LIVRE BLANC

# Caractéristiques de cybersécurité des produits Axis

— firmware signé

— Amorçage sécurisé

— Axis Edge Vault

— Identifiant de périphérique Axis

— Vidéo signée

Novembre 2021

AXIS COMMUNICATIONS

# Table des matières

# 1 Avant-propos

Ce document décrit certaines fonctions disponibles dans les produits Axis pour atténuer les cybermenaces et contrer certains types d'attaques. Les fonctions sont les suivantes :

- firmware signé
- amorçage sécurisé
- Axis Edge Vault
- identifiant du périphérique Axis
- vidéo signée.

Les menaces décrites sont les suivantes :

- sabotage du firmware
- sabotage de la chaîne d'approvisionnement
- extraction de clés privées
- remplacement non autorisé de dispositif
- modification de la vidéo.

## 1.1 Firmware signé

La signature de firmware est mise en œuvre par l'éditeur du logiciel, qui signe l'image du firmware avec une clé privée. Lorsque cette signature est associée à un firmware, le dispositif 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.

## 1.2 Démarrage sécurisé

L'amorçage sécurisé est un processus d'amorçage constitué d'une chaîne ininterrompue de logiciels validés par cryptographie, commençant dans la mémoire immuable (ROM d'amorçage). Comme il repose sur l'utilisation d'un firmware signé, l'amorçage sécurisé garantit qu'un dispositif ne peut démarrer qu'avec le firmware autorisé.

## 1.3 Axis Edge Vault

Axis Edge Vault est un module sécurisé de calcul cryptographique utilisable pour les opérations cryptographiques sur des certificats stockés de manière sécurisée. Edge Vault assure un stockage protégé des falsifications assurant la protection des secrets de chaque dispositif. Il forme un socle sécurisé pour la mise en œuvre de fonctions de sécurité plus évoluées.

## 1.4 Identifiant de périphérique Axis

l'identifiant de périphérique Axis est comparable à un passeport numérique, unique pour chaque dispositif. Il est stocké de manière sécurisée et permanente dans Edge Vault sous forme de certificat signé par le

certificat racine Axis. L'identifiant de périphérique Axis est conçu pour prouver l'origine du dispositif, offrant un niveau de fiabilité renforcé du dispositif tout au long du cycle de vie du produit.

### 1.5 Vidéo signée

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 son identifiant de périphérique Axis unique, stocké en toute sécurité dans Axis Edge Vault, pour ajouter une signature au flux vidéo. À la lecture, le lecteur vidéo indique si la vidéo est intacte. La signature vidéo permet donc de remonter la vidéo jusqu'à la caméra d'origine et de vérifier qu'elle n'a pas été modifiée après avoir quitté la caméra.

# 2 Glossaire

**Certificat** : en cryptographie, un certificat est un document signé attestant de l'origine et des propriétés d'une paire de clés. Le certificat est signé par une autorité de certification (AC). Si le système fait confiance à l'autorité de certification, il fait également confiance aux certificats qu'elle délivre.

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

**FIPS** : Federal Information Processing Standards, normes de chiffrement et de sécurité des données, publiées aux États-Unis par le NIST (National Institute of Standards and Technology).

**ROM immuable** : permet de stocker de manière sécurisée les clés publiques de confiance et le programme utilisés pour comparer les signatures afin qu'elles ne puissent pas être remplacées.

**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.

**TLS** : Transport Layer Security, norme Internet de protection du trafic réseau. TLS représente le S (de sécurisé) dans HTTPS.

# 3 Introduction

Axis applique les bonnes pratiques de gestion et de réponse aux failles de sécurité dans ses produits afin de réduire l'exposition de ses clients aux cyber-risques. Il n'existe cependant aucun moyen de garantir que les produits et les services sont exempts de défauts exploitables pour mener des attaques malveillantes. Cela n'est pas spécifique à Axis, il s'agit plutôt d'une situation générale pour tous les dispositifs réseau. En revanche, Axis peut garantir qu'il déploie toujours des efforts concertés à chaque étape afin de s'assurer que vos dispositifs et services Axis présentent le plus faible risque possible.

Pour en savoir plus sur la sécurité des produits et les vulnérabilités détectées, consultez la page *www.axis.com/support/product-security*. Sur cette page, vous pouvez également télécharger le Guide de protection Axis, qui détaille les mesures à prendre pour réduire le risque des menaces courantes.

Ce livre blanc présente des cyberattaques plausibles et les méthodes pour les éviter dans les produits Axis. Il décrit en particulier la façon dont les fonctions de firmware signé et d'amorçage sécurisé peuvent empêcher le sabotage du firmware et de la chaîne d'approvisionnement. Nous abordons également l'utilisation d'un module TPM (Trusted Platform Module) et d'Axis Edge Vault, tous deux utilisables pour sécuriser les clés privées. Axis Edge Vault sert à stocker en toute sécurité l'identifiant de périphérique Axis pour renforcer son degré de fiabilité. Axis Edge Vault et l'ID de périphérique Axis permettent également d'utiliser la signature de vidéo, qui sert à vérifier que la vidéo n'a pas été modifiée après avoir quitté la caméra.

