI)*
2   *Axis device ID*
3   *Axis device ID securely stored in the tamper-protected secure keystore, provided through a cryptographic computing module on the Axis device.*

IEEE 802.1AR is based on the IEEE 802.1X standard for network access control, which is enabled by default in Axis devices with the Axis device ID pre-selected. This allows for secure identification and authentication of the Axis device through an 802.1X-capable IT infrastructure, even in the factory default state.

The Axis device ID certificate comes in various cryptographic configurations (2048-bit RSA, 4096-bit RSA, ECC-P256). They are enabled by default to allow for secure device connections and identification through IEEE 802.1X network access control as well as HTTPS.

Axis manages its own dedicated IEEE 802.1AR public key infrastructure (PKI) for factory provisioning the Axis device ID during the manufacturing process. The Axis device ID is signed by the intermediate certificate which in turn is signed by the Axis root certificate. Both the root CA and intermediate CA are securely stored in cryptographic computing modules that are geographically separated. This prevents malicious extraction in case of a security breach at Axis production facilities. More information about the Axis PKI infrastructure can be found at *www.axis.com/support/public-key-infrastructure-repository*

Axis IEEE 802.1AR public-key infrastructure (PKI) for factory provisioning the Axis device ID during the manufacturing process. Axis device ID (1), which is a certificate incorporating the serial number of the product, is signed by an Axis device ID intermediate CA (2), which was signed by the Axis device ID root CA (3). Dedicated hardware security modules (HSM) are used for secure factory provisioning.

1 Reference
2 Sign

Example of an Axis device ID.

3.2 Secure network onboarding

When you buy an Axis device, you can perform a manual examination before you start using it. By visually inspecting the device and using prior knowledge about the look and feel of Axis products, you can be convinced that the device originates from Axis. However, you can do that type of inspection only if you have physical access to the device. So, when you communicate with a device over a network, how can you be sure that you are communicating with the correct device and be able to verify its identity? Neither networked equipment nor software on servers can perform a physical inspection. As a security measure, it has been common practice to first interact with a new device over a closed network, where it can be provisioned safely.

The Axis device ID provides your network with cryptographically verifiable proof that a specific device was produced by Axis and that the network connection to the device is indeed served by that very device. The Axis device ID can be used during the IEEE 802.1X network authentication process to gain access to a provisioning network where further software updates and configuration of the Axis device is performed before the Axis device is moved into the production network.

By using the Axis device ID, the overall security can be increased and time for deployment of devices can be reduced, since more automated and cost-efficient controls can be used for device installation and configuration.
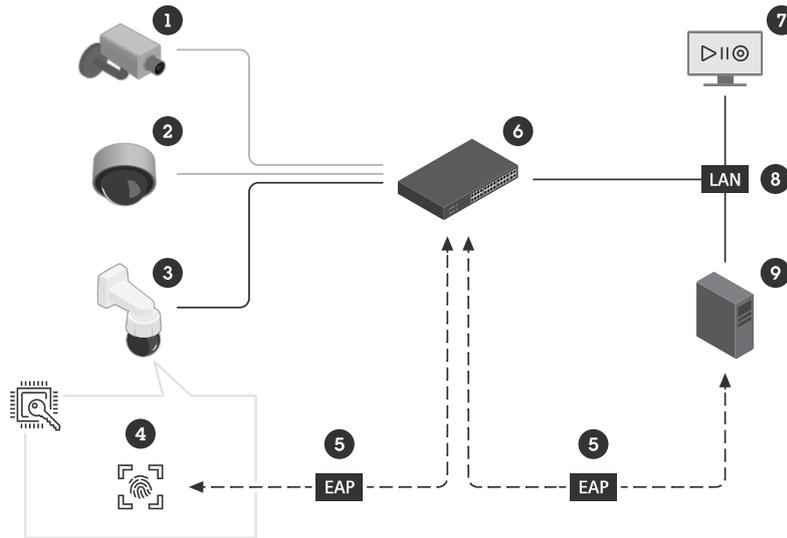
Secure network onboarding. You can instruct your authentication server (9) to automatically accept Axis devices (3) on to the network (8) and VMS (7). This is made possible by using the device serial numbers and Axis device ID (4) as a fingerprint or authentication.

1   Non-authorized device (must be onboarded manually)
2   Third-party device
3   Axis device
4   Axis device ID, securely stored in the tamper-protected secure keystore
5   802.1X EAP-TLS network authentication of the Axis device via Axis device ID certificate
6   Managed switch (authenticator)
7   VMS (device verification)
8   LAN protected by 802.1X
9   RADIUS (network authentication server)

More detailed description of the onboarding process. IEEE 802.1AR for secure device identity defines a method for how to identify a device (1) through IEEE 802.1X EAP requests (EAP-TLS) using a RADIUS server (3) to grant device access to the network.

