DOCUMENTO TECNICO

Funzionalità di cybersecurity dei dispositivi Axis

— firmware con firma digitale

— Secure Boot

— Axis Edge Vault

— ID dispositivo Axis

— video con firma

Novembre 2021

Sommario

1 Sommario

Questo documento descrive alcune funzionalità dei dispositivi Axis che possono attenuare le minacce informatiche e contrastare tipi di attacchi specifici. Le funzionalità sono:

- firmware con firma digitale
- Secure Boot
- Axis Edge Vault
- ID dispositivo Axis
- video con firma.

Tra le minacce descritte figurano:

- manomissione del firmware
- manomissione della catena di fornitura
- estrazione delle chiavi private
- sostituzione non autorizzata del dispositivo
- manomissione del video.

1.1 Firmware con firma digitale

Il firmware con firma digitale viene implementato dal fornitore del software, che firma l'immagine del firmware con una chiave privata. Quando questa firma è collegata a un firmware, un dispositivo convalida il firmware prima di accettare di installarlo. Se il dispositivo rileva che l'integrità del firmware è compromessa, l'aggiornamento del firmware viene rifiutato.

1.2 Secure Boot

Secure Boot è un processo di avvio costituito da una catena ininterrotta di software crittograficamente convalidati eseguita da una memoria non modificabile (bootrom). Essendo basato sull'uso del firmware firmato, Secure Boot assicura che un dispositivo possa essere avviato solo con firmware autorizzato.

1.3 Axis Edge Vault

Axis Edge Vault è un modulo di calcolo protetto che può essere utilizzato per operazioni crittografiche sui certificati custoditi in sicurezza. Edge Vault è un sistema di archiviazione antimanomissione che consente a ogni dispositivo di proteggere i suoi segreti. È alla base di un'implementazione sicura di funzionalità di protezione più avanzate.

1.4 ID dispositivo Axis

L'ID dispositivo Axis è come un passaporto digitale, unico per ogni dispositivo. È archiviato in sicurezza e in modo permanente in Edge Vault come certificato firmato dal certificato root Axis. L'ID dispositivo Axis è progettato per dimostrare l'origine del dispositivo, introducendo un nuovo livello di attendibilità in tutto il ciclo di vita del prodotto.

1.5 Video con firma

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 un ID dispositivo Axis, custodito in sicurezza in Axis Edge Vault, per aggiungere una firma al flusso video. Quando il video viene riprodotto, il file player indica se il video è intatto o meno. Dunque, il video firmato consente di risalire alla telecamera di origine e verificare che le immagini non sia state manomesse dopo aver lasciato la telecamera.

2 Glossario

Certificato: in crittografia, un certificato è un documento firmato che attesta l'origine e le proprietà di una coppia di chiavi. Il certificato è firmato da un'autorità di certificazione (CA). Se il sistema si fida della CA, si fida anche dei certificati emessi da essa.

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

FIPS: Federal Information Processing Standards, standard emessi negli Stati Uniti dal NIST (National Institute of Standards and Technology) per la codifica e la sicurezza dei dati.

ROM non modificabile: consente di archiviare in sicurezza le chiavi pubbliche attendibili e il programma utilizzati per confrontare le firme, in modo che non possano essere sovrascritti.

Provisioning: il processo di 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.

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

3 Introduzione

Axis adotta le migliori prassi nel settore per la gestione e la reazione alle vulnerabilità di sicurezza sui dispositivi, al fine di ridurre al minimo i rischi informatici per i clienti. Non c'è modo di garantire che i dispositivi e i servizi siano esenti da difetti che possono essere sfruttati per attacchi dannosi. Ciò non vale specificamente per Axis, bensì rappresenta una condizione generale per tutti i dispositivi di rete. Axis può garantire il massimo impegno in tutte le fasi di lavoro per assicurare il minor rischio possibile ai dispositivi e ai servizi Axis.

Per maggiori informazioni sulla sicurezza dei prodotti e le vulnerabilità rilevate, visitare *www.axis.com/support/product-security*. Per maggiori informazioni sulle misure che è possibile intraprendere per ridurre i rischi delle minacce più comuni, scaricare la Axis Hardening Guide dalla stessa pagina.

Questo documento tecnico esamina alcuni attacchi informatici plausibili e spiega come evitarli sui dispositivi Axis. Descrive in modo specifico il firmware con firma digitale e Secure Boot, due funzionalità che possono prevenire la manomissione del firmware e della catena di fornitura. Inoltre, spiega come utilizzare un TPM (Trusted Platform Module) e Axis Edge Vault per proteggere le chiavi private. Axis Edge Vault viene utilizzato per archiviare in modo sicuro l'ID del dispositivo Axis, aumentando il livello di attendibilità dei dispositivi. Axis Edge Vault e l'ID dispositivo Axis consentono anche l'utilizzo di un video firmato, funzionalità che consente di verificare che il video non sia stato manomesso dopo aver lasciato la telecamera.

4 Rilevamento di manomissioni del firmware

Un possibile attacco, che un avversario potrebbe tentare dopo aver fallito altri tentativi di violare il sistema, consiste nel convincere il proprietario a installare applicazioni, firmware o altri moduli software modificati. Il software modificato può includere codice dannoso con uno scopo specifico. La raccomandazione comune è di non installare mai alcun software da un'origine non affidabile al 100%. Nel contesto di un sistema video, può essere presente un "man in the middle" che potrebbe modificare un firmware del dispositivo e indurre gli utenti finali ad installarlo. Non si tratta di un'operazione semplice e l'avversario deve essere molto abile e determinato. Deve comprendere in modo estremamente dettagliato la progettazione del firmware Axis e il funzionamento del firmware su un dispositivo. Tuttavia, tali avversari possono esistere se il valore dell'attacco a un sistema specifico è sufficientemente elevato. La contromisura comune è l'utilizzo del firmware firmato da parte del fornitore del software.

