BIAŁA KSIĘGA

Funkcje cyberbezpieczeństwa w produktach Axis

— oprogramowanie sprzętowe z podpisem

— bezpieczne uruchamianie

— Axis Edge Vault

— ID urządzenia Axis

— wideo z podpisem

Listopad 2021

AXIS COMMUNICATIONS

Spis treści

1 Streszczenie

W tym dokumencie opisano wybrane funkcje produktów Axis, które mogą podnosić poziom cyberbezpieczeństwa i powstrzymywać niektóre rodzaje ataków. Są to następujące funkcje:

- oprogramowanie sprzętowe z podpisem,
- bezpieczny start,
- Axis Edge Vault,
- ID urządzenia Axis,
- wideo z podpisem.

Do zagrożeń potencjalnie powstrzymywanych przez te funkcje należą:

- sabotaż oprogramowania sprzętowego,
- sabotaż łańcucha dostaw,
- wyodrębnianie kluczy prywatnych,
- nieautoryzowana wymiana urządzenia,
- manipulowanie obrazem wideo.

1.1 Oprogramowanie sprzętowe z podpisem

Podpisywanie oprogramowania sprzętowego jest realizowane w ten sposób, że dostawca oprogramowania podpisuje obraz tego oprogramowania za pomocą klucza prywatnego. Urządzenie będzie sprawdzać oprogramowanie sprzętowe na podstawie załączonego podpisu przed zaakceptowaniem jego instalacji. Jeżeli urządzenie wykryje naruszenie integralności oprogramowania sprzętowego, aktualizacja oprogramowania zostanie zablokowana.

1.2 Bezpieczny start

Bezpieczny start to proces składający się z nieprzerwanego łańcucha oprogramowania zweryfikowanego kryptograficznie, rozpoczynający się w pamięci niezmiennej (rozruchowej pamięci ROM). Dzięki wykorzystaniu podpisanego oprogramowania sprzętowego bezpieczny start gwarantuje uruchomienie urządzenia wyłącznie z autoryzowanym oprogramowaniem sprzętowym.

1.3 Axis Edge Vault,

Axis Edge Vault to bezpieczny moduł kryptograficzny, który można stosować do wykonywania operacji kryptograficznych na bezpiecznie przechowywanych certyfikatach. Edge Vault oferuje zabezpieczoną przed manipulacjami pamięć, w której każde urządzenie może chronić swoje sekrety. Stanowi fundament dla bezpiecznej implementacji bardziej zaawansowanych funkcji zabezpieczających.

1.4 ID urządzenia Axis,

ID urządzenia Axis pełni rolę unikalnego cyfrowego paszportu urządzenia. Jest na stałe bezpiecznie przechowywany w module Edge Vault jako certyfikat podpisany certyfikatem głównym firmy Axis. ID

urządzenia Axis dowodzi pochodzenia urządzenia i pozwala osiągnąć nowy poziom zaufania do urządzenia w całym cyklu jego użytkowania.

1.5 Wideo z podpisem

Wideo z podpisem umożliwia potwierdzenie autentyczności dowodu bez konieczności potwierdzenia całego łańcucha pochodzenia pliku wideo. Każda kamera dodaje do strumienia wideo swój niepowtarzalny ID urządzenia Axis, bezpiecznie przechowywany w jej module Axis Edge Vault. W trakcie odtwarzania wideo program odtwarzający informuje o tym, czy materiał jest nienaruszony. Podpis w materiale wideo umożliwia zatem ustalenie, z której kamery ten materiał pochodzi, i wykrycie ewentualnych manipulacji w materiale po tym, jak opuścił on kamerę.

2 Glosariusz

Certyfikat — w kryptografii certyfikat jest podpisanym dokumentem potwierdzającym pochodzenie i właściwości pary kluczy. Certyfikat jest podpisany przez jednostkę certyfikującą (CA) i w przypadku, gdy system ufa jednostce certyfikującej, będzie również ufać wystawionym przez nią certyfikatom.

Jednostka certyfikująca, CA — źródło zaufania do łańcucha certyfikatów. Służy do potwierdzania autentyczności i wiarygodności bazowych certyfikatów.

FIPS — Federal Information Processing Standard, normy szyfrowania i bezpieczeństwa danych wydane w USA przez instytut NIST (National Institute of Standards and Technology).

Niezmienna pamięć ROM — do bezpiecznego przechowywania zaufanych kluczy publicznych i programu służącego do porównywania podpisów, tak aby nie można było ich zmodyfikować.

Obsługa administracyjna — proces przygotowania i wyposażenia urządzenia do pracy w sieci. Wymaga dostarczenia danych o konfiguracji i ustawień zasad z punktu centralnego do urządzenia. Urządzenie jest wyposażone w klucze i certyfikaty.

Kryptografia kluczy publicznych — asymetryczny system kryptograficzny, w którym każda osoba może zaszyfrować wiadomość za pomocą *klucza publicznego* odbiorcy, ale tylko odbiorca — za pomocą *klucza prywatnego* — może odszyfrować wiadomość. Można używać tego systemu do szyfrowania i podpisywania wiadomości.

TLS — Transport Layer Security, internetowy standard ochrony ruchu sieciowego. TLS jest komponentem protokołu HTTPS oznaczonym literą S (secure — bezpieczny).

3 Wprowadzenie

Axis stosuje w swoich produktach najlepsze praktyki branżowe ograniczania podatności i reagowania na ataki — w celu zminimalizowania ekspozycji klienta na zagrożenia cybernetyczne. Nigdy nie ma jednak stuprocentowej gwarancji, że produkty czy usługi będą wolne od wad, które mogą zostać wykorzystane do przeprowadzenia złośliwych ataków. Nie dotyczy to tylko produktów firmy Axis, lecz wszystkich urządzeń sieciowych. Firma Axis może jednak zagwarantować, że na każdym możliwym etapie podejmuje skoordynowane wysiłki, aby zminimalizować ryzyko związane z urządzeniami i usługami Axis.

Więcej informacji na temat zabezpieczeń produktów i wykrytych słabych punktów można znaleźć na stronie *www.axis.com/support/product-security*. Więcej informacji o środkach, jakie użytkownicy mogą podejmować w celu minimalizacji typowych rodzajów ryzyka, zawiera publikacja Axis Hardening Guide, którą można pobrać z tej samej strony.

W publikacji tej opisano prawdopodobne cyberataki i możliwości zapobiegania im w produktach Axis. Wyjaśniono szczegółowo, w jaki sposób podpisane oprogramowanie sprzętowe i bezpieczny start uniemożliwiają sabotaż oprogramowania sprzętowego oraz łańcucha dostaw. Uwzględniono również wykorzystanie modułu TPM (Trusted Platform Module) i Axis Edge Vault — rozwiązań, które można wykorzystać do zabezpieczenia kluczy prywatnych. Axis Edge Vault służy do bezpiecznego przechowywania ID urządzenia Axis, który pozwala na osiągnięcie nowego poziomu zaufania do urządzeń. Axis Edge Vault oraz ID urządzenia Axis pozwalają także na stosowanie wideo z podpisem — funkcji sprawdzającej, czy materiał wideo nie został zmanipulowany po opuszczeniu kamery.

