

Recursos de segurança cibernética em produtos Axis

- firmware assinado
- inicialização segura
- Axis Edge Vault
- ID de dispositivo Axis
- vídeo assinado

Novembro 2021

Sumário

1	Resumo	3
1.1	Firmware assinado	3
1.2	Inicialização segura	3
1.3	Axis Edge Vault	3
1.4	ID de dispositivo Axis	3
1.5	– Vídeo assinado	4
2	Glossário	4
3	Introdução	5
4	Detecção de violação de firmware	5
4.1	Assinatura de firmware	5
4.2	Firmware assinado na Axis	6
5	Prevenção de violações na cadeia de suprimentos	7
5.1	Inicialização segura	7
5.2	Inicialização segura da Axis	7
5.3	Inicialização segura e certificados de firmware personalizados	8
6	Segredos protegidos contra violação	8
6.1	ID de dispositivo Axis	8
7	Armazenamento de chave seguro	9
7.1	Armazenamento seguro de certificados com Axis Edge Vault	10
7.2	Armazenamento de chave seguro com um TPM (Trusted Platform Module)	10
7.3	Certificação FIPS 140-2	10
8	IEEE 802.1 AR – Verificação de dispositivo com o ID de dispositivo Axis	11
9	Detecção de violação de vídeo	13
9.1	– Vídeo assinado	13

1 Resumo

Este documento descreve alguns dos recursos disponíveis nos produtos Axis que podem mitigar ameaças cibernéticas e combater tipos específicos de ataques. Os recursos são:

- firmware assinado
- inicialização segura
- Axis Edge Vault
- ID de dispositivo Axis
- vídeo assinado.

As ameaças descritas incluem:

- violação de firmware
- violação da cadeia de suprimentos
- extração de chaves privadas
- substituição não autorizada de dispositivos.
- violação de vídeo.

1.1 Firmware assinado

O firmware assinado é implementado pelo fornecedor do software que assina a imagem de firmware com uma chave privada. Quando um firmware tem essa assinatura conectada a ele, um dispositivo valida o firmware antes de aceitar instalá-lo. Se o dispositivo detectar que a integridade do firmware está comprometida, a atualização do firmware será rejeitada.

1.2 Inicialização segura

A inicialização segura é um processo de inicialização que consiste em uma cadeia inquebrável de software validada criptograficamente e que começa em uma memória imutável (ROM de inicialização). Baseada no uso de firmware assinado, a inicialização segura garante que um dispositivo possa ser inicializado somente com firmware autorizado.

1.3 Axis Edge Vault

O Axis Edge Vault é um módulo de computação criptográfica seguro que pode ser usado para operações criptográficas em certificados armazenados com segurança. O Edge Vault fornece armazenamento protegido contra violações, permitindo que cada dispositivo proteja os próprios segredos. Ele estabelece uma base para a implementação segura de recursos de segurança mais avançados.

1.4 ID de dispositivo Axis

O ID de dispositivo Axis funciona como um passaporte digital e é exclusivo para cada unidade do dispositivo. Ele é armazenado de forma segura e permanente no Edge Vault como um certificado assinado

pelo certificado raiz da Axis. O ID de dispositivo Axis foi projetado para provar a origem do dispositivo, permitindo um novo nível de confiança em relação ao dispositivo durante o ciclo de vida do produto.

1.5 – Vídeo assinado

O vídeo assinado garante que a evidência em vídeo possa ser confirmada como não manipulada sem provar a cadeia de custódia do arquivo de vídeo. Cada câmera usa um ID de dispositivo Axis único mantido seguro no Axis Edge Vault para adicionar uma assinatura ao stream de vídeo. Quando o vídeo é reproduzido, o reprodutor de arquivos mostra se o vídeo está intacto. O vídeo assinado, portanto, torna possível rastrear o vídeo de volta à câmera de origem e verificar se o vídeo não foi adulterado depois de sair da câmera.

2 Glossário

Certificado – Em criptografia, um certificado é um documento assinado que atesta a origem e as propriedades de um par de chaves. O certificado é assinado por uma autoridade de certificação (CA) e, se o sistema confiar na autoridade de certificação, ele também confiará nos certificados emitidos por ela.

Autoridade de certificação, CA – A raiz de confiança para uma cadeia de certificados. Ele é usado para comprovar a autenticidade e a veracidade de certificados subjacentes.

FIPS – Federal Information Processing Standards, padrões para criptografia de dados e segurança de dados emitidos nos EUA pelo NIST (National Institute of Standards and Technology).

ROM imutável – Para armazenar com segurança as chaves públicas confiáveis e os programas que são usados para comparar assinaturas para que eles não possam ser sobrescritos.

Provisionamento – O processo de preparar e equipar um dispositivo para a rede. Isso envolve a distribuição de dados de configuração e configurações de políticas para o dispositivo a partir de um ponto central. O dispositivo é fornecido com chaves e certificados.

Criptografia de chave pública – Um sistema de criptografia assimétrica em que qualquer pessoa pode criptografar uma mensagem usando a *chave pública* do receptor, mas somente o receptor – usando a *chave privada* – pode descriptografar a mensagem. Ela pode ser usada para criptografar e assinar mensagens.

TLS – Transport Layer Security, padrão da Internet usado para proteger o tráfego da rede. O TLS fornece o S (de segurança) em HTTPS.

3 Introdução

A Axis segue as melhores práticas do setor para gerenciar e responder a vulnerabilidades de segurança em nossos produtos para minimizar a exposição dos clientes a riscos cibernéticos. Não há como garantir que os produtos e serviços sejam inteiramente livres de falhas capazes de ser exploradas por ataques maliciosos. E isso não é específico da Axis, mas sim uma condição geral para todos os dispositivos de rede. O que a Axis pode garantir é que sempre fazemos um esforço em conjunto em todos os estágios possíveis para garantir que o menor risco possível esteja associado aos seus dispositivos e serviços Axis.

Para obter mais informações sobre a segurança do produto e as vulnerabilidades descobertas, consulte www.axis.com/support/product-security. Para obter mais informações sobre as medidas que você pode tomar para reduzir os riscos de ameaças comuns, baixe o Guia para aumento do nível de proteção Axis na mesma página.