4.1 Firma del firmware

Il firmware firmato è implementato dal fornitore del software, che firma l'immagine del firmware con una chiave privata segreta. Quando questa firma è collegata a un firmware, un dispositivo convalida il firmware prima di accettare di installarlo. Se il dispositivo rileva che l'integrità del firmware è compromessa, l'aggiornamento del firmware viene rifiutato.

Il processo di firma del firmware viene avviato tramite il calcolo di un valore di hash crittografico. Il valore viene quindi firmato con la chiave privata di una coppia di chiavi privata/pubblica prima che la firma sia collegata all'immagine del firmware.

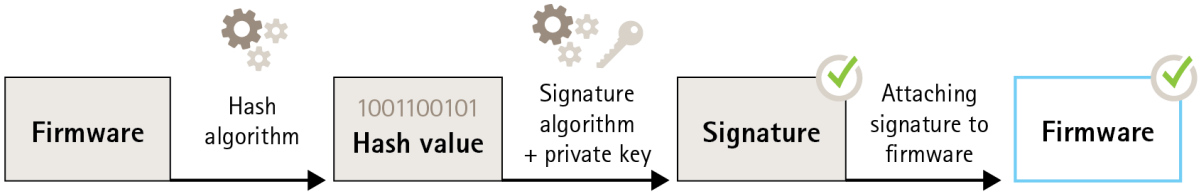

Figure 1. Il processo di firma del firmware.

Prima di un aggiornamento del firmware, è necessario verificare il nuovo firmware. Per assicurarsi che il nuovo firmware non sia stato modificato, viene utilizzata 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 del firmware e confrontandolo con il valore hash convalidato dalla firma, è possibile verificare l'integrità del firmware.

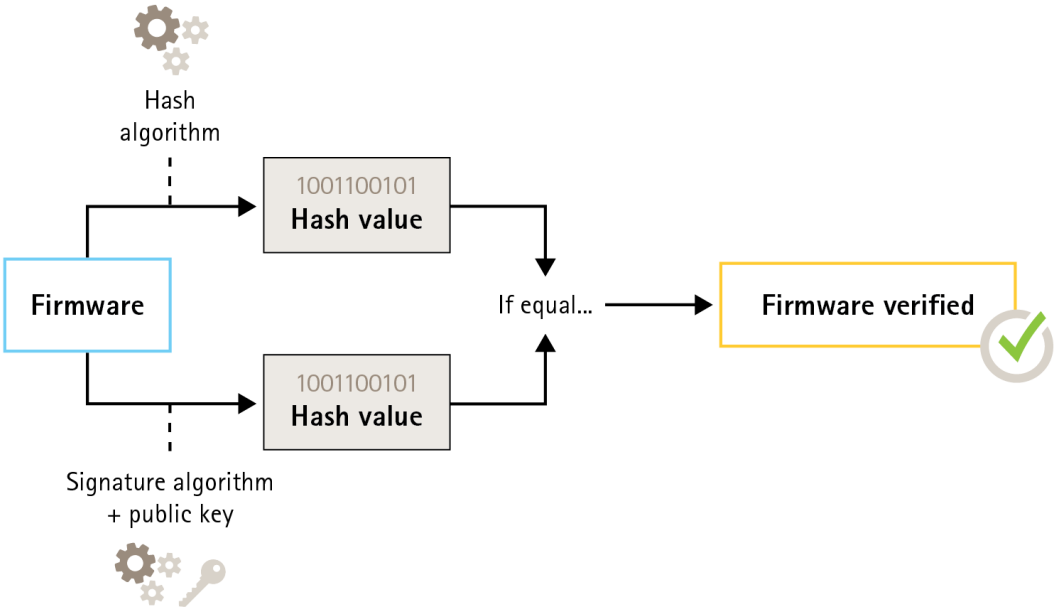

Figure 2. Il processo di verifica del firmware firmato.

4.2 Firmware firmato di Axis

Il firmware con firma digitale Axis si basa sul metodo di crittografia a chiave pubblica RSA consolidato nel 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 firmware è garantita da una firma del contenuto dell'immagine. Una firma principale verifica diverse firme secondarie; la verifica avviene mentre l'immagine viene scompattata.

5 Prevenzione della manomissione della catena di fornitura

La firma del firmware protegge un dispositivo, in tutti i futuri aggiornamenti del firmware, dall'installazione di un firmware compromesso. Ma cosa succede se un "man in the middle" altera il dispositivo durante il tragitto dal fornitore all'utente finale? Un avversario che abbia fisicamente accesso al dispositivo durante il transito potrebbe eseguire un attacco, ad esempio compromettendo la partizione di avvio del dispositivo, aggirando il controllo dell'integrità del firmware per installare un firmware alterato e dannoso prima che il dispositivo venga distribuito.

5.1 Secure Boot

Secure Boot è un processo di avvio costituito da una catena ininterrotta di software crittograficamente convalidati eseguita da una memoria non modificabile (bootrom). Essendo basato sull'uso del firmware firmato, Secure Boot assicura che un dispositivo possa essere avviato solo con firmware 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 blocco di firmware caricato dalla memoria flash. La bootrom funge da radice attendibile 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.

