

# Axis Edge Vault

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

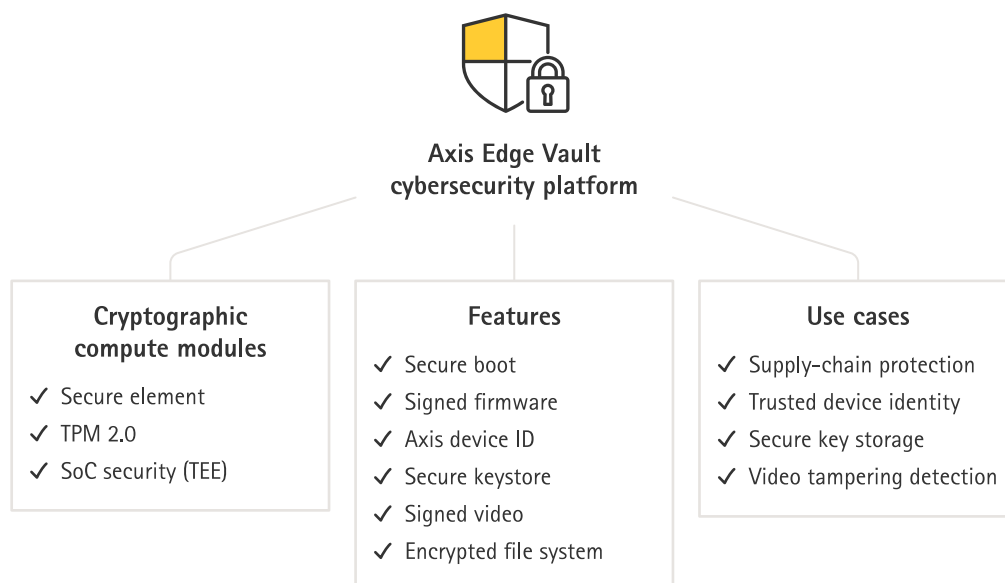
- identité du périphérique de confiance
- stockage sécurisé des clés
- détection de sabotage des vidéos
- protection de la chaîne d'approvisionnement

Avril 2023

# 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 *firmware 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.

Avec Axis Edge Vault, les périphériques Axis réduisent l'exposition des clients aux risques de sécurité en empêchant l'espionnage et l'extraction malveillante d'informations sensibles. Axis Edge Vault permet également au périphérique Axis d'être une unité fiable et de confiance au sein du réseau du client.



- **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. À la lecture, le lecteur vidéo 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.

- **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 firmware signé, la racine de confiance de la chaîne ne peut pas être établie. Le démarrage sécurisé, associé au firmware signé, fournit une chaîne ininterrompue de logiciels validés de manière cryptographique, à partir de la mémoire inaltérable (démarrage ROM). Le démarrage sécurisé garantit qu'un périphérique ne peut être démarré uniquement avec un firmware signé, ce qui empêche le sabotage de la chaîne d'approvisionnement physique. Avec le firmware signé, le périphérique est aussi capable de valider un nouveau firmware avant d'accepter son installation. Si le périphérique détecte que l'intégrité du firmware est compromise ou que le firmware n'est pas signé par Axis, la mise à niveau du firmware sera rejetée. Ceci protège les périphériques du sabotage du firmware.

# Table des matières

1	Introduction	5
2	– Identité du périphérique de confiance	5
	2.1 Identification sécurisée de périphérique avec l'identifiant de périphérique Axis	5
	2.2 Intégration sécurisée au réseau	8
3	Stockage sécurisé des clés	10
	3.1 Fichier de clés sécurisé	10
	3.2 Critères communs et FIPS 140	11
	3.3 Protection de clés privées	12
	3.4 Protection des clés de contrôle d'accès	12
	3.5 Protection des clés du système de fichiers	13
4	Protection contre le sabotage des vidéos	14
	4.1 Vidéo signée	15
5	– Protection de la chaîne d'approvisionnement	17
	5.1 Démarrage sécurisé	17
	5.2 Firmware signé	17
6	Glossaire	19

# 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 étudieront pourquoi le firmware signé et le démarrage sécurisé sont des mesures fondamentales pour contrer le sabotage du firmware 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 — 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 de réseau peut vérifier son intégrité et son authenticité selon un procédé semblable à celui de fournir une preuve de votre identité aux autorités en montrant votre passeport à l'aéroport.

### 2.1 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 de provisionnement pour la configuration initiale du périphérique et la mise à jour du firmware.

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*, IDDevID). 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.

