Firmware signé, démarrage sécurisé et sécurité des clés privées

Caractéristiques de cybersécurité des produits Axis

Juillet 2020

AXIS COMMUNICATIONS

Table des matières

1 Résumé

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
- démarrage sécurisé
- module de plateforme sécurisée (TPM)
- Axis Edge Vault avec identifiant de périphérique Axis.

Les menaces décrites sont les suivantes :

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

1.1 Firmware signé

Le firmware signé est mis en œuvre par le fournisseur du logiciel, qui signe l'image du firmware avec une clé privée. Lorsque cette signature est associée à un firmware, le périphérique valide le firmware avant d'accepter de l'installer. Si le périphérique détecte que l'intégrité du firmware est compromise, la mise à niveau du firmware est rejetée.

1.2 Démarrage sécurisé

Le 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). Basé sur l'utilisation d'un firmware signé, le démarrage sécurisé garantit qu'un périphérique ne peut démarrer qu'avec le firmware autorisé.

1.3 TPM

Un TPM est un composant qui procure un ensemble de fonctions cryptographiques adaptées à la protection des informations contre les accès non autorisés. Les clés privées sont stockées dans le TPM et 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 reste sécurisée même en cas de faille de sécurité. Le TPM utilisé dans certains produits Axis est certifié pour répondre aux exigences de la norme FIPS 140-2.

1.4 Axis Edge Vault avec identifiant de périphérique Axis

La nouvelle norme internationale IEEE 802.1AR décrit une procédure d'automatisation et de sécurisation de l'identification d'un périphérique sur un réseau. Sur les produits Axis, ces mesures de sécurité sont mises en œuvre via Axis Edge Vault et l'identifiant de périphérique Axis. Edge Vault peut être utilisé pour des problèmes cryptographiques sur des certificats stockés de manière sécurisée. La partie privée des certificats reste dans Edge Vault même lorsqu'elle est utilisée. L'identifiant de périphérique Axis est stocké de manière

sécurisée et permanente dans Edge Vault en tant que certificat signé par le certificat racine Axis, ce qui accroît le niveau de confiance du périphérique tout au long du cycle de vie du produit.

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 (CA). Si le système fait confiance à l'autorité de certification, 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.

FIPS : Federal Information Processing Standards, normes de cryptage et de sécurité des données, émises 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 périphérique pour le réseau. Cela implique l'envoi de données de configuration et de paramètres de stratégie au périphérique à partir d'un point central. Le périphérique est fourni avec des clés et des certificats.

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

TLS : Transport Layer Security (sécurité de la couche de transport), norme Internet assurant la protection du trafic sur le réseau. TLS fournit le S (pour « sécurisé ») de HTTPS.

3 Présentation

Axis respecte les meilleures pratiques du secteur en matière 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 aucun moyen de garantir que les produits et les services sont exempts de défauts pouvant être exploités pour mener des attaques malveillantes. Cela n'est pas spécifique à Axis, il s'agit plutôt d'une situation générale pour tous les périphériques réseau. Axis garantit de toujours faire un effort concerté à chaque étape possible afin de s'assurer que le moins de risques possibles sont associés à vos périphériques et à vos services Axis.

Pour plus d'informations sur la sécurité des produits et les vulnérabilités découvertes, consultez *www.axis.com/support/product-security*. Pour plus d'informations sur les mesures que vous pouvez prendre afin de réduire les risques de menaces courantes, téléchargez le guide de renforcement de la sécurité Axis sur *www.axis.com/cybersecurity*.

Ce livre blanc présente des cyberattaques plausibles et la façon dont elles peuvent être évitées dans les produits Axis. Il décrit en particulier la façon dont les fonctions de firmware signé et de démarrage sécurisé peuvent empêcher le sabotage du firmware et le sabotage de la chaîne d'approvisionnement. Nous abordons également l'utilisation d'un module de plateforme sécurisée (TPM) et d'Axis Edge Vault, qui peuvent tous les deux être utilisés pour sécuriser les clés privées. Axis Edge Vault sert à stocker de manière sécurisée l'identifiant de périphérique Axis, ce qui accroît le niveau de confiance du périphérique.

