DOCUMENTO TÉCNICO

Axis Edge Vault

Es la plataforma de ciberseguridad basada en hardware que protege los dispositivos de Axis. Estas son las ventajas que aporta:

— Identidad de dispositivos validada

— Almacenamiento seguro de claves

— Detección de manipulación del vídeo

— Protección de la cadena de suministro

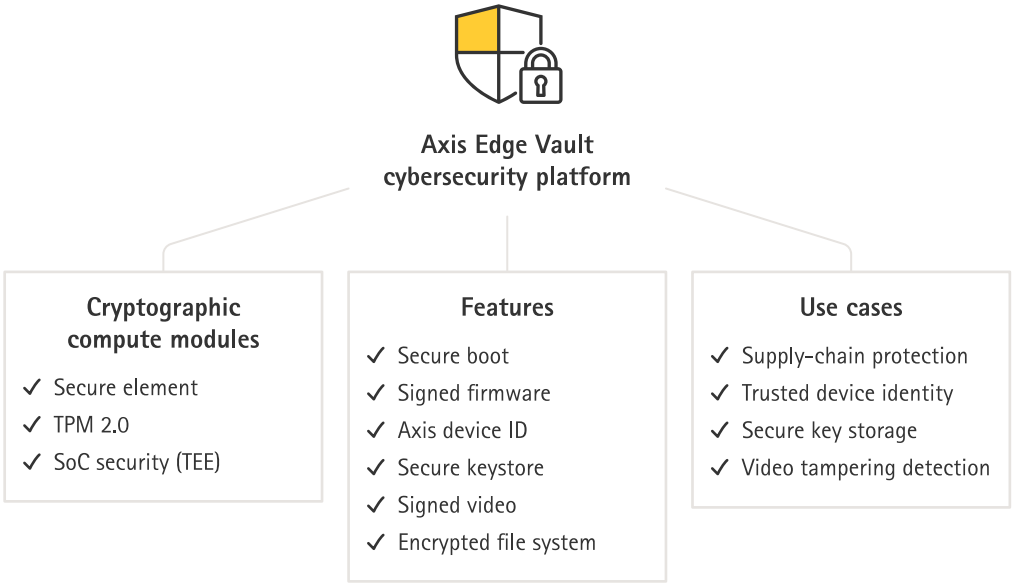
Abril 2023

AXIS COMMUNICATIONS

Resumen

Axis Edge Vault es una plataforma de ciberseguridad basada en hardware que protege el dispositivo Axis. Tiene dos sólidos pilares: los módulos de computación criptográfica (elemento seguro y TPM) y la seguridad del SoC (TEE y arranque seguro), combinados con una amplia experiencia en la seguridad de los dispositivos en el extremo. La piedra angular de Axis Edge Vault es su sólida raíz de confianza, establecida por el *arranque seguro* y el *firmware firmado*. Estas funciones hacen posible una cadena ininterrumpida de software validado criptográficamente para la cadena de confianza, que es la base de todas las operaciones seguras.

Los dispositivos Axis con Axis Edge Vault minimizan la exposición de los clientes a riesgos de ciberseguridad, puesto que impiden la interceptación del tráfico y la extracción maliciosa de información delicada. Además, con Axis Edge Vault el cliente tiene la garantía de que añade a su red un dispositivo validado y de confianza.



- **Identidad de dispositivos validada**: la posibilidad de verificar el origen del dispositivo es fundamental para poder confiar en su identidad. Durante la producción, se asigna a los dispositivos con Axis Edge Vault un certificado de ID de dispositivo de Axis único y conforme con el estándar IEEE 802.1AR en la propia fábrica. Es como una especie de pasaporte para demostrar el origen del dispositivo. El ID de dispositivo se guarda de forma segura y permanente en el almacén de claves seguro como certificado firmado por el certificado raíz de Axis. La infraestructura de TI del cliente puede utilizar el ID de dispositivo para el onboarding automático y la identificación segura del dispositivo.
- **Almacenamiento seguro de claves**: el almacén de claves seguro es un espacio de almacenamiento para la información criptográfica que está integrado en el hardware y protegido frente a manipulaciones. Garantiza la seguridad del ID de dispositivo de Axis y también de la información criptográfica cargada por el cliente e impide el acceso sin autorización y la extracción maliciosa en caso de que se produzca un incidente de seguridad.
- **Detección de manipulación del vídeo**: El vídeo firmado permite verificar que no se han manipulado las pruebas de vídeo sin necesidad de demostrar la cadena de custodia del archivo de vídeo. Cada vídeo utiliza su propia clave de firma de vídeo única, almacenada de forma segura en el almacén de claves seguro, para añadir una firma a la transmisión de vídeo. Cuando se reproduce el vídeo, el reproductor de

archivos muestra si el vídeo está intacto. El vídeo firmado permite conectar el vídeo con la cámara de origen y verifica que el vídeo no se ha manipulado tras salir de la cámara.

- **Protección de la cadena de suministro**: Axis Edge Vault necesita una base segura que actúe como raíz de confianza. Sin el arranque seguro y el firmware firmado, no posible establecer la cadena de la raíz de confianza. El arranque seguro, junto con el firmware firmado, crean una cadena ininterrumpida de software validado criptográficamente, empezando por la memoria inmutable (ROM de arranque). Arranque seguro significa que un dispositivo solo puede arrancar con firmware firmado por Axis, lo que cierra la puerta a una manipulación de la cadena de suministro física. Con el firmware firmado, el dispositivo puede validar también el nuevo firmware antes de aceptar instalarlo. Si detecta que se ha vulnerado su integridad o que no ha sido firmado por Axis, se rechazará la actualización. Su objetivo es proteger los dispositivos frente a las manipulaciones del firmware.

Índice

1 Introducción

Axis sigue las prácticas de referencia en el sector en todo lo relacionado con la seguridad de los productos. El objetivo es doble: minimizar la exposición de los clientes a los riesgos de ciberseguridad y dar las máximas garantías de seguridad al integrar el dispositivo Axis en la red del cliente.

Axis Edge Vault es una plataforma de ciberseguridad basada en hardware que protege el dispositivo Axis. Tiene dos sólidos pilares: los módulos de computación criptográfica (elemento seguro y TPM) y la seguridad del SoC (TEE y arranque seguro), combinados con una amplia experiencia en la seguridad de los dispositivos en el extremo.

Este documento técnico detalla el modelo multicapa de Axis para garantizar la seguridad de sus dispositivos y repasa también los riesgos más habituales y cómo prevenirlos. Axis Edge Vault necesita una base segura que actúe como raíz de confianza. Por este motivo, vamos a analizar también aspectos relacionados con la seguridad de los dispositivos Axis en la cadena de suministro y por qué son tan importantes el firmware firmado y el arranque seguro para impedir las manipulaciones del firmware y en la cadena de suministro física.

En *https://www.axis.com/support/cybersecurity/resources* tiene más información sobre la seguridad de los productos, las vulnerabilidades descubiertas y las medidas que puede tomar para reducir los riesgos vinculados a las amenazas más habituales.

El último capítulo de este documento es un glosario.

2 Identidad de dispositivos validada

En las redes de seguridad de confianza cero actuales ("no confiar, verificar siempre"), es absolutamente imprescindible poder verificar el origen del dispositivo, su autenticidad y sus conexiones. Un dispositivo de red puede verificar su integridad y autenticidad de forma parecida a como nosotros mostramos nuestro pasaporte a las autoridades para verificar nuestra identidad en un aeropuerto.

2.1 Identificación segura de dispositivos con el ID de dispositivo de Axis

El estándar internacional *IEEE 802.1AR* define un método para automatizar la identificación de un dispositivo a través de una red y garantizar su validez. Si la comunicación se envía a un módulo de computación criptográfica integrada, el dispositivo puede devolver una respuesta de identificación fiable de acuerdo con el estándar. La infraestructura de red puede utilizar esta respuesta fiable para permitir el onboarding automático y seguro del dispositivo en una red de aprovisionamiento para la configuración inicial y las actualizaciones de firmware.

