DOCUMENTO TECNICO

Ottobre 2026

# Sommario

Pur essendo basato su una piattaforma aperta, il sistema Body Cam Axis offre un altissimo livello di sicurezza.

Per garantire la sicurezza in caso di smarrimento della telecamera, questa si basa su una piattaforma ridotta al minimo senza componenti software superflui. Più funzionalità sono invece disponibili sul system controller, che in genere è meno esposto alle minacce fisiche. Inoltre, la memoria interna della telecamera è crittografata tramite AES-256 per impedire l'accesso non autorizzato ai dati. La comunicazione mediante IPv6 e certificati garantisce che la telecamera scarichi i dati solo verso il system controller specifico o il sistema a cui appartiene.

Quando i dati vengono scaricati dalla telecamera al system controller, viene utilizzata una connessione di rete crittografata tramite HTTPS. I dati vengono archiviati solo per un breve periodo nel dispositivo di archiviazione crittografato tramite AES-256 del system controller; quindi, vengono trasferiti ulteriormente con un'altra connessione HTTPS alla destinazione dei contenuti.

La sicurezza e l'integrità del system controller sono rafforzate ulteriormente da un TPM (Trusted Platform Module) conforme a FIPS 140-2. Altre funzionalità che il sistema body cam condivide con molti dispositivi Axis sono OS firmato, secure boot e il video firmato.

Quando le riprese sono in flusso dal vivo tramite AXIS Body Worn Live, le società possono scegliere tra una soluzione ospitata da Axis (cloud) o una soluzione gestita autonomamente (in loco). In entrambi i casi, i dati sono crittografati at rest, in transit e del tutto crittografati end-to-end direttamente sul client del visualizzatore. Inoltre, l'amministratore controlla rigorosamente chi può visualizzare il flusso dal vivo, specificando addirittura il computer, il client e le credenziali dell'utente.

# Indice


1 Sigle e terminologia 4
2 Introduzione 4
3 Sicurezza in caso di smarrimento della telecamera 4
4 Sicurezza nel trasferimento dei dati 4
5 Altre funzionalità di sicurezza 5
6 Sicurezza con AXIS Body Worn Live 5
6.1 Deployment ospitato da Axis 6
6.2 Implementazione auto-ospitata 6

# 1 Sigle e terminologia

**BWC.** Body Cam

**VMS.** Sistema di gestione video

**EMS.** Sistema di gestione prove

**Destinazione dei contenuti.** Posizione che memorizza le registrazioni e i dati, provenienti ad esempio dalle Body Cam. Esempi di destinazioni dei contenuti: sistemi di gestione video, sistemi di gestione prove e server multimediali.

# 2 Introduzione

Il sistema Body Cam Axis si basa su una piattaforma aperta, che ne facilita l'integrazione con sistemi esterni per la gestione dei video e delle prove. Tuttavia, offre un livello molto elevato di sicurezza del sistema, obiettivo principale in ogni fase di implementazione.

Questo documento tecnico illustra il flusso di dati tra i componenti del sistema Body Cam Axis. In particolare, descrive le misure adottate per proteggere il sistema e i suoi dati, dalla registrazione con la Body Cam fino alla destinazione dei contenuti. Mostriamo inoltre come i flussi dal vivo vengano crittografati con AXIS Body Worn Live in entrambi i suoi modelli di implementazione.

# 3 Sicurezza in caso di smarrimento della telecamera

Essendo utilizzata tutti i giorni, la Body Cam è esposta fisicamente al rischio di furti e atti vandalici. Per ridurne gli effetti sono stati adottati diversi accorgimenti di progettazione, per mantenere la sicurezza del sistema e dei dati anche in caso di smarrimento della telecamera.

Ad esempio, la Body Cam è basata su una piattaforma software ridotta al minimo rispetto a quella di altre telecamere Axis e tutti i componenti software non necessari sono stati rimossi. La telecamera e il system controller non supportano VAPIX né protocolli come FTP, SSH e SNMP. Inoltre, la telecamera non dispone di funzionalità server. L'integrazione con altri sistemi, come VMS ed EMS, è invece gestita dal system controller, che in genere è meno esposto alle minacce fisiche rispetto alle telecamere.

