WHITE PAPER

Axis Edge Vault

La piattaforma di cybersecurity basata su hardware che protegge i dispositivi Axis offrendo:

— la protezione della catena di fornitura

— un'identità del dispositivo attendibile

— l'archiviazione sicura delle chiavi

— il rilevamento di manomissioni nel video

Aprile 2024

AXIS COMMUNICATIONS

Sommario

Axis Edge Vault è una piattaforma hardware di cybersecurity che protegge il dispositivo Axis. È basata su solidi moduli di calcolo crittografico (Secure Element e TPM) e sicurezza del SoC (TEE e Secure Boot), combinati con le competenze di Axis nella sicurezza dei dispositivi edge. Axis Edge Vault si fonda su una radice di attendibilità molto forte, grazie a *Secure Boot* e al *SO firmato* ("SO" è l'abbreviazione di "sistema operativo"). Queste funzionalità permettono di avere una catena ininterrotta di software convalidato crittograficamente per la catena di fiducia da cui dipendono tutte le operazioni sicure.

I dispositivi dotati di Edge Vault riducono al minimo l'esposizione dei clienti ai rischi di cybersecurity, impedendo le intercettazioni e l'estrazione delle informazioni sensibili da parte di malintenzionati. Inoltre, Axis Edge Vault consente al dispositivo Axis di essere un'unità attendibile nella rete del cliente.

Piattaforma di cybersecurity Axis Edge Vault

Moduli di calcolo crittografico	Caratteristiche	Casi d'uso
• Secure Element • TPM 2.0 • Sicurezza del SoC (TEE)	• Secure Boot • SO firmato • ID dispositivo Axis • Archivio chiavi sicuro (keystore) • Video con firma • File system criptato	• Protezione della catena di fornitura • Identità del dispositivo attendibile • Archiviazione sicura delle chiavi • Rilevamento di manomissioni nel video

- **Protezione della catena di fornitura**: Axis Edge Vault richiede fondamenta sicure che costituiscano una radice di attendibilità. Senza l'ausilio di Secure Boot e del sistema operativo firmato, non è possibile comporre una catena a partire dalla radice di attendibilità. Secure Boot e il sistema operativo firmato costituiscono una catena ininterrotta di software convalidato crittograficamente, a partire dalla memoria immutabile (boot ROM). Secure Boot garantisce che un dispositivo possa avviarsi solo con un sistema operativo firmato, impedendo la manomissione fisica della catena di fornitura. Con il sistema operativo firmato, il dispositivo è anche in grado di convalidare il nuovo software del dispositivo prima di accettarne l'installazione. Se il dispositivo rileva che l'integrità è compromessa o che il software non è firmato da Axis, l'aggiornamento viene rifiutato. In questo modo, i dispositivi sono protetti dalla manomissione del software.
- **Identità del dispositivo attendibile**: poter verificare l'origine del dispositivo è fondamentale per stabilire che la sua identità è attendibile. Durante la produzione, ai dispositivi con Axis Edge Vault viene assegnato un certificato ID univoco e conforme a IEEE 802.1AR. È come avere un passaporto per dimostrare l'origine del dispositivo. L'ID del dispositivo viene archiviato in modo sicuro e permanente nell'archivio chiavi come certificato firmato dal certificato radice Axis. L'ID del dispositivo può essere utilizzato dall'infrastruttura IT del cliente per l'onboarding e l'identificazione in sicurezza del dispositivo.
- **Archiviazione sicura delle chiavi**: il keystore fornisce un'archiviazione delle informazioni crittografiche basata su hardware e protetta dalle manomissioni. Protegge l'ID del dispositivo Axis e le informazioni crittografiche caricate dal cliente e impedisce l'accesso non autorizzato e l'estrazione dannosa in caso di violazioni di sicurezza.

- **Rilevamento di manomissioni nel video**: il video firmato consente di dimostrare che le prove video non sono state manomesse senza dimostrare la catena di custodia del file. Ogni telecamera utilizza la propria chiave di firma univoca, memorizzata in sicurezza nell'archivio chiavi, per aggiungere una firma al flusso video. Quando si riproduce il video, il *file player* Axis mostra se è intatto. Il video firmato consente di risalire alla telecamera di origine e verifica che le immagini non siano state manomesse dopo aver lasciato la telecamera.

Sommario

1 Introduzione

Axis segue le best practice del settore implementando la sicurezza sui suoi prodotti. Questo avviene per ridurre al minimo l'esposizione del cliente ai rischi per la cybersecurity e per rendere il dispositivo Axis attendibile nella rete del cliente.

Axis Edge Vault è una piattaforma hardware di cybersecurity che protegge il dispositivo Axis. Si basa su solidi moduli di calcolo crittografico (Secure Element e TPM) e sicurezza del SoC (TEE e Secure Boot), combinati con le competenze di Axis nella sicurezza dei dispositivi edge.

Questo documento tecnico illustra l'approccio a più livelli per la sicurezza dei dispositivi edge Axis, spiegando anche quali sono i rischi più comuni e come prevenirli. Axis Edge Vault richiede fondamenta sicure che costituiscano una radice di attendibilità. Pertanto, vengono esaminati anche gli aspetti di sicurezza della catena di fornitura dei dispositivi Axis e viene spiegato come il SO firmato (sistema operativo con firma digitale) e Secure Boot siano fondamentali per contrastare la manomissione del software e la manomissione fisica della catena di fornitura.

Su *https://www.axis.com/support/cybersecurity/resources* è possibile trovare ulteriori informazioni sulla sicurezza dei prodotti, sulle vulnerabilità rilevate e sulle misure da adottare per ridurre i rischi.

L'ultimo capitolo di questo documento contiene un glossario.

2 Protezione della catena di fornitura

Axis Edge Vault richiede fondamenta sicure che costituiscano una radice di attendibilità. La definizione della radice di attendibilità inizia dal processo di avvio del dispositivo. Sui dispositivi Axis, il meccanismo basato su hardware *Secure Boot* verifica il sistema operativo (AXIS OS) da cui viene avviato il dispositivo. AXIS OS, a sua volta, è firmato crittograficamente utilizzando il *sistema operativo firmato* durante la sua creazione.

Secure Boot e il sistema operativo firmato sono strettamente correlati. Garantiscono che il sistema operativo o il software del dispositivo non siano stati manomessi (da chiunque abbia accesso fisico al dispositivo) prima dell'utilizzo del dispositivo e che, dopo l'utilizzo, il dispositivo non possa installare aggiornamenti software compromessi o senza firma del codice. Insieme, Secure Boot e il sistema operativo firmato creano una catena ininterrotta di software convalidato crittograficamente per la catena di fiducia da cui dipendono tutte le operazioni sicure.

2.1 Secure Boot

Il meccanismo Secure Boot è un processo di avvio costituito da una catena ininterrotta di software crittograficamente convalidati, a partire da una memoria non modificabile (boot ROM). Secure Boot garantisce che un dispositivo possa avviarsi solo con il sistema operativo autorizzato.

Il processo di avvio viene avviato dalla bootrom che convalida il bootloader. Quindi, Secure Boot verifica in tempo reale le firme integrate per ogni componente software caricato dalla memoria flash. La boot ROM funge da radice di attendibilità e il processo di avvio continua solo se ogni firma viene verificata.

Ogni parte della catena autentica la parte successiva, ottenendo in definitiva un kernel Linux verificato e un file system root verificato.