Con el objetivo de cumplir con el estándar IEEE 802.1AR, todos nuestros dispositivos incorporan un certificado de ID de dispositivo de Axis instalado en fábrica y de carácter único (identificador de dispositivo inicial IEEE 802.1AR, IDevID). El ID de dispositivo de Axis se guarda en un almacén de claves seguro protegido frente a manipulaciones que se encuentra en un módulo de computación criptográfica integrado

en el propio dispositivo. Esta identidad es única para cada dispositivo Axis y está diseñada para demostrar el origen del dispositivo.

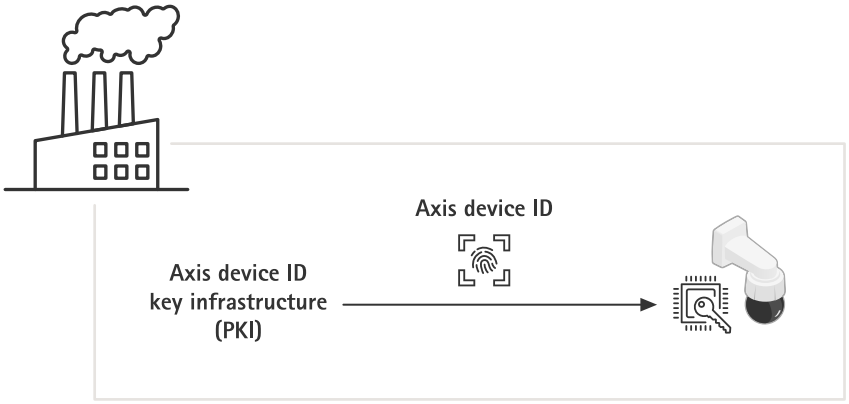


Figure 1. Durante el proceso de fabricación de una unidad, se guarda el ID de dispositivo de Axis único en el almacén de claves seguro de la unidad.

El estándar IEEE 802.1AR se basa en el estándar IEEE 802.1X para el control de acceso a redes, que está activado de forma predeterminada en los dispositivos Axis con el ID de dispositivo de Axis preseleccionado. Esto abre la puerta a la identificación y autenticación seguras del dispositivo Axis en una infraestructura de TI compatible con 802.1X, incluso con los ajustes predeterminados de fábrica.

El ID de dispositivo de Axis se presenta con diferentes configuraciones criptográficas (RSA de 2048 bits, RSA de 4096 bits, ECC-P256). Están activadas por omisión para permitir las conexiones e identificación seguras del dispositivo a través del control de acceso a la red IEEE 802.1X y también de HTTPS.

Axis gestiona su propia infraestructura de clave pública (PKI) IEEE 802.1AR para el aprovisionamiento en fábrica del ID de dispositivo de Axis durante el proceso de fabricación. El ID de dispositivo de Axis está firmado por el certificado intermedio, que a su vez está firmado por el certificado raíz de Axis. Tanto la CA raíz como la CA intermedia se guardan en módulos de computación criptográfica, que están separados geográficamente. De este modo, evitamos posible extracciones de información por parte de actores maliciosos en el caso de que se produzca algún incidente de seguridad en

el centro de producción de Axis. Tiene más información sobre la infraestructura PKI de Axis en *www.axis.com/support/public-key-infrastructure-repository*

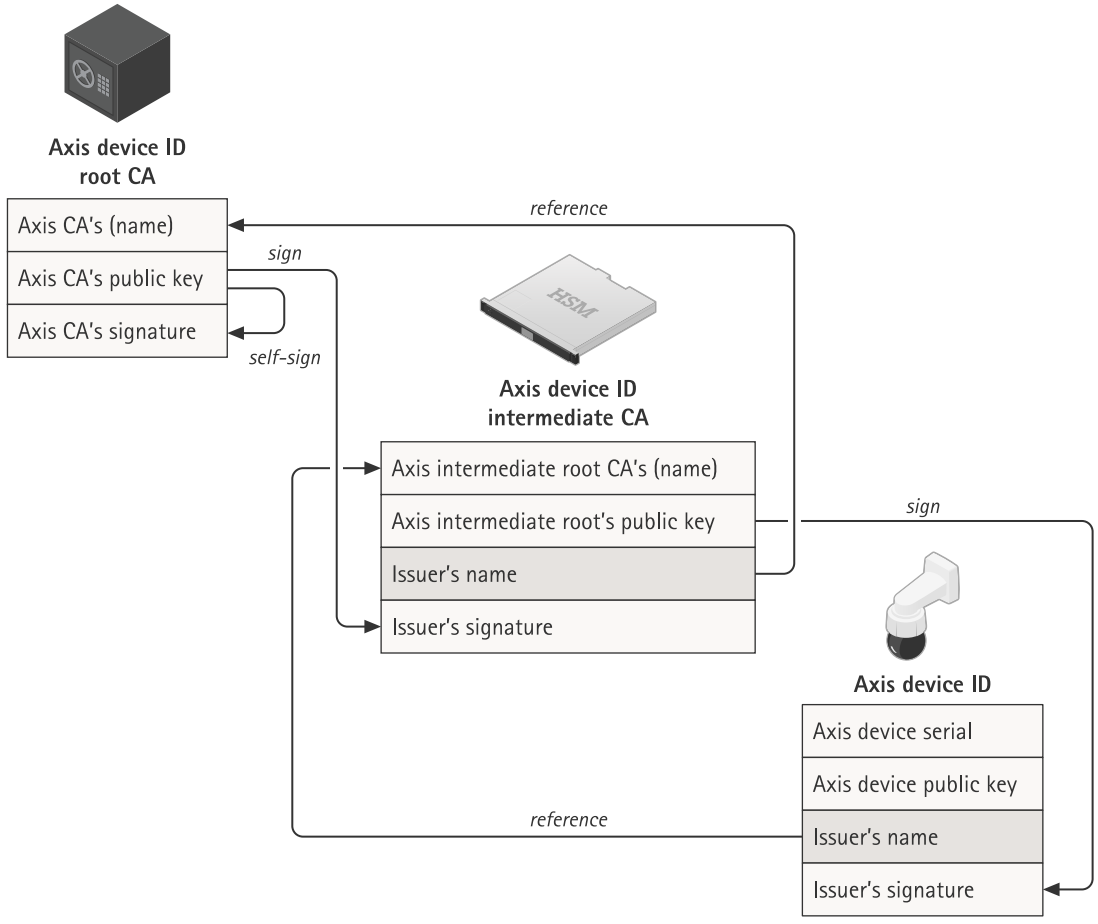


Figure 2. La infraestructura de clave pública (PKI) IEEE 802.1AR de Axis para el aprovisionamiento en fábrica del ID de dispositivo de Axis durante el proceso de fabricación. El ID de dispositivo de Axis, que es un certificado con el número de serie del producto, está firmado por una CA intermedia, firmado a su vez por la CA raíz del ID de dispositivo de Axis. Como la CA raíz de Axis tiene un valor enorme y debe guardarse en una caja fuerte, se necesita la CA intermedia durante el aprovisionamiento en fábrica.

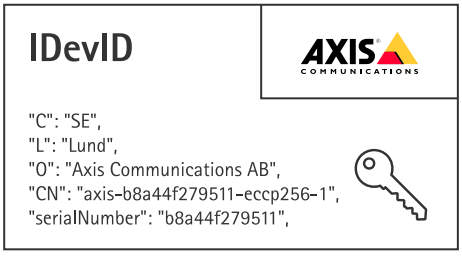


Figure 3. Ejemplo de un ID de dispositivo de Axis.

2.2 Onboarding a través de una red segura

Cuando compra un dispositivo Axis, puede examinarlo antes de empezar a usarlo. A través de la inspección visual y también de su experiencia previa con otros productos Axis, puede tener la seguridad de que el dispositivo es realmente de Axis. Sin embargo, este tipo de inspección previa solo es posible si tiene acceso físico al dispositivo. Pero, ¿qué pasa cuando se comunica con un dispositivo a través de una red? ¿Cómo puede tener la seguridad de que se está comunicando con el dispositivo correcto y verificar su identidad? Ni el equipo de red ni el software de los servidores pueden realizar una inspección física. Como medida de seguridad, habitualmente se empieza por iniciar la interacción con un nuevo dispositivo en una red cerrada, lo que permite un aprovisionamiento seguro.