4 Wykrywanie sabotażu oprogramowania sprzętowego

Jednym z możliwych kierunków ataku, potencjalnie stosowanym po niepowodzeniu innych prób złamania zabezpieczeń systemu, jest skłonienie właściciela systemu do zainstalowania zmienionych aplikacji, oprogramowania sprzętowego lub innych modułów oprogramowania. Zmienione oprogramowanie może zawierać szkodliwy kod o określonym przeznaczeniu. Powszechnym zaleceniem jest nieinstalowanie żadnego oprogramowania, które nie pochodzi z całkowicie zaufanego źródła. W kontekście systemu wizyjnego może pojawić się atakujący, który zmieni oprogramowanie sprzętowe urządzenia i nakłoni użytkowników końcowych do jego instalacji. Nie jest to proste, a przeciwnik musi być bardzo dobrze wyszkolony i zdeterminowany. Musi bardzo szczegółowo znać projekt oprogramowania sprzętowego Axis i sposób jego działania w urządzeniu. Jeśli jednak atak na określony system ma wystarczająco wysoką wartość, taki śmiałek może się pojawić. Często stosowanym środkiem zaradczym jest używanie podpisanego oprogramowania sprzętowego.

4.1 Podpisywanie oprogramowania sprzętowego

Podpisywanie oprogramowania sprzętowego jest realizowane w ten sposób, że dostawca oprogramowania podpisuje obraz tego oprogramowania za pomocą klucza prywatnego, który nie jest ujawniany. Urządzenie będzie sprawdzać oprogramowanie sprzętowe na podstawie załączonego podpisu przed zaakceptowaniem jego instalacji. Jeżeli urządzenie wykryje naruszenie integralności oprogramowania sprzętowego, aktualizacja oprogramowania zostanie zablokowana.

Proces podpisywania oprogramowania sprzętowego rozpoczyna się od obliczenia skrótu kryptograficznego. Następnie skrót jest podpisywany kluczem prywatnym z pary klucz prywatny/publiczny, po czym podpis jest dołączany do obrazu oprogramowania sprzętowego.

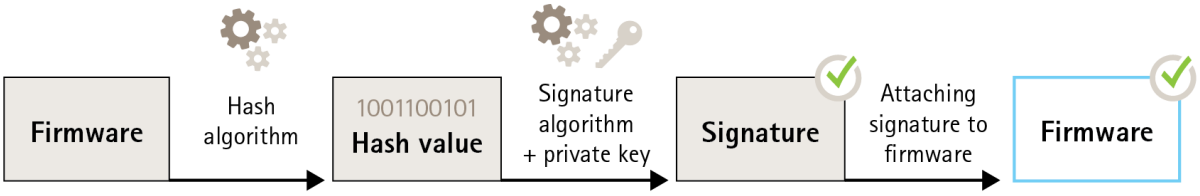

Figure 1. Proces podpisywania oprogramowania sprzętowego.

Przed aktualizacją oprogramowania sprzętowego należy zweryfikować nowe oprogramowanie sprzętowe. Aby upewnić się, że nowe oprogramowanie sprzętowe nie zostało zmienione w sposób nieuprawniony, używa się klucza publicznego (dostarczanego z produktem Axis) w celu potwierdzenia, że skrót został rzeczywiście podpisany przy użyciu pasującego klucza prywatnego. Poprzez obliczenie skrótu oprogramowania sprzętowego i porównanie go z tym zweryfikowanym skrótem z podpisu można potwierdzić integralność oprogramowania sprzętowego.

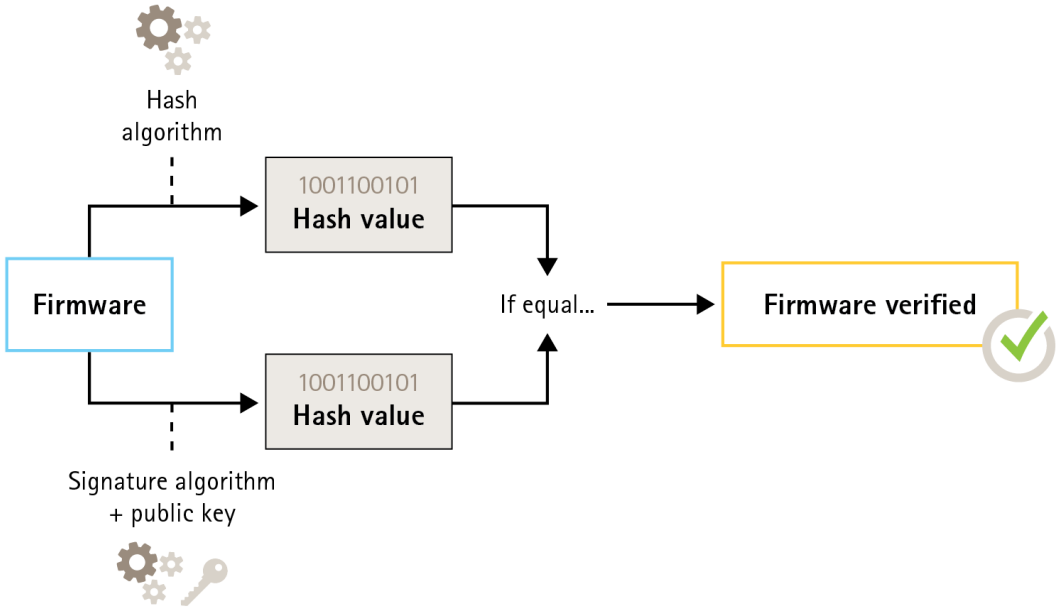

Figure 2. Proces weryfikacji podpisanego oprogramowania sprzętowego.

4.2 Podpisane oprogramowanie sprzętowe Axis

Podpisane przez firmę Axis oprogramowanie sprzętowe jest oparte na powszechnie przyjętej w branży metodzie szyfrowania RSA z kluczem publicznym. Klucz prywatny jest przechowywany w ściśle chronionej lokalizacji w firmie Axis, natomiast klucz publiczny jest osadzany w urządzeniach Axis. Integralność obrazu całego oprogramowania sprzętowego jest zapewniona poprzez podpisanie zawartości obrazu. Podpis podstawowy służy do weryfikacji szeregu podpisów dodatkowych w trakcie rozpakowywania obrazu.