Esse white paper apresenta alguns ataques cibernéticos plausíveis e como eles podem ser evitados em produtos Axis. Ele descreve especificamente como os recursos com firmware assinado e inicialização segura podem impedir a violação do firmware e a violação da cadeia de suprimentos. Também abordamos o uso de um TPM (Trusted Platform Module) e do Axis Edge Vault, os quais podem ser usados para proteger chaves privadas. O Axis Edge Vault é usado para armazenar com segurança o ID de dispositivo Axis, o que permite um novo nível de confiança de dispositivo. O Axis Edge Vault e o ID de dispositivo Axis também permitem usar vídeo assinado, um recurso que serve para verificar se o vídeo não foi adulterado depois de sair da câmera.

4 Detecção de violação de firmware

Um possível vetor de ataque que um indivíduo mal-intencionado pode tentar explorar após falhar em outras tentativas de violação do sistema é fazer com que o proprietário do sistema instale aplicativos, firmware ou outros módulos de software adulterados. O software adulterado pode incluir código mal-intencionado com uma finalidade específica. A recomendação comum é nunca instalar qualquer software de uma fonte em que você não confia plenamente. Em um contexto de sistema de vídeo, pode haver um "homem no meio" que poderia alterar um firmware de dispositivo e enganar os usuários finais para instalá-lo. Isso não é um exercício fácil, e o adversário precisa ser muito experiente e determinado. Ele precisa de uma compreensão extremamente detalhada do design do firmware Axis e de como o firmware opera em um dispositivo. Ainda assim, esses adversários poderão existir se o valor proporcionado pelo ataque a um sistema específico for alto o suficiente. A contramedida usual é o fornecedor de software usar firmware assinado.

4.1 Assinatura de firmware

O firmware assinado é implementado pelo fornecedor de software que assina a imagem de firmware com uma chave privada, a qual é mantida em segredo. Quando um firmware tem essa assinatura conectada a ele, um dispositivo valida o firmware antes de aceitar instalá-lo. Se o dispositivo detectar que a integridade do firmware está comprometida, a atualização do firmware será rejeitada.

O processo de autenticação do firmware é iniciado por meio da computação de um valor de hash criptográfico. O valor, em seguida, é assinado com a chave privada de um par de chave pública/privada antes que a assinatura seja associada à imagem do firmware.

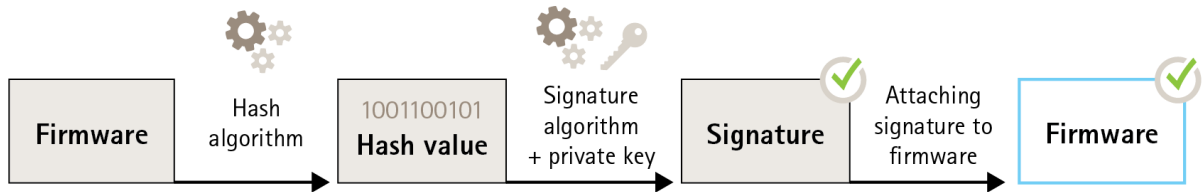


Figure 1. O processo de assinatura do firmware.

Antes de uma atualização de firmware, o novo firmware deve ser verificado. Para garantir que o novo firmware não seja modificado, a chave pública (incluída com o produto Axis) é usada para confirmar se o valor de hash foi realmente assinado com a chave privada correspondente. Ao também calcular o valor de hash do firmware e compará-lo a esse valor de hash validado a partir da assinatura, a integridade do firmware pode ser verificada.

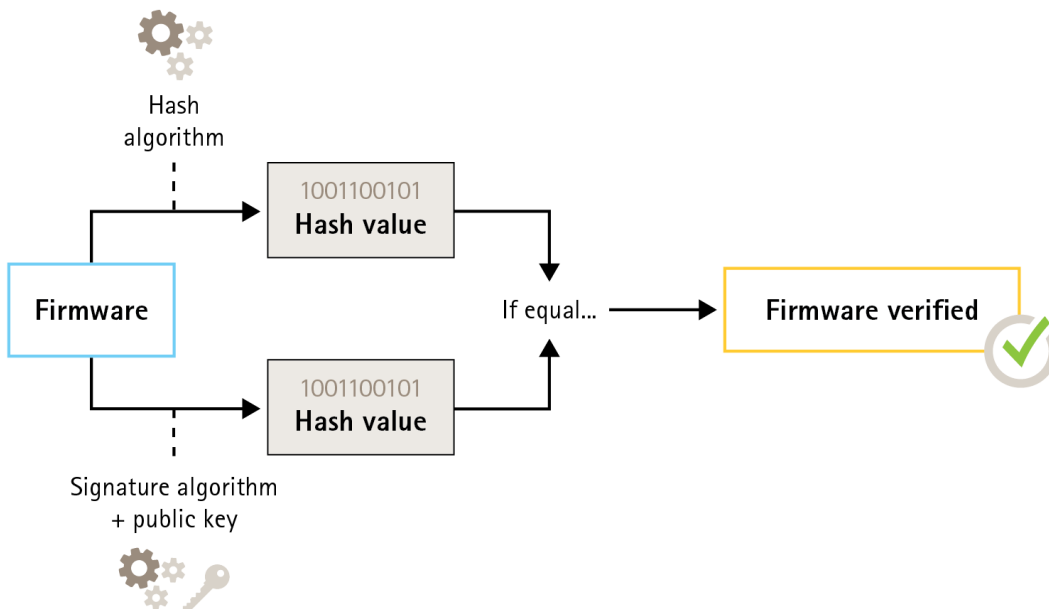


Figure 2. O processo de verificação do firmware assinado.

4.2 Firmware assinado na Axis

O firmware assinado Axis baseia-se no método de criptografia de chave pública RSA amplamente aceito pelo setor. A chave privada é armazenada em um local altamente protegido na Axis, enquanto a chave

pública é incorporada aos dispositivos Axis. A integridade de toda a imagem do firmware é garantida por uma assinatura do conteúdo da imagem. Uma assinatura primária verifica várias assinaturas secundárias, sendo verificada enquanto a imagem é descompactada.