El ID de dispositivo de Axis ofrece a su red una prueba verificable criptográficamente de que un dispositivo concreto ha sido producido por Axis y que la conexión de red al dispositivo tiene al otro lado efectivamente ese dispositivo. Se puede usar el ID de dispositivo de Axis durante el proceso de autenticación de red IEEE 802.1X para acceder a una red de aprovisionamiento donde se llevan operaciones de actualización del firmware y configuración del dispositivo Axis antes de que este dispositivo se incorpore a la red de producción.

Al utilizar el ID de dispositivo de Axis, aumenta la seguridad general y se reduce el tiempo de implantación de los dispositivos, porque pueden utilizarse controles más automatizados y eficientes para la instalación y la configuración.

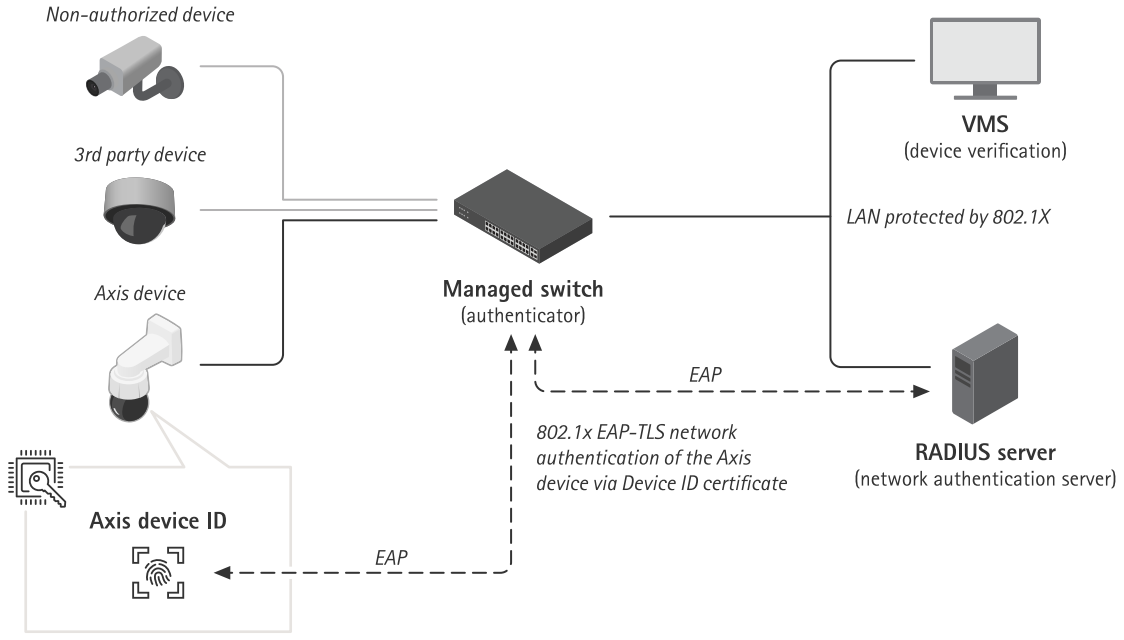


Figure 4. Onboarding a través de una red segura. Puede ordenar a su servidor de autenticación que acepte automáticamente los dispositivos Axis en la red usando los números de serie del dispositivo y el ID de dispositivo de Axis. En este contexto, el ID de dispositivo de Axis se convierte en una huella dactilar que garantiza el onboarding seguro y automático de los dispositivos. En el caso de los dispositivos no autorizados, el onboarding debe realizarse manualmente.

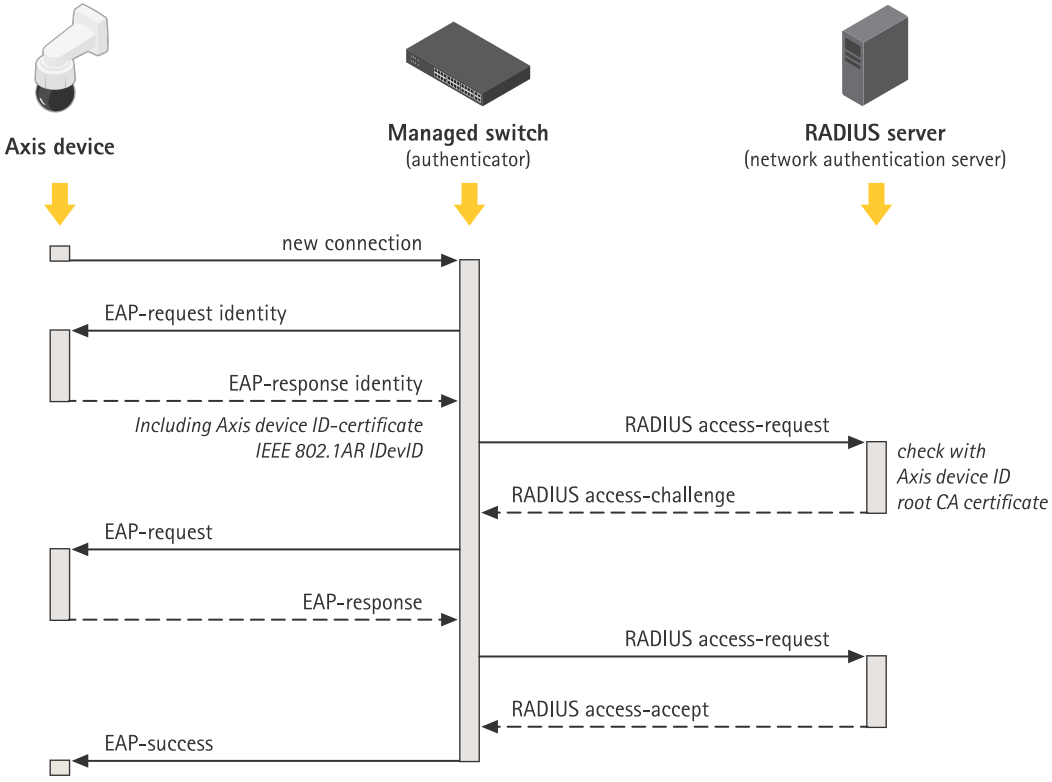


Figure 5. Descripción más detallada del proceso de onboarding. IEEE 802.1AR para la identidad segura del dispositivo define un método para identificar un dispositivo a través de peticiones del Extensible Authentication Protocol IEEE 802.1X (EAP-TLS) usando un servidor Remote Authentication Dial-In User Service (RADIUS) para dar acceso al dispositivo a la red.

El ID de dispositivo de Axis, una fuente de la verdad adicional integrada en el propio dispositivo, también permite supervisar los dispositivos y llevar a cabo operaciones de verificación y autenticación periódicamente según los principios de redes de conocimiento cero.

