DOCUMENTO TÉCNICO

Prestaciones de ciberseguridad de los productos Axis

— firmware firmado

— arranque seguro

— Axis Edge Vault

— ID de dispositivo de Axis

— vídeo firmado

Noviembre 2021

Índice

1 **Resumen** 3

1.1 Firmware firmado 3

1.2 Arranque seguro 3

1.3 Axis Edge Vault 3

1.4 ID de dispositivo de Axis 3

1.5 Vídeo firmado 4

2 **Glosario** 4

3 **Introducción** 5

4 **Detección de manipulaciones del firmware** 5

4.1 Firma del firmware 5

4.2 Firmware firmado en Axis 6

5 **Prevención de manipulaciones en la cadena de suministro** 7

5.1 Arranque seguro 7

5.2 Arranque seguro de Axis 7

5.3 Arranque seguro y certificados de firmware personalizados 8

6 **Secretos protegidos frente a manipulaciones** 8

6.1 ID de dispositivo de Axis 8

7 **Almacenamiento seguro de claves** 9

7.1 Almacenamiento seguro de certificados con Axis Edge Vault 10

7.2 Almacenamiento seguro de claves con un TPM (módulo de plataforma fiable) 10

7.3 Certificación FIPS 140-2 10

8 **IEEE 802.1 AR – verificación del dispositivo con el ID de dispositivo de Axis** 11

9 **Detección de manipulación del vídeo** 13

9.1 Vídeo firmado 13

1 Resumen

Este documento describe algunas de las prestaciones disponibles en los productos Axis que pueden mitigar las amenazas cibernéticas y contrarrestar determinados tipos de ataques. Estas prestaciones son:

- firmware firmado
- arranque seguro
- Axis Edge Vault
- ID de dispositivo de Axis
- vídeo firmado

Entre las amenazas abordadas aquí encontramos:

- manipulación del firmware
- manipulación de la cadena de suministro
- extracción de claves privadas
- sustitución de dispositivo no autorizada
- manipulación del vídeo.

1.1 Firmware firmado

El firmware firmado lo implementa el proveedor del software que firma la imagen de firmware con una clave privada. 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.

1.2 Arranque seguro

El 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). Como se basa en el uso del firmware firmado, el arranque seguro garantiza que el dispositivo solo puede iniciarse con firmware autorizado.

1.3 Axis Edge Vault

Axis Edge Vault es un módulo de computación criptográfica segura, que puede utilizarse para realizar operaciones criptográficas en certificados almacenados de forma segura. Edge Vault incluye un almacenamiento protegido frente a manipulaciones, que permite a cada dispositivo proteger sus secretos. Dicho almacenamiento es la base para la implementación de funciones de seguridad más avanzadas sin riesgos.

1.4 ID de dispositivo de Axis

El ID de dispositivo de Axis funciona como un pasaporte digital: es único para cada dispositivo. Se almacena de forma segura y permanente en Edge Vault como un certificado firmado por el certificado raíz

de Axis. El ID de dispositivo de Axis está diseñado para demostrar el origen del dispositivo, lo que abre la puerta a un nuevo nivel de confianza en el dispositivo a lo largo del ciclo de vida del producto.

1.5 Vídeo firmado

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 cámara utiliza su ID de dispositivo de Axis único, guardado de forma segura en Axis Edge Vault, para añadir una firma a la transmisión de vídeo. Cuando se reproduce el vídeo, el reproductor de archivos muestra si el vídeo está intacto. En resumen, 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.

2 Glosario

Certificado: en criptografía, un certificado es un documento firmado que acredita el origen y las propiedades de un par de claves. El certificado está firmado por una autoridad de certificación (CA) y, si el sistema confía en la CA, entonces también confiará en los certificados emitidos por esta autoridad.

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.

FIPS: Estándares Federales de Procesamiento de la Información, estándares de cifrado de datos y seguridad de datos emitidos en Estados Unidos por el NIST (National Institute of Standards and Technology).

ROM inmutable: para almacenar de forma segura las claves públicas de confianza y el programa que se utilizan para comparar firmas de modo que no se puedan sobrescribir.

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.

TLS – Transport Layer Security o seguridad de la capa de transporte. Es un estándar de Internet para proteger el tráfico de la red. TLS aporta la S (de seguridad) a HTTPS.

3 Introducción

Axis sigue las mejores prácticas del sector para gestionar las vulnerabilidades de seguridad de sus productos y darles respuesta, con el fin de minimizar la exposición de los clientes a los riesgos cibernéticos. No hay forma de garantizar que los productos y servicios estén libres de fallos que puedan aprovecharse para perpetrar ataques malintencionados. Esto no es específico de Axis, sino que algo común a todos los dispositivos de red. Lo que Axis sí puede garantizar es un esfuerzo coordinado en cada fase del proceso para minimizar los riesgos a los que están expuestos sus dispositivos y servicios de Axis.

Para informarse sobre la seguridad de los productos y las vulnerabilidades identificadas, visite *www.axis.com/support/product-security*. Si desea conocer las medidas que puede adoptar para reducir los riesgos frente a las amenazas más comunes, descargue la Axis Hardening Guide desde la misma página.

En este documento técnico se presentan algunos ciberataques plausibles y se explica cómo se pueden prevenir en los productos Axis. En concreto, explica como el firmware firmado y el arranque seguro pueden impedir la manipulación del firmware y de la cadena de suministro. También aborda el uso de un módulo de plataforma fiable (TPM) y de Axis Edge Vault, que pueden utilizarse para proteger las claves privadas. Axis Edge Vault se utiliza para almacenar de forma segura el ID de dispositivo de Axis, lo que abre la puerta a un nuevo nivel de confianza de los dispositivos. Axis Edge Vault y el ID de dispositivo de Axis permiten también usar vídeo firmado, una función para verificar que no se ha manipulado el vídeo tras salir de la cámara.

