LIVRE BLANC

Axis Edge Vault

La plateforme de cybersécurité matérielle qui protège les périphériques Axis en offrant :

— protection de la chaîne d'approvisionnement

— identité du périphérique de confiance

— stockage sécurisé des clés

— détection de sabotage des vidéos

Avril 2024

Avant-propos

Axis Edge Vault fournit une plateforme de cybersécurité matérielle qui protège les périphériques Axis. Elle repose sur des bases solides constituées de modules de calcul cryptographique (élément sécurisé et TPM) et d'une sécurité SoC (TEE et démarrage sécurisé), associés au savoir-faire en matière de sécurité des dispositifs périphériques. Une racine de confiance solide est le point d'ancrage d'Axis Edge Vault. Celle-ci est possible grâce au *démarrage sécurisé* et au *système d'exploitation signé*. Ces fonctions permettent une chaîne ininterrompue de logiciels validés de manière cryptographique pour la chaîne de confiance qui sécurise toutes les opérations qui dépendent d'elle.

Les périphériques Axis avec Edge Vault minimisent l'exposition des clients aux risques de cybersécurité en empêchant les écoutes électroniques et l'extraction malveillante des informations sensibles. Axis Edge Vault permet également au périphérique Axis d'être une unité fiable et de confiance au sein du réseau du client.

Plateforme de cybersécurité Axis Edge Vault

Modules de calcul cryptographique	Points forts	Scénarios d'utilisation
• Élément de sécurité • TPM 2.0 • Sécurité du SoC (environnement TEE)	• Démarrage sécurisé • Système d'exploitation signé • Identifiant du périphérique Axis • Fichier de clés sécurisé • Vidéo signée • Système de fichiers crypté	• — Protection de la chaîne d'approvisionnement • — Identité du périphérique de confiance • Stockage sécurisé des clés • Détection des modifications à la vidéo

- **Protection de la chaîne d'approvisionnement** : Axis Edge Vault nécessite une base solide servant de racine de confiance. Sans l'aide du démarrage sécurisé et du système d'exploitation signé, la racine de confiance de la chaîne ne peut pas être établie. Le démarrage sécurisé, associé au système d'exploitation signé, fournit une chaîne ininterrompue de logiciels validés de manière cryptographique, à partir de la mémoire inaltérable (ROM d'amorçage). Le démarrage sécurisé garantit qu'un périphérique ne peut être démarré qu'avec un système d'exploitation signé, ce qui empêche le sabotage de la chaîne d'approvisionnement physique. Avec le système d'exploitation signé, le périphérique est aussi capable de valider un nouveau logiciel de dispositif avant d'accepter son installation. Si le périphérique détecte que l'intégrité est compromise ou que le logiciel du périphérique n'est pas signé par Axis, la mise à niveau sera rejetée. Ceci protège les périphériques du sabotage du logiciel.
- **Identité du périphérique de confiance** : Être capable de vérifier l'origine du périphérique est essentiel pour instaurer la confiance dans l'identité du périphérique. Pendant la production, avec Axis Edge Vault, un certificat d'identifiant de périphérique Axis unique, provisionné en usine et conforme IEEE 802.1AR est assigné à chaque périphérique. Ceci fonctionne comme un passeport pour prouver l'origine du périphérique. L'identifiant de périphérique est stocké de façon permanente dans un fichier de clés sécurisé sous la forme d'un certificat signé par le certificat racine Axis. L'identifiant de périphérique peut être exploité par l'infrastructure IT du client pour l'intégration sécurisée et automatisée du périphérique et son identification sécurisée.

- **Stockage sécurisé des clés** : Le fichier de clés sécurisé fournit un stockage matériel des informations cryptographiques protégé contre le sabotage. Le fichier de clés sécurisé protège l'identifiant de périphérique Axis ainsi que les informations cryptographiques chargées par le client et empêche l'accès non-autorisé et l'extraction malveillante en cas de faille de sécurité.
- **Détection de sabotage des vidéos** : La signature vidéo garantit que les preuves vidéo peuvent être confirmées intactes sans avoir à démontrer la chaîne de possession du fichier vidéo. Chaque caméra utilise sa clé de signature de vidéo unique, qui est stockée dans un fichier de clés sécurisé, pour ajouter une signature dans le flux vidéo. Lors de la lecture de la vidéo, le *lecteur de fichiers* d'Axis indique si la vidéo est intacte. La signature vidéo permet de remonter la vidéo jusqu'à l'origine de la caméra et de vérifier qu'elle n'a pas été modifiée après avoir quitté la caméra.

Table des matières

1 Introduction

Axis suit les meilleures pratiques du secteur en mettant en œuvre des mesures sécurité dans nos produits. Ceci dans le but de réduire l'exposition des clients aux risques de cybersécurité et de faire du périphérique Axis une unité de confiance sur le réseau du client.

Axis Edge Vault fournit une plateforme de cybersécurité matérielle qui protège les périphériques Axis. Elle repose sur des bases solides constituées de modules de calcul cryptographique (élément sécurisé et TPM) et d'une sécurité SoC (TEE et démarrage sécurisé), associés au savoir-faire en matière de sécurité des dispositifs périphériques.

Ce livre blanc définit l'approche multidimensionnelle des dispositifs périphériques.Axis et présente les risques courants ainsi que la manière de les éviter. Axis Edge Vault nécessite une base solide servant de racine de confiance. Par conséquent, nous aborderons également les aspects de sécurité de la chaîne d'approvisionnement des périphériques Axis et étudierons pourquoi le système d'exploitation signé et le démarrage sécurisé sont des mesures fondamentales pour contrer le sabotage du logiciel et de la chaîne d'approvisionnement physique.

Sur *https://www.axis.com/support/cybersecurity/resources*, vous pouvez trouver davantage d'informations concernant la sécurité des produits, les vulnérabilités découvertes et les mesures que vous pouvez prendre pour réduire les risques des menaces courantes.

Le dernier chapitre de ce livre blanc comprend un glossaire.

2 — Protection de la chaîne d'approvisionnement

Axis Edge Vault nécessite une base solide servant de racine de confiance. L'établissement de la racine de confiance débute lors du processus de démarrage du périphérique. Dans les périphériques Axis, le mécanisme matériel de *démarrage sécurisé* vérifie de quel système d'exploitation (AXIS OS) le périphérique démarre. Le système d'exploitation AXIS, en retour, est signé de façon cryptographique (en utilisant le *système d'exploitation signé*) pendant le processus de génération.

Le démarrage sécurisé et le système d'exploitation signé sont liés l'un à l'autre. Ils assurent que le système d'exploitation ou le logiciel du périphérique n'est pas modifié (par quiconque pouvant accéder physiquement au périphérique) avant que le périphérique ne soit déployé et que, après déploiement, le périphérique ne peut pas installer de mises à jour de logiciel compromis ou non signé par code. Le démarrage sécurisé et le système d'exploitation signé créent une chaîne ininterrompue de logiciels validés de manière cryptographique pour la chaîne de confiance qui sécurise toutes les opérations qui dépendent d'elle.

2.1 Démarrage sécurisé

Le mécanisme de démarrage sécurisé est un processus de démarrage constitué d'une chaîne ininterrompue de logiciels validés par cryptographie, commençant dans la mémoire immuable (ROM de démarrage). Le démarrage sécurisé permet de s'assurer qu'un appareil ne peut démarrer qu'avec un système d'exploitation autorisé.

Le processus d'amorçage est lancé par la ROM d'amorçage qui valide le programme d'amorçage. Le démarrage sécurisé vérifie ensuite, en temps réel, les signatures intégrées de chaque composant logiciel chargé depuis la mémoire flash. La ROM de démarrage sert de racine de confiance et le processus de

démarrage ne continue que si chaque signature est vérifiée. Chaque partie de la chaîne authentifie la partie suivante, aboutissant ainsi à un noyau Linux vérifié et à un système de fichiers racine vérifié.