5 Ochrona łańcucha dostaw przed sabotażem

Podpisywanie oprogramowania sprzętowego chroni urządzenie, w tym także wszystkie przyszłe aktualizacje oprogramowania sprzętowego, przed zainstalowaniem zmodyfikowanego w sposób nieautoryzowany oprogramowania sprzętowego. Ale co zrobić w przypadku ataku typu „man in the middle" prowadzącego do zmiany urządzenia w drodze między dostawcą a użytkownikiem końcowym? Przeciwnik, który ma fizyczny dostęp do urządzenia podczas transportu, mógłby przeprowadzić atak, na przykład poprzez modyfikację partycji rozruchowej urządzenia i ominięcie sprawdzania integralności oprogramowania sprzętowego, aby zainstalować zmienione, szkodliwe oprogramowanie sprzętowe jeszcze przed wprowadzeniem urządzenia do użytku.

5.1 Bezpieczny start

Bezpieczny start to proces składający się z nieprzerwanego łańcucha oprogramowania zweryfikowanego kryptograficznie, rozpoczynający się w pamięci niezmiennej (rozruchowej pamięci ROM). Dzięki wykorzystaniu podpisanego oprogramowania sprzętowego bezpieczny start gwarantuje uruchomienie urządzenia wyłącznie z autoryzowanym oprogramowaniem sprzętowym.

Proces startu jest inicjowany przez rozruchową pamięć ROM, która dokonuje weryfikacji programu inicjującego. Następnie w czasie rzeczywistym sprawdzane są osadzone podpisy wszystkich bloków oprogramowania sprzętowego ładowanych z pamięci flash. Rozruchowa pamięć ROM służy jako źródło zaufania, a proces uruchamiania jest kontynuowany tylko pod warunkiem, że każdy podpis zostanie zweryfikowany. Każdy element tego łańcucha uwierzytelnia następny element, co skutkuje zweryfikowanym jądrem systemu Linux i zweryfikowanym bazowym systemem plików.

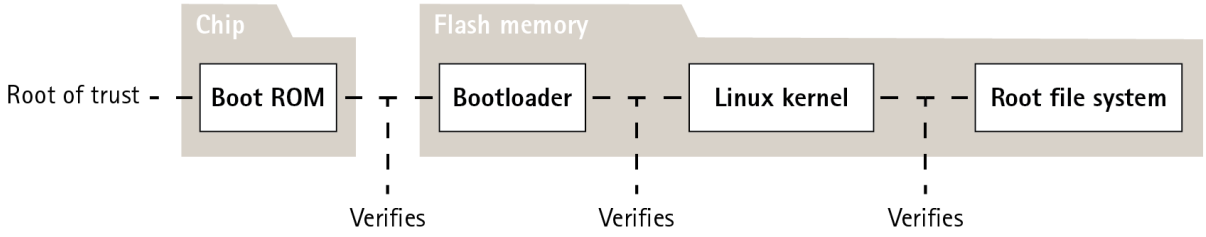

Figure 3. Proces bezpiecznego startu.

5.2 Bezpieczny start Axis

W wielu urządzeniach istotne jest wykluczenie możliwości zmian funkcji niskopoziomowych. Podczas gdy inne mechanizmy bezpieczeństwa funkcjonują powyżej oprogramowania niskopoziomowego, bezpieczny start działa jak podstawowa tarcza bezpieczeństwa, która chroni te mechanizmy przed możliwością obejścia.

W przypadku urządzenia z bezpiecznym startem oprogramowanie sprzętowe zainstalowane w pamięci flash jest chronione przed modyfikacją. Domyślny obraz fabryczny jest chroniony, natomiast konfiguracja pozostaje niezabezpieczona. Bezpieczny start gwarantuje, że po przywróceniu ustawień fabrycznych urządzenie Axis jest całkowicie pozbawione złośliwego oprogramowania.

5.3 Bezpieczny start i niestandardowe certyfikaty oprogramowania sprzętowego

Bezpieczny start sprawia, że urządzenie jest bezpieczniejsze, ale jednocześnie komplikuje zmianę oprogramowania sprzętowego, utrudniając wczytanie tymczasowego oprogramowania, np. wersji testowej lub innego niestandardowego oprogramowania sprzętowego Axis. Firma Axis wdrożyła jednak mechanizm zatwierdzający takie zmienione oprogramowanie sprzętowe na poszczególnych urządzeniach. Takie oprogramowanie sprzętowe jest podpisywane w inny sposób, po zatwierdzeniu zarówno przez właściciela, jak i firmę Axis; użycie tej opcji powoduje utworzenie niestandardowego certyfikatu oprogramowania sprzętowego. Certyfikat zezwala na uruchomienie niestandardowego oprogramowania sprzętowego wyłącznie na zatwierdzonym urządzeniu, które jest identyfikowane po unikalnym numerze seryjnym i ID czipu. Niestandardowe certyfikaty oprogramowania sprzętowego może tworzyć tylko firma Axis, ponieważ to ona posiada klucz potrzebny do ich podpisywania.

6 Tajemnice chronione przed manipulacjami

Podstawowym wymogiem stawianym każdemu zabezpieczonemu systemowi rozproszonemu jest zdolność do weryfikacji połączeń i zapobiegania podsłuchiwaniu ruchu. W tym celu każde urządzenie musi chronić swoje tajemnice, przechowując je w pamięci zabezpieczonej przed manipulacjami. Taką pamięcią jest moduł Axis Edge Vault. Stanowi on fundament, na którym można bezpiecznie budować bardziej zaawansowane funkcje zabezpieczające.

6.1 ID urządzenia Axis

Podczas produkcji każdego egzemplarza urządzenia sieciowego Axis w jego module Axis Edge Vault jest bezpiecznie instalowany „paszport cyfrowy", tak zwany ID urządzenia. Ten identyfikator jest unikatowy dla każdego egzemplarza urządzenia i został zaprojektowany tak, aby można było ustalić źródło tego egzemplarza. ID urządzenia Axis to zbiór certyfikatów używanych do podpisywania wyzwań prezentowanych modułowi Edge Vault przez osadzone oprogramowanie sprzętowe produktu. Odpowiedź będąca wynikiem tej operacji jest odsyłana do odbiorcy, który może użyć kluczy publicznych firmy Axis do potwierdzenia autentyczności odpowiedzi.

Certyfikat to niewielki zestaw danych, który zawiera klucz publiczny i metadane opisujące klucz, a także podpis wystawcy potwierdzający ważność certyfikatu. Hierarchia certyfikatów to sposób na udowodnienie pochodzenia certyfikatu.

Możemy posłużyć się analogią między ID urządzenia Axis a paszportem. Rząd kraju, wydając danej osobie paszport, poświadcza w ten sposób, że posiadacz paszportu jest faktycznie osobą w nim wskazaną. W podobny sposób główny certyfikat CA w ID urządzenia Axis potwierdza certyfikaty składające się na ID urządzenia Axis. Strażnik graniczny co do zasady zakłada, że rząd kraju poprawnie wystawił

paszport. Podobnie system bezpieczeństwa sieci działa z założeniem, że główny certyfikat CA w ID urządzenia prawidłowo potwierdza certyfikat urządzenia Axis podłączonego do sieci.

