WHITE PAPER

Axis Edge Vault

Plataforma de segurança cibernética baseada em hardware que protege os dispositivos Axis ao fornecer:

— identidade de confiança de dispositivos

— armazenamento seguro de chave

— detecção de violações de vídeo

— proteção da cadeia de fornecimento

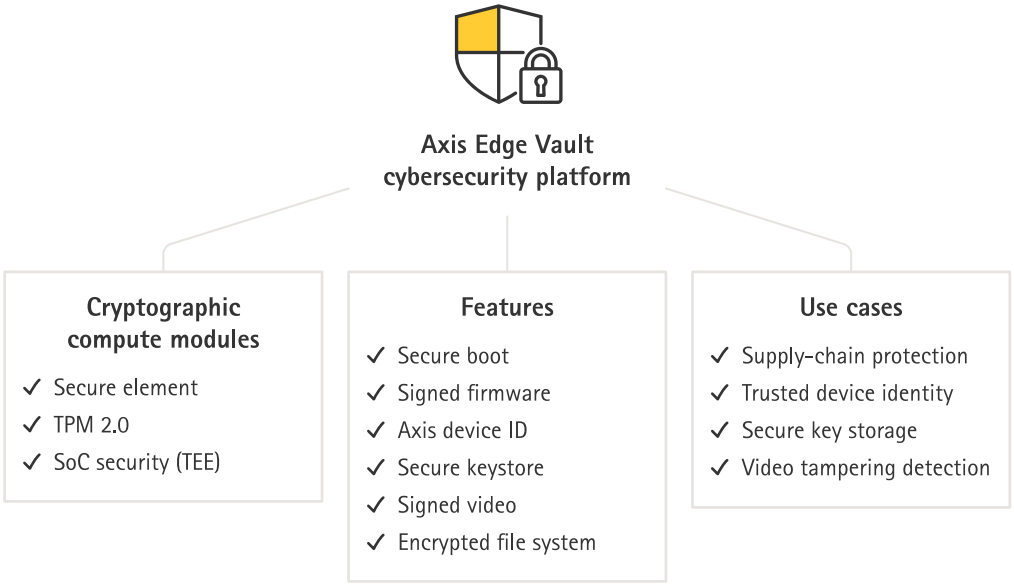
Abril 2023

AXIS COMMUNICATIONS

Resumo

O Axis Edge Vault fornece uma plataforma de segurança cibernética baseada em hardware que protege o dispositivo Axis. Ele depende de uma base sólida de módulos de computação criptográfica (elemento seguro e TPM) e segurança SoC (TEE e inicialização segura), combinada com a experiência em segurança de dispositivos de borda. O Axis Edge Vault tem seu ponto de ancoragem na raiz robusta de confiança, estabelecida pela *inicialização segura* junto com o *firmware assinado*. Esses recursos permitem uma cadeia ininterrupta de software criptograficamente validado para a cadeia de confiança da qual dependem todas as operações seguras.

Os dispositivos Axis com o Axis Edge Vault minimizam a exposição do cliente a riscos de segurança cibernética, impedindo a espionagem e a extração maliciosa de informações confidenciais. O Axis Edge Vault também permite que o dispositivo Axis seja uma unidade confiável dentro da rede do cliente.



- **Identidade de confiança de dispositivos**: É crucial conseguir verificar a origem do dispositivo para estabelecer confiança na identidade do dispositivo. Durante a produção, os dispositivos com o Axis Edge Vault recebem um certificado de ID de dispositivo Axis exclusivo, fornecido de fábrica e compatível com IEEE 802.1AR. Isso funciona como um passaporte para comprovar a origem do dispositivo. A ID do dispositivo é armazenada de forma segura e permanente no armazenamento seguro de chaves como um certificado assinado pelo certificado raiz do Axis. A ID do dispositivo pode ser aproveitada pela infraestrutura de TI do cliente para integração segura automatizada e identificação segura do dispositivo.
- **Armazenamento seguro de chaves**: O armazenamento seguro de chaves fornece armazenamento de informações criptográficas com base em hardware e protegido contra violação. O armazenamento seguro de chaves protege a ID do dispositivo Axis, bem como as informações criptográficas carregadas pelo cliente, e impede o acesso não autorizado e a extração maliciosa no caso de uma violação de segurança.
- **Detecção de violações de vídeo**: 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 sua própria chave de assinatura de vídeo exclusiva, que é guardada de forma segura no armazenamento seguro de chaves 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 torna possível rastrear o vídeo de volta à câmera de origem e verificar se o vídeo não foi violado depois que foi retirado da câmera.

- **Proteção da cadeia de fornecimento**: O Axis Edge Vault requer uma base segura que atue como a raiz da confiança. Sem a ajuda da inicialização segura e do firmware assinado, a raiz da cadeia de confiança não pode ser estabelecida. A inicialização segura, junto com o firmware assinado, fornecem uma cadeia ininterrupta de software criptograficamente validado, começando na memória imutável (ROM de inicialização). A inicialização segura garante que um dispositivo possa inicializar apenas com o firmware assinado pela Axis, o que evita a violação da cadeia física de fornecimento. Com o firmware assinado, o dispositivo também é capaz de validar o novo firmware antes de aceitar instalá-lo. Se o dispositivo detectar que a integridade do firmware está comprometida ou o firmware não é assinado pela Axis, a atualização do firmware será rejeitada Isso protege os dispositivos contra violações de firmware.

Sumário

1 Introdução

A Axis segue as melhores práticas do setor na implementação de segurança em nossos produtos. Isso é feito para minimizar a exposição do cliente a riscos de segurança cibernética e para tornar o dispositivo Axis uma unidade confiável na rede do cliente.

O Axis Edge Vault fornece uma plataforma de segurança cibernética baseada em hardware que protege o dispositivo Axis. Ele se baseia em uma base sólida de módulos de computação criptográfica (elemento seguro e TPM) e segurança SoC (TEE e inicialização segura), combinada com a experiência em segurança de dispositivos de borda.

Este white paper descreve a abordagem multicamadas da segurança de dispositivos de borda da Axis, apresenta os riscos comuns e como eles podem ser evitados. O Axis Edge Vault requer uma base segura que atue como a raiz da confiança. Portanto, também examinaremos os aspectos de segurança da cadeia de fornecimento dos dispositivos Axis e aprenderemos como o firmware assinado e a inicialização segura são medidas fundamentais que combatem a violação de firmware e a violação da cadeia física de fornecimento.

Em *https://www.axis.com/support/cybersecurity/resources* você pode encontrar mais informações sobre segurança do produto, vulnerabilidades descobertas e as medidas que você pode tomar para reduzir os riscos de ameaças.

O último capítulo deste white paper contém um glossário.

2 Identidade de confiança de dispositivos

Em redes modernas de segurança zero-trust ("nunca confie, sempre verifique"), é essencial a capacidade de verificar a origem do dispositivo, sua autenticidade e suas conexões. Um dispositivo em rede pode verificar a integridade e a autenticidade de maneira semelhante à forma como você fornece a verificação de sua identidade às autoridades ao mostrar seu passaporte no aeroporto.

2.1 Identificação segura do dispositivo com ID do dispositivo Axis

O padrão internacional *IEEE 802.1 AR* define o método para automatizar e proteger a identificação de um dispositivo em uma rede. Se a comunicação for encaminhada para um módulo de computação criptográfica incorporado, o dispositivo poderá retornar uma resposta de identificação confiável de acordo com o padrão. Essa resposta confiável pode ser usada pela infraestrutura em rede para permitir a integração automatizada e segura do dispositivo em uma rede de provisão para configuração inicial do dispositivo e atualizações de firmware.