4 Detección de manipulaciones del firmware

Un posible vector de ataque que un hacker podría intentar aprovechar tras fracasar otros intentos de vulnerar el sistema, es conseguir que el propietario del sistema instale aplicaciones, firmware u otros módulos de software que han sido alterados. El software modificado puede incluir código malicioso con un fin específico. La recomendación habitual es no instalar ningún software procedente de una fuente en la que no confíe plenamente. En el contexto de los sistemas de vídeo, puede haber un "man in the middle" (o ataque de intermediario) que altere el firmware del dispositivo y trate de persuadir a los usuarios finales para que lo instalen. Sin embargo, no es una misión sencilla y el hacker debe tener conocimientos especializados y estar muy decidido. Debe conocer hasta el más mínimo detalle del firmware de Axis y saber cómo funciona el firmware en un dispositivo. De todos modos, los hackers pueden intentarlo si el valor de atacar un sistema específico es lo suficientemente alto. Para evitar que se salgan con la suya, los proveedores de software suelen utilizar firmware firmado.

4.1 Firma del firmware

El firmware firmado lo implementa el proveedor del software que firma la imagen de firmware con una clave privada (que se mantiene en secreto). 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.

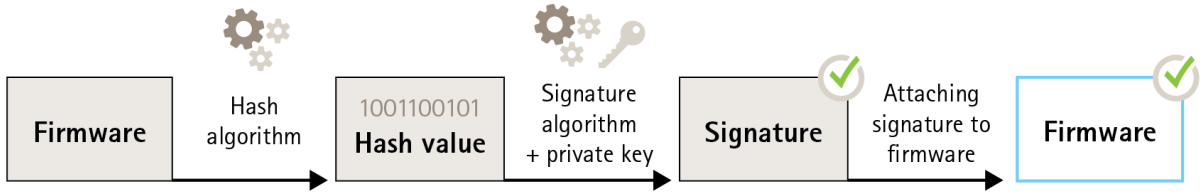

Figure 1. El proceso de firma del firmware.

Antes de actualizar el firmware, el nuevo firmware debe verificarse. A fin de garantizar que el nuevo firmware no se ha modificado, la clave pública (incluida con el producto de Axis) se utiliza 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.

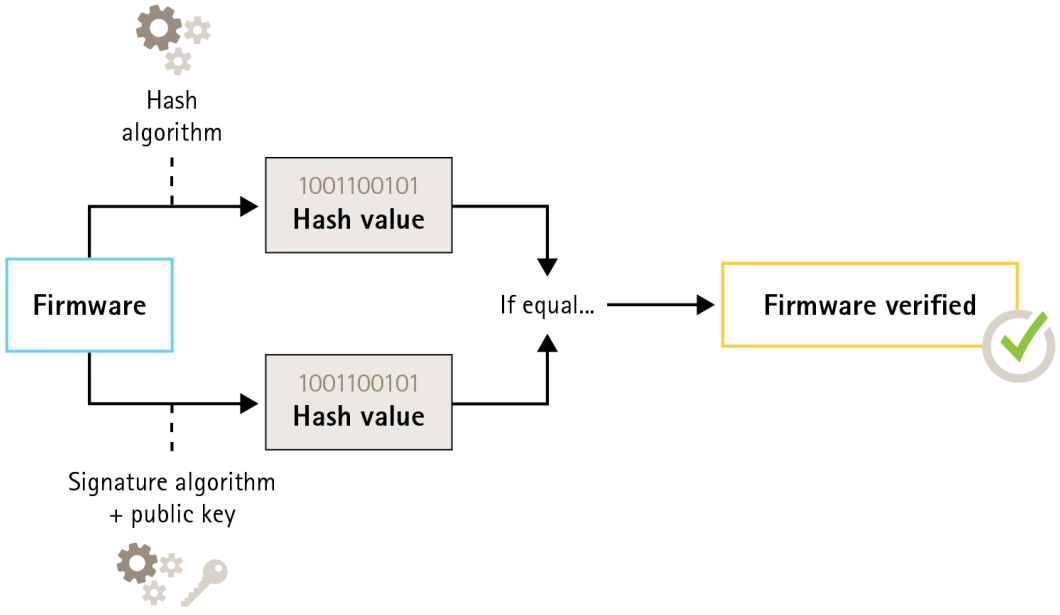

Figure 2. El proceso de verificación del firmware firmado.

4.2 Firmware firmado en Axis

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 se verifican mientras la imagen se descomprime.

5 Prevención de manipulaciones en la cadena de suministro

La firma del firmware protege un dispositivo, en todas las futuras actualizaciones de firmware, frente a la instalación de un firmware no seguro. Pero ¿qué sucede si alguien modifica el dispositivo en algún punto del camino entre el proveedor y el usuario final? Una persona que disponga de acceso físico al dispositivo durante el proceso podría perpetrar un ataque, como poner en peligro la partición de arranque del dispositivo o anular la comprobación de la integridad del firmware para instalar un firmware modificado y malicioso antes de la implementación del dispositivo.

5.1 Arranque seguro

El 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). Como se basa en el uso del firmware firmado, el arranque seguro garantiza que el dispositivo solo puede iniciarse 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 siempre y cuando cada firma puede verificarse. 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.

