Firmware firmato, avvio sicuro e sicurezza delle chiavi private

Caratteristiche di sicurezza informatica dei dispositivi Axis

Luglio 2020

Indice

1 **Riepilogo** 3

1.1 Firmware firmato 3

1.2 Avvio sicuro 3

1.3 TPM 3

1.4 Axis Edge Vault con ID dispositivo Axis 3

2 **Glossario** 4

3 **Introduzione** 5

4 **Rilevamento manomissione del firmware** 5

4.1 Firma del firmware 5

4.2 Firmware firmato di Axis 6

5 **Prevenzione manomissione della catena di fornitura** 7

5.1 Avvio sicuro 7

5.2 Avvio sicuro Axis 7

5.3 Avvio sicuro e certificati firmware personalizzati 8

6 **Sicurezza delle chiavi private** 8

6.1 Archiviazione sicura delle chiavi con un TPM (Trusted Platform Module) 8

6.2 Certificazione FIPS 140-2 8

7 **IEEE 802.1AR - verifica dispositivo con l'ID dispositivo Axis** 9

7.1 Axis Edge Vault 12

7.2 ID dispositivo Axis 12

1 Riepilogo

Questo documento descrive alcune delle funzionalità disponibili nei dispositivi Axis che possono attenuare le minacce cibernetiche e contrastare tipi di attacchi specifici. Le funzionalità sono:

- firmware firmato
- avvio sicuro
- Trusted Platform Module (TPM)
- Axis Edge Vault con ID dispositivo Axis.

Le minacce descritte includono:

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

1.1 Firmware firmato

Il firmware firmato 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 convaliderà il firmware prima di accettare di installarlo. Se il dispositivo rileva che l'integrità del firmware è compromessa, l'aggiornamento del firmware verrà rifiutato.

1.2 Avvio sicuro

L'avvio sicuro 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, l'avvio sicuro assicura che un dispositivo possa essere avviato solo con firmware autorizzato.

1.3 TPM

Un TPM è un componente che fornisce un set di funzioni di crittografia adatte alla protezione delle informazioni da accessi non autorizzati. Le chiavi private vengono memorizzate nel TPM e 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 rimane protetta anche in caso di violazione della sicurezza. Il TPM utilizzato nei dispositivi Axis selezionati è certificato per soddisfare i requisiti di FIPS 140-2.

1.4 Axis Edge Vault con ID dispositivo Axis

Il nuovo standard internazionale IEEE 802.1AR descrive una procedura per la modalità di automazione e protezione dell'identificazione di un dispositivo su una rete. Nei dispositivi Axis, queste misure di sicurezza vengono implementate mediante l'uso di Axis Edge Vault e dell'ID dispositivo Axis. Edge Vault può essere utilizzato per i problemi di crittografia quando si lavora su certificati archiviati in modo sicuro. La parte privata dei certificati rimane in Edge Vault anche quando viene utilizzata. L'ID dispositivo Axis è

memorizzato in modo sicuro e permanente in Edge Vault come certificato firmato dal certificato root di Axis e ciò consente un nuovo livello di attendibilità dei dispositivi per tutta la durata del dispositivo.

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) e se il sistema si fida della CA, si fiderà anche dei certificati emessi da essa.

Autorità di certificazione, CA: la radice di attendibilità per 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: per 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 attrezzaggio 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: un sistema di crittografia asimmetrico in cui qualsiasi persona può crittografare un messaggio utilizzando la *chiave pubblica* del destinatario, ma solo il destinatario, utilizzando la *chiave privata*, può decriptare il messaggio. Può essere utilizzata per crittografare e firmare i messaggi.

TLS: Transport Layer Security, standard Internet per la protezione del traffico di rete. TLS fornisce la S (di sicurezza) all'HTTPS.