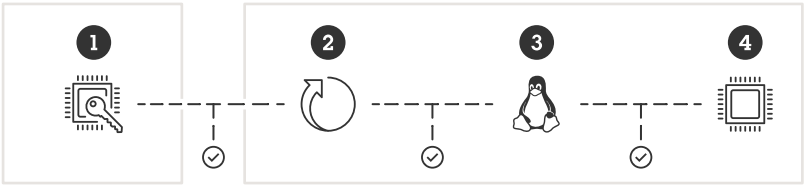

Figure 1. Nel processo Secure Boot, ogni parte della catena autentica la successiva, dando origine a un file system root verificato.

1 *Boot ROM (root of trust) sul SoC*
2 *Bootloader*
3 *Kernel Linux*
4 *File system root*

In molti dispositivi, è importante che la funzionalità di basso livello sia impossibile da modificare. Se oltre al software di livello inferiore sono integrati altri meccanismi di sicurezza, Secure Boot funge da livello di base sicuro che impedisce l'aggiramento di tali meccanismi. Per un dispositivo con Secure Boot, il sistema operativo installato nella memoria flash è protetto da modifiche, mentre la configurazione rimane non protetta. Secure Boot garantisce il corretto stato del dispositivo, anche dopo un ripristino delle impostazioni di fabbrica. Ma affinché Secure Boot funzioni, deve verificare in fase di avvio che il sistema operativo sia firmato da Axis.

2.2 SO firmato

Il sistema operativo Axis firmato prevede la firma del codice da parte di Axis sull'immagine del software del dispositivo con una chiave privata che rimane segreta. All'avvio del dispositivo, Secure Boot verifica che il software del dispositivo Axis sia firmato. Se il dispositivo rileva che l'integrità del software del dispositivo è compromessa, il dispositivo non funziona. Quando si aggiorna il software del dispositivo, la versione esistente di AXIS OS firmato sul dispositivo controlla automaticamente che anche il nuovo AXIS OS sia firmato. In caso contrario, l'aggiornamento viene rifiutato.

Il processo di firma del codice del sistema operativo viene avviato calcolando un valore hash crittografico. Il valore viene quindi firmato con la chiave privata di una coppia di chiavi privata/pubblica, quindi la firma viene collegata all'immagine di AXIS OS.

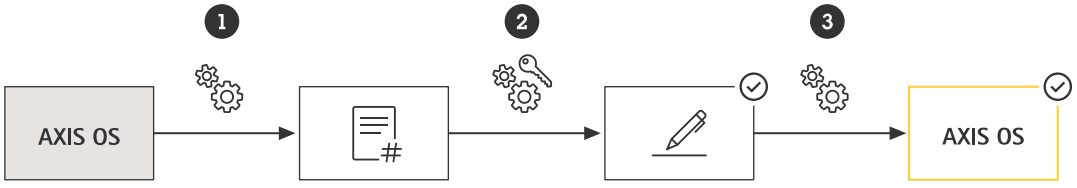

Figure 2. Il processo di firma del codice del sistema operativo.

1 *Viene creato un valore hash crittografico per AXIS OS.*
2 *La firma viene creata combinando l'hash e la chiave privata.*
3 *La firma viene aggiunta alla versione e al file binario di AXIS OS.*

Prima di un aggiornamento è necessario verificare l'autenticità del nuovo aggiornamento software. A questo scopo si utilizza la chiave pubblica (inclusa nel dispositivo Axis) per verificare che il valore di hash sia stato effettivamente firmato con la chiave privata corrispondente. Calcolando anche il valore hash e confrontandolo con il valore hash convalidato dalla firma, è possibile verificare l'integrità. Se la firma non è valida o l'immagine di AXIS OS è stata manomessa, l'avvio dei dispositivi Axis viene interrotto.

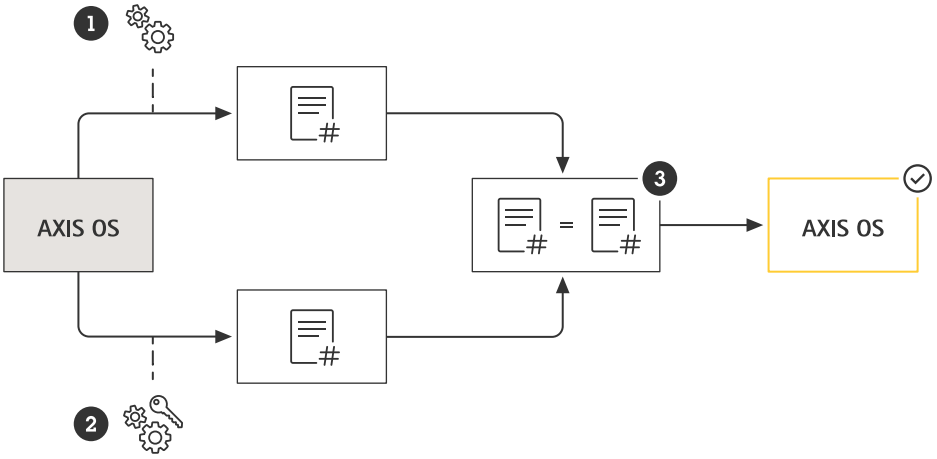

Figure 3. Il processo di verifica del sistema operativo firmato.

1 *Calcolo del valore hash di AXIS OS*
2 *Utilizzo della chiave pubblica per confermare il valore hash dalla firma*
3 *Solo se i risultati corrispondono, la firma viene verificata con successo.*

Il sistema operativo Axis firmato si basa sul metodo di crittografia a chiave pubblica RSA accettato dal settore. La chiave privata viene memorizzata in un luogo strettamente sorvegliato presso Axis, mentre la chiave pubblica è incorporata sui dispositivi Axis. L'integrità dell'intera immagine del software è garantita da una firma. Una firma principale verifica diverse firme secondarie mentre l'immagine viene scompattata.

Per le build di prova e personalizzate, Axis ha implementato un meccanismo che approva i singoli dispositivi affinché accettino immagini non di produzione. Queste immagini sono firmate in codice utilizzando una chiave dedicata, con l'approvazione sia del proprietario che di Axis, e danno origine a una firma personalizzata. Se installato sui dispositivi approvati, il certificato consente l'uso di un'immagine personalizzata che può essere eseguita solo sul dispositivo approvato, in base al numero seriale univoco e all'ID del chip. I certificati personalizzati possono essere creati solo da Axis, che possiede la chiave per firmarli.

3 Identità del dispositivo attendibile

Nelle moderne reti di sicurezza zero-trust ("fidarsi mai, verificare sempre"), la capacità di verificare l'origine del dispositivo, la sua autenticità e le sue connessioni è fondamentale. Un dispositivo di rete può verificare la sua integrità e autenticità come quando si mostra un documento di identità in aeroporto.

3.1 Identificazione sicura del dispositivo con l'ID dispositivo Axis

Lo standard internazionale *IEEE 802.1AR* definisce un metodo di automazione e protezione dell'identificazione di un dispositivo in una rete. Se la comunicazione viene inoltrata in un modulo di

calcolo crittografico incorporato, il dispositivo può restituire una risposta di identificazione attendibile in base allo standard. Questa risposta può essere utilizzata dall'infrastruttura di rete per consentire l'onboarding automatico e sicuro del dispositivo in una rete provvisoria per la configurazione iniziale del dispositivo e gli aggiornamenti del software.

Per garantire la conformità a IEEE 802.1AR, Axis produce la maggior parte dei dispositivi con un certificato Axis Device ID univoco e fornito in fabbrica (IEEE 802.1AR Initial Device Identifier, IDevID). L'ID del dispositivo Axis è archiviato in modo sicuro nel keystore antimanomissione, disponibile tramite un modulo di calcolo crittografico sul dispositivo. Questa identità è univoca per ogni dispositivo Axis ed è concepita per dimostrarne l'origine.