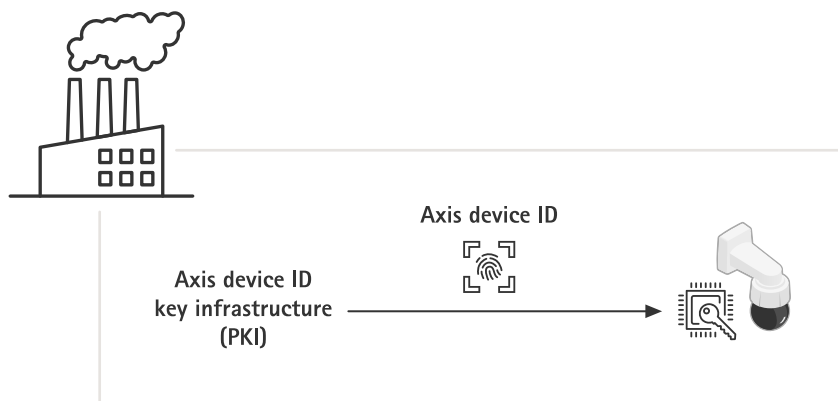


Figure 1. Lors du processus de fabrication de l'unité, l'identifiant de périphérique Axis unique est stocké dans le fichier de clés sécurisé de l'unité.

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 de 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 trouver davantage d'informations concernant l'infrastructure PKI Axis sur [www.axis.com/support/public-key-infrastructure-repository](http://www.axis.com/support/public-key-infrastructure-repository)

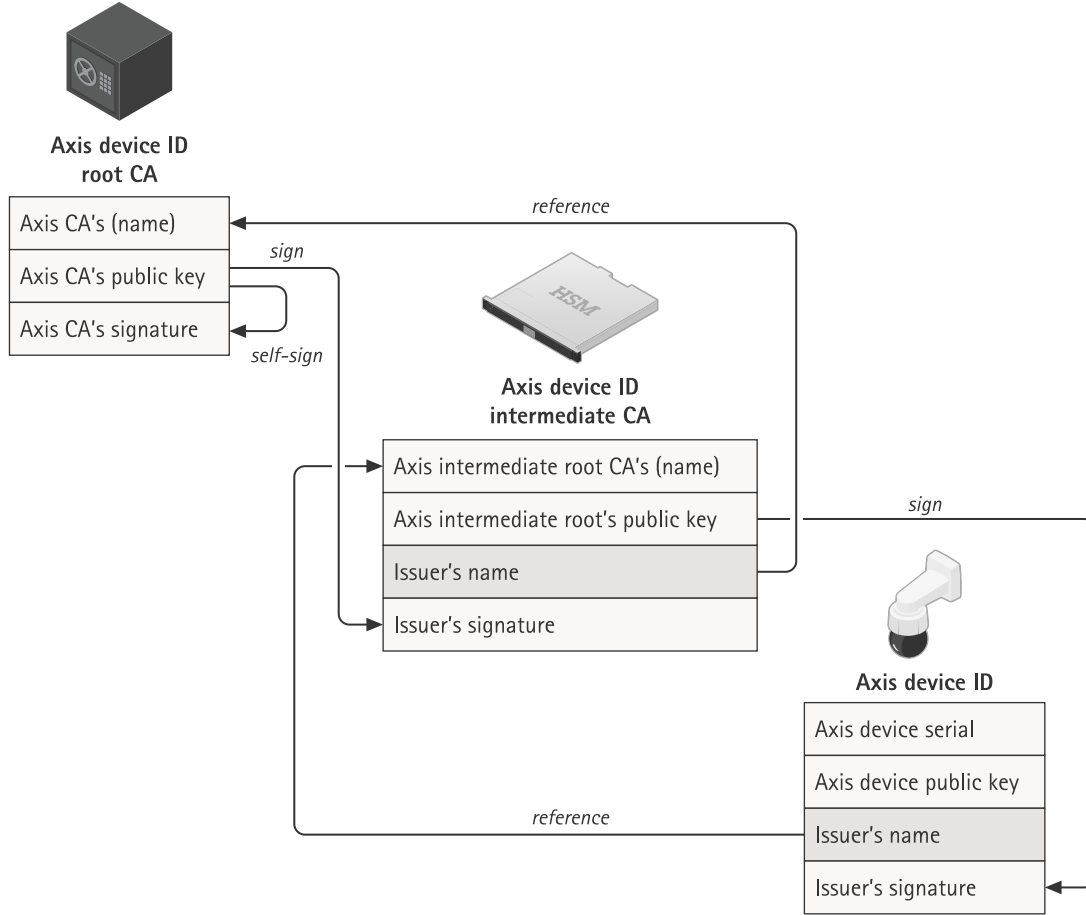


Figure 2. Infrastructure à clés publiques (PKI) IEEE 802.1AR Axis pour le provisionnement en usine de l'identifiant de périphérique Axis pendant le processus de fabrication. L'identifiant de périphérique Axis, qui constitue un certificat incorporé au numéro de série du produit, est signé par une CA intermédiaire qui a été signée par la CA racine de l'identifiant de périphérique Axis. Étant donné que la CA racine Axis a beaucoup de valeur et doit être stockée dans un coffre, la CA intermédiaire est nécessaire pendant le provisionnement en usine.



Figure 3. Exemple d'identifiant de périphérique Axis.

## 2.2 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 disposez 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 firmware 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.

