Firmware firmado, arranque seguro y seguridad de claves privadas

Características de ciberseguridad de los productos Axis

Julio 2020

Índice

1 Resumen

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

- firmware firmado
- arranque seguro
- módulo de plataforma segura (TPM)
- Axis Edge Vault con ID de dispositivo de AXIS.

Entre las amenazas que se explican se incluyen:

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

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 comprometida, 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). Al estar basado en el uso del firmware firmado, el arranque seguro garantiza que un dispositivo pueda iniciarse solo con un firmware autorizado.

1.3 TPM

Un TPM es un componente que proporciona un conjunto de características de cifrado adecuadas para proteger la información frente a accesos no autorizados. Las claves privadas se almacenan en el TPM y 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 permanecerá segura incluso en caso de violación de seguridad. El TPM que se utiliza en productos de Axis seleccionados está certificado para cumplir con los requisitos de la norma FIPS 140-2.

1.4 Axis Edge Vault con ID de dispositivo de AXIS

El nuevo estándar internacional IEEE 802.1AR describe un procedimiento para automatizar y asegurar la identificación de un dispositivo a través de una red. En los productos de Axis, estas medidas de seguridad se implementan mediante el uso de Axis Edge Vault e ID de dispositivo de AXIS. Edge Vault se puede utilizar para solicitudes criptográficas que funcionen en certificados guardados de forma segura. La parte privada

de los certificados permanece en Edge Vault incluso cuando se está utilizando. El ID de dispositivo de Axis se almacena de forma segura y permanente en Edge Vault como certificado firmado por el certificado root de Axis, lo que permite un nuevo nivel de confianza del dispositivo a lo largo del ciclo de vida útil del producto.

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 ella.

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 información, estándares de cifrado de datos y seguridad de datos emitidos en Estados Unidos por el NIST (Instituto Nacional de Estándares y Tecnología).

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 y equipamiento de un dispositivo para la red. Este proceso implica la entrega de los datos de configuración y la configuración de directivas al dispositivo desde un punto central. El dispositivo recibe claves y certificados.

Criptografía de clave pública: sistema de criptografía asimétrica en el que cualquier persona puede 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: seguridad de la capa de transporte, estándar de Internet para proteger el tráfico de red. TLS proporciona la S (de seguridad) en HTTPS.

3 Introducción

Axis sigue las mejores prácticas de la industria para gestionar y responder a las vulnerabilidades de seguridad de nuestros productos, con el fin de minimizar la exposición del cliente a los riesgos cibernéticos. No hay forma de garantizar que los productos y servicios estén libres de fallos que puedan aprovecharse para ataques malintencionados. Esto no es específico de Axis, sino que es una condición general de todos los dispositivos de red. Lo que Axis sí puede garantizar es que siempre hacemos un esfuerzo concertado en cada fase posible para garantizar que sus dispositivos y servicios de Axis se asocian con el menor riesgo posible.

Para obtener más información sobre la seguridad de los productos y las vulnerabilidades detectadas, consulte *www.axis.com/support/product-security*. Para obtener más información sobre las medidas que usted puede adoptar para reducir los riesgos de amenazas comunes, descargue Guía de fortalecimiento de Axis en *www.axis.com/cybersecurity*.

En este documento técnico se presentan algunos ciberataques plausibles y cómo se pueden prevenir en los productos Axis. El documento describe en concreto cómo las características firmadas el firmware y el arranque seguro pueden impedir la manipulación del firmware y la manipulación de la cadena de suministro. También se trata 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 permite un nuevo nivel de confianza de dispositivos.

4 Detección de manipulaciones de firmware

Un posible vector de ataque que un adversario podría intentar aprovechar después de fallar otros intentos de vulnerar el sistema, es conseguir que el propietario del sistema instale aplicaciones modificadas, firmware u otros módulos de software. 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 un contexto de sistema de vídeo puede haber un "man in the middle" (o ataque de intermediario) que podría alterar el firmware del dispositivo y atraer a los usuarios finales para que lo instalen. Este no es un ejercicio sencillo, por lo que el adversario debe tener conocimientos especializados y estar muy decidido. Se necesita una comprensión extremadamente detallada del diseño del firmware de Axis y de cómo funciona el firmware en un dispositivo. Aún así, estos adversaries podrían existir si el valor de atacar un sistema específico es lo suficientemente alto. La contramedida habitual es que el proveedor de software utilice firmware firmado.