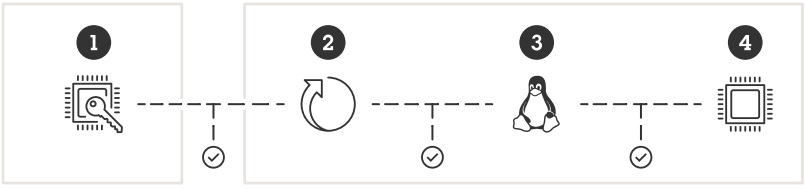

Figure 1. Dans le processus de démarrage sécurisé, chaque parie de la chaîne authentifie la suivante. Il en résulte un système de fichiers racine vérifié.

1 *ROM d'amorçage (racine de confiance) sur le SoC*
2 *Programme d'amorçage*
3 *Noyau Linux*
4 *Système de fichiers racine*

Dans de nombreux dispositifs, il est essentiel que les fonctionnalités de bas niveau soient impossibles à modifier. Si d'autres mécanismes de sécurité sont créés par-dessus le logiciel de bas niveau, l'amorçage sécurisé sert de couche de base sécurisée qui protège ces mécanismes des détournements. Dans le cas d'un périphérique doté d'un système de démarrage sécurisé, le système d'exploitation installé dans la mémoire flash est protégé contre toute modification, tandis que la configuration n'est pas protégée. Le démarrage sécurisé garantit le bon fonctionnement du périphérique, même après une remise en paramètres d'usine. Mais pour que le démarrage sécurisé fonctionne, il doit s'assurer que le démarrage vérifie la signature du système d'exploitation par Axis.

2.2 Système d'exploitation signé

Le système d'exploitation signé Axis implique la signature par code Axis de l'image logicielle du périphérique avec une clé privée gardée secrète. Au démarrage du périphérique, le démarrage sécurisé d'un périphérique Axis vérifie que le logiciel du périphérique est signé. Si le périphérique détecte que l'intégrité de son logiciel est compromise, il ne fonctionnera pas. Lors de la mise à niveau du logiciel du périphérique, le système d'exploitation AXIS existant et signé vérifie automatiquement que le nouveau système d'exploitation AXIS est également signé. Si ce n'est pas le cas, la mise à niveau sera rejetée.

Le processus de système d'exploitation signé par code est lancé par le calcul d'une valeur de hachage cryptographique. La valeur est ensuite signée avec la clé privée d'une paire de clés privée/publique avant que la signature soit associée à l'image du système d'exploitation AXIS.

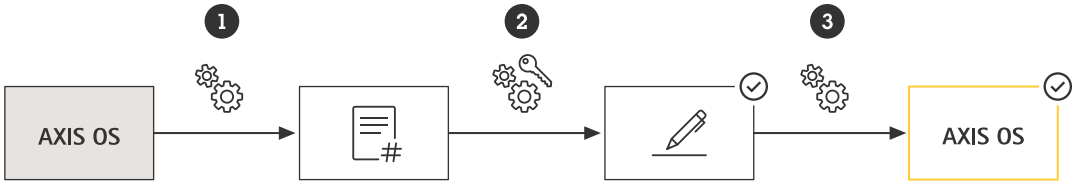

Figure 2. Le processus de signature par code du système d'exploitation.

1 *Une valeur de hachage cryptographique pour AXIS OS est créée.*
2 *La signature est créée en combinant le hachage et la clé privée.*
3 *La signature est ajoutée à la version et au binaire du système d'exploitation AXIS.*

Avant une mise à niveau, l'authenticité de la nouvelle mise à jour du logiciel doit être vérifiée. Pour s'en assurer, la clé publique (fournie avec le produit Axis) est utilisée pour confirmer que la valeur de hachage a bien été signée avec la clé privée correspondante. En calculant également la valeur de hachage et en la comparant à cette valeur de hachage validée provenant de la signature, l'intégrité peut être vérifiée. La procédure de démarrage des périphériques Axis sera annulée si la signature est invalide ou si l'image du système d'exploitation AXIS a été modifiée.

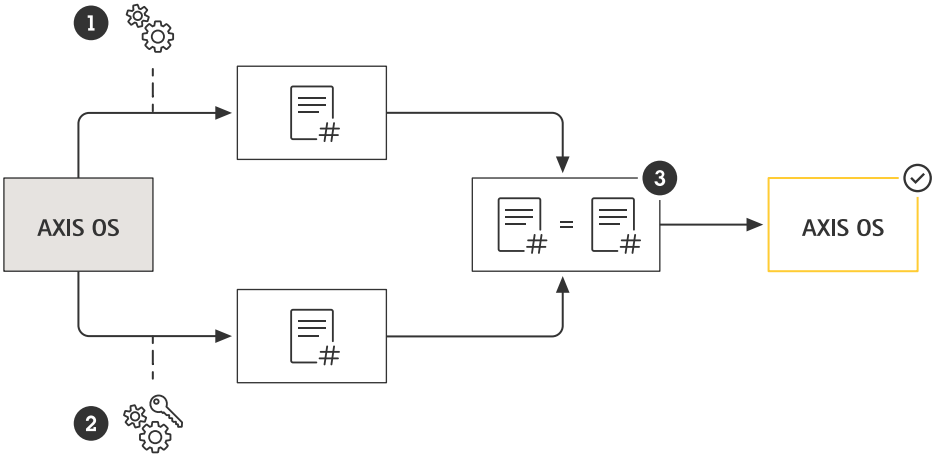

Figure 3. Processus de vérification du système d'exploitation signé.

1 *Calcul de la valeur de hachage d'AXIS OS*
2 *Utilisation de la clé publique pour confirmer la valeur de hachage à partir de la signature*
3 *Si et seulement si les résultats correspondent, la signature est confirmée correcte.*

Le système d'exploitation signé Axis est basé sur la méthode de cryptage RSA à clé publique reconnue par le secteur. La clé privée est stockée dans un lieu bien gardé par Axis, tandis que la clé publique est intégrée aux dispositifs Axis. L'intégrité de l'image logicielle complète est assurée par une signature. Une signature principale permet de vérifier plusieurs signatures secondaires, qui sont vérifiées lorsque l'image est décompressée.

Pour des tests ou des configurations personnalisées, Axis a mis en œuvre un mécanisme qui approuve des périphériques individuels pour accepter les images hors production. Cette image est signée par code à l'aide d'une clé dédiée à cet effet, avec l'approbation du propriétaire et d'Axis, et donne lieu à une signature personnalisée. Lorsqu'il est installé dans le périphérique approuvé, le certificat permet l'utilisation d'une image personnalisée exécutable uniquement sur ce périphérique, déterminé par son numéro de série unique et son ID processeur. Seul Axis peut créer des certificats personnalisés, car Axis possède la clé pour les signer.

3 — Identité du périphérique de confiance

Dans les réseaux de sécurité à confiance zéro modernes (« Ne faites jamais confiance, vérifiez toujours »), la capacité de vérifier l'origine du périphérique, son authenticité et ses connexions est un besoin fondamental. Un périphérique réseau peut vérifier son intégrité et son authenticité d'une manière similaire à celle qui consiste à présenter son passeport aux autorités de l'aéroport pour vérification d'identité.

3.1 Identification sécurisée de périphérique avec l'identifiant de périphérique Axis

La norme internationale *IEEE 802.1AR* définit une méthode d'automatisation et de sécurisation de l'identification d'un périphérique sur un réseau. Si la communication est transmise à un module de calcul cryptographique intégré, le périphérique peut renvoyer une réponse d'identification de confiance conformément à la norme. Cette réponse de confiance peut être utilisée par l'infrastructure réseau pour permettre l'intégration automatisée et sécurisée du périphérique au réseau provisionnel pour la configuration initiale du périphérique et la mise à jour du logiciel.

Pour nous conformer à la norme IEEE 802.1AR, nous provisionnons en usine un certificat d'identifiant de périphérique Axis unique dans la plupart des périphériques que nous fabriquons (Identifiant de périphérique initial IEEE 802.1AR, IDevID). L'identifiant de périphérique Axis est stocké dans un fichier de clés sécurisé et protégé contre le sabotage, fourni par un module de calcul cryptographique intégré au périphérique. Cet identifiant est unique pour chaque périphérique Axis. Il est conçu pour prouver l'origine du périphérique.