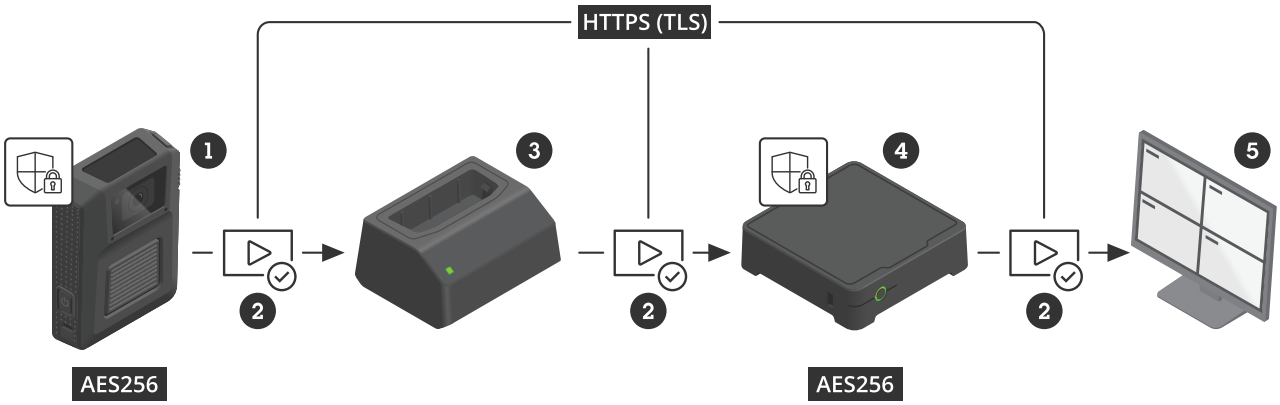
La memoria interna della Body Cam è crittografata tramite AES-256 per impedire l'accesso non autorizzato ai dati in caso di smarrimento della telecamera.

La telecamera scarica i dati solo su uno specifico system controller o sistema a cui appartiene, ciò avviene perché la body cam e il system controller comunicano tramite IPv6 e utilizzano certificati. Ogni volta che la telecamera viene inserita nella docking station, i certificati vengono rinnovati automaticamente in modo che corrispondano a quelli più recenti del system controller.

Se una telecamera dovesse essere scollegata e lontana dal sistema per otto settimane, entrerà in modalità sicura e imposterà il blocco della connessione per motivi di sicurezza. Per essere nuovamente ammessi nel sistema, è necessaria una verifica manuale tramite la passphrase della chiave principale. In questo modo, una telecamera che è stata smarrita o assente per molto tempo non può essere aggiunta di nuovo senza che qualcuno se ne accorga, perché rappresenterebbe un rischio per la sicurezza.

# 4 Sicurezza nel trasferimento dei dati

Normalmente, a fine turno la Body Cam viene riposta nella docking station e contiene video e metadati. Tutti i dati vengono scaricati tramite la docking station al system controller utilizzando una connessione di rete crittografata tramite HTTPS (HTTP con TLS). I dati vengono conservati nel controller di sistema solo per un breve periodo, sul relativo dispositivo di archiviazione SSD, che è crittografato utilizzando AES-256. Il controller di sistema trasferisce quindi i dati, tramite HTTPS, alla destinazione del contenuto.




*Trasferimento e memorizzazione dei dati in sicurezza dalla Body Cam (1) alla destinazione dei contenuti (5).*

1 *Body Cam con Axis Edge Vault*
2 *Video firmato (funzionalità di cybersecurity)*
3 *Stazione di ricarica*
4 *System controller con Axis Edge Vault*
5 *Destinazione dei contenuti*

È inoltre disponibile il supporto per l'utilizzo di una chiave di crittografia dalla destinazione dei contenuti per crittografare i dati della Body Cam e del system controller, qualora la destinazione dei contenuti fornisca una chiave di crittografia pubblica. In questo caso, i dati sono protetti da un ulteriore livello di crittografia quando vengono inviati alla destinazione dei contenuti.

# 5 Altre funzionalità di sicurezza

La sicurezza e l'integrità del system controller sono rafforzate ulteriormente da un TPM (Trusted Platform Module) conforme a FIPS 140-2.

Sia la Body Cam che il system controller sono dotati di Axis Edge Vault, una piattaforma di cybersecurity basata su hardware che protegge tutti i dati sui dispositivi e abilita diverse funzionalità di sicurezza. Ad esempio, il file system è crittografato e la chiave è protetta da Axis Edge Vault. *Secure Boot* garantisce che i dispositivi possano avviarsi solo con software del dispositivo autorizzato. *OS firmato* consente di rifiutare gli aggiornamenti se l'integrità del software è compromessa. Il *video firmato* offre un ulteriore livello di protezione aggiungendo un checksum crittografico al flusso video. Questo consente di risalire in modo attendibile alla singola telecamera Axis che ha prodotto il video, verificando che non sia stato manomesso.