4.1 Firma de 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 comprometida, 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.

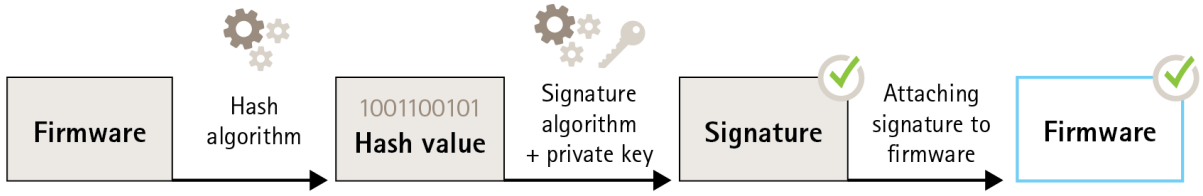

Figure 1. El proceso de firma del firmware.

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 (que se incluye 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.

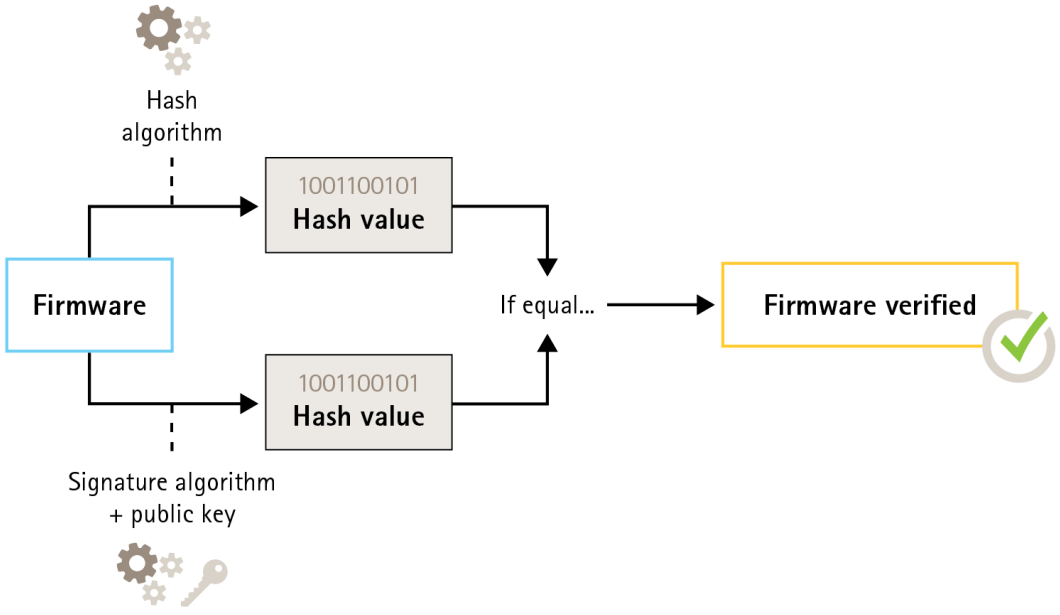

Figure 2. El proceso de verificación del firmware firmado.

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 una ubicación cuidadosamente guardada en 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 están verificando mientras la imagen se desempaqueta.

5 Prevención de manipulaciones en la cadena de suministro

La firma de firmware protege un dispositivo, en todas las futuras actualizaciones de firmware, frente a la instalación de un firmware comprometido. Pero ¿qué sucede si alguien modifica el dispositivo cuando se encuentra de camino entre el proveedor y el usuario final? Un adversario que disponga de acceso físico al dispositivo durante el tránsito podría realizar un ataque, como poner en peligro la partición de arranque del dispositivo, omitiendo la comprobación de la integridad del firmware para instalar un firmware alterado y malintencionado antes de que se implemente el 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). Al estar basado en el uso del firmware firmado, el arranque seguro garantiza que un dispositivo pueda iniciarse solo con un firmware autorizado.

La ROM de arranque valida el cargador de arranque, iniciando el proceso de arranque. A continuación, el arranque seguro comprueba, en tiempo real, las firmas integradas de cada bloque de firmware que se cargue desde la memoria flash. La ROM de arranque sirve como root de confianza y el proceso de arranque continúa mientras se comprueba 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 root verificado.