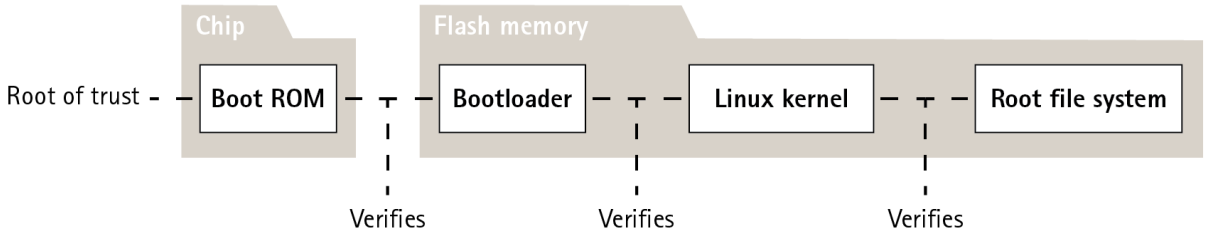

Figure 3. El proceso de arranque seguro.

5.2 Arranque seguro de Axis

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 dispositivo Axis está totalmente libre de malware tras restablecer la configuración predeterminada de fábrica.

5.3 Arranque seguro y certificados de firmware personalizados

Si bien el arranque seguro hace que el producto sea más seguro, también reduce la flexibilidad al trabajar con diferentes firmware, por lo que es más complicado cargar en el producto cualquier firmware provisional, como firmware de prueba u otro firmware personalizado de Axis. Sin embargo, Axis ha implementado un mecanismo que aprueba unidades individuales para aceptar firmware todavía en fase de preproducción. 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 las unidades aprobadas, el certificado permite utilizar un firmware personalizado que se ejecuta únicamente en la unidad aprobada, 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 Secretos protegidos frente a manipulaciones

Uno de los requisitos básicos de cualquier sistema distribuido seguro es la posibilidad de verificar conexiones y evitar la intercepción. Y para cumplirlo es necesario que cada dispositivo proteja sus propios secretos usando un almacenamiento seguro protegido frente a manipulaciones. Axis Edge Vault cuenta con un almacenamiento de este tipo y, sobre esta sólida base, pueden implementarse funciones de seguridad más avanzadas.

6.1 ID de dispositivo de Axis

Durante el proceso de producción de cada dispositivo de red Axis, se instala de forma segura un "pasaporte digital" denominado ID de dispositivo de Axis en el Axis Edge Vault de la unidad. Esta identidad es única para cada unidad y está diseñada para demostrar el origen del dispositivo. El ID de dispositivo de Axis es una colección de certificados que se utiliza en el área criptográfica del módulo para firmar las solicitudes presentadas por el firmware del producto integrado en Edge Vault. La respuesta de esta operación se envía al receptor, que puede utilizar las claves públicas de Axis para validar la autenticación de la respuesta.

Un certificado es un pequeño conjunto de datos que combina una clave pública y metadatos que describen la clave, junto con una firma del emisor que atestigua la validez del certificado. Una jerarquía de certificado es una forma de demostrar la procedencia del certificado.

Para entenderlo mejor, vamos a ver una analogía entre el ID de dispositivo de Axis y un pasaporte. Si dispone de un pasaporte, el gobierno de su país garantiza que usted es la persona que el pasaporte indica que es. De forma similar, todos los certificados de ID de dispositivo de Axis están respaldados por un certificado de CA raíz del ID de dispositivo de Axis. Al igual que un agente de aduanas confía en que el gobierno de su país ha emitido correctamente su pasaporte, un sistema de seguridad de red confía en que

el certificado de CA raíz del ID de dispositivo de Axis ha comprobado correctamente el certificado de Axis de una unidad conectada a la red.

