LIVRE BLANC

La sécurité dans la solution de caméra-piéton d'Axis

Octobre 2026

Avant-propos

Bien qu'il soit basé sur une plateforme ouverte, le système de caméra-piéton Axis bénéficie d'un niveau de sécurité très élevé.

Pour garantir la sécurité en cas de perte de la caméra, celle-ci est basée sur une plateforme minimisée, sans composants logiciels superflus. Davantage de fonctionnalités sont plutôt placées dans le contrôleur système, qui est généralement moins exposé aux menaces physiques. En outre, le stockage interne de la caméra est chiffré selon la norme AES-256 afin d'empêcher tout accès non autorisé aux données. La communication basée sur IPv6 et les certificats garantissent que la caméra téléchargera les données uniquement vers le contrôleur système spécifique ou le système auquel elle appartient.

Lorsque les données sont transférées de la caméra au contrôleur système, une connexion réseau chiffrée HTTPS est utilisée. Les données ne sont que brièvement stockées dans le dispositif de stockage chiffré AES-256 du contrôleur système, avant d'être transférées, au moyen d'une autre connexion chiffrée HTTPS, vers la destination du contenu.

La sécurité et l'intégrité du contrôleur système sont encore renforcées par un TPM (trusted platform module) conforme à la norme FIPS 140-2. D'autres caractéristiques, que le système de caméra-piéton partage avec de nombreux autres dispositifs Axis, sont le SE signé, le démarrage sécurisé et la vidéo signée.

Lorsque les images sont diffusées en direct via AXIS Body Worn Live, les sociétés peuvent choisir entre un déploiement hébergé par Axis (dans le cloud) ou un déploiement auto-hébergé (sur site). Dans les deux cas, les données sont chiffrées au repos et en transit, et bénéficient d'un chiffrement complet de bout en bout jusqu'au client de l'observateur. De plus, l'administrateur contrôle strictement qui peut visionner le flux de données vidéo en direct, jusqu'au niveau de l'ordinateur, du client et des identifiants de l'utilisateur.

Table des matières

1 Acronymes et terminologie 4
2 Introduction 4
3 Sécurité en cas de perte de la caméra 4
4 Sécurité dans le transfert de données 4
5 Autres fonctions de sécurité 5
6 Sécurité avec AXIS Body Worn Live 5
6.1 Déploiement hébergé par Axis 6
6.2 Déploiement en auto-hébergement 6

1 Acronymes et terminologie

BWC. Caméra-piéton

VMS. Système de gestion vidéo

EMS. Système de gestion des preuves

Destination du contenu. Lieu où sont stockés les enregistrements et les données provenant, par exemple, de caméras-piétons. Les systèmes de gestion vidéo, les systèmes de gestion des preuves (EMS) et les serveurs multimédia sont des exemples de destinations de contenu.

2 Introduction

Le système de caméra-piéton Axis est basé sur une plateforme ouverte, ce qui facilite l'intégration avec des systèmes externes pour la gestion vidéo et la gestion des preuves. Néanmoins, il bénéficie d'un très haut niveau de sécurité car il s'agissait de l'objectif principal à chaque étape de la mise en œuvre du système.

Ce livre blanc décrit le flux de données entre les composants du système Axis de caméra-piéton. Nous décrivons en particulier les mesures prises pour sécuriser le système et ses données, depuis l'enregistrement d'une caméra-piéton jusqu'à la destination du contenu. Nous montrons également comment les flux de données vidéo en direct sont cryptés avec AXIS Body Worn Live, quel que soit le modèle de déploiement utilisé.

3 Sécurité en cas de perte de la caméra

De par son utilisation quotidienne, la caméra-piéton est physiquement exposée aux risques de vol et de vandalisme. Plusieurs caractéristiques de conception du système ont été utilisées pour atténuer les effets de ces menaces, de sorte que la sécurité du système et des données soit maintenue même en cas de disparition d'une caméra.