1   Axis device
2   Managed switch (authenticator)
3   RADIUS server (network authentication server)
4   New connection
5   EAP-request identity
6   EAP-response identity, including Axis device ID certificate, IEEE 802.1AR IDevID
7   RADIUS access-request
8   RADIUS access-challenge
9   EAP-success

Apart from providing an additional, built-in source of trust, Axis device ID also provides a means to keep track of devices and allows for periodic verification and authentication according to zero-trust networking principles.
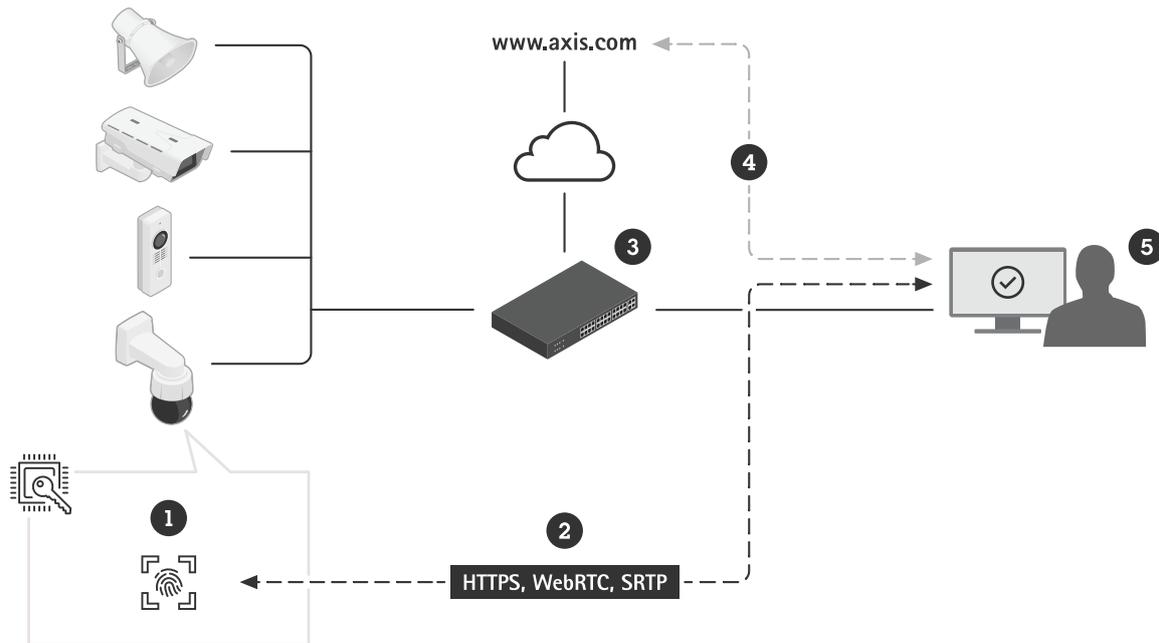
After a device has been securely onboarded, software applications (5) in other parts of the system can use the Axis device ID (1) and cryptographic operations to verify and authenticate the device in various TLS-based communication (2). The Axis device ID is verifiable by the publicly available Axis device ID root CA certificate (4).

1   *Axis device ID securely stored in the tamper-protected secure keystore*
2   *TLS-based communication (HTTPS, WebRTC, SRTP)*
3   *Managed switch*
4   *Axis device ID root CA certificate (downloadable at www.axis.com/support/public-key-infrastructure-repository*
5   *VMS or other software (device verification)*
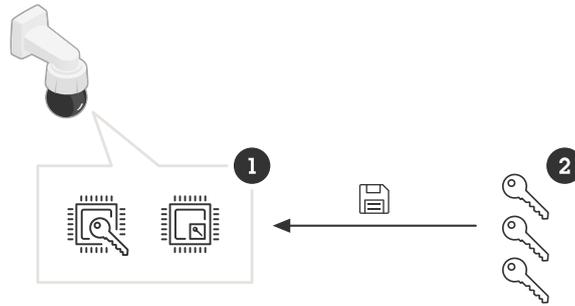
4   Secure key storage

Traditionally, sensitive X.509 cryptographic information (private keys) is stored in a device's file system. It is protected by the user account access policy only, which provides basic protection because the user account is not easily compromised. However, in the event of a security breach, this cryptographic information would be unprotected and accessible for an adversary.

