BIAŁA KSIĘGA

Axis Edge Vault

Sprzętowa platforma cyberbezpieczeństwa, która chroni urządzenia Axis, dbając o następujące aspekty:

— ochrona łańcucha dostaw

— wiarygodna tożsamość urządzenia

— bezpieczne przechowywanie kluczy

— detekcja manipulacji w materiale wizyjnym

Kwiecień 2024

AXIS COMMUNICATIONS

Streszczenie

Axis Edge Vault to sprzętowa platforma cyberbezpieczeństwa chroniąca urządzenie Axis. Rozwiązanie to jest oparte na mocnych podstawach zapewnianych przez kryptograficzne moduły obliczeniowe (bezpieczny element i TPM) oraz zabezpieczenia procesora SoC (TEE i bezpieczny start), a także na specjalistycznej wiedzy z zakresu bezpieczeństwa urządzeń brzegowych. Axis Edge Vault ma swoje umocowanie w solidnym źródle zaufania, jakie zapewnia funkcja *bezpiecznego startu* oraz *podpisany system operacyjny*. Funkcje te zapewniają ciągły łańcuch zweryfikowanego kryptograficznie oprogramowania, co jest podstawą łańcucha zaufania, od którego zależą wszystkie wymagające bezpieczeństwa operacje.

Urządzenia Axis z Edge Vault minimalizują narażenie klienta na cyberzagrożenia, zapobiegając podsłuchiwaniu i złośliwemu wykradaniu poufnych informacji. Axis Edge Vault sprawia też, że urządzenie Axis może być zaufaną i niezawodną jednostką w sieci klienta.

Platforma cyberbezpieczeństwa Axis Edge Vault

Kryptograficzne moduły obliczeniowe	Cechy	Zastosowania
• Bezpieczny element • TPM 2.0 • Zabezpieczenia procesora SoC (TEE)	• Bezpieczny start • Podpisany system operacyjny • Identyfikator urządzenia axis • Bezpieczny magazyn kluczy • Podpisany materiał wizyjny • Zaszyfrowany system plików	• Ochrona łańcucha dostaw • Wiarygodna tożsamość urządzenia • Bezpieczne przechowywanie kluczy • Wykrywanie manipulacji w materiale wideo

- **Ochrona łańcucha dostaw** — Axis Edge Vault wymaga bezpiecznego fundamentu pełniącego funkcję źródła zaufania. Bez wsparcia zapewnianego przez funkcje bezpiecznego startu i podpisany system operacyjny nie można uzyskać łańcucha zaufania. Bezpieczny start oraz podpisany system operacyjny zapewniają ciągłość łańcucha kryptograficznie zweryfikowanego oprogramowania, rozpoczynający się w niezmiennej pamięci operacyjnej (rozruchowej pamięci ROM). Funkcja bezpiecznego startu sprawia, że urządzenie może być uruchamiane tylko z podpisanym systemem operacyjnym, co uniemożliwia fizyczne manipulacje na poziomie łańcucha dostaw. Dzięki podpisanemu systemowi operacyjnemu urządzenie może też zweryfikować swoje nowe oprogramowanie, zanim zezwoli na jego instalację. W przypadku wykrycia, że integralność została naruszona lub oprogramowanie urządzenia nie jest podpisane przez Axis, aktualizacja tego oprogramowania zostanie zablokowana. Chroni to urządzenia przed ingerencją w oprogramowanie.

- **Wiarygodna tożsamość urządzenia** — możliwość zweryfikowania pochodzenia urządzenia jest kluczowa z perspektywy wiarygodności tożsamości urządzenia. Podczas produkcji urządzenia z rozwiązaniem Axis Edge Vault mają przypisywany unikatowy fabryczny i zgodny ze standardem IEEE 802.1AR certyfikat znany jako identyfikator urządzenia Axis. Jest on swego rodzaju paszportem, który potwierdza pochodzenie urządzenia. Identyfikator urządzenia jest bezpiecznie i trwale przechowywany w bezpiecznym magazynie kluczy w postaci certyfikatu podpisanego za pomocą certyfikatu głównego Axis. Identyfikator urządzenia może być wykorzystywany w ramach infrastruktury IT klienta w celu automatycznego bezpiecznego wdrażania i bezpiecznej identyfikacji urządzeń.

- **Bezpieczne przechowywanie kluczy** – bezpieczny magazyn kluczy zapewnia sprzętowe, zabezpieczone przed manipulacją przechowywanie informacji kryptograficznych. Bezpieczny magazyn kluczy chroni identyfikator urządzenia Axis oraz informacje kryptograficzne załadowane przez klienta i zapobiega nieautoryzowanemu dostępowi oraz złośliwemu wykradaniu danych w razie włamania do systemu.
- **Detekcja manipulacji w materiale wizyjnym** – podpis dodany do materiału wizyjnego umożliwia potwierdzenie autentyczności dowodowej bez konieczności potwierdzenia całego łańcucha pochodzenia pliku wideo. Każda kamera podpisuje materiał wizyjny za pomocą własnego unikatowego klucza, który jest bezpiecznie przechowywany w bezpiecznym magazynie kluczy. Podczas odtwarzania nagrania wideo *odtwarzacz plików* Axis pokazuje, czy materiał wizyjny pozostaje nienaruszony. Podpisany materiał wizyjny umożliwia ustalenie, z której kamery materiał pochodzi, i wykrycie ewentualnych nieuprawnionych modyfikacji wprowadzonych w materiale po tym, jak opuścił on kamerę.

Spis treści

1 Wprowadzenie

Axis wdraża zabezpieczenia w swoich produktach zgodnie z najlepszymi praktykami branżowymi. Ma to na celu zminimalizowanie narażenia klienta na ryzyko związane z cyberbezpieczeństwem oraz przekształcenie urządzenia Axis w zaufaną jednostkę w sieci klienta.