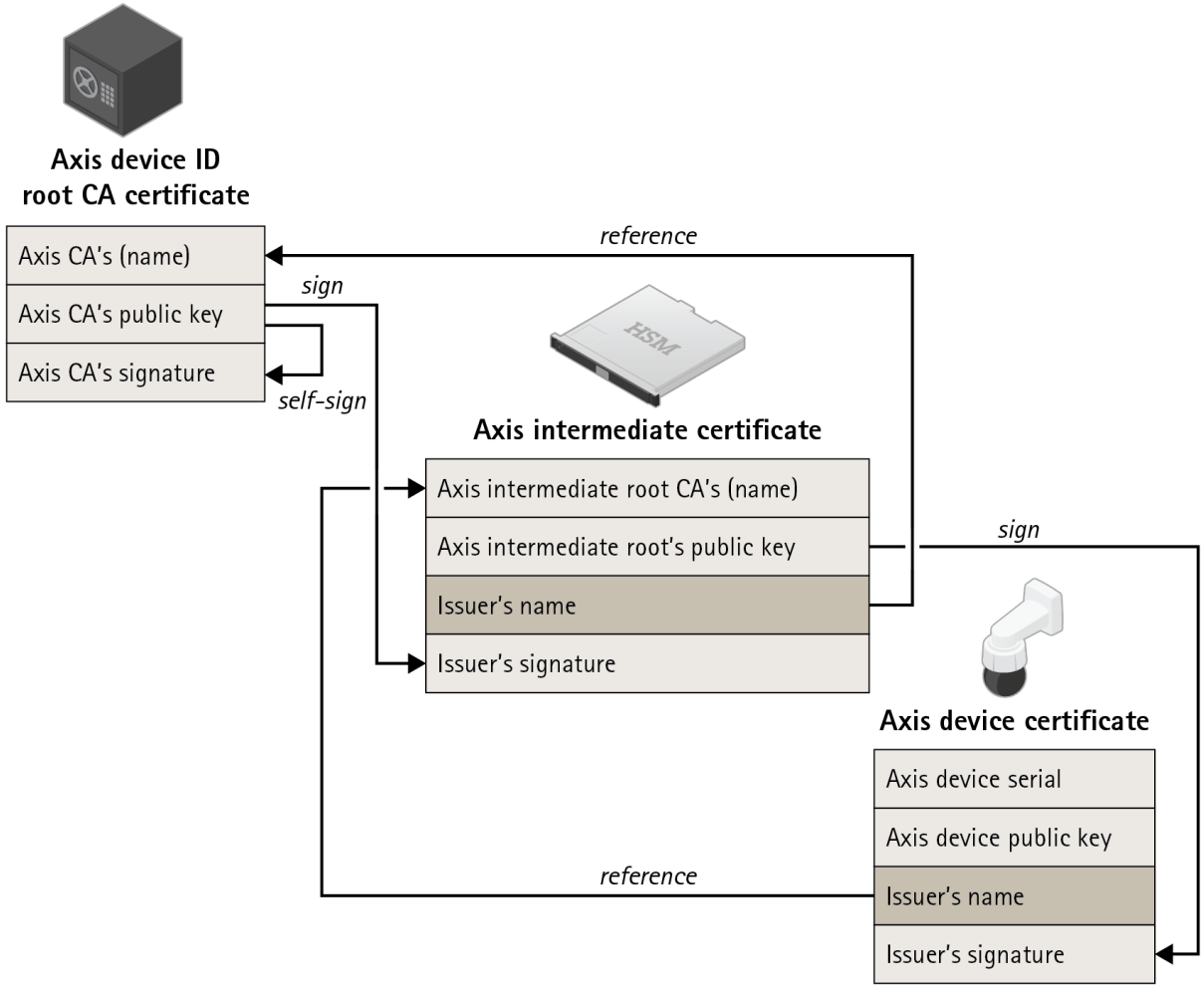

Figure 4. El ID del dispositivo de Axis, que es un certificado que incorpora el número de serie del producto, está firmado por un certificado intermedio, firmado por el certificado raíz de Axis. Dado que el certificado raíz de Axis es extremadamente importante y debe guardarse en un lugar seguro, se necesita el certificado intermedio durante el aprovisionamiento en la fábrica.

7 Almacenamiento seguro de claves

Los dispositivos de Axis son compatibles con HTTPS (cifrado de red) y 802.1X (control de acceso a la red), que utilizan TLS (seguridad de la capa de transporte). Los certificados digitales de TLS utilizan un par de claves pública/privada. La clave privada se almacena en el dispositivo, mientras que la clave pública se incluye en el certificado. Es importante tener en cuenta que si no se utiliza HTTPS ni 802.1X, no hay ninguna clave que proteger.

Un hacker podría intentar extraer la clave privada y el certificado del dispositivo e instalarlos en un equipo utilizado para perpetrar un ataque. En el caso de HTTPS, la clave privada podría utilizarse para la intercepción del tráfico de red cifrado entre el dispositivo y el VMS. O, en caso de suplantación de la red, el equipo atacante podría acceder al VMS haciéndose pasar por un dispositivo legítimo. En el caso de

802.1X, el hacker podría utilizar la clave privada para obtener acceso a una red con protección 802.1X, haciéndose pasar por un dispositivo de confianza.

Por lo general, los certificados y las claves privadas se almacenan en el sistema de archivos de un dispositivo, protegidos por la política de acceso a la cuenta y utilizados en el entorno informático normal. En la mayoría de los casos, esto es suficiente porque no es fácil poner en riesgo la cuenta. Tenga en cuenta que los certificados se pueden revocar si se sospecha que hay peligro, de modo que la clave privada deja de ser operativa.

En el caso de algunos usuarios finales de sistemas críticos, es mayor el riesgo de que hackers experimentados intenten atacar el dispositivo para extraer la clave privada. En estas circunstancias, se puede utilizar Axis Edge Vault de modo que sea prácticamente imposible extraerla incluso en caso de vulneración de la seguridad del dispositivo.

7.1 Almacenamiento seguro de certificados con Axis Edge Vault

Axis Edge Vault es un módulo de computación criptográfica segura en forma de chip montado en la placa base del producto. Edge Vault puede almacenar certificados de forma segura y se puede utilizar para operaciones criptográficas en certificados almacenados de forma segura.

No es necesario que los certificados almacenados en Edge Vault salgan de allí cuando llega el momento de utilizarlos. Permanecen de forma segura en Edge Vault incluso cuando se utilizan, ya que el hardware criptográfico que usa la clave está instalado en el mismo chip físico.

7.2 Almacenamiento seguro de claves con un TPM (módulo de plataforma fiable)

Un TPM es un componente que proporciona un determinado conjunto de funciones de cifrado adecuadas para proteger la información frente a accesos no autorizados. La clave privada se almacena en el TPM y nunca sale del TPM. Todas las operaciones criptográficas que requieren el uso de la clave privada se envían al TPM para su procesamiento. Esto garantiza que la parte secreta del certificado nunca sale del entorno seguro del TPM y sigue siendo segura aunque se produzca una vulneración de la seguridad.

7.3 Certificación FIPS 140-2

En algunos productos y casos de uso concretos, puede existir la obligación normativa de usar un TPM para proteger la información, que a veces se suma a la obligación de conformidad con FIPS 140-2. FIPS (Estándar Federal de Procesamiento de la Información) 140-2 es un estándar de seguridad de la información para módulos criptográficos establecido por el NIST (National Institute of Standards and Technology), un organismo estadounidense.