# 4 Détection de sabotage du firmware

Si ses tentatives précédentes d'effraction du système ont échoué, un cybercriminel peut exploiter un autre vecteur d'attaque : pousser le propriétaire du système à installer des applications, un firmware ou d'autres modules logiciels modifiés. Le logiciel modifié peut contenir un code malveillant ayant un but précis. Il est généralement recommandé de ne jamais installer de logiciel provenant d'une source en laquelle vous n'avez pas totalement confiance. Dans le cadre d'un système vidéo, un « intermédiaire » pourrait modifier le firmware d'un dispositif et inciter les utilisateurs finaux à l'installer. Il ne s'agit pas d'une tâche facile et l'adversaire doit être très qualifié et déterminé. Il doit connaître parfaitement la conception du firmware Axis et la manière dont il fonctionne sur un dispositif. Pourtant, ce type de cybercriminel peut exister si l'attaque d'un système présente un intérêt suffisamment fort. La contre-mesure habituelle pour l'éditeur de logiciel consiste à utiliser un firmware signé.

## 4.1 Signature du firmware

Le firmware signé est mis en œuvre par l'éditeur du logiciel, qui signe l'image du firmware avec une clé privée tenue secrète. Lorsque cette signature est associée à un firmware, le dispositif 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.

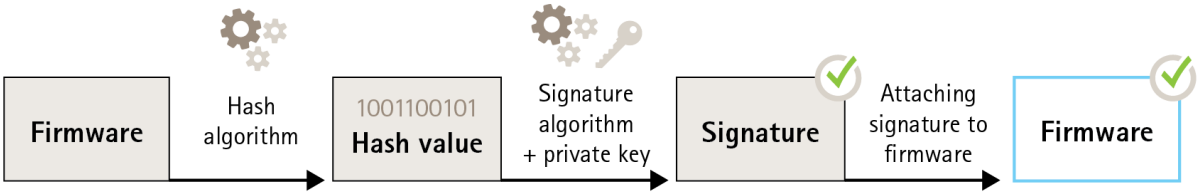


*Figure 1. Processus de signature du firmware.*

Avant une mise à niveau du firmware, le nouveau firmware doit être vérifié. Pour garantir que le nouveau firmware n'est pas modifié, 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.

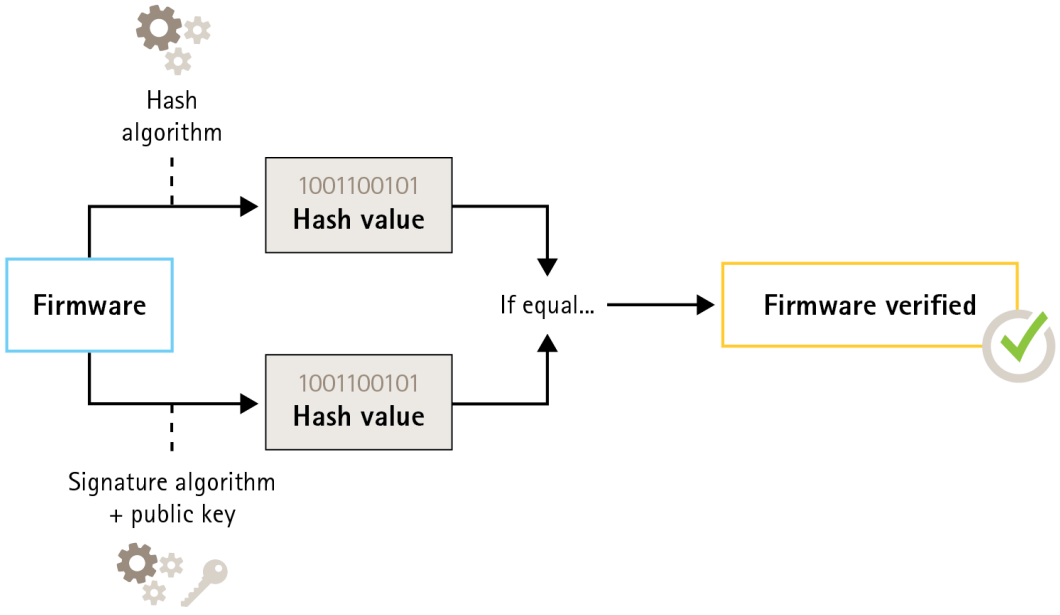


*Figure 2. Processus de vérification du firmware signé.*

## 4.2 Signature de firmware chez Axis

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 un certain nombre de signatures secondaires, qui sont vérifiées lorsque l'image est décompressée.

# 5 Prévention du sabotage de la chaîne d'approvisionnement

La signature du firmware protège un dispositif, lors de toutes les mises à jour futures du firmware, contre l'installation d'un firmware compromis. Mais qu'arrive-t-il si un intermédiaire modifie le dispositif lors de son acheminement entre le fournisseur et l'utilisateur final ? Un cybercriminel qui peut accéder physiquement au dispositif pendant son transport peut mener une attaque, par exemple en piratant la partition d'amorçage du dispositif pour contourner le contrôle d'intégrité du firmware et installer un firmware malveillant modifié avant le déploiement du dispositif.

## 5.1 Démarrage sécurisé

L'amorçage sécurisé est un processus d'amorçage constitué d'une chaîne ininterrompue de logiciels validés par cryptographie, commençant dans la mémoire immuable (ROM d'amorçage). Comme il repose sur l'utilisation d'un firmware signé, l'amorçage sécurisé garantit qu'un dispositif ne peut démarrer qu'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 d'amorçage sert de racine de confiance et le processus d'amorçage 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.