3 Introduzione

Axis segue le migliori prassi nel settore per la gestione e la reazione alle vulnerabilità della sicurezza nei nostri dispositivi al fine di ridurre al minimo i rischi di sicurezza informatica 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 è una caratteristica specifica di Axis, bensì rappresenta una condizione generale per tutti i dispositivi di rete. Axis può garantire che facciamo sempre uno sforzo concertato in tutte le fasi possibili per garantire che il minor rischio possibile sia associato ai dispositivi e ai servizi Axis.

Per ulteriori informazioni sulla sicurezza del dispositivo e le vulnerabilità rilevate, vedere *www.axis.com/support/product-security*. Per ulteriori informazioni sulle misure che è possibile adottare per ridurre i rischi di minacce comuni, scaricare la Guida alla protezione Axis da *www.axis.com/cybersecurity*.

Questo white paper presenta alcuni attacchi cibernetici plausibili e il modo in cui possono essere evitati nei dispositivi Axis. Descrive in modo specifico come le funzionalità firmware firmato e avvio sicuro possono prevenire la manomissione del firmware e della catena di fornitura. Si discute anche l'uso di un TPM (Trusted Platform Module) e di Axis Edge Vault, che possono essere utilizzati per proteggere le chiavi private. Axis Edge Vault viene utilizzato per archiviare in modo sicuro l'ID dispositivo Axis, che consente un nuovo livello di attendibilità dei dispositivi.

4 Rilevamento manomissione del firmware

Un possibile vettore di attacco che un avversario potrebbe tentare di sfruttare dopo aver fallito con altri tentativi di violare il sistema consiste nel convincere il proprietario del sistema 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%. In un contesto di 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. Ha bisogno di una comprensione estremamente dettagliata della progettazione del firmware Axis e del funzionamento del firmware in un dispositivo. Tuttavia, tali avversari possono esistere se il valore dell'attacco di 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 mantenuta segreta. Quando questa firma è collegata a un firmware, un dispositivo convaliderà il firmware prima di accettare di installarlo. Se il dispositivo rileva che l'integrità del firmware è compromessa, l'aggiornamento del firmware verrà 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.

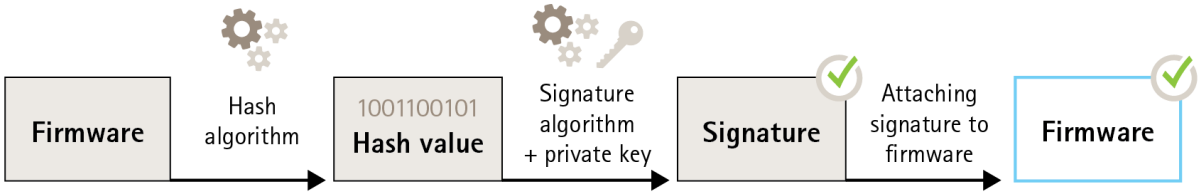

Figure 1. Il processo di firma del firmware.

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 di hash del firmware e confrontandolo con questo valore hash convalidato dalla firma, è possibile verificare l'integrità del firmware.