Para estar em conformidade com o IEEE 802.1AR, fabricamos a maioria de nossos dispositivos com certificado de ID de dispositivo Axis exclusivo e fornecido de fábrica (identificador inicial de dispositivo IEEE 802.1AR, IDevID). A ID do dispositivo Axis é armazenada com segurança no armazenamento seguro de chaves, protegido contra violação, fornecido por meio de um módulo de computação criptográfica

no próprio dispositivo. Essa identidade é exclusiva para cada dispositivo Axis, e foi desenvolvida para comprovar a origem do dispositivo.

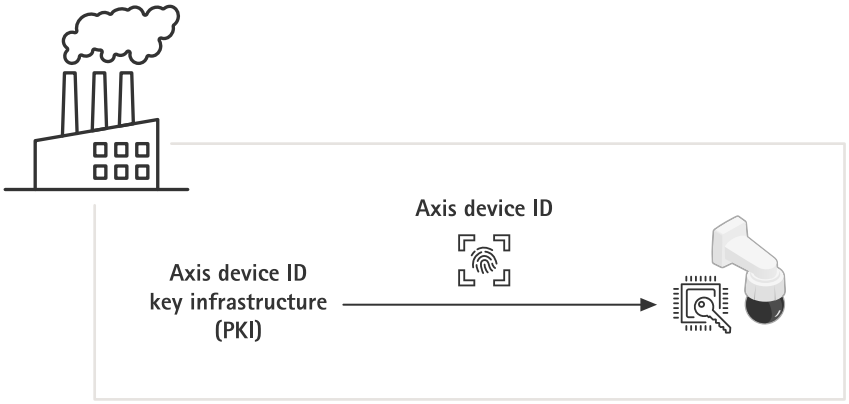


Figure 1. Durante o processo de fabricação de uma unidade, a ID exclusiva do dispositivo Axis é armazenada no armazenamento seguro de chaves da unidade.

O IEEE 802.1AR é baseado no padrão IEEE 802.1X para controle de acesso à rede, que é habilitado por padrão em dispositivos Axis com a ID de dispositivo Axis pré-selecionada. Isso permite a identificação e a autenticação seguras do dispositivo Axis por meio da infraestrutura de TI compatível com 802.1X, mesmo no estado padrão de fábrica.

O certificado da ID do dispositivo Axis vem em várias configurações criptográficas (2048 bits RSA, 4096 bits RSA, ECC-P256). Elas são ativadas por padrão para permitir conexões seguras de dispositivos e identificação por meio do controle de acesso à rede IEEE 802.1X, bem como HTTPS.

A Axis gerencia sua própria infraestrutura de chave pública (PKI) IEEE 802.1AR dedicada para fornecer de fábrica, a ID do dispositivo Axis durante o processo de manufatura. A ID do dispositivo Axis é assinada pelo certificado intermediário que, por sua vez, é assinado pelo certificado raiz do Axis. Tanto a CA raiz quanto a CA intermediária são armazenadas com segurança em módulos de computação criptográfica, separados geograficamente. Isso evita a extração maliciosa em caso de violação de segurança nas

instalações de produção da Axis. Mais informações sobre a infraestrutura Axis PKI podem ser encontradas em *www.axis.com/support/public-key-infrastructure-repository*

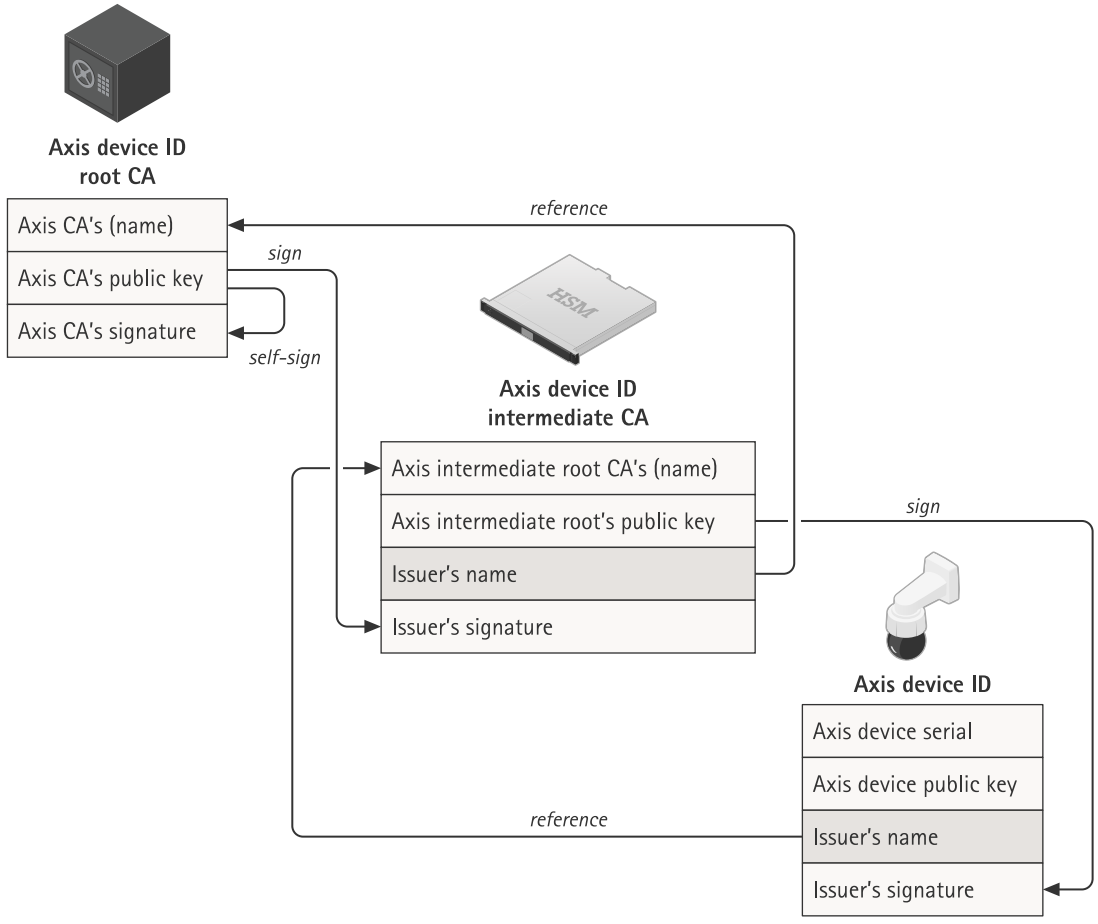


Figure 2. Infraestrutura de chave pública (PKI) IEEE 802.1AR da Axis, para provisionamento de fábrica da ID do dispositivo Axis durante o processo de manufatura. A ID do dispositivo Axis, que é um certificado que incorpora o número de série do produto, é assinada por uma CA intermediária que foi assinada pela CA raiz da ID do dispositivo Axis. Como a CA raiz da Axis é muito valiosa e precisa ser armazenada em um cofre, a CA intermediária é necessária durante o provisionamento na fábrica.