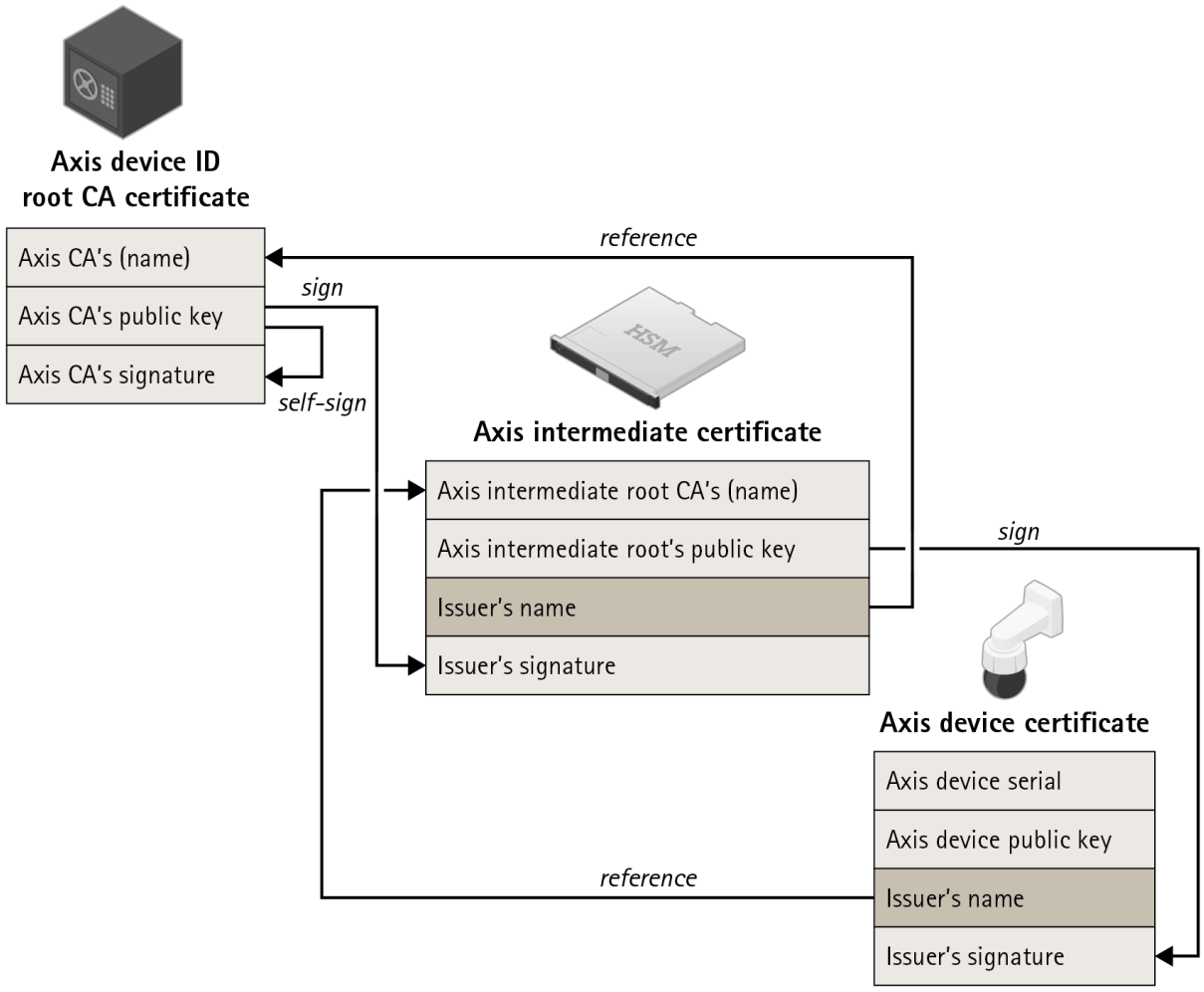

Figure 4. ID urządzenia Axis, który jest certyfikatem zawierającym numer seryjny produktu, podpisywany jest certyfikatem pośredniczącym podpisanym przez główny certyfikat Axis. Ponieważ główny certyfikat firmy Axis jest bardzo wartościowy i musi być przechowywany w doskonale zabezpieczonym miejscu, przy produkcji urządzeń używany jest certyfikat pośredni.

7 Bezpieczne przechowywanie klucza

Urządzenia Axis obsługują protokoły HTTPS (szyfrowanie komunikacji sieciowej) i 802.1X (kontrola dostępu do sieci), które z kolei wykorzystują protokół TLS (Transport Layer Security). Cyfrowe certyfikaty TLS wykorzystują parę kluczy publiczny/prywatny. Klucz prywatny jest przechowywany w urządzeniu, natomiast klucz publiczny jest zawarty w certyfikacie. Trzeba pamiętać, że jeżeli nie jest używany ani protokół HTTPS, ani 802.1X, to nie istnieją klucze, które trzeba byłoby chronić.

Przeciwnik może próbować wyodrębnić klucz prywatny i certyfikat z urządzenia, a następnie zainstalować je na atakującym komputerze. W przypadku protokołu HTTPS ten klucz prywatny może posłużyć do podsłuchiwania szyfrowanego ruchu sieciowego między urządzeniem a VMS. Komputer atakujący mógłby również uzyskać dostęp do VMS, udając uprawnione urządzenie. W przypadku protokołu 802.1X przeciwnik

może użyć klucza prywatnego, aby uzyskać dostęp do sieci zabezpieczonej protokołem 802.1X, udając urządzenie zaufane.

Certyfikaty i klucze prywatne są zazwyczaj przechowywane w systemie plików urządzenia, chronione przez zasady dostępu do konta i używane w normalnym środowisku komputerowym. W większości przypadków jest to wystarczające, ponieważ nie można łatwo włamać się na konto. Należy pamiętać, że jeśli pojawi się podejrzenie naruszenia zabezpieczeń, certyfikaty można odwołać — tak by klucz prywatny stał się bezużyteczny.

Niektórzy użytkownicy systemów o krytycznym znaczeniu mogą być narażeni na zwiększone ryzyko ataku zdeterminowanych i dobrze wyszkolonych przeciwników, którzy będą próbowali dostać się do urządzenia, aby wyodrębnić klucz prywatny. Jednak wyodrębnienie klucza przechowywanego w module Axis Edge Vault jest praktycznie niemożliwe, nawet jeśli zabezpieczenia urządzenia zostaną złamane.

7.1 Bezpieczne przechowywanie certyfikatów w module Axis Edge Vault

Axis Edge Vault to kryptograficzny moduł obliczeniowy w postaci układu scalonego umieszczonego na płytce drukowanej w urządzeniu. Edge Vault może bezpiecznie przechowywać certyfikaty i można go używać do wykonywania operacji kryptograficznych na tych certyfikatach.

Certyfikaty przechowywane w module Edge Vault nie muszą go opuszczać na czas użycia przez urządzenie. Wynika to z faktu, że sprzęt kryptograficzny operujący na kluczu znajduje się w tym samym fizycznym układzie scalonym, co Edge Vault.