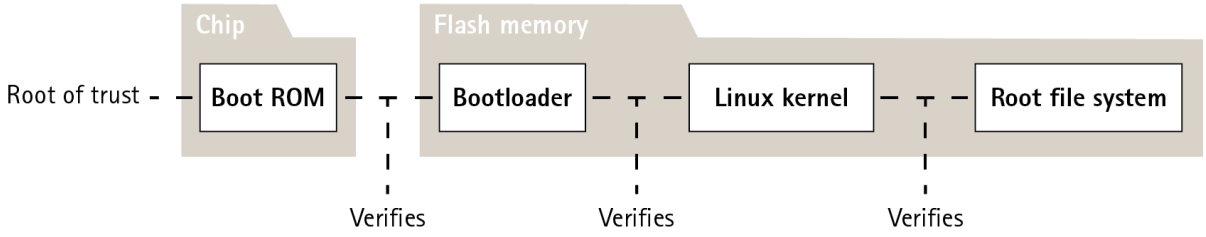

Figure 3. Il processo di avvio sicuro.

5.2 Axis Secure Boot

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 firmware installato nella memoria flash è protetto dalla modifica. L'immagine predefinita di fabbrica è protetta, mentre la configurazione rimane non protetta. Secure Boot garantisce che il dispositivo Axis sia completamente privo di eventuali malware dopo un ripristino delle impostazioni di fabbrica.

5.3 Secure Boot e certificati firmware personalizzati

Sebbene la funzione Secure Boot renda il dispositivo più sicuro, riduce anche la flessibilità con firmware diversi; dunque, è più complicato caricare sul dispositivo qualsiasi firmware temporaneo, ad esempio firmware di prova o altro firmware personalizzato da Axis. Tuttavia, Axis ha implementato un meccanismo che autorizza singole unità ad accettare tale firmware non di produzione. Questo firmware è firmato in modo diverso, con l'approvazione sia del proprietario che di Axis, e dà come risultato un certificato firmware personalizzato. Se installato sulle unità approvate, il certificato consente l'uso di un firmware personalizzato che può essere eseguito solo sull'unità approvata, in base al numero seriale univoco e all'ID del chip. I certificati firmware personalizzati possono essere creati solo da Axis, che possiede la chiave per firmarli.

6 Segreti protetti dalle manomissioni

Un requisito di base di ogni sistema distribuito protetto è la possibilità di verificare i collegamenti e impedire l'intercettazione. Per questo, ogni dispositivo deve proteggere i suoi segreti utilizzando un sistema di archiviazione sicuro antimanomissione. Axis Edge Vault è un sistema di questo tipo e, in base a queste premesse, consente di implementare funzionalità di sicurezza più avanzate.

6.1 ID dispositivo Axis

Durante la produzione di ogni dispositivo di rete Axis, un "passaporto digitale" denominato ID dispositivo Axis è installato in modo sicuro nell'Axis Edge Vault dell'unità. Questa identità è univoca per ogni unità ed è concepita per dimostrarne l'origine. L'ID dispositivo Axis è un insieme di certificati utilizzato nella parte relativa all'operazione di crittografia del modulo per segnalare i problemi presentati dal firmware incorporato del dispositivo a Edge Vault. La risposta da questa operazione viene rispedita al destinatario, che può utilizzare le chiavi pubbliche Axis per convalidare l'autenticazione della risposta.

Un certificato è una piccola porzione di dati che combina una chiave pubblica, e i metadati che descrivono la chiave, con una firma dell'emittente che attesta la validità del certificato. Una gerarchia dei certificati è un modo per dimostrare la provenienza del certificato.

Facciamo un'analogia tra l'ID dispositivo Axis e un passaporto. Se avete un passaporto, il governo del vostro paese garantisce che voi e l'individuo indicato sul passaporto siete davvero la stessa persona. In modo analogo, tutti i certificati ID dispositivo Axis sono avallati da un Certificato CA root per ID dispositivo. Proprio come un agente doganale confida che il governo del vostro paese abbia emesso correttamente il

passaporto, un sistema di sicurezza di rete confida che il Certificato CA root dell'ID dispositivo Axis abbia verificato correttamente un certificato Axis dell'unità connessa alla rete.