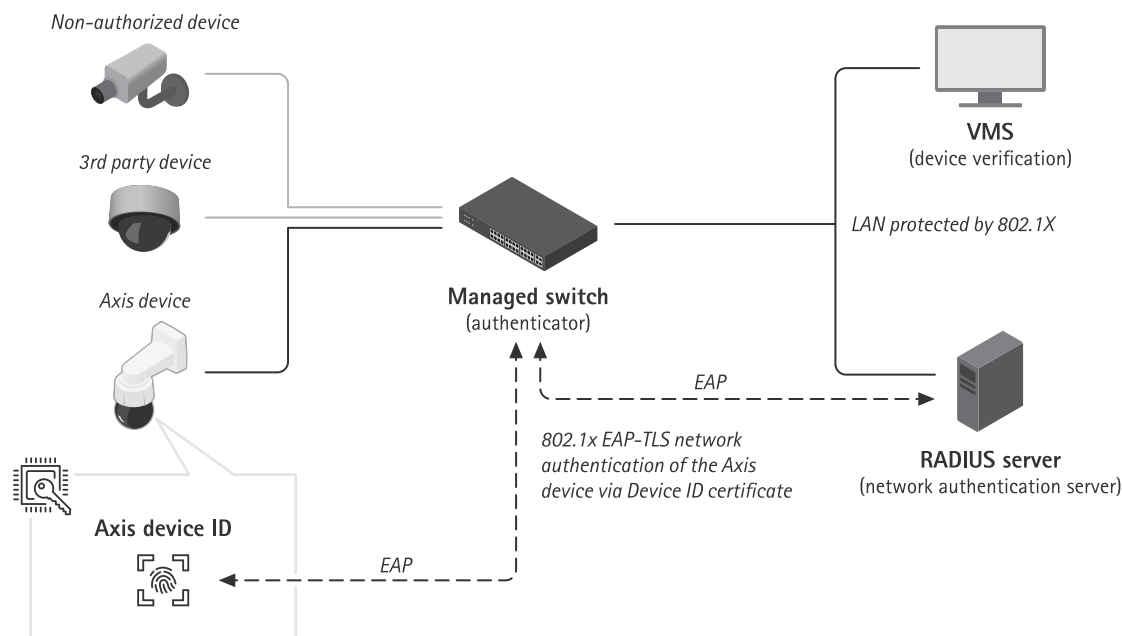


Figure 4. Intégration sécurisée au réseau. Vous pouvez ordonner à votre serveur d'authentification d'accepter automatiquement les périphériques Axis sur le réseau à l'aide des numéros de série des périphériques et de l'identifiant de périphérique Axis. L'identifiant de périphérique Axis sert d'empreinte digitale qui garantit l'intégration sécurisée et automatisée des périphériques. Les périphériques non-autorisés doivent être intégrés manuellement.



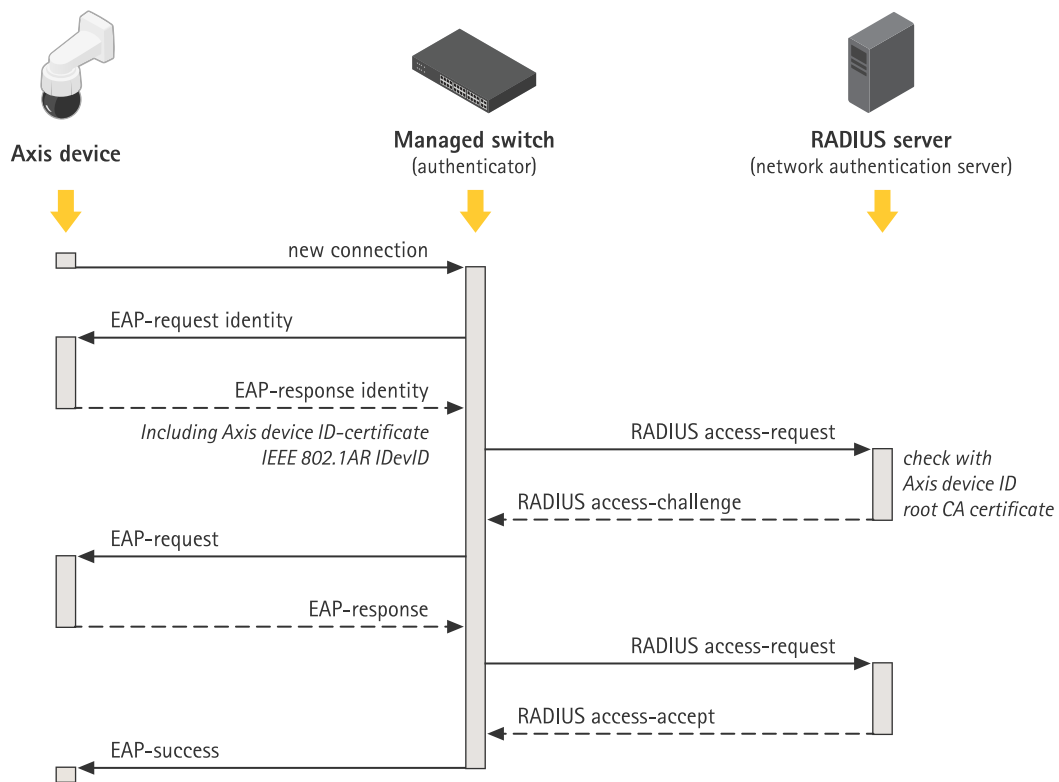


Figure 5. Description plus détaillée du processus d'intégration. Le norme IEEE 802.1AR, relative à l'identifiant de périphérique sécurisé, définit une méthode d'identification d'un périphérique via des requêtes de Protocole d'authentification extensible (EAP-TLS) de la norme IEEE 802.1X à l'aide du serveur RADIUS (Remote Authentication Dial-In User Service) pour accorder au périphérique l'accès au réseau.