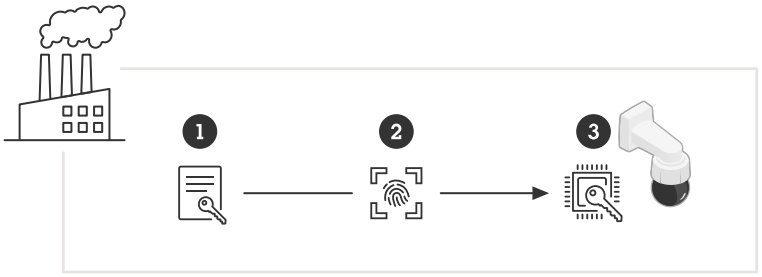

Figure 4. In fase di produzione, l'ID univoco del dispositivo Axis (2) viene memorizzato nell'archivio chiavi sicuro del dispositivo (3).

1 *Infrastruttura chiave ID dispositivo Axis (PKI)*
2 *ID dispositivo Axis*
3 *L'ID dispositivo Axis è archiviato in modo sicuro nel keystore antimanomissione, disponibile tramite un modulo di calcolo crittografico sul dispositivo Axis.*

IEEE 802.1AR si basa sullo standard IEEE 802.1X per il controllo degli accessi alla rete, abilitato per impostazione predefinita sui dispositivi Axis con l'ID dispositivo preselezionato. Questo consente di identificare e autenticare in sicurezza il dispositivo Axis tramite un'infrastruttura IT compatibile con 802.1X, anche con le impostazioni predefinite di fabbrica.

Il certificato Axis Device ID è disponibile in varie configurazioni crittografiche (RSA a 2048 bit, RSA a 4096 bit, ECC-P256). Queste sono abilitate per impostazione predefinita per consentire connessioni e identificazioni sicure del dispositivo tramite il controllo degli accessi alla rete IEEE 802.1X e HTTPS.

Axis gestisce la sua infrastruttura a chiave pubblica (PKI) IEEE 802.1AR per creare in fabbrica l'ID del dispositivo Axis durante la produzione. L'ID dispositivo Axis è firmato dal certificato intermedio, che a sua volta è firmato dal certificato radice Axis. Il CA radice e il CA intermedio sono archiviati in modo sicuro in moduli di calcolo crittografico separati geograficamente. Questo impedisce l'estrazione dannosa in caso di

violazioni di sicurezza presso gli impianti di produzione Axis. Per ulteriori informazioni sull'infrastruttura PKI di Axis, visitare il sito: *www.axis.com/support/public-key-infrastructure-repository*

Figure 5. Infrastruttura a chiave pubblica (PKI) IEEE 802.1AR per creare l'ID dispositivo Axis durante la produzione. L'ID dispositivo Axis (1), che è un certificato che incorpora il numero di serie del prodotto, è firmato da un CA intermedio dell'ID dispositivo Axis (2), firmato precedentemente dal CA radice dell'ID dispositivo Axis (3). Per il provisioning sicuro in fabbrica vengono utilizzati moduli di sicurezza hardware dedicati (HSM).

A Riferimento
B Firma

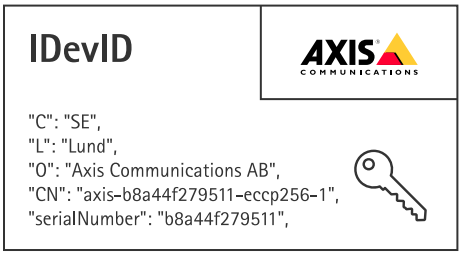

Figure 6. Esempio di ID dispositivo Axis.

3.2 Onboarding di rete sicuro

Quando si acquista un dispositivo Axis, è possibile eseguire un esame manuale prima di iniziare a utilizzarlo. Ispezionando visivamente il dispositivo e utilizzando le conoscenze precedenti sull'aspetto dei prodotti Axis, si può avere la certezza che il dispositivo provenga da Axis. Tuttavia, questa ispezione è possibile solo se si ha fisicamente accesso al dispositivo. Ma quando si comunica con un dispositivo in rete, come si può essere sicuri di comunicare con il dispositivo corretto e verificarne l'identità? Né le apparecchiature di rete né il software sui server possono eseguire un'ispezione fisica. Per precauzione, è prassi comune interagire per la prima volta con un nuovo dispositivo su una rete chiusa, dove il provisioning dell'unità può avvenire in sicurezza.

L'ID del dispositivo Axis fornisce alla rete la prova crittograficamente verificabile che un dispositivo specifico è stato prodotto da Axis e che la connessione di rete è effettivamente fornita da tale dispositivo. L'ID dispositivo Axis può essere utilizzato durante l'autenticazione di rete IEEE 802.1X per accedere a una rete di provisioning in cui si eseguono ulteriori aggiornamenti del software e configurazioni del dispositivo Axis prima che questo venga spostato nella rete di produzione.

Utilizzando l'ID dispositivo Axis, è possibile aumentare la sicurezza complessiva e ridurre il tempo necessario per il deployment dei dispositivi, perché è possibile utilizzare controlli più automatizzati ed economici per l'installazione e la configurazione.

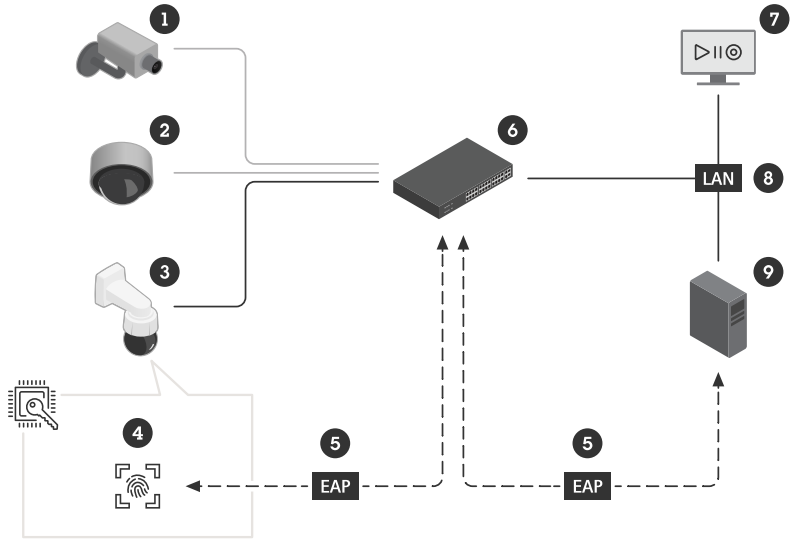

Figure 7. Onboarding di rete sicuro. È possibile indicare al server di autenticazione (9) di accettare automaticamente i dispositivi Axis (3) sulla rete (8) e sul VMS (7). Questo è possibile utilizzando i numeri di serie del dispositivo e l'ID del dispositivo Axis (4) come impronta digitale o autenticazione.

1 *Dispositivo non autorizzato (deve essere integrato manualmente)*
2 *Dispositivo di terze parti*
3 *Dispositivo Axis*
4 *ID dispositivo Axis, memorizzato nell'archivio chiavi sicuro antimanomissione*
5 *Autenticazione di rete 802.1X EAP-TLS del dispositivo Axis tramite certificato ID dispositivo Axis*
6 *Switch gestito (autenticatore)*
7 *VMS (verifica del dispositivo)*
8 *LAN protetta da 802.1X*
9 *RADIUS (server di autenticazione di rete)*

Figure 8. Descrizione più dettagliata del processo di onboarding. IEEE 802.1AR per l'identità protetta del dispositivo definisce un metodo per identificare un dispositivo (1) tramite le richieste EAP IEEE 802.1X (EAP-TLS) utilizzando un server RADIUS (3) per concedere l'accesso del dispositivo alla rete.