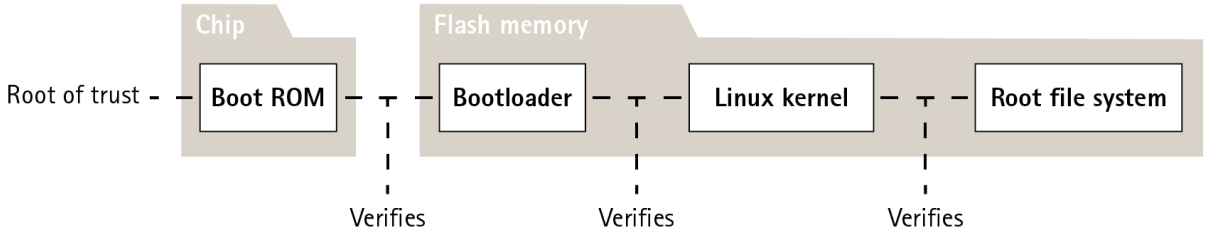


*Figure 3. Processus d'amorçage sécurisé.*

## 5.2 Amorçage sécurisé Axis

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. L'amorçage sécurisé garantit que le dispositif Axis est complètement exempt d'éventuels logiciels malveillants après une remise en paramètres d'usine.

### 5.3 Amorçage sécurisé et certificats de firmware personnalisés

L'amorçage sécurisé rend le produit plus sûr, mais il manque de souplesse avec d'autres firmwares. Le chargement d'un firmware Axis provisoire, de test, personnalisé ou autre dans le produit est plus compliqué. C'est pourquoi Axis a mis en place un mécanisme qui habilite des dispositifs individuels à accepter ce genre de 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 dispositif approuvé, le certificat permet d'utiliser un firmware personnalisé exécutable uniquement sur ce dispositif, 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 Secrets protégés des falsifications

Une condition de base pour un système distribué sécurisé est la capacité de vérifier les connexions et d'éviter les interceptions. Chaque dispositif doit donc protéger ses secrets par un stockage sécurisé, protégé des falsifications. Axis Edge Vault fournit ce type de stockage et permet de mettre en œuvre des fonctions de sécurité plus évoluées sur cette base.

### 6.1 ID de dispositif Axis

Pendant la production de chaque dispositif réseau Axis, un « passeport numérique », appelé ID de dispositif Axis, est installé de manière sécurisée dans Axis Edge Vault au sein du dispositif. Cet identifiant est unique pour chaque dispositif. Il est conçu pour prouver l'origine du dispositif. L'identifiant de périphérique Axis est un ensemble de certificats utilisés dans la partie des opérations cryptographiques du module pour signer les demandes présentées à Edge Vault par le firmware intégré du dispositif. La réponse à cette opération est renvoyée au destinataire qui peut utiliser des clés publiques Axis pour valider l'authentification de la réponse.

Un certificat est un petit élément de données associant une clé publique et des métadonnées décrivant la clé ainsi qu'une signature provenant de l'émetteur, attestant de la validité du certificat. Une hiérarchie de certification est un moyen de prouver la provenance du certificat.

Établissons un parallèle entre l'identifiant de périphérique Axis et un passeport. Si vous détenez un passeport, le gouvernement de votre pays garantit que vous êtes bien la personne indiquée sur le passeport. De la même manière, tous les certificats de l'identifiant de périphérique Axis sont approuvés par un certificat d'AC racine d'identifiant de périphérique. De la même façon qu'un agent des douanes fait confiance au gouvernement de votre pays pour avoir correctement délivré votre passeport, un système de

sécurité de réseau fait confiance au certificat d'AC racine d'identifiant de périphérique Axis pour avoir correctement vérifié le certificat Axis d'un dispositif connecté au réseau.