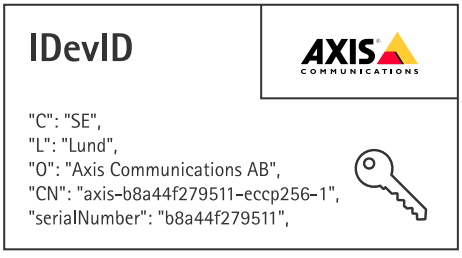


Figure 3. Exemplo de uma ID de dispositivo Axis.

2.2 Integração segura em rede

Ao comprar um dispositivo Axis, você pode fazer um exame manual antes de começar a usá-lo. Ao inspecionar visualmente o dispositivo e usar conhecimento prévio sobre a aparência dos produtos Axis, você pode comporvar que o dispositivo um original da Axis. No entanto, você só consegue fazer esse tipo de inspeção se tiver acesso físico ao dispositivo. Portanto, quando você se comunica com um dispositivo em uma rede, como pode ter certeza de que está se comunicando com o dispositivo correto e pode verificar a identidade? Nem o equipamento de rede nem o software nos servidores podem realizar uma inspeção física. Como medida de segurança, a prática comum é interagir primeiro com um novo dispositivo por meio de uma rede fechada, em que ele pode ser provisionado de forma segura.

A ID do dispositivo Axis fornece à sua rede uma prova criptograficamente verificável de que um dispositivo específico foi produzido pela Axis e de que a conexão da rede com ele é fornecida por esse dispositivo. A ID do dispositivo Axis pode ser usada durante o processo de autenticação de rede IEEE 802.1X para obter acesso a uma rede de provisionamento em que atualizações de firmware e configuração adicionais do dispositivo Axis serão executadas antes que o dispositivo Axis seja movido para a rede de produção.

Ao usar a ID do dispositivo Axis, a segurança geral pode ser aumentada e o tempo para implantação de dispositivos reduzido, pois controles mais automatizados e econômicos podem ser usados para a instalação e configuração de dispositivos.

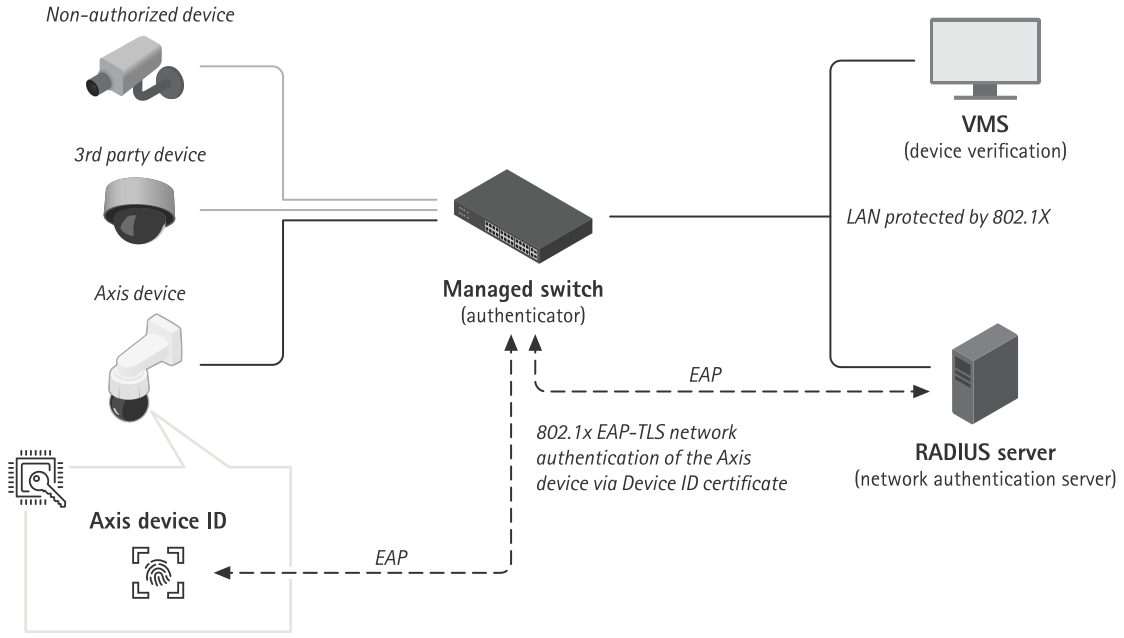


Figure 4. Integração segura em rede. Você pode instruir seu servidor de autenticação para aceitar automaticamente os dispositivos Axis na rede usando o número de série do dispositivo e a ID do dispositivo Axis. A ID do dispositivo Axis é usada como uma impressão digital que garante que os dispositivos sejam integrados de forma segura e automática. Dispositivos não autorizados devem ser integrados manualmente.

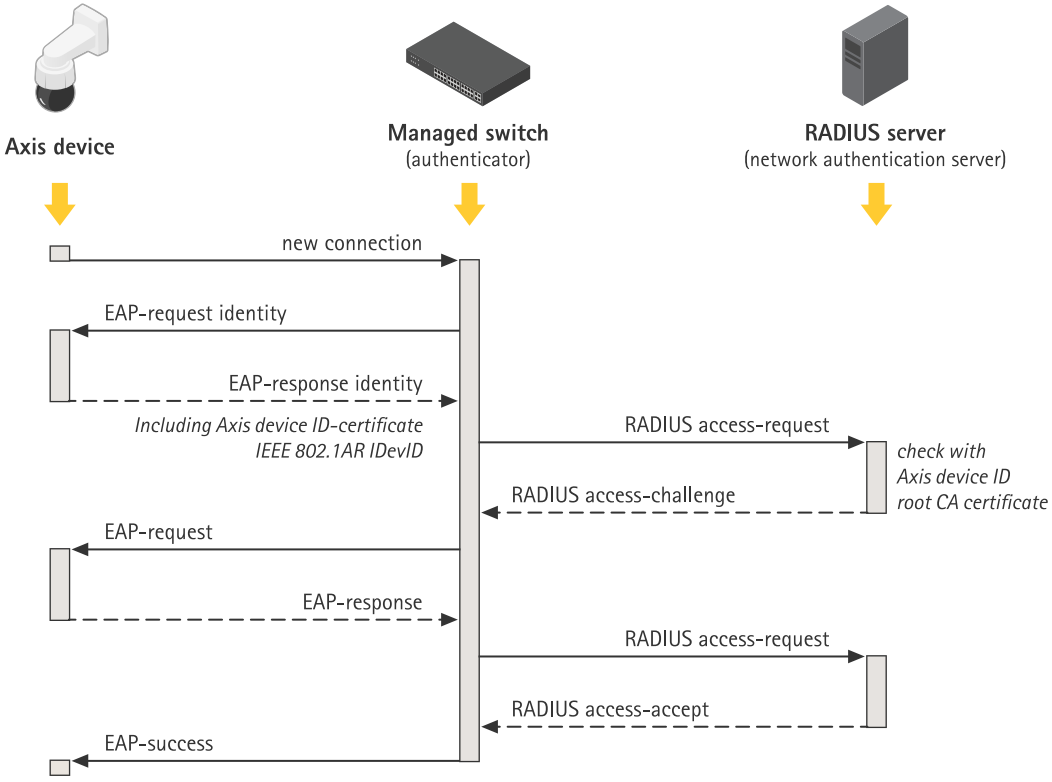


Figure 5. Descrição mais detalhada do processo de integração. O IEEE 802.1AR para identidade segura de dispositivo define um método para identificar um dispositivo por meio de solicitações de protocolo de autenticação extensível IEEE 802.1X (EAP-TLS) usando um servidor RADIUS (Remote Authentication Dial-In User Service) para conceder acesso do dispositivo à rede.