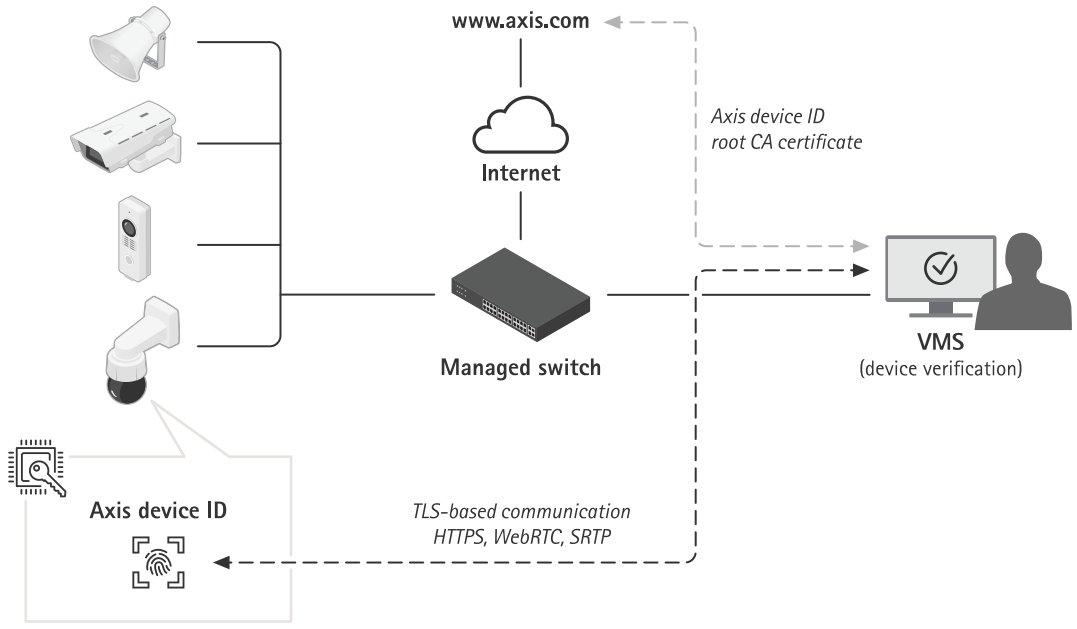


Figure 6. Una vez realizado el onboarding seguro de un dispositivo, las aplicaciones de software de otras partes del sistema pueden usar el ID de dispositivo de Axis y las operaciones criptográficas para verificar el dispositivo en distintas comunicaciones a través de TLS. El ID de dispositivo de Axis se puede verificar mediante el certificado CA raíz del ID de dispositivo de Axis de carácter público, que puede descargarse desde axis.com.

3 Almacenamiento seguro de claves

La información criptográfica X.509 delicada (claves privadas) suele guardarse en el sistema de archivos de un dispositivo. Está protegida únicamente por la política de acceso a la cuenta del usuario, que ofrece una protección básica porque no es fácil hackear la cuenta del usuario. Sin embargo, cuando hay un incidente de seguridad, esta información criptográfica puede quedar desprotegida y un actor malicioso podría acceder a ella.

Desde el punto de vista de la seguridad, el almacén de claves seguro es imprescindible para guardar y proteger la información criptográfica. Allí no se guarda solo información criptográfica delicada incluida en el ID de dispositivo de Axis y el vídeo firmado. La información cargada por el usuario puede disfrutar de este mismo nivel de protección.

3.1 Almacén de claves seguro

La información criptográfica más sensible (las claves privadas) se guarda en el almacén de claves seguro del dispositivo, un elemento de hardware protegido contra manipulaciones. De este modo, se evitan las extracciones maliciosas incluso en caso de incidentes de seguridad. Además, las claves privadas se mantienen a salvo en el almacén de claves seguro, incluso mientras se están utilizando. Un actor malicioso no tendrá acceso al almacén de claves seguro y no podrá interceptar el tráfico de red, acceder a la red a través de claves IEEE 802.1X ni extraer otras claves privadas.

El almacén de claves reside en un módulo de computación criptográfica basado en hardware. En función de los requisitos de seguridad, un dispositivo Axis puede tener uno o varios módulos de este tipo, como un TPM 2.0 (Trusted Platform Module) o un elemento seguro y/o un TEE (Trusted Execution Environment).

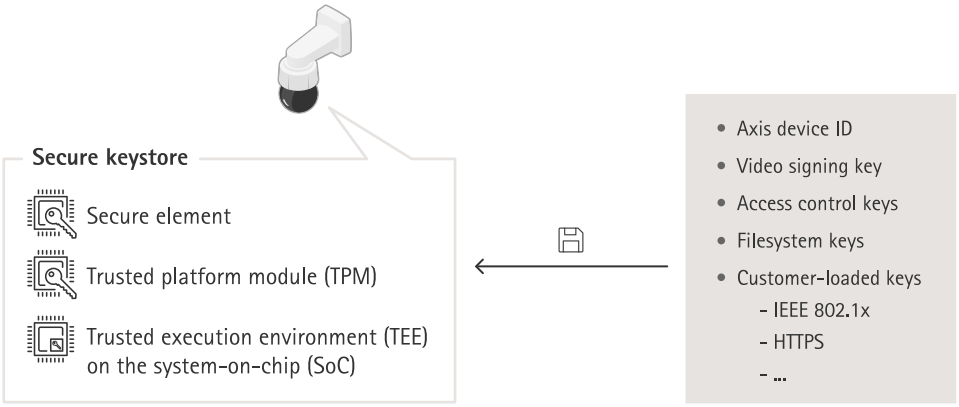


Figure 7. En el almacén de claves seguro de los dispositivos Axis se puede utilizar un elemento seguro, un TPM o un TEE. Todos protegen las claves privadas y garantizan la ejecución segura de operaciones criptográficas.

El TPM y el elemento seguro son módulos de computación criptográfica basados en hardware que se montan en la placa base justo al lado del procesador principal del SoC. El TEE es un área segura del propio procesador principal del SoC.

El TPM, el elemento seguro y el TEE protegen las claves privadas y garantizan la ejecución segura de operaciones criptográficas. En caso de que se produzca un incidente de seguridad, impiden el acceso sin autorización y la extracción maliciosa de información.

3.2 Common Criteria y FIPS 140

Los módulos de computación criptográfica pueden certificarse aplicando los Common Criteria Evaluation Levels (CC EAL) y también los niveles de conformidad FIPS 140 (1-4). Estas certificaciones se utilizan para determinar la corrección y la integridad de las operaciones criptográficas y para verificar diferentes medidas de protección contra manipulaciones, como la autoverificación, la resistencia a la manipulación y otras protecciones. Encontrará más información sobre la certificación en la hoja de datos de cada dispositivo Axis o en el selector de productos de Axis. Axis exige que los módulos de hardware de computación criptográfica integrados cuenten como mínimo con la certificación Common Criteria EAL4 y/o FIPS 140-2/3 de nivel 2.

3.2.1 Common Criteria

Common Criteria (CC) (también conocido como Common Criteria for Information Technology Security Evaluation) es un estándar internacional (ISO/IEC 15408) para la certificación de la seguridad de los productos tecnológicos. Common Criteria pone en manos de fabricantes e implementadores un marco para especificar los requisitos de funcionamiento y garantía bajo la etiqueta de objetivos de seguridad, que pueden agruparse en perfiles de protección.

Los objetivos de seguridad declarados son evaluados por laboratorios de pruebas independientes certificados, condición previa para convertirse en productos certificados y aparecer en la base de datos de Common Criteria. Los requisitos y la exhaustividad de la evaluación realizada por el laboratorio se reflejan en el EAL (Evaluation Assurance Level, nivel de garantía de evaluación) asignado, desde EAL 1 (pruebas de funcionamiento) hasta EAL 7 (verificación formal del diseño y pruebas). Por lo tanto, Common Criteria puede abarcar desde los sistemas operativos y los cortafuegos hasta los TPM y los pasaportes.

Encontrará más información sobre los requisitos de certificación Common Criteria en el sitio web de Common Criteria: *www.commoncriteriaportal.org/*

3.2.2 FIPS 140

Los estándares FIPS (Federal Information Processing Standard) 140-2 y 140-3 son estándares de seguridad de la información para los módulos de computación criptográfica creados por el NIST (National Institute of Standards and Technology), un organismo estadounidense de referencia. FIPS 140-3 sustituyó FIPS 140-2 en 2019. La validación por parte de un laboratorio de pruebas certificado por el NIST garantiza que el sistema del módulo y la criptografía del módulo están correctamente implementados. En resumen, la certificación requiere una descripción, especificación y verificación del módulo de computación criptográfica, algoritmos aprobados, modos de funcionamiento aprobados y pruebas de encendido.

Encontrará más información sobre los requisitos de certificación de FIPS 140-2 y FIPS 140-3 en el sitio web de NIST *www.nist.gov*

3.3 Protección de claves privadas

Si un actor malicioso consigue extraer la clave privada, podría interceptar tráfico de red con cifrado HTTPS o hacerse pasar por el dispositivo en cuestión y acceder a una red con protección 802.1X.