4 Détection de sabotage du firmware

Un vecteur d'attaque pouvant être exploité par un adversaire ayant échoué dans d'autres tentatives de violation du système consiste à faire installer, par le propriétaire du système, 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 périphérique 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 disposer d'une compréhension extrêmement détaillée de la conception du firmware Axis et de la manière dont le firmware fonctionne sur un périphérique. Pourtant, ces adversaires peuvent exister si l'attaque d'un système présente un intérêt suffisamment fort. La contre-mesure habituelle pour le fournisseur de logiciel consiste à utiliser un firmware signé.

4.1 Signature du firmware

Le firmware signé est mis en œuvre par le fournisseur du logiciel, qui signe l'image du firmware avec une clé privée tenue secrète. Lorsque cette signature est associée à un firmware, le périphérique valide le firmware avant d'accepter de l'installer. Si le périphérique 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.

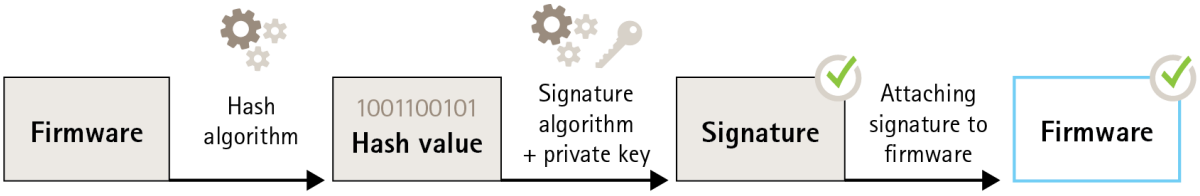

Figure 1. Processus de signature du firmware.

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.

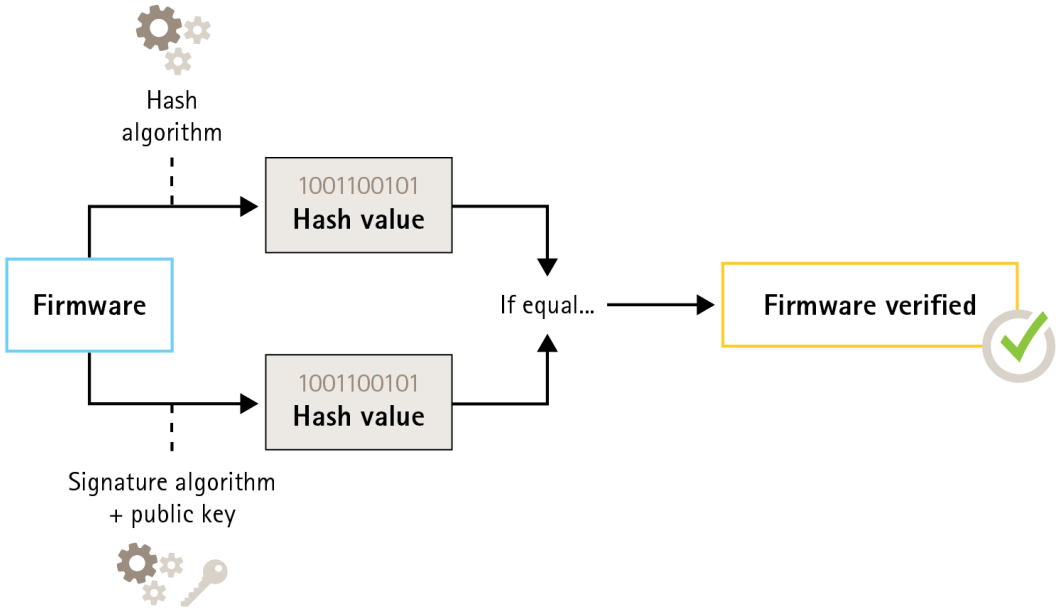

Figure 2. Processus de vérification du firmware signé.

4.2 Firmware signé chez Axis

Le firmware signé AXIS est basé sur la méthode de cryptage RSA à clé publique reconnue par le secteur. La clé privée est stockée dans un emplacement étroitement protégé par Axis, tandis que la clé publique

est intégrée aux périphériques Axis. L'intégrité de la totalité de 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 périphérique, 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 périphérique lors de son acheminement entre le fournisseur et l'utilisateur final ? Un adversaire disposant d'un accès physique au périphérique pendant le transit peut mener une attaque, notamment compromettre la partition de démarrage du périphérique, contourner le contrôle d'intégrité du firmware afin d'installer un firmware malveillant modifié avant le déploiement du périphérique.

5.1 Démarrage sécurisé

Le 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). Basé sur l'utilisation d'un firmware signé, le démarrage sécurisé garantit qu'un périphérique ne peut démarrer qu'avec le firmware autorisé.