Além de fornecer uma fonte adicional e integrada de confiança, aID de dispositivo Axis também fornece um meio de rastrear dispositivos e permite a verificação e a autenticação periódicas de acordo com os princípios de rede zero-trust.

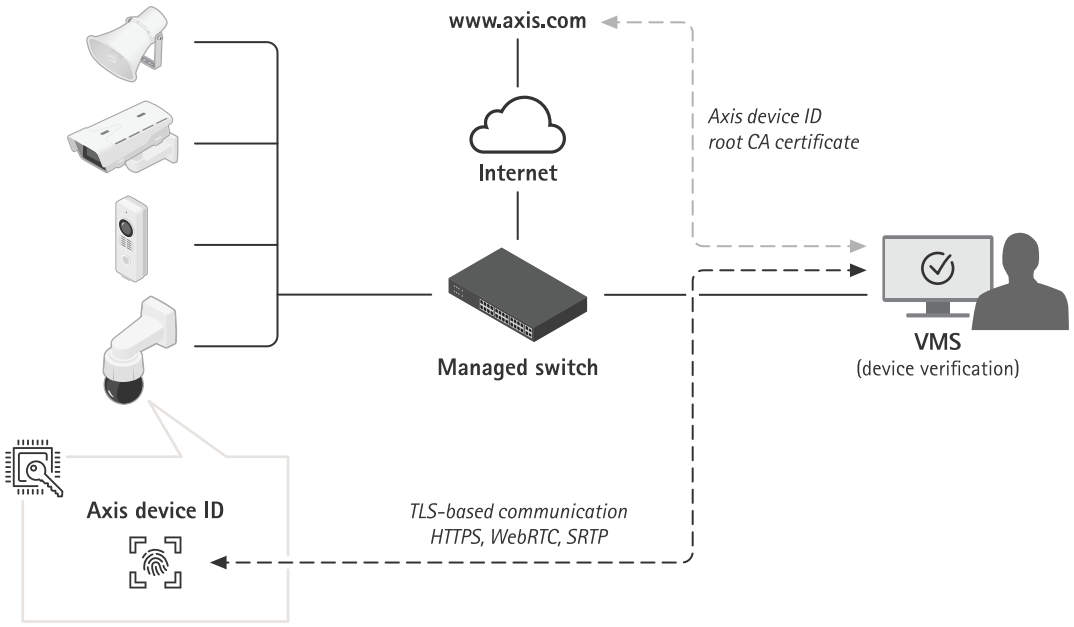


Figure 6. Após a integração segura de um dispositivo, os aplicativos de software em outras partes do sistema podem usar a ID do dispositivo Axis e as operações criptográficas para fazer a verificação do dispositivo em várias comunicações baseadas em TLS. A ID do dispositivo Axis pode ser verificada pelo certificado CA raiz da ID do dispositivo Axis (disponível publicamente) que pode ser baixado em axis.com.

3 Armazenamento de chave seguro

Normalmente, as informações criptográficas X.509 confidenciais (chaves privadas) são armazenadas no sistema de arquivos de um dispositivo. Ele é protegido apenas pela política de acesso à conta do usuário, que fornece proteção básica, porque a conta do usuário não é facilmente violada. No entanto, no caso de uma violação de segurança, essas informações criptográficas ficariam desprotegidas e acessíveis a um inimigo.

De um aspecto de segurança, o armazenamento seguro de chaves é essencial no armazenamento e proteção das informações criptográficas. Não apenas as informações criptográficas confidenciais (incluídas no ID do dispositivo Axis e no vídeo assinado) são armazenadas no armazenamento seguro de chaves, como também as informações carregadas pelo cliente podem ser protegidas da mesma maneira.

3.1 Armazenamento seguro de chaves

As informações criptográficas confidenciais (chaves privadas) são armazenadas no armazenamento seguro de chaves, protegidas contra violação baseada em hardware do dispositivo. Isso evita a extração maliciosa, mesmo em casos de violação de segurança. Além disso, as chaves privadas permanecem protegidas no armazenamento seguro de chaves, mesmo quando estão sendo usadas. Um possível invasor não terá acesso ao armazenamento seguro de chaves e não poderá espionar o tráfego de rede, obter acesso à rede por meio de chaves IEEE 802.1X ou extrair outras chaves privadas.

O armazenamento seguro de chaves é disponibilizado por meio de um módulo de computação criptográfica baseado em hardware. Dependendo dos requisitos de segurança, um dispositivo Axis pode ter um ou vários desses módulos, como um TPM 2.0 (Módulo de Plataforma Confiável) ou um elemento seguro e/ou um TEE (Ambiente Confiável de Execução).

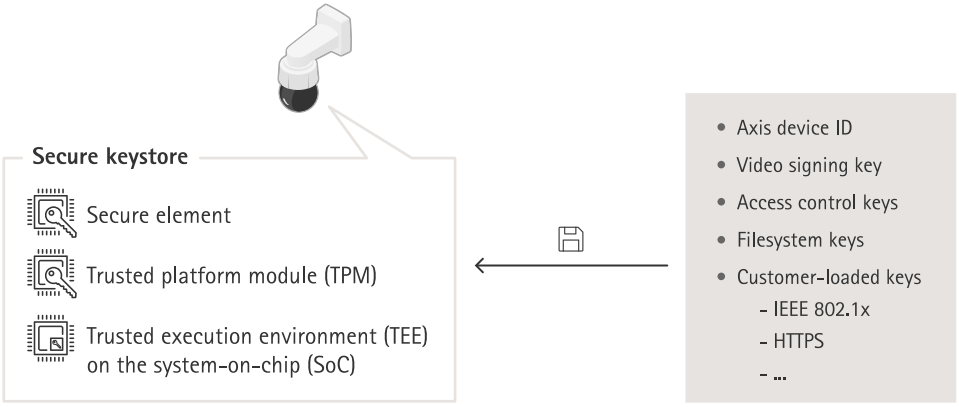


Figure 7. O recurso de armazenamento seguro de chaves em dispositivos Axis pode empregar um elemento seguro, um TPM ou um TEE. Todos eles fornecem proteção de chaves privadas e execução segura de operações criptográficas.

O TPM e o elemento seguro são módulos de computação criptográfica de hardware montados em PCB ao lado do processador principal do SoC. O TEE é uma área segura do próprio processador principal do SoC.

O TPM, o elemento seguro e o TEE fornecem proteção de chaves privadas e execução segura de operações criptográficas. No caso de uma violação de segurança, o acesso não autorizado e a extração maliciosa são evitados.

3.2 Critérios comuns e FIPS 140

Os módulos de computação criptográfica podem ser certificados usando os níveis de avaliação de critérios comuns (CC EAL), bem como os níveis de conformidade FIPS 140 (1-4). Essas certificações são usadas para determinar a exatidão e a integridade das operações criptográficas, e para verificar várias contramedidas de violação, como autoverificação, resistência à violação e outras medidas de resistência. Você pode encontrar informações sobre a certificação na folha de dados de um dispositivo Axis ou no seletor de produtos Axis. A Axis exige que seus módulos incorporados de computação criptográfica de hardware sejam certificados n mínimo de acordo com os Critérios comuns EAL4 e/ou FIPS 140-2/3 nível 2.