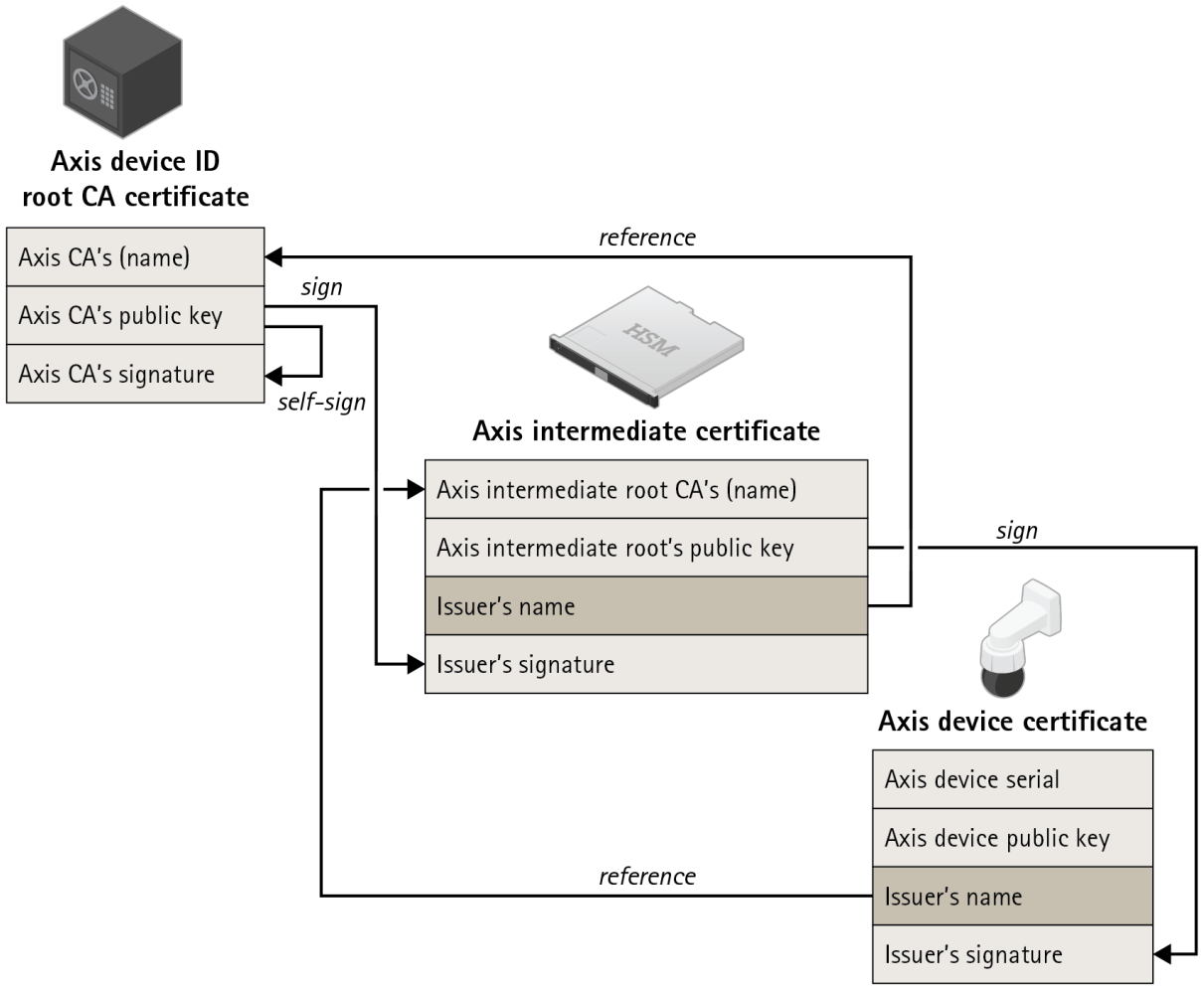


*Figure 4. L'identifiant de périphérique Axis, qui est un certificat intégrant le numéro de série du produit, est signé par un certificat intermédiaire qui a été signé par le certificat racine Axis. Vu que le certificat racine Axis est très précieux et qu'il doit être stocké dans un coffre-fort, le certificat intermédiaire est nécessaire pendant le provisionnement en usine.*

# 7 Stockage sécurisé des clés

Les dispositifs Axis prennent en charge les protocoles HTTPS (chiffrement réseau) et 802.1X (contrôle d'accès au réseau), qui utilisent tous les deux le protocole TLS (Transport Layer Security). Les certificats numériques de TLS utilisent une paire de clés publique/privée. La clé privée est stockée dans le dispositif, tandis que la clé publique est incluse dans le certificat. Notons que si ni HTTPS, ni 802.1X ne sont utilisés, il n'y a aucune clé à protéger.

Un pirate pourrait essayer d'extraire la clé privée et le certificat du dispositif et les installer sur un ordinateur d'attaque. Dans le cas d'HTTPS, cette clé privée pourrait servir à écouter le trafic réseau entre le dispositif et le logiciel VMS. De même, si l'ordinateur d'attaque usurpe le réseau en prétendant être un

dispositif légitime, il pourrait accéder au logiciel VMS. Dans le cas de 802.1X, l'adversaire pourrait utiliser la clé privée pour accéder à un réseau protégé par 802.1X, en se faisant passer pour un dispositif de confiance.

Les certificats et les clés privées sont généralement stockés dans le système de fichiers d'un dispositif, protégés par la stratégie d'accès du compte et utilisés dans l'environnement informatique normal. Dans la plupart des cas, ces précautions suffisent car le compte ne peut pas être facilement compromis. Notons que les certificats peuvent être révoqués s'ils sont suspectés d'être compromis, rendant la clé privée inutilisable.

Certains utilisateurs finaux de systèmes critiques peuvent être exposés à un risque accru, où des cybercriminels déterminés et compétents essaient de forcer le dispositif pour en extraire la clé privée. Axis Edge Vault peut servir à stocker la clé de sorte qu'il est pratiquement impossible de l'extraire, même lorsque le dispositif est compromis.

## 7.1 Stockage sécurisé des certificats avec Axis Edge Vault

Axis Edge Vault est un module de calcul cryptographique sécurisé, sous la forme d'une puce montée sur la carte électronique du produit. Edge Vault peut stocker des certificats de manière sécurisée et servir à des opérations cryptographiques sur des certificats stockés de manière sécurisée.

Les certificats stockés dans Edge Vault n'ont pas besoin de quitter cet emplacement pour être utilisés par le dispositif. Ils restent de manière sécurisée dans Edge Vault même lorsqu'ils sont utilisés, car le matériel cryptographique qui intervient sur la clé est installé sur la même puce physique.

## 7.2 Stockage de clé sécurisé avec un module TPM

Un TPM est un composant qui procure un ensemble de fonctions cryptographiques adaptées à la protection des informations contre les accès non autorisés. La clé privée est stockée dans le TPM et ne le quitte jamais. Toutes les opérations cryptographiques nécessitant l'utilisation de la clé privée sont envoyées au TPM pour traitement. Cela garantit que la partie secrète du certificat ne quitte jamais l'environnement sécurisé au sein du TPM et reste sécurisée même en cas de faille de sécurité.

## 7.3 Certification FIPS 140-2

Pour certains produits et scénarios d'utilisation, l'utilisation d'un module TPM peut être une obligation légale pour protéger les informations, parfois conjuguée à une exigence de conformité FIPS 140-2. FIPS (Federal Information Processing Standard) 140-2 est une norme de sécurité informatique pour les modules cryptographiques, publiée aux États-Unis par le NIST (National Institute of Standards and Technology).

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 cryptographique, des algorithmes approuvés, des modes de fonctionnement approuvés et des tests de mise sous tension.