Los dispositivos Axis son compatibles con varios protocolos TLS (Transport Layer Security) para la comunicación segura. Estos protocolos se basan en la protección de información criptográfica X.509, como el ID de dispositivo de Axis (IEEE 802.1AR), HTTPS (cifrado de red) y 802.1X (control de acceso a la red), entre otros.

Los certificados digitales X.509 de TLS utilizan un certificado y el par de claves pública y privada correspondiente para la comunicación entre dos hosts en la red. La clave privada se guarda en el almacén de claves seguro y nunca sale de allí, aunque se utilice para descifrar la información. El certificado y la clave pública son conocidos, el dispositivo Axis puede compartirlos y se utilizan para cifrar la información.

3.4 Protección de las claves de control de acceso

La protección de la información criptográfica utilizada en las soluciones de control de acceso de Axis, como el Open Supervised Device Protocol (OSDP) Secure Channel, es otro ejemplo de por qué es importante contar con un almacenamiento de claves protegido por el hardware.

OSDP Secure Channel es un modelo de autenticación y cifrado basado en AES-128 de uso común para proteger la comunicación entre controladores de puertas y dispositivos periféricos como lectores.

Se utiliza la clave simétrica AES, Secure Channel Base Key (SCBK), compartida por el controlador de puerta y el lector para iniciar la autenticación mutua y generar un juego de claves de sesión para cifrar los datos de comunicación entre los controladores de puerta y los lectores.

Para una seguridad integral de extremo a extremo, es imprescindible guardar la clave maestra (MK) y la SCBK en el almacén de claves seguro del controlador de puerta en red Axis. La clave maestra se obtiene a partir de una clave SCBK única para cada lector Axis conectado. Asimismo, la SCBK individual, que se asigna de forma segura a un lector Axis durante la fase de instalación, debe guardarse también en el almacén de claves seguro del lector. En el caso del lector, la seguridad es todavía más crítica porque normalmente se instala en el lado de la puerta sin protección.

Con este sistema, se protegen las claves OSDP Secure Channel en ambos extremos de un entorno protegido por el hardware. De este modo, se evitan las extracciones maliciosas incluso en caso de incidentes de seguridad.

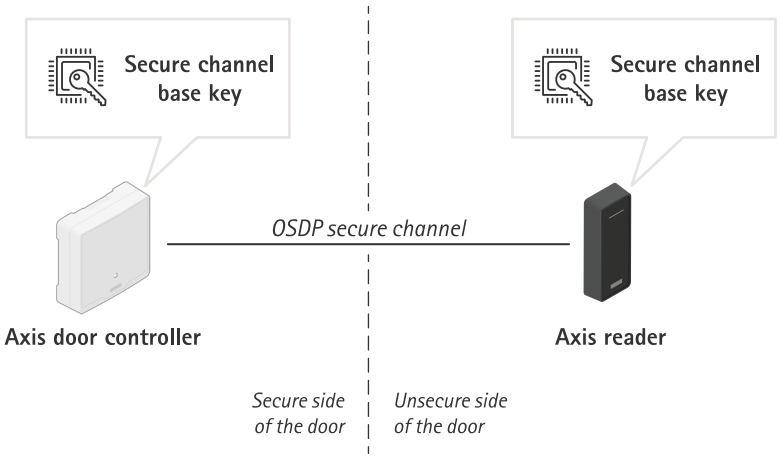


Figure 8. Uso de un almacén de claves seguro en control de acceso para una seguridad integral. Tanto la clave maestra como la Secure Channel Base Key (SCBK) se guardan en sendos almacenes de claves seguro, en dispositivos colocados a ambos lados de la puerta.

3.5 Protección de las claves del sistema de archivos

Un dispositivo Axis en funcionamiento tiene ajustes e información específicos del cliente. Lo mismo ocurre cuando un dispositivo Axis pasa al cliente después de que un distribuidor o integrador de sistemas haya preconfigurado unos servicios. Si consigue acceder físicamente al dispositivo Axis, un actor malicioso podría tratar de extraer información del sistema de archivos desmontando la memoria flash y utilizando un lector flash. Por lo tanto, es importante proteger el sistema de archivos de lectura/escritura para evitar la extracción de información confidencial y la manipulación de los ajustes en caso de robo del dispositivo Axis o acceso sin autorización al mismo.

El almacén de claves seguro impide la filtración maliciosa de información y evita que pueda manipularse la configuración aplicando un potente cifrado al sistema de archivos. Al apagar el dispositivo Axis, se cifra la información presente en el sistema de archivos. Durante el proceso de arranque, se descifra el sistema de archivos de lectura/escritura con una clave AES-XTS-Plain64 de 256 bits. Eso permite montar el sistema de archivos para que el dispositivo Axis pueda usarlo. La clave de cifrado del sistema de archivos se genera

para cada dispositivo en fábrica y vuelve a generarse con cada actualización de firmware, por lo que no es siempre la misma a lo largo de todo el ciclo de vida del dispositivo.

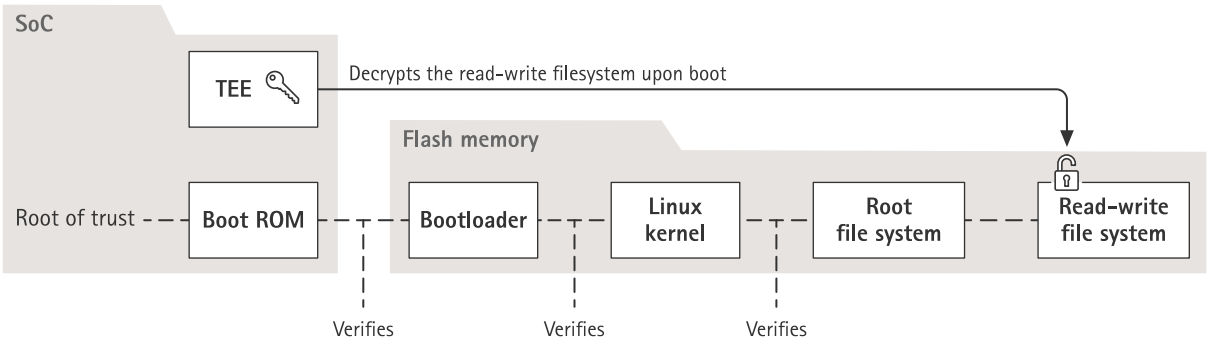


Figure 9. El TEE situado en el interior del SoC guarda la clave utilizada para descifrar el sistema de archivos raíz.

4 Protección para evitar la manipulación del vídeo

Una premisa básica en el sector de la seguridad es que el vídeo grabado con cámaras de vigilancia es auténtico y fiable. El vídeo firmado es una función desarrollada para mantener y reforzar aún más la confianza en el vídeo como prueba. Esta función permite verificar la autenticidad del vídeo, de modo que garantiza que no se ha editado ni manipulado desde que salió de la cámara.