From a security aspect, the secure keystore is critical for storing and protecting cryptographic information. Not only is the sensitive cryptographic information, included in the Axis device ID and signed video, stored in the secure keystore, but customer-loaded information can also be protected in the same manner.

4.1 Secure keystore

Sensitive cryptographic information (private keys) is stored in the device's hardware-based, tamper-protected secure keystore. This prevents malicious extraction even in the event of a security breach. Also, the private keys stay protected in the secure keystore even when they are being used. A potential adversary will not have access to the secure keystore, and cannot perform eavesdropping on network traffic, gain network access through IEEE 802.1X keys, or extract other private keys.

The secure keystore is provided through a hardware-based cryptographic computing module. Depending on the security requirements, an Axis device can have either one or multiple such modules, like a TPM 2.0 (Trusted Platform Module) or a secure element, and/or a TEE (Trusted Execution Environment).

The secure keystores (1) provide protection of private keys (2) and secure execution of cryptographic operations.

1   *Secure keystores, which can be a secure element, a TPM, or a TEE (on the SoC)*
2   *Private keys, such as Axis device ID, video signing key, access control keys, filesystem keys, and customer-loaded keys (such as IEEE 802.1X and HTTPS)*
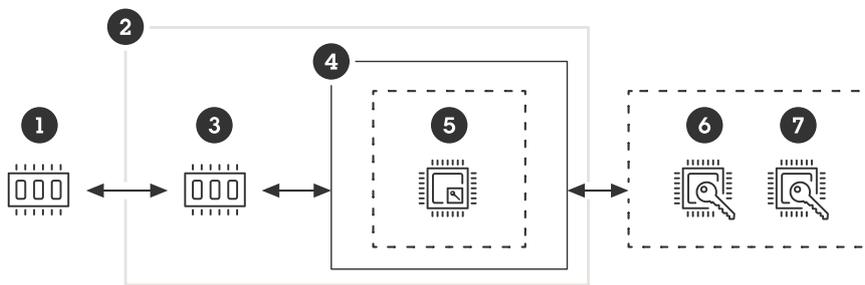
Devices with Axis Edge Vault hold hardware cryptographic computing modules (secure element (6) and TPM (7)) that are PCB-mounted right next to the SoC's main processor (4). The TEE (5) is a secure area of the SoC's main processor itself. The SoC-embedded boot ROM (3) is responsible for executing secure boot procedures and making sure that only signed OS software images from the flash memory (1) are used to boot the device.

1   *Flash memory (for signed OS, read-write file system)*
2   *SoC*
3   *Boot ROM (for secure boot)*
4   *CPU*
5   *TEE (for secure keystore)*
6   *Secure element (for secure keystore)*
7   *TPM (for secure keystore)*

The TPM, secure element, and TEE all provide protection of private keys and secure execution of cryptographic operations. In the event of a security breach, unauthorized access and malicious extraction are prevented.

4.2 Common Criteria and FIPS 140

Cryptographic computing modules may be certified using the Common Criteria Evaluation Levels (CC EAL) as well as the FIPS 140 compliance levels (1-4). These certifications are used to determine the correctness and integrity of cryptographic operations and to verify various tamper-countermeasures, such as self-verification, tamper resistance, and other resistance measures. You can find information about the certification on the datasheet of an Axis device or in the *Axis product selector*. Axis requires its incorporated hardware cryptographic computing modules to be certified at least according to Common Criteria EAL4 and/or FIPS 140-2/3 Level 2/3.

4.2.1   Common Criteria

Common Criteria (CC) (also known as Common Criteria for Information Technology Security Evaluation) is an international standard (ISO/IEC 15408) for IT product security certification. Common Criteria provides a

framework for manufacturers and implementers to specify the security functional and assurance requirements as Security Targets, which can be grouped into Protection Profiles.

These claimed Security Targets are then evaluated by certified independent testing laboratories before being listed as certified products in the Common Criteria database. The requirements on and thoroughness of evaluation by the testing lab are conveyed through an assigned EAL (Evaluation Assurance Level) ranging from EAL 1 — functionally tested, to EAL 7 — formally verified design and tested. This means that Common Criteria can span from operating systems and firewalls to TPMs and passports.

More details about the certification requirements of Common Criteria can be found at the Common Criteria website, *www.commoncriteriaportal.org/*

4.2.2 FIPS 140

FIPS (Federal Information Processing Standards) 140-2 and 140-3 are information security standards for cryptographic computing modules and the use of cryptographic algorithms, issued by NIST (National Institute of Standards and Technology) and adopted as a requirement by US and Canadian federal governments. FIPS 140-3 supersedes FIPS 140-2 in 2019 as its updated version. 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 computing module, approved algorithms, approved modes of operation, and power-up tests.