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 criptográfico, algoritmos aprobados, modos de funcionamiento aprobados y pruebas de encendido.

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

7.3.1 TPM certificado en productos Axis

El TPM utilizado en determinados productos Axis cumple los requisitos de FIPS 140-2. Concretamente, se ajusta al nivel de seguridad 2 del estándar, lo que significa que el TPM cumple también los requisitos de autorización basada en roles y pruebas de manipulación, entre otros.

8 IEEE 802.1 AR - verificación del dispositivo con el ID de dispositivo de Axis

Una persona que compre un dispositivo de red de Axis puede realizar un examen manual antes de empezar a usarlo. Inspeccionando visualmente el producto y comprobando que tiene el aspecto propio de los productos Axis, el cliente puede tener la tranquilidad de que el dispositivo realmente procede de Axis. Sin embargo, este tipo de inspección solo la puede realizar una persona con acceso físico al producto. Pero cuando se comunica con un producto no aprovisionado a través de una red, ¿cómo puede estar seguro de que se está comunicando con la unidad correcta? ¿Cómo puede saber que el dispositivo no se ha sustituido de forma no autorizada? Ni el equipo de red ni el software de los servidores pueden realizar una inspección física. Como medida de seguridad, a menudo se opta por empezar a interactuar con un nuevo producto a través de una red cerrada, en que la unidad se puede aprovisionar de forma segura.

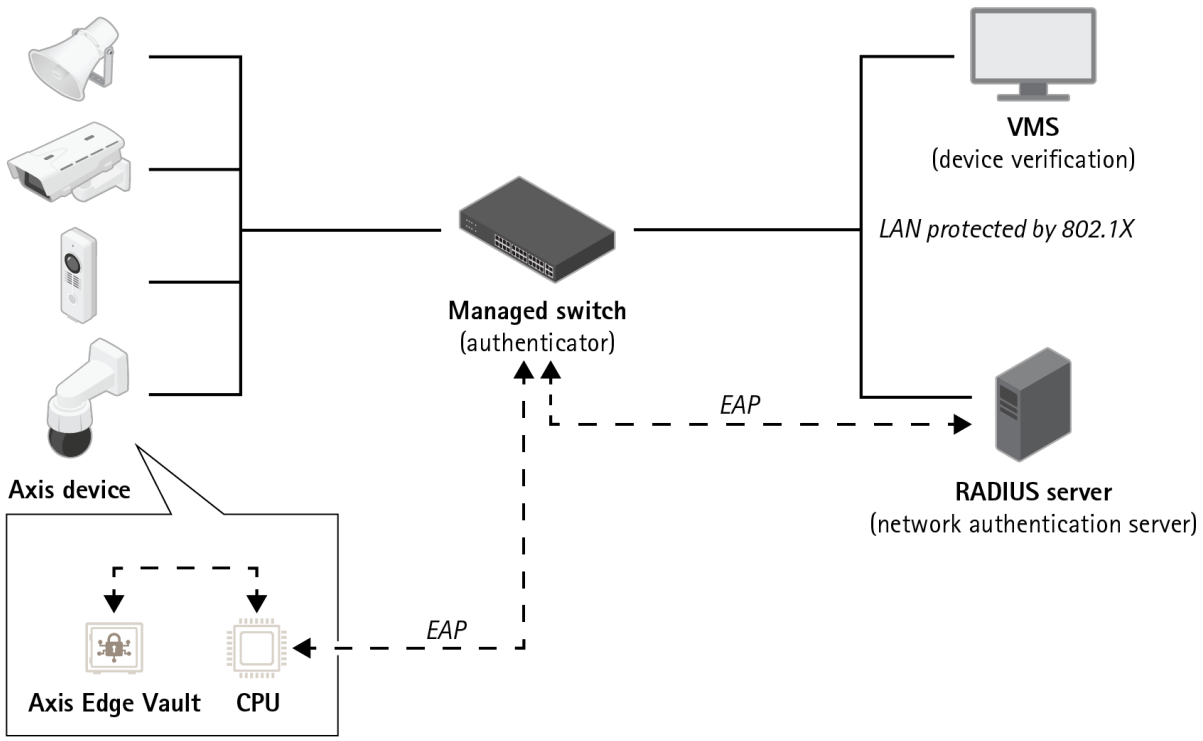

Figure 5. Los clientes pueden ordenar a su servidor de autenticación que acepte automáticamente en la red los productos Axis adquiridos utilizando los números de serie del dispositivo y el ID de dispositivo de Axis.

El nuevo estándar internacional IEEE 802.1AR (*https://1.ieee802.org/security/802-1ar/*) define un método para automatizar y garantizar la identificación de un dispositivo en una red. Si la comunicación se envía a

un módulo seguro integrado, la unidad puede devolver una respuesta de identificación fiable de acuerdo con el estándar.