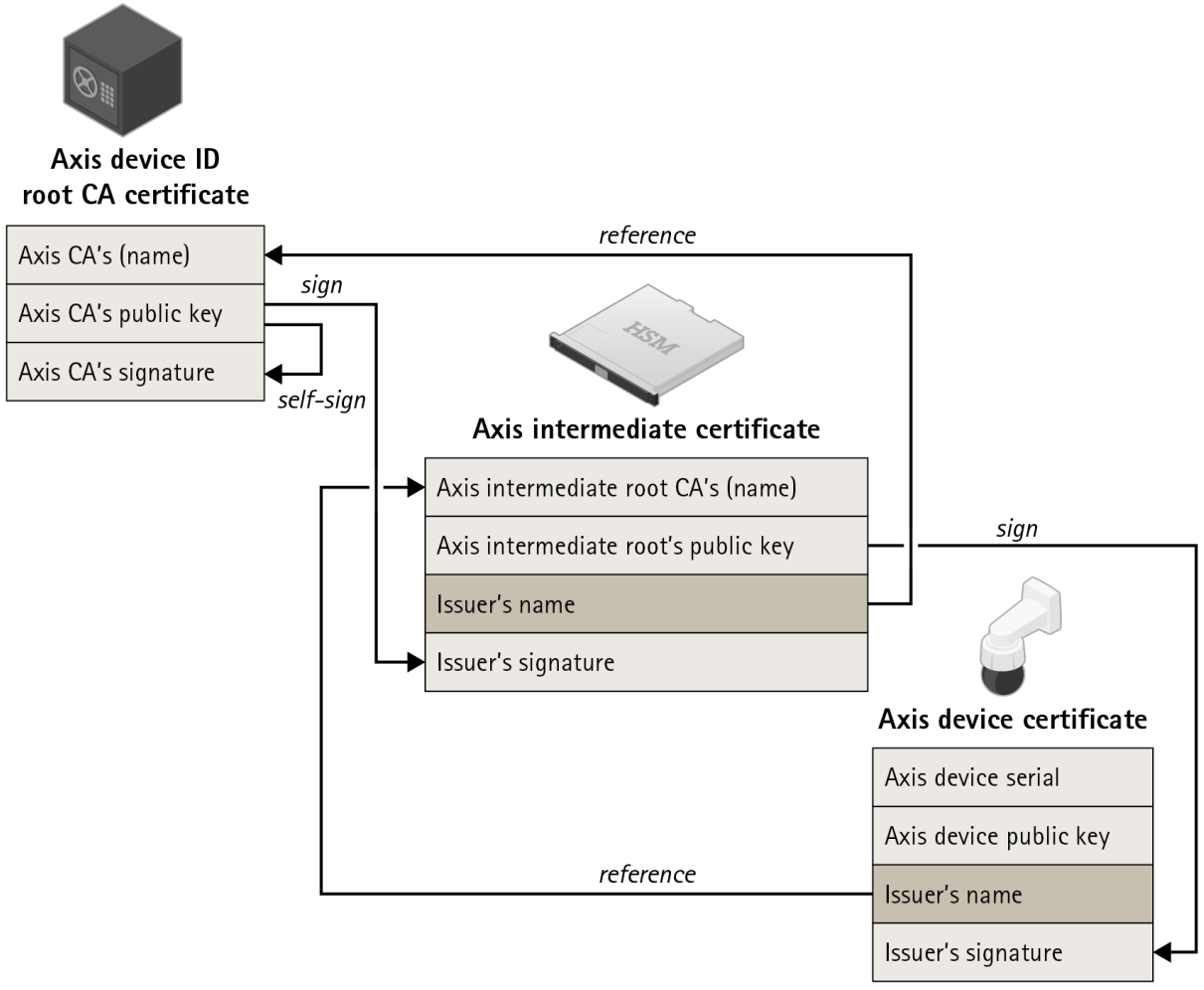

Figure 4. L'ID dispositivo Axis, che è un certificato che incorpora il numero di serie del prodotto, è firmato da un certificato intermedio firmato dal certificato root Axis. Poiché il certificato root Axis è molto prezioso e deve essere custodito in cassaforte, è necessario il certificato intermedio durante il provisioning in fabbrica.

7 Archiviazione sicura delle chiavi

I dispositivi Axis supportano HTTPS (crittografia di rete) e 802.1X (controllo degli accessi di rete), che utilizzano TLS (Transport Layer Security). I certificati digitali di TLS utilizzano una coppia di chiavi pubblica/privata. La chiave privata viene memorizzata sul dispositivo, mentre la chiave pubblica è inclusa nel certificato. Tenere presente che, se non si utilizza né HTTPS né 802.1X, non esistono chiavi da proteggere.

Un avversario potrebbe tentare di estrarre la chiave privata e il certificato dal dispositivo e installarli su un computer che sta eseguendo un attacco. Nel caso di HTTPS, la chiave privata potrebbe essere utilizzata per intercettare un traffico di rete crittografato tra il dispositivo e il software di gestione video (VMS). Oppure, in caso di spoofing, il computer che attacca potrebbe avere accesso al VMS fingendo di essere un dispositivo legittimo. Nel caso di 802.1X, l'avversario potrebbe utilizzare la chiave privata per accedere a una rete protetta da 802.1X, fingendosi un dispositivo affidabile.

I certificati e le chiavi private vengono generalmente archiviati nel file system di un dispositivo, protetti dal criterio di accesso all'account e utilizzati nel normale ambiente di calcolo. Nella maggior parte dei casi, basta questo per far sì che l'account non sia facilmente compromesso. Si noti che i certificati possono essere revocati se si sospetta che siano stati compromessi, rendendo inutile la chiave privata.

Alcuni utenti finali di sistemi critici potrebbero rischiare di più di incontrare avversari determinati e qualificati che tentano di violare il dispositivo per estrarre la chiave privata. Axis Edge Vault può essere utilizzato per memorizzare la chiave in modo tale che sia quasi impossibile estrarla, anche se il dispositivo è compromesso.

7.1 Archiviazione sicura dei certificati con Axis Edge Vault

Axis Edge Vault è un modulo di calcolo crittografico sicuro in forma di chip montato sul PCB all'interno del dispositivo. Edge Vault offre la possibilità di archiviare in modo sicuro i certificati e può essere utilizzato per le operazioni di crittografia su certificati archiviati in modo sicuro.

Non è necessario spostare i certificati archiviati in Edge Vault da quest'ultimo perché possano essere utilizzati dal dispositivo. Permangono in modo sicuro su Edge Vault anche quando vengono utilizzati, poiché l'hardware di crittografia che funziona sulla chiave è installato sullo stesso chip fisico.

7.2 Archiviazione sicura delle chiavi con un TPM (Trusted Platform Module)

Un TPM è un componente che fornisce un determinato set di funzioni di crittografia adatte a proteggere le informazioni dagli accessi non autorizzati. La chiave privata viene memorizzata nel TPM e non lo lascia mai. Tutte le operazioni di crittografia che richiedono l'utilizzo della chiave privata vengono inviate al TPM per essere elaborate. In questo modo, la parte segreta del certificato non lascia mai l'ambiente sicuro all'interno del TPM e rimane protetta anche in caso di violazioni di sicurezza.

7.3 Certificazione FIPS 140-2

Per alcuni prodotti e aree di applicazione, potrebbe essere obbligatorio utilizzare un TPM per proteggere le informazioni, talvolta in combinazione con un requisito di conformità FIPS 140-2. FIPS (Federal Information Processing Standard) 140-2 è uno standard di sicurezza informatica per moduli crittografici emesso negli Stati Uniti dal NIST (National Institute of Standards and Technology).