5 Prevenção de violações na cadeia de suprimentos

A assinatura de firmware protege um dispositivo – em todas as futuras atualizações de firmware – contra a instalação de um firmware comprometido. Mas e se alguém no meio do caminho alterar o dispositivo entre o fornecedor e o usuário final? Um indivíduo mal-intencionado com acesso físico ao dispositivo durante o transporte poderia realizar um ataque, como comprometer a partição de inicialização do dispositivo e ignorar a verificação de integridade do firmware para instalar um firmware adulterado antes de o dispositivo ser implantado.

5.1 Inicialização segura

A inicialização segura é um processo de inicialização que consiste em uma cadeia inquebrável de software validada criptograficamente e que começa em uma memória imutável (ROM de inicialização). Baseada no uso de firmware assinado, a inicialização segura garante que um dispositivo possa ser inicializado somente com firmware autorizado.

O processo de inicialização é iniciado pela ROM de inicialização que valida o bootloader. A inicialização segura então verifica, em tempo real, as assinaturas incorporadas para cada bloco de firmware que é carregado da memória flash. A ROM de inicialização serve como raiz de confiança, e o processo de inicialização continua somente enquanto cada assinatura é verificada. Cada parte da cadeia autentica a parte seguinte. No final, o resultado é um kernel Linux e um sistema de arquivos raiz verificados.

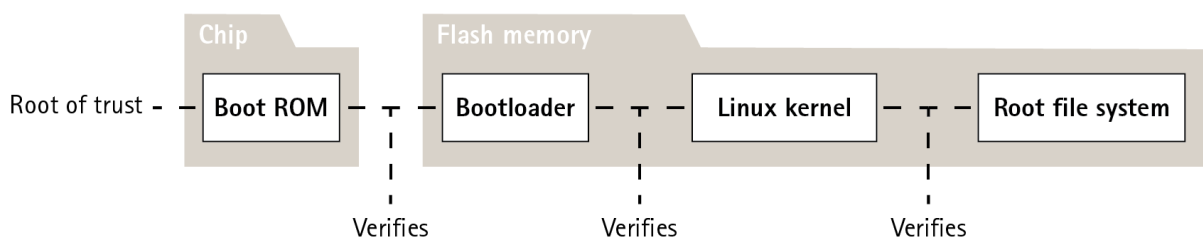


Figure 3. O processo de inicialização segura.

5.2 Inicialização segura da Axis

Em muitos dispositivos, é importante que a funcionalidade de baixo nível seja impossível de mudar. Quando outros mecanismos de segurança estão integrados ao software de nível inferior, a inicialização segura funciona como uma camada de base segura que impede que esses mecanismos sejam burlados.

Em um dispositivo com inicialização segura, o firmware instalado na memória flash é protegido contra modificação. A imagem padrão de fábrica é protegida, enquanto a configuração permanece desprotegida.

A inicialização segura garante que o dispositivo Axis seja completamente protegido contra possíveis malwares após uma reinicialização para os padrões de fábrica.

5.3 Inicialização segura e certificados de firmware personalizados

Embora a inicialização segura torne o produto mais seguro, ela também reduz a flexibilidade com diferentes firmwares. É mais complicado carregar qualquer firmware temporário, como firmwares de teste ou outro firmware personalizado da Axis no produto. No entanto, a Axis implementou um mecanismo que aprova unidades individuais para aceitarem firmwares que não são de produção. Esse firmware é assinado de uma forma diferente, com aprovação tanto do proprietário como da Axis, o que resulta em um certificado de firmware personalizado. Quando instalado nas unidades aprovadas, o certificado permite o uso de um firmware personalizado que pode ser executado apenas na unidade aprovada, com base em seu número de série exclusivo e ID de chip. Os certificados de firmware personalizados podem ser criados apenas pela Axis, uma vez que a Axis possui a chave para assiná-los.

6 Segredos protegidos contra violação

Um requisito básico para qualquer sistema distribuído seguro é a capacidade de verificar as conexões e evitar espionagem. Isso exige que cada dispositivo proteja seus segredos usando um armazenamento seguro protegido contra violações. O Axis Edge Vault oferece esse armazenamento e, com base nesse fundamento, recursos de segurança mais avançados podem ser implementados com segurança.

6.1 ID de dispositivo Axis

Durante a produção de cada unidade de dispositivo de rede Axis, um "passaporte digital" denominado ID de dispositivo Axis é instalado com segurança no Axis Edge Vault da unidade. Essa identidade é exclusiva para cada unidade e foi desenvolvida para comprovar a origem do dispositivo. O ID de dispositivo Axis é um conjunto de certificados que é usado na parte de operação de criptografia do módulo para assinar os desafios apresentados pelo firmware do produto incorporado ao Edge Vault. A resposta dessa operação é enviada de volta para o receptor que pode usar as chaves públicas da Axis para validar a autenticação da resposta.

Um certificado é um pequeno trecho de dados que combina uma chave pública e metadados que descrevem a chave junto com uma assinatura do emissor atestando a validade do certificado. Uma hierarquia de certificados é uma forma de provar a origem do certificado.

Vamos considerar uma analogia entre o ID de dispositivo Axis e um passaporte. Se você tem um passaporte, o governo do seu país fornece a garantia de que você é a pessoa que o passaporte alega ser. De forma semelhante, todos os certificados de ID de dispositivo Axis são endossados por um certificado CA raiz de ID de dispositivo Axis. Assim como um agente de imigração confia no governo do seu país para ter

emitido corretamente seu passaporte, um sistema de segurança de rede confia no certificado CA raiz do ID de dispositivo Axis para verificar corretamente o certificado Axis de uma unidade conectada à rede.