Par exemple, la caméra-piéton est basée sur une plate-forme logicielle réduite par rapport aux autres caméras Axis, et tous les composants logiciels inutiles ont été supprimés. La caméra et le contrôleur système ne prennent pas en charge VAPIX, ni les protocoles tels que FTP, SSH ou SNMP. De plus, la caméra ne dispose d'aucune fonctionnalité de serveur. L'intégration avec d'autres systèmes, tels que le VMS et l'EMS, est assurée par le contrôleur système, qui est généralement moins exposé aux menaces physiques que les caméras.

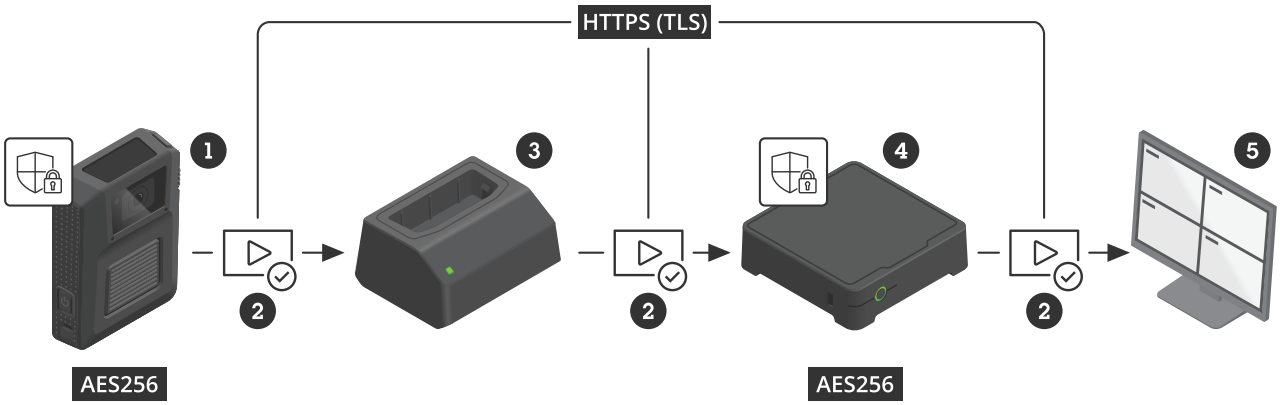
Le stockage interne de la caméra-piéton est chiffré à l'aide de la technologie AES-256 afin d'empêcher tout accès non autorisé aux données en cas de perte de la caméra.

La caméra téléchargera les données uniquement vers le contrôleur système spécifique ou le système auquel elle appartient. En effet, la caméra-piéton et le contrôleur système communiquent par IPv6 et utilisent des certificats. Les certificats sont automatiquement renouvelés pour correspondre à la dernière version du contrôleur système chaque fois que la caméra est placée sur sa station d'accueil.

Si une caméra est déconnectée du système et reste hors du système pendant huit semaines, elle passera en mode sécurisé et verrouillera la connexion pour des raisons de sécurité. Pour être à nouveau accepté dans le système, une vérification manuelle à l'aide de la phrase de passe principale est nécessaire. Cela permet de s'assurer qu'une caméra perdue ou absente depuis longtemps ne peut pas être rajoutée de manière inaperçue, ce qui pourrait constituer un risque pour la sécurité.

4 Sécurité dans le transfert de données

Dans le cadre d'une utilisation classique, la caméra-piéton est placée sur sa station d'accueil après une période de travail complète et contient des vidéos et des métadonnées. Toutes les données sont transférées par la station d'accueil au contrôleur système au moyen d'une connexion réseau chiffrée avec HTTPS (HTTP avec TLS). Les données ne sont stockées que brièvement dans le contrôleur du système, sur son dispositif de stockage SSD, qui est chiffré à l'aide de l'algorithme AES-256. Le contrôleur du système transfère ensuite les données, via HTTPS, vers la destination du contenu.