3.2.1 Critérios comuns

Os Critérios comuns (CC) (também conhecido como Critérios Comuns para Avaliação de Segurança de Tecnologia da Informação) é um padrão internacional (ISO/IEC 15408) para certificação de segurança de produtos de TI. Os Critérios comuns fornecem uma estrutura para fabricantes e implementadores especificarem os requisitos funcionais e de garantia de segurança como alvos de segurança, que podem ser agrupados em perfis de proteção.

Esses objetivos de segurança reivindicados são então avaliados por laboratórios de testes independentes e certificados, antes de serem listados como produtos certificados no banco de dados dos Critérios comuns. Os requisitos e o rigor da avaliação pelo laboratório de testes são informados por meio de um EAL (Nível de garantia de avaliação) atribuído, variando de EAL 1 — testado funcionalmente a EAL 7 — projeto

formalmente verificado e testado. Isso significa que os Critérios comuns podem abranger desde sistemas operacionais e firewalls até TPMs e passaportes.

Para obter mais detalhes sobre os requisitos de certificação dos Critérios comuns, acesse o site dos Critérios comuns: *www.commoncriteriaportal.org/*

3.2.2 FIPS 140

O FIPS (Padrão Federal de Processamento de Informações) 140-2 e o 140-3 são padrões de segurança de informações para módulos de computação criptográfica, emitidos nos EUA pelo NIST (Instituto Nacional de Padrões e Tecnologia). O FIPS 140-3 substituiu o FIPS 140-2 em 2019 como sua versão atualizada. 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 computação criptográfica, dos algoritmos aprovados, dos modos de operação aprovados e dos testes de energia.

Mais detalhes sobre os requisitos de certificação do FIPS 140-2 e do FIPS 140-3 podem ser encontrados no site do NIST, *www.nist.gov*

3.3 Proteção de chaves privadas

Para um invasor, a extração da chave privada permitiria espionar o tráfego em rede criptografado por HTTPS ou fingir ser o dispositivo verdadeiro e obter acesso a uma rede protegida por 802.1X.

Os dispositivos Axis são compatíveis com vários protocolos baseados em TLS (Segurança da Camada de Transporte) para comunicação segura. Eles dependem da proteção de informações criptográficas X.509, como ID do dispositivo Axis (IEEE 802.1AR), HTTPS (criptografia de rede), 802.1X (controle de acesso à rede) e outros.

Os certificados digitais X.509 de TLS usam um certificado e um par de chaves públicas e privadas correspondentes para que dois hosts em rede se comuniquem. A chave privada é armazenada no armazenamento seguro de chaves e nunca sai dele, mesmo quando é usada para descriptografar dados. O certificado verdadeiro e a chave pública são conhecidos, podem ser compartilhados pelo dispositivo Axis e são usados para criptografar dados.

3.4 Proteção de chaves de controle de acesso

A proteção das informações criptográficas usadas nas soluções de controle de acesso da Axis, como o Canal seguro Open Supervised Device Protocol (OSDP), é outro exemplo da importância do armazenamento de chaves protegidas por hardware.

O Canal seguro OSDP é um esquema de criptografia e autenticação baseado em AES-128, amplamente usado para proteger a comunicação entre controladores de porta e dispositivos periféricos, como leitores.

A chave simétrica AES, Chave Base do Canal Seguro (SCBK), compartilhada pelo controlador de porta e leitor, é usada para iniciar a autenticação mútua e, posteriormente, para gerar um conjunto de chaves de sessão para criptografar os dados de comunicação entre controladores de porta e leitores.

Para alcançar a verdadeira segurança de ponta a ponta, a chave mestra (MK) e o SCBK precisam ser armazenados com segurança no armazenamento seguro de chaves do controlador de porta de rede da Axis. A Chave Mestra deriva uma chave SCBK exclusiva por leitor Axis conectado. Além disso, o SCBK individual, que é distribuído com segurança durante a fase de instalação para um leitor Axis, precisa ser armazenado

com segurança no armazenamento seguro de chaves do leitor. O leitor é mais crítico, considerando que normalmente é instalado no lado inseguro da porta.

Dessa forma, as chaves do Canal Seguro OSDP são protegidas em ambas as extremidades em um ambiente protegido por hardware. Isso evita a extração maliciosa, mesmo em casos de violação de segurança.

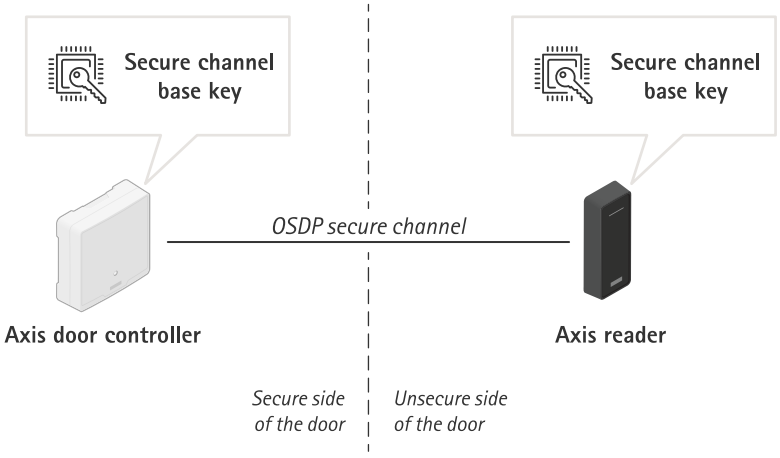


Figure 8. Obtenção da segurança de ponta a ponta com armazenamento seguro de chaves no controle de acesso. A chave mestra e a chave base do canal seguro individual (SCBK) são armazenadas em chaves seguras, em dispositivos em cada lado da porta.

3.5 Proteção das chaves do sistema de arquivos

Um dispositivo Axis em operação carrega informações e configurações específicas do cliente. O mesmo se aplica quando o dispositivo Axis está em trânsito para o cliente de um distribuidor ou integrador de sistemas que forneceu serviços de pré-configuração. Quando um invasor mal-intencionado consegue acessar fisicamente o dispositivo Axis, ele pode tentar extrair informações do sistema de arquivos desmontando a memória flash e acessando-a por meio de um dispositivo leitor de flash. Portanto, proteger o sistema de arquivos de leitura e gravação contra extração de informações confidenciais ou violações de configuração é uma proteção importante para quando o dispositivo Axis for roubado ou ocorrer uma invasão.

O armazenamento seguro de chaves impede a extração maliciosa de informações e impede a violação da configuração ao impor uma criptografia robusta no sistema de arquivos. Quando o dispositivo Axis é desligado, as informações no sistema de arquivos são criptografadas. Durante o processo de inicialização, o sistema de arquivos de leitura/gravação é descriptografado com uma chave AES-XTS-Plain64 256 bits para que o sistema de arquivos possa ser montado e usado pelo dispositivo Axis. A chave de criptografia do sistema de arquivos é gerada exclusivamente por dispositivo no padrão de fábrica e regenerada a

cada atualização de firmware seguinte, o que significa que a chave nunca é a mesma durante todo o ciclo de vida do dispositivo.