1 *Dispositivo Axis*
2 *Switch gestito (autenticatore)*
3 *Server RADIUS (server di autenticazione di rete)*
A *Nuova connessione*
B *EAP-Request Identity*

C EAP-Response Identity, incluso il certificato ID dispositivo Axis, IEEE 802.1AR IDevID
D RADIUS Access-Request
E RADIUS Access-Challenge
F EAP-Success

Oltre a essere un'ulteriore fonte di attendibilità, l'ID dispositivo Axis è anche un mezzo per monitorare i dispositivi e consente la verifica periodica e l'autenticazione secondo i principi zero-trust.

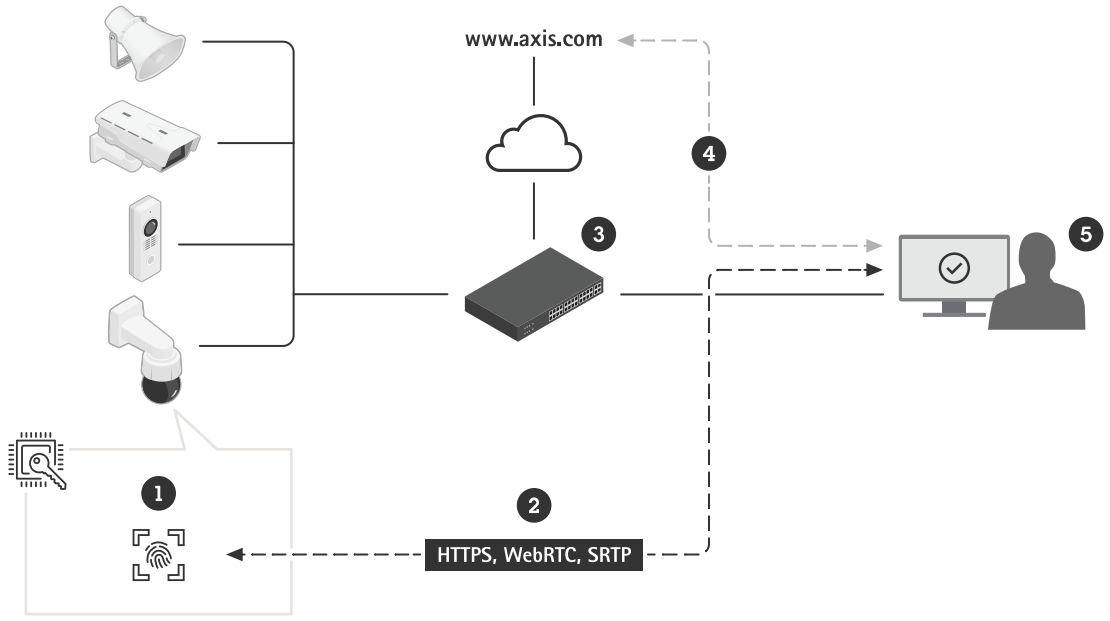

Figure 9. Dopo l'onboarding sicuro di un dispositivo, le applicazioni software (5) di altre parti del sistema possono utilizzare l'ID dispositivo Axis (1) e le operazioni crittografiche per verificare e autenticare il dispositivo in varie comunicazioni basate su TLS (2). L'ID del dispositivo Axis è verificabile tramite il certificato CA radice dell'ID del dispositivo Axis disponibile pubblicamente (4).

1 ID dispositivo Axis memorizzato nell'archivio chiavi sicuro antimanomissione
2 Comunicazione basata su TLS (HTTPS, WebRTC, SRTP)
3 Switch gestito
4 Certificato CA radice dell'ID dispositivo Axis (scaricabile all'indirizzo www.axis.com/support/public-key-infrastructure-repository)
5 VMS o altro software (verifica del dispositivo)

4 Archiviazione sicura delle chiavi

Tradizionalmente, le informazioni crittografiche sensibili X.509 (chiavi private) vengono archiviate nel file system di un dispositivo. Le informazioni sono protette solo dal criterio di accesso dell'account utente, che offre una protezione di base perché l'account utente non viene compromesso facilmente. Tuttavia, in caso di violazione di sicurezza, le informazioni crittografiche non sono protette e sono accessibili a un malintenzionato.

Dal punto di vista della sicurezza, l'archivio chiavi è fondamentale per la memorizzazione e la protezione delle informazioni crittografiche. Nel keystore sicuro vengono archiviate non solo le informazioni

crittografiche sensibili, incluse nell'ID del dispositivo Axis e nel video firmato: anche le informazioni caricate dal cliente possono essere protette allo stesso modo.

4.1 Archivio chiavi sicuro (keystore)

Le informazioni crittografiche sensibili (chiavi private) vengono memorizzate sul dispositivo in un archivio chiavi basato su hardware e protetto dalle manomissioni. Questo accorgimento impedisce l'estrazione dannosa anche in caso di violazione di sicurezza. Inoltre, le chiavi private rimangono protette nel keystore anche quando vengono utilizzate. Un eventuale malintenzionato non ha accesso all'archivio chiavi e non può intercettare il traffico di rete, accedere alla rete tramite chiavi IEEE 802.1X né estrarre altre chiavi private.

L'archivio chiavi sicuro è disponibile tramite un modulo di calcolo crittografico basato su hardware. A seconda dei requisiti di sicurezza, un dispositivo Axis può avere uno o più moduli di questo tipo, come TPM 2.0 (Trusted Platform Module) o Secure Element e/o TEE (Trusted Execution Environment).

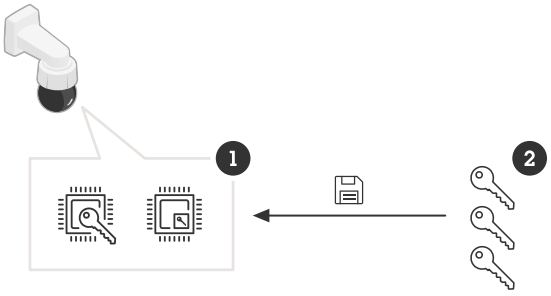

Figure 10. Gli archivi chiavi sicuri (1) consentono la protezione delle chiavi private (2) e l'esecuzione sicura delle operazioni crittografiche.

1 *Keystore sicuri, che possono essere Secure Element, TPM o TEE (sul SoC)*
2 *Chiavi private, come ID dispositivo Axis, chiave di firma video, chiavi di controllo accessi, chiavi del file system e chiavi caricate dal cliente (come IEEE 802.1X e HTTPS)*

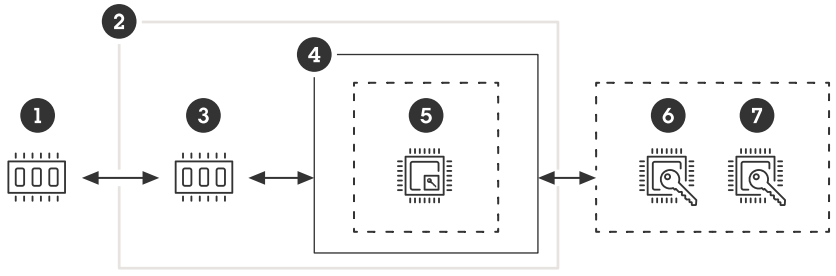

Figure 11. I dispositivi con Axis Edge Vault contengono moduli di elaborazione crittografica hardware (Secure Element (6) e TPM (7)) montati su PCB accanto al processore principale del SoC (4). TEE (5) è un'area sicura del processore principale del SoC. La boot ROM incorporata nel SoC (3) ha il compito di eseguire le procedure di avvio sicure e garantire che, per avviare il dispositivo, vengano utilizzate solo le immagini del software del sistema operativo firmate dalla memoria flash (1).