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 crittografia, degli algoritmi approvati, delle modalità di funzionamento approvate e dei test di accensione.

Per maggiori informazioni sui requisiti di certificazione FIPS 140-2, visitare il sito del NIST: *www.nist.gov*

7.3.1 TPM certificato sui dispositivi Axis

Il TPM utilizzato su alcuni prodotti Axis è certificato per soddisfare i requisiti FIPS 140-2. Nello specifico, è certificato al livello di sicurezza 2 dello standard, ovvero soddisfa anche altri requisiti per l'autorizzazione basata sui ruoli e l'antimanomissione.

8 IEEE 802.1AR - verifica del dispositivo con l'ID dispositivo Axis

Un utente che acquista un dispositivo di rete Axis può esaminarlo manualmente prima di iniziare a utilizzarlo. Ispezionando visivamente il dispositivo e basandosi sull'aspetto dei dispositivi Axis precedenti, il cliente può convincersi che il dispositivo abbia davvero avuto origine da Axis. Tuttavia, questo controllo può essere eseguito solo da una persona che ha fisicamente accesso al dispositivo. Ma quando si comunica in rete con un dispositivo per il quale non è stato effettuato il provisioning, come si può essere certi di comunicare con l'unità giusta, o che il dispositivo non sia stato sostituito senza autorizzazione? Né le apparecchiature di rete né il software sui server possono eseguire un'ispezione fisica. Come misura di sicurezza, la prima volta che si interagisce con un nuovo dispositivo si utilizza una rete chiusa, dove il provisioning dell'unità può avvenire in modo protetto.

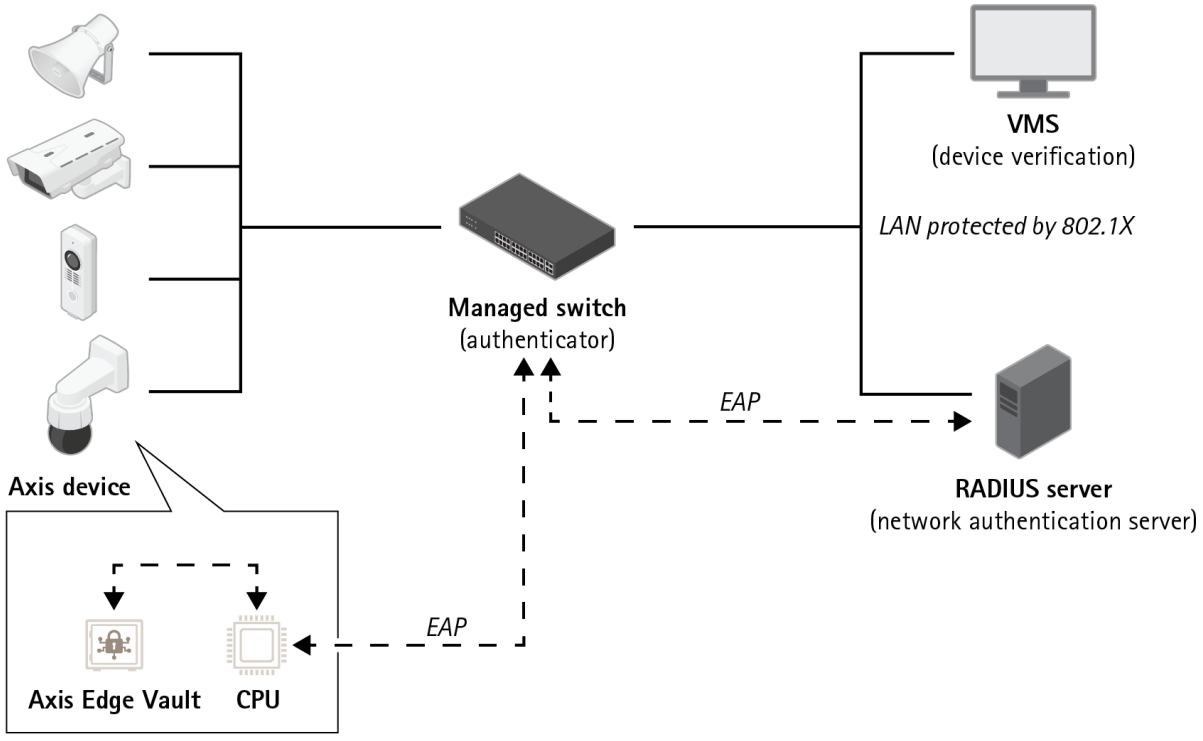

Figure 5. I clienti possono istruire il server di autenticazione perché ammetta automaticamente sulla rete i dispositivi Axis acquistati utilizzando i numeri di serie dei dispositivi e l'ID dispositivo Axis.

Il nuovo standard internazionale IEEE 802.1 AR (*https://1.ieee802.org/security/802-1ar/*) definisce un metodo per la modalità di automazione e protezione dell'identificazione di un dispositivo su una rete. Se la

comunicazione viene inoltrata in un modulo di protezione incorporato, l'unità può restituire una risposta di identificazione affidabile in base allo standard.