7.2 Bezpieczne przechowywanie kluczy w module TPM (Trusted Platform Module)

Moduł TPM to komponent realizujący określony zestaw funkcji kryptograficznych, stosowany do ochrony informacji przed dostępem osób nieupoważnionych. W module TPM przechowywany jest klucz prywatny. Klucz ten nigdy nie opuszcza modułu TPM, ponieważ wszystkie operacje kryptograficzne wymagające użycia klucza prywatnego są kierowane do modułu TPM i w nim wykonywane. Gwarantuje to, że tajna część certyfikatu nigdy nie opuści bezpiecznego środowiska i pozostanie bezpieczna nawet w przypadku naruszenia zabezpieczeń.

7.3 Certyfikat FIPS 140-2

W niektórych produktach i zastosowaniach używanie modułu TPM do ochrony informacji jest wymagane z mocy prawa. Niekiedy równocześnie wymagana jest zgodność z normą FIPS 140-2. FIPS (Federal Information Processing Standard) 140-2 to norma bezpieczeństwa modułów kryptograficznych wydana w USA przez instytut NIST (National Institute of Standards and Technology).

Walidacja dokonana przez laboratorium certyfikowane przez NIST potwierdza prawidłowe wdrożenie aspektów systemowych i kryptograficznych modułu. Wymagania certyfikacyjne obejmują opis, specyfikację i weryfikację modułu kryptograficznego, zatwierdzone algorytmy, zatwierdzone tryby pracy oraz testów po włączeniu zasilania.

Więcej informacji o wymaganiach związanych z certyfikacją FIPS 140-2 można znaleźć w witrynie internetowej instytutu NIST pod adresem *www.nist.gov*

7.3.1 Certyfikowany moduł TPM w produktach Axis

Moduł TPM używany w wybranych produktach Axis uzyskał certyfikat potwierdzający jego zgodność z wymaganiami normy FIPS 140-2. W szczególności jest certyfikowany na zgodność z poziomem Security Level 2 tej normy, co oznacza, że spełnia także, między innymi, wymagania dotyczące autoryzacji na podstawie ról i zachowywania dowodów manipulacji.

8 IEEE 802.1AR — weryfikacja urządzeń na podstawie ID urządzenia Axis

Nowo zakupione urządzenie sieciowe Axis można przed użyciem sprawdzić wzrokowo i manualnie. Dzięki wzrokowej kontroli produktu i wcześniejszej wiedzy o wyglądzie i działaniu produktów Axis klient może upewnić się, że rzeczywiście ma do czynienia z produktem firmy Axis. Taką kontrolę może jednak przeprowadzić tylko osoba, która ma fizyczny dostęp do produktu. Ale jeśli komunikujemy się z nowym (jeszcze niewdrożonym) produktem tylko za pośrednictwem sieci, to skąd możemy mieć pewność, że jest to faktycznie oryginalne urządzenie? Że nie zostało podmienione? Urządzenia w sieci ani programy na serwerach nie mogą przeprowadzać kontroli fizycznej. Dlatego ze względów bezpieczeństwa pierwsze interakcje z nowym produktem często podejmuje się najpierw w sieci zamkniętej, w której można bezpiecznie wdrożyć urządzenie.

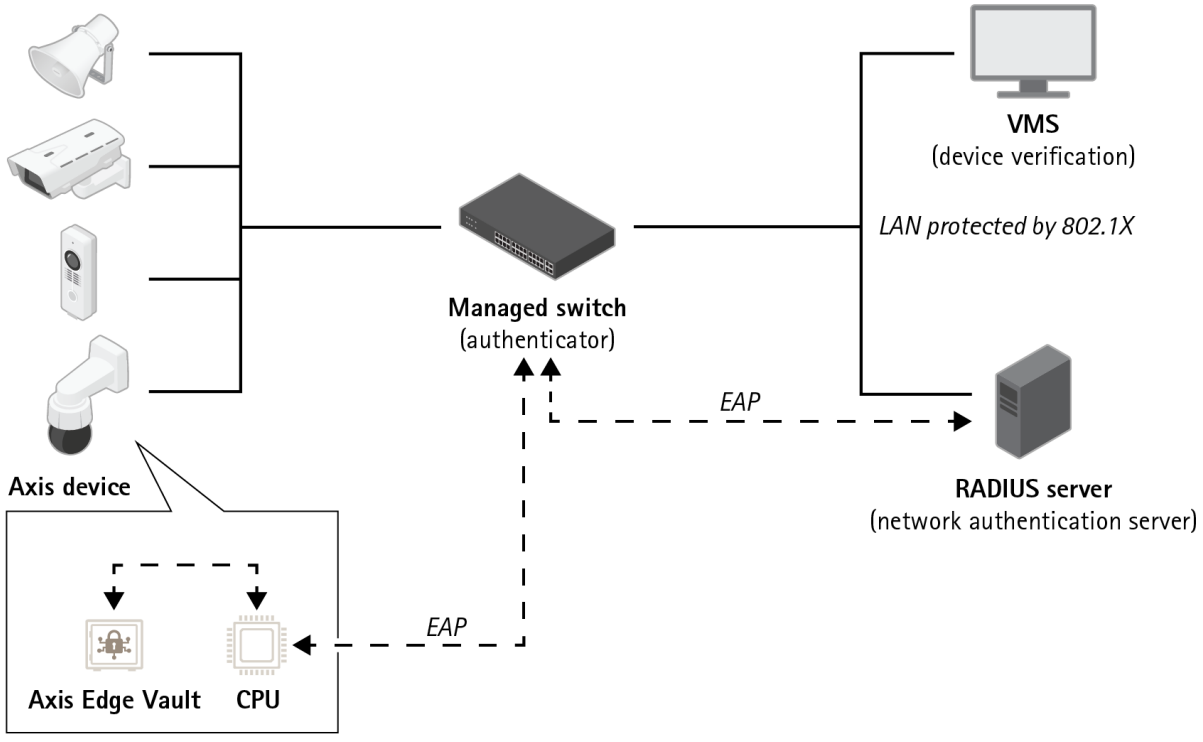

Figure 5. Klienci mogą tak skonfigurować serwer uwierzytelniania, aby automatycznie akceptował zakupione produkty Axis w sieci na podstawie ich numerów seryjnych i ID urządzenia Axis.

Nowa norma międzynarodowa IEEE 802.1AR (*https://1.ieee802.org/security/802-1ar/*) definiuje metodę automatyzacji i zabezpieczania identyfikacji urządzeń w sieci. Jeżeli komunikacja jest przekazywana do

wbudowanego bezpiecznego modułu, urządzenie może zwracać wiarygodną odpowiedź identyfikacyjną zgodnie tą normą.