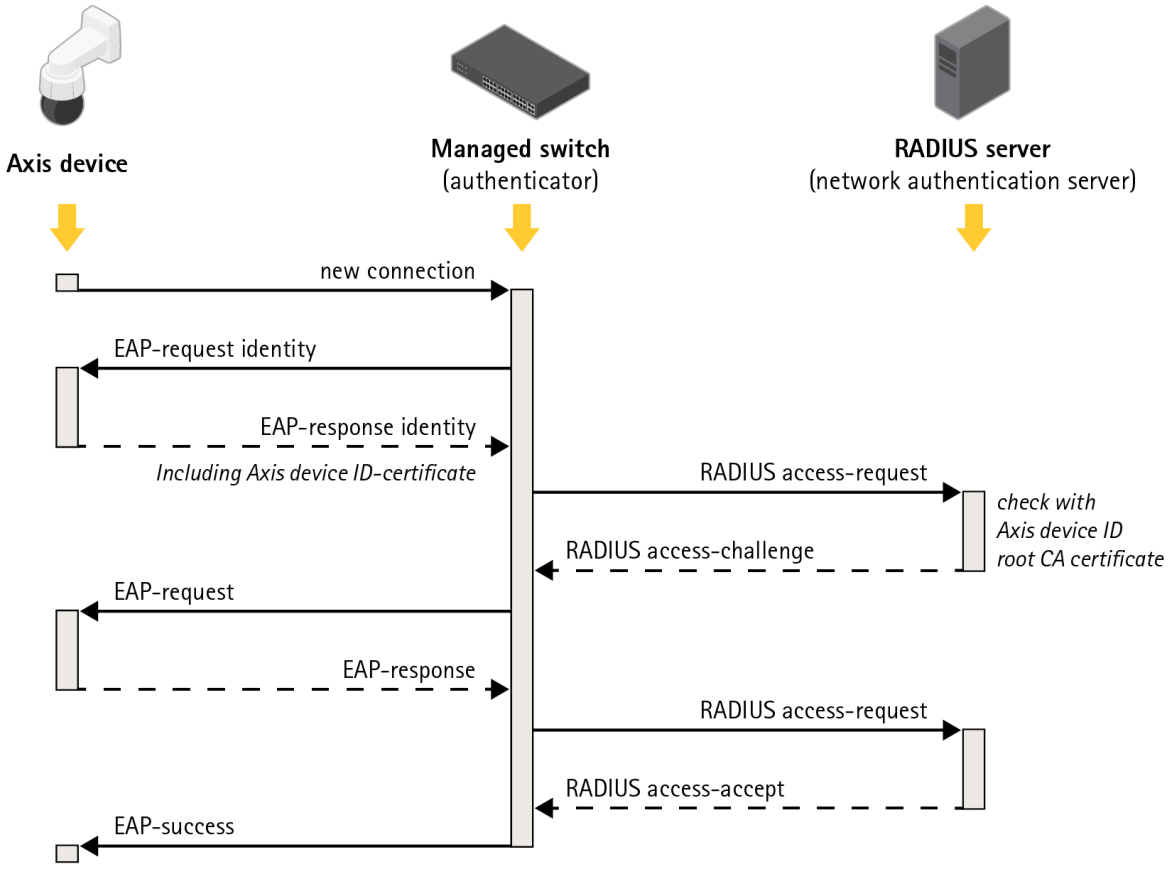

Figure 6. IEEE 802.1AR define un método para identificar un dispositivo en una red mediante un protocolo que envía solicitudes de protocolo de autenticación extensible (EAP) al switch que utiliza el servicio de usuario de acceso telefónico de autenticación remota (RADIUS): solicitudes para conceder acceso.

En los productos Axis, estas medidas de seguridad se implementan utilizando Axis Edge Vault y el ID de dispositivo de Axis. Axis Edge Vault es un módulo seguro en el que se instala el ID de dispositivo de Axis, un conjunto de certificados para verificar la identificación del dispositivo. Estas prestaciones ofrecen a su red una prueba criptográficamente verificable de que una unidad específica ha sido producida por Axis y que la conexión de red a la unidad es atendida efectivamente por esa misma unidad.

Un dispositivo con ID de dispositivo de Axis se ha aprovisionado en la fábrica (con claves y certificados). Este aprovisionamiento puede ser utilizado posteriormente por un cliente para aprovisionar el dispositivo sobre el terreno con otras claves o certificados para que pueda acceder a algunos de los recursos de red del cliente.

Mediante la identificación de la unidad con el ID de dispositivo de Axis, se puede reducir el tiempo de implantación de los dispositivos, porque es necesario realizar menos operaciones con el dispositivo antes de instalarlo y configurarlo en la red deseada. Otra ventaja es que el ID de dispositivo de Axis, aparte de

proporcionar una fuente de confianza integrada adicional, también ofrece una vía para controlar los dispositivos de un sistema de grandes dimensiones.