Axis Edge Vault to sprzętowa platforma cyberbezpieczeństwa chroniąca urządzenie Axis. Rozwiązanie to bazuje na mocnych podstawach zapewnianych przez kryptograficzne moduły obliczeniowe (bezpieczny element i TPM) oraz zabezpieczenia procesora SoC (TEE i bezpieczny start), a także na specjalistycznej wiedzy z zakresu bezpieczeństwa urządzeń brzegowych.

W niniejszej białej księdze przedstawiono wielowarstwowe podejście do kwestii bezpieczeństwa urządzeń brzegowych Axis oraz zaprezentowano typowe czynniki ryzyka i sposoby zapobiegania im. Axis Edge Vault wymaga bezpiecznego fundamentu pełniącego funkcję źródła zaufania. W związku z tym przyjrzymy się też aspektom bezpieczeństwa łańcucha dostaw urządzeń Axis i opowiemy, jak podpisany system operacyjny i funkcja bezpiecznego startu stanowią podstawowe środki przeciwdziałania manipulacjom związanym z oprogramowaniem oraz fizycznym manipulacjom w łańcuchu dostaw.

Na stronie *https://www.axis.com/support/cybersecurity/resources* można znaleźć więcej informacji na temat bezpieczeństwa produktów, wykrytych luk w zabezpieczeniach oraz środków, które można podjąć w celu obniżenia ryzyka związanego z typowymi zagrożeniami.

Ostatni rozdział niniejszego dokumentu zawiera słownik pojęć.

2 Ochrona łańcucha dostaw

Axis Edge Vault wymaga bezpiecznego fundamentu pełniącego funkcję źródła zaufania. Ustanowienie źródła zaufania zaczyna się na etapie procesu uruchamiania urządzenia. W przypadku urządzeń Axis sprzętowy mechanizm *bezpiecznego startu* weryfikuje system operacyjny (AXIS OS), z którego jest uruchamiane urządzenie. AXIS OS z kolei jest podpisany kryptograficznie (*podpisany system operacyjny*) podczas kompilacji.

Funkcja bezpiecznego startu i podpisany system operacyjny są ze sobą powiązane. Zapewniają one, że system operacyjny czy oprogramowanie urządzenia nie zostały poddane manipulacji (przez osobę mającą fizyczny dostęp do urządzenia) przed wdrożeniem urządzenia i że po wdrożeniu urządzenie nie zainstaluje aktualizacji, których zabezpieczenia zostały naruszone lub które mają niepodpisany kod. Razem bezpieczny start i podpisany system operacyjny tworzą ciągły łańcuch kryptograficznie zweryfikowanego oprogramowania na potrzeby łańcucha zaufania, od którego zależą wszystkie wymagające bezpieczeństwa operacje.

2.1 Bezpieczny start

Mechanizm bezpiecznego startu to proces uruchamiania obejmujący ciągły łańcuch zweryfikowanego kryptograficznie oprogramowania, który ma swój początek w niezmiennej pamięci operacyjnej (rozruchowej pamięci ROM). Funkcja bezpiecznego startu gwarantuje, że urządzenie można uruchomić tylko z autoryzowanym systemem operacyjnym.

Proces startu jest inicjowany przez rozruchową pamięć ROM, która dokonuje weryfikacji programu inicjującego. Bezpieczny start polega na sprawdzeniu w czasie rzeczywistym podpisów osadzonych w każdym komponencie oprogramowania ładowanym z pamięci flash. Rozruchowa pamięć ROM stanowi źródło zaufania, a proces uruchamiania jest kontynuowany tylko pod warunkiem zweryfikowania każdego

podpisu. Każdy element tego łańcucha uwierzytelnia następny element, co skutkuje zweryfikowanym jądrem systemu Linux i zweryfikowanym bazowym systemem plików.

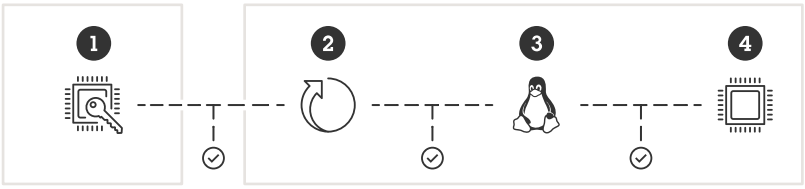

Figure 1. W procesie bezpiecznego startu każdy element łańcucha uwierzytelnia następny element. Ostatecznym wynikiem tego procesu jest zweryfikowany bazowy system plików.

1 *Rozruchowa pamięć ROM (źródło zaufania) w procesorze SoC*
2 *Program inicjujący*
3 *Jądro systemu Linux*
4 *Bazowy system plików*

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 funkcją bezpiecznego startu system operacyjny zainstalowany w pamięci flash jest chroniony przed modyfikacją, podczas gdy konfiguracja pozostaje niezabezpieczona. Bezpieczny start gwarantuje prawidłowy stan urządzenia nawet po przywróceniu ustawień fabrycznych. Aby jednak funkcja bezpiecznego startu działała jak należy, w jej ramach musi zostać przeprowadzona weryfikacja, czy system operacyjny został podpisany przez Axis.

2.2 Podpisany system operacyjny

Podpisany system operacyjny Axis oznacza podpisanie przez Axis kodu obrazu oprogramowania urządzenia przy użyciu klucza prywatnego, który jest utrzymywany w ścisłej tajemnicy. Podczas uruchamiania urządzenia funkcja bezpiecznego startu urządzenia Axis sprawdza, czy oprogramowanie urządzenia jest podpisane. W przypadku wykrycia, że integralność oprogramowania urządzenia jest zagrożona, urządzenie nie zostaje uruchomione. Podczas uaktualnień oprogramowania urządzenia istniejący podpisany system operacyjny AXIS OS automatycznie sprawdza, czy nowy system AXIS OS także jest podpisany. W przypadku braku podpisu uaktualnienie zostaje odrzucone.

Proces podpisywania kodu systemu operacyjnego rozpoczyna się od obliczenia wartości skrótu kryptograficznego. Następnie wartość jest podpisywana kluczem prywatnym z pary klucza prywatnego i publicznego, zanim podpis zostanie dodany do obrazu systemu AXIS OS.