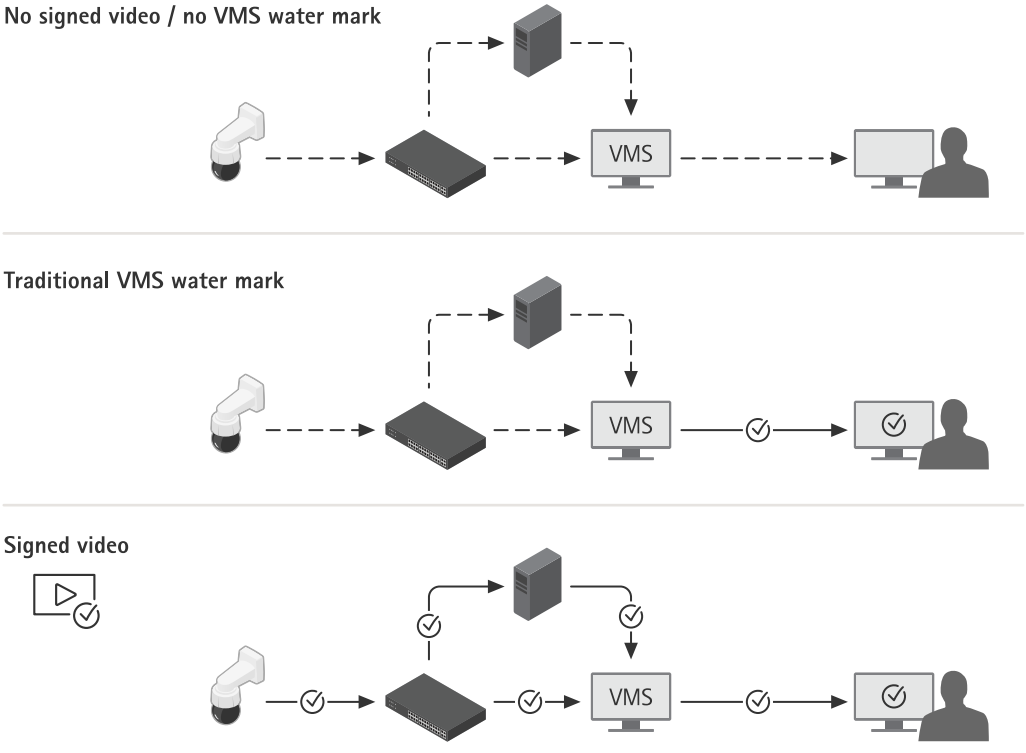


Figure 10. Verificación de la autenticidad del vídeo.

Vista superior: Un vídeo pasa por muchas fases desde que sale de la cámara hasta que llega a la persona que ve la grabación. Un atacante experto puede manipular el vídeo en alguna de estas transiciones.

Centro: Con la marca de agua que el VMS añade al vídeo durante la exportación, se verifican algunos pasos pero no hay garantía de que el vídeo no se haya manipulado en una fase anterior.

Vista inferior: El vídeo firmado garantiza que el vídeo no se ha manipulado en ningún paso desde que sale de la cámara hasta que lo ve la persona que mira la grabación exportada. Además, podemos saber de qué dispositivo ha salido el vídeo.

4.1 Vídeo firmado

Con la prestación de vídeo firmado de código abierto desarrollada por Axis, se puede utilizar la firma en una transmisión de vídeo para garantizar que el vídeo está intacto y también para comprobar su origen identificando la cámara con la que se grabó. De este modo, es posible demostrar la autenticidad del vídeo sin necesidad de verificar la cadena de custodia del archivo del vídeo.

Cuando un sistema de cámaras de seguridad graba un incidente, es probable que la policía reciba el vídeo en forma de archivos de vídeo exportados en una memoria USB y que los guarde en un EMS (sistema de gestión de pruebas). Al exportar el vídeo de la cámara, el agente de policía puede ver que el vídeo está correctamente firmado. Y si se utiliza más adelante en un proceso judicial, el tribunal puede ver y verificar a qué hora se grabó el vídeo, con qué cámara y si se han modificado o eliminado fotogramas. Con el reproductor de archivos de Axis, cualquier persona con una copia del vídeo puede ver esta información.

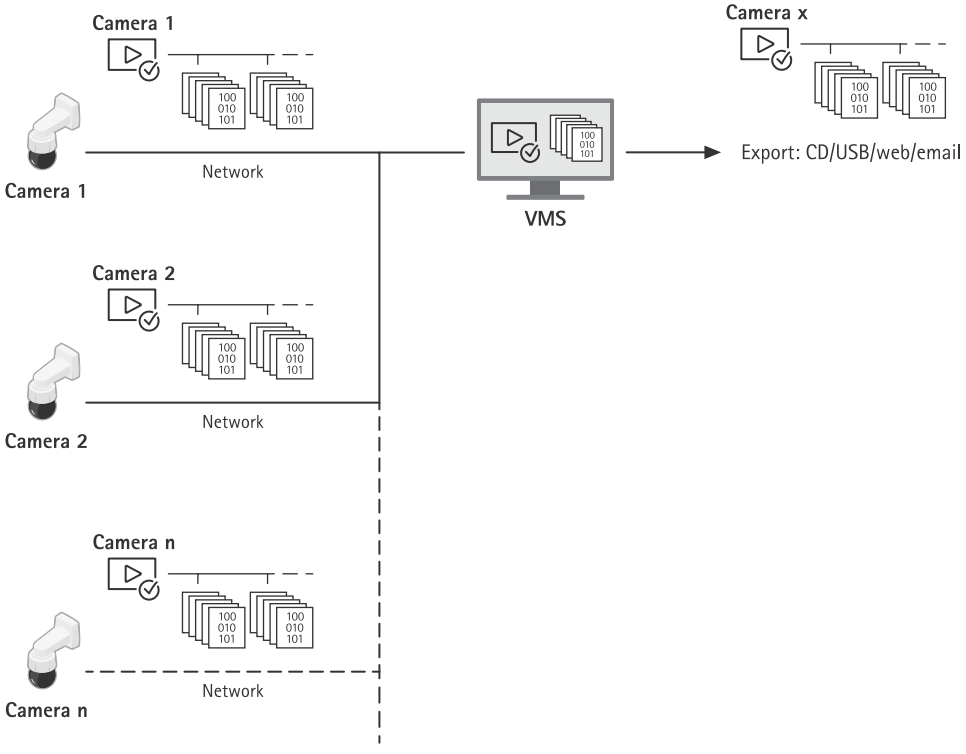


Figure 11. La firma se añade en la propia cámara, lo que permite verificar el contenido en todas y cada una de las fases, desde la fuente hasta el uso final del vídeo.

Cada vídeo utiliza su propia clave de firma de vídeo única, almacenada en el almacén de claves seguro, para añadir una firma a la transmisión de vídeo. Para firmar, se calcula un hash para cada fotograma de vídeo

(incluidos los metadatos) y se firma el hash combinado. Luego, la firma se guarda en la transmisión en unos campos de metadatos concretos (cabecera SEI).