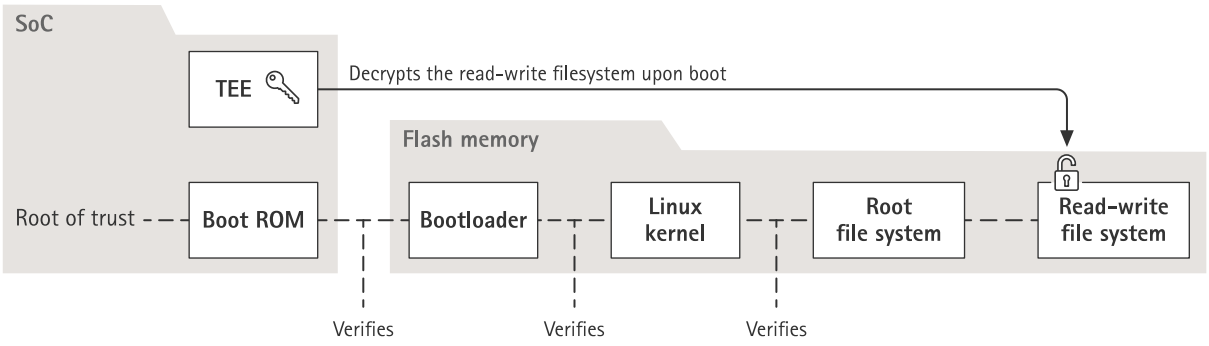


Figure 9. O TEE dentro do SoC contém a chave para descriptografar o sistema de arquivos raiz.

4 Proteção 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.

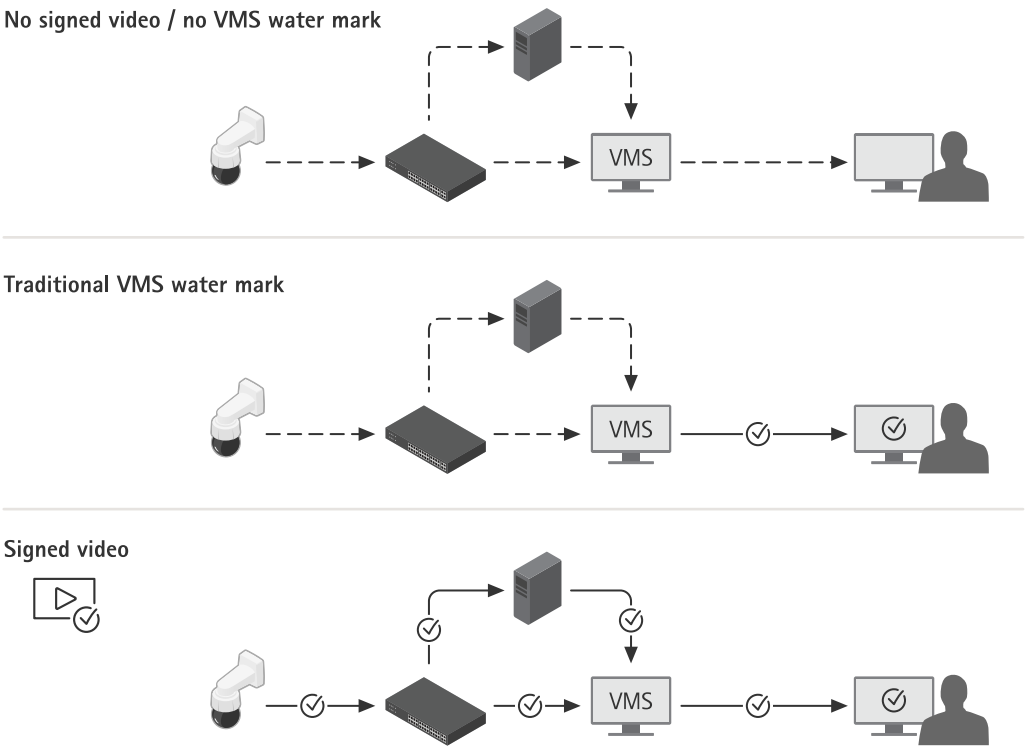


Figure 10. Verificação de autenticidade de vídeo.

Topo: Um vídeo passa por muitas etapas, desde a câmera até a pessoa que assiste à gravação. Um invasor habilidoso pode violar o vídeo em qualquer uma dessas transições.

No meio: Com a marca d'água VMS adicionada ao vídeo durante a exportação, algumas etapas são verificadas, mas não há garantia de que o vídeo não tenha sido violado em um estágio anterior.

Parte inferior: O vídeo assinado garante que o vídeo não foi violado em nenhuma etapa do caminho da câmera para a pessoa que visualiza a gravação exportada. O vídeo pode ser rastreado de volta até o dispositivo que o gravou.

4.1 — Vídeo assinado

Com o recurso Vídeo assinado desenvolvido pela Axis, que foi proativamente disponibilizado como código aberto, 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 receber o vídeo como arquivo de vídeo exportado em um pendrive e salvá-lo 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 reprodutor de arquivos da Axis, qualquer pessoa com uma cópia do vídeo pode visualizar essas informações.

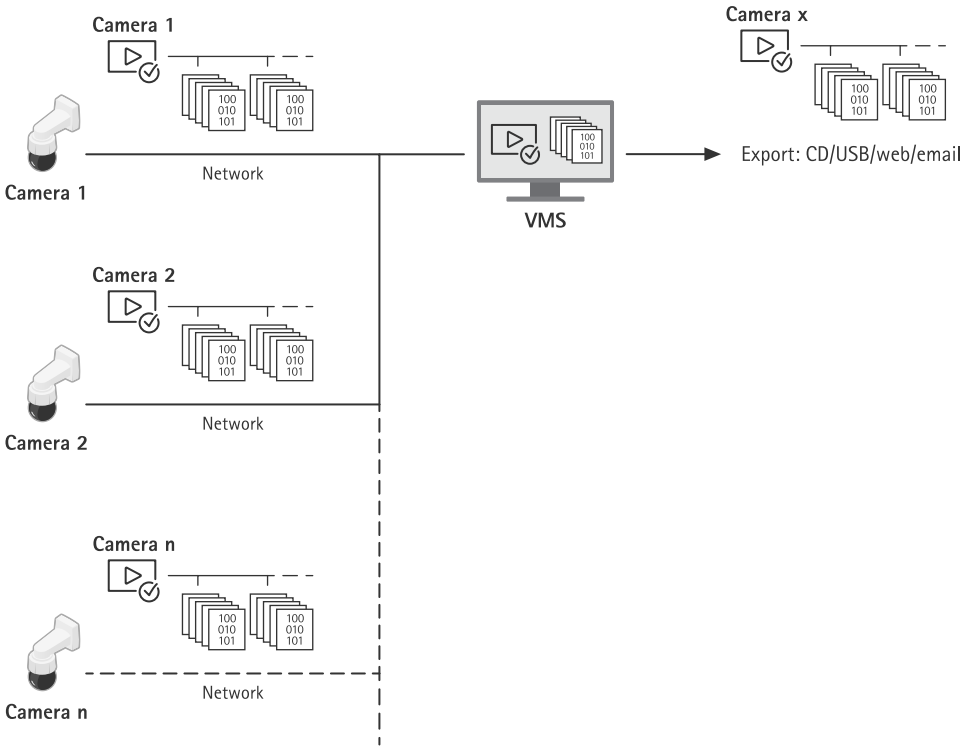


Figure 11. A assinatura já está na câmera, possibilitando a verificação do conteúdo em todas as etapas, desde a origem até o uso final do vídeo.

Cada câmera usa sua própria chave de assinatura de vídeo exclusiva, que é guardada no armazenamento seguro de chaves, para adicionar uma assinatura ao stream de vídeo. Isso é feito ao calcular um hash de

cada quadro de vídeo, incluindo os metadados e assinando o hash. A assinatura então é armazenada no stream, em campos de metadados dedicados (o cabeçalho SEI).