Stockage et transfert des données sécurisées de la caméra-piéton (1) vers la destination du contenu (5).

1 *Caméra-piéton avec Axis Edge Vault*
2 *Signature de vidéo (fonction de cybersécurité)*
3 *Station d'accueil*
4 *Contrôleur système avec Axis Edge Vault*
5 *Destination du contenu*

Il est également possible d'utiliser une clé de chiffrement de la destination du contenu pour chiffrer les données dans la caméra-piéton et le contrôleur système si la destination du contenu fournit une clé de cryptage publique. Dans ce cas, les données bénéficient d'une couche supplémentaire de chiffrement lorsqu'elles sont envoyées à la destination du contenu.

5 Autres fonctions de sécurité

La sécurité et l'intégrité du contrôleur système sont encore renforcées par un TPM (trusted platform module) conforme à la norme FIPS 140-2.

La caméra-piéton et le contrôleur système sont tous deux dotés d'Axis Edge Vault, une plateforme matérielle de cybersécurité qui protège toutes les données des dispositifs et fournit plusieurs fonctions de sécurité. Par exemple, le système de fichiers est chiffré et la clé est protégée par Axis Edge Vault. Du fait de l'*amorçage sécurisé*, les dispositifs ne peuvent démarrer qu'avec un logiciel de dispositif autorisé. Du fait du *SE signé*, les dispositifs rejettent les mises à niveau si l'intégrité du logiciel est compromise. La *vidéo signée* crée une couche de protection supplémentaire en ajoutant un total de contrôle cryptographique au flux vidéo. Cela permet de retracer de manière fiable la vidéo jusqu'à la caméra Axis unique où elle a été produite, vérifiant ainsi que la séquence n'a pas été altérée.

Pour en savoir plus sur la vidéo signée et Axis Edge Vault, rendez-vous sur *developer.axis.com/video-streaming-and-recording/signed-video/* et sur *axis.com/solutions/edge-vault*

Le seul moyen pour l'utilisateur de la caméra de visionner la vidéo enregistrée sur le terrain est d'utiliser l'application AXIS Body Worn Assistant. Si l'application est activée, la caméra-piéton transmet la vidéo directement à l'application, mais aucun matériel vidéo n'est stocké pour un accès ultérieur dans le cache ou la mémoire du dispositif qui exécute l'application. Il y a également une incrustation dans le flux vidéo pour dissuader l'utilisation de dispositifs d'enregistrement secondaires pour capturer la vidéo. Si cela se produit malgré tout, le clip vidéo peut être retracé jusqu'à l'utilisateur de la caméra-piéton par le biais de l'incrustation. Le connecteur compatible USB-C de la caméra-piéton ne peut en aucun cas être utilisé pour visionner, supprimer ou télécharger la vidéo.

6 Sécurité avec AXIS Body Worn Live

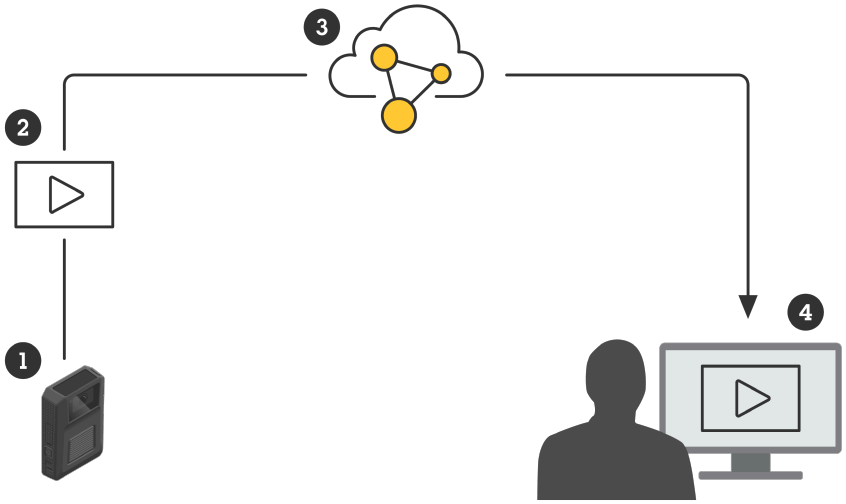
AXIS Body Worn Live est une application qui permet d'accéder aux données en direct des caméras-piétons Axis. En fournissant aux utilisateurs un flux vidéo et audio en direct ainsi que d'autres données, telles que les coordonnées de localisation, AXIS Body Worn Live offre une connaissance situationnelle inégalée d'un incident