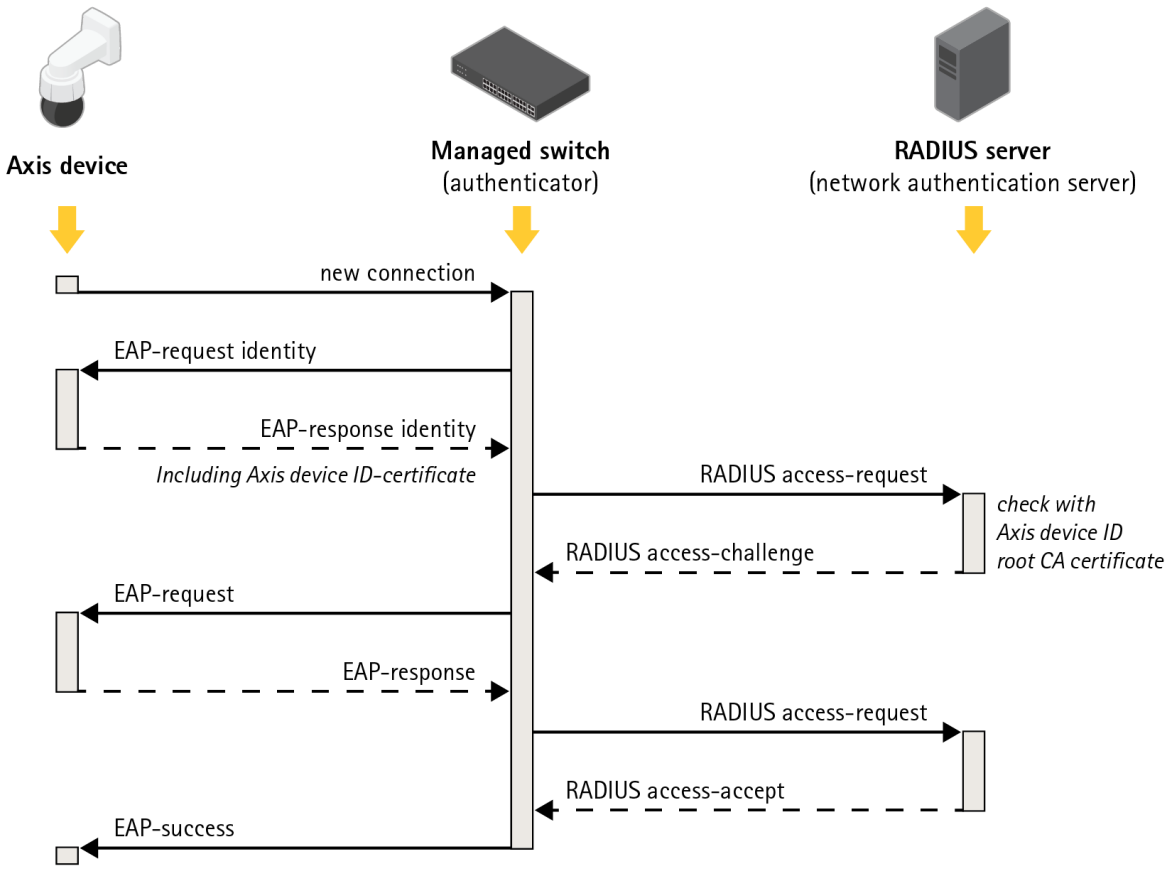

Figure 6. Norma IEEE 802.1AR definiuje protokół identyfikacji urządzeń polegający na wysyłaniu do przełącznika żądań EAP (Extensible Authentication Protocol) i wykorzystywaniu żądań RADIUS (Remote Authentication Dial-In User Service) do udzielania dostępu.

W produktach Axis te środki bezpieczeństwa są zrealizowane poprzez zastosowanie modułu Axis Edge Vault oraz ID urządzenia Axis. Axis Edge Vault to zabezpieczony moduł, w którym zapisany jest ID urządzenia, czyli zestaw certyfikatów służących do weryfikowania identyfikacji urządzenia. Funkcje te dostarczają sieci weryfikowalny kryptograficznie dowód tego, że konkretne urządzenie zostało wyprodukowane przez firmę Axis oraz że połączenie sieciowe z tym urządzeniem jest faktycznie przez nie obsługiwane.

Urządzenie z ID urządzenia Axis zostało podczas produkcji wyposażone w klucze i certyfikaty. Klient może je później wykorzystać do wdrożenia urządzenia w swojej instalacji przy użyciu innych kluczy i/lub certyfikatów umożliwiających dostęp do zasobów sieciowych klienta.

Możliwość identyfikacji urządzenia na podstawie ID urządzenia Axis skraca czas potrzebny na wdrożenie, ponieważ ogranicza zakres czynności, które trzeba wykonać przed zainstalowaniem i skonfigurowaniem urządzenia w docelowej sieci. Kolejną korzyścią jest fakt, że ID urządzenia Axis, oprócz zapewniania

dodatkowego, wbudowanego źródła zaufania, oferuje możliwość ewidencjonowania urządzeń w dużym systemie.