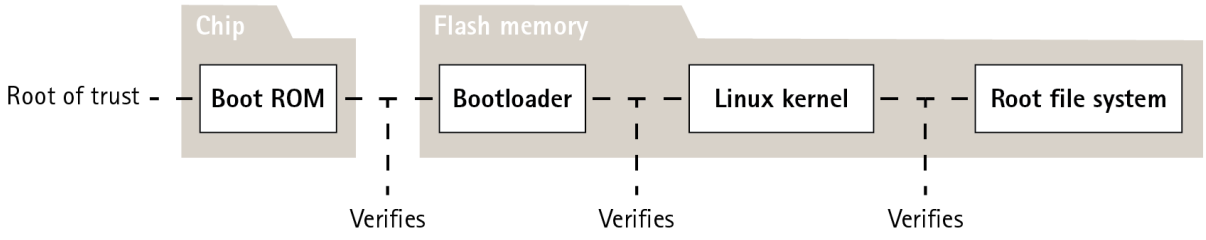

Figure 3. El proceso de arranque seguro.

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 se ha limpiado completamente del posible malware tras una configuración predeterminada de fábrica.

5.3 Arranque seguro y certificados de firmware personalizados

Mientras que el arranque seguro hace que el producto sea más seguro, también reduce la flexibilidad con diferentes firmware, por lo que es más complicado cargar en el producto cualquier firmware provisional, como el firmware de prueba u otro firmware personalizado de Axis. Sin embargo, Axis ha implementado un mecanismo que aprueba unidades individuales para aceptar este tipo de 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. Cuando se instala en las unidades aprobadas, el certificado permite el uso de un firmware personalizado que solo puede ejecutarse en la unidad aprobada, según su número de serie e ID de chip exclusivos. Los certificados de firmware personalizados solo puede crearlos Axis, ya que Axis posee la clave para firmarlos.

6 Seguridad de las claves privadas

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. Tenga en cuenta que si no se utiliza 802.1X, no hay ninguna clave que proteger.

Un adversario podría intentar extraer la clave privada y el certificado del dispositivo e instalarlos en un equipo atacante. En el caso de HTTPS, es posible utilizar la clave privada para espiar el tráfico de red cifrado entre el dispositivo y el VMS. O bien, si está suplantando a la red, el equipo atacante podría acceder al VMS fingiendo ser un dispositivo legítimo. En el caso de 802.1X, el adversario 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 directiva de acceso a la cuenta y utilizados en el entorno informático normal. En la mayoría de los casos, esto es suficiente porque la cuenta no se ve comprometida fácilmente. Tenga en cuenta que los certificados se pueden revocar si se sospecha que hay peligro, haciendo que la clave privada resulte inútil.

Algunos usuarios finales de sistemas críticos pueden experimentar un mayor riesgo de adversarios determinados y experimentados que intenten atacar el dispositivo para extraer la clave privada. Un módulo de plataforma segura (TPM) almacena la clave de forma que no es posible extraerla, incluso cuando el dispositivo se ve comprometido.

6.1 Almacenamiento de claves seguras con un TPM (módulo de plataforma fiable)

Un TPM es un componente que proporciona un determinado conjunto de características de cifrado adecuadas para proteger la información frente a accesos no autorizados. La clave privada se almacena en el TPM y nunca abandona el 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 dejará el entorno seguro del TPM y seguirá siendo segura incluso en caso de violación de seguridad.

6.2 Certificación FIPS 140-2

En el caso de algunos productos y casos de uso, es posible que sea necesario utilizar un TPM para proteger la información, en ocasiones junto con un requisito de conformidad con FIPS 140-2. FIPS (estándares federales de procesamiento de información) 140-2 es un estándar de seguridad de la información para los módulos criptográficos emitidos por el NIST (Instituto Nacional de Estándares y Tecnología).

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.

Puede encontrar más información sobre los requisitos de certificación de FIPS 140-2 en el sitio web del NIST *https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards*

6.2.1 TPM certificado en productos Axis

El TPM que se utiliza en productos de Axis seleccionados está certificado para cumplir con los requisitos de la norma FIPS 140-2. Más concretamente, está certificado para el nivel de seguridad 2 de la norma, lo que significa que el TPM también cumple con los requisitos para autorización basada en funciones y evidencia de manipulaciones, entre otros requisitos.