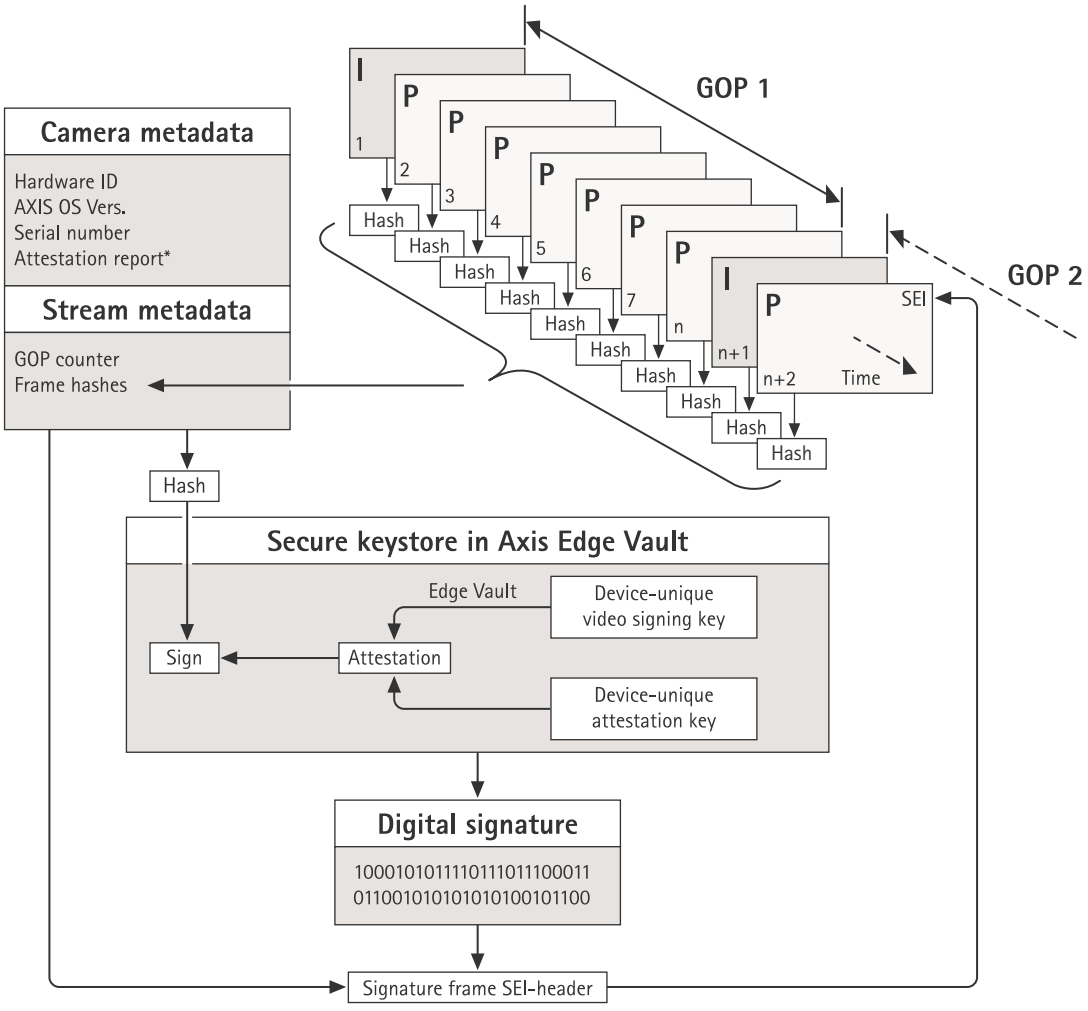


Figure 12. Representación gráfica de cómo se añade una firma a los metadatos del vídeo. El contenido de cada fotograma de un grupo de imágenes (GOP) se une con un hash de metadatos de la cámara y metadatos de la transmisión. El resultado es el hash del GOP, que se firma en Edge Vault. Luego, la firma y los metadatos se añaden a una cabecera SEI posterior, que se transporta junto con la transmisión.

* *Puede utilizarse el informe de autentificación para verificar el origen y la procedencia del par de claves utilizado para firmar. La verificación de la autentificación de la clave permite comprobar que la clave está almacenada de forma segura en el hardware de un dispositivo concreto. Esta información avala el origen del vídeo.*

La firma en sí se realiza utilizando una clave de firma de vídeo específica del dispositivo, que se certifica con una clave de certificación única del dispositivo. El informe de certificación se adjunta a la transmisión al inicio y a intervalos periódicos, normalmente una vez cada hora. Como los metadatos contienen el hash de cada fotograma, es posible detectar qué fotograma es correcto. Para completar el proceso de firma, es necesario proteger la estructura del grupo de imágenes (GOP) del vídeo. Y eso se consigue incluyendo el hash del primer fotograma I del GOP siguiente en la firma. De este modo, se evitan cortes no detectables o la reordenación de los fotogramas. Y en el improbable caso de que se pierdan fotogramas durante la transmisión o de que los contenidos sufran daños durante su almacenamiento, se notificará de la misma forma.

5 Protección de la cadena de suministro

Axis Edge Vault necesita una base segura que actúe como raíz de confianza. El proceso para establecer la raíz de confianza empieza durante el arranque del dispositivo. En los dispositivos Axis, el mecanismo de *arranque seguro* basado en el hardware verifica el sistema operativo (AXIS OS) desde el que arranca el dispositivo. A su vez, AXIS OS es firmado criptográficamente (*firmware firmado*) durante el proceso de creación.

El arranque seguro y el firmware firmado están profundamente unidos. Garantizan que el firmware no ha sido manipulado (por personas con acceso físico al dispositivo) antes de la implantación del dispositivo y que, una vez implantado, el dispositivo no instala actualizaciones de firmware con riesgos de seguridad. Juntos, el arranque seguro y el firmware firmado crean una cadena ininterrumpida de software validado criptográficamente para la cadena de confianza, que es la base de todas las operaciones seguras.

5.1 Arranque seguro

El mecanismo de arranque seguro es un proceso de arranque que consta de una cadena ininterrumpida de software validado criptográficamente, comenzando por la memoria inmutable (ROM de arranque). Arranque seguro significa que un dispositivo solo puede arrancar con firmware autorizado.

La ROM de arranque valida el cargador de arranque e inicia el proceso de arranque. A continuación, el arranque seguro comprueba, en tiempo real, las firmas integradas de cada bloque de firmware que se carga desde la memoria flash. La ROM de arranque sirve como raíz de confianza y el proceso de arranque continúa si puede verificarse cada firma. Cada parte de la cadena autentifica la siguiente parte y, en última instancia, genera un kernel de Linux verificado y un sistema de archivos raíz verificado.

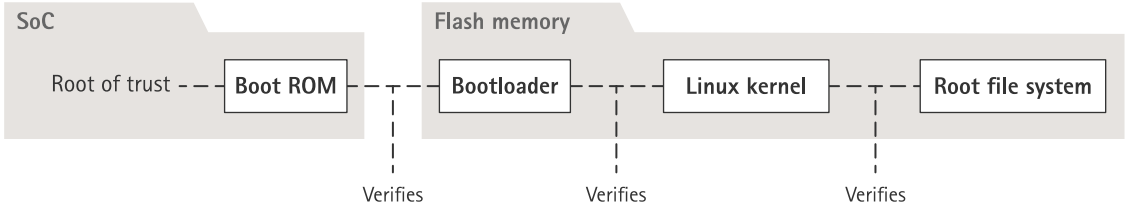


Figure 13. En el proceso de arranque seguro, cada parte de la cadena autentica la siguiente. El resultado final es un sistema de archivos raíz verificado.

En muchos dispositivos es importante que la funcionalidad de bajo nivel resulte imposible de modificar. Cuando se crean otros mecanismos de seguridad sobre el software de nivel inferior, el arranque seguro actúa como una capa base segura que protege contra la elusión de dichos mecanismos. En el caso de un dispositivo con arranque seguro, el firmware instalado en la memoria flash está protegido contra modificaciones. La imagen predeterminada de fábrica está protegida, mientras que la configuración permanece sin protección. El arranque seguro garantiza que el estado del dispositivo es correcto, incluso tras restaurar la configuración predeterminada de fábrica. Sin embargo, solo funciona si durante el arranque se comprueba que el firmware está firmado por Axis.

5.2 Firmware firmado

Firmware firmado por Axis significa que Axis firma la imagen del firmware con una clave privada secreta. Cuando un firmware tiene adjunta esta firma, un dispositivo validará el firmware antes de aceptar la

instalación. Si el dispositivo detecta que la integridad del firmware está en riesgo, se rechazará la actualización del firmware.

El proceso de firma del firmware se inicia mediante el cálculo de un valor de hash criptográfico. A continuación, el valor se firma con la clave privada de un par de claves privada/pública antes de que la firma se adjunte a la imagen de firmware.

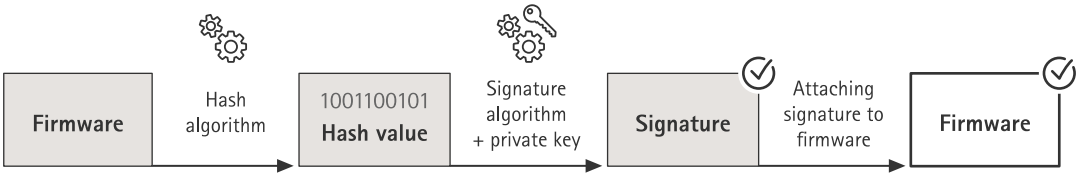


Figure 14. El proceso de firma del firmware.

Antes de actualizar el firmware, hay que verificar su autenticidad. Para hacerlo, se utiliza la clave pública (que se incluye con el producto de Axis) para confirmar que el valor hash se ha firmado realmente con la clave privada correspondiente. Al calcular también el valor hash del firmware y compararlo con este valor hash validado a partir de la firma, se puede verificar la integridad del firmware. El proceso de arranque de los dispositivos Axis se detiene si se detecta una firma de firmware que no es válida o si se ha manipulado la imagen del firmware.