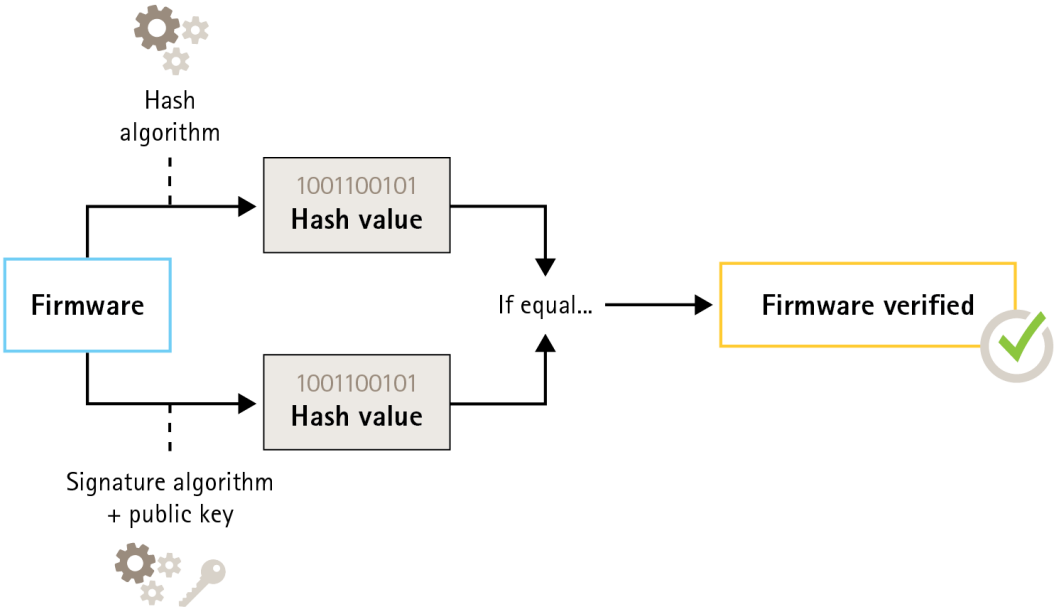

Figure 2. Il processo di verifica del firmware firmato.

4.2 Firmware firmato di Axis

Il firmware firmato di Axis si basa sul metodo di crittografia a chiave pubblica RSA accettato dal settore. La chiave privata viene memorizzata in un'ubicazione strettamente sorvegliata presso Axis mentre la chiave

pubblica è incorporata nei 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 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 tra il fornitore e l'utente finale? Un avversario che abbia accesso fisico 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 Avvio sicuro

L'avvio sicuro 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, l'avvio sicuro assicura che un dispositivo possa essere avviato solo con firmware autorizzato.

Il processo di avvio viene avviato dalla bootrom che convalida il bootloader. L'avvio sicuro quindi 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.

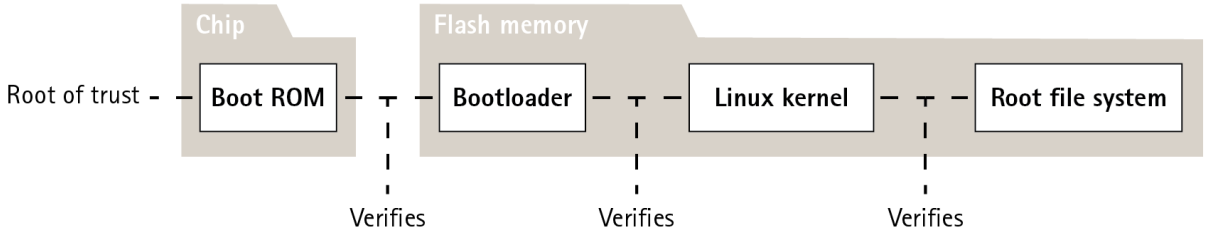

Figure 3. Il processo di avvio sicuro.

5.2 Avvio sicuro Axis

In molti dispositivi, è importante che la funzionalità di basso livello sia impossibile da modificare. Quando altri meccanismi di sicurezza sono costruiti al di sopra del software di livello inferiore, l'avvio sicuro funge da livello di base sicuro che impedisce che quei meccanismi siano aggirati.

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

5.3 Avvio sicuro e certificati firmware personalizzati

Sebbene l'avvio sicuro renda il dispositivo più sicuro, riduce anche la flessibilità con firmware diversi, rendendo più complicato caricare nel 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 risulta in un certificato firmware personalizzato. Se installato nelle unità approvate, il certificato consente l'utilizzo di un firmware personalizzato che può essere eseguito solo sull'unità approvata, in base al numero di serie e all'ID del chip univoci. I certificati firmware personalizzati possono essere creati solo da Axis, poiché Axis detiene la chiave per firmarli.