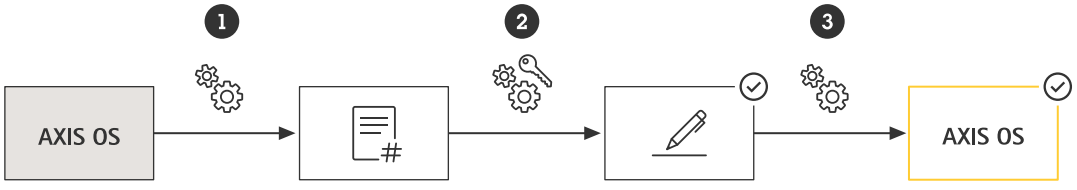

Figure 2. Proces podpisywania kodu systemu operacyjnego.

1 *Zostaje utworzona wartość skrótu kryptograficznego dla systemu AXIS OS.*
2 *Zostaje utworzony podpis przez połączenie skrótu i klucza prywatnego.*

3 *Podpis jest dodawany do wersji i pliku binarnego systemu AXIS OS.*

Przed uaktualnieniem musi zostać zweryfikowana autentyczność aktualizacji oprogramowania. Służy do tego klucz publiczny (dostarczany z produktem Axis), za pomocą którego można sprawdzić, czy wartość skrótu została rzeczywiście została podpisana przy użyciu pasującego klucza prywatnego. Dzięki obliczeniu wartości skrótu i porównaniu go z tą zweryfikowaną wartością skrótu z podpisu można sprawdzić integralność. Gdyby się okazało, że podpis jest nieprawidłowy lub obraz systemu AXIS OS został zmanipulowany, uruchamianie urządzenia Axis zostałoby przerwane.

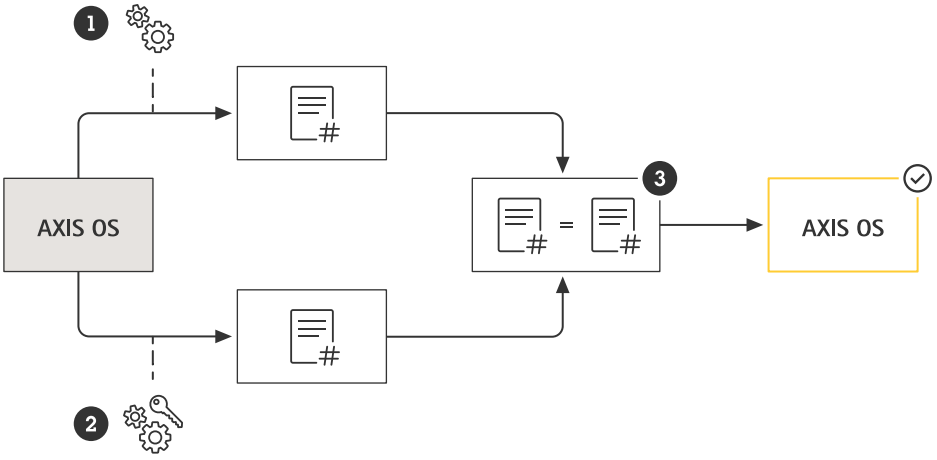

Figure 3. Proces weryfikacji podpisanego systemu operacyjnego.

1 *Obliczanie wartości skrótu systemu AXIS OS*
2 *Sprawdzanie wartości skrótu z podpisu za pomocą klucza publicznego*
3 *Podpis zostaje pomyślnie zweryfikowany tylko wtedy, gdy wartości wynikowe są zgodne.*

Podpisany system operacyjny Axis jest oparty na przyjętej w branży metodzie szyfrowania RSA. Klucz prywatny jest przechowywany w ściśle chronionej lokalizacji w firmie Axis, natomiast klucz publiczny jest osadzany w urządzeniach Axis. Podpis poświadcza integralność całego obrazu oprogramowania. Podpis podstawowy służy do weryfikacji kilku podpisów dodatkowych podczas rozpakowywaniu obrazu.

Na potrzeby testowych i niestandardowych kompilacji firma Axis wdrożyła mechanizm zatwierdzania poszczególnych urządzeń w celu zezwolenia na obrazy przygotowane poza standardowymi procesami produkcji. Obraz ten zawiera kod podpisany przy użyciu klucza przeznaczonego do tego celu po zatwierdzeniu zarówno przez właściciela, jak i Axis, w wyniku czego powstaje niestandardowy podpis. Certyfikat umożliwia uruchomienie niestandardowego obrazu wyłącznie na zatwierdzonych urządzeniach, które są identyfikowane za pomocą ich unikatowych numerów seryjnych i identyfikatorów układów. Niestandardowe certyfikaty może tworzyć tylko firma Axis, ponieważ to ona ma klucz potrzebny do ich podpisania.

3 Wiarygodna tożsamość urządzenia

W nowoczesnych systemach z zasadami bezpieczeństwa opartego na zerowym zaufaniu („nie wolno ufać, zawsze trzeba weryfikować") możliwość weryfikacji pochodzenia urządzenia, jego autentyczności i połączeń jest nadrzędną potrzebą. Urządzenie sieciowe może zweryfikować integralność i autentyczność w sposób przypominający okazanie paszportu funkcjonariuszom na lotnisku w celu weryfikacji tożsamości.

3.1 Bezpieczna identyfikacja urządzenia za pomocą identyfikatora urządzenia Axis

Międzynarodowy standard *IEEE 802.1AR* określa metodę automatyzowania i zabezpieczania identyfikacji urządzenia za pośrednictwem sieci. Jeśli komunikacja jest przekazywana do osadzonego kryptograficznego modułu obliczeniowego, urządzenie może zwrócić wiarygodną odpowiedź identyfikującą zgodnie z tym standardem. Ta wiarygodna odpowiedź może zostać wykorzystana przez infrastrukturę sieciową do zautomatyzowanego i bezpiecznego wdrożenia urządzenia w sieci inicjowania obsługi administracyjnej w celu jego wstępnego skonfigurowania oraz zainstalowania aktualizacji oprogramowania.