Customers can be assured that their products can be operated according to government specifications. This gives customers peace of mind when audits from government authorities are performed. Organizations that are not FIPS 140-regulated are ensured that their product adhere to government-defined standards. More details about the certification requirements of FIPS 140-2 and FIPS 140-3 can be found at the NIST website *www.nist. gov*

For a complete system to be FIPS 140-compliant, every component of the system needs to comply with FIPS 140. For example, the video management system, the recording server, as well as connected devices such as cameras, would need to comply. A device is FIPS 140-compliant when at least either a software-certified or a hardware-certified module is used.

Axis devices with AXIS OS version 12 or later feature the FIPS 140-certified, software-based (OpenSSL) Axis cryptographic module. Most new Axis devices incorporate both a FIPS 140-certified hardware cryptographic module, as well as the software-based cryptographic module. This enables the optimal solution of using the software-certified module for serving software-based applications such as HTTPS and IEEE 802.1X on the operating system level, together with the hardware-certified module for secure key storage.
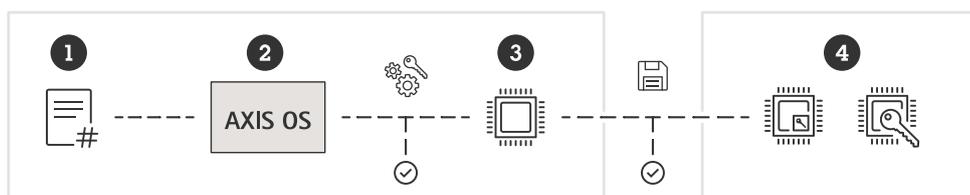
Use of FIPS 140-compliant cryptographic software and hardware modules in an Axis device. Applications (1) are served through the Axis cryptographic module, embedded in AXIS OS (2) of the Axis device. The Axis cryptographic module performs cryptographic operations, both symmetric and asymmetric, utilizing the SoC (3) and/or the embedded hardware-based cryptographic computing modules (4) for secure key storage.

1   *Applications that require cryptography or are TLS-based (such as HTTPS, webRTC, and 802.1X)*
2   *AXIS OS with embedded software-based cryptographic module (NIST certificate: https://csrc.nist.gov/ projects/cryptographic-module-validation-program/certificate/4621*
3   *SoC*
4   *Embedded hardware-based cryptographic computing modules*

4.3 Protection of private keys

For an adversary, extracting the private key would allow them to eavesdrop on HTTPS-encrypted network traffic, or pretend to be the actual device and get access to an 802.1X-protected network.

Axis devices support various TLS-based (Transport Layer Security) protocols for secure communication. Axis device ID (IEEE 802.1AR), HTTPS (network encryption), and 802.1X (network access control) rely on X.509 cryptographic information protection.

The X.509 digital certificates of TLS use a certificate and corresponding public and private key pair for two hosts in the network to communicate. The private key is stored in the secure keystore and never leaves it, even while it is used to decrypt data. The actual certificate and public key are known, can be shared by the Axis device, and are used to encrypt data.

## 4.4 Protection of access control keys

The protection of the cryptographic information used in Axis access control solutions, such as Open Supervised Device Protocol (OSDP) Secure Channel is another example of why hardware-protected key storage is important.

OSDP Secure Channel is a widely used AES-128 based encryption and authentication scheme to protect communication between door controllers and peripheral devices such as readers.

The AES symmetric key, Secure Channel Base Key (SCBK), shared by door controller and reader, is used to initiate the mutual authentication, and later generate a set of session keys to encrypt the communication data between door controllers and readers.

To achieve true end-to-end security, the Master Key (MK) and the SCBK need to be securely stored within the secure keystore of the Axis network door controller. The Master Key derives a unique SCBK key per connected Axis reader. Also, the individual SCBK, which is distributed securely during the installation phase to an Axis reader, needs to be securely stored in the secure keystore of the reader. The reader is more critical, considering it is normally installed on the unsecure side of the door.

In this way, the OSDP Secure Channel keys are protected at both ends in a hardware-protected environment. This prevents malicious extraction even in the event of a security breach.
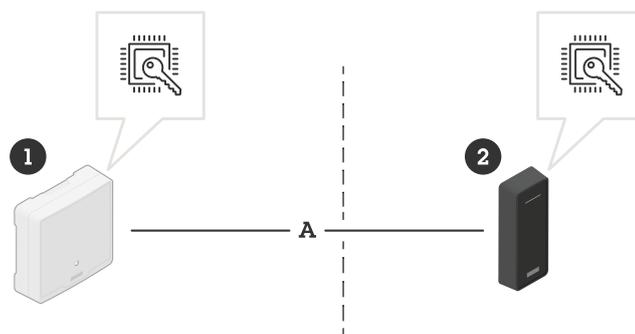
Achieving end-to-end security with secure keystore in access control. The master key and the individual secure channel base key (SCBK) are both stored in secure keystores, in devices on each side of the door.