Pour en savoir plus sur les conditions de certification FIPS 140-2, rendez-vous sur le site web du NIST à l'adresse *www.nist.gov*

### 7.3.1 TPM certifié dans les produits Axis

Le module TPM utilisé dans certains produits Axis est certifié FIPS 140-2. Plus précisément, il est certifié au niveau de sécurité 2 de la norme, c'est-à-dire que le module TPM satisfait également les critères relatifs entre autres aux autorisations basées sur les rôles et aux preuves de sabotage.

# 8 IEEE 802.1AR - vérification de dispositif avec l'identifiant de périphérique Axis

Une personne qui achète un dispositif réseau Axis peut effectuer un examen manuel avant de commencer à l'utiliser. En inspectant visuellement le produit et avec une connaissance préalable de l'apparence des produits Axis, le client peut être convaincu que le produit provient vraiment d'Axis. Cependant, ce type d'inspection ne peut être effectué que par une personne ayant un accès physique au produit. Par conséquent, lorsque vous communiquez avec un produit non provisionné sur un réseau, comment pouvez-vous être sûr de communiquer avec le bon ? Que le dispositif n'a pas été remplacé sans autorisation ? Aucun équipement réseau ou logiciel sur serveur ne peut effectuer une inspection physique. Par mesure de sécurité, il est courant d'interagir avec un nouveau produit d'abord sur un réseau fermé, permettant de provisionner le dispositif de manière sécurisée.

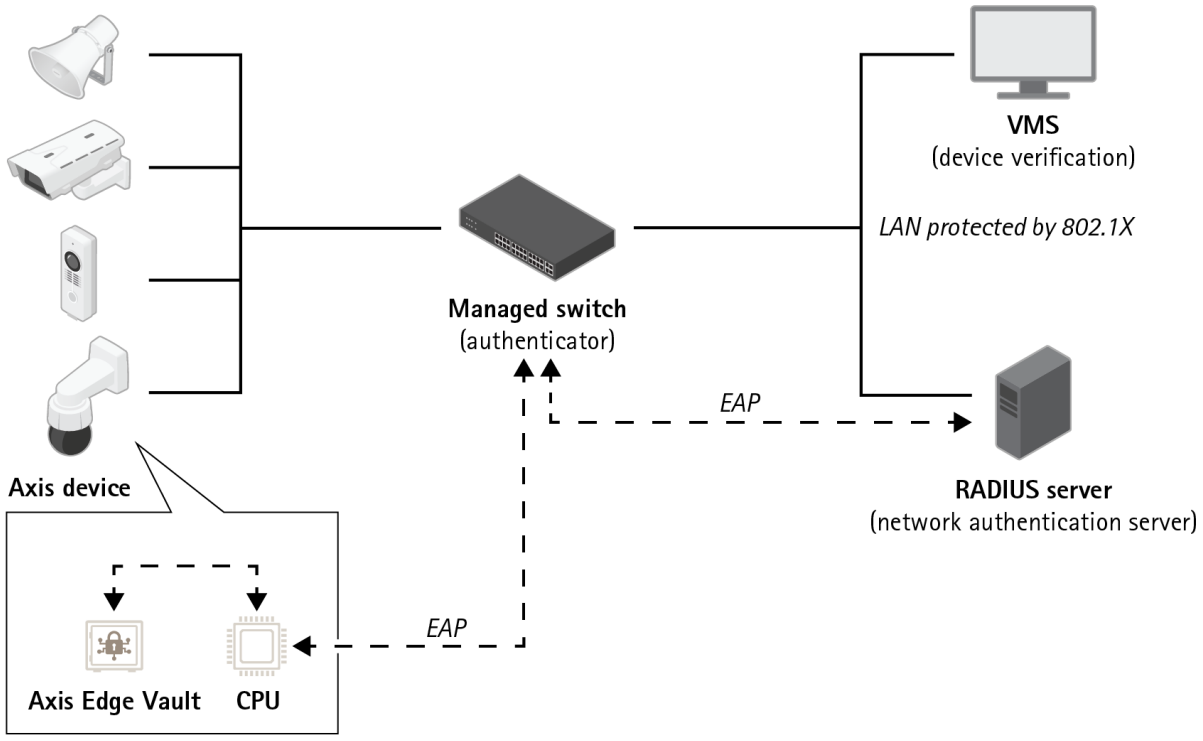


*Figure 5. Les clients peuvent demander à leur serveur d'authentification d'accepter automatiquement sur le réseau les produits Axis achetés, à l'aide des numéros de série des dispositifs et de l'identifiant de périphérique Axis.*

La nouvelle norme internationale IEEE 802.1AR (*https://1.ieee802.org/security/802-1ar/*) définit une méthode d'automatisation et de sécurisation de l'identification d'un dispositif sur un réseau. Si la

communication est transmise à un module sécurisé intégré, le dispositif peut renvoyer une réponse d'identification de confiance conformément à la norme.