6 Sicurezza delle chiavi private

I dispositivi Axis supportano HTTPS (crittografia di rete) e 802.1X (controllo degli accessi di rete), entrambi utilizzano TLS (Transport Layer Security). I certificati digitali di TLS utilizzano una coppia di chiavi pubblica/privata. La chiave privata viene memorizzata nel dispositivo mentre la chiave pubblica è inclusa nel certificato. Si noti 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 il traffico di rete criptato tra il dispositivo e il VMS. Oppure, se lo spoofing della rete, il computer che esegue l'attacco 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 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 sperimentare un rischio maggiore di avversari determinati e qualificati che tentano di violare il dispositivo per estrarre la chiave privata. Un TPM (trusted platform module) archivia la chiave in modo che sia quasi impossibile estrarla, anche quando il dispositivo viene compromesso.

6.1 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 alla protezione delle informazioni da accessi non autorizzati. La chiave privata è memorizzata nel TPM e non lascia mai il TPM. Tutte le operazioni di crittografia che richiedono l'uso 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 al sicuro anche in caso di violazione della sicurezza.

6.2 Certificazione FIPS 140-2

Per alcuni dispositivi e casi di utilizzo, può essere un requisito normativo utilizzare un TPM per proteggere le informazioni, talvolta in combinazione con un requisito della conformità a FIPS 140-2. FIPS (Federal Information Processing Standard) 140-2 è uno standard di sicurezza delle informazioni per i moduli di crittografia, rilasciato 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 correttamente implementati. 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.

Ulteriori dettagli sui requisiti di certificazione di FIPS 140-2 possono essere trovati sul sito Web del NIST *https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards*

6.2.1 TPM certificato nei dispositivi Axis

Il TPM utilizzato nei dispositivi Axis selezionati è certificato per soddisfare i requisiti di FIPS 140-2. Più specificamente, è certificato al livello di sicurezza 2 dello standard, il che significa che il TPM soddisfa anche i requisiti per l'autorizzazione basata sui ruoli e le prove di avvenuta manomissione, tra gli altri requisiti.

7 IEEE 802.1AR - verifica dispositivo con l'ID dispositivo Axis

Un utente che acquista un dispositivo di rete Axis può eseguire un esame manuale prima di iniziare a utilizzarlo. Ispezionando visivamente il dispositivo e utilizzando le conoscenze precedenti sull'aspetto dei dispositivi Axis, il cliente può sentirsi convinto che il dispositivo abbia davvero avuto origine da Axis. Tuttavia, questo tipo di controllo può essere eseguito solo da una persona con accesso fisico al dispositivo. Pertanto, quando si comunica su rete con un dispositivo per il quale non è stato effettuato il provisioning, come si può essere certi di comunicare con l'unità giusta? 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, era comune interagire per la prima volta con un nuovo dispositivo su una rete chiusa, dove il provisioning dell'unità può avvenire in sicurezza.