Per ulteriori informazioni sui video firmati e su Axis Edge Vault, consultare *developer.axis.com/video-streaming-and-recording/signed-video/* e *axis.com/solutions/edge-vault*

Per l'utilizzatore della telecamera, l'unico modo di visualizzare il video registrato sul campo è tramite l'applicazione AXIS Body Worn Assistant. Se l'applicazione è abilitata, la Body Cam trasmette il video direttamente all'applicazione, ma nessun materiale viene archiviato per un successivo accesso nella cache o nella memoria del dispositivo che esegue l'applicazione. Nel flusso video viene anche utilizzata una sovrimpressione, che scoraggia l'uso di dispositivi di registrazione secondari per acquisire le immagini. Anche se così fosse, è possibile risalire all'utente della Body Cam tramite la sovrimpressione. Il connettore USB-C della Body Cam non può essere utilizzato in alcun modo per visualizzare, eliminare o scaricare il video.

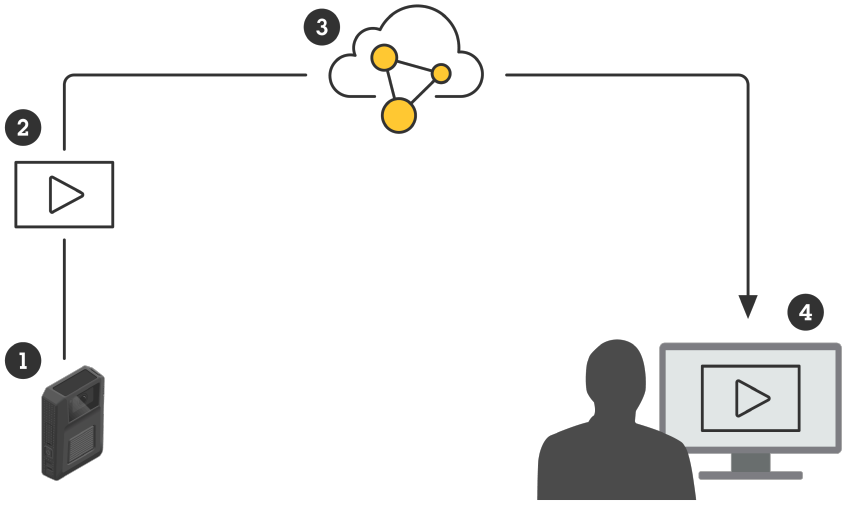
# 6 Sicurezza con AXIS Body Worn Live

AXIS Body Worn Live è un'applicazione che consente di accedere in tempo reale ai dati acquisiti dalle Body Cam Axis. Trasmettendo agli utenti un flusso dal vivo di video, audio e altri dati (come le coordinate della posizione) in tempo reale, AXIS Body Worn Live offre un quadro della situazione molto dettagliato di un evento in corso. Per soddisfare le diverse esigenze organizzative in materia di Infrastruttura e sovranità dei dati, è disponibile in due modelli di implementazione: ospitato da Axis e auto-ospitato.

Indipendentemente dla modello di implementazione, l'amministratore del sistema dlla telecamera body cam ha il controllo totale delle persone autorizzate a visualizzare il flusso in diretta. I dati vengono crittografati in modo tale che solo i visualizzatori esplicitamente approvati dall'amministratore possano decriptare e visualizzare il video. L'amministratore può inoltre revocare l'accesso in base ai ruoli per salvaguardare l'integrità dei dati. Per le implementazioni ospitate da Axis, il visualizzatore deve accedere al browser web autorizzato, al VMS e alle credenziali utente corrette. Per le installazioni auto-ospitate, il visualizzatore deve accedere alla rete locale e disporre delle credenziali utente corrette. Nessun altro, nemmeno Axis, può accedere al flusso dal vivo, e Axis non ha accesso alle chiavi di crittografia end-to-end create dagli utenti.

## 6.1 Deployment ospitato da Axis

Quando viene utilizzato come servizio basato su cloud, tutti i dati e i file ospitati su AXIS Body Worn Live vengono crittografati utilizzando AES-256 at rest. Tutti i canali di comunicazione sono protetti da HTTPS con TLS, utilizzando certificati firmati da autorità di certificazione affidabili. Oltre alla crittografia per il transito, AXIS Body Worn Live aggiunge un ulteriore livello di crittografia end-to-end reale, con la suite di cifratura XChaCha20-Poly1305.