en cours. Afin de répondre aux différentes exigences des sociétés en matière d'infrastructure et de souveraineté des données, il est disponible en deux modèles de déploiement : hébergé par Axis ou en auto-hébergement.

Quel que soit le modèle, l'administrateur du système de caméra-piéton contrôle entièrement les personnes qui peuvent visionner le flux de données vidéo en direct. Les données sont chiffrées de telle sorte que seuls des spectateurs approuvés par l'administrateur peuvent déchiffrer et visionner la vidéo. L'administrateur peut également révoquer les droits d'accès en fonction des rôles afin de garantir l'intégrité des données. Pour les déploiements hébergés par Axis, le spectateur doit disposer d'un accès au navigateur Web autorisé, au système de gestion vidéo (VMS) et aux identifiants d'utilisateur appropriés. Pour les déploiements en auto-hébergement, le spectatilisateur doit avoir accès au réseau local et disposer des identifiants d'accès appropriés. Personne d'autre, pas même Axis, ne peut accéder au flux de données vidéo en direct, et Axis n'a pas accès aux clés de chiffrement de bout en bout créées par les utilisateurs.

6.1 Déploiement hébergé par Axis

Lorsqu'il est utilisé en tant que service cloud, toutes les données et tous les fichiers hébergés dans AXIS Body Worn Live sont chiffrés au repos à l'aide de l'algorithme AES-256. Tous les canaux de communication sont sécurisés à l'aide de HTTPS avec TLS, en utilisant des certificats signés par des autorités de certification de confiance. Outre le chiffrement de la transmission, AXIS Body Worn Live ajoute une couche de véritable chiffrement de bout en bout grâce à la suite de chiffrement XChaCha20-Poly1305.



Flux de données vidéo en direct sécurisé avec chiffrement de bout en bout dans un déploiement hébergé par Axis

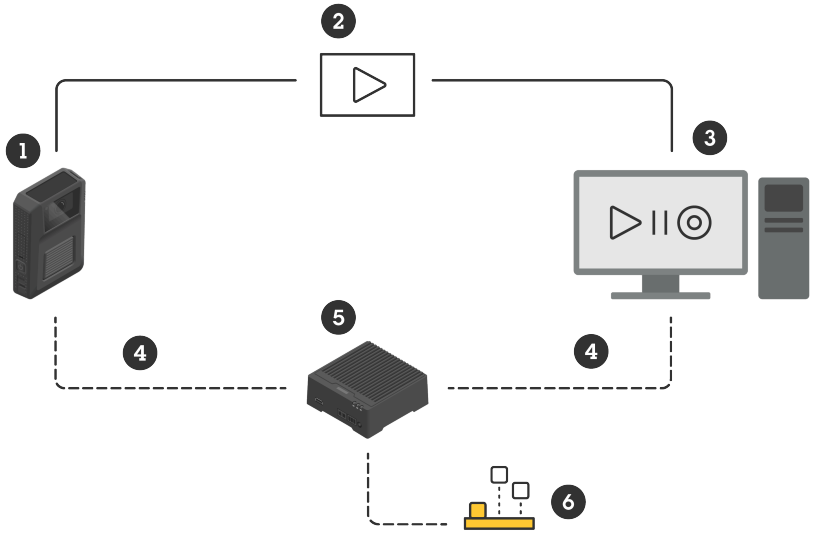
1 *La caméra-piéton enregistre des vidéos en direct ainsi que d'autres données. Les données sont déjà cryptées dans la caméra.*
2 *Flux de données vidéo en direct (crypté de bout en bout).*
3 *Hébergé sur le cloud par Axis. Les données et les fichiers sont chiffrés à l'aide de l'algorithme AES-256.*
4 *Client web . Les données sont déchiffrées dans le navigateur de l'opérateur.*