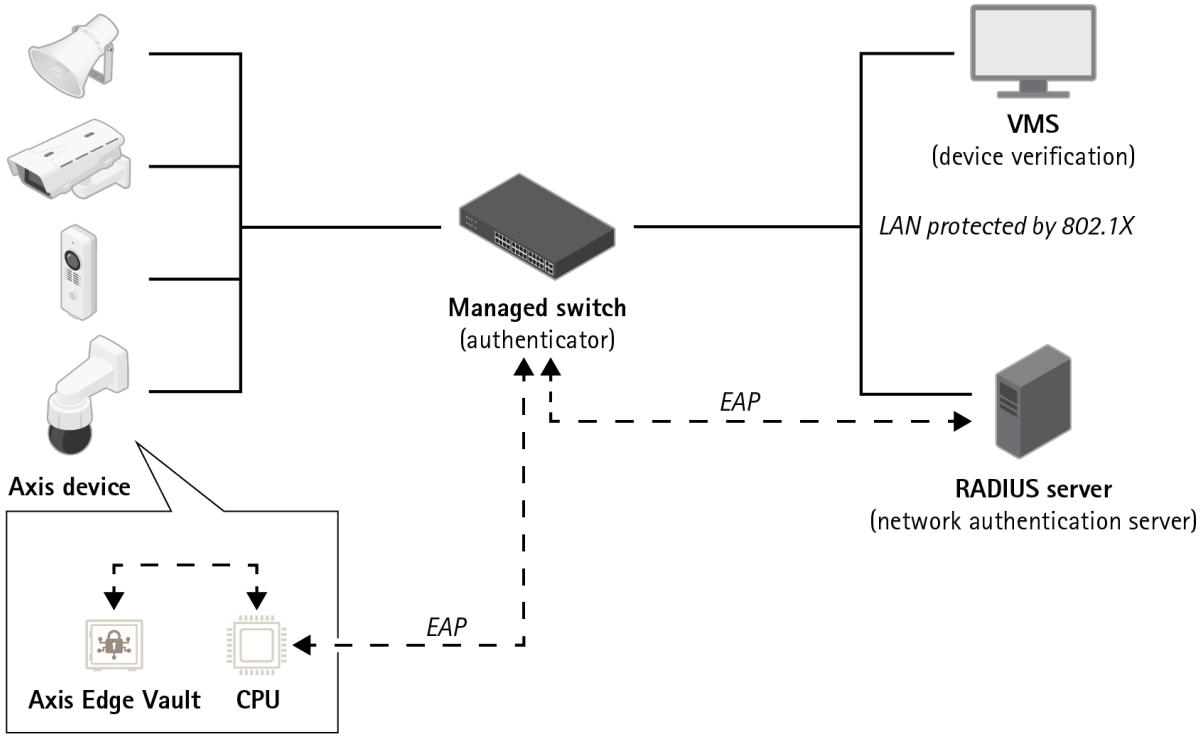

Figure 4. I clienti possono istruire il server di autenticazione perché ammetta automaticamente sulla rete i dispositivi Axis acquistati utilizzando i numeri di serie dei dispositivi e l'ID dispositivo Axis.

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.