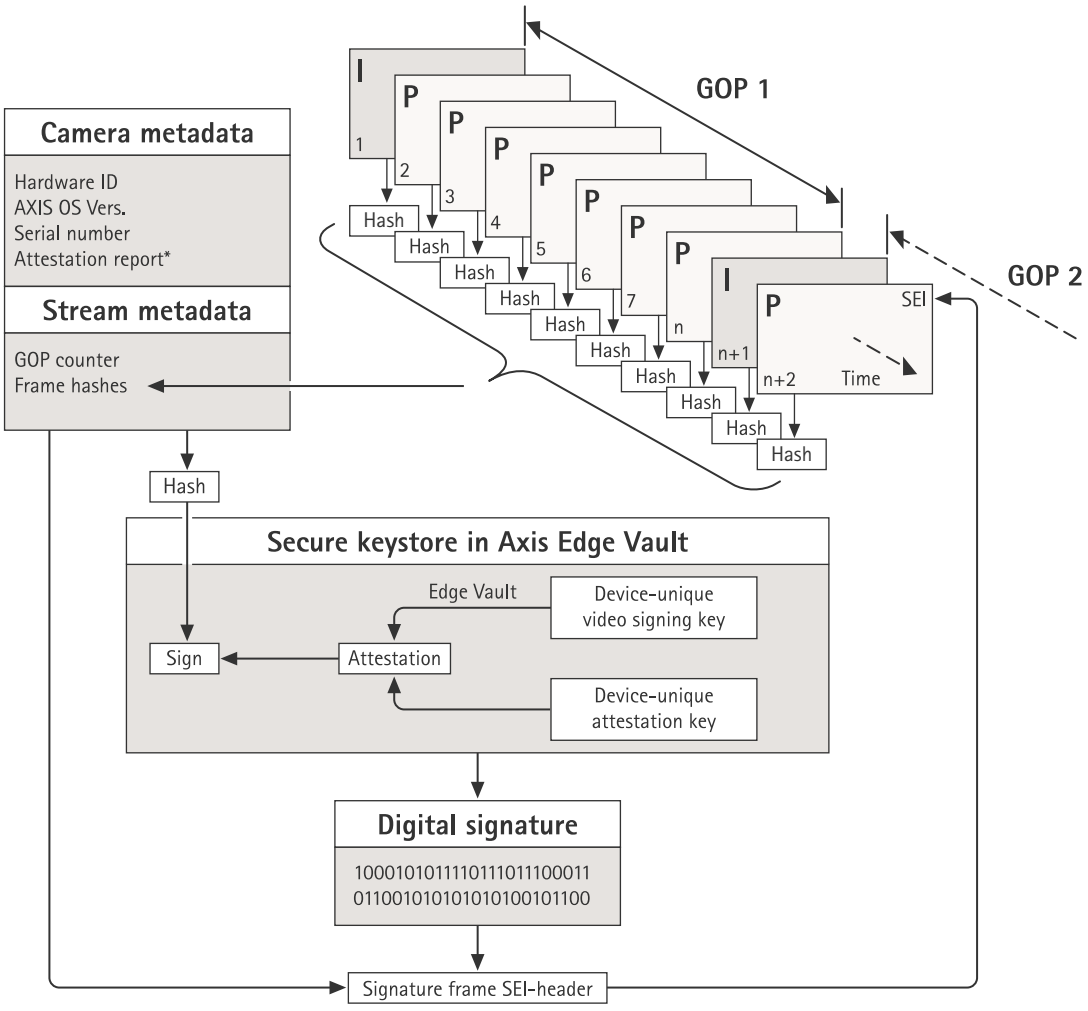


Figure 12. Uma representação gráfica de como uma assinatura é adicionada aos metadados do vídeo. O conteúdo de cada frame de um grupo de imagens (GOP) é concatenado como hash junto com um hash dos metadados da câmera e dos metadados do stream. Isso forma o hash do GOP, que é assinado no Edge Vault. A 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 verdadeira é feita usando uma chave de assinatura de vídeo exclusiva do dispositivo, que é atestada usando uma chave de certificação exclusiva do dispositivo. O relatório de certificação é anexado ao stream no início e, depois, em intervalos periódicos, geralmente 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 do grupo de imagens (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. O improvável evento de perda de frames durante o streaming ou os danos ao conteúdo durante o armazenamento serão sinalizados da mesma forma.

5 Proteção da cadeia de fornecimento

O Axis Edge Vault requer uma base segura que atue como a raiz da confiança. O estabelecimento da raiz de confiança começa no processo de inicialização do dispositivo. Nos dispositivos Axis, o mecanismo *inicialização segura*, baseado em hardware, verifica o sistema operacional (AXIS OS) a partir do qual o dispositivo está inicializando. O AXIS OS, por sua vez, é assinado criptograficamente (*firmware assinado*) durante o processo de compilação.

A inicialização segura e o firmware assinado se conectam. Eles verificam se o firmware não foi violado (por qualquer pessoa com acesso físico ao dispositivo) antes de o dispositivo ser implantado e, após a implantação, asseguram que o dispositivo não instale atualizações comprometidas de firmware. Juntos, a inicialização segura e o firmware assinado criam uma cadeia ininterrupta de software criptograficamente validado para a cadeia de confiança da qual dependem todas as operações seguras.

5.1 Inicialização segura

O mecanismo de 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). A inicialização segura garante que um dispositivo possa inicializar apenas 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 se 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.

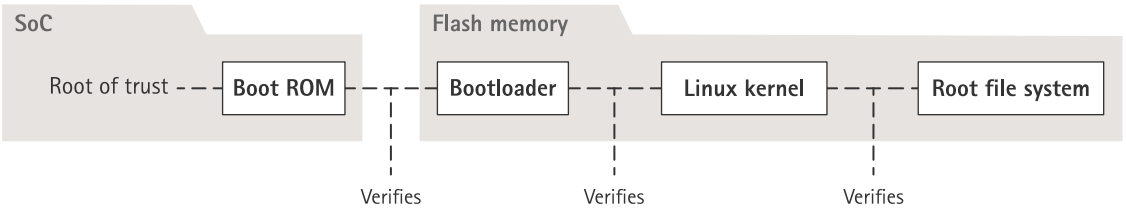


Figure 13. No processo de inicialização segura, cada parte da cadeia autentica a próxima. Em última análise, isso resulta em um sistema de arquivos raiz verificado.

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 o estado correto do dispositivo, mesmo após um padrão de fábrica. Mas, para que a inicialização segura funcione, ela deve garantir que a inicialização verifique se o firmware está assinado pela Axis.

5.2 Firmware assinado

O firmware assinado pela Axis envolve a assinatura da imagem do firmware pela Axis com uma chave privada que é mantida em segredo. Se o firmware tiver uma assinatura conectada a ele, um dispositivo validará 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.

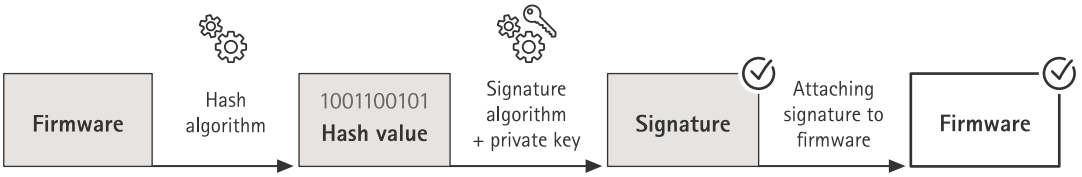


Figure 14. O processo de assinatura do firmware.