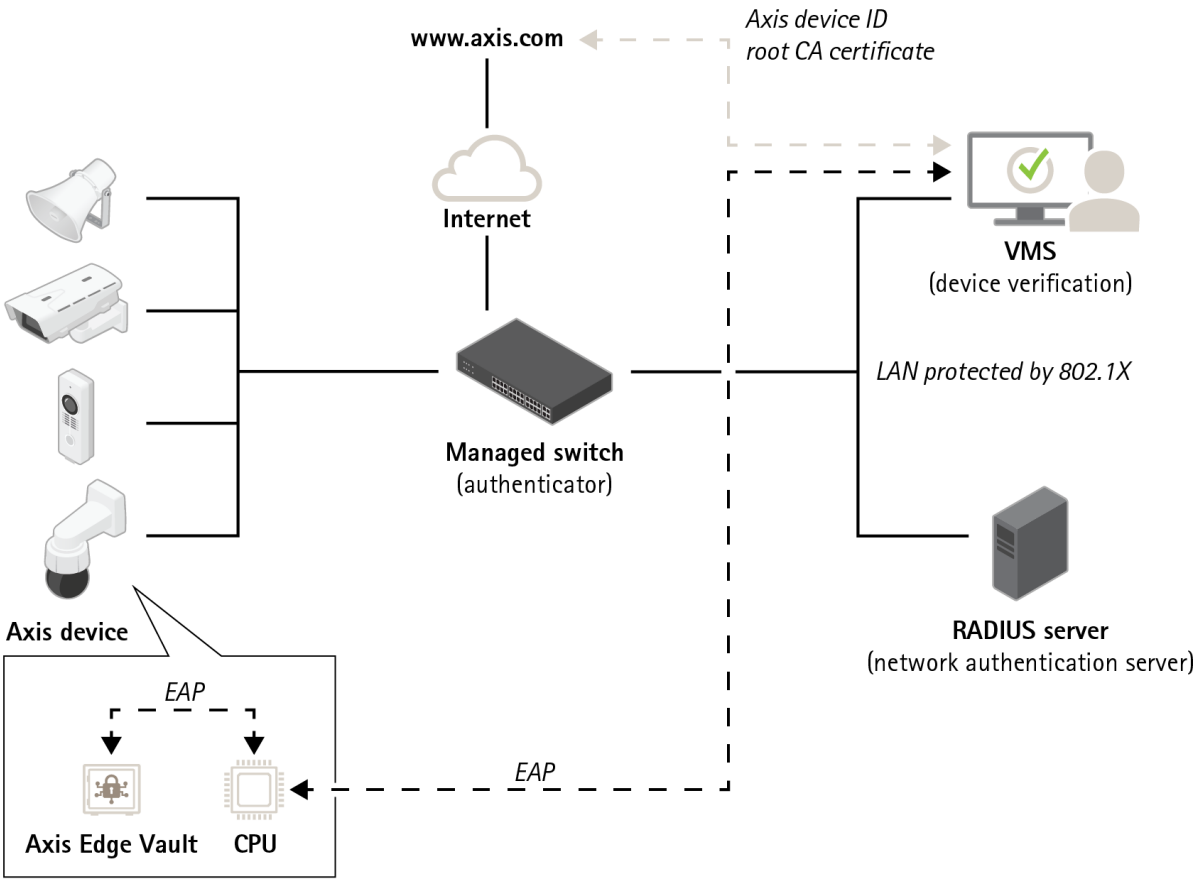

Figure 7. Las aplicaciones de software de otras partes del sistema pueden utilizar el ID de dispositivo de Axis y operaciones criptográficas para verificar con quién se están comunicando. El ID de dispositivo de Axis ha sido verificado por el certificado de CA raíz del ID de dispositivo de Axis público desde axis.com.

9 Detección de 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.

9.1 Vídeo firmado

Con la prestación de vídeo firmado de 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 extraiga el vídeo exportando los archivos 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.

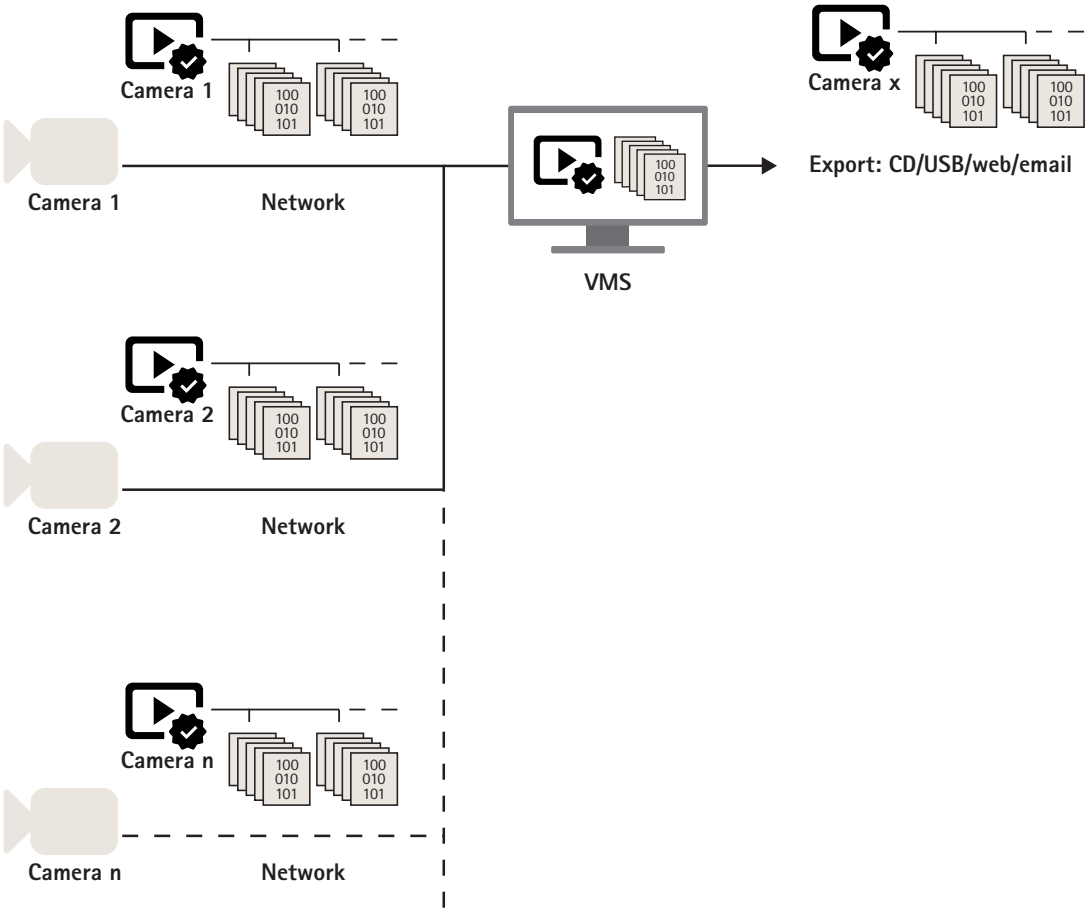

Figure 8. La firma se añade en la propia cámara, lo que permite verificar el contenido en todas y cada una de las fases, desde la fuente hasta el uso final del vídeo.