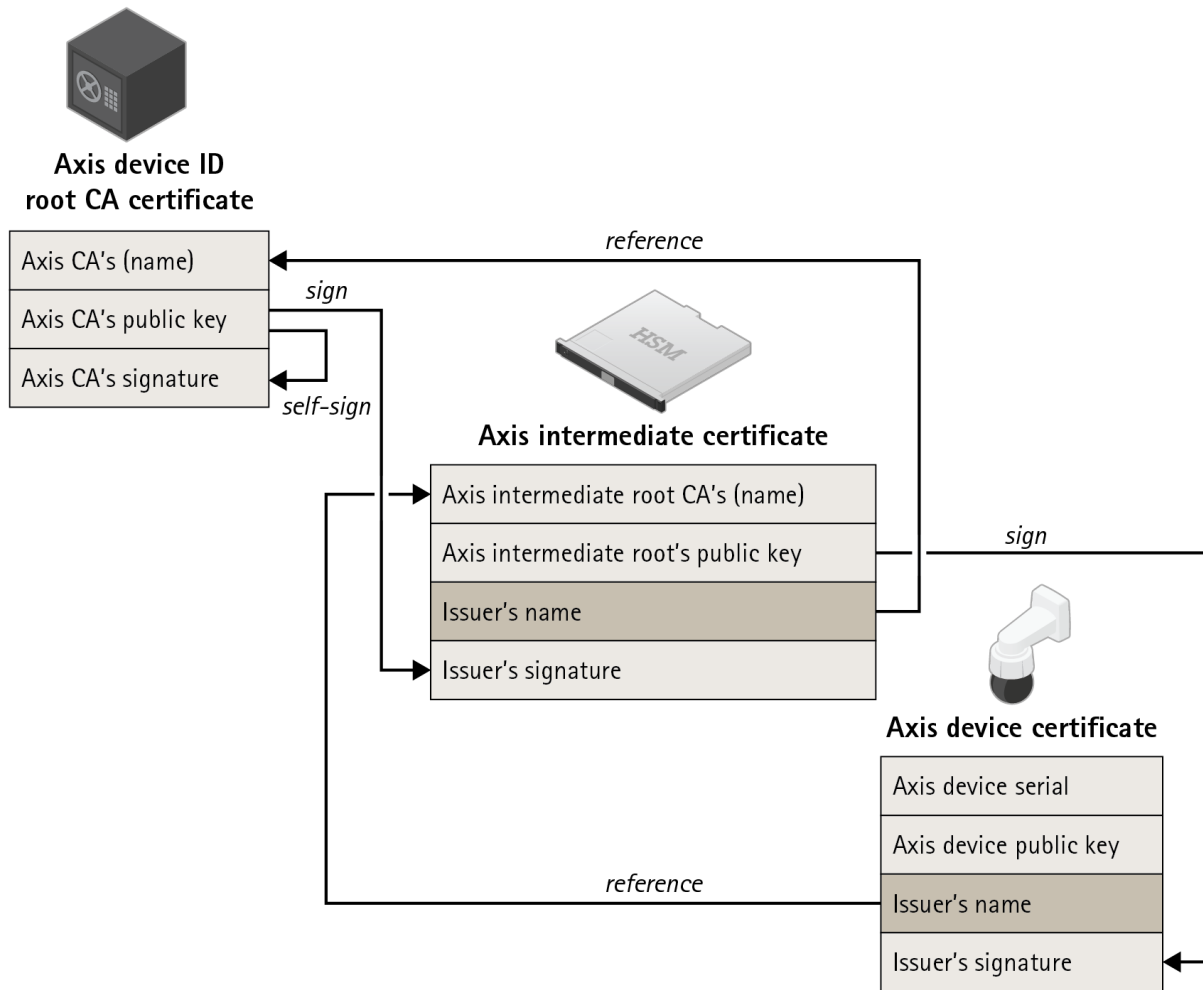


Figure 4. O ID de dispositivo Axis, que é um certificado que incorpora o número de série do produto, é assinado por um certificado intermediário que foi assinado pelo certificado raiz da Axis. Como o certificado raiz Axis é muito valioso e precisa ser armazenado em um cofre, o certificado intermediário é necessário durante o provisionamento na fábrica.

7 Armazenamento de chave seguro

Os dispositivos Axis oferecem suporte a HTTPS (criptografia de rede) e 802.1X (controle de acesso à rede) que usam TLS (Transport Layer Security). Os certificados digitais da TLS usam um par de chaves pública/privada. A chave privada é armazenada no dispositivo enquanto a chave pública está incluída no certificado. Observe que, se nem o HTTPS nem o 802.1X forem usados, não haverá chaves para proteger.

Um indivíduo mal-intencionado pode tentar extrair a chave privada e o certificado do dispositivo e instalá-las em um computador de ataque. No caso do HTTPS, essa chave privada pode ser usada para espionar o tráfego de rede criptografado entre o dispositivo e o VMS. Em caso de spoofing da rede, o computador que ataca pode obter acesso ao VMS fingindo ser um dispositivo legítimo. No caso do 802.1X,

o adversário poderia usar a chave privada para obter acesso a uma rede protegida por 802.1X fingindo ser um dispositivo confiável.

Os certificados e chaves privadas normalmente são armazenados no sistema de arquivos de um dispositivo, protegidos pela política de acesso à conta e usados no ambiente de computação normal. Na maioria dos casos, isso é suficiente, pois a conta não é facilmente comprometida. Observe que certificados poderão ser revogados se houver suspeita de comprometimento, tornando a chave privada inútil.

Alguns usuários finais de sistemas críticos podem enfrentar um risco maior de adversários determinados e experientes que tentam violar o dispositivo para extrair a chave privada. O Axis Edge Vault pode ser usado para armazenar a chave de forma que seja quase impossível extraí-la, mesmo quando o dispositivo está comprometido.

7.1 Armazenamento seguro de certificados com Axis Edge Vault

O Axis Edge Vault é um módulo de computação de criptografia segura na forma de um chip montado na placa de circuito impresso do produto. O Edge Vault permite armazenar certificados com segurança e pode ser usado em operações de criptografia em certificados armazenados de forma segura.

Os certificados armazenados no Edge Vault não precisam deixá-lo para ser usados pelo dispositivo. Eles permanecem em segurança no Edge Vault até mesmo quando estão sendo usados, pois o hardware de criptografia que opera a chave está instalado no mesmo chip físico.

7.2 Armazenamento de chave seguro com um TPM (Trusted Platform Module)

Um TPM é um componente que fornece um determinado conjunto de recursos de criptografia adequados para a proteção de informações contra acesso não autorizado. A chave privada é armazenada no TPM e nunca deixa o TPM. Todas as operações de criptografia que exigem o uso da chave privada são enviadas para o TPM para processamento. Isso garante que a parte secreta do certificado nunca saia do ambiente seguro dentro do TPM e permaneça protegida mesmo em caso de violação de segurança.