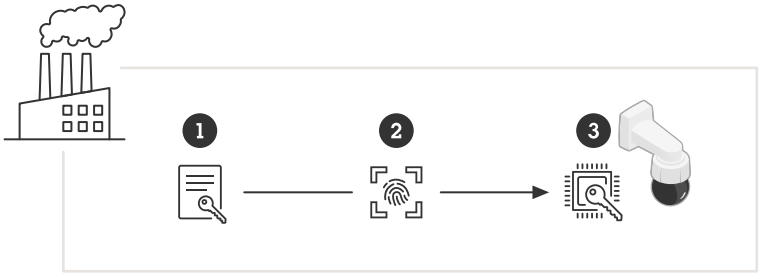

Figure 4. Lors du processus de fabrication du dispositif Axis, son ID unique (2) est stocké dans le fichier de clés sécurisé du dispositif (3).

1 *Infrastructure de clés d'ID de dispositif Axis (PKI)*
2 *Identifiant du périphérique Axis*
3 *L'ID de dispositif Axis est stocké dans un fichier de clés sécurisé et protégé contre le sabotage, fourni par un module de calcul cryptographique intégré au dispositif Axis.*

La norme IEEE 802.1AR se fonde sur la norme IEEE 802.1X pour le contrôle d'accès au réseau, qui est activé par défaut dans les périphériques Axis avec l'identifiant de périphérique Axis pré-sélectionné. Ceci permet l'identification et l'authentification sécurisées du périphérique Axis grâce à une infrastructure IT compatible 802.1X, même avec les paramètres d'usine par défaut.

Le certificat d'identifiant de périphérique Axis se présente sous différentes configurations cryptographiques (clé RSA 2048 bits, clé RSA 4096 bits, ECC-P256). Elles sont activées par défaut pour permettre de sécuriser les connexions et l'identification du périphérique via le contrôle d'accès au réseau IEEE 802.1X ainsi que le protocole HTTPS.

Axis gère sa propre infrastructure à clés publiques (PKI) IEEE 802.1AR dédiée pour le provisionnement en usine de l'identifiant de périphérique Axis pendant le processus de fabrication. L'identifiant de périphérique Axis est signé par le certificat intermédiaire qui est signé en retour par le certificat racine Axis. La CA racine et la CA intermédiaire sont stockés de façon sécurisée dans des modules de calcul cryptographiques géographiquement distincts. Ceci empêche l'extraction malveillante en cas de faille de sécurité sur les

sites de production Axis. Vous pouvez trouvez davantage d'informations concernant l'infrastructure PKI Axis sur *www.axis.com/support/public-key-infrastructure-repository*

Figure 5. Infrastructure à clés publiques (PKI) IEEE 802.1AR Axis pour le provisionnement en usine de l'identifiant de périphérique Axis pendant le processus de fabrication. L'ID de dispositif Axis (1), qui est un certificat intégrant le numéro de série du produit, est signé par une CA intermédiaire d'ID de dispositif Axis (2), elle-même signée par la CA racine de l'ID de dispositif Axis (3). Des modules matériels de sécurité (HSM) spécialisés sont utilisés pour le provisionnement sécurisé en usine.

A Référence
B Signature

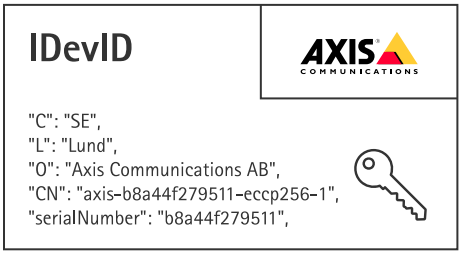

Figure 6. Exemple d'identifiant de périphérique Axis.

3.2 Intégration sécurisée au réseau

Lorsque vous achetez un périphérique Axis, vous pouvez réaliser un examen manuel avant de commencer à l'utiliser. En inspectant visuellement le périphérique et à partir de connaissances antérieures concernant l'aspect des produits Axis, vous pouvez vous assurer que le périphérique a été fabriqué par Axis. Cependant, vous pouvez faire ce type d'inspections uniquement si vous disposer d'un accès physique au périphérique. Par conséquent, lorsque vous communiquez avec un périphérique sur un réseau, comment s'assurer de communiquer avec le bon périphérique et comment vérifier son identité ? Aucun équipement réseau ou logiciel sur serveur ne peut effectuer une inspection physique. Par mesure de sécurité, interagir d'abord avec un nouveau périphérique sur un réseau fermé, où il peut être provisionné de manière sécurisée, est une pratique courante.

L'identifiant de périphérique Axis fournit à votre réseau des preuves vérifiables par cryptographie qu'un périphérique donné a été produit par Axis et que la connexion réseau au périphérique est effectivement assurée par ce périphérique. L'identifiant de périphérique Axis peut être utilisé pendant le processus d'authentification de réseau IEEE 802.1X pour accéder à un réseau de provisionnement où d'autres mises à jour du logiciel et configurations du périphérique Axis sont réalisées avant que le périphérique Axis ne soit intégré au réseau de production.

Avec l'identifiant de périphérique Axis, la sécurité générale peut être renforcée et le temps de déploiement des périphériques peut être réduit, étant donné que des mesures automatisées et moins coûteuses peuvent être prises pour l'installation et la configuration du périphérique.

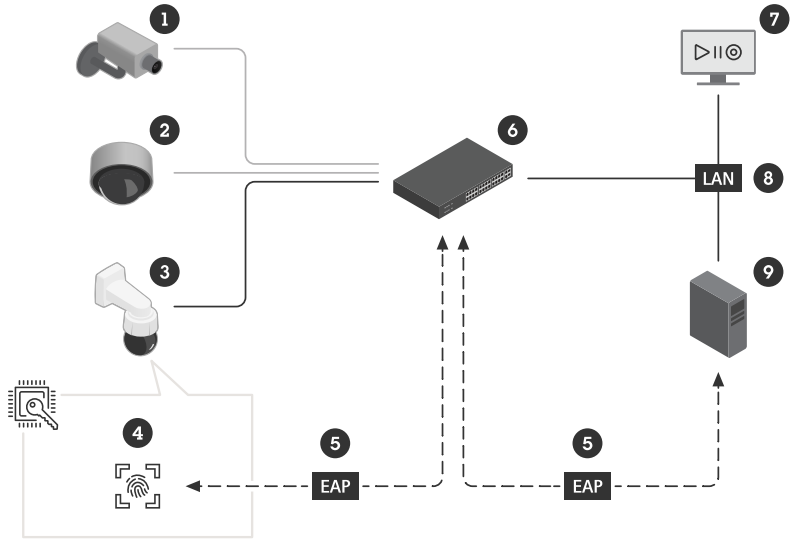

Figure 7. Intégration sécurisée au réseau. Vous pouvez ordonner à votre serveur d'authentification (9) d'accepter automatiquement les dispositifs Axis (3) sur le réseau (8) et dans le système VMS (7). Cela est possible en utilisant les numéros de série des dispositifs et l'identifiant de périphérique Axis (4) comme une empreinte digitale ou une authentification.

1 *Dispositif non autorisé (à intégrer manuellement)*
2 *Dispositif d'un autre fabricant*
3 *Dispositif Axis*
4 *ID de dispositif Axis, stocké en toute sécurité dans le fichier de clés sécurisé et protégé contre le sabotage*
5 *Authentification réseau 802.1X EAP-TLS du dispositif Axis via le certificat d'ID de dispositif Axis*
6 *Switch manageable (authentifiant)*
7 *VMS (vérification des dispositifs)*
8 *LAN protégé par 802.1X*
9 *RADIUS (serveur d'authentification réseau)*

Figure 8. Description plus détaillée du processus d'inscription. La norme IEEE 802.1AR d'identification sécurisée des dispositifs définit une méthode d'identification d'un dispositif (1) via des requêtes IEEE 802.1X EAP (EAP-TLS) à l'aide d'un serveur RADIUS (3) pour autoriser le dispositif à accéder au réseau.