1 *Memoria flash (per sistema operativo firmato, file system di lettura-scrittura)*
2 *SoC*

3 *Boot ROM (per Secure Boot)*
4 *CPU*
5 *TEE (per archivio chiavi sicuro)*
6 *Secure Element (per archivio chiavi sicuro)*
7 *TPM (per archivio chiavi sicuro)*

TPM, Secure Element e TEE garantiscono la protezione delle chiavi private e l'esecuzione sicura delle operazioni crittografiche. In caso di violazione di sicurezza, impediscono l'accesso non autorizzato e l'estrazione dannosa.

4.2 Common Criteria e FIPS 140

I moduli di calcolo crittografico possono essere certificati utilizzando i livelli di valutazione Common Criteria (CC EAL) e i livelli di conformità FIPS 140 (1-4). Queste certificazioni vengono utilizzate per determinare la correttezza e l'integrità delle operazioni crittografiche e per verificare varie contromisure antimanomissione, come l'autoverifica, la resistenza alle manomissioni e altre. È possibile trovare informazioni sulla certificazione nella scheda tecnica di un dispositivo Axis o nel *Selettore prodotti Axis*. Axis richiede che i suoi moduli hardware di calcolo crittografico integrati siano certificati almeno secondo Common Criteria EAL4 e/o FIPS 140-2/3 Level 2/3.

4.2.1 Common Criteria

Common Criteria (CC) (noto anche come Common Criteria for Information Technology Security Evaluation) è uno standard internazionale (ISO/IEC 15408) per la certificazione della sicurezza dei prodotti IT. Common Criteria è un framework che consente a produttori e implementatori di specificare i requisiti funzionali e di garanzia come obiettivi di sicurezza, che possono essere raggruppati in profili di protezione.

Gli obiettivi di sicurezza dichiarati vengono quindi valutati da laboratori di prova indipendenti e certificati per poi essere elencati come prodotti certificati nel database Common Criteria. I requisiti e la completezza della valutazione da parte del laboratorio di prova sono trasmessi assegnando un EAL (Evaluation Assurance Level) che va da EAL 1 (testato funzionalmente) a EAL 7 (progetto verificato formalmente e testato). Questo significa che Common Criteria può spaziare da sistemi operativi e firewall fino a TPM e passaporti.

Per maggiori informazioni sui requisiti di certificazione Common Criteria, visitare il sito di Common Criteria: *www.commoncriteriaportal.org/*

4.2.2 FIPS 140

FIPS (Federal Information Processing Standards) 140-2 e 140-3 sono standard di sicurezza delle informazioni per i moduli di elaborazione crittografica e l'uso di algoritmi crittografici, emessi dal NIST (National Institute of Standard e tecnologia) e adottati come requisito dai governi federali degli Stati Uniti e del Canada. FIPS 140-3 ha sostituito FIPS 140-2 nel 2019 come versione aggiornata. La convalida da parte di un laboratorio di test certificato dal NIST assicura che il sistema e la crittografia del modulo siano implementati correttamente. In breve, la certificazione richiede la descrizione, la specifica e la verifica del modulo di calcolo crittografico, degli algoritmi approvati, delle modalità di funzionamento approvate e dei test di accensione.

I clienti hanno anche la certezza che i prodotti possono essere utilizzati secondo le specifiche governative, per la massima tranquillità in caso di audit da parte delle autorità. Alle aziende non regolamentate FIPS 140 viene garantito che i prodotti rispettano gli standard definiti dal governo. Per maggiori informazioni sui requisiti di certificazione FIPS 140-2 e FIPS 140-3, visitare il sito del NIST: *www.nist.gov*

Affinché un sistema completo sia conforme a FIPS 140, deve essere conforme ogni suo componente, come il sistema di gestione video, il server di registrazione e i dispositivi collegati (es. le telecamere). Un dispositivo è conforme a FIPS 140 quando viene utilizzato almeno un modulo certificato tramite software o hardware.

I dispositivi Axis con AXIS OS versione 12 o successiva dispongono del modulo crittografico Axis basato su software (OpenSSL) certificato FIPS 140. La maggior parte dei nuovi dispositivi Axis integra sia un modulo crittografico hardware certificato FIPS 140 sia il modulo crittografico basato su software. In questo modo si ha la soluzione ottimale, utilizzando il modulo certificato software per servire applicazioni basate su software come HTTPS e IEEE 802.1X a livello di sistema operativo e il modulo certificato hardware per l'archiviazione sicura delle chiavi.

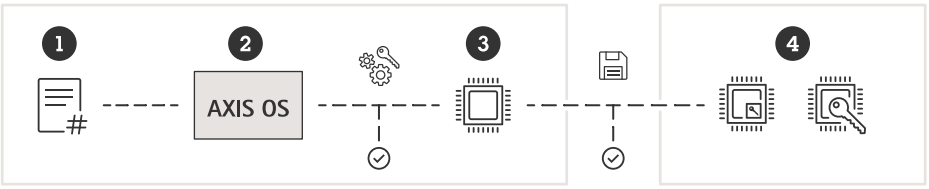

Figure 12. Uso di software di crittografia e moduli hardware conformi a FIPS 140 su un dispositivo Axis. Le applicazioni (1) vengono servite tramite il modulo crittografico Axis, integrato in AXIS OS (2) del dispositivo Axis. Il modulo crittografico Axis esegue operazioni crittografiche, sia simmetriche che asimmetriche, utilizzando il SoC (3) e/o i moduli di elaborazione crittografica basati su hardware (4) per l'archiviazione sicura delle chiavi.

1. *Applicazioni che richiedono crittografia o basate su TLS (come HTTPS, webRTC e 802.1X)*
2. *AXIS OS con modulo crittografico integrato basato su software (certificato NIST: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4621)*
3. *SoC*
4. *Moduli di calcolo crittografico integrati basati su hardware*

4.3 Protezione delle chiavi private

A un malintenzionato, l'estrazione della chiave privata consentirebbe di intercettare il traffico di rete crittografato tramite HTTPS o di fingersi il dispositivo per accedere a una rete protetta da 802.1X.

I dispositivi Axis supportano vari protocolli basati su TLS (Transport Layer Security) per comunicazioni sicure. L'ID dispositivo Axis (IEEE 802.1AR), HTTPS (crittografia di rete) e 802.1X (controllo dell'accesso alla rete) si basano sulla protezione delle informazioni crittografiche X.509.

I certificati digitali X.509 di TLS utilizzano un certificato e la corrispondente coppia di chiavi pubblica e privata per la comunicazione tra due host in rete. La chiave privata viene memorizzata nell'archivio chiavi sicuro e non lo lascia mai, anche se viene utilizzata per decriptare i dati. Il certificato e la chiave pubblica effettivi sono noti, possono essere condivisi dal dispositivo Axis e vengono utilizzati per crittografare i dati.

4.4 Protezione delle chiavi di controllo accessi

La protezione delle informazioni crittografiche utilizzate nelle soluzioni di controllo accessi Axis, come OSDP (Open Supervised Device Protocol) Secure Channel, è un altro esempio che ribadisce l'importanza dell'archiviazione delle chiavi protetta da hardware.

OSDP Secure Channel è uno schema di crittografia e autenticazione basato su AES-128; è ampiamente utilizzato per proteggere la comunicazione tra i door controller e le periferiche come i lettori.