7.3 Certificação FIPS 140-2

Para alguns produtos e casos de uso, pode ser um requisito regulatório usar um TPM para proteger informações, às vezes em combinação com um requisito de conformidade com o FIPS 140-2. O FIPS (Federal Information Processing Standard) 140-2 é um padrão de segurança da informação para módulos criptográficos, emitido nos EUA pelo NIST (National Institute of Standards and Technology).

A validação por um laboratório de testes certificado pelo NIST garante que o sistema de módulos e a criptografia do módulo sejam implementados corretamente. Em resumo, o certificado requer descrição, especificação e verificação do módulo de criptografia, dos algoritmos aprovados, dos modos de operação aprovados e dos testes de energia.

Mais detalhes sobre os requisitos de certificação do FIPS 140-2 podem ser encontrados no site do NIST, www.nist.gov

7.3.1 TPM certificado em produtos Axis

O TPM usado em produtos Axis selecionados é certificado para atender aos requisitos do FIPS 140-2. Mais especificamente, ele é certificado para o Nível de Segurança 2 do padrão, o que significa que o TPM também atende aos requisitos de autorização baseada em função e evidência de violação, entre outros requisitos.

8 IEEE 802.1 AR – Verificação de dispositivo com o ID de dispositivo Axis

Uma pessoa comprando um dispositivo de rede Axis pode realizar um exame manual antes de começar a usá-lo. Com a inspeção visual do produto e o uso do conhecimento prévio sobre a aparência dos produtos Axis, o cliente pode se sentir convencido de que o produto é um produto genuíno da Axis. No entanto, esse tipo de inspeção pode ser feito somente por uma pessoa com acesso físico ao produto. Assim, quando você se comunica com um produto não provisionado por meio de uma rede, como é possível ter certeza de que você está se comunicando com a unidade correta? De que o dispositivo não foi substituído sem autorização? Nem o equipamento de rede nem o software nos servidores podem realizar uma inspeção física. Como medida de segurança, é comum interagir primeiro com um novo produto por meio de uma rede fechada, na qual a unidade pode ser provisionada de forma segura.

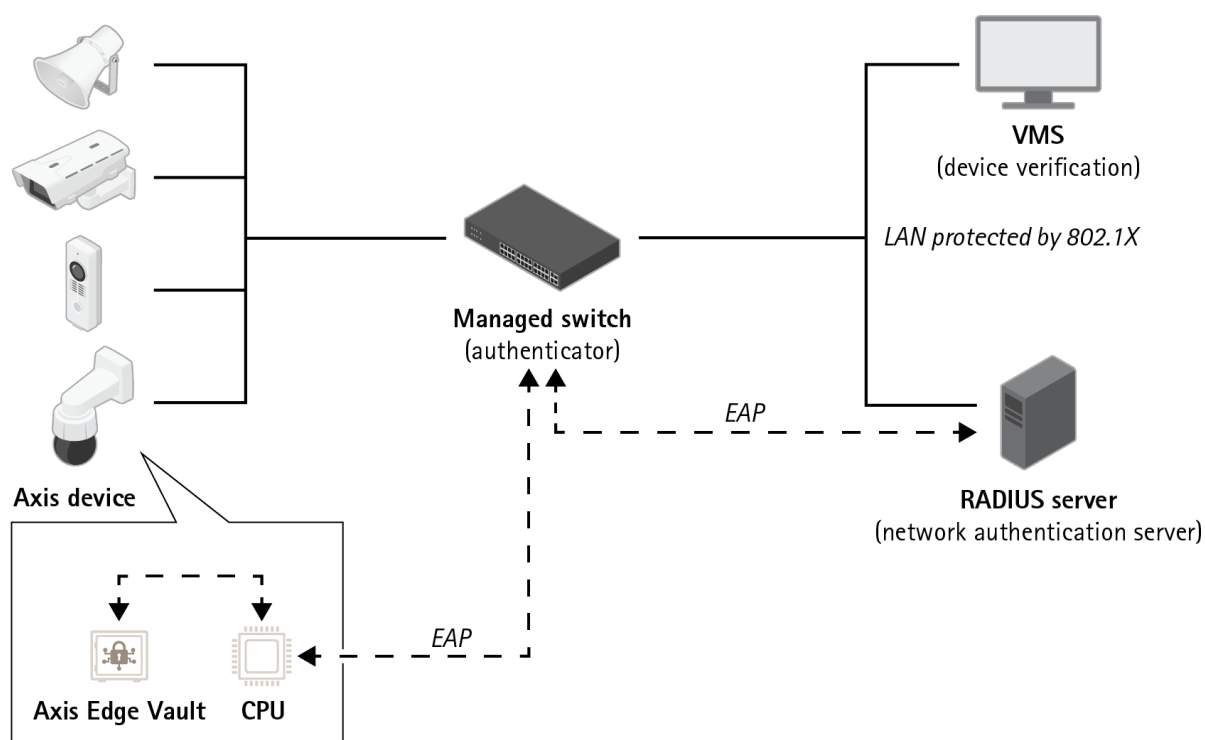


Figure 5. Os clientes podem instruir o servidor de autenticação a aceitar automaticamente na rede produtos Axis comprados usando os números de série dos dispositivos e o ID de dispositivo Axis.

O novo padrão internacional IEEE 802.1 AR (<https://1.ieee802.org/security/802-1ar/>) define um método para automatizar e proteger a identificação de um dispositivo em uma rede. Se a comunicação for encaminhada

para um módulo seguro incorporado, a unidade poderá retornar uma resposta de identificação confiável de acordo com o padrão.