1 *Dispositif Axis*
2 *Switch manageable (authentifiant)*
3 *Serveur RADIUS (serveur d'authentification réseau)*

A Nouvelle connexion
B EAP-demande d'identité
C EAP-réponse d'identité, notamment identité de périphérique Axis-certificat, IEEE 802.1AR IDevID
D Accès RADIUS-demande
- Accès RADIUS-challenge
F EAP-réussite

En plus d'offrir une source de confiance complémentaire et intégrée, l'identifiant de périphérique Axis permet également d'assurer le suivi des périphériques et de réaliser des vérifications et authentifications régulières selon les principes de réseau à confiance zéro.

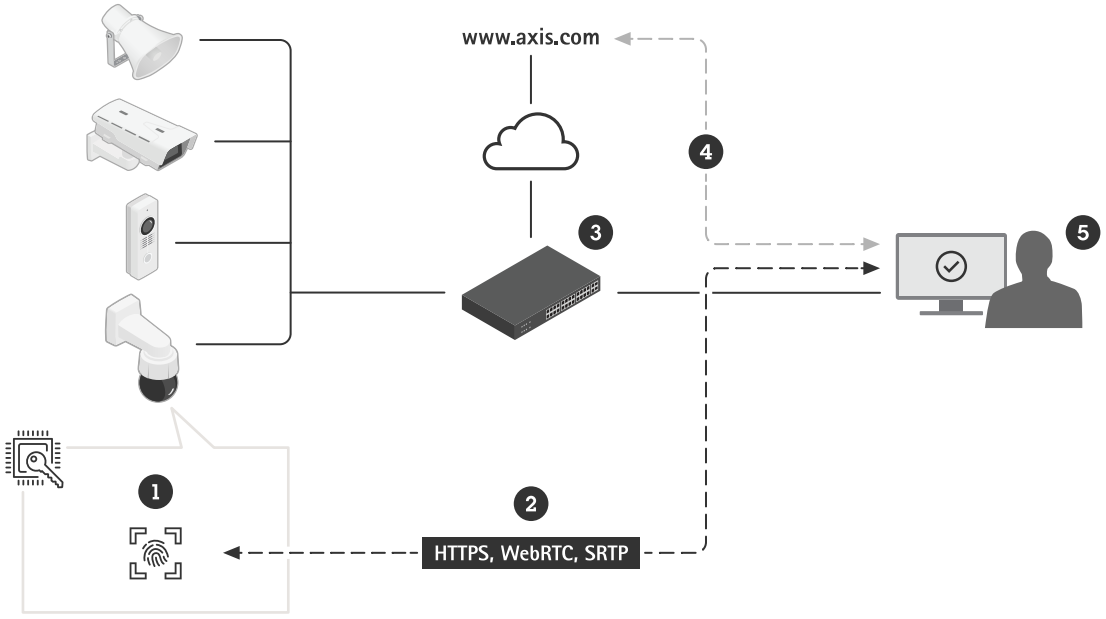

Figure 9. Après l'inscription sécurisée d'un dispositif, les applications logicielles (5) d'autres parties du système peuvent utiliser l'ID de dispositif Axis (1) et des opérations cryptographiques pour vérifier et authentifier le dispositif dans divers protocoles de communication de type TLS (2). L'identifiant de périphérique Axis est vérifiable grâce au certificat de l'autorité de certification racine de l'identifiant de périphérique Axis disponible publiquement (4).

1 *ID de dispositif Axis stocké en toute sécurité dans le fichier de clés sécurisé et protégé contre le sabotage*
2 *Communication basée sur TLS (HTTPS, WebRTC, SRTP)*
3 *Switch manageable*
4 *Certificat de l'autorité de certification racine de l'identifiant de périphérique Axis (téléchargeable à l'adresse suivante www.axis.com/support/public-key-infrastructure-repository*
5 *VMS ou autre logiciel (vérification de dispositif)*

4 Stockage sécurisé des clés

Traditionnellement, les informations cryptographiques X.509 sensibles (clés privées) sont stockées dans un système de fichiers du périphérique. Il est uniquement protégé par la politique d'accès au compte utilisateur, qui fournit une protection de base parce que le compte utilisateur n'est pas compromis

facilement. Cependant, en cas de faille de sécurité, ces informations cryptographiques ne seront pas protégées et seront accessibles à la concurrence.

Du point de vue de la sécurité, le fichier de clés sécurisé est crucial pour le stockage et la protection des informations cryptographiques. Les informations cryptographiques sensibles, y compris dans l'identifiant de périphérique Axis et dans la vidéo signée, ne sont pas seulement stockées dans un fichier de clés sécurisé mais les informations chargées par le client peuvent également être protégées de la même manière.

4.1 Fichier de clés sécurisé

Les informations cryptographiques sensibles (clés privées) sont stockées dans un fichier de clés matériel sécurisé et protégé contre le sabotage. Ceci empêche toute extraction malveillante même en cas de faille de sécurité. Par ailleurs, les clés privées restent protégées dans le fichier de clés sécurisé même lorsqu'elles sont utilisées. Un concurrent potentiel n'aura pas accès au fichier de clés sécurisé et ne pourra pas vous espionner sur le trafic réseau, obtenir l'accès via des clés IEEE 802.1X ou extraire d'autres clés privées.

Le fichier de clés sécurisé est fourni via un module de calcul cryptographique matériel. Selon les exigences de sécurité en vigueur, un périphérique Axis peut être doté soit d'un ou de plusieurs modules de ce type, tels qu'un module Trusted Platform Module (TPM 2.0), soit d'un élément sécurisé, et/ou d'un environnement TEE de confiance.

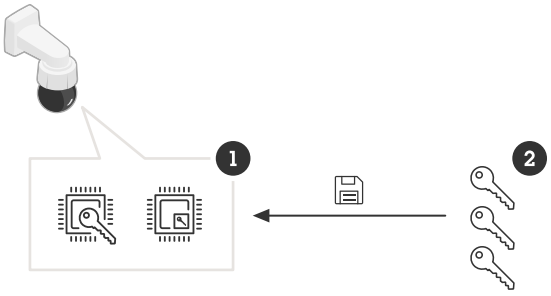

Figure 10. Les fichiers de clés sécurisés (1) protègent les clés privées (2) et assurent l'exécution sécurisée des opérations cryptographiques.

1 *Fichiers de clés sécurisés, qui peuvent être un élément sécurisé, un module TPM ou un environnement TEE (sur le SoC)*
2 *Clés privées, par exemple ID de dispositif Axis, clé de signature vidéo, clés de contrôle d'accès, clés du système de fichiers et clés chargées par le client (par ex. IEEE 802.1X et HTTPS)*

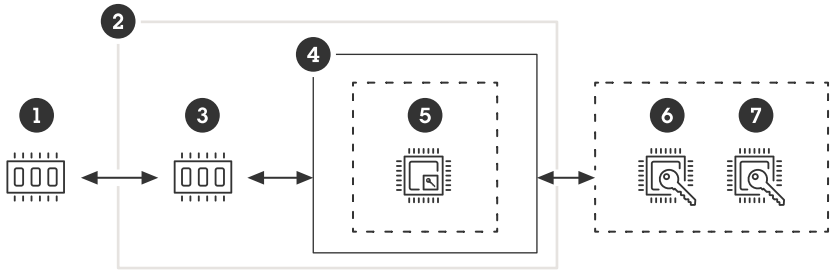

Figure 11. Les périphériques équipés d'Axis Edge Vault contiennent des modules informatiques cryptographiques matériels (élément sécurisé (6) et TPM (7)) qui sont montés sur le circuit imprimé juste à

côté du processeur principal du SoC (4). Le TEE (5) est une zone sécurisée du processeur principal du SoC. La ROM d'amorçage intégrée au SoC (3) est chargée d'exécuter les procédures de démarrage sécurisé et de veiller à ce que seules les images logicielles du système d'exploitation signé provenant de la mémoire flash (1) soient utilisées pour amorcer le périphérique.