Aby zachować zgodność ze standardem IEEE 802.1AR, większość naszych urządzeń jest produkowana z unikatowym dla danego urządzenia i fabrycznie przypisanym certyfikatem nazywanym identyfikatorem urządzenia Axis (IEEE 802.1AR Initial device identifier, IDevID — pierwszy identyfikator urządzenia). Identyfikator urządzenia Axis jest bezpiecznie przechowywany w zabezpieczonym przed manipulacją bezpiecznym magazynie kluczy udostępnianym przez kryptograficzny moduł obliczeniowy w samym urządzeniu. Identyfikator ten jest unikatowy dla każdego urządzenia Axis i zaprojektowany tak, aby potwierdzał pochodzenie danego urządzenia.

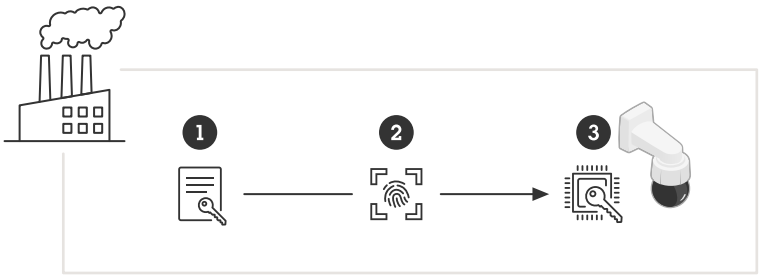

Figure 4. Podczas procesu produkcji urządzenia unikatowy identyfikator urządzenia Axis (2) jest zapisywany w bezpiecznym magazynie kluczy urządzenia (3).

1 *Infrastruktura kluczy (PKI) identyfikatorów urządzeń Axis*
2 *Identyfikator urządzenia axis*
3 *Identyfikator urządzenia Axis bezpiecznie przechowywany w chronionym przed manipulacją bezpiecznym magazynie kluczy udostępnianym przez kryptograficzny moduł obliczeniowy w urządzeniu Axis.*

Standard IEEE 802.1AR jest oparty na standardzie IEEE 802.1X dotyczącym kontroli dostępu do sieci, która jest domyślnie włączona w przypadku urządzeń Axis z wybranym identyfikatorem urządzenia Axis. Pozwala to na bezpieczne zidentyfikowanie i uwierzytelnienie urządzenia Axis przez infrastrukturę IT obsługującą standard 802.1X — nawet w domyślnym stanie fabrycznym urządzenia.

Certyfikat identyfikatora urządzenia Axis jest dostępny w różnych konfiguracjach kryptograficznych (2048-bitowy klucz RSA, 4096-bitowy klucz RSA, ECC-P256). Są one domyślnie włączone, aby umożliwiać bezpieczne połączenia z urządzeniami i identyfikację przez funkcję kontroli dostępu do sieci IEEE 802.1X, a także HTTPS.

Axis zarządza własną, specjalną infrastrukturą kluczy publicznych (public key infrastructure — PKI) IEEE 802.1AR w celu fabrycznego przypisywania identyfikatorów urządzeń Axis podczas produkcji. Identyfikator urządzenia Axis jest podpisany przez certyfikat pośredni, który z kolei jest podpisany przez certyfikat główny Axis. Zarówno główny urząd certyfikacji, jak i pośrednie urzędy certyfikacji są bezpiecznie przechowywane w kryptograficznych modułach obliczeniowych, odseparowanych geograficznie. Zapobiegnie to ich złośliwej

kradzieży w razie włamania do obiektów produkcyjnych Axis. Więcej informacji na temat infrastruktury PKI Axis można znaleźć na stronie *www.axis.com/support/public-key-infrastructure-repository*.

Figure 5. Infrastruktura kluczy publicznych (PKI) IEEE 802.1AR Axis na potrzeby fabrycznego przypisywania identyfikatorów urządzeń Axis podczas produkcji. Identyfikator urządzenia Axis (1), który jest certyfikatem zawierającym numer seryjny produktu, jest podpisany przez pośredniczący urząd certyfikacji identyfikatorów urządzeń Axis (2), który z kolei jest podpisany przez główny urząd certyfikacji identyfikatorów urządzeń Axis (3). Do bezpiecznego fabrycznego przypisywania identyfikatorów są używane specjalne sprzętowe moduły zabezpieczeń.

A Odniesienie
B Podpisanie

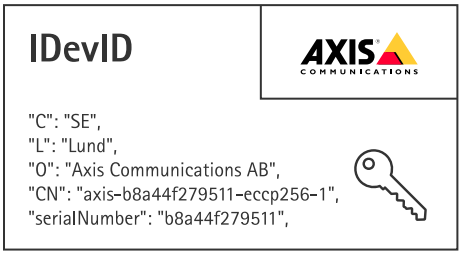

Figure 6. Przykładowy identyfikator urządzenia Axis.

3.2 Bezpieczne wdrożenie w sieci

Przed oddaniem kupionego urządzenia Axis można je zbadać ręcznie. Na podstawie wzrokowej kontroli urządzenia oraz swojej dotychczasowej wiedzy o wyglądzie oraz ogólnym charakterze produktów Axis, można dojść do przekonania, że urządzenie pochodzi od firmy Axis. Jednak taka kontrola jest możliwa tylko wtedy, gdy się ma fizyczny dostęp do urządzenia. Jak więc w przypadku komunikowania się z urządzeniem przez sieć zyskać pewność, że jest to właściwe urządzenie, i jak zweryfikować jego tożsamość? Urządzenia w sieci ani programy na serwerach nie mogą przeprowadzać kontroli fizycznej. Ze względów bezpieczeństwa początkowe interakcje z nowym urządzeniem często podejmuje się w sieci zamkniętej, w której możliwa jest bezpieczne zainicjowanie obsługi administracyjnej urządzeń.