1   *Axis door controller installed on the secure side of the door*
2   *Axis reader installed on the unsecure side of the door*
3   *OSDP secure channel communication*

4.5 Protection of the filesystem keys

An Axis device in operation carries customer-specific configuration and information. The same is true for when the Axis device is in transit to the customer from a distributor or system integrator that provided pre-configuration services. When physical access to the Axis device is achieved, a malicious adversary could try to

extract information from the file system by demounting the flash memory and accessing it through a flash reader device. Therefore, protecting the read-writeable file system against extraction of sensitive information or configuration tampering is an important protection for when the Axis device has been stolen or intrusion is achieved.

The secure keystore prevents the malicious exfiltration of information and prevents configuration tampering by enforcing strong encryption upon the file system. When the Axis device is powered off, the information on the file system is encrypted. During the boot process, the read-write file system is decrypted with an AES-XTS-Plain64 256bit key so that the file system can be mounted and used by the Axis device. The file system encryption key is uniquely generated per device upon factory default and regenerated upon every following software update, meaning that the key is never the same throughout the device lifecycle.
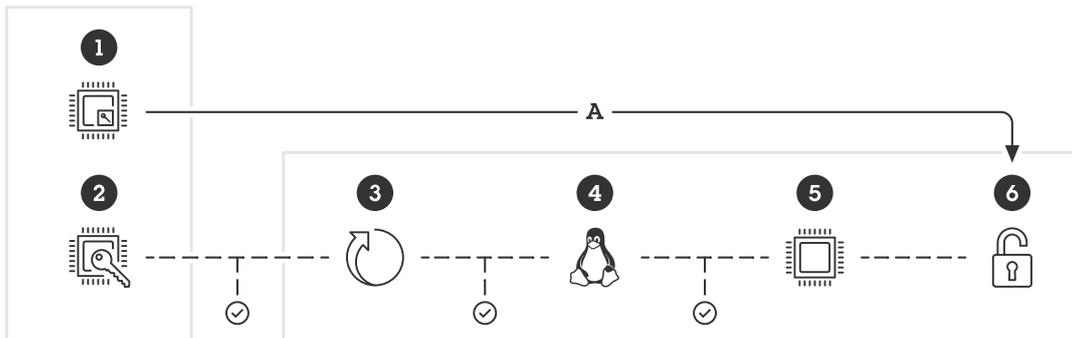

The TEE (1) and the boot ROM (2) are embedded on the SoC. During the boot process, the read-write file system (6) is decrypted (by the TEE) so that the file system can be mounted and used by the Axis device. In the boot process, each part of the chain: bootloader (3), Linux kernel (4), and root file system (5), is verified and authenticates the next sub-system in the flash memory. This ultimately results in a verified root file system.

1   *TEE*
2   *Boot ROM*
3   *Bootloader*
4   *Linux kernel*
5   *Root file system*
6   *Read-write file system*
7   *The TEE decrypts the read-write file system.*