1. *Mémoire flash (pour le système d'exploitation signé, système de fichiers en lecture-écriture)*
2. *SoC*
3. *ROM d'amorçage (pour le démarrage sécurisé)*
4. *Processeur*
5. *TEE (pour le fichier de clés sécurisé)*
6. *Élément sécurisé (pour le fichier de clés sécurisé)*
7. *TPM (pour le fichier de clés sécurisé)*

Le TPM, l'élément sécurisé et le TEE permettent tous de protéger les clés privées et de sécuriser l'exécution des opérations cryptographiques. En cas de faille de sécurité, l'accès non-autorisé et l'extraction malveillante sont impossibles.

4.2 Critères communs et FIPS 140

Les modules de calcul cryptographique peuvent être certifiés à l'aide des Niveaux d'évaluation selon les critères communs (CC EAL) ainsi que des niveaux de conformité à les normes FIPS 140 (1-4). Ces certifications sont utilisées pour déterminer l'exactitude et l'intégrité des opérations cryptographiques et pour vérifier diverses contre-mesures au sabotage, telles que l'auto-vérification, la résistance au sabotage et d'autres mesures de résistance. Vous pouvez consulter des informations concernant la certification sur la fiche technique d'un périphérique Axis ou dans le *sélecteur de produits Axis*. Axis impose à ses modules de calcul cryptographique matériels intégrés d'être au moins certifiés conformément aux Critères communs EAL4 et/ou aux normes 140-2/3 niveau 2/3.

4.2.1 Critères communs

Les Critères communs (CC) (également dénommés Critères communs d'évaluation de la sécurité des technologies de l'information) sont une norme internationale (ISO/IEC 15408) pour la certification de sécurité des produits IT. Les Critères communs fournissent un cadre aux fabricants et exécutants pour définir les Objectifs de sécurité à partir des exigences d'assurance et fonctionnelles en matière de sécurité, qui peuvent être regroupées dans les Profils de protection.

Ces Objectifs de sécurité invoqués sont ensuite évalués par des laboratoires d'essais indépendants et certifiés avant d'être listés comme produits certifiés dans la base de données des Critères communs. Les exigences et l'exhaustivité de l'évaluation réalisée par le laboratoire d'essais sont ensuite transmis par un EAL assigné (Niveau d'assurance d'évaluation) classé de EAL 1 — fonctions testes, à EAL 7 — conception formellement vérifiée et testée. Cela signifie que les Critères communs peuvent s'étendre aux systèmes d'exploitation et pare-feux, jusqu'aux TPM et passeports.

Pour en savoir plus sur les conditions de certification des Critères communs, consultez le site web des critères communs, *www.commoncriteriaportal.org/*

4.2.2 FIPS 140

Les normes FIPS (Federal Information Processing Standards) 140-2 et 140-3 sont des normes de sécurité de l'information pour les modules informatiques cryptographiques et l'utilisation d'algorithmes cryptographiques, publiées par le NIST (National Institute of Standards and Technology) et adoptées comme exigence par les gouvernements fédéraux des États-Unis et du Canada. FIPS 140-3 a remplacé

FIPS 140-2 en 2019 en tant que version mise à jour. La validation par un laboratoire de test certifié NIST garantit que le système et la cryptographie du module sont correctement mis en œuvre. En résumé, la certification nécessite une description, une spécification et une vérification du module de calcul cryptographique, des algorithmes approuvés, des modes de fonctionnement et des tests de mise sous tension.

Les clients peuvent être assurés que leurs produits peuvent être utilisés conformément aux spécifications gouvernementales. Cela permet aux clients d'avoir l'esprit tranquille lorsque des audits sont effectués par les autorités gouvernementales. Les organisations qui ne sont pas réglementées par la norme FIPS 140 sont assurées que leurs produits respectent les normes définies par le gouvernement. Pour en savoir plus sur les conditions de certification FIPS 140-2 et FIPS 140-3, rendez-vous sur le site web du NIST à l'adresse *www.nist.gov*

Pour qu'un système complet soit conforme à la norme FIPS 140, chaque composant du système doit être conforme à la norme FIPS 140. Par exemple, le système de gestion vidéo, le serveur d'enregistrement, ainsi que les dispositifs connectés tels que les caméras, devraient être conformes. Un périphérique est conforme à la norme FIPS 140 lorsqu'il utilise au moins un module certifié par logiciel ou un module certifié par matériel.

Les périphériques Axis dotés de la version 12 ou ultérieure du système d'exploitation AXIS sont équipés du module cryptographique Axis (OpenSSL) certifié FIPS 140 et basé sur un logiciel. La plupart des nouveaux périphériques Axis intègrent un système de cryptographie matérielle certifié FIPS 140 ainsi que le module cryptographique logiciel. Cela permet d'optimiser l'utilisation du module certifié par logiciel pour les applications logicielles telles que HTTPS et IEEE 802.1X au niveau du système d'exploitation, ainsi que le module certifié par matériel pour le stockage sécurisé des clés.

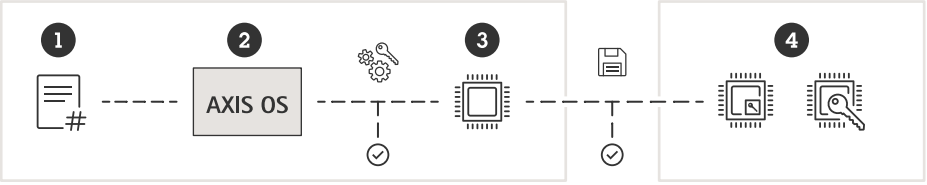

Figure 12. Utilisation de logiciels et de modules matériels cryptographiques conformes à la norme FIPS 140 dans un périphérique Axis. Les applications (1) sont servies par le module cryptographique Axis, intégré dans le système d'exploitation AXIS (2) du périphérique Axis. Le module cryptographique Axis effectue des opérations cryptographiques, à la fois symétriques et asymétriques, en utilisant le SoC (3) et/ou les modules de calcul cryptographique matériels intégrés (4) pour le stockage sécurisé des clés.

1. *Applications nécessitant une cryptographie ou basées sur TLS (telles que HTTPS, webRTC et 802.1X)*
2. *Système d'exploitation AXIS avec module cryptographique logiciel intégré (certificat NIST : https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4621*
3. *SoC*
4. *Modules de calcul cryptographique matériels intégrés*

4.3 Protection de clés privées

Pour un concurrent, l'extraction de la clé privée peut leur permettre d'espionner sur le trafic réseau encrypté par HTTPS ou de prétendre être le véritable périphérique pour accéder à un réseau 802.1X protégé.

Les périphériques Axis prennent en charge divers protocoles TLS (Sécurité de la couche de transport) pour une communication sécurisée. L'ID de périphérique Axis, (IEEE 802.1AR), HTTPS (chiffrement réseau) et 802.1X (contrôle d'accès réseau) reposent sur la protection des informations cryptographiques X.509.

Le certificat numérique X.509 du TLS utilise un certificat et la paire de clés publique et privée correspondante pour permettre à deux hébergeurs du réseau de communiquer. La clé privée est stocké dans le fichier de clés sécurisé et ne le quitte jamais, même lorsqu'elle est utilisée pour décrypter des données. Le certificat concerné et la clé publique sont connus, peuvent être partagés par le périphérique Axis et sont utilisés pour encrypter les données.

4.4 Protection des clés de contrôle d'accès

La protection des informations cryptographiques utilisées dans les solutions de contrôle d'accès Axis, telle que le canal sécurisé du protocole OSDP (Open Supervised Device Protocol), est un exemple de l'importance du stockage de clés matériel protégé.

Le canal sécurisé du protocole OSDP est un schéma de cryptage et d'authentification AES-128 largement utilisé pour protéger la communication entre les contrôleurs de porte et les périphériques tels que les lecteurs.

La clé symétrique AES, Clé de base du canal sécurisé (SCBK), partagée par le contrôleur et le lecteur de la porte, est utilisée pour initier une authentification mutuelle et générer ultérieurement un ensemble de clés de session pour encrypter les données de communication entre les contrôleurs et les lecteurs de portes.