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.

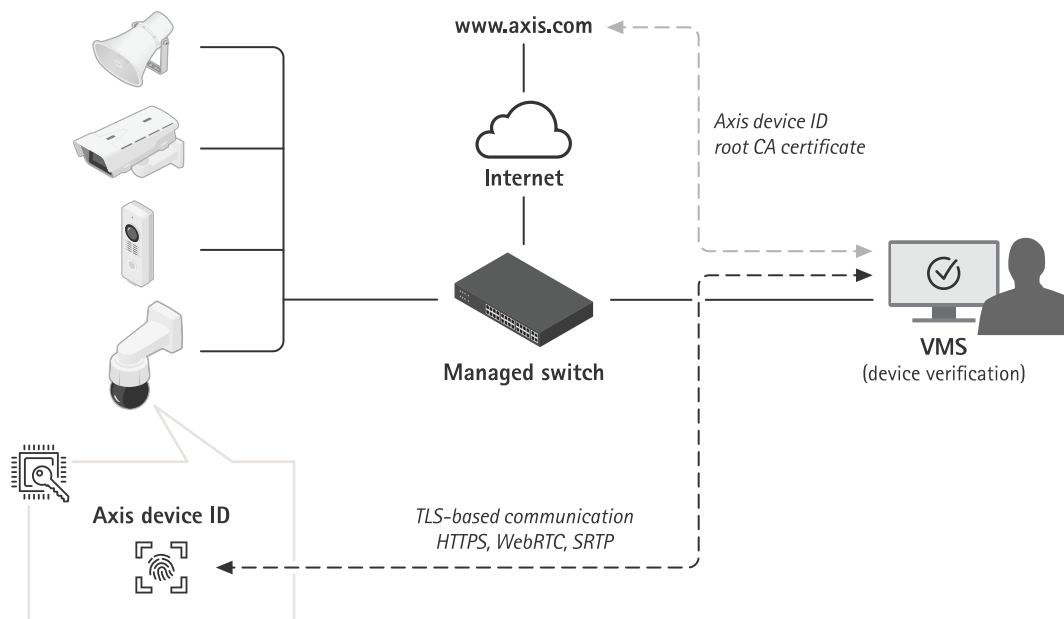


Figure 6. Après l'intégration sécurisée d'un périphérique, les applications de logiciel dans d'autres parties du système peuvent utiliser l'identifiant de périphérique Axis et les opérations cryptographiques pour vérifier le périphérique dans divers communication de type TLS. L'identifiant de périphérique Axis peut être vérifié à l'aide du certificat de la CA racine de l'identifiant de périphérique Axis, téléchargeable sur [axis.com](http://axis.com).

### 3 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.

#### 3.1 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, un périphérique Axis peut posséder un ou plusieurs modules de ce type, tels qu'un TPM 2.0 (Module de plateforme de confiance) ou un élément sécurisé et/ou un TEE (Environnement d'exécution de confiance).

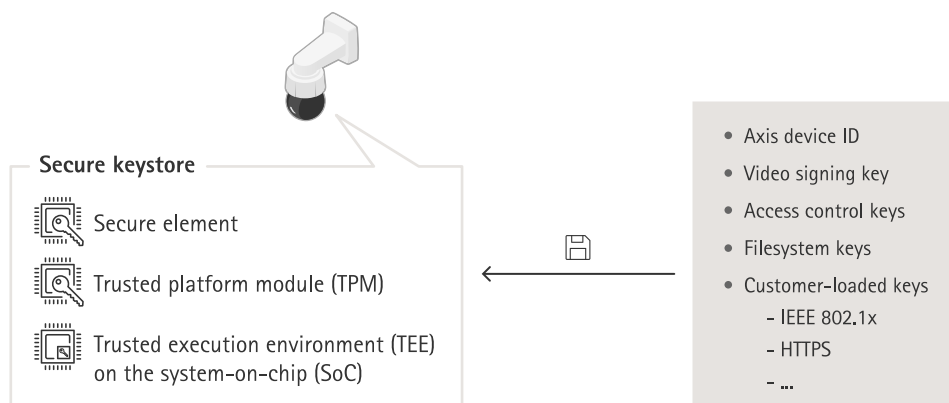


Figure 7. Le fichier de clés sécurisé présent dans les périphériques Axis peut employer un élément sécurisé, un TPM ou un TEE. Ils permettent tous de protéger les clés privées et de sécuriser l'exécution des opérations cryptographiques.