Antes de uma atualização de firmware, a autenticidade do novo firmware deve ser verificada. Para garantir isso, 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. O processo de inicialização dos dispositivos Axis será abortado caso a assinatura do firmware fosse inválida ou a imagem do firmware fosse violada.

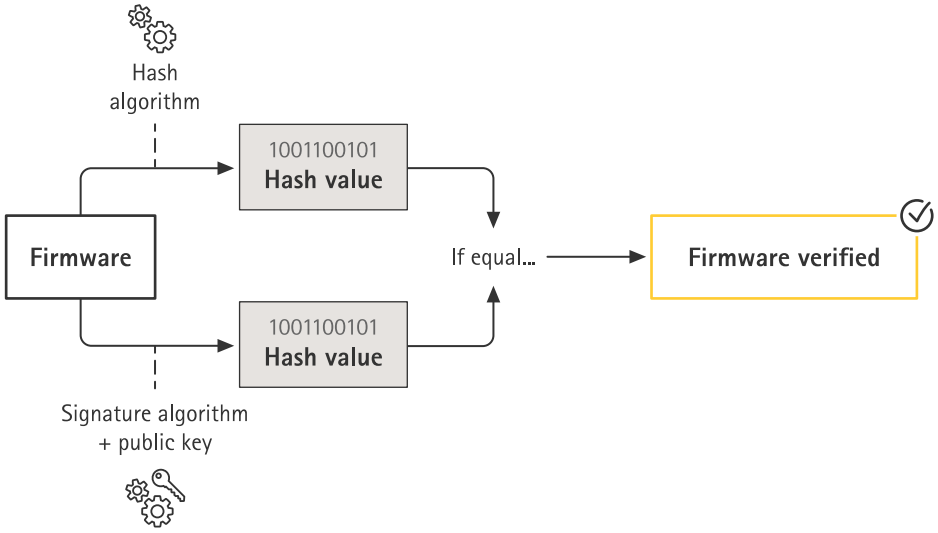


Figure 15. O processo de verificação do firmware assinado.

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. A assinatura primária verifica várias assinaturas secundárias durante a descompactação da imagem.

Para compilações de firmware personalizadas e de teste, a Axis implementou um mecanismo que aprova dispositivos individuais para aceitar firmware de não 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 nos dispositivos aprovados, o certificado permite o uso de um firmware personalizado que pode ser executado apenas no dispositivos aprovados, com base no 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 Glossário

ID do dispositivo Axis: certificado exclusivo do dispositivo com chaves correspondentes que podem comprovar a autenticidade de um dispositivo Axis. O dispositivo Axis é fornecido de fábrica com uma ID de dispositivo Axis guardada no armazenamento seguro de chaves. A ID do dispositivo Axis é baseada no padrão internacional IEEE 802.1AR (IDevID, identificador inicial do dispositivo), que define um método para identificação automatizada e segura.

Axis Edge Vault: plataforma de segurança cibernética baseada em hardware que protege o dispositivo Axis. Ele se baseia em uma base sólida de módulos de computação criptográfica (elemento seguro e TPM) e segurança SoC (TEE e inicialização segura), combinada com a experiência em segurança de dispositivos de borda.

Certificado: documento assinado que atesta a origem e as propriedades de um par de chaves pública/privada. 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: raiz de confiança para uma cadeia de certificados. Ele é usado para comprovar a autenticidade e a veracidade de certificados subjacentes.

Critérios comuns (CC): padrão internacional para certificação de segurança de produtos de TI. Também referenciado como Critérios Comuns para Avaliação de Segurança de Tecnologia da Informação, ISO/IEC 15408.

FIPS 140: série de padrões de segurança de computadores dos EUA usados para aprovar módulos de computação criptográfica. O FIPS (Padrão Federal de Processamento de Informações) 140 define os requisitos sobre como um módulo criptográfico deve ser projetado e implementado para mitigar os riscos de violação do módulo.

ROM imutável (memória de somente leitura): memória de somente leitura que armazena com segurança as chaves públicas confiáveis e o programa usado para comparar assinaturas para que não possam ser sobrescritas.

Provisionamento: 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: 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.

Inicialização segura: recurso para impedir o carregamento de software não autorizado durante a inicialização do dispositivo. A inicialização segura usa firmware assinado que garante que apenas o software Axis autorizado seja usado para inicializar o dispositivo.

Elemento seguro: módulo de computação criptográfica que fornece armazenamento de chaves privadas baseado em hardware e protegido contra violação e execução segura de operações criptográficas. Ao contrário do TPM, as interfaces de hardware e software de um elemento seguro não são padronizadas, mas específicas do fabricante.

Armazenamento seguro de chaves: ambiente protegido contra violações para proteção de chaves privadas e execução segura de operações criptográficas. Ele evita acesso não autorizado e extração maliciosa em caso de violação de segurança. Dependendo dos requisitos de segurança, um dispositivo Axis pode ter um ou vários módulos de computação criptográfica baseados em hardware que fornecem um armazenamento seguro de chaves, protegido por hardware.

Firmware assinado: firmware que foi assinado digitalmente por uma parte confiável. O dispositivo Axis verifica a autenticidade da imagem do firmware antes de executar uma atualização de firmware. O firmware assinado é um requisito no processo de inicialização segura.

Vídeo assinado: recurso que mantém e fortalece a confiança no vídeo como prova. O vídeo assinado fornece detecção e autenticidade de violações de vídeo e é usado para garantir que o vídeo esteja intacto e possa ser rastreado de volta até uma câmera Axis específica. As chaves de assinatura para vídeo assinado ficam dentro do armazenamento seguro de chaves do dispositivo Axis.

Segurança da Camada de Transporte (TLS): padrão da Internet, usado para proteger o tráfego em rede. O TLS fornece o S (de segurança) em HTTPS.

Ambiente de Execução Confiável (TEE): fornece armazenamento de chaves privadas baseado em hardware e protegido contra violações, e execução segura de operações criptográficas. Ao contrário do elemento seguro e do TPM, o TEE é uma área isolada de hardware segura do processador principal do sistema em chip (SoC).

Módulo de Plataforma Confiável (TPM): módulo de computação criptográfica que fornece armazenamento de chaves privadas baseado em hardware e protegido contra violação, e execução segura de operações criptográficas. Os TPMs são componentes de computador padronizados internacionalmente (TPM 1.2, TPM 2.0), definidos pelo *Grupo de Computação Confiável (TCG)*.

Segurança zero-trust: abordagem moderna para segurança de TI em que dispositivos conectados e infraestrutura de TI (como redes, computadores, servidores, serviços em nuvem e aplicativos) precisam identificar, validar e autenticar uns aos outros para obter controles de alta segurança.

Sobre a Axis Communications

A Axis torna possível um mundo mais inteligente e seguro criando soluções para melhorar a segurança e o desempenho dos negócios. Como empresa de tecnologia de rede e líder do setor, a Axis oferece soluções em vigilância por vídeo, controle de acesso, intercomunicação e áudio. Nossas soluções são aprimoradas por aplicativos de análise inteligentes e apoiados por treinamento de alta qualidade.

A Axis tem cerca de 4.000 funcionários dedicados em mais de 50 países e colabora com parceiros de tecnologia e integração de sistemas em todo o mundo para fornecer soluções aos clientes. A Axis foi fundada em 1984 e tem sede em Lund, Suécia