Pour assurer une véritable sécurité de bout en bout, la Clé principale (MK) et la clé SCBK doivent être stockées dans le fichier de clés sécurisé du contrôleur de porte du réseau Axis. La Clé principale dérive une clé SCBK unique par lecteur Axis connecté. Par ailleurs, la clé SCBK individuelle, qui est distribuée de façon individuelle pendant la phase d'installation à un lecteur Axis, doit être stockée dans le fichier de clés sécurisé du lecteur. Le lecteur est plus important sachant qu'il est normalement installé du côté non-sécurisé de la porte.

De cette façon, les clés de canal sécurisé du protocole OSDP sont protégées aux deux bouts dans un environnement matériel protégé. Ceci empêche toute extraction malveillante même en cas de faille de sécurité.

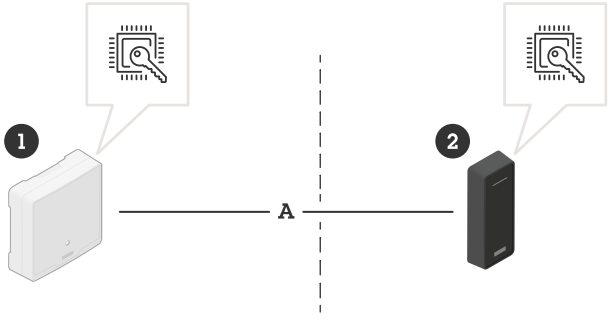

Figure 13. Assurer une sécurité de bout en bout avec un fichier de clés sécurisé en contrôle d'accès. La clé principale et la clé de base individuelle du canal sécurisé (SCBK) sont toutes deux stockées dans les fichiers de clés sécurisés, dans les périphériques de chaque côte dé la porte.

1 Contrôleur de porte Axis installé du côté protégé de la porte
2 Lecteur Axis installé du côté non protégé de la porte
A Communication par canal sécurisé OSDP

4.5 Protection des clés du système de fichiers

Un périphérique Axis en fonctionnement contient la configuration et les informations spécifiques au client. Il en va de même lorsque le périphérique Axis est en transit d'un distributeur ou d'un intégrateur système qui fournit des services de pré-configuration vers le client. Lorsque l'accès physique au périphérique Axis est obtenu, un concurrent malveillant peut essayer d'extraire les informations à partir du système de fichiers en démontant la mémoire Flash et en y accédant via un lecteur Flash. Par conséquent, protéger le système de fichiers en lecture-écriture contre l'extraction d'informations sensibles ou le sabotage de la configuration est essentiel lorsque le périphérique Axis a été volé ou lorsqu'il y eu intrusion.

Le fichier de clés sécurisé empêche l'exfiltration malveillante d'informations et le sabotage de la configuration en faisant respecter un cryptage renforcé dans le système de fichiers. Lorsque le périphérique Axis est allumé, les informations du système de fichiers sont encryptées. Pendant le processus de démarrage, le système de fichiers est décrypté avec une clé AES-XTS-Plain64 256 bits pour que le système de fichiers puisse être monté et utilisé par le périphérique Axis. La clé de chiffrement du système de fichiers est générée de façon unique par périphérique avec les paramètres d'usine par défaut et régénérée lors de chaque mise à jour du logiciel, ce qui signifie que la clé n'est jamais la même tout au long de la vie du périphérique.

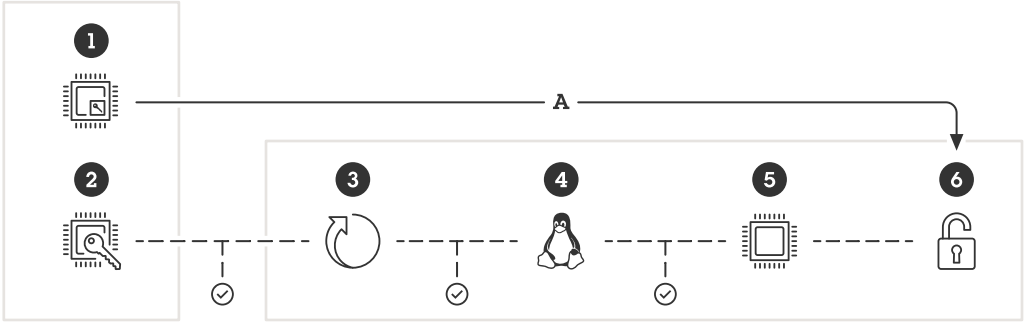

Figure 14. L'environnement TEE (1) et la ROM d'amorçage (2) sont intégrés au SoC. Pendant le processus d'amorçage, le système de fichiers en lecture-écriture (6) est déchiffré (par l'environnement TEE) pour que le système de fichiers puisse être monté et utilisé par le dispositif Axis. Dans le processus d'amorçage, chaque maillon de la chaîne (programme d'amorçage (3), noyau Linux (4) et système de fichiers racine (5)) est vérifié et authentifie le sous-système suivant dans la mémoire flash. Il en résulte un système de fichiers racine vérifié.

1 Environnement TEE
2 ROM d'amorçage
3 Programme d'amorçage
4 Noyau Linux
5 Système de fichiers racine
6 Système de fichiers en lecture-écriture
A L'environnement TEE déchiffre le système de fichiers en lecture-écriture.

5 Protection contre le sabotage des vidéos

Le marché de la sécurité est associé à un postulat fondamental : la vidéo enregistrée par les caméras de surveillance est authentique et fiable. La signature de vidéo est une fonction mise au point pour préserver et renforcer la crédibilité de la vidéo en tant que preuve. En vérifiant l'authenticité de la vidéo, cette fonction permet de garantir qu'elle n'a pas été éditée ou falsifiée après avoir quitté la caméra.

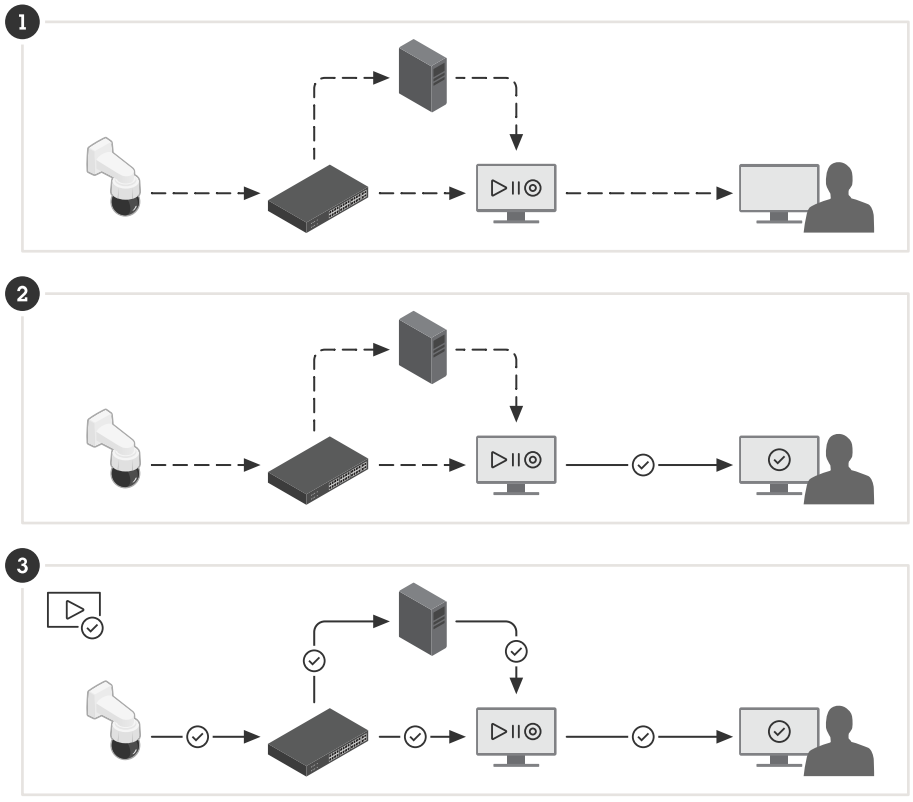

Figure 15. Vérifier l'authenticité de la vidéo.