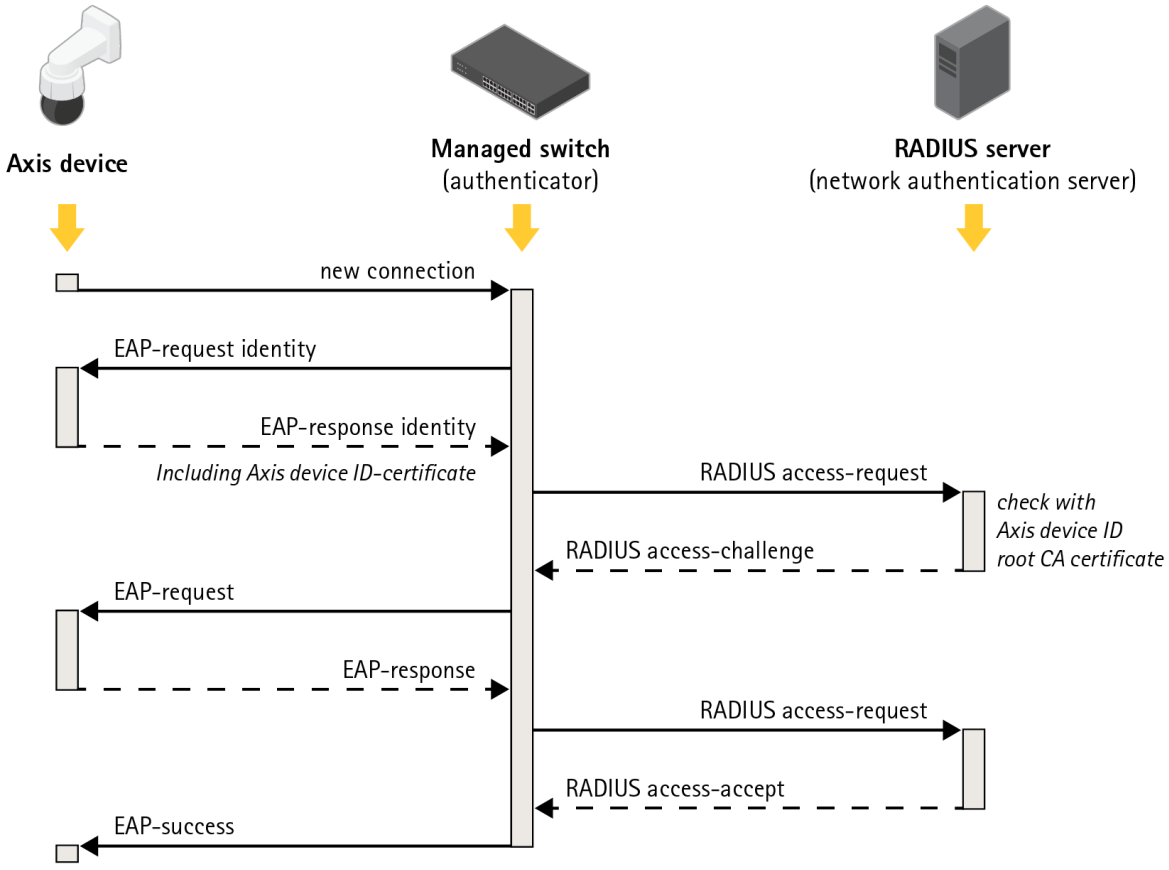

Figure 6. IEEE 802.1AR definisce un metodo per identificare un dispositivo su una rete seguendo un protocollo che invia le richieste di protocollo EAP (Extensible Authentication Protocol) allo switch, che utilizza richieste RADIUS (Remote Authentication Dial-in User Service) per concedere l'accesso.

Sui prodotti Axis, queste misure di sicurezza vengono implementate utilizzando Axis Edge Vault e l'ID dispositivo Axis. Axis Edge Vault è un modulo sicuro su cui è installato l'ID dispositivo Axis, una raccolta di certificati che consente di verificare le informazioni sul dispositivo. Queste funzionalità forniscono alla rete la prova crittograficamente verificabile che un'unità specifica è stata prodotta da Axis e che la connessione di rete all'unità è effettivamente fornita da quell'unità.

Un prodotto con ID dispositivo Axis è stato sottoposto a provisioning in fabbrica (con chiavi e certificati). Il provisioning può essere utilizzato in seguito da un cliente per dotare ulteriormente il dispositivo sul campo di altre chiavi e/o certificati, consentendo di accedere ad alcune risorse di rete del cliente.

Identificando l'unità con l'ID dispositivo Axis, è possibile ridurre il tempo di distribuzione dei dispositivi, poiché ci sono meno operazioni da eseguire con il dispositivo prima di installarlo e configurarlo sulla rete

desiderata. Un altro vantaggio è che l'ID dispositivo Axis, oltre a fornire un'ulteriore fonte di attendibilità integrata, è anche un mezzo per tenere traccia dei dispositivi in un sistema di grandi dimensioni.