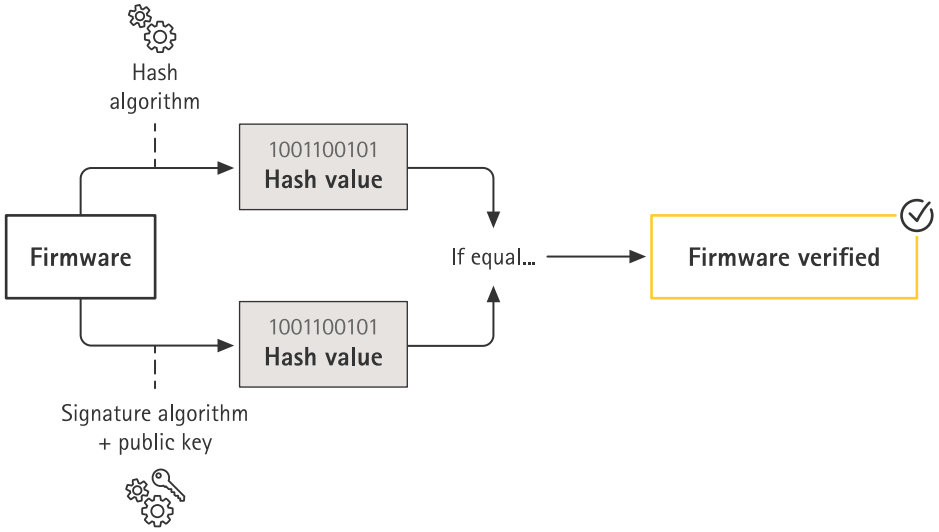


Figure 15. El proceso de verificación del firmware firmado.

El firmware firmado de Axis se basa en el método de cifrado de clave pública RSA aceptado por el sector. La clave privada se almacena en un lugar cuidadosamente protegido por Axis, mientras que la clave pública está integrada en los dispositivos de Axis. La integridad de toda la imagen del firmware está garantizada por una firma del contenido de la imagen. Una firma principal verifica varias firmas secundarias, que verifican mientras la imagen se desempaqueta.

En el caso de las versiones de prueba y personalizadas del firmware, Axis ha implementado un mecanismo que permite a dispositivos concretos aceptar firmware que no es de producción. Este firmware se firma de otra manera, con aprobación por parte del propietario y de Axis, lo que genera un certificado de firmware personalizado. Al instalarlo en los dispositivos aprobados, el certificado permite utilizar un firmware

personalizado que se ejecuta únicamente en el dispositivo aprobado, utilizando su número de serie e ID de chip para verificarlo. Los certificados de firmware personalizados solo puede crearlos Axis, puesto que Axis tiene la clave para firmarlos.

6 Glosario

ID de dispositivo de Axis: un certificado único con las claves correspondientes que demuestran la autenticidad de un dispositivo Axis. El ID de dispositivo de Axis viene instalado de fábrica y se guarda en el almacén de claves seguro. Se basa en el estándar internacional IEEE 802.1AR (IDevID, identificador inicial del dispositivo), que define un método para la identificación automática y segura.

Axis Edge Vault: la plataforma de ciberseguridad basada en hardware que protege el dispositivo Axis. Tiene dos sólidos pilares: los módulos de computación criptográfica (elemento seguro y TPM) y la seguridad del SoC (TEE y arranque seguro), combinados con una amplia experiencia en la seguridad de los dispositivos en el extremo.

Certificado: documento firmado que da fe del origen y las propiedades de un par de claves pública/privada. El certificado está firmado por una autoridad de certificación (CA) y, si el sistema confía en la CA, también confiará en los certificados emitidos por la misma.

Autoridad de certificación (CA): la raíz de confianza para una cadena de certificados. Se utiliza para demostrar la autenticidad y la veracidad de los certificados subyacentes.

Common Criteria (CC): estándar internacional para la certificación de seguridad de los productos tecnológicos. Se conoce también como Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408.

FIPS 140: una serie de estándares de seguridad informática de Estados Unidos que se utilizan para aprobar módulos de computación criptográfica. FIPS (Federal Information Processing Standard) 140 define los requisitos para el diseño y la implementación de un módulo criptográfico con el objetivo de reducir los riesgos de manipulación de los módulos.

ROM (memoria de solo lectura) inmutable: la memoria de solo lectura guarda de forma segura las claves públicas validadas y el programa que se utiliza para comparar firmas, de modo que no puedan sobrescribirse.

Aprovisionamiento: el proceso de preparación de un dispositivo para la red. Este proceso implica el envío de datos de configuración y ajustes sobre políticas al dispositivo desde un punto central. El dispositivo recibe claves y certificados.

Criptografía de clave pública: sistema de criptografía asimétrica que permite a cualquier persona cifrar un mensaje utilizando la *clave pública* del receptor, pero solo el receptor (que utiliza la *clave privada*) puede descifrar el mensaje. Se puede utilizar para cifrar y firmar mensajes.

Arranque seguro: prestación que impide que pueda cargarse software no autorizado mientras el dispositivo arranca. El arranque seguro utiliza firmware firmado que garantiza que solo se utiliza software Axis autorizado para arrancar el dispositivo.

Elemento seguro: módulo de computación criptográfica con un almacén de hardware para las claves privadas con protección frente a manipulaciones y ejecución segura de las operaciones criptográficas. A diferencia del TPM, las interfaces de hardware y software de un elemento seguro no son estándar, sino específicas de cada fabricante.

Almacén de claves seguro: entorno a prueba de manipulaciones para la protección de claves privadas y la ejecución segura de operaciones criptográficas. Impide el acceso sin autorización y las extracciones

maliciosas en caso de incidentes de seguridad. En función de los requisitos de seguridad, un dispositivo Axis puede tener uno o varios módulos de computación criptográfica basados en hardware, el lugar donde se encuentra el almacén de claves seguro protegido por el hardware.

Firmware firmado: firmware firmado digitalmente por una entidad de confianza. El dispositivo Axis verifica la autenticidad de la imagen del firmware antes de instalar una actualización de firmware. El firmware firmado es un requisito imprescindible del proceso de arranque seguro.

Vídeo firmado: función diseñada para conservar y reforzar la confianza en el vídeo como prueba. El vídeo firmado detecta manipulaciones y garantiza la autenticidad. Se utiliza para demostrar que el vídeo está intacto y tiene su origen en una cámara concreta de Axis. Las claves utilizadas para firmar el vídeo están en el almacén de claves seguro del dispositivo Axis.

Transport Layer Security (TLS): estándar de internet para proteger el tráfico de la red. TLS aporta la S (de seguridad) a HTTPS.

Trusted Execution Environment (TEE): almacenamiento protegido frente a manipulaciones y basado en hardware para claves privadas y la ejecución segura de operaciones criptográficas. A diferencia del elemento seguro y del TPM, el TEE es un área aislada segura situada en el procesador principal del sistema en chip (SoC).

Trusted Platform Module (TPM): módulo de computación criptográfica con un almacén de hardware para las claves privadas con protección frente a manipulaciones y ejecución segura de las operaciones criptográficas. Los TPM son componentes informáticos sujetos a estándares internacionales (TPM 1.2, TPM 2.0) definidos por el *Trusted Computing Group (TCG)*.

Seguridad de confianza cero: modelo de seguridad de TI según el cual los dispositivos conectados y la infraestructura de TI (redes, ordenadores, servidores, servicios en la nube y aplicaciones) deben identificarse, validarse y autenticarse de forma recurrente para reforzar su seguridad.

T10190380/ES/M1.9/2304

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro a través de soluciones para mejorar la seguridad y el rendimiento empresarial. Como empresa de tecnología de red y líder del sector, Axis ofrece soluciones de videovigilancia, control de acceso y sistemas de audio e intercomunicación. Se ven reforzadas por aplicaciones de análisis inteligentes y respaldadas por formación de alta calidad.

Axis tiene alrededor de 4000 empleados dedicados en más de 50 países y colabora con socios de integración de sistemas y tecnología en todo el mundo para ofrece soluciones personalizadas. Axis se fundó en 1984 y la sede está en Lund, Suecia