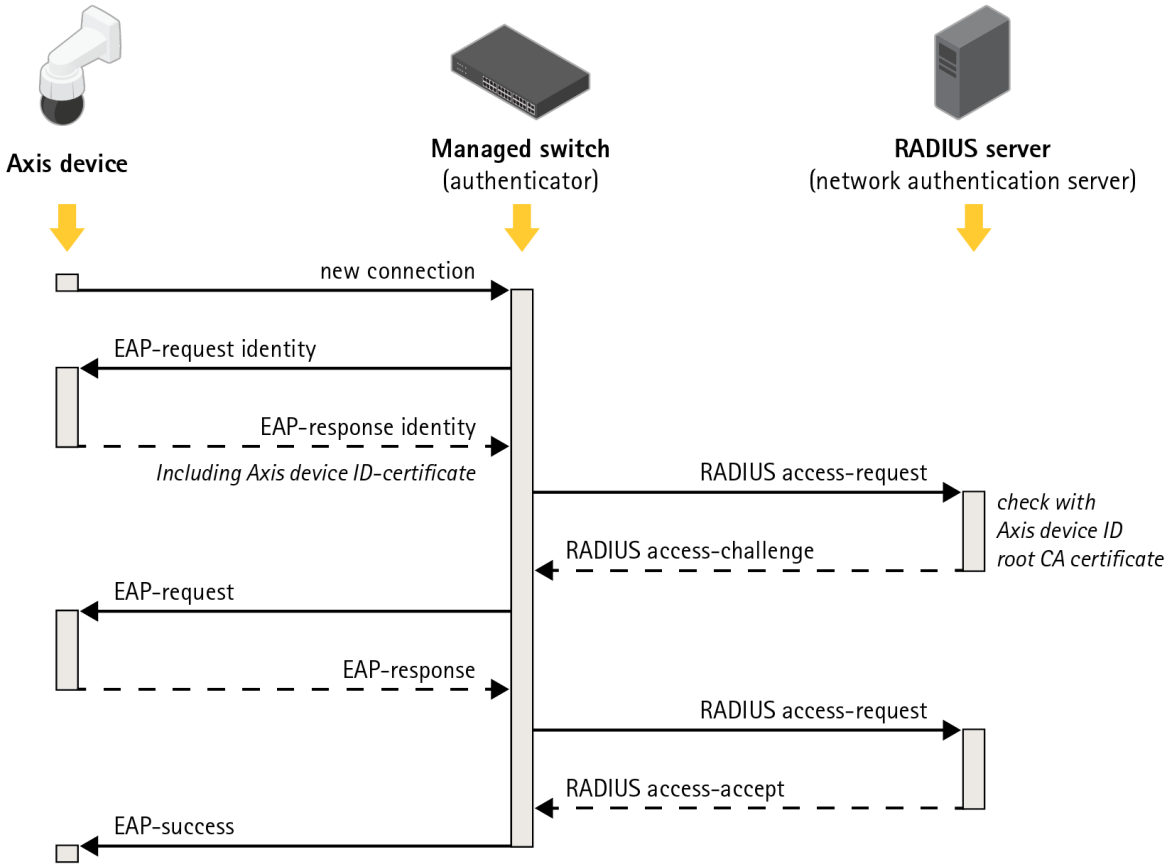


*Figure 6. IEEE 802.1AR définit une méthode d'identification d'un dispositif sur un réseau en suivant un protocole qui envoie des requêtes EAP (Extensible Authentication Protocol) au commutateur qui utilise des requêtes RADIUS (Remote Authentication Dial-In User Service) pour autoriser l'accès.*

Dans les produits Axis, ces mesures de sécurité sont mises en œuvre au travers d'Axis Edge Vault et de l'identifiant de périphérique Axis. Axis Edge Vault est un module sécurisé dans lequel est installé l'identifiant de périphérique Axis, un ensemble de certificats permettant de vérifier l'identifiant du dispositif. Ces fonctions fournissent à votre réseau des preuves vérifiables par cryptographie qu'un dispositif donné a été produit par Axis et que la connexion réseau au dispositif est effectivement assurée par ce dispositif.

Un dispositif avec un identifiant de périphérique Axis a été provisionné en usine (avec des clés et des certificats). Ce provisionnement peut être utilisé ultérieurement par un client pour provisionner à nouveau le dispositif sur le terrain avec d'autres clés et/ou certificats lui permettant d'accéder à certaines ressources réseau du client.

En identifiant le dispositif avec l'identifiant de périphérique Axis, il est possible de réduire les délais de déploiement des dispositifs, car les dispositifs nécessitent moins de travail avant de les installer et de les configurer sur le réseau prévu. Un autre avantage est que l'identifiant de périphérique Axis,

indépendamment de fournir une source de confiance intégrée supplémentaire, procure également un moyen de suivre les dispositifs dans un grand système.