7 IEEE 802.1 AR - verificación del dispositivo con 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. Al inspeccionar visualmente el producto y aplicar sus conocimientos previos de aspecto de los productos de Axis, el cliente puede sentir la tranquilidad de que el producto 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, se ha utilizado para interactuar primero con un nuevo producto a través de una red cerrada, en la que la unidad se puede aprovisionar de forma segura.

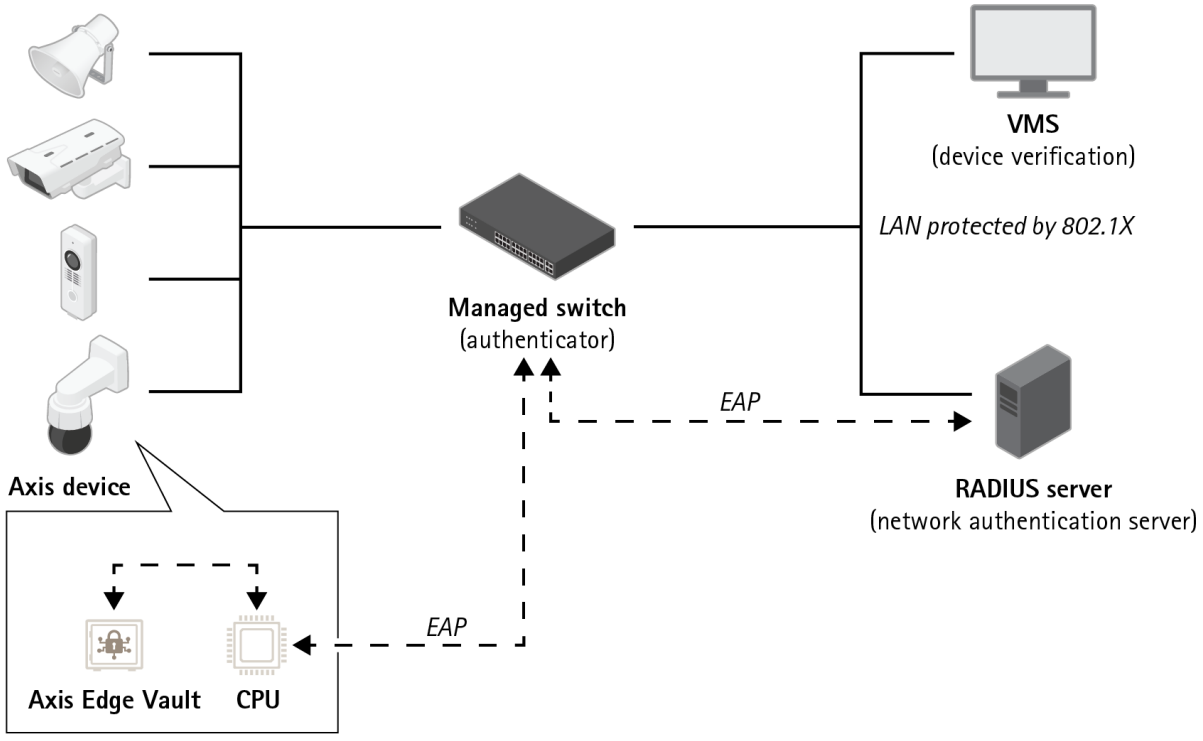

Figure 4. Los clientes pueden indicar a su servidor de autenticación que acepte automáticamente los productos Axis adquiridos en la red mediante los números de serie del dispositivo y el ID de dispositivo de AXIS.

El nuevo estándar internacional IEEE 802.1AR (*https://1.ieee802.org/security/802-1ar/*) define un método para automatizar y asegurar la identificación de un dispositivo a través de 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.