La chiave simmetrica AES, Secure Channel Base Key (SCBK), condivisa dal door controller e dal lettore, viene utilizzata per avviare l'autenticazione reciproca e quindi generare un set di chiavi di sessione per crittografare i dati di comunicazione tra i door controller e i lettori.

Per una sicurezza end-to-end vera e propria, la Master Key (MK) e l'SCBK devono essere memorizzate in sicurezza nell'archivio chiavi sicuro del door controller Axis. Dalla Master Key deriva una chiave SCBK univoca per ogni lettore Axis collegato. Inoltre, la singola SCBK, distribuita in modo sicuro durante l'installazione su un lettore Axis, deve essere memorizzata nell'archivio chiavi sicuro del lettore. Il lettore è più critico, considerando che normalmente è installato sul lato non sicuro della porta.

In questo modo, le chiavi OSDP Secure Channel sono protette su entrambi i lati in un ambiente protetto da hardware. Questo accorgimento impedisce l'estrazione dannosa anche in caso di violazione di sicurezza.

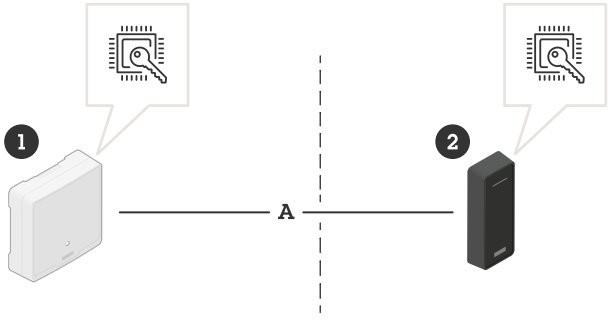

Figure 13. Sicurezza end-to-end con l'archivio chiavi sicuro nel controllo accessi. La Master Key e la singola Secure Channel Base Key (SCBK) sono memorizzate in archivi chiavi sicuri nei dispositivi su ogni lato della porta.

1 Door controller Axis installato sul lato sicuro della porta
2 Lettore Axis installato sul lato non sicuro della porta
A Comunicazione tramite canale sicuro OSDP

4.5 Protezione delle chiavi del file system

Un dispositivo Axis in funzione contiene configurazioni e informazioni specifiche per ogni cliente. Lo stesso vale quando il dispositivo Axis è in transito verso il cliente da un distributore o un integratore di sistemi che ha fornito servizi di preconfigurazione. Una volta ottenuto l'accesso fisico al dispositivo Axis, un malintenzionato potrebbe tentare di estrarre informazioni dal file system smontando la memoria flash e accedendovi tramite un apposito lettore. Pertanto, la protezione del file system leggibile e scrivibile dall'estrazione di informazioni riservate o dalla manomissione della configurazione è importante in caso di furto o intrusione nel dispositivo Axis.

L'archivio chiavi sicuro impedisce l'esfiltrazione dannosa di informazioni e previene la manomissione della configurazione applicando una crittografia avanzata al file system. Quando il dispositivo Axis è spento, le informazioni sul file system vengono crittografate. Durante l'avvio, il file system di lettura-scrittura viene decriptato con una chiave AES-XTS-Plain64 a 256 bit, in modo che il file system possa essere montato e utilizzato dal dispositivo Axis. La chiave di crittografia del file system viene generata in modo univoco per

ogni dispositivo in base alle impostazioni di fabbrica e rigenerata a ogni successivo aggiornamento del software: questo significa che non è mai la stessa per tutto il ciclo di vita del dispositivo.

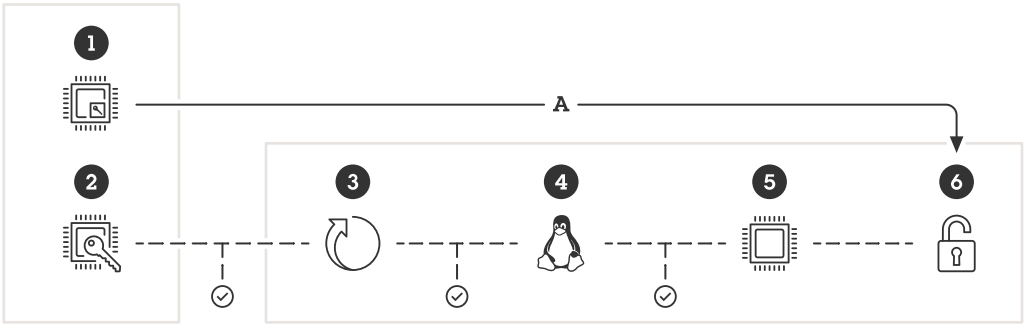

Figure 14. Il TEE (1) e la boot ROM (2) sono integrati nel SoC. Durante il processo di avvio, il file system di lettura-scrittura (6) viene decrittografato (tramite TEE) in modo che possa essere montato e utilizzato dal dispositivo Axis. Nel processo di avvio, ciascun elemento della catena – bootloader (3), kernel Linux (4) e file system root (5) – viene verificato e autentica il sottosistema successivo nella memoria flash. dando origine a un file system root verificato.

1 TEE
2 Boot ROM
3 Bootloader
4 Kernel Linux
5 File system root
6 File system di lettura-scrittura
A Il TEE decodifica il file system di lettura-scrittura.

5 Protezione dalle manomissioni nel video

Una premessa fondamentale nel settore della sicurezza è che il video registrato dalle telecamere di sorveglianza sia autentico e attendibile. Il video con firma è una funzionalità sviluppata per mantenere e aumentare ulteriormente la fiducia nel video come prova. Verificando l'autenticità del video, la funzionalità offre uno strumento per garantire che il video non sia stato modificato o manomesso dopo aver lasciato la telecamera.

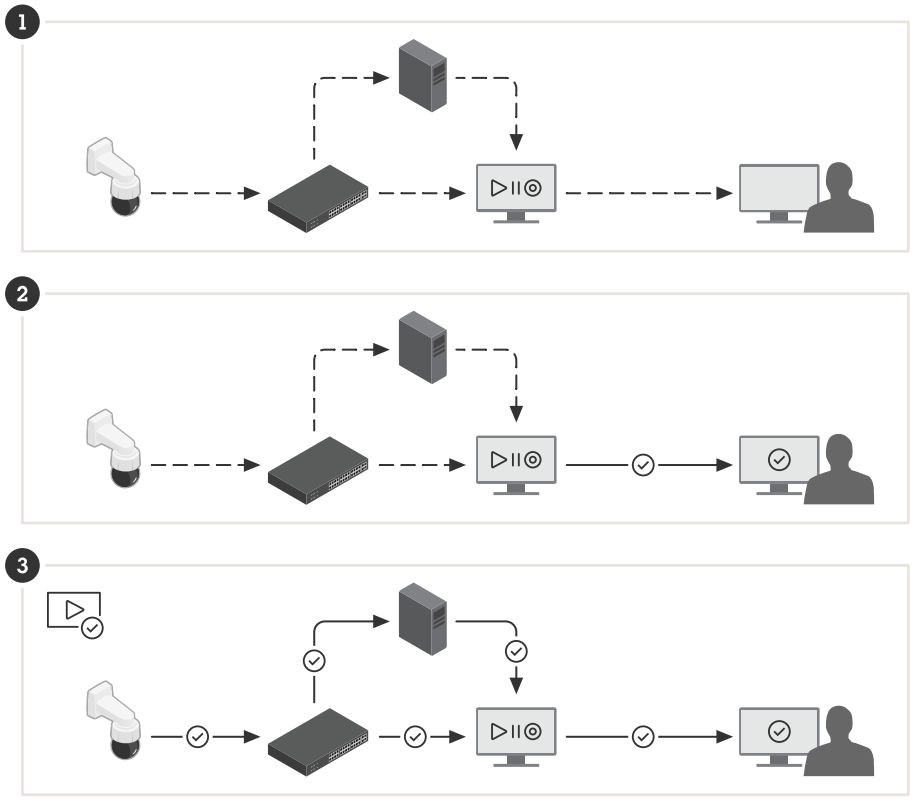

Figure 15. Verifica dell'autenticità del video.