Identyfikator urządzenia Axis dostarcza sieci nadający się do weryfikacji kryptograficznej dowód, że dane urządzenie zostało wyprodukowane przez Axis oraz że połączenie sieciowe z tym urządzeniem jest rzeczywiście przez to urządzenie obsługiwane. Identyfikatora urządzenia Axis można użyć podczas uwierzytelniania zgodnie ze standardem IEEE 802.1X w celu uzyskania dostępu do sieci inicjowania obsługi administracyjnej, w której przeprowadza się aktualizacje oprogramowania oraz konfigurację urządzenia Axis, zanim zostanie ono przeniesione do sieci produkcyjnej.

Dzięki funkcji identyfikatorów urządzeń Axis można podwyższyć ogólny poziom bezpieczeństwa środowiska i przyspieszyć wdrożenia urządzeń, ponieważ pozwala ona na instalowanie oraz konfigurowanie urządzeń przy użyciu bardziej zautomatyzowanych i ekonomicznych mechanizmów kontroli.

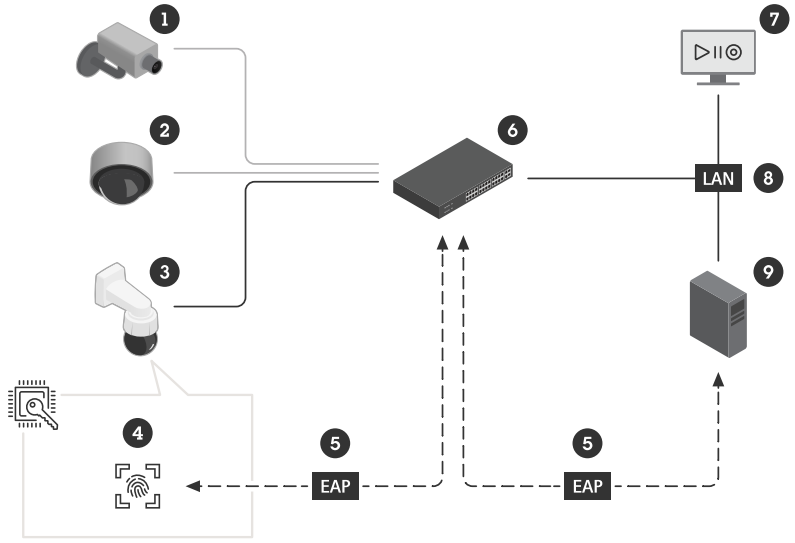

Figure 7. Bezpieczne wdrożenie w sieci. Można poinstruować serwer uwierzytelniania (9), aby automatycznie akceptował urządzenia Axis (3) w sieci (8) i systemie do zarządzania materiałem wizyjnym (7). W tym celu można wykorzystać numery seryjne urządzeń i identyfikator urządzenia Axis (4) jako odcisk palca, czyli dane uwierzytelniające.

1 *Urządzenie nieautoryzowane (trzeba je wdrożyć ręcznie)*
2 *Urządzenie innego producenta*
3 *Urządzenie Axis*
4 *Identyfikator urządzenia Axis, bezpiecznie przechowywany w chronionym przed manipulacjami bezpiecznym magazynie kluczy*
5 *Uwierzytelnianie dostępu urządzenia Axis do sieci zgodnie ze standardem 802.1X EAP-TLS za pomocą certyfikatu identyfikatora urządzenia Axis*
6 *Zarządzany przełącznik (urządzenie uwierzytelniające)*
7 *System zarządzania materiałem wizyjnym (weryfikacja urządzenia)*
8 *Sieć lokalna chroniona przy użyciu protokołu 802.1X*
9 *RADIUS (sieciowy serwer uwierzytelniania)*

Figure 8. Bardziej szczegółowy opis procesu wdrażania. IEEE 802.1AR na potrzeby bezpiecznej tożsamości urządzeń definiuje metodę identyfikacji urządzenia (1) za pośrednictwem żądań w ramach obsługiwanego w standardzie IEEE 802.1X protokołu EAP (EAP-TLS) z wykorzystaniem serwera RADIUS (3) w celu przyznania urządzeniu dostępu do sieci.

1 *Urządzenie Axis*

2 Zarządzany przełącznik (urządzenie uwierzytelniające)
3 Serwer RADIUS (sieciowy serwer uwierzytelniania)
A Nowe połączenie
B EAP-request identity
C EAP-response identity, w tym identyfikator-certyfikat urządzenia Axis, IEEE 802.1AR IDevID
D RADIUS access-request
E RADIUS access-challenge
F EAP-success

Identyfikator urządzenia Axis nie tylko stanowi dodatkowe, wbudowane źródło zaufania, ale też udostępnia środki umożliwiające śledzenie urządzeń oraz umożliwia okresowe weryfikacje i uwierzytelnianie zgodnie z zasadami sieci opartych na zerowym zaufaniu.