5   Video tampering protection

A basic premise in the security industry is that video recorded by surveillance cameras is authentic and can be trusted. Signed video is a feature developed to maintain and further strengthen the confidence in video as evidence. By verifying video authenticity, the feature provides a means to ensure that video has not been edited or tampered with after it left the camera.
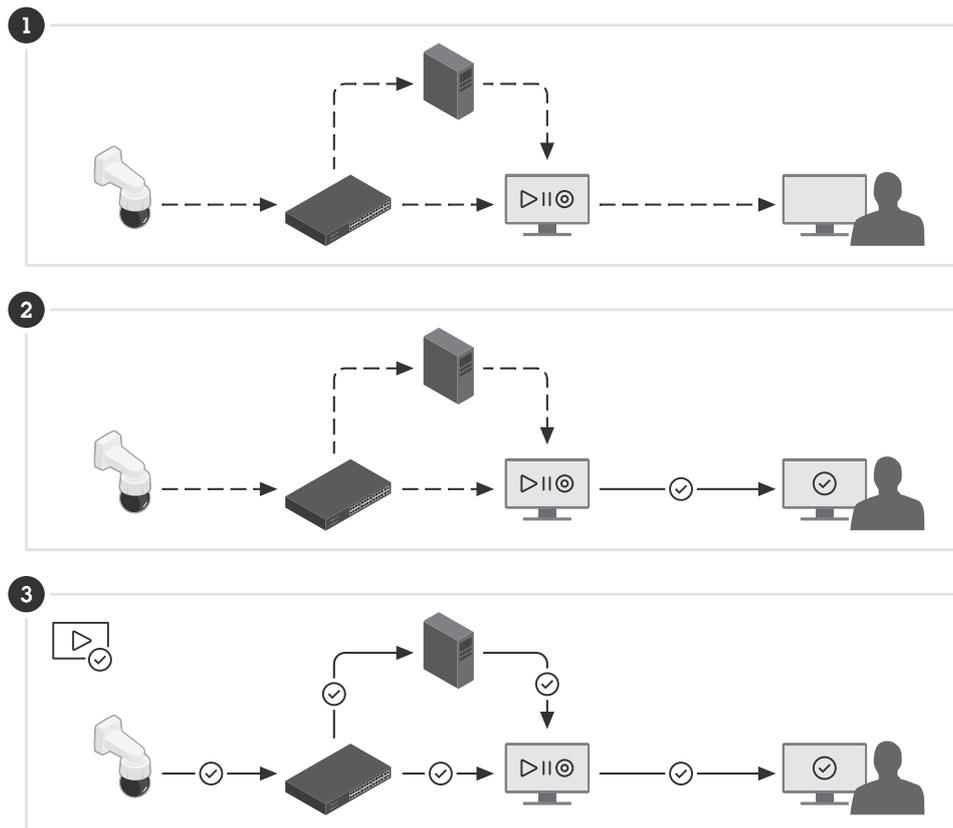
Verifying video authenticity.

1   A video passes many steps on its way from the camera to a person viewing the recording. A skilled attacker can tamper with the video in any of these transitions.
2   With VMS watermarking added to the video during export, some steps are verified but there is no guarantee that the video had not been tampered with on an earlier stage.
3   Signed video provides a means to make sure that the video has not been tampered with in any step on its way from the camera to a person viewing the exported recording. The video can be traced back to the device that recorded it.

5.1 Signed video

With the Axis-developed signed video feature, which was proactively open-sourced, a signature in the video stream can be used to safeguard that the video is intact and verify its origin by tracing it back to the camera that produced it. This makes it possible to prove the video authenticity without having to prove the chain of custody of the video file.

After an incident has been recorded by a security camera system, the police may receive the video as exported video files on a USB stick and save them in an EMS (evidence management system). While exporting the video from the camera, the police officer can see that the video is correctly signed. If it is later used in a prosecution process, the court can control and verify at what time the video was recorded, by which camera, and whether any video frames have been altered or removed. With *Axis signed media verifier*, anyone with a copy of the video can see this information.
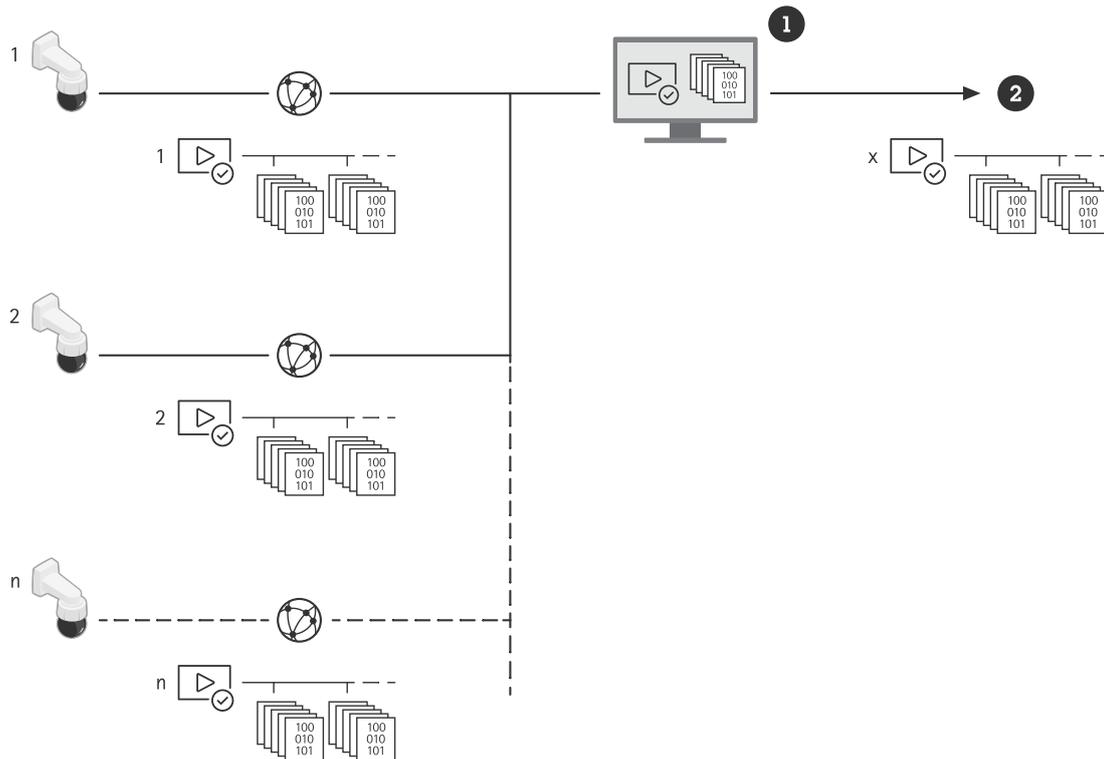
The signature is added already in the camera, enabling verification of the content at every step from the source to the final use of the video.