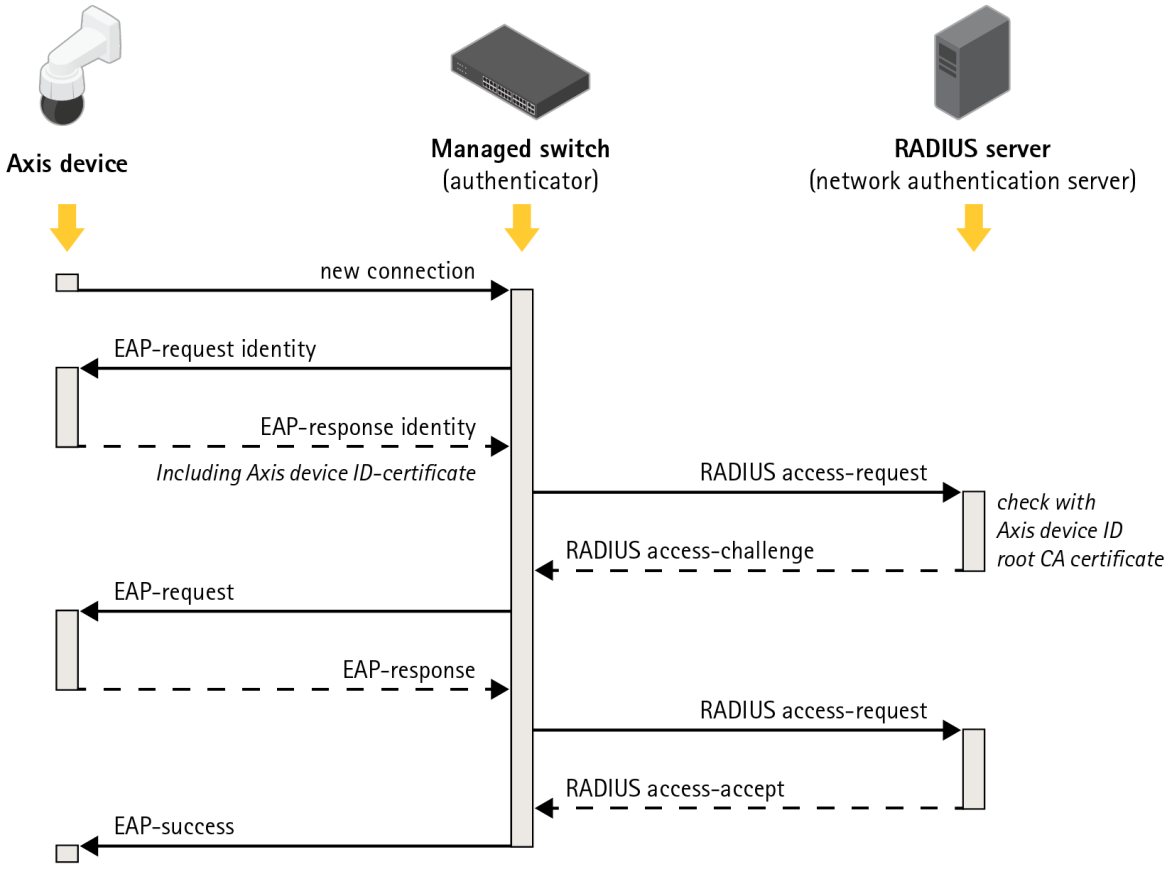

Figure 5. IEEE 802.1AR define un método para identificar un dispositivo a través de una red mediante un protocolo que envía solicitudes de protocolo de autenticación extensible (AEP) al switch que utiliza el servicio de usuario de acceso telefónico de autenticación remota (RADIUS): solicitudes para conceder acceso.

En los productos de Axis, estas medidas de seguridad se implementan mediante el uso de Axis Edge Vault e ID de dispositivo de AXIS. Axis Edge Vault es un módulo seguro en el que está instalado el ID de dispositivo de AXIS, una colección de certificados para verificar la identificación de dispositivos. Estas características ofrecen a su red pruebas criptográficamente comprobables 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 proporcionar más información de campo sobre el dispositivo con otras claves o certificados, lo que le permite 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 despliegue de los dispositivos, porque es necesario realizar menos trabajos 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 proporciona un medio para controlar los dispositivos de un sistema de gran tamaño.

7.1 Axis Edge Vault

Axis Edge Vault es un módulo de cómputo de cifrado seguro en forma de chip montado en los PCB dentro del producto. Edge Vault es capaz de almacenar certificados de forma segura y se puede utilizar para operaciones criptográficas en certificados almacenados de forma segura.

Los certificados que se almacenan en Edge Vault no necesitan abandonarlo para ser utilizados por el dispositivo. Permanecen de forma segura en Edge Vault incluso cuando se utilizan, ya que el hardware criptográfico que opera en la clave se instala en el mismo chip físico.

7.2 ID de dispositivo de AXIS

Durante la producción de cada unidad de 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 de funcionamiento 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.