1 *Dalla telecamera alla persona che guarda la registrazione, un video attraversa molte fasi. Un utente esperto può manomettere il video in ognuna di queste fasi.*
2 *Con la filigrana VMS aggiunta al video durante l'esportazione, alcuni passaggi vengono verificati, ma non vi è alcuna garanzia che il video non sia stato manomesso in una fase precedente.*
3 *Il video con firma è uno strumento per verificare che le immagini non siano state manomesse in nessuna fase del percorso dalla telecamera alla persona che guarda la registrazione esportata. Il video può essere ricondotto al dispositivo che lo ha registrato.*

5.1 Video con firma

Con la funzionalità di video con firma, sviluppata da Axis e pubblicata proattivamente in open source, è possibile utilizzare una firma sul flusso video per salvaguardarne l'integrità e verificarne l'origine risalendo alla telecamera che lo ha prodotto. Questo consente di dimostrare l'autenticità del video senza dover dimostrare la catena di custodia del file.

Dopo la registrazione di un evento con un sistema di telecamere di sicurezza, le forze di polizia possono ricevere il video esportato su una memoria USB e salvarlo in un sistema di gestione prove (EMS). Quando esporta il video dalla telecamera, l'agente può verificare che il video sia firmato correttamente. Se in seguito il video è utilizzato in un processo, la corte può controllare e verificare l'ora di registrazione del

video, quale telecamera lo ha registrato e se sono stati alterati o rimossi fotogrammi. Con il *file player* Axis, chiunque abbia una copia del video può vedere queste informazioni.

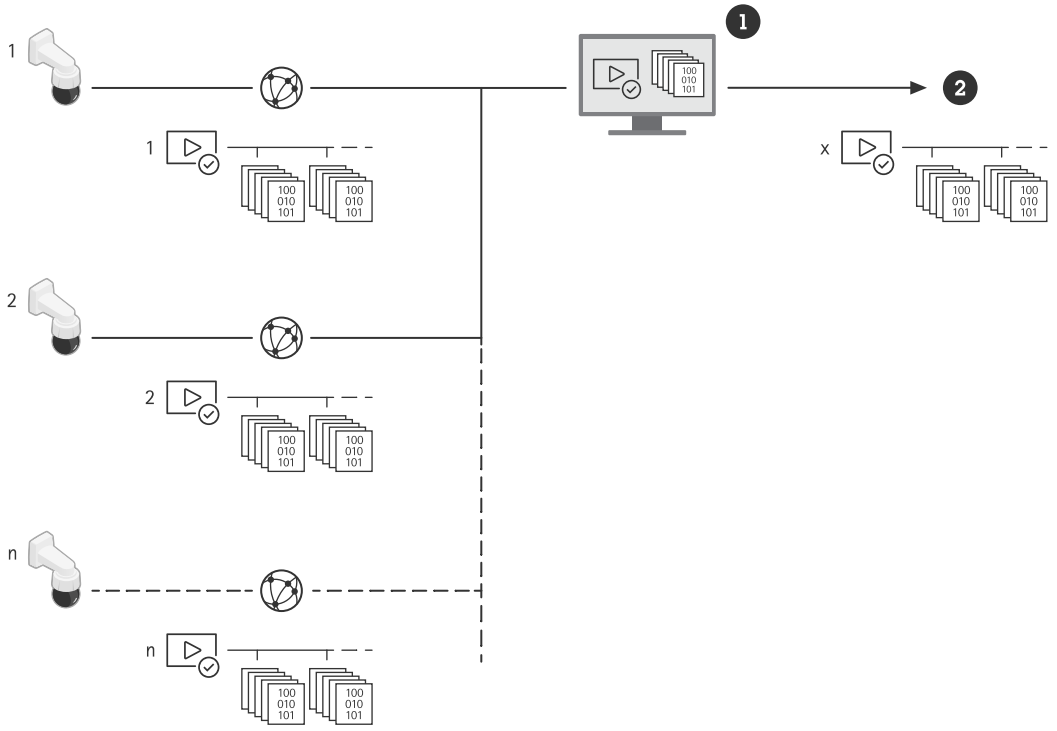

Figure 16. La firma viene aggiunta già sulla telecamera, consentendo la verifica dei contenuti in ogni fase: dalla sorgente sino all'uso finale del video.

1 *VMS*
2 *Esportazione video su CD/USB/web/e-mail*

Ogni telecamera utilizza la propria chiave di firma univoca, memorizzata nell'archivio chiavi sicuro, per aggiungere una firma al flusso video. Questa operazione viene svolta calcolando un hash per ogni

fotogramma video, compresi i metadati, e firmando l'hash combinato. Quindi, la firma viene memorizzata nel flusso in campi dedicati dei metadati (intestazione SEI).

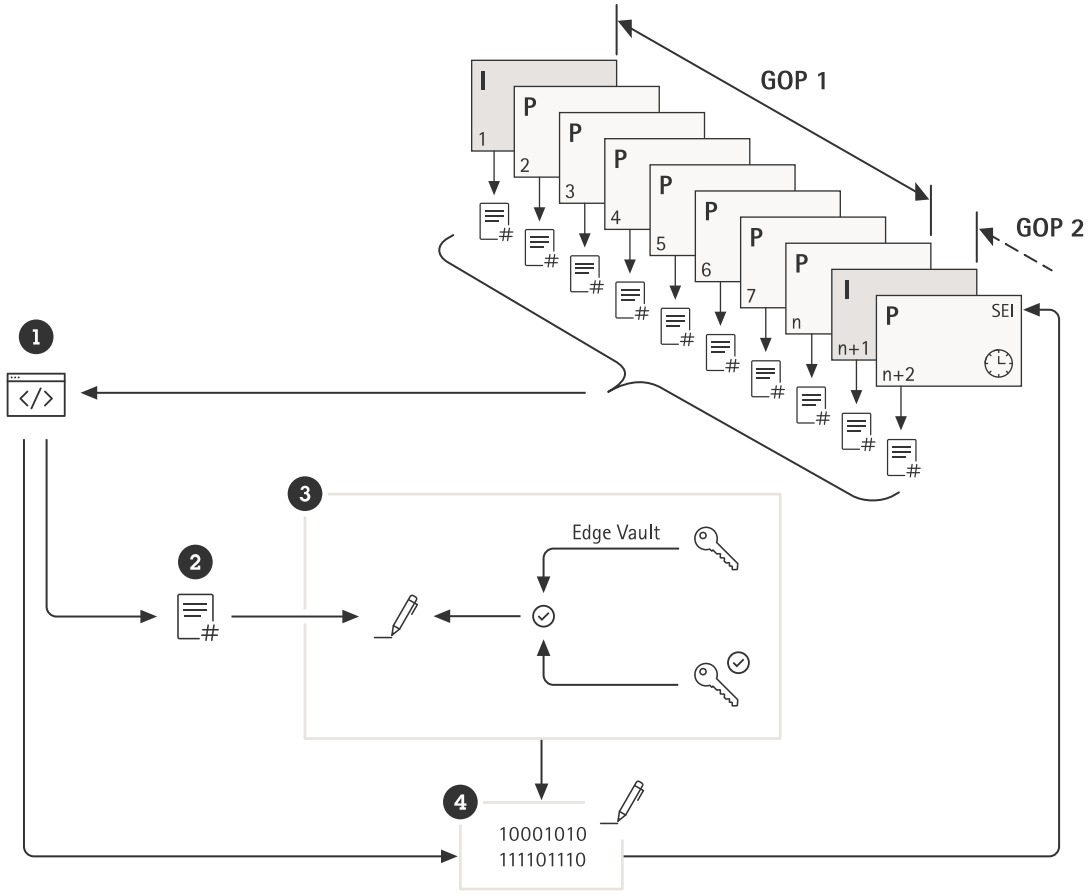

Figure 17. Rappresentazione grafica della procedura di aggiunta di una firma al flusso video. Il contenuto di ogni fotogramma di un GOP (Group of Pictures) viene elaborato insieme a un hash di metadati (1). Ciò costituisce l'hash GOP (2), che viene firmato in Edge Vault (3) utilizzando la chiave di firma video univoca del dispositivo e la chiave di attestazione. La firma digitale (4) e i metadati (1) vengono quindi aggiunti a un'intestazione SEI successiva che viene trasportata insieme al flusso.