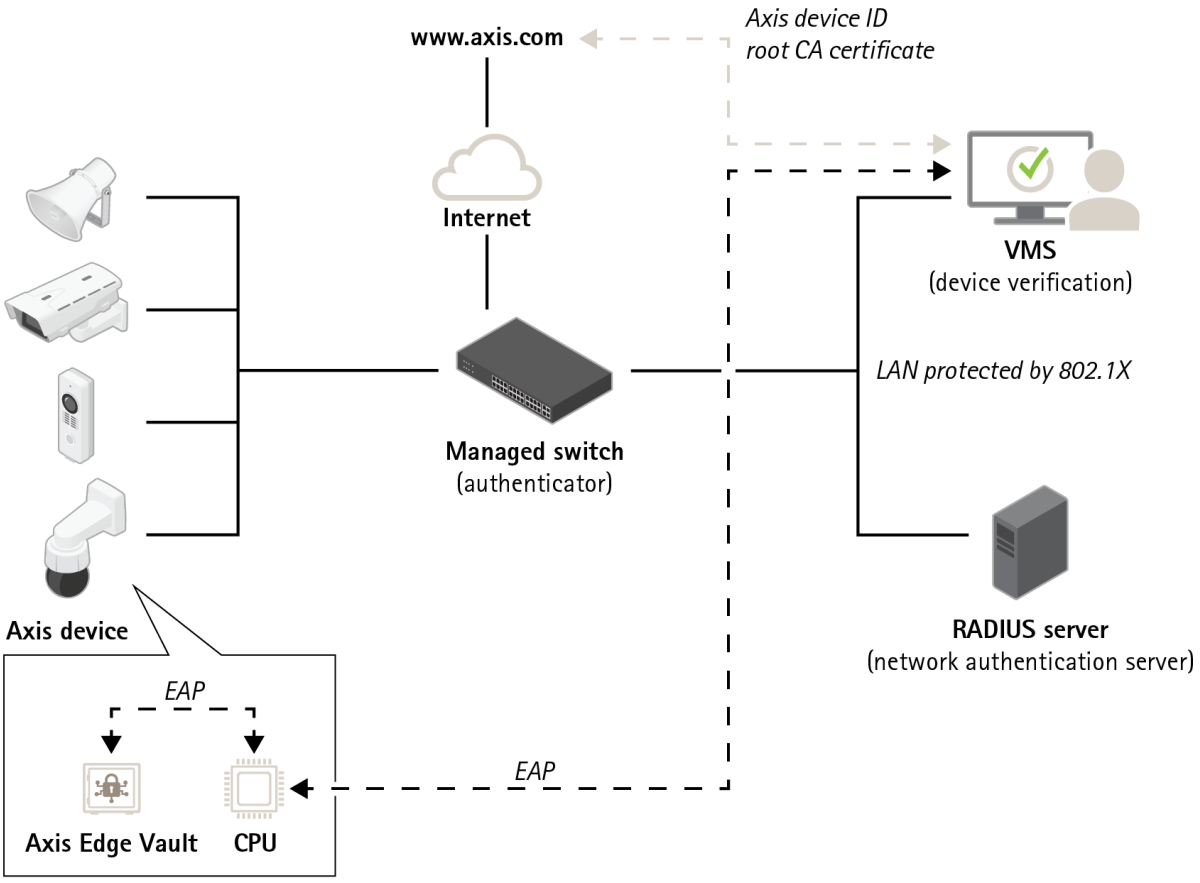

Figure 7. Aplikacje w innych częściach systemu mogą używać ID urządzenia Axis i operacji kryptograficznych, aby sprawdzić, z „kim" faktycznie się komunikują. Każdy ID urządzenia Axis został zweryfikowany za pomocą przeznaczonego do tego celu publicznego certyfikatu głównego CA firmy Axis z domeny axis.com.

9 Wykrywanie manipulacji w materiale wideo

Fundamentalnym założeniem w sektorze ochrony jest autentyczność i wiarygodność nagrań wideo rejestrowanych przez kamery do nadzoru. Wideo z podpisem to funkcja opracowana po to, by dodatkowo wzmocnić zaufanie do nagrań wideo traktowanych jako materiał dowodowy. Taka weryfikacja autentyczności nagrania potwierdza, że materiał nie został zmontowany lub zmanipulowany po tym, jak opuścił kamerę.

9.1 Wideo z podpisem

Oferowana przez firmę Axis funkcja wideo z podpisem pozwala na wykorzystanie podpisu w strumieniu wideo do zabezpieczenia go przed manipulacją i weryfikacji pochodzenia, tj. ustalenia, która kamera ten strumień wygenerowała. W ten sposób można dowieść autentyczności nagrania wideo bez konieczności odtwarzania całego łańcucha pochodzenia pliku wideo.

Po zarejestrowaniu incydentu przez kamerę systemu dozorowego policja może wyodrębnić nagrania wideo jako pliki wyeksportowane na pendrive USB i zapisać je w systemie zarządzania materiałem dowodowym (EMS, evidence management system). Eksportując wideo z kamery, funkcjonariusz widzi, czy materiał wideo jest prawidłowo podpisany. Jeśli zostanie później wykorzystany w postępowaniu prokuratorskim, sąd może zweryfikować moment nagrania wideo, ustalić, z której kamery ono pochodzi, oraz czy którekolwiek klatki zostały zmienione lub usunięte. Korzystając z odtwarzacza plików oferowanego przez firmę Axis, każda osoba dysponująca kopią nagrania wideo może zapoznać się z tymi informacjami.

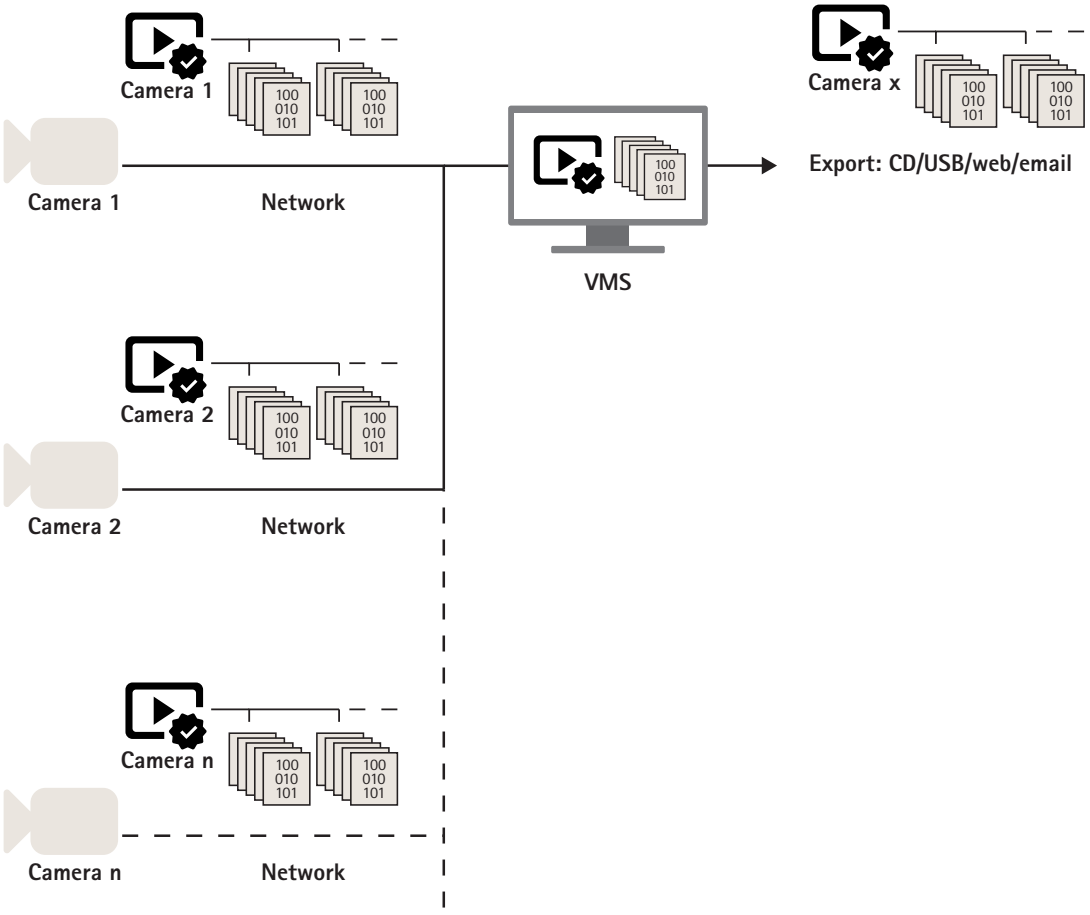

Figure 8. Podpis jest dodawany już w kamerze, pozwalając na weryfikację treści na każdym etapie, od źródła do ostatniego zastosowania materiału wideo.