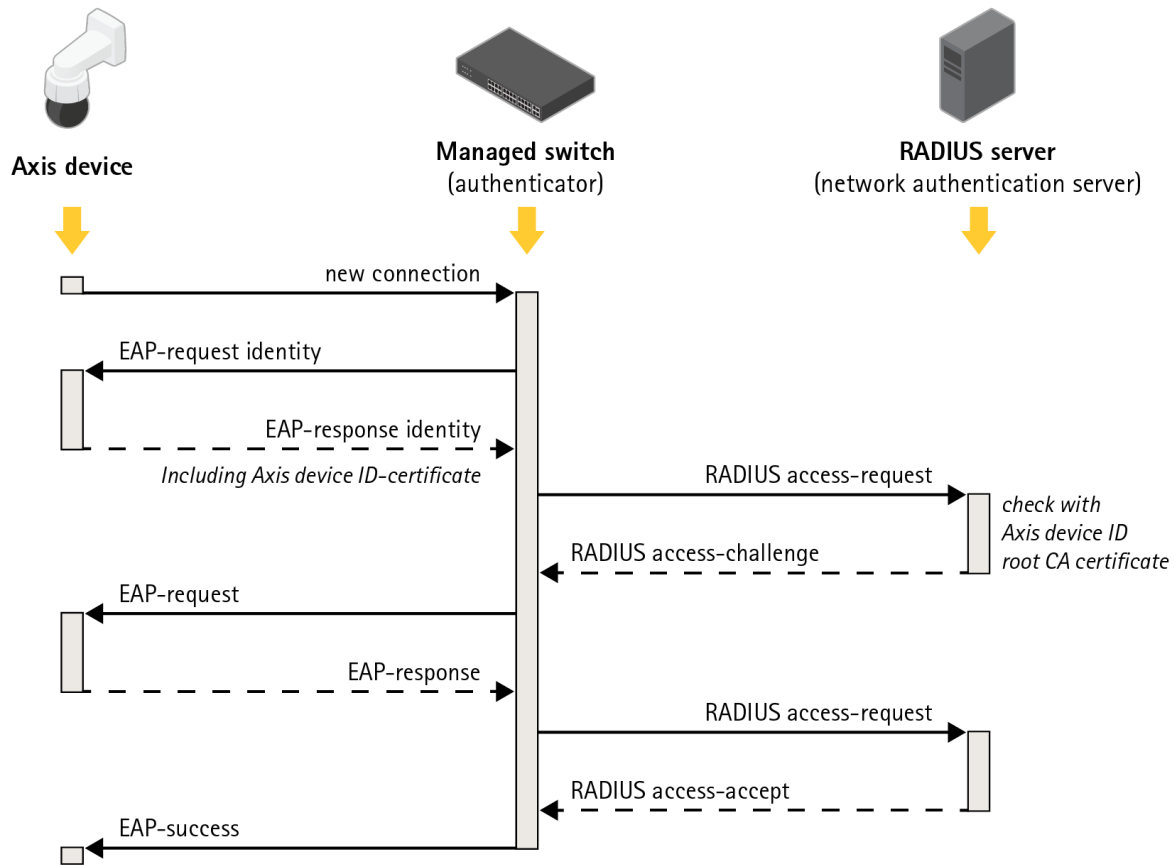


Figure 6. O IEEE 802.1 AR define um método para identificar um dispositivo em uma rede de acordo com um protocolo para enviar solicitações de Extensible Authentication Protocol (AEP) para o switch que usa solicitações de Remote Authentication Dial-in User Service (RADIUS) para conceder acesso.

Nos produtos Axis, essas medidas de segurança são implementadas com o uso do Axis Edge Vault e do ID de dispositivo Axis. O Axis Edge Vault é um módulo seguro no qual o ID do dispositivo Axis, uma coleção de certificados usada para verificar a identificação do dispositivo, está instalado. Esses recursos fornecem à sua rede uma prova criptograficamente verificável de que uma unidade específica foi produzida pela Axis e que a conexão de rede com a unidade é fornecida por essa unidade.

Um dispositivo com ID de dispositivo Axis foi provisionado na fábrica (com chaves e certificados). Este provisionamento pode ser usado posteriormente por um cliente para provisionar ainda mais o dispositivo no campo com outras chaves e/ou certificados, permitindo que ele acesse alguns dos recursos de rede do cliente.

Ao identificar a unidade com o ID de dispositivo Axis, o tempo para a implantação de dispositivos pode ser reduzido, pois menos trabalho precisa ser feito com o dispositivo antes de instalá-lo e configurá-lo na

rede desejada. Outro benefício é que o ID de dispositivo Axis, além de ser uma fonte de confiança interna adicional, também oferece meios de rastrear dispositivos em um sistema de grande porte.