6.2 Déploiement en auto-hébergement

Les sociétés appliquant des politiques strictes qui exigent que l'infrastructure reste entièrement au sein de leurs propres environnements réseau contrôlés peuvent installer localement l'application serveur AXIS Body Worn Live, Self Hosted sur un dispositif. Ce dispositif serveur peut être l'AXIS W401 Body Worn Activation Kit ou l' AXIS-D3110 MK II Connectivity Hub. Aucune vidéo ni aucune donnée sensible n'est jamais stockée sur le dispositif serveur local ; celui-ci sert exclusivement à maintenir la connexion. Le canal de communication utilisé pour la transmission de données multimédia entre les caméras et les intégrations est sécurisé à l'aide du protocole DTLS 1.0 ou d'une version ultérieure. Le canal de communication utilisé pour transmettre les signaux

et les événements entre le serveur et les intégrations est sécurisé via HTTPS à l'aide de certificats fournis par le client et du protocole TLS 1.2 ou d'une version ultérieure.

Lorsque les données sont diffusées en continu via la version auto-hébergée, le serveur local configure de manière sécurisée une liaison WebRTC avec authentification par certificat entre le serveur et la caméra-piéton (BWC). Une fois établie, une connexion peer-to-peer cryptée s'établit directement entre la caméra-piéton (BWC) et le client WebRTC de l'observateur (tel qu'un système de gestion vidéo (VMS). Le flux vidéo étant transmis directement via cette connexion cryptée, sans stockage intermédiaire, toute interception non autorisée est ainsi empêchée. Le système est conçu pour fonctionner au sein de réseaux fermés et segmentés, sans nécessiter d'accès à internet, ce qui permet de réduire au minimum la surface d'attaque face aux menaces externes.



Flux de données vidéo en direct sécurisé dans un environnement auto-hébergé

1 *La caméra-piéton enregistre des vidéos en direct ainsi que d'autres données. Les données sont déjà cryptées dans la caméra.*
2 *Diffusion de flux de données peer-to-peer (cryptée).*
3 *Client WebRTC de Viewer.*
4 *Signalisation WebRTC.*
5 *AXIS Body Worn Live, dispositif serveur auto-hébergé.*
6 *AXIS Body Worn Live, application serveur auto-hébergée. Ceci sert à configurer la signalisation WebRTC.*

À propos d'Axis Communications

En améliorant la sûreté, la sécurité, l'efficacité opérationnelle et l'intelligence économique, Axis contribue à un monde plus sûr et plus intelligent. Leader de son secteur dans les technologies sur IP, Axis propose des solutions en vidéosurveillance, contrôle d'accès, visiophonie et systèmes audio. Ces solutions sont enrichies par des applications d'analyse intelligente et soutenues par des formations de haute qualité.

L'entreprise emploie environ 5000 personnes dans plus de 50 pays et collabore avec des partenaires technologiques et intégrateurs de systèmes du monde entier pour fournir des solutions sur mesure à ses clients. Axis a été fondée en 1984, son siège est situé à Lund en Suède.aboutaxis_text2

© 2020 — 2026 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC et VAPIX sont des marques déposées d'Axis AB dans différentes juridictions. Toutes les autres marques sont la propriété de leurs détenteurs respectifs.Nous nous réservons le droit d'effectuer des modifications sans préavis.trademarkdisclaimer