1 *Une vidéo passe de nombreuses étapes de la caméra jusqu'au visionnage de l'enregistrement. Un pirate compétent peut saboter la vidéo à chacune de ces transitions.*
2 *Avec l'ajout du filigrane VMS à la vidéo pendant l'exportation, certaines étapes sont vérifiées, mais il n'existe aucune garantie que la vidéo n'ait pas été modifiée à une étape précédente.*
3 *Une vidéo signée permet de s'assurer que celle-ci n'a pas été sabotée à l'une des étapes, depuis la caméra jusqu'au visionnage de l'enregistrement exporté. La vidéo peut être reliée au périphérique qui l'a enregistrée.*

5.1 Vidéo signée

Avec la fonction de signature de vidéo développée par Axis, qui est disponible de façon proactive en open-source, une signature dans le flux vidéo peut servir à protéger l'intégrité de la vidéo et à vérifier son origine en remontant à la caméra qui l'a produite. Cette fonction permet ainsi de prouver l'authenticité de la vidéo sans avoir à démontrer la chaîne de détention du fichier vidéo.

Lorsqu'un système de caméra vidéo enregistre un incident, la police peut recevoir la vidéo sous forme de fichiers vidéo exportés sur une clé USB et les enregistrer dans un système de gestion de preuves (EMS, Evidence Management System). Lorsqu'il exporte la vidéo de la caméra, l'agent de police peut vérifier si la vidéo est correctement signée. Si elle est ultérieurement utilisée dans une procédure judiciaire, le tribunal peut contrôler la date et l'heure d'enregistrement de la vidéo, la caméra correspondante et les éventuels

changements ou suppressions d'images vidéo. Avec le *lecteur de fichiers* Axis, quiconque disposant d'un exemplaire de la vidéo peut consulter ces informations.

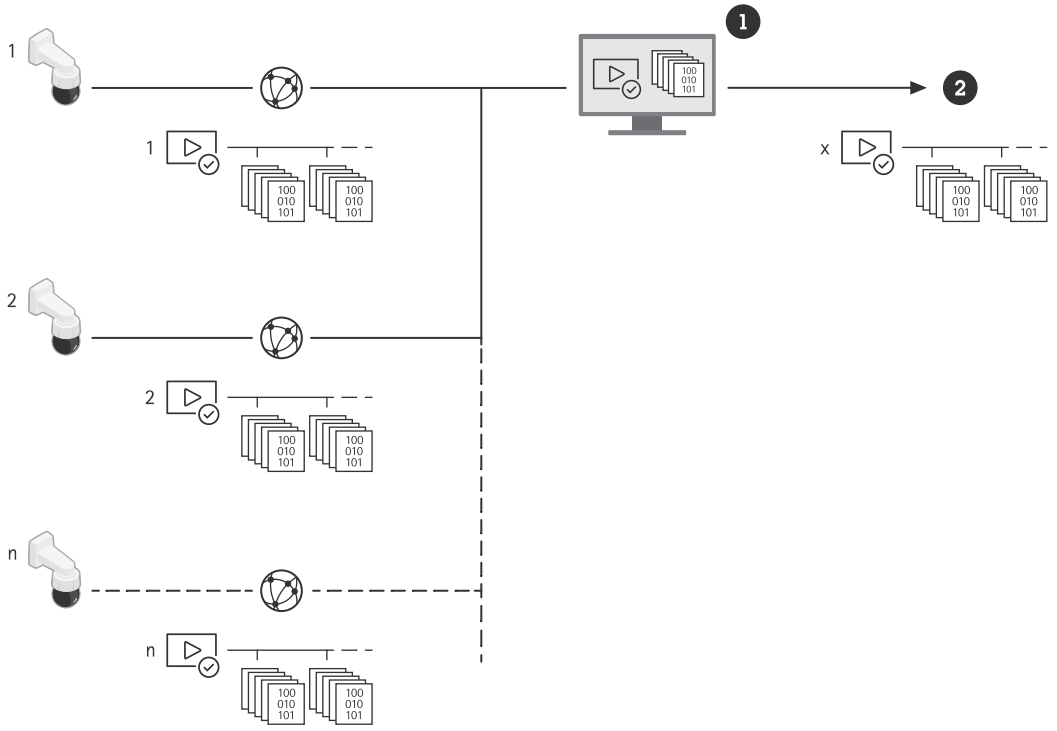

Figure 16. Comme la signature est ajoutée au niveau de la caméra, il est possible de vérifier le contenu à chaque étape, de la source à l'utilisation finale de la vidéo.

1 *VMS*
2 *Exportation de la vidéo vers CD/USB/web/e-mail*

Chaque caméra utilise sa clé de signature de vidéo unique, qui est stockée dans un fichier de clés sécurisé, pour ajouter une signature dans le flux vidéo. Cette opération passe par le calcul d'un hachage de chaque

image vidéo, y compris ses métadonnées, puis par la signature du hachage combiné. La signature est ensuite stockée dans des champs de métadonnées dédiés du flux vidéo (en-tête SEI).

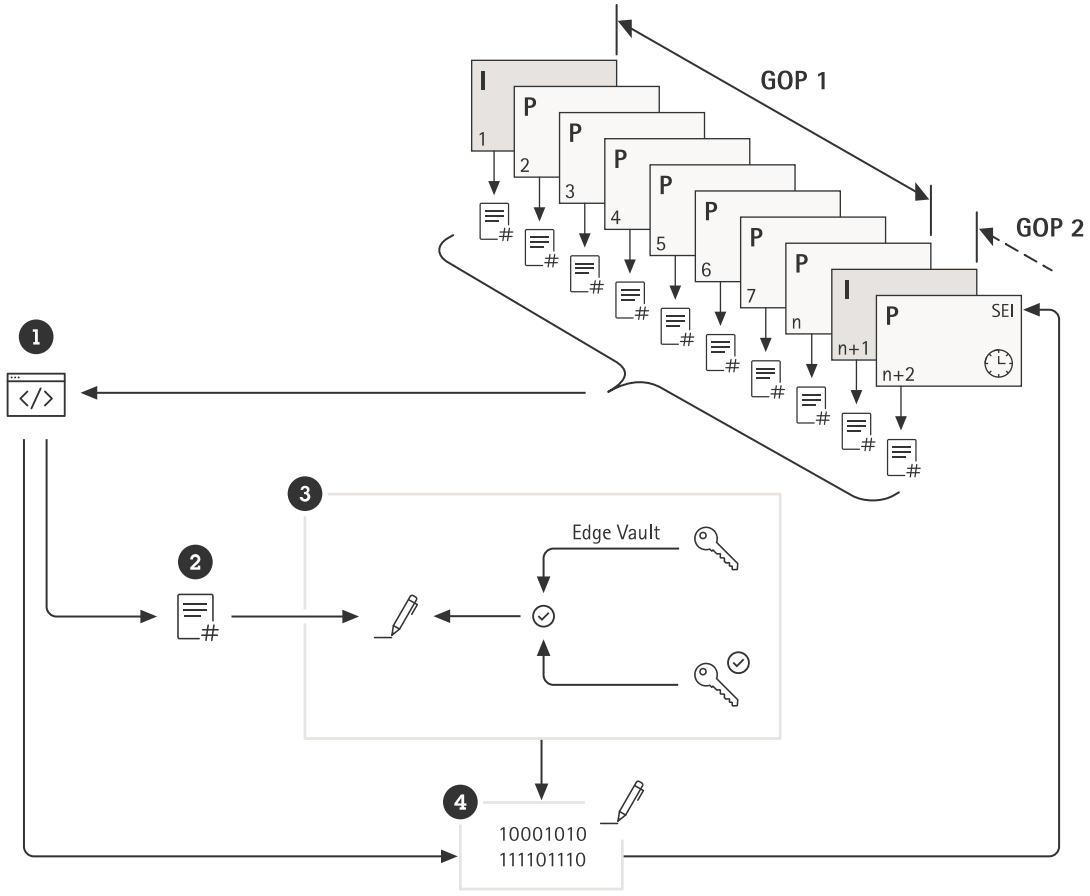

Figure 17. Représentation graphique de l'ajout d'une signature au flux vidéo. Le contenu de chaque image d'un groupe d'images (GOP) fait l'objet d'un hachage, en parallèle au hachage des métadonnées (1). Le résultat forme le hachage GOP (2), qui est signé dans Edge Vault (3) à l'aide de la clé de signature vidéo et de la clé d'attestation uniques au dispositif. La signature numérique (4) et les métadonnées (1) sont ensuite ajoutées à un en-tête SEI ultérieur, transmis aux côtés du flux vidéo.