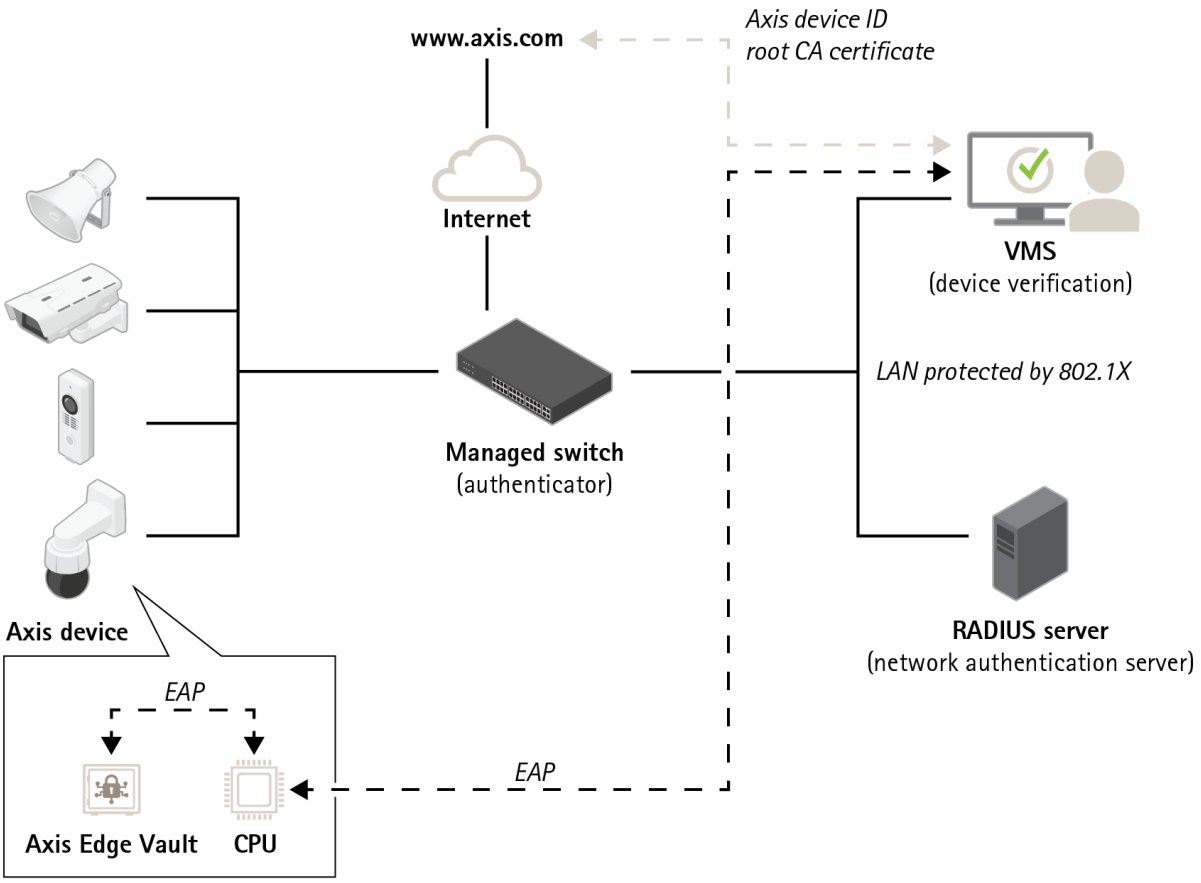

Figure 7. Le applicazioni software in altre parti del sistema possono utilizzare l'ID dispositivo Axis e le operazioni di crittografia per verificare con chi sta comunicando. L'ID dispositivo Axis è stato verificato dal certificato CA root pubblico dell'ID dispositivo Axis di axis.com.

9 Rilevamento di 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.

9.1 Video con firma

Con la funzionalità di video con firma Axis, 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 estrarre il video esportandolo 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.

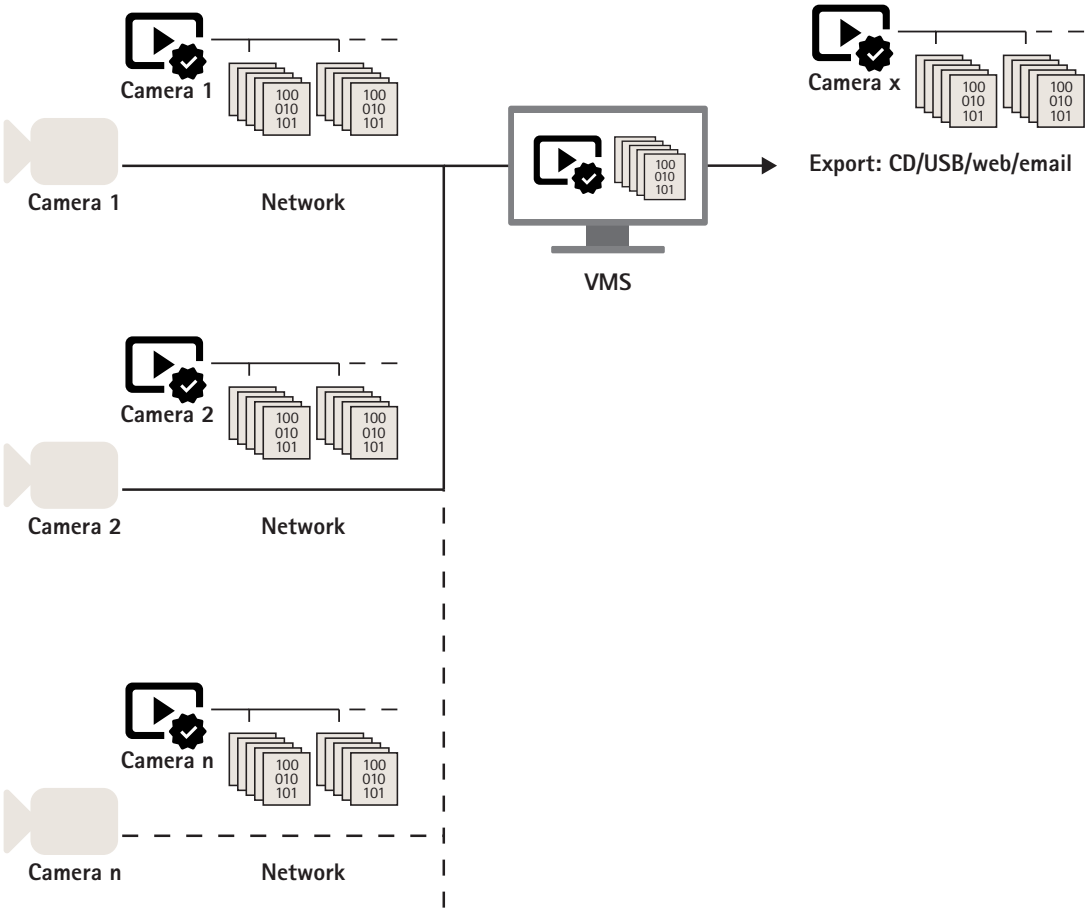

Figure 8. La firma viene aggiunta già sulla telecamera, consentendo la verifica dei contenuti in ogni fase: dalla sorgente sino all'utilizzo finale del video.