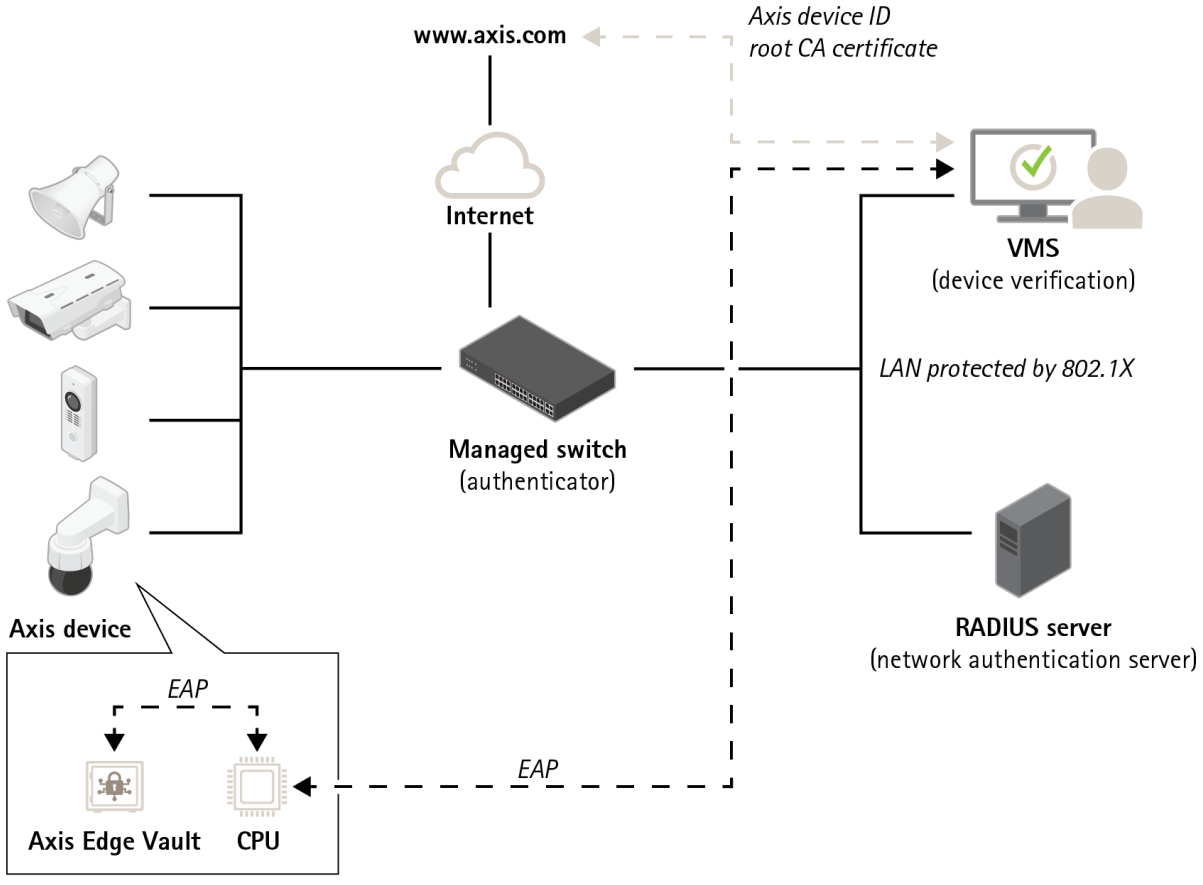

Figure 6. Las aplicaciones de software de otras partes del sistema pueden utilizar el ID de dispositivo de AXIS y las operaciones criptográficas para verificar con quién se está comunicando. El ID de dispositivo de AXIS ha sido verificado por el certificado CA root de ID de dispositivo de AXIS público desde axis.com.

7.2.1 Jerarquías de certificados

Un certificado es una pequeña pieza de datos que combina una clave pública y los 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. Consideremos 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 de hecho 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 CA root 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 CA root de ID de dispositivo de AXIS ha comprobado correctamente el certificado de Axis de una unidad conectada a la red.

