

LIVRE BLANC

# Caméras-piétons Axis

Sécurité système

Juin 2023

## 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 firmware signé, le démarrage sécurisé et la vidéo signée.

Lorsque des séquences sont diffusées en direct via AXIS Body Worn Live, les données sont chiffrées au repos, pendant le transport et dans le navigateur Web du visionneur. Elles sont également chiffrées de bout en bout avec le protocole XChaCha20-Poly1305. En outre, l'administrateur contrôle qui peut voir le flux en direct, jusqu'à l'ordinateur, le navigateur web et les informations d'identification de l'utilisateur spécifiques.

# 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	5
5	Autres fonctions de sécurité	5
6	Sécurité avec AXIS Body Worn Live	6

# 1 Acronymes et terminologie

BWC.Caméra-piéton

VMS.Système de gestion vidéo

EMS.Evidence Management System

**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. Les différents supports de stockage sont également mis en évidence, y compris les considérations supplémentaires en matière de sécurité.

## 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. En outre, la caméra n'a pas de fonction 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 à l'aide de 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 retirée du système pendant plus de quatre semaines, le contrôleur système accepte les anciens certificats pendant une période de grâce de huit semaines. Si une caméra est absente plus longtemps, elle doit être à nouveau acceptée manuellement dans le système, à l'aide de la phrase d'authentification de la clé principale. 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 système, sur son dispositif de stockage SSD qui est chiffré à l'aide d'AES-256. Le contrôleur système transfère ensuite les données, via HTTPS, vers la destination du contenu.

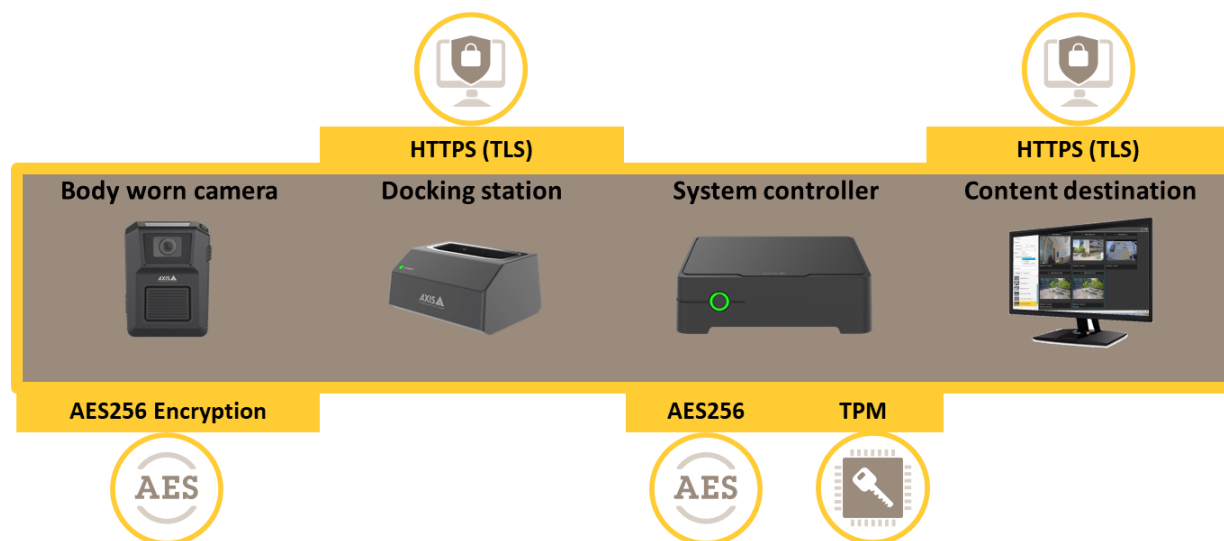


Figure 1. Stockage et transfert des données sécurisés de la caméra-piéton vers la destination du contenu.

Il est également possible d'utiliser une clé de cryptage à partir de la destination du contenu pour chiffrer les données dans la caméra-piéton et le contrôleur système, si la destination du contenu choisit de fournir 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. Le contrôleur système dispose également d'une fonction de *démarrage sécurisé*, qui garantit que le dispositif ne peut démarrer qu'avec un firmware autorisé.

En outre, le contrôleur système et la caméra-piéton (BWC) disposent tous deux d'un *firmware signé*, qui leur permet de rejeter les mises à jour du firmware si l'intégrité de ce dernier 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.

Voir [www.axis.com/developer-community/signed-video](http://www.axis.com/developer-community/signed-video) pour plus de détails sur la vidéo signée, ou [www.axis.com/solutions/built-in-cybersecurity-features](http://www.axis.com/solutions/built-in-cybersecurity-features) pour plus de détails sur les fonctions de cybersécurité Axis.

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. Elle est initialement fournie en tant que service basé sur le nuage.

Avec AXIS Body Worn Live, les données sont chiffrées non seulement au repos (pendant le stockage) et en transit, mais aussi de bout en bout entre la caméra et le navigateur Web de l'utilisateur.

Toutes les données et tous les fichiers hébergés dans AXIS Body Worn Live sont chiffrés à l'aide de la norme 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. AXIS Body Worn Live ajoute également une couche supplémentaire de véritable chiffrement de bout en bout avec le protocole XChaCha20-Poly1305.

L'administrateur du système de caméra-piéton contrôle entièrement les personnes qui peuvent visionner le flux en direct. Les données sont chiffrées de telle sorte que seuls les spectateurs approuvés par l'administrateur peuvent déchiffrer et visionner la vidéo. Le spectateur doit disposer du bon ordinateur, du bon navigateur web et des bonnes informations d'identification. Personne d'autre, pas même Axis, ne peut accéder au flux en direct. L'administrateur peut également révoquer l'accès.



# 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.