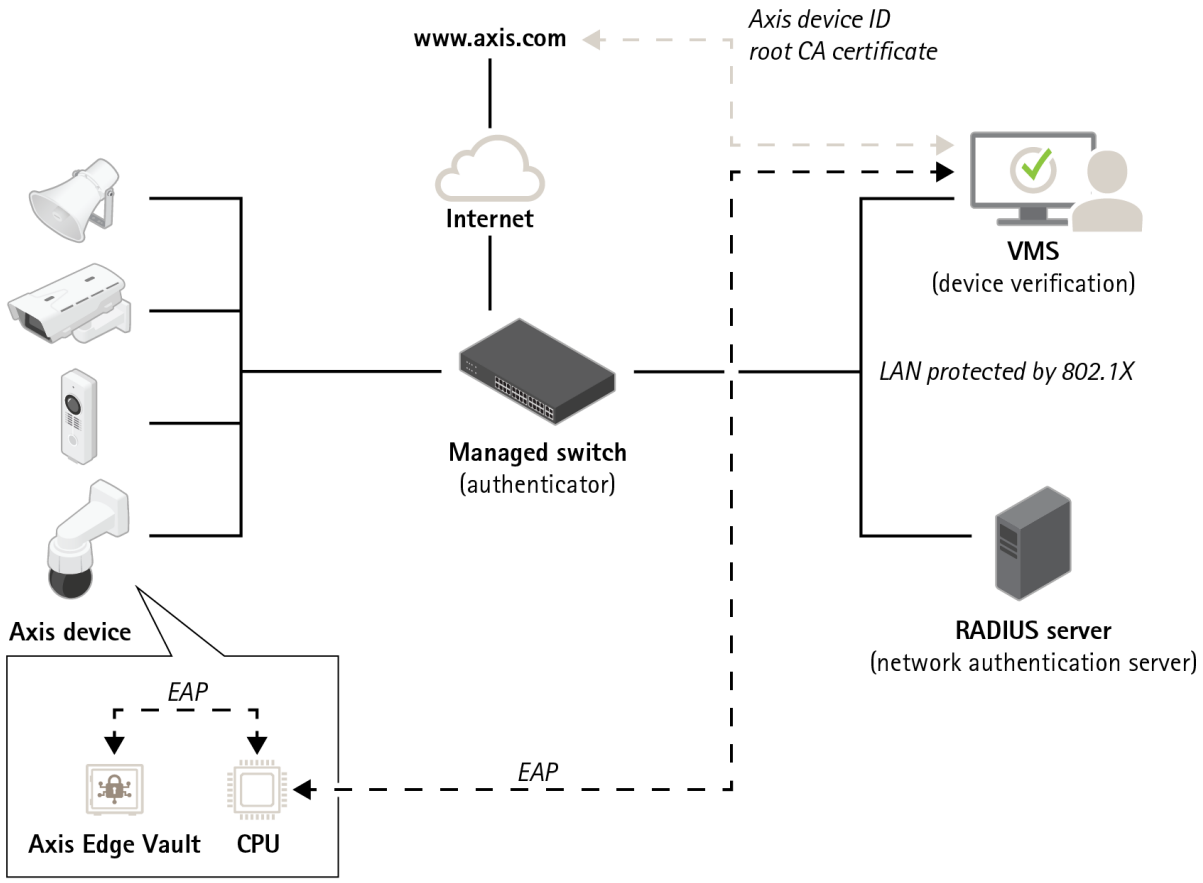


*Figure 7. Les applications logicielles dans d'autres parties du système peuvent utiliser l'identifiant de périphérique Axis et les opérations cryptographiques pour vérifier avec qui la communication est effectuée. L'identifiant de périphérique Axis a été vérifié par le certificat d'AC racine d'identifiant de périphérique Axis public sur axis.com.*

# 9 Détection des modifications à la vidéo

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.

## 9.1 Vidéo signée

Avec la fonction Axis de signature de vidéo, 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 extraire 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.

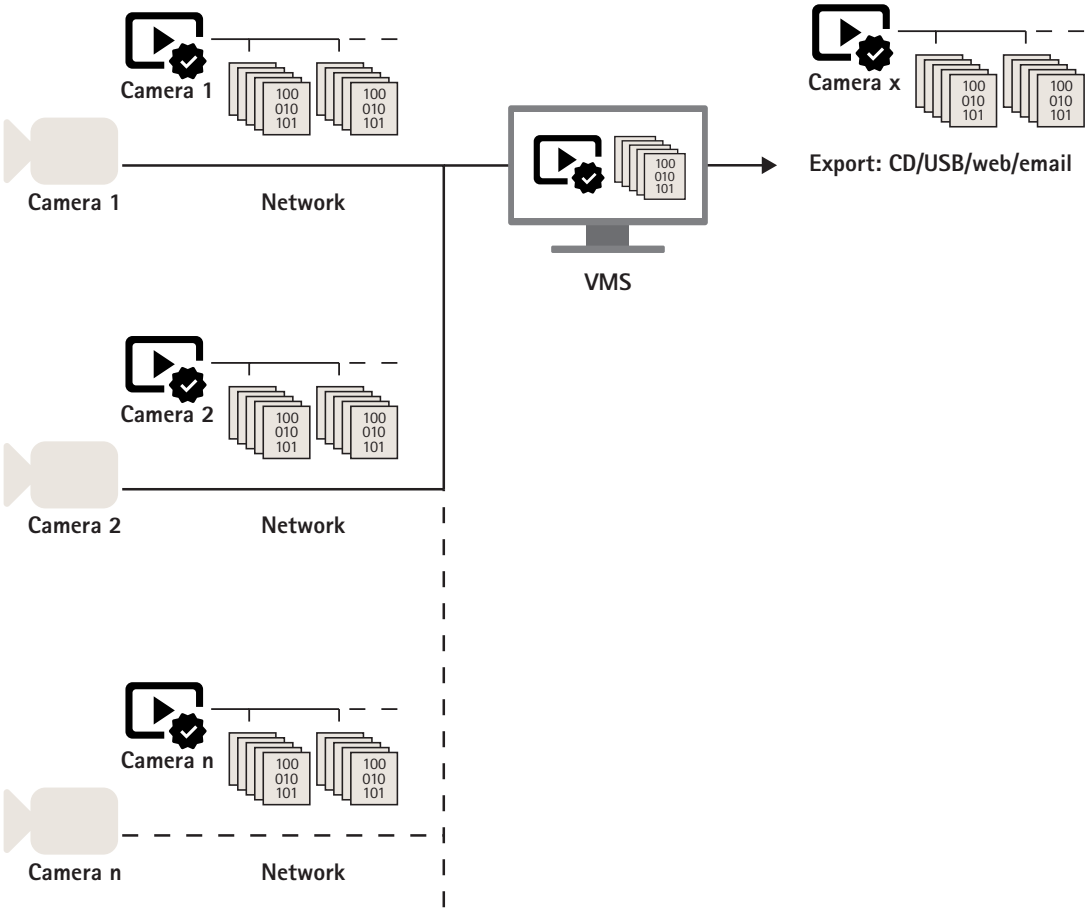


*Figure 8. Comme la signature est ajoutée au niveau de la caméra, il est possible de vérifier le contenu à chaque étape, de la source à l'usage final de la vidéo.*

Chaque caméra utilise son identifiant de périphérique unique dans Axis Edge Vault pour ajouter une signature au 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 dans Edge Vault. La signature est ensuite stockée dans des champs de métadonnées dédiés du flux vidéo (en-tête SEI).