Le processus de démarrage est lancé par la ROM de démarrage qui valide le chargeur de démarrage. Le démarrage 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.

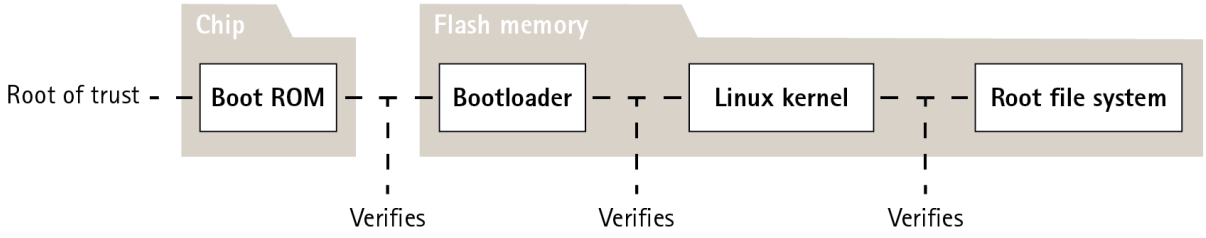

Figure 3. Processus de démarrage sécurisé.

5.2 Démarrage sécurisé Axis

Dans de nombreux périphériques, il est important que les fonctionnalités de bas niveau soient impossibles à modifier. Si d'autres mécanismes de sécurité sont créés sur le logiciel de niveau inférieur, le démarrage sécurisé sert de couche de base sécurisée qui protège ces mécanismes contre les contournements.

Sur un périphérique avec un démarrage 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 que le périphérique Axis est complètement exempt d'éventuels logiciels malveillants après une remise en paramètres d'usine.

5.3 Démarrage sécurisé et certificats de firmware personnalisés

Bien que le démarrage sécurisé rende le produit plus sûr, il réduit également la flexibilité avec différents firmwares, ce qui complique le chargement de tout firmware temporaire, comme le firmware de test ou tout autre firmware personnalisé d'Axis, dans le produit. Cependant, AXIS a mis en place un système qui permet aux unités individuelles d'accepter ce firmware non productif. 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 les unités approuvées, le certificat permet d'utiliser un firmware personnalisé qui ne peut être exécuté que sur l'unité approuvée, en fonction de son numéro de série et de sa puce ID uniques. Les certificats de firmware personnalisés peuvent être créés uniquement par Axis, car Axis détient la clé pour les signer.

6 Sécurité des clés privées

Les périphériques Axis prennent en charge les protocoles HTTPS (cryptage de 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 périphérique, tandis que la clé publique est incluse dans le certificat. Veuillez noter que si ni HTTPS ni 802.1X ne sont utilisés, il n'y a aucune clé à protéger.

Un adversaire pourrait essayer d'extraire la clé privée et le certificat du périphérique et de les installer sur un ordinateur attaquant. Dans le cas de HTTPS, cette clé privée pourrait être utilisée pour espionner le trafic crypté sur le réseau entre le périphérique et le VMS. Ou en cas d'usurpation du réseau, l'ordinateur attaquant pourrait accéder au VMS en se faisant passer pour un périphérique légitime. 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 périphérique de confiance.

Les certificats et les clés privées sont généralement stockés dans le système de fichiers d'un périphérique, protégés par la stratégie d'accès du compte et utilisés dans l'environnement informatique normal. Dans la plupart des cas, cela est suffisant car le compte ne peut pas être facilement compromis. Veuillez noter 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 présenter un risque accru d'adversaires déterminés et compétents qui essaient de faire effraction dans le périphérique pour extraire la clé privée. Un module de plateforme sécurisée (TPM) stocke la clé de façon à ce que son extraction soit quasiment impossible, même si le périphérique est compromis.

6.1 Stockage de clé sécurisé avec un TPM (module de plateforme sécurisée)

Un TPM est un composant qui procure un certain 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 quitte jamais le TPM. 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.

6.2 Certification FIPS 140-2

Pour certains produits et cas d'utilisation, l'utilisation d'un TPM peut être une exigence réglementaire pour protéger les informations, parfois en combinaison avec une exigence de conformité à la norme FIPS 140-2. FIPS (Federal Information Processing Standard) 140-2 est une norme de sécurité de l'information pour les modules cryptographiques, émise 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 et des tests de mise sous tension.