Le TPM et l'élément sécurisé sont des modules de calcul cryptographiques matériels montés sur une PCB (carte de circuits imprimés) tout près du processeur principal du SoC (Système sur puce). Le TEE est une zone sécurisée du processeur principal du SoC.

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.

## 3.2 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 ces 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.

### 3.2.1 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 testées, 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/](http://www.commoncriteriaportal.org/)

### 3.2.2 FIPS 140

FIPS (normes fédérales de traitement de l'information) 140-2 et 140-3 sont des normes relatives à la sécurité de l'information pour les modules de calcul cryptographique, publiées aux États-Unis par le NIST (Institut national des normes et technologies). FIPS 140-3 est la version mise à jour en 2019 de la norme FIPS 140-2 et l'a remplacée. 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.

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](http://www.nist.gov)

## 3.3 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. Ceci s'appuie sur la protection des informations cryptographiques X.509 telle que l'identifiant de périphérique Axis (IEEE 802.1AR), le protocole HTTPS (cryptage du réseau), 802.1X (Contrôle d'accès au réseau) et autres.

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 stockée 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.

## 3.4 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.

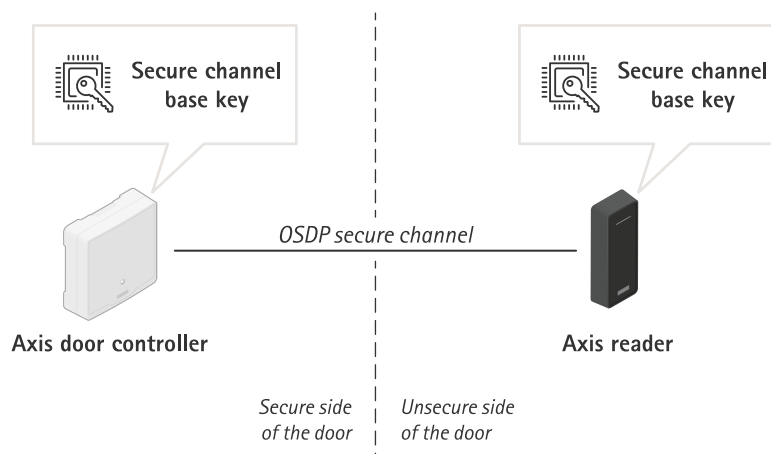


Figure 8. Assurer une sécurité de bout en bout avec un fichier de clés sécurisé en contrôle d'accès. La clé principale et la clé de base individuelle du canal sécurisé (SCBK) sont toutes deux stockées dans les fichiers de clés sécurisés, dans les périphériques de chaque côté de la porte.

### 3.5 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 firmware, ce qui signifie que la clé n'est jamais la même tout au long de la vie du périphérique.

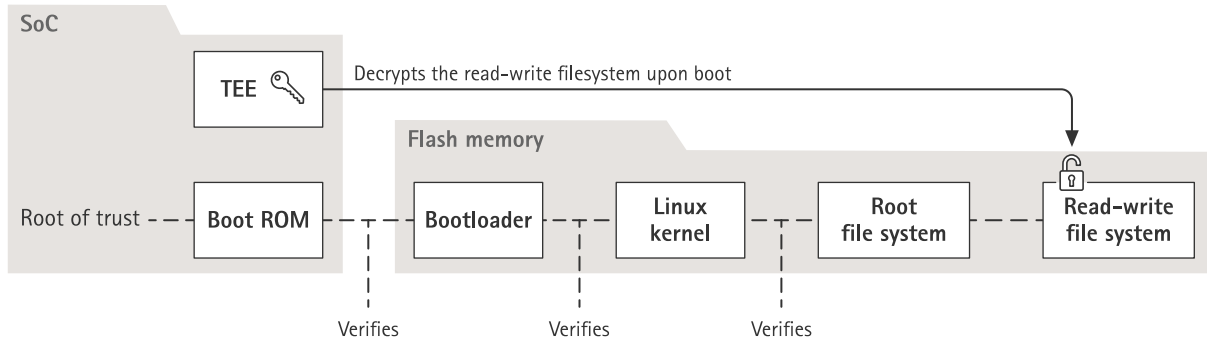


Figure 9. Le TEE dans le SoC détient la clé pour décrypter le système de fichiers racine.