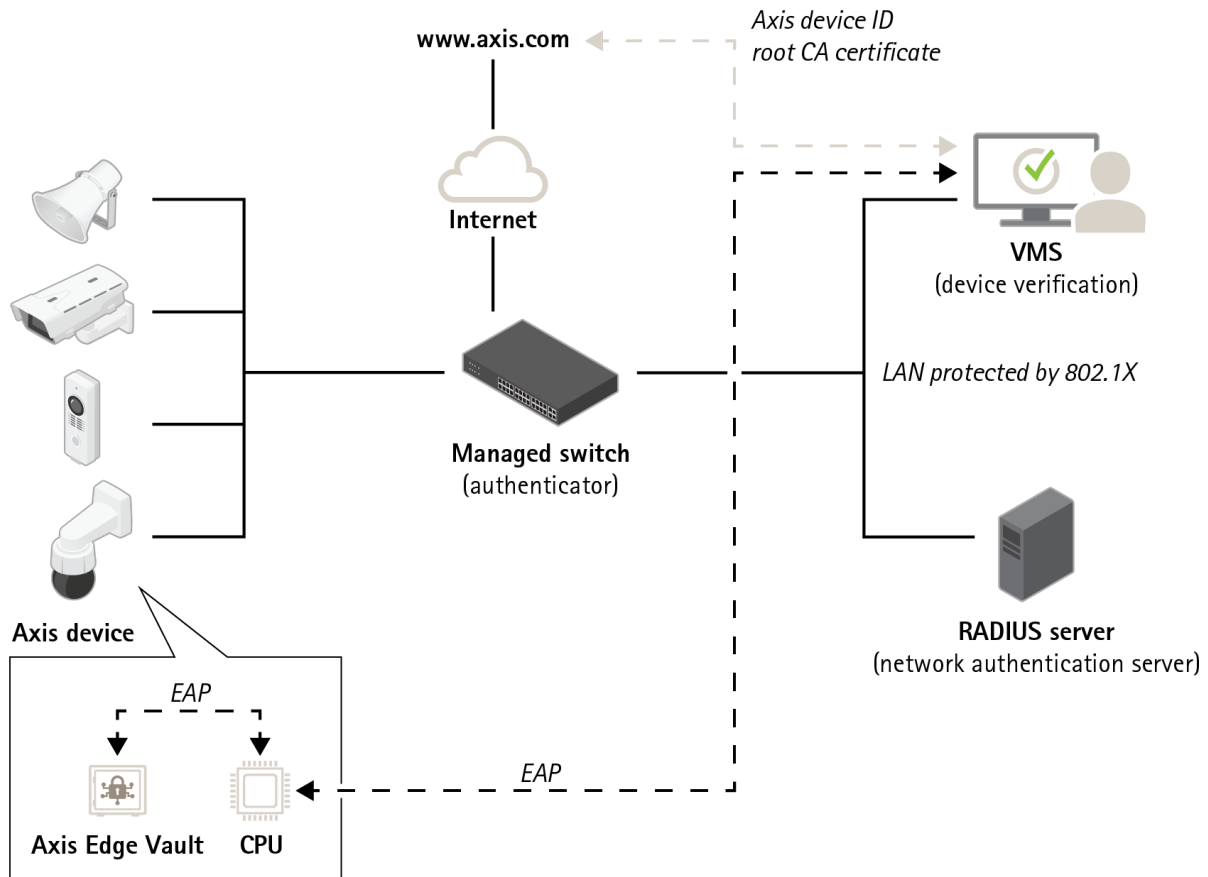


Figure 7. Aplicativos de software em outras partes do sistema podem usar o ID de dispositivo Axis e operações de criptografia para verificar com quem eles estão se comunicando. O ID de dispositivo Axis foi verificado pelo certificado CA raiz do ID de dispositivo Axis do axis.com.

9 Detecção de violação de vídeo

Uma premissa básica no setor de segurança é que os vídeos gravados por câmeras de monitoramento são autênticos e confiáveis. Vídeo assinado é um recurso desenvolvido para manter e aumentar a confiança nos vídeos como evidências. Ao verificar a autenticidade do vídeo, o recurso oferece uma forma de garantir que o vídeo não foi editado ou manipulado após sair da câmera.

9.1 – Vídeo assinado

Com o recurso Vídeo assinado da Axis, é possível usar uma assinatura no stream de vídeo para garantir que o vídeo está intacto e verificar sua origem rastreando-o de volta à câmera que o produziu. Isso torna possível provar a autenticidade do vídeo sem ter que provar a cadeia de custódia do arquivo de vídeo.

Após a gravação de um incidente por um sistema de câmeras de segurança, a polícia pode extrair o vídeo como arquivos de vídeo exportados em um pendrive e salvá-los em um EMS (sistema de gerenciamento de

evidências). Ao exportar o vídeo da câmera, o policial pode ver se o vídeo está assinado corretamente. Se for usado posteriormente em um processo de acusação, o tribunal pode controlar e verificar que horas e por qual câmera o vídeo foi gravado e se algum quadro do vídeo foi alterado ou removido. Com o reproduutor de arquivos da Axis, qualquer pessoa com uma cópia do vídeo pode visualizar essas informações.

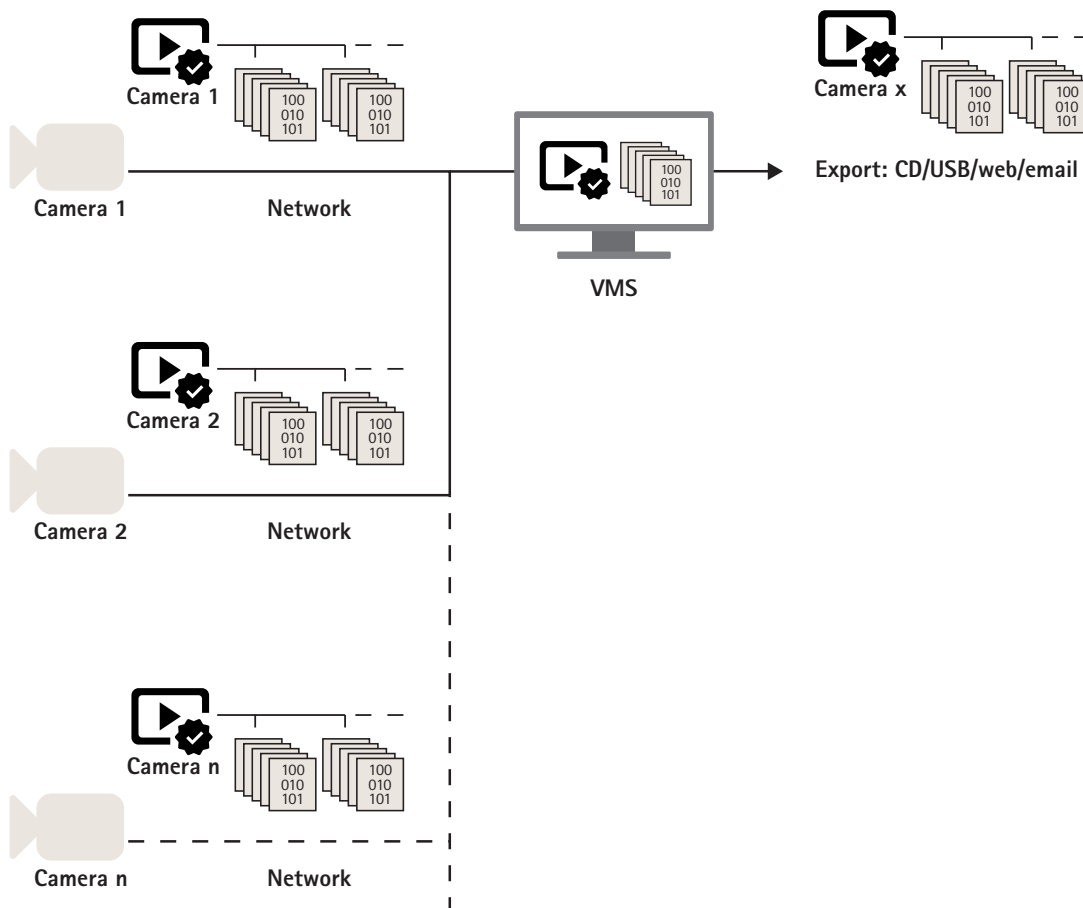


Figure 8. A assinatura já está na câmera, possibilitando a verificação do conteúdo em todas as etapas desde a origem até o uso final do vídeo.