Vous trouverez plus d'informations sur les exigences de certification de la norme FIPS 140-2 sur le site Web du NIST *https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards*

6.2.1 TPM certifié dans les produits Axis

Le TPM utilisé dans certains produits Axis est certifié pour répondre aux exigences de la norme FIPS 140-2. Plus spécifiquement, elle est certifiée conformément au niveau de sécurité 2 de la norme, ce qui signifie que le TPM répond également, entre autres, aux exigences d'autorisation basée sur des rôles et de preuves de sabotage.

7 IEEE 802.1AR - vérification de périphérique avec l'identifiant de périphérique Axis

Une personne qui achète un périphérique 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 la bonne unité ? Que le périphérique n'a pas été remplacé sans autorisation ? Aucun équipement en réseau et aucun logiciel sur serveur ne peut effectuer

une inspection physique. Par mesure de sécurité, il est courant d'interagir d'abord avec un nouveau produit sur un réseau fermé, où l'unité peut être approvisionnée de manière sécurisée.

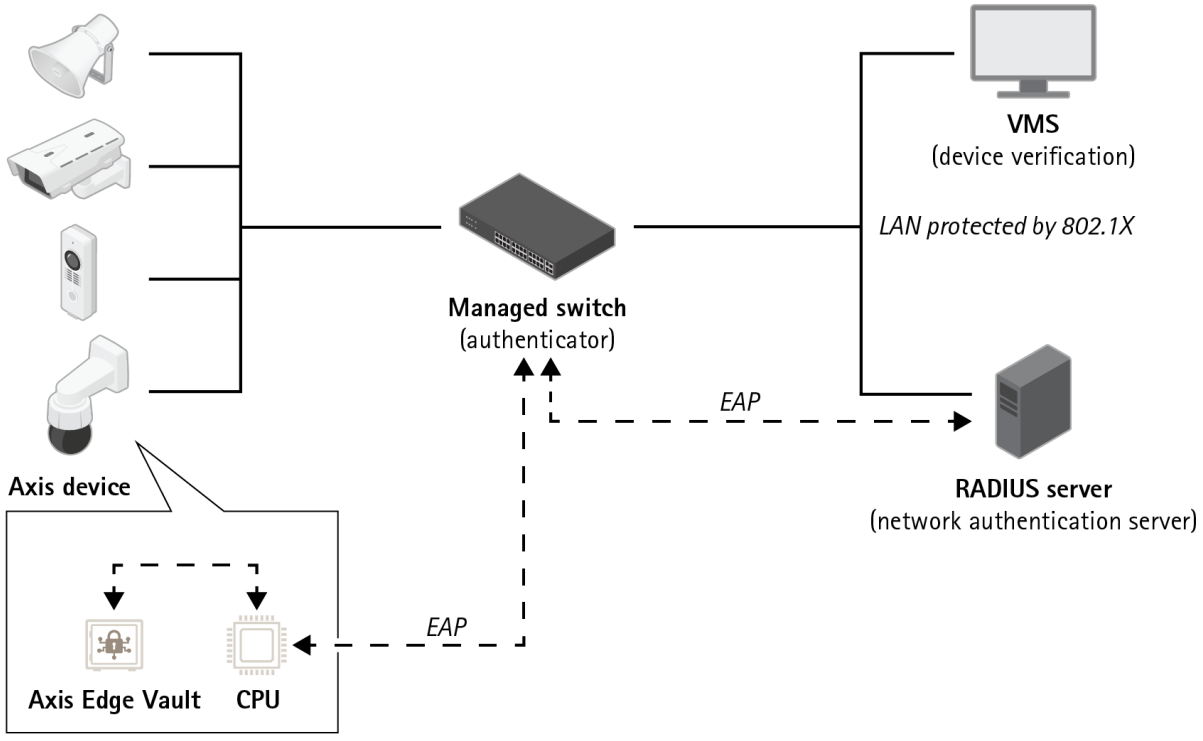

Figure 4. Les clients peuvent demander à leur serveur d'authentification d'accepter automatiquement les produits Axis achetés sur le réseau à l'aide des numéros de série des périphériques et de l'identifiant de périphérique Axis.