1. *Métadonnées uniques au dispositif (ID matériel, version d'AXIS OS, numéro de série et rapport d'attestation*) et métadonnées du flux (compteur GOP et hachages d'images)*
2. *Hachage GOP*
3. *Axis Edge Vault*
4. *Signature numérique*

* *Le rapport d'attestation peut servir à vérifier l'origine et la provenance de la paire de clés utilisée pour la signature. La vérification de l'attestation des clés permet de s'assurer que la clé est stockée de manière sécurisée dans le matériel d'un dispositif donné. Cette méthode authentifie l'origine de la vidéo.*

La signature effective est réalisée à l'aide d'une clé de signature de vidéo unique au dispositif qui est attestée en utilisant une clé d'attestation unique au dispositif. La clé d'attestation est jointe au début du flux puis à intervalles réguliers, généralement une fois toutes les heures. Comme les métadonnées contiennent le hachage de chaque image individuelle, il est possible de détecter laquelle est correcte. Pour terminer le processus de signature, la structure du groupes d'images (GOP) de la vidéo doit être protégée. Pour ce faire, le hachage de la première image I du GOP suivant est inclus dans la signature.

Cette opération évite les coupes indétectables ou la réorganisation des images. Dans le cas improbable où des images seraient perdues pendant la diffusion ou endommagées pendant le stockage, ceci pourrait être signalé de la même manière.

6 Glossaire

Identifiant de périphérique Axis : un certificat de périphérique unique avec les clés correspondantes qui prouvent l'authenticité du périphérique Axis. Le périphérique Axis est le provisionnement en usine avec un identifiant de périphérique Axis stocké dans le fichier de clés sécurisé. L'identifiant de périphérique Axis est fondé sur la norme internationale IEEE 802.1AR (IDevID, Identifiant de périphérique initial), qui définit une méthode d'identification automatisée et sécurisée.

Axis Edge Vault : la plateforme de cybersécurité matérielle qui protège les périphériques Axis. Elle repose sur des bases solides constituées de modules de calcul cryptographique (élément sécurisé et TPM) et d'une sécurité SoC (TEE et démarrage sécurisé), associés au savoir-faire en matière de sécurité des dispositifs périphériques.

Certificat : un document signé qui atteste de l'origine et des propriétés d'une paire de clés publique/privée. Le certificat est signé par une Autorité de certification (CA). Si le système fait confiance à la CA, il fait également confiance aux certificats qu'elle délivre.

Autorité de certification (CA) : racine de confiance d'une chaîne de certification. Elle sert à prouver l'authenticité et la véracité des certificats sous-jacents.

Critères communs (CC) : une norme internationale pour la certification en matière de sécurité des produits IT. Également dénommés Critères communs d'évaluation de la sécurité des technologies de l'information, ISO/IEC 15408.

FIPS 140 : une série de normes américaines de sécurité informatique utilisées pour approuver les modules de calcul cryptographiques. FIPS (normes fédérales de traitement de l'information) 140 définit les exigences concernant la façon dont un module cryptographique doit être conçu et mis en œuvre pour atténuer les risques de sabotage du module.

ROM inaltérable (mémoire à lecture seule) : la mémoire à lecture seule qui stocke de façon sécurisée les clés publiques de confiance et le programme utilisé pour comparer les signatures, pour qu'elles ne soient pas réenregistrées.

Provisionnement : processus de préparation et d'équipement d'un dispositif pour le réseau. Cela implique l'envoi de données de configuration et de paramètres de stratégie au dispositif à partir d'un point central. Le dispositif est fourni avec des clés et des certificats.

Cryptographie à clé publique : système de cryptographie asymétrique où une personne peut chiffrer un message à l'aide de la *clé publique* du destinataire, mais seul le destinataire, à l'aide de la *clé privée*, peut déchiffrer le message. Peut être utilisé pour chiffrer et signer des messages.

Démarrage sécurisé : une fonction pour empêcher le chargement de logiciels non-autorisés pendant le démarrage du périphérique. Le démarrage sécurisé utilise un système d'exploitation signé qui garantit que seul le logiciel Axis autorisé est employé pour démarrer le périphérique.

Élément sécurisé : un module de calcul cryptographique qui fournit un stockage matériel des clés privées protégé contre le sabotage et sécurise l'exécution des opérations cryptographiques. Au contraire du TPM, les interfaces matérielle et logicielle d'un élément sécurisé ne sont pas standardisées mais spécifiques au fabricant.

Fichier de clés sécurisé : un environnement protégé du sabotage pour la protection des clés privées et l'exécution sécurisée des opérations cryptographiques. Il empêche l'accès non-autorisé et l'extraction malveillante en cas de faille de sécurité. Selon les exigences de sécurité, un périphérique de sécurité peut posséder un ou plusieurs modules de calcul cryptographique matériels, qui fournissent un fichier de clés matériel protégé et sécurisé.

Système d'exploitation signé : logiciel du périphérique dont l'image de fichier a été signée numériquement par code par un tiers de confiance. Un système d'exploitation signé est une exigence du processus de démarrage sécurisé visant à s'assurer que le périphérique ne s'amorce qu'à partir d'une image logicielle de confiance. Dans les produits basés sur le système d'exploitation AXIS, le périphérique vérifie l'intégrité et l'authenticité de l'image logicielle de l'appareil avant d'effectuer une mise à jour.

Vidéo signée : une fonction qui maintient et renforce la confiance dans les vidéos en tant que preuve. Un vidéo signée permet la détection du sabotage d'une vidéo et confire son authenticité. Elle est utilisée pour assurer l'intégrité de la vidéo et remonter jusqu'à une caméra Axis en particulier. Les clés de signature pour une vidéo signée se trouve dans le fichier de clés sécurisé du périphérique Axis.

Sécurité de la couche de transport (TLS) : une norme Internet de protection du trafic réseau. TLS représente le S (de sécurisé) dans HTTPS.

Environnement d'exécution de confiance (TEE) : fournit un stockage matériel des clés privées protégé contre le sabotage et sécurise l'exécution des opérations cryptographiques. Au contraire de l'élément sécurisé et du TPM, le TEE est une zone matérielle sécurisée du processeur principal du système sur puce (SoC).

Module de plateforme de confiance (TPM) : un module de calcul cryptographique qui fournit un stockage matériel des clés privées protégé contre le sabotage et sécurise l'exécution des opérations cryptographiques. Les TPM sont des composants informatiques normalisés à l'échelle internationale (TPM 1.2, TPM 2.0) définis par le *Groupe informatique de confiance (TCG)*.

Sécurité à zéro confiance : une approche moderne de la sécurité des IT où les périphériques connectés et l'infrastructure IT (tels que les réseaux, les services cloud et les applications) doivent s'identifier, se valider et s'authentifier mutuellement de façon récurrente pour instaurer des mesures de sécurité élevée.

À propos d'Axis Communications

En concevant des solutions qui améliorent la sécurité et les performances de l'entreprise, Axis crée monde plus clairvoyant et plus sûr. En tant qu'entreprise de technologie de réseau et leader de l'industrie, Axis propose des solutions de vidéosurveillance, de contrôle d'accès, d'interphonie et de systèmes audio. Les performances de ces solutions sont améliorées grâce à des applications d'analyse intelligentes et une formation de haute qualité.

Axis emploie près de 4 000 personnes dans plus de 50 pays et collabore avec des partenaires technologiques et d'intégration de systèmes dans le monde entier pour fournir des solutions clients adaptées. Axis a été fondée en 1984 et le siège social se trouve à Lund, en Suède