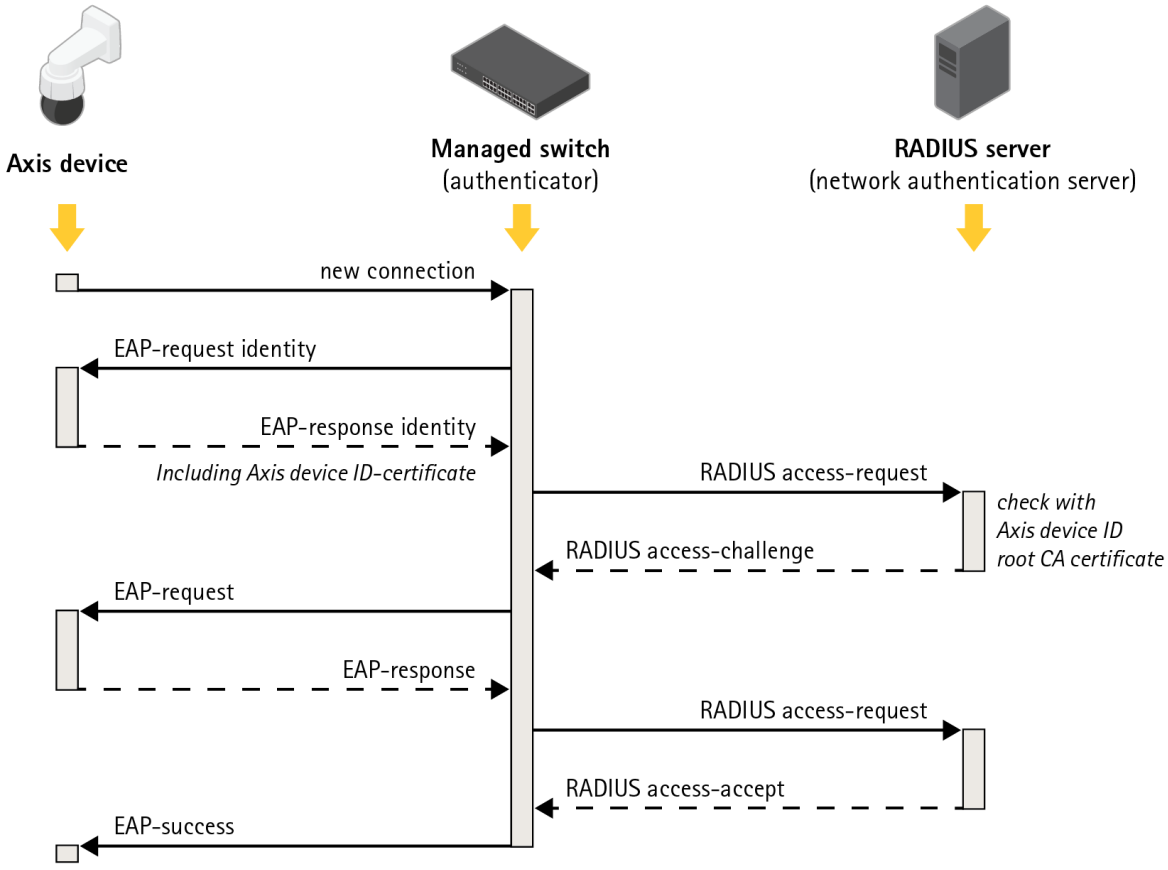

Figure 5. IEEE 802.1AR definisce un metodo per identificare un dispositivo su una rete seguendo un protocollo che invia le richieste di protocollo AEP (Extensible Authentication Protocol) allo switch che utilizza richieste RADIUS (Remote Authentication Dial-in User Service) per concedere l'accesso.

Nei dispositivi Axis, queste misure di sicurezza vengono implementate mediante l'uso di Axis Edge Vault e dell'ID dispositivo Axis. Axis Edge Vault è un modulo sicuro in cui è installato l'ID dispositivo Axis, una raccolta di certificati per verificare l'identificazione del 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 dispositivo con ID dispositivo Axis è stato sottoposto a provisioning in fabbrica (con chiavi e certificati). Questo provisioning può essere successivamente utilizzato 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 che è necessario eseguire con il dispositivo prima di installarlo e configurarlo sulla rete desiderata. Un altro vantaggio è rappresentato dal fatto che l'ID del dispositivo Axis, oltre a fornire un'ulteriore fonte di attendibilità integrata, fornisce anche un mezzo per tenere traccia dei dispositivi in un sistema di grandi dimensioni.

7.1 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 ID dispositivo Axis

Durante la produzione di ogni unità 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 progettata 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.