## 4 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.

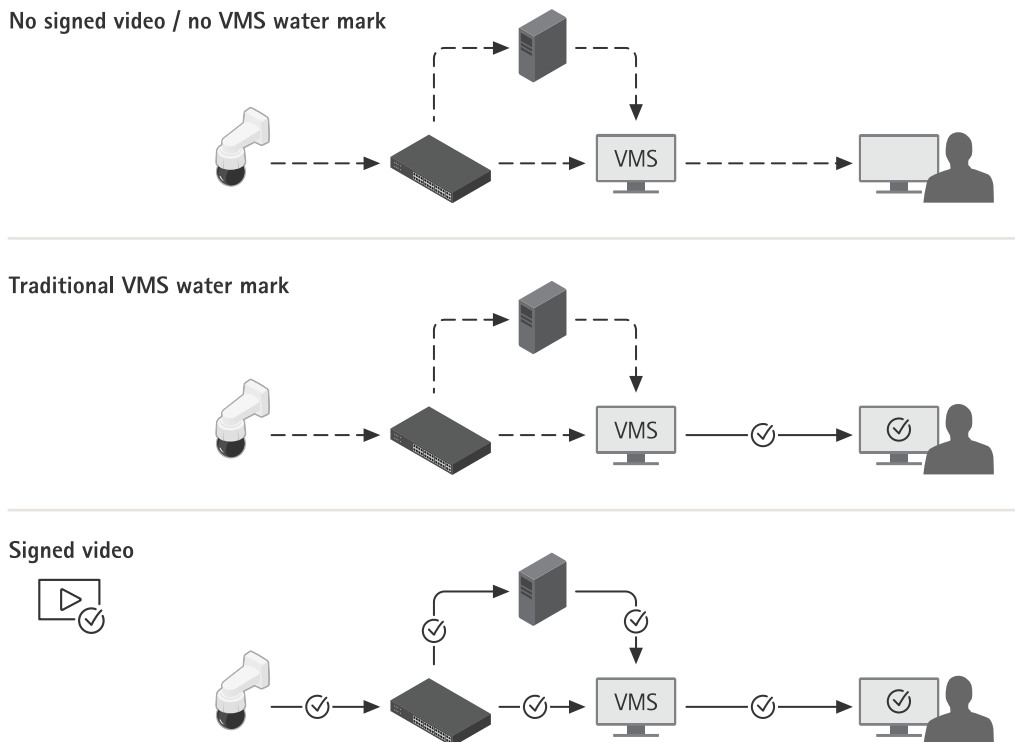


Figure 10. Vérifier l'authenticité de la vidéo.

Haut: 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.

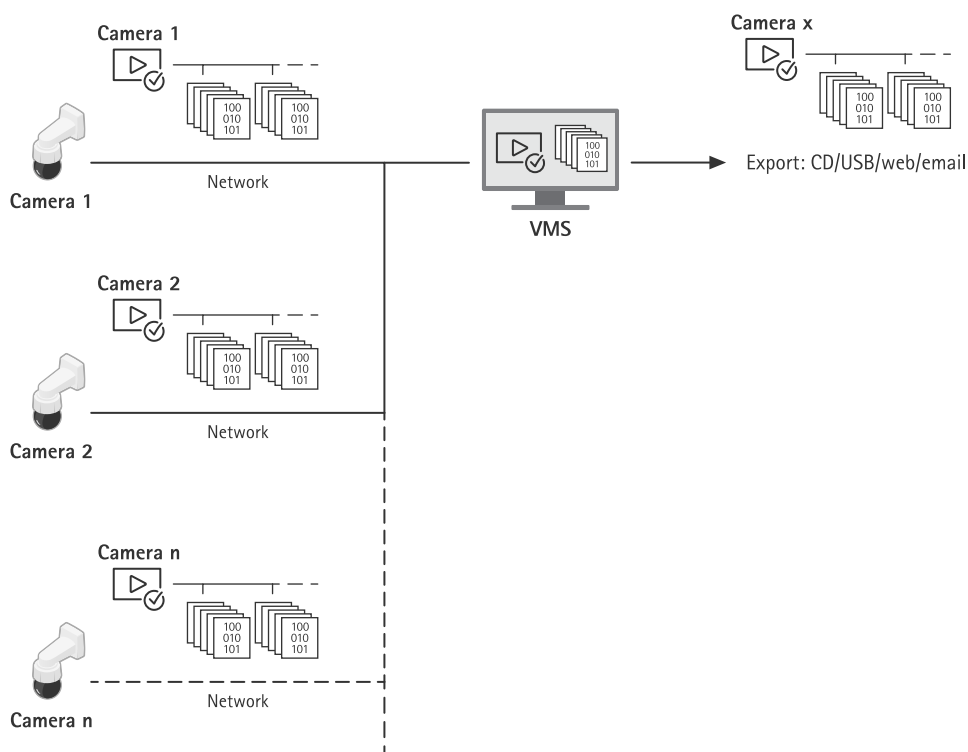
*Milieu : Avec l'ajout du filigrane VMS à la vidéo pendant l'exportation, certaines étapes sont vérifiées mais il n'existe aucune garantie que la vidéo n'ait pas été modifiée à une étape précédente.*

*Fond: Une vidéo signée garantit 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.*

## 4.1 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 11. 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.*

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).