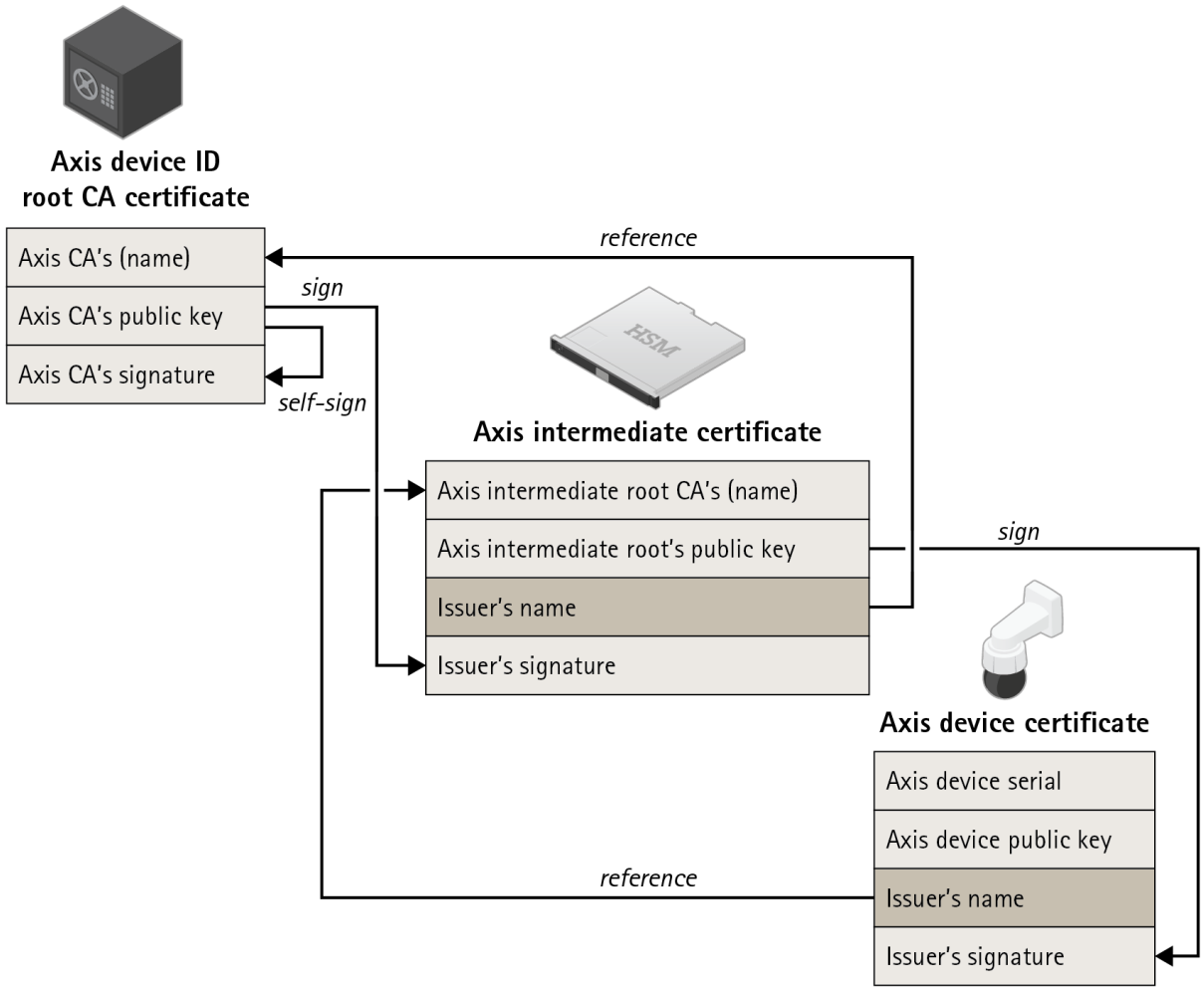

Figure 7. El ID del dispositivo de Axis, que es un certificado que incorpora el número de serie del producto, está firmado por un certificado intermedio, firmado por el certificado root de Axis. Dado que el certificado root de Axis es muy valioso y debe almacenarse en un lugar seguro, se necesita el certificado intermedio durante el aprovisionamiento en la fábrica.

T10154694/ES/M1.8/2007

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.

Axis cuenta con más de 3.500 empleados especializados en más de 50 países, y proporciona soluciones a sus clientes en colaboración con empresas asociadas de todo el mundo. Fue fundada en 1984 y su sede central se encuentra en Lund, Suecia.

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