*Riproduzione sicura del flusso dal vivo con crittografia end-to-end in una soluzione ospitata da Axis*

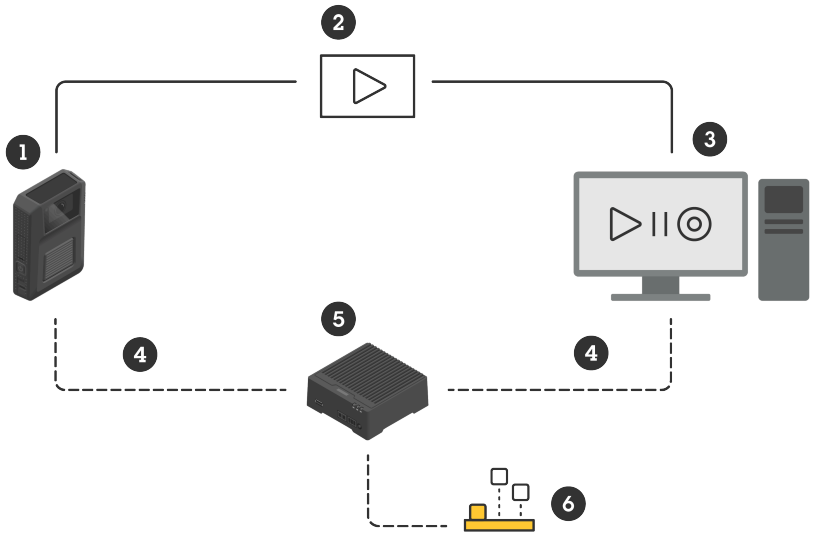
1. *La body cam registra video in diretta e altri dati. I dati vengono crittografati direttamente nella telecamera.*
2. *Streaming dal vivo (crittografia end-to-end).*
3. *Cloud ospitato da Axis. I dati e i file vengono crittografati utilizzando AES-256.*
4. *Client web. I dati vengono decriptati nel browser web dell'utente.*

## 6.2 Implementazione auto-ospitata

Le società con politiche rigorose, che richiedono che l'infrastruttura rimanga interamente all'interno dei propri ambienti di rete controllati possono installare localmente su un dispositivo l'applicazione server AXIS Body Worn Live, Self Hosted. Questo dispositivo server può essere il kit AXIS W401 Body Worn Activation Kit o un hub di connettività AXIS D3110 Mk II Connectivity Hub. Nessun video né dato sensibile viene mai archiviato at rest sul dispositivo server locale; quest'ultimo serve esclusivamente per mantenere la connessione. Il canale di comunicazione per la trasmissione multimediale tra telecamere e integrazioni è protetto tramite DTLS 1.0 o versioni successive. Il canale di comunicazione per la trasmissione di segnali ed eventi tra il server e le integrazioni è protetto tramite HTTPS con certificati forniti dal cliente e da TLS 1.2 o versioni successive.

Quando i dati vengono trasmessi in flusso utilizzando la versione auto-ospitata, il server locale effettua l'impostazione sicura della segnalazione WebRTC con autenticazione basata su certificato tra server e BWC. Una volta stabilita, viene creata una connessione peer-to-peer crittografata direttamente tra la telecamera BWC e il client WebRTC del visualizzatore (ad esempio un sistema di gestione video, VMS). Poiché il flusso video viene

inviato direttamente tramite questa connessione crittografata senza alcuna archiviazione intermedia, si impedisce qualsiasi intercettazione non autorizzata. Il sistema è progettato per funzionare in reti chiuse, segmentate senza richiedere l'accesso a internet, riducendo così al minimo la superficie di attacco contro le minacce esterne.




*Flusso dal vivo sicuro in una soluzione auto-ospitata*

1 *La body cam registra video in diretta e altri dati. I dati vengono crittografati direttamente nella telecamera.*
2 *Streaming peer-to-peer (criptato).*
3 *Client WebRTC del visualizzatore.*
4 *Segnalazione WebRTC.*
5 *Dispositivo server AXIS Body Worn Live, Self Hosted.*
6 *App del server AXIS Body Worn Live, Self Hosted. È utilizzata per l'impostazione della segnalazione WebRTC.*

# Informazioni su Axis Communications

Axis permette di creare un mondo più intelligente e sicuro migliorando la sicurezza, la protezione, l'efficienza operativa e la business intelligence. In qualità di azienda leader nelle tecnologie di rete, Axis offre videosorveglianza, controllo accessi, intercom e soluzioni audio, che supporta con applicazioni analitiche intelligenti e una formazione di alta qualità.

Axis ha oltre 5000 dipendenti in più di 50 paesi e collabora con partner tecnologici e integratori di sistemi in tutto il mondo per fornire soluzioni ai clienti. Fondata nel 1984, Axis è una società con sede a Lund, in Svezia.

© 2020 – 2026 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC e VAPIX sono marchi registrati di Axis AB in diverse giurisdizioni. Tutti gli altri marchi sono proprietà dei rispettivi proprietari.Axis Communications AB si riserva il diritto di apportare modifiche senza preavviso.