Ogni telecamera utilizza un ID dispositivo Axis in Axis Edge Vault 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 in Edge Vault. Quindi, la firma viene memorizzata nel flusso in campi dedicati dei metadati (intestazione SEI).

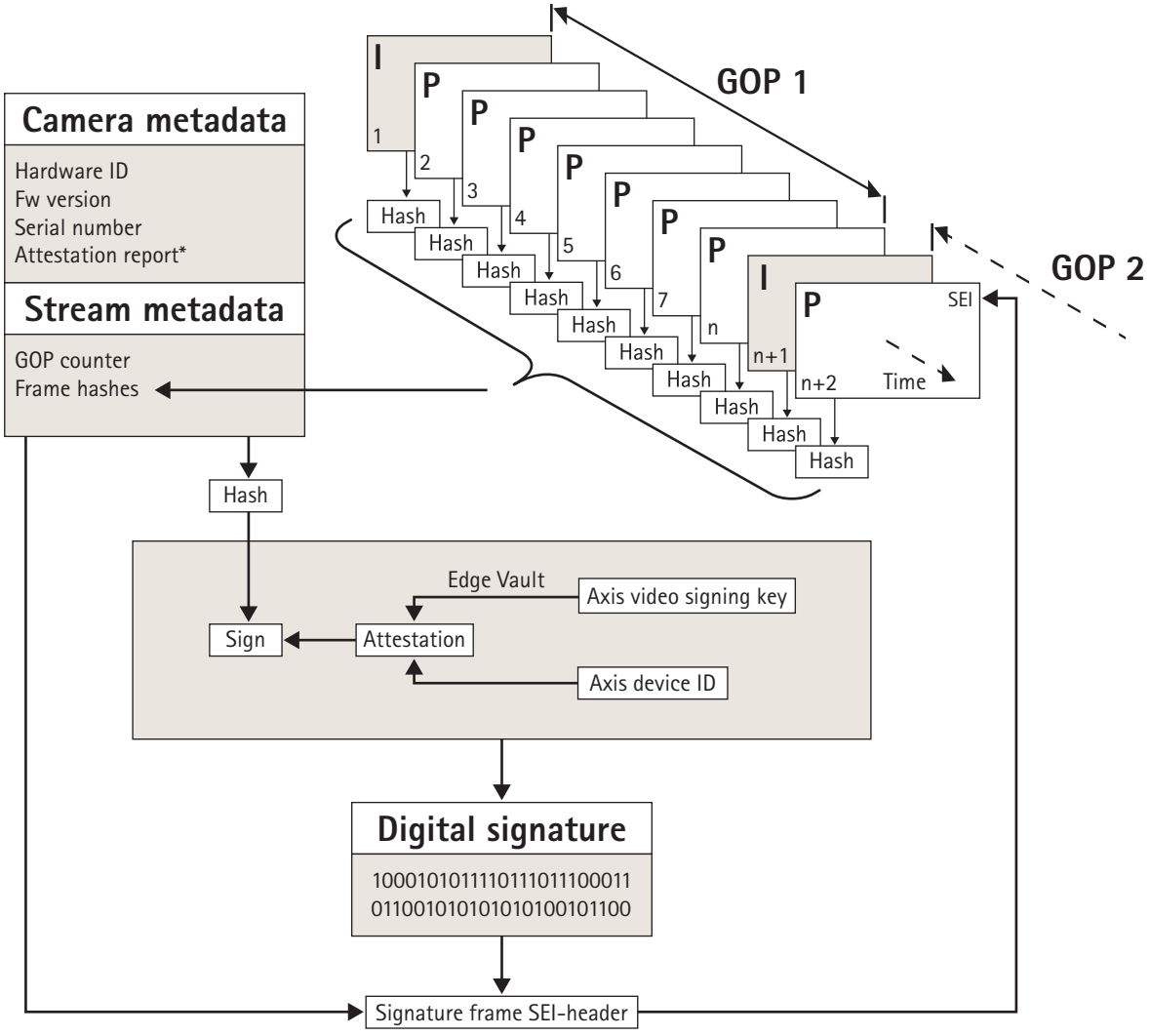

Figure 9. Ai metadati video viene aggiunta una rappresentazione grafica di come è stata aggiunta la firma. Il contenuto di ogni fotogramma di un GOP viene elaborato insieme a un hash di metadati della telecamera e metadati di flusso. Questo forma l'hash GOP, che viene firmato in Edge Vault. La firma e i metadati vengono quindi aggiunti a un'intestazione SEI successiva che viene trasportata insieme al flusso.

* *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 di firma video specifica per unità, che viene attestata dall'ID dispositivo univoco per ogni prodotto Axis. Il report di attestazione viene allegato al flusso all'inizio e a intervalli periodici, normalmente 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 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. Seppur molto improbabili, eventuali perdite di fotogrammi durante lo streaming o danni al contenuto durante l'archiviazione vengono segnalati allo stesso modo.

T10154694/IT/M3.2/2111

Informazioni su Axis Communications

Axis consente un mondo più intelligente e più sicuro creando soluzioni di rete che forniscono informazioni per migliorare la sicurezza e nuovi modi di condurre un'attività. In qualità di leader del settore nel video di rete, Axis offre prodotti e servizi per la videosorveglianza e l'analisi, controllo degli accessi, sistemi di citofoni e audio. Axis ha più di 3.800 dipendenti in oltre 50 paesi e collabora con partner di tutto il mondo per fornire soluzioni ai clienti. Axis è stata fondata nel 1984 e la sua sede principale si trova a Lund, in Svezia.

Per ulteriori informazioni su Axis, si prega di visitare il nostro sito Web *axis.com*.