WHITE PAPER

Body Cam Axis

Sicurezza del sistema

Giugno 2023

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 il firmware firmato, Secure Boot e il video firmato.

Quando il filmato viene trasmesso in live streaming tramite AXIS Body Worn Live, i dati vengono crittografati a riposo, durante il trasporto e nel browser web dell'utente. Inoltre, sono crittografati in modalità end-to-end tramite il protocollo XChaCha20-Poly1305. L'amministratore può anche controllare le persone autorizzate a visualizzare il flusso in diretta fino al computer specifico, al browser web e alle credenziali dell'utente.

Sommario

1 Sigle e terminologia

VMS: Video Management System, sistema di gestione video

EMS: Evidence Management System, 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. Inoltre, elenca i vari supporti di archiviazione e ulteriori considerazioni sulla sicurezza.

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 ha 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, 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 rimane sganciata e lontana dal sistema per più di quattro settimane, è previsto un periodo di tolleranza durante il quale il system controller accetta certificati meno recenti per otto settimane. Se una telecamera rimane sganciata più a lungo, deve essere nuovamente accettata manualmente nel sistema utilizzando la passphrase della chiave master. 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 potrebbe rappresentare 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 archiviati solo per un breve periodo nel system controller, in un dispositivo di archiviazione SSD crittografato tramite AES-256. Quindi, il system controller trasferisce i dati tramite HTTPS alla destinazione dei contenuti.

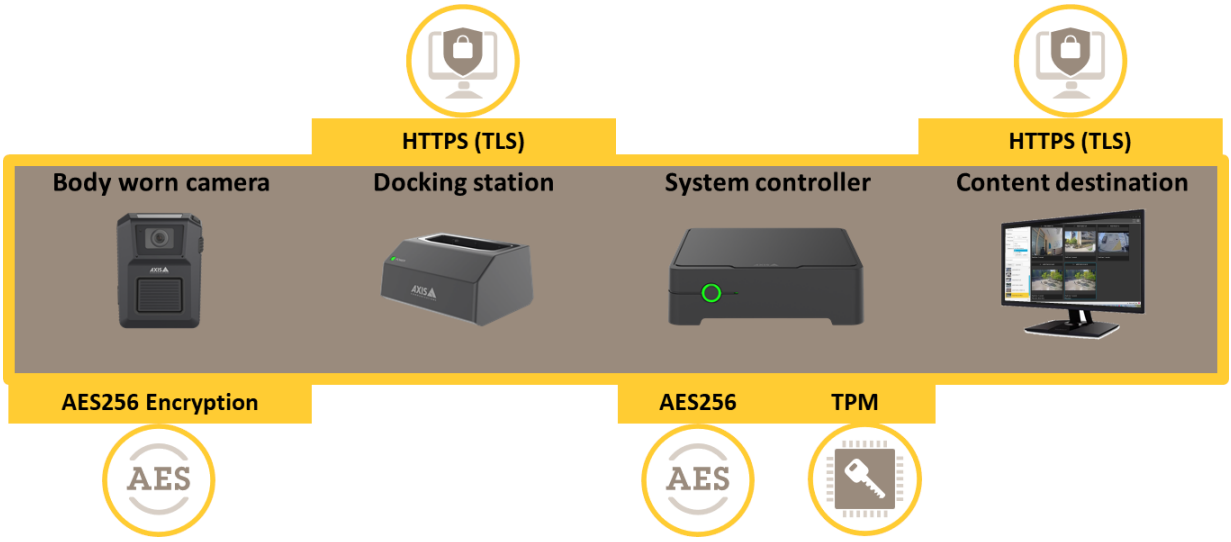

Figure 1. Memorizzazione dei dati e trasferimento dei dati in sicurezza dalla Body Cam alla destinazione dei contenuti.

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 scelga di fornire 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. Il system controller dispone inoltre della funzione *Secure Boot*, che assicura che il dispositivo possa avviarsi solo con firmware autorizzato.

Inoltre, sia il system controller che la Body Cam dispongono di un *firmware firmato*, che rifiuta gli aggiornamenti se la sua integrità 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.

Vedere *www.axis.com/developer-community/signed-video* per ulteriori dettagli sul video firmato o *www.axis.com/solutions/built-in-cybersecurity -features* per ulteriori dettagli sulle funzionalità di cybersecurity Axis.

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 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. Inizialmente è disponibile come servizio cloud-based.

Con AXIS Body Worn Live, i dati vengono crittografati non solo a riposo (in memoria) e in transito, ma anche in modalità end-to-end tra la telecamera e il browser web dell'utente.

Tutti i dati e i file contenuti in AXIS Body Worn Live sono crittografati tramite AES-256. Tutti i canali di comunicazione sono protetti tramite HTTPS con TLS, utilizzando certificati firmati da autorità di certificazione attendibili. AXIS Body Worn Live offre anche un ulteriore livello di crittografia end-to-end con il protocollo XChaCha20-Poly1305.

L'amministratore del sistema Body Cam può controllare totalmente le persone autorizzate a visualizzare il flusso in diretta. I dati vengono crittografati in modo tale che solo gli utenti approvati dall'amministratore possano decriptare e visualizzare il video. L'utente deve avere il computer giusto, il browser web giusto e le credenziali giuste. Nessun altro, neanche Axis, può accedere al flusso in diretta. L'amministratore può anche revocare l'accesso.

T10155258/IT/M2.4/2306

Informazioni su Axis Communications

Axis consente un mondo più intelligente e più sicuro creando soluzioni per migliorare la sicurezza e le prestazioni aziendali. Come società di tecnologie di rete e leader nel settore, Axis offre soluzioni nella videosorveglianza, controllo degli accessi, interfono e sistemi audio. Queste sono ottimizzate da applicazioni di analisi intelligente e supportate da formazione di alta qualità.

Axis ha circa 4.000 impiegati dedicati in più di 50 paesi e collabora con partner di tecnologia e integrazione di sistema in tutto il mondo per offrire soluzioni di clienti. Fondata nel 1984, Axis e con sede a Lund, in Svezia