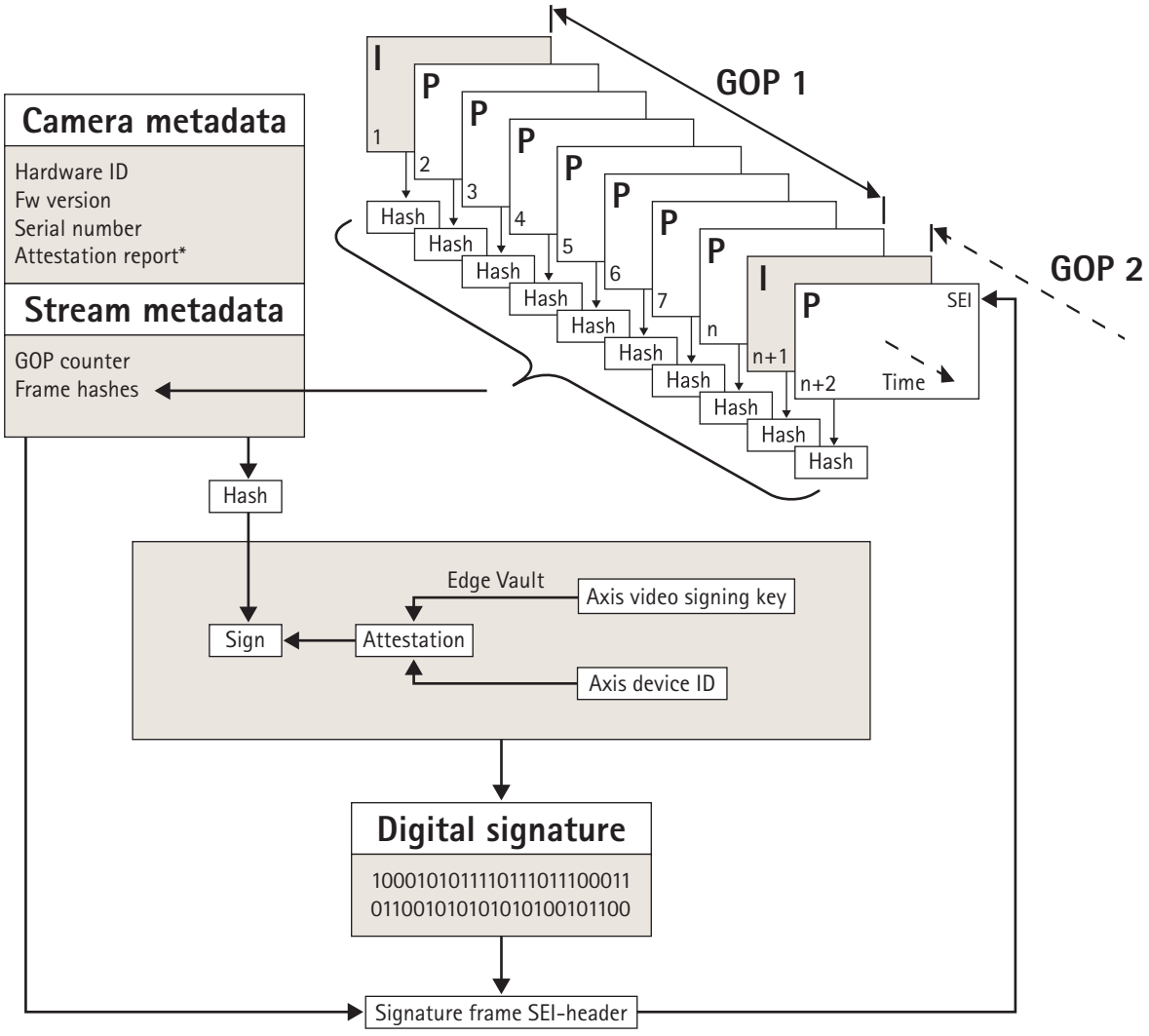


*Figure 9. Représentation graphique de l'ajout d'une signature aux métadonnées de la vidéo. Le contenu de chaque image d'un groupe d'images (GOP) fait l'objet d'un hachage, en parallèle au hachage des métadonnées de la caméra et des métadonnées du flux. Il en résulte le hachage du GOP, qui est signé 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 en elle-même est réalisée à l'aide d'une clé de signature vidéo propre au dispositif, qui est attestée par l'identifiant de périphérique Axis exclusif au dispositif. Le rapport d'attestation est joint au flux dès le départ, puis ensuite à intervalles réguliers, en général une fois par heure. 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 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. Les événements peu probables de perte d'image dans la transmission du flux ou d'endommagement du contenu pendant l'enregistrement seront signalés de la même manière.

T10154694/FR/M3.2/2111

# À propos d'Axis Communications

En concevant des solutions réseau qui améliorent la sécurité et permettent le développement de nouvelles façons de travailler, Axis contribue à un monde plus sûr et plus clairvoyant. Leader technologique de la vidéo sur IP, Axis propose des produits et services axés sur la vidéosurveillance, l'analyse vidéo, le contrôle d'accès, l'interphonie et les systèmes audio. Axis emploie plus de 3 800 personnes dans plus de 50 pays et collabore avec des partenaires du monde entier pour fournir des solutions clients adaptées. Axis a été fondée en 1984 et elle a son siège à Lund, en Suède.

Pour plus d'informations sur Axis, rendez-vous sur notre site Web *axis.com*.