    1   *VMS*
    2   *Video export to CD/USB/web/email*

Each camera uses its unique video signing key, which is stored in the secure keystore, to add a signature into the video stream. This is done by computing a hash of each video frame, including metadata, and signing the combined hash. The signature is then stored in the stream in dedicated metadata fields (the SEI header).
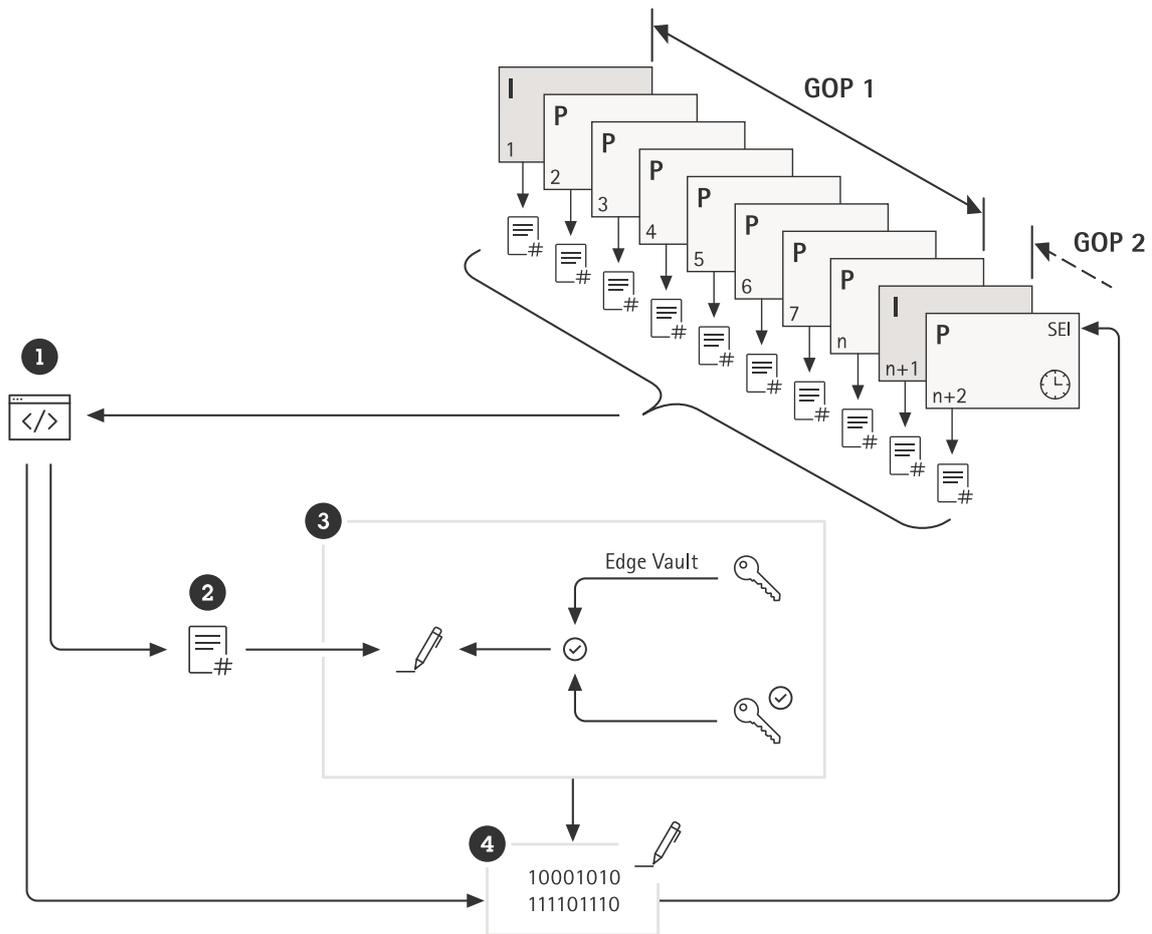
A graphical representation of how a signature is added to the video stream. The content of each frame of a group of pictures (GOP) is hashed together with a hash of metadata (1). This forms the GOP hash (2), which is signed in Edge Vault (3) using the device-unique video signing key and attestation key. The digital signature (4) and metadata (1) are then added to a later SEI header that is transported along the stream.