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 périphérique sur un réseau. Si

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

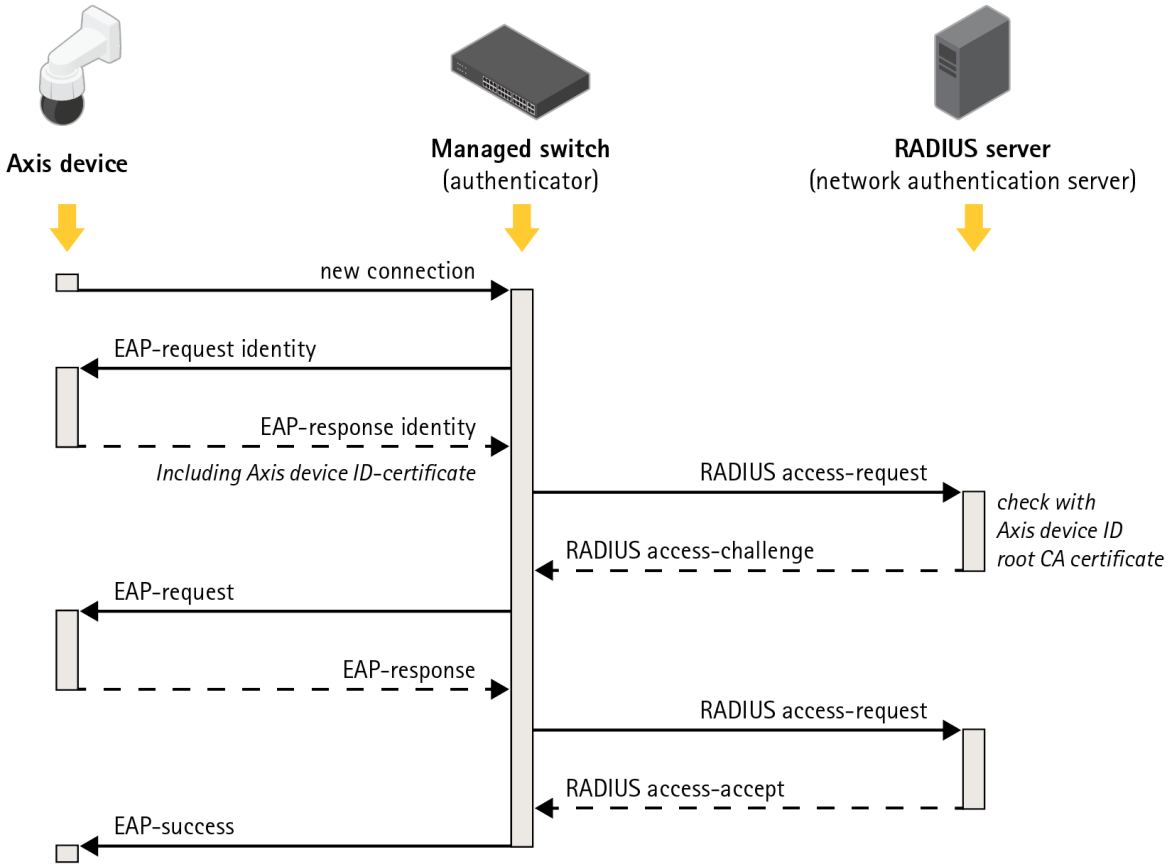

Figure 5. IEEE 802.1AR définit une méthode d'identification d'un périphérique sur un réseau en suivant un protocole qui envoie des requêtes Extensible Authentication Protocol (EAP) au commutateur qui utilise des requêtes Remote Authentication Dial-In User Service (RADIUS) pour autoriser l'accès.

Sur les produits Axis, ces mesures de sécurité sont mises en œuvre via Axis Edge Vault et l'identifiant de périphérique Axis. Axis Edge Vault est un module sécurisé dans lequel l'identifiant de périphérique Axis, collection de certificats permettant de vérifier l'identification du périphérique, est installé. Ces fonctions fournissent à votre réseau des preuves vérifiables par cryptographie qu'une unité donnée a été produite par Axis et que la connexion réseau à l'unité est effectivement assurée par cette unité.

Un périphérique avec l'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 périphérique sur le terrain avec d'autres clés et/ou certificats lui permettant d'accéder à certaines ressources réseau du client.

En identifiant l'unité avec l'identifiant de périphérique Axis, le temps de déploiement des périphériques peut être réduit, car les périphériques 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 périphériques dans un grand système.

7.1 Axis Edge Vault

Axis Edge Vault est un module de calcul cryptographique sécurisé, sous la forme d'une puce montée sur la carte de circuit imprimé à l'intérieur du produit. Edge Vault peut stocker des certificats de manière sécurisée et peut être utilisé pour des opérations cryptographiques sur des certificats stockés de manière sécurisée.