Cada câmera usa um ID de dispositivo Axis único no Axis Edge Vault para adicionar uma assinatura ao stream de vídeo. Isso é feito com o cálculo de um hash de cada quadro de vídeo, incluindo os metadados, e

a assinatura do hash combinado no Edge Vault. A assinatura então é armazenada no stream, em campos de metadados dedicados (o cabeçalho SEI).

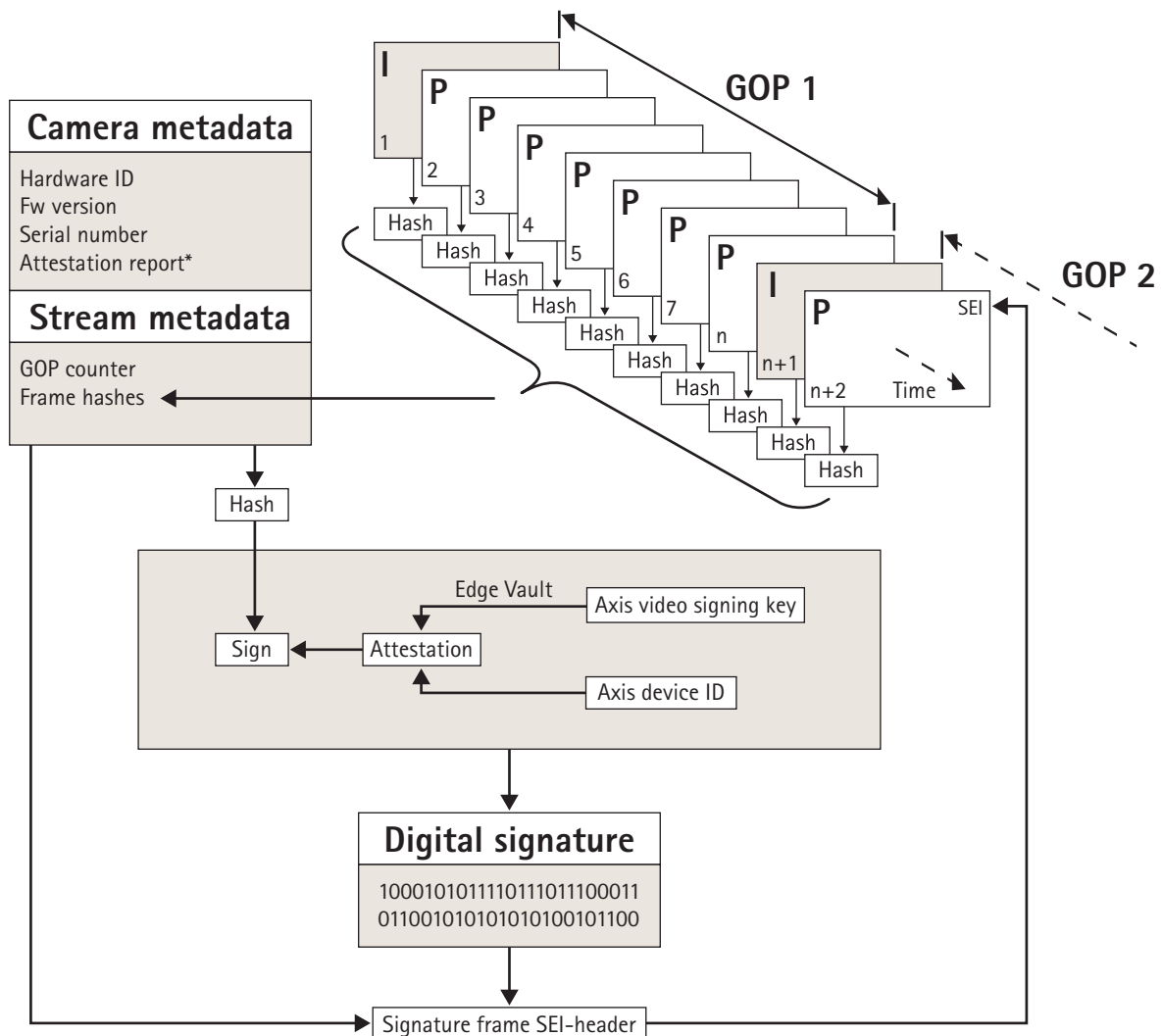


Figure 9. Uma representação gráfica de como uma assinatura é adicionada aos metadados do vídeo. O conteúdo de cada frame de um GOP é concatenado como hash junto com um hash dos metadados da câmera e dos metadados do stream. Isso forma o hash do GOP, que é assinado no Edge Vault. A assinatura e os metadados são então adicionados a um cabeçalho SEI posterior que é transportado ao longo do stream.

* O relatório de atestado pode ser usado para verificar a origem do par de chaves usado para assinatura. Com a verificação do atestado da chave, é possível garantir que a chave está armazenada com segurança no hardware de um dispositivo específico. Isso garante a origem do vídeo.

A assinatura real é feita usando uma chave de assinatura de vídeo específica da unidade atestada para o ID de dispositivo Axis exclusivo do dispositivo. O relatório de atestado é anexado ao stream no início e, depois, em intervalos periódicos, normalmente uma vez a cada hora. Como os metadados contêm o hash de cada quadro individual, é possível detectar qual quadro individual está correto. Para completar a assinatura,

a estrutura GOP do vídeo deve ser protegida. Isso é feito incluindo na assinatura o hash do primeiro quadro I do próximo GOP. Isso evita cortes indetectáveis ou a reordenação dos quadros. As improváveis perdas de frames durante o streaming ou os danos ao conteúdo ao armazená-lo também serão sinalizados assim.

Sobre a Axis Communications

A Axis torna possível um mundo mais inteligente e seguro criando soluções de rede capazes de fornecer percepções para melhorar a segurança e novas maneiras de fazer negócios. Como líder do setor em vídeo em rede, a Axis oferece produtos e serviços de para sistemas de vigilância e análise de vídeo, controle de acesso, intercomunicação e áudio. A Axis conta com mais de 3.800 funcionários dedicados em mais de 50 países e colabora com parceiros em todo o mundo para fornecer soluções aos clientes. A Axis foi fundada em 1984 e sua sede é em Lund, Suécia.

Para obter mais informações sobre a Axis, visite nosso site axis.com.