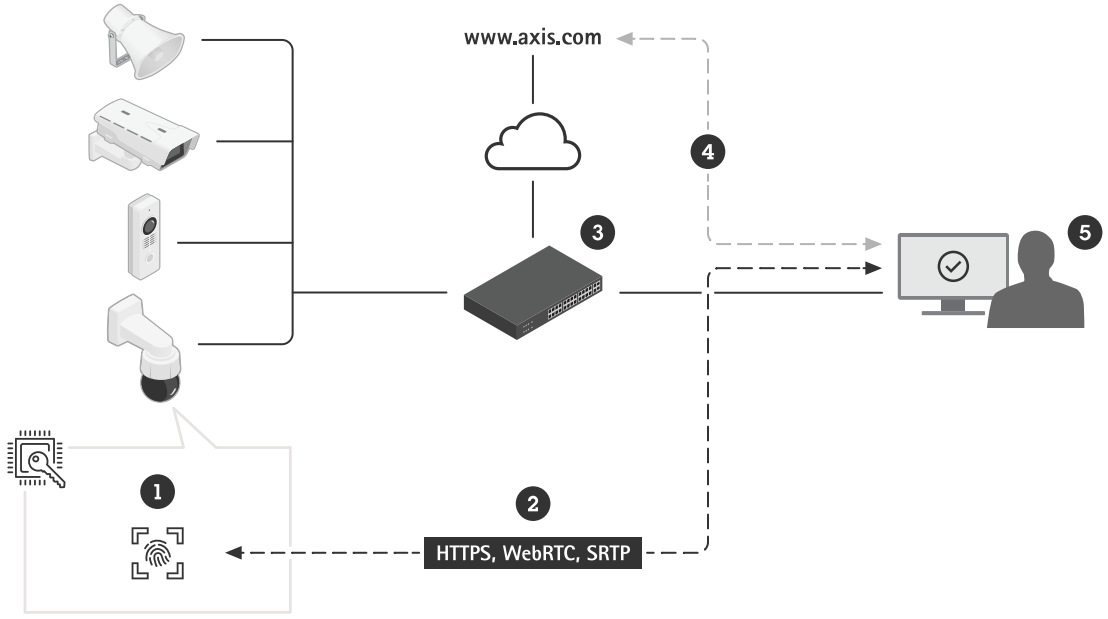

Figure 9. Po bezpiecznym wdrożeniu urządzenia aplikacje (5) działające w innych częściach systemu mogą używać identyfikatora urządzenia Axis (1) i operacji kryptograficznych do weryfikacji i uwierzytelnienia urządzenia w ramach różnego rodzaju komunikacji opartej na protokole TLS (2). Identyfikator urządzenia Axis można zweryfikować za pomocą publicznie dostępnego certyfikatu głównego urzędu certyfikacji Axis (4).

1 Identyfikator urządzenia Axis bezpiecznie przechowywany w chronionym przed manipulacjami bezpiecznym magazynie kluczy
2 Komunikacja oparta na protokole TLS (HTTPS, WebRTC, SRTP)
3 Zarządzany przełącznik
4 Certyfikat głównego urzędu certyfikacji identyfikatora urządzenia Axis (do pobrania ze strony www.axis.com/support/public-key-infrastructure-repository)
5 VMS lub inne oprogramowanie (weryfikacja urządzenia)

4 Bezpieczne przechowywanie kluczy

Tradycyjnie wrażliwe informacje kryptograficzne związane z certyfikatami X.509 (klucze prywatne) są przechowywane w systemie plików urządzenia. Jest on chroniony tylko przez zasady dostępu do konta użytkownika, które zapewniają podstawową ochronę, ponieważ nie jest łatwo złamać zabezpieczenia konta

użytkownika. Jednak w przypadku włamania do systemu takie informacje kryptograficzne są pozbawione ochrony i dostępne dla hakera.

Z perspektywy bezpieczeństwa wspomniany bezpieczny magazyn kluczy jest wprost niezbędny do przechowywania i ochrony informacji kryptograficznych. Bezpieczny magazyn kluczy może służyć nie tylko do przechowywania wrażliwych informacji kryptograficznych uwzględnianych w identyfikatorze urządzenia Axis i podpisanym materiale wizyjnym — podobnie mogą być chronione informacje przekazane przez klientów.

4.1 Bezpieczny magazyn kluczy

Wrażliwe informacje kryptograficzne (klucze prywatne) są przechowywane w urządzeniu w sprzętowym, chronionym przed manipulacjami magazynie kluczy. Zapobiega to złośliwym kradzieżom tych danych nawet w przypadku włamania do systemu. Poza tym klucze prywatne przez cały czas pozostają pod ochroną w bezpiecznym magazynie kluczy — nawet wtedy, gdy są używane. Ewentualny atakujący nie będzie mieć dostępu do bezpiecznego magazynu kluczy i nie będzie mógł podsłuchiwać ruchu sieciowego, uzyskiwać dostępu do sieci przy użyciu kluczy IEEE 802.1X ani wykradać innych kluczy prywatnych.

Bezpieczny magazyn kluczy jest udostępniany przez sprzętowy kryptograficzny moduł obliczeniowy. Zależnie od wymaganego poziomu bezpieczeństwa urządzenie Axis może być wyposażone w jeden lub kilka takich modułów, np. TPM 2.0 (Trusted Platform Module), bezpieczny element lub TEE (Trusted Execution Environment).

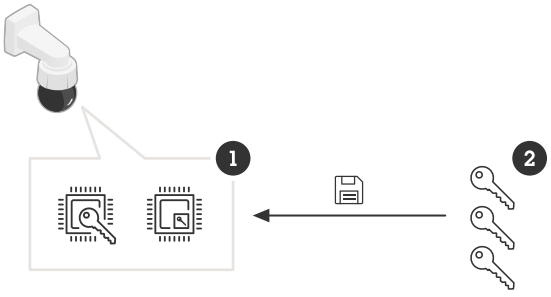

Figure 10. Bezpieczne magazyny kluczy (1) zapewniają ochronę kluczy prywatnych (2) i bezpieczne wykonanie operacji kryptograficznych.

1. *Bezpieczne magazyny kluczy, które mogą być bezpiecznym elementem, modułem TPM lub środowiskiem TEE (w procesorze SoC)*
2. *Klucze prywatne, takie jak identyfikator urządzenia Axis, klucz do podpisywania materiału wizyjnego, klucze do kontroli dostępu, klucze systemu plików i klucze załadowane przez klienta (takie jak IEEE 802.1X czy HTTPS)*

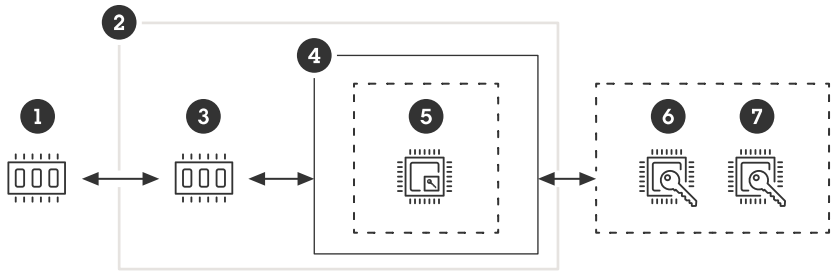

Figure 11. Urządzenia z Axis Edge Vault są wyposażone w sprzętowe kryptograficzne moduły obliczeniowe — bezpieczny element (6) i TPM (7) — montowane na płytce drukowanej tuż obok głównego procesora SoC (4). TEE (5) zaś jest bezpiecznym obszarem w głównym procesorze SoC. Wbudowana w procesor SoC rozruchowa pamięć ROM (3) odpowiada za wykonywanie procedur bezpiecznego startu i zapewnienie, by do rozruchu urządzenia były używane tylko podpisane obrazy systemu operacyjnego z pamięci flash (1).