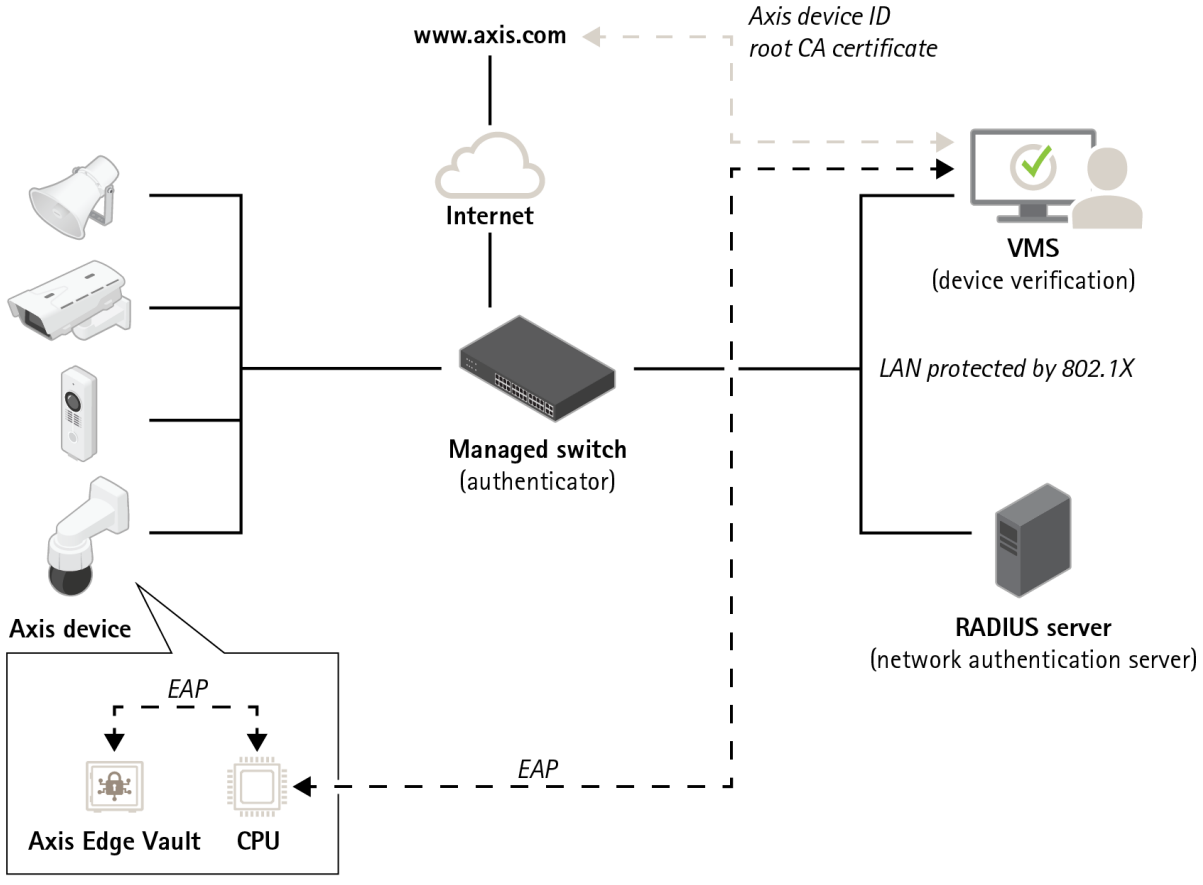

Figure 6. Le applicazioni software in altre parti del sistema possono utilizzare l'ID dispositivo AXIS e le operazioni di crittografia per verificare con chi sta comunicando. L'ID dispositivo Axis è stato verificato dal certificato CA root pubblico dell'ID dispositivo Axis di axis.com.

7.2.1 Gerarchie di certificati

Un certificato è una piccola porzione di dati che combina una chiave pubblica e i metadati che descrivono la chiave insieme a una firma dell'emittente attestante la validità del certificato.

Una gerarchia dei certificati è un modo per dimostrare la provenienza del certificato. Consideriamo 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 nel passaporto siete davvero la stessa persona. In modo analogo, tutti i certificati ID dispositivo Axis sono sostenuti da un Certificato CA root per ID dispositivo. Proprio come un agente doganale confida che il governo del vostro paese abbia correttamente emesso 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.