1   Device-unique metadata (hardware ID, AXIS OS version, serial number, and attestation report*) and stream metadata (GOP counter and frame hashes)
2   GOP hash
3   Axis Edge Vault
4   Digital signature

* The attestation report can be used to verify the origin and provenance of the key pair used for signing. By verifying the key attestation one can ensure that the key is securely stored in hardware in a specific device. This secures the origin of the video.

The actual signing is done using a device-unique video signing key that is attested using a device-unique attestation key. The attestation report is attached to the stream at start and then at periodic intervals, typically once every hour. Since the metadata contains each individual frame hash, it is possible to detect which individual frame is correct. To make the signing complete, the group of pictures (GOP) structure of the video must be protected. This is done by including the hash of the first I-frame of the next GOP, in the signature. This prevents undetectable cuts or reordering of the frames. In the unlikely event that frames are lost during streaming, or damaged during storage, this can be flagged in the same way.

6   Glossary

Axis device ID: a device-unique certificate with corresponding keys that can prove the authenticity of an Axis device. The Axis device is factory-provisioned with an Axis device ID that is stored in the secure keystore. Axis device ID is based on the international standard IEEE 802.1AR (IDevID, Initial device identifier), which defines a method for automated, secure identification.

Axis Edge Vault: the hardware-based cybersecurity platform that safeguards the Axis device. It builds on a strong foundation of cryptographic computing modules (secure element and TPM) and SoC security (TEE and secure boot), combined with expertise in edge device security.

Certificate: a signed document that attests the origin and properties of a public/private key pair. The certificate is signed by a Certificate Authority (CA), and if the system trusts the CA, 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.

Common Criteria (CC): an international standard for IT product security certification. Also referred to as Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408.

FIPS 140: a series of U.S. computer security standards that are used to approve cryptographic computing modules. FIPS (Federal Information Processing Standard) 140 defines requirements on how a cryptographic module should be designed and implemented to mitigate risks of module tampering.

Immutable ROM (read-only memory): the read-only memory that safely stores the trusted public keys and the program that is used to compare signatures, so that they cannot 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.

Secure boot: a feature to prevent the loading of unauthorized software during startup of the device. Secure boot uses signed OS that ensures that only authorized Axis software is used to boot the device.

Secure element: a cryptographic computing module that provides hardware-based, tamper-protected storage of private keys and secure execution of cryptographic operations. Unlike the TPM, the hardware- and software interfaces of a secure element are non-standardized but manufacturer-specific.

Secure keystore: a tamper-protected environment for the protection of private keys and secure execution of cryptographic operations. It prevents unauthorized access and malicious extraction in the event of a security breach. Depending on security requirements, an Axis device can have either one or multiple hardware-based cryptographic computing modules, which provide a hardware-protected secure keystore.

Signed OS or signed operating system: device software whose file image has been digitally code-signed by a trusted party. Signed OS is a requirement in the secure boot process to ensure the device is booting only from a trusted software image. In AXIS OS-based products, the device verifies the integrity and authenticity of the device software image prior to performing an update.

Signed video: a feature that maintains and strengthens the confidence in video as evidence. Signed video provides video tampering detection and authenticity and is used to safeguard that the video is intact and traceable back to a particular Axis camera. The signing keys for signed video reside within the secure keystore of the Axis device.

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

Trusted Execution Environment (TEE): provides hardware-based, tamper-protected storage of private keys and secure execution of cryptographic operations. Unlike secure element and TPM, the TEE is a secure, hardware isolated area of the system-on-chip's (SoC) main processor.

Trusted Platform Module (TPM): a cryptographic computing module that provides hardware-based, tamper-protected storage of private keys and secure execution of cryptographic operations. TPMs are internationally standardized (TPM 1.2, TPM 2.0) computer components defined by the *Trusted Computing Group (TCG)*.

Zero-trust security: a modern approach to IT security where connected devices and IT infrastructure (such as networks, computers, servers, cloud-services, and applications) need to recurrently identify, validate, and authenticate each other to achieve high security controls.

About Axis Communications

Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 5,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.

AXIS
COMMUNICATIONS