1. *Metadati univoci del dispositivo (ID hardware, versione di AXIS OS, numero di serie e report di attestazione*) e metadati del flusso (contatore GOP e hash dei frame)*
2. *Hash GOP*
3. *Axis Edge Vault*
4. *Firma digitale*

* *Il report di attestazione può essere utilizzato per verificare l'origine la provenienza della coppia di chiavi utilizzata per la firma. Verificando l'attestazione della chiave, è possibile garantire che la chiave sia memorizzata in sicurezza nell'hardware di un dispositivo specifico. Questo accorgimento protegge l'origine del video.*

La firma effettiva viene eseguita utilizzando una chiave univoca per il dispositivo, attestata mediante una chiave di attestazione univoca. Il report di attestazione viene allegato all'inizio del flusso e a intervalli periodici, in genere una volta all'ora. Poiché i metadati contengono hash per i singoli fotogrammi, è possibile individuare ogni singolo frame corretto. Per completare la firma, la struttura GOP (Group of Pictures) del video deve essere protetta. Questa operazione viene svolta includendo l'hash del primo I-frame

del GOP successivo nella firma. In questo modo si impediscono tagli non rilevabili o il riordinamento dei fotogrammi. Nell'improbabile eventualità che i fotogrammi vengano persi durante la trasmissione o danneggiati durante l'archiviazione, è possibile segnalarlo allo stesso modo.

6 Glossario

ID dispositivo Axis: certificato univoco con chiavi corrispondenti che può provare l'autenticità di un dispositivo Axis. L'ID dispositivo viene creato in fabbrica Axis e memorizzato nell'archivio chiavi sicuro (keystore). Si basa sullo standard internazionale IEEE 802.1AR (IDevID, Initial Device Identifier), che definisce un metodo per l'identificazione automatica e sicura.

Axis Edge Vault: piattaforma hardware di cybersecurity che protegge il dispositivo Axis. Si basa su solidi moduli di calcolo crittografico (Secure Element e TPM) e sicurezza del SoC (TEE e Secure Boot), combinati con le competenze di Axis nella sicurezza dei dispositivi edge.

Certificato: documento firmato che attesta l'origine e le proprietà di una coppia di chiavi pubblica/privata. Il certificato è firmato da un'autorità di certificazione (CA); se il sistema si fida della CA, si fida anche dei certificati che emette.

Autorità di certificazione (CA): radice di attendibilità di una catena di certificati. Viene utilizzata per provare l'autenticità e la veridicità dei certificati sottostanti.

Common Criteria (CC): standard internazionale per la certificazione della sicurezza dei prodotti IT. Viene anche detto Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408.

FIPS 140: serie di standard di cybersecurity statunitensi utilizzati per approvare i moduli di calcolo crittografico. FIPS (Federal Information Processing Standard) 140 definisce i requisiti di progettazione e implementazione di un modulo crittografico per ridurre i rischi di manomissione.

ROM immutabile (memoria di sola lettura): memoria di sola lettura che archivia in sicurezza le chiavi pubbliche attendibili e il programma utilizzato per confrontare le firme, in modo che non possano essere sovrascritte.

Provisioning: preparazione e attrezzamento di un dispositivo per la rete. Ciò comporta la fornitura al dispositivo dei dati di configurazione e delle impostazioni dei criteri da un punto centrale. Il dispositivo viene fornito con le chiavi e i certificati.

Crittografia a chiave pubblica: sistema di crittografia asimmetrico in cui qualsiasi persona può crittografare un messaggio utilizzando la *chiave pubblica* del destinatario. Utilizzando la *chiave privata*, solo il destinatario può decriptare il messaggio. Può essere utilizzata per crittografare e firmare messaggi.

Secure Boot: funzione che impedisce il caricamento di software non autorizzato durante l'avvio del dispositivo. Secure Boot utilizza un sistema operativo con firma digitale, il quale garantisce che per l'avvio del dispositivo si usi solo software Axis autorizzato.

Secure Element: modulo di calcolo crittografico che offre l'archiviazione basata su hardware e protetta da manomissione delle chiavi private, nonché l'esecuzione sicura delle operazioni crittografiche. A differenza del TPM, le interfacce hardware e software di Secure Element non sono standardizzate ma specifiche per ogni produttore.

Archivio chiavi (keystore) sicuro: ambiente protetto da manomissioni per la protezione delle chiavi private e l'esecuzione sicura di operazioni crittografiche. Impedisce l'accesso non autorizzato e l'estrazione dannosa in caso di violazione di sicurezza. A seconda dei requisiti di sicurezza, un dispositivo Axis può disporre di uno o più moduli di elaborazione crittografica, che forniscono un keystore sicuro protetto da hardware.

SO firmato o sistema operativo con firma digitale: software del dispositivo la cui immagine è stata firmata digitalmente in codice da una parte attendibile. Il sistema operativo firmato è un requisito del processo di avvio sicuro (Secure Boot), per garantire che il dispositivo venga avviato solo da un'immagine software attendibile. Nei prodotti basati su AXIS OS, il dispositivo verifica l'integrità e l'autenticità dell'immagine software del dispositivo prima di eseguire un aggiornamento.

Video con firma: funzione che mantiene e aumenta l'attendibilità del video come prova. Il video con firma autentica il video o ne rileva le manomissioni e viene utilizzato per garantire che sia intatto e riconducibile a una particolare telecamera Axis. Le chiavi di firma dei video risiedono nell'archivio chiavi sicuro del dispositivo Axis.

Transport Layer Security (TLS): standard Internet per la protezione del traffico di rete. Allo standard TLS si deve la "S" (sicuro) di HTTPS.

Trusted Execution Environment (TEE): fornisce l'archiviazione delle chiavi private basata su hardware e protetta da manomissione, nonché l'esecuzione sicura delle operazioni crittografiche. A differenza di Secure Element e TPM, il TEE è un'area protetta e isolata del processore principale del System-on-Chip (SoC).

Trusted Platform Module (TPM): modulo di calcolo crittografico che fornisce l'archiviazione basata su hardware e protetta da manomissione delle chiavi private, nonché l'esecuzione sicura delle operazioni crittografiche. I TPM sono componenti informatici standardizzati a livello internazionale (TPM 1.2, TPM 2.0) e definiti dal *Trusted Computing Group (TCG)*.

Sicurezza zero-trust: approccio moderno alla sicurezza in cui i dispositivi connessi e l'infrastruttura IT (reti, computer, server, servizi cloud e applicazioni) devono identificarsi, convalidarsi e autenticarsi a vicenda per ottenere controlli di sicurezza elevati.

T10190380/IT/M3.5/2404

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