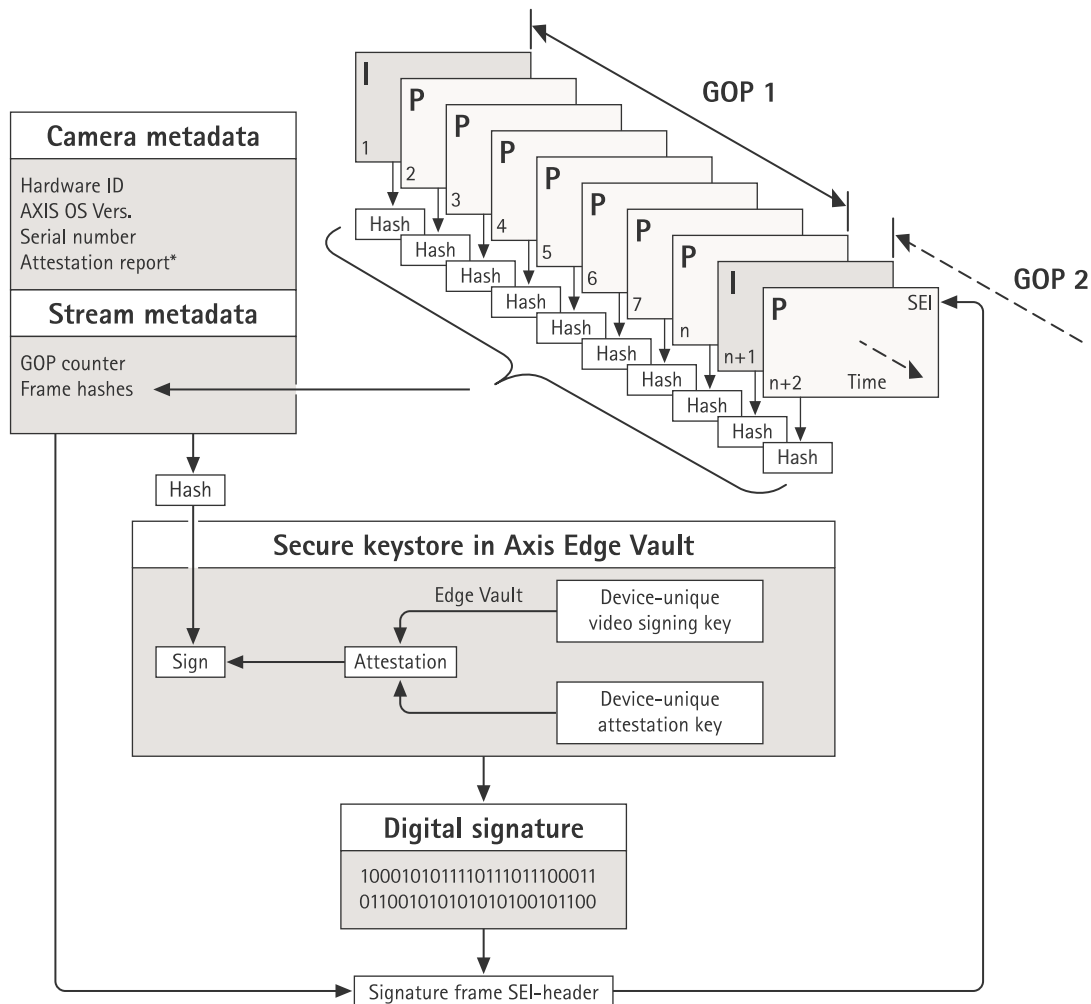


Figure 12. Représentation graphique de l'ajout d'une signature aux métadonnées de la vidéo. Le contenu de chaque image d'un groupe d'images (GOP) fait l'objet d'un hachage, en parallèle au hachage des métadonnées de la caméra et des métadonnées du flux. Il en résulte le hachage du GOP, qui est signé dans Edge Vault. La signature et les métadonnées sont ensuite ajoutées à un en-tête SEI ultérieur, transmis aux côtés du flux vidéo.

\* 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. L'événement peu probables de perte d'images dans la transmission du flux ou d'endommagement du contenu pendant le stockage seront signalés de la même manière.



## 5 — 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. AXIS OS, e retour, est signé de façon cryptographique (*firmware signé*) pendant le processus de génération.

Le démarrage sécurisé et le firmware signé sont liés l'un à l'autre. Ils assurent que le firmware 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 firmware compromis. Le démarrage sécurisé et le firmware signé créent ininterrompue de logiciels validés de manière cryptographique pour la chaîne de confiance qui sécurise toutes les opérations qui dépendent d'elle.

### 5.1 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 garantit qu'un périphérique peut démarrer seulement avec le firmware autorisé.

Le processus d'amorçage est lancé par la ROM d'amorçage qui valide le programme d'amorçage. L'amorçage sécurisé vérifie ensuite en temps réel les signatures intégrées de chaque bloc de firmware 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.

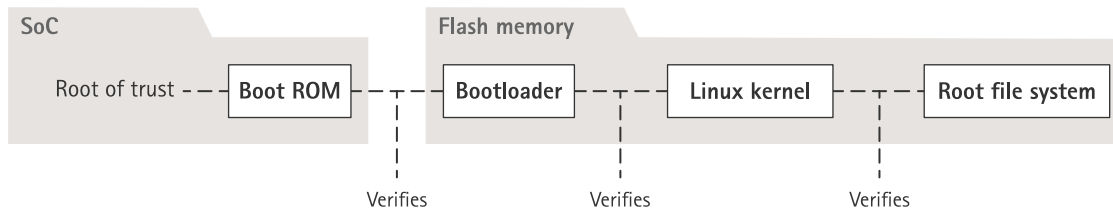


Figure 13. Dans le processus de démarrage sécurisé, chaque partie de la chaîne authentifie la suivante. Il en résulte un système de fichiers racine vérifié.