Cada cámara utiliza su ID de dispositivo de Axis único en Axis Edge Vault 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 en Edge Vault. Luego, la firma se guarda en la transmisión en unos campos de metadatos concretos (cabecera SEI).

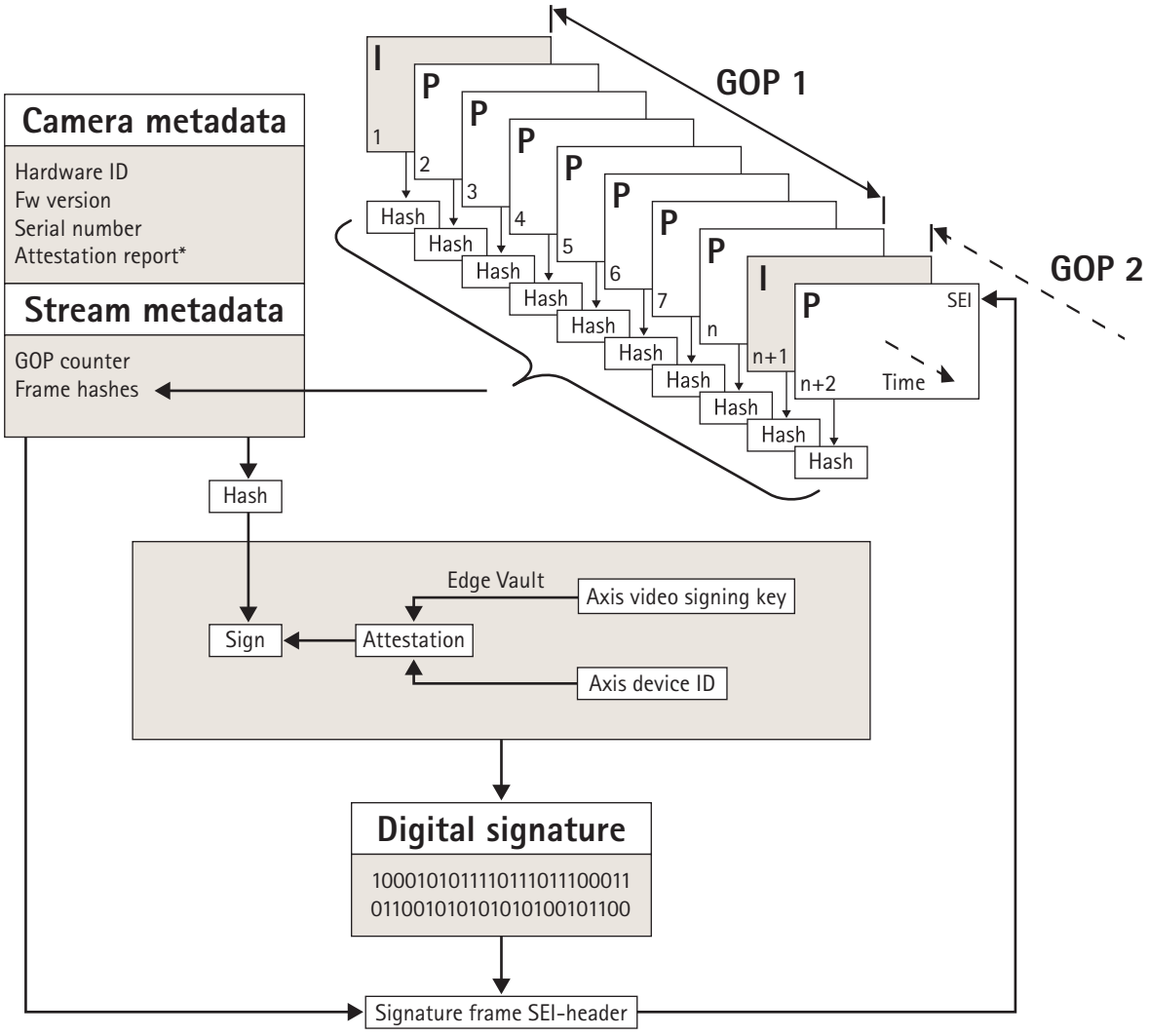

Figure 9. Representación gráfica de cómo se añade una firma a los metadatos del vídeo. El contenido de cada fotograma de un GOP se une con un hash de metadatos de la cámara y metadatos de la transmisión. El resultado es el hash del GOP, que se firma en Edge Vault. Luego, la firma y los metadatos se añaden 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 se realiza utilizando una clave para la firma de vídeo específica para la unidad, avalada por el ID de dispositivo de Axis único de cada dispositivo. El informe de autentificación se adjunta a la transmisión al principio y cada cierto tiempo, normalmente 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 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 al guardarlos, se notificará de la misma forma.

T10154694/ES/M3.2/2111

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro a través de soluciones en red que mejoran la seguridad y suponen una nueva manera de hacer negocios. Como líder de la industria del vídeo en red, Axis pone a su disposición productos y servicios de videovigilancia y analítica, control de accesos y sistemas de audio e intercomunicación. Axis cuenta con más de 3800 empleados especializados en más de 50 países, y proporciona soluciones a sus clientes en colaboración con empresas asociadas de todo el mundo. Fundada en 1984, su sede central se encuentra en Lund, Suecia.

Para más información sobre Axis, visite nuestro sitio web *axis.com*.