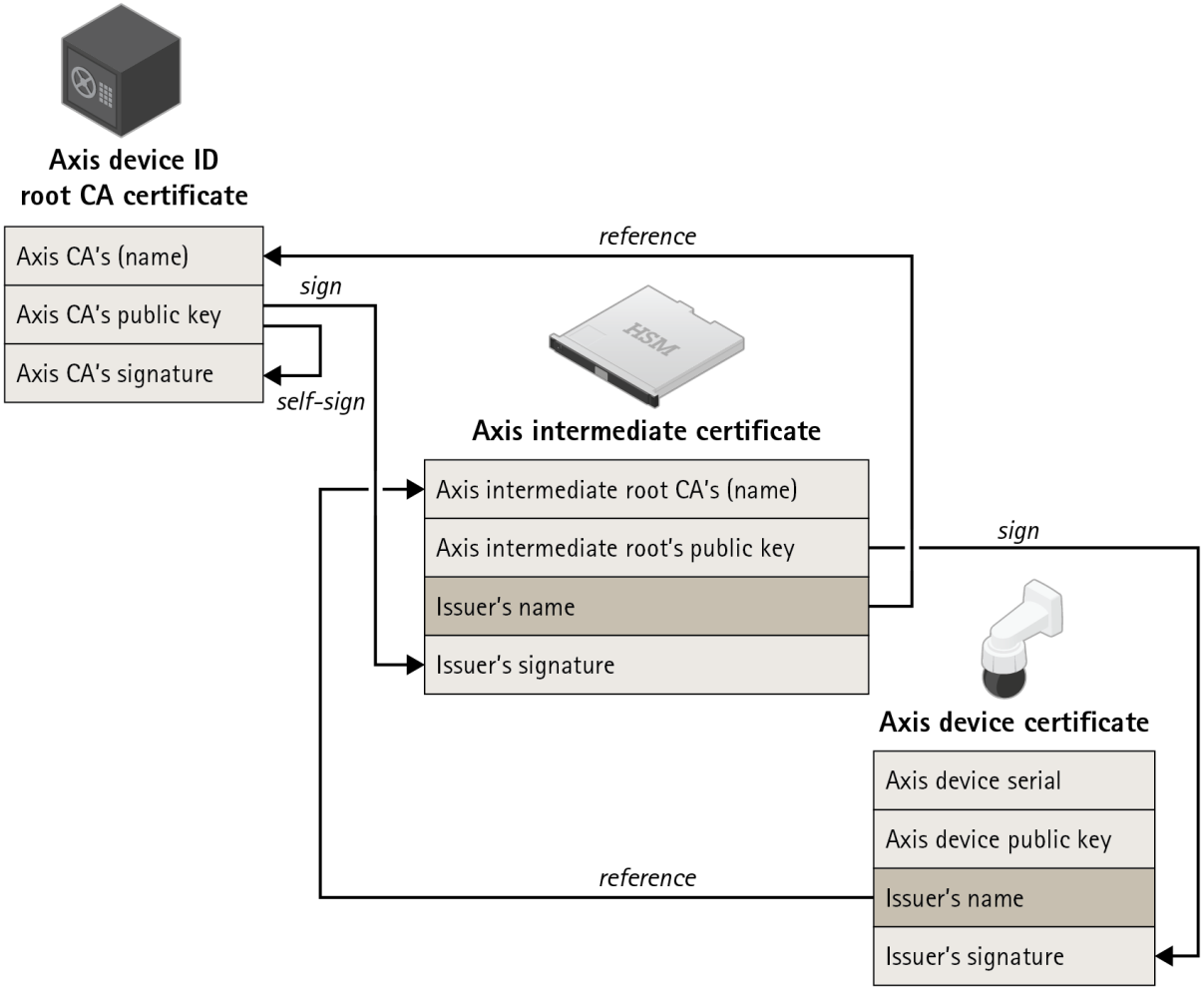

Figure 7. L'ID dispositivo Axis, che è un certificato che incorpora il numero di serie del prodotto, è firmato da un certificato intermedio firmato dal certificato root Axis. Poiché il certificato root Axis è molto prezioso ed è necessario archiviarlo in una cassetta di sicurezza, è necessario il certificato intermedio durante il provisioning in fabbrica.

T10154694/IT/M1.8/2007

Informazioni su Axis Communications

Axis permette di creare un mondo più intelligente e sicuro grazie a soluzioni di rete che migliorano la sicurezza e forniscono nuove opportunità di business. In qualità di leader nel settore dei video di rete, Axis offre prodotti e servizi per la videosorveglianza e l'analisi dei video, il controllo degli accessi e gli impianti audio.

Axis ha oltre 3500 dipendenti in più di 50 paesi e collabora con partner in tutto il mondo per fornire soluzioni ai clienti. Fondata nel 1984, Axis è una società con sede a Lund, in Svezia.

Per ulteriori informazioni su Axis, visitare il sito web *axis.com*.