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. Sur un dispositif doté d'un amorçage sécurisé, le firmware installé dans la mémoire Flash est protégé contre les modifications. L'image d'usine par défaut est protégée, tandis que la configuration reste non 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 firmware par Axis.

### 5.2 Firmware signé

Le firmware signé Axis implique la signature par Axis de l'image du firmware avec une clé privée gardée secrète. Lorsque cette signature est associée à un firmware, le périphérique valide le firmware avant

d'accepter de l'installer. Si le dispositif détecte que l'intégrité du firmware est compromise, la mise à niveau du firmware est rejetée.

Le processus de signature du firmware 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 firmware.

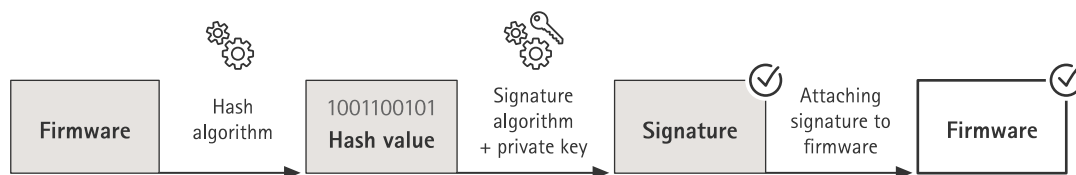


Figure 14. Processus de signature du firmware.

Avant une mise à niveau du firmware, l'authenticité du nouveau firmware 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 du firmware et en la comparant à cette valeur de hachage validée provenant de la signature, l'intégrité du firmware peut être vérifiée. La procédure de démarrage des périphériques Axis sera annulée si la signature du firmware est invalide ou si l'image du firmware a été modifiée.

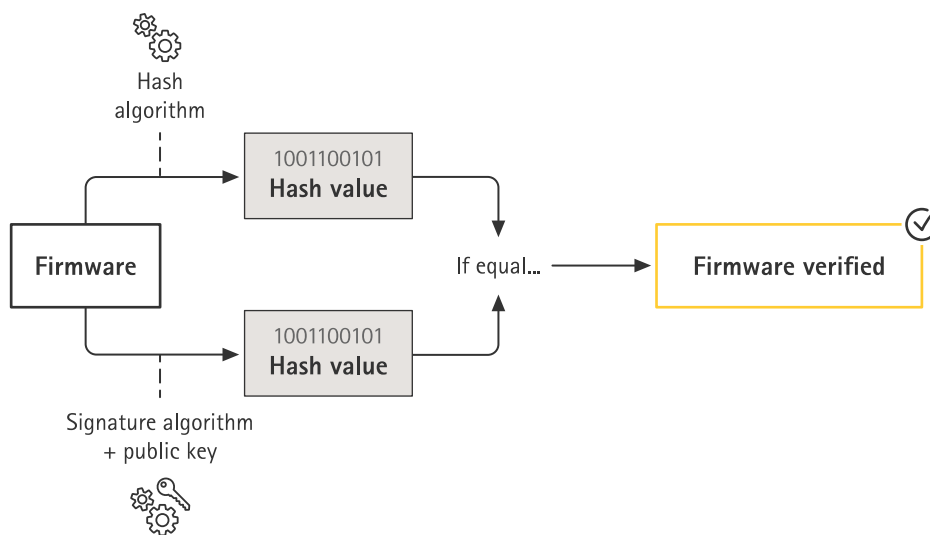


Figure 15. Processus de vérification du firmware signé.

La signature de firmware Axis repose sur la méthode reconnue de chiffrement à clé publique RSA. 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 toute l'image du firmware est assurée par une signature du contenu de l'image. Une signature principale permet de vérifier plusieurs signatures secondaires, qui sont vérifiées lorsque l'image est décompressée.

Pour des tests ou des configurations personnalisées du firmware, Axis a mis en œuvre un mécanisme qui approuve des périphériques individuels pour accepter le firmware hors production. Ce firmware est signé de façon différente, avec l'approbation du propriétaire et d'Axis, et génère un certificat de firmware personnalisé. Lorsqu'il est installé dans le périphérique approuvé, le certificat permet l'utilisation d'un

firmware personnalisé exécutable uniquement sur ce périphérique, déterminé par son numéro de série unique et son ID processeur. Seul Axis peut créer des certificats de firmware personnalisé, car Axis possède la clé pour les signer.

## 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 firmware 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.

**Firmware signé :** firmware qui a été signé numériquement par une partie de confiance. Le périphérique Axis vérifie l'authenticité de l'image du firmware avant de réaliser une mise à jour du firmware. Le firmware signé est une exigence du processus de démarrage sécurisé.

**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 confirme 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 trouvent 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 un 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.