1. *Pamięć flash (w przypadku podpisanego systemu operacyjnego — system plików dostępny do odczytu i zapisu)*
2. *SoC*
3. *Rozruchowa pamięć ROM (na potrzeby bezpiecznego startu)*
4. *Procesor*
5. *TEE (na potrzeby bezpiecznego magazynu kluczy)*
6. *Bezpieczny element (na potrzeby bezpiecznego magazynu kluczy)*
7. *TPM (na potrzeby bezpiecznego magazynu kluczy)*

Każdy z tych modułów — TPM, bezpieczny element i TEE — zapewnia ochronę kluczy prywatnych i bezpieczne wykonywanie operacji kryptograficznych. W razie włamania do systemu wszelkie operacje nieautoryzowanego dostępu i złośliwej kradzieży danych są blokowane.

4.2 Common Criteria i FIPS 140

Kryptograficzne moduły obliczeniowe mogą być certyfikowane według poziomów ocen Common Criteria Evaluation Level (CC EAL), a także poziomów zgodności standardu FIPS 140 (1–4). Certyfikaty te służą do ustalania poprawności i integralności operacji kryptograficznych oraz do weryfikowania różnych środków przeciwdziałania manipulacjom, takich jak samoweryfikacja, odporność na manipulacje i inne czynniki uodparniające. Informacje na temat tych certyfikatów można znaleźć na karcie danych urządzenia Axis lub w *selektorze produktów Axis*. Firma Axis wymaga, aby jej wbudowane sprzętowe kryptograficzne moduły obliczeniowe były certyfikowane zgodnie z wymogami co najmniej standardów Common Criteria EAL4 i/lub FIPS 140-2/3 Level 2/3.

4.2.1 Common Criteria

Common Criteria (CC), (znany też pod nazwą Common Criteria for Information Technology Security Evaluation), to międzynarodowy standard (ISO/IEC 15408) dotyczący certyfikacji bezpieczeństwa produktów IT. Common Criteria zapewnia producentom i specjalistom ds. wdrożeń ramy na potrzeby określania wymogów w zakresie funkcjonalności i zabezpieczeń w formie celów bezpieczeństwa, które można grupować w profile ochrony.

Te deklarowane cele bezpieczeństwa są następnie oceniane przez certyfikowane niezależne laboratoria testowe zanim produkty zostaną wskazane jako certyfikowane w bazie danych Common Criteria.

Wymagania i dokładność oceny dokonywanej przez laboratorium testowe są wyrażane przez przypisany poziom EAL (Evaluation Assurance Level) — od EAL 1 (przetestowano pod względem funkcjonalności) po EAL 7 (formalnie zweryfikowano projekt i przetestowano). Oznacza to, że Common Criteria może obejmować różne rozwiązania: od systemów operacyjnych i zapór po układy TPM i paszporty.

Więcej informacji o wymaganiach związanych z certyfikacją Common Criteria można znaleźć w witrynie internetowej Common Criteria: *www.commoncriteriaportal.org/*.

4.2.2 FIPS 140

FIPS (Federal Information Processing Standard — federalny standard przetwarzania informacji) 140-2 i 140-3 to wydane przez NIST (National Institute of Standards and Technology) oraz przyjęte jako wymagane przez rządy federalne Stanów Zjednoczonych i Kanady standardy bezpieczeństwa informacji opracowane z myślą o kryptograficznych modułach obliczeniowych i stosowaniu algorytmów kryptograficznych. W 2019 roku FIPS 140-3 zastąpił FIPS 140-2 jako jego zaktualizowana wersja. Walidacja dokonana przez laboratorium certyfikowane przez NIST potwierdza prawidłowe wdrożenie aspektów systemowych i kryptograficznych modułu. Podsumowując, certyfikacja wymaga opisu, specyfikacji i weryfikacji kryptograficznego modułu obliczeniowego, zatwierdzonych algorytmów, zatwierdzonych trybów pracy oraz testów zasilania.

Klienci mają pewność, że ich produkty mogą być użytkowane w zgodzie ze specyfikacjami administracji publicznej. Dzięki temu nie mają najmniejszych powodów do zmartwień podczas audytów prowadzonych przez rozmaite organy. Organizacje, które nie podlegają FIPS 140, mają pewność, że ich produkty są zgodne ze standardami określonymi przez administrację publiczną. Więcej informacji o wymaganiach związanych z certyfikacją FIPS 140-2 i FIPS 140-3 można znaleźć w witrynie internetowej instytutu NIST pod adresem *www.nist.gov*

Aby cały system był zgodny ze standardem FIPS 140, musi być z nim zgodny każdy element tego systemu, na przykład system zarządzania materiałem wizyjnym, serwer rejestrujący, a także wszelkie podłączone urządzenia, takie jak kamery. Urządzenie jest zgodne ze standardem FIPS 140, gdy jest w nim zastosowany co najmniej moduł z certyfikatem programowym lub moduł z certyfikatem sprzętowym.

Urządzenia Axis z systemem operacyjnym AXIS OS w wersji 12 lub nowszej są wyposażone w programowy (OpenSSL) moduł kryptograficzny Axis z certyfikatem FIPS 140. Większość nowych urządzeń Axis zawiera zarówno sprzętowy moduł kryptograficzny z certyfikatem FIPS 140, jak i moduł programowy. Oznacza to optymalne rozwiązanie polegające na używaniu modułu z certyfikatem programowym do obsługi aplikacji w warstwie oprogramowania, takich jak HTTPS i IEEE 802.1X na poziomie systemu operacyjnego, oraz modułu z certyfikatem sprzętowym na potrzeby bezpiecznego przechowywania kluczy.