Każda kamera dodaje do strumienia wideo swój niepowtarzalny ID urządzenia Axis, zapisany w jej module Axis Edge Vault. W tym celu oblicza skrót każdej klatki, dodaje do niego metadane i podpisuje taki złożony

skrót w module Edge Vault. Następnie podpis jest umieszczany w strumieniu, w przeznaczonych na niego polach metadanych (nagłówku SEI).

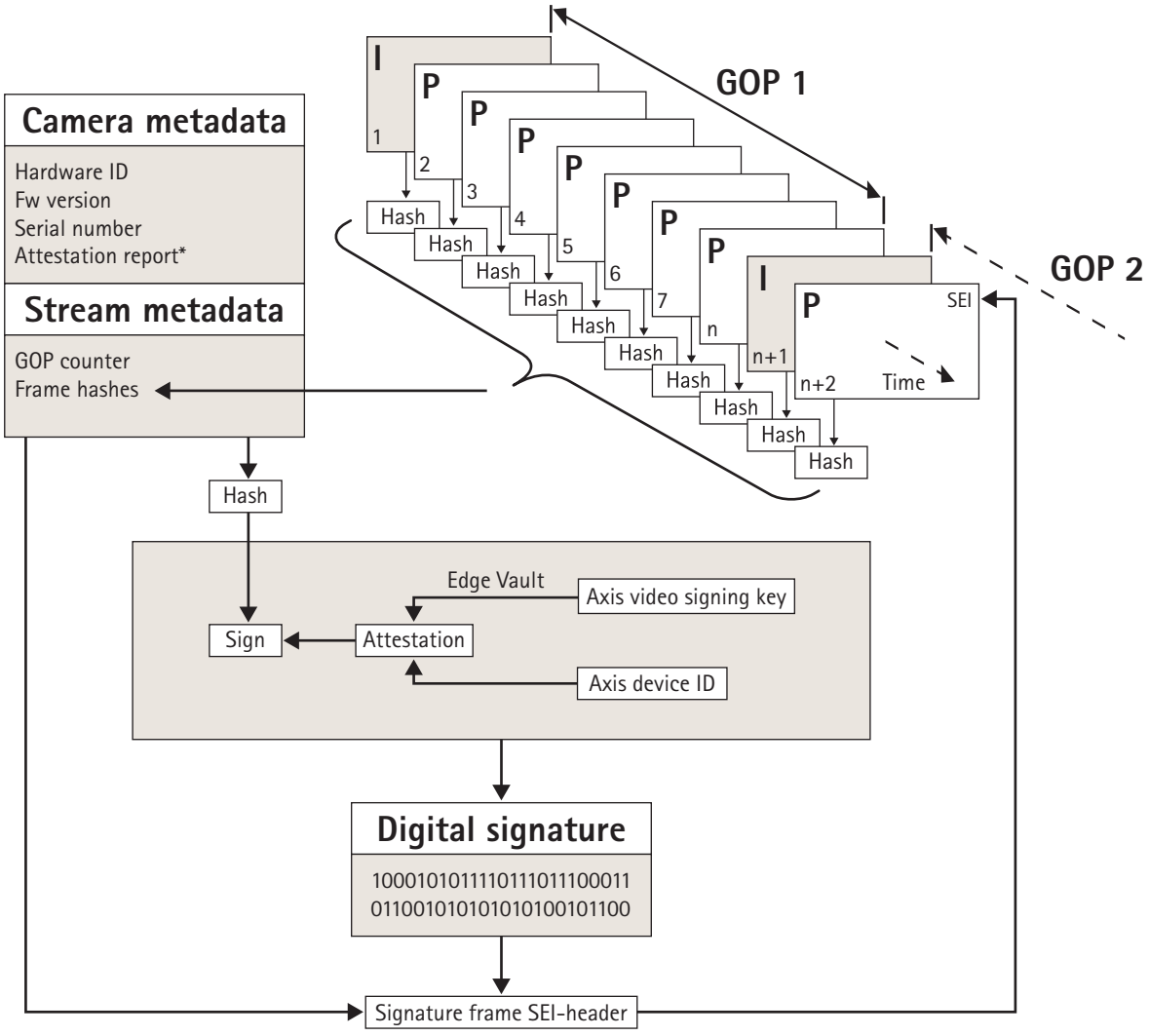

Figure 9. Ilustracja sposobu dodawania podpisu do metadanych wideo. Skrót zawartości każdej klatki grupy obrazów (GOP) jest łączony ze skrótem metadanych kamery i metadanymi strumienia. W ten sposób powstaje skrót GOP, który jest podpisywany w module Edge Vault. Następnie podpis i metadane są dodawane do tworzonego później nagłówka SEI przesyłanego razem ze strumieniem.

* *Na podstawie poświadczenia można zweryfikować pochodzenie i historię posiadania pary kluczy użytej do podpisywania. Weryfikacja poświadczenia klucza zapewnia bezpieczne przechowanie klucza w sprzęcie konkretnego urządzenia. W ten sposób zabezpieczana jest informacja o pochodzeniu wideo.*

Do właściwego podpisywania używany jest przypisany do konkretnego urządzenia klucz poświadczony w oparciu o ID urządzenia Axis (ten identyfikator również jest przypisany do konkretnego urządzenia). Poświadczenie jest umieszczane w strumieniu na jego początku i w regularnych odstępach czasu, zwykle co godzinę. Ponieważ metadane zawierają skrót każdej klatki, można weryfikować poprawność

poszczególnych klatek. Aby proces podpisywania był kompletny, należy także zabezpieczyć strukturę GOP materiału wideo. To zabezpieczenie polega na umieszczeniu w podpisie skrótu pierwszej klatki kluczowej następnej grupy GOP. Wyklucza ono możliwość niezauważonych usunięć lub zmian kolejności klatek. W ten sam sposób będą sygnalizowane ewentualne, mało prawdopodobne, przypadki utraty klatek podczas przesyłania strumienia lub uszkodzenia treści w trakcie przechowywania.

O firmie Axis Communications

Axis umożliwia tworzenie mądrzejszego i bezpieczniejszego świata, tworząc sieć rozwiązań, które zapewniają wgląd w poprawę bezpieczeństwa i nowe sposoby prowadzenia biznesu. Jako lider branży sieciowych systemów wideo firma Axis oferuje produkty i usługi do monitoringu wideo i analityki, systemy kontroli dostępu, systemy domofonowe i rozwiązania audio. Axis zatrudnia ponad 3800 pracowników w ponad 50 krajach i współpracuje z partnerami na całym świecie, aby dostarczać rozwiązania dla klientów. Firma Axis została założona w 1984 roku i ma swoją siedzibę szwedzkim mieście Lund.

Więcej informacji o firmie Axis można znaleźć na stronie internetowej firmy pod adresem *axis.com*.

©2020 - 2021 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC i VAPIX są zastrzeżonymi znakami towarowymi firmy Axis AB w różnych jurysdykcjach. Wszystkie inne znaki towarowe są własnością odpowiednich podmiotów. Zastrzegamy sobie prawo do wprowadzania zmian bez uprzedniego powiadomienia.