Les certificats stockés dans Edge Vault ne doivent pas le quitter pour être utilisés par le périphérique. 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 Identifiant de périphérique Axis

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

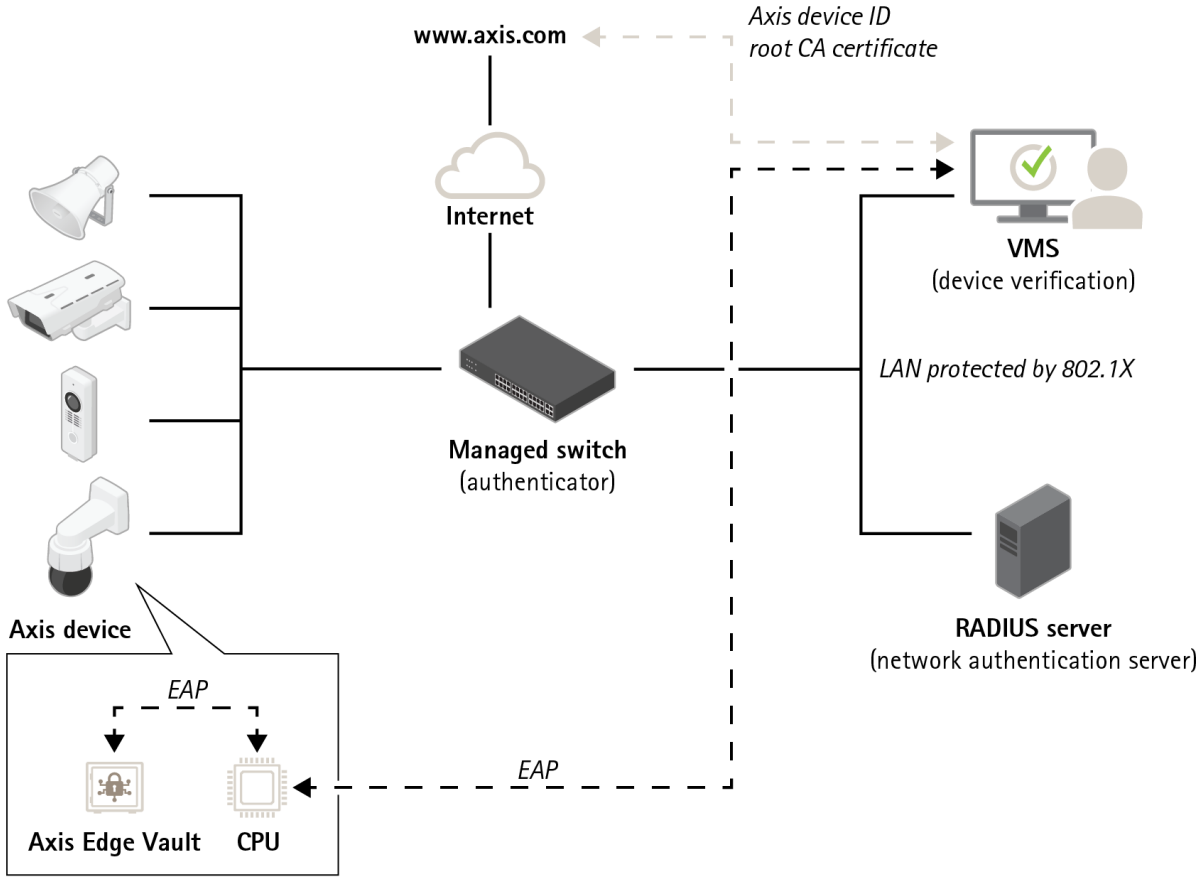

Figure 6. Les applications logicielles dans d'autres parties du système peuvent utiliser l'identifiant de périphérique Axis et les opérations cryptographiques pour vérifier avec qui la communication est effectuée. L'identifiant de périphérique Axis a été vérifié par le certificat CA racine d'identifiant de périphérique Axis public sur axis.com.

7.2.1 Hiérarchies de certification

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. Faisons une analogie 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 d'identifiant de périphérique Axis sont approuvés par un certificat CA 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 CA racine d'identifiant de périphérique Axis pour avoir correctement vérifié le certificat Axis d'une unité connectée au réseau.

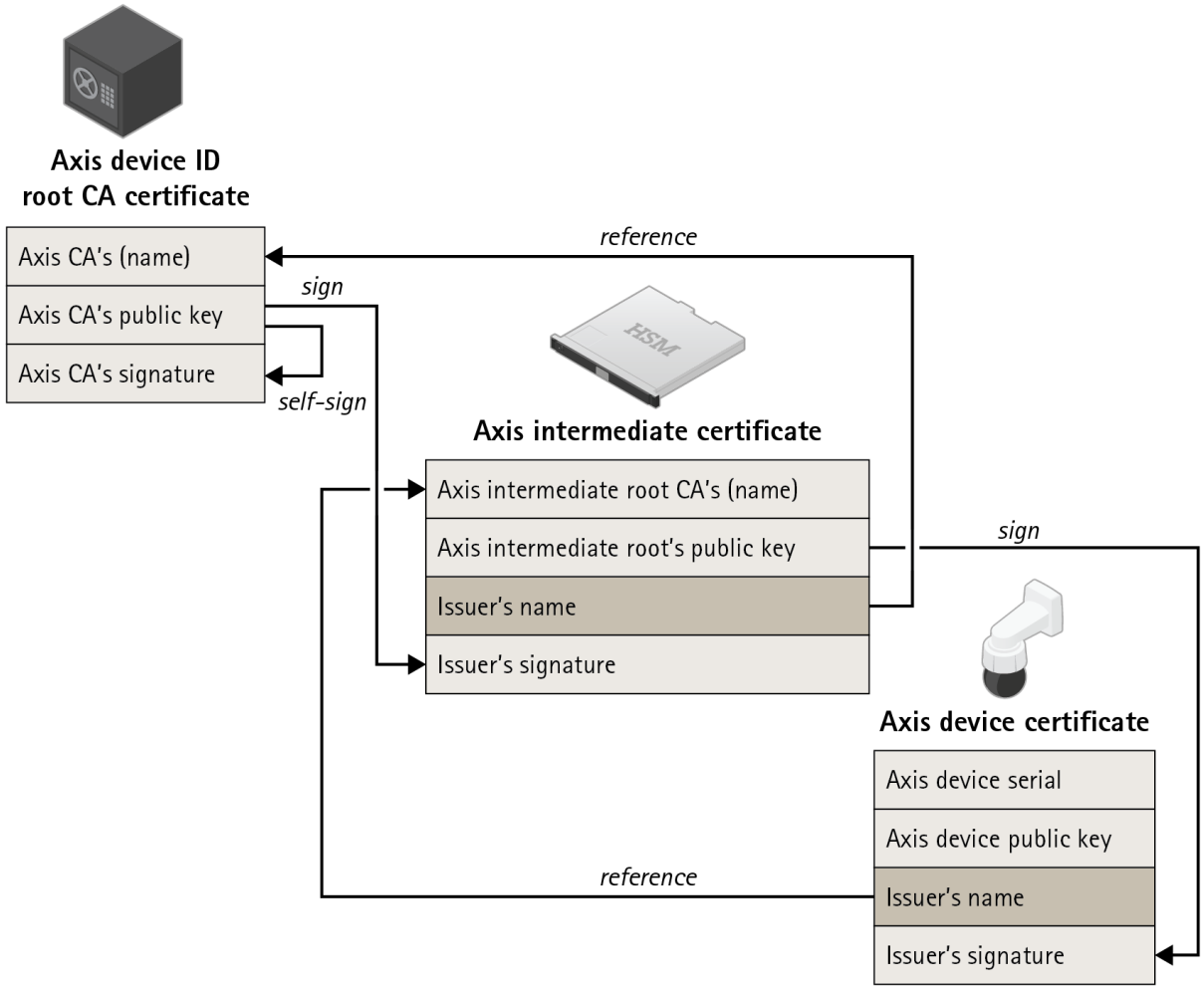

Figure 7. L'identifiant de périphérique Axis, qui est un certificat intégrant le numéro de série du produit, est signé par un certificat intermédiaire qui a été signé par le certificat racine Axis. Vu que le certificat racine Axis est très précieux et qu'il doit être stocké dans un coffre-fort, le certificat intermédiaire est nécessaire pendant le provisionnement en usine.

A 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 et les systèmes audio.

L'entreprise emploie plus de 3500 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, son siège est situé à Lund en Suède.

Pour en savoir plus, visitez notre site web *axis.com*.