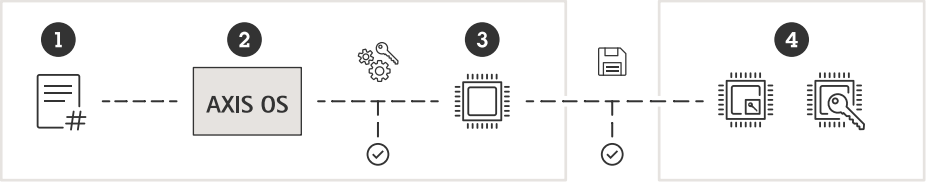

Figure 12. Zastosowanie programowego i sprzętowego modułu kryptograficznego zgodnego ze standardem FIPS 140 w urządzeniu Axis. Aplikacje (1) są obsługiwane przez moduł kryptograficzny Axis wbudowany w system operacyjny AXIS OS (2) urządzenia Axis. Moduł kryptograficzny Axis wykonuje operacje kryptograficzne — zarówno symetryczne, jak i asymetryczne — używając procesora SoC (3) i/lub wbudowanych sprzętowych kryptograficznych modułów obliczeniowych (4) w celu bezpiecznego przechowywania kluczy.

1 Aplikacje wymagające kryptografii lub oparte na TLS (takie jak HTTPS, webRTC i 802.1X)

2 *AXIS OS z wbudowanym programowym modułem kryptograficznym; certyfikat NIST: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4621*
3 *SoC*
4 *Wbudowane sprzętowe kryptograficzne moduły obliczeniowe*

4.3 Ochrona kluczy prywatnych

Wydobycie danych klucza prywatnego pozwoliłoby złośliwemu atakującemu na podsłuchiwanie ruchu sieciowego szyfrowanego protokołem HTTPS lub podszycie się pod rzeczywiste urządzenie i uzyskanie dostępu do sieci chronionej za pomocą protokołu 802.1X.

W celu bezpiecznej komunikacji urządzenia Axis obsługują różne protokoły oparte na protokole TLS (Transport Layer Security). Identyfikator urządzenia Axis (IEEE 802.1AR), HTTPS (szyfrowanie w sieci) i 802.1X (kontrola dostępu do sieci) opierają się na kryptograficznej ochronie informacji X.509.

Certyfikaty cyfrowe X.509 protokołu TLS używają certyfikatu i odpowiadającej mu pary kluczy — publicznego i prywatnego — do komunikacji między dwoma hostami w sieci. Klucz prywatny jest przechowywany w bezpiecznym magazynie kluczy i nigdy tego magazynu nie opuszcza, nawet wtedy, gdy jest używany do odszyfrowania danych. Sam certyfikat i klucz publiczny są znane, mogą być udostępniane przez urządzenie Axis i służą do szyfrowania danych.

4.4 Ochrona kluczy do kontroli dostępu

Ochrona informacji kryptograficznych używanych w rozwiązaniach kontroli dostępu Axis, takich jak Open Supervised Device Protocol (OSDP) Secure Channel, to kolejny przykład ilustrujący duże znaczenie sprzętowej ochrony przechowywanych kluczy.

OSDP Secure Channel to powszechnie stosowany schemat szyfrowania i uwierzytelniania oparty na standardzie AES-128, służący do ochrony komunikacji między kontrolerami drzwi a urządzeniami peryferyjnymi, na przykład czytnikami.

Klucz symetryczny AES, klucz Secure Channel Base Key (SCBK), używany przez zarówno kontroler drzwi, jak i czytnik, służy do inicjowania wzajemnego uwierzytelniania, a następnie generowania zestawu kluczy sesyjnych w celu szyfrowania danych przesyłanych między kontrolerami drzwi i czytnikami.

Aby uzyskać prawdziwie kompleksowe bezpieczeństwo, klucz główny (master key — MK) i klucz SCBK muszą być bezpiecznie przechowywane w bezpiecznym magazynie kluczy sieciowego kontrolera drzwi Axis. Klucz główny wyprowadza unikatowy klucz SCBK dla każdego podłączonego czytnika Axis. Indywidualny klucz SCBK, bezpiecznie przekazywany w fazie instalacji do czytnika Axis, również musi być bezpiecznie przechowywany w bezpiecznym magazynie kluczy czytnika. Czytnik ma bardziej krytyczne znaczenie, zważywszy, że zwykle jest instalowany po niezabezpieczonej stronie drzwi.

W ten sposób klucze OSDP Secure Channel są chronione po obu stronach w środowisku zabezpieczonym sprzętowo. Zapobiega to złośliwym kradzieżom tych danych nawet w przypadku włamania do systemu.

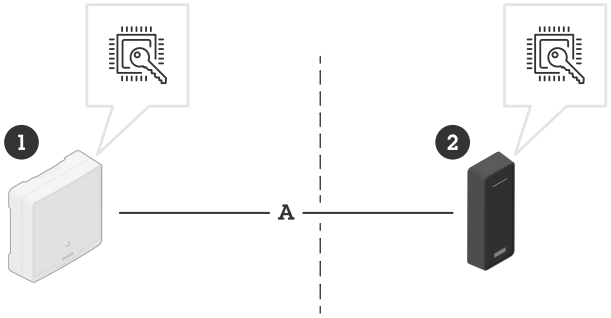

Figure 13. Uzyskiwanie kompleksowego bezpieczeństwa za pomocą bezpiecznego magazynu kluczy w systemie kontroli dostępu. Klucz główny i indywidualny klucz SCBK są przechowywane w bezpiecznych magazynach kluczy w urządzeniach po obu stronach drzwi.

1 Kontroler drzwi Axis zainstalowany po bezpiecznej stronie drzwi
2 Czytnik Axis zainstalowany po niezabezpieczonej stronie drzwi
A Komunikacja OSDP Secure Channel

4.5 Ochrona kluczy systemu plików

Działające urządzenie Axis zawiera konfigurację i informacje związane z danym klientem. Podobnie jest w przypadku urządzenia Axis transportowanego do klienta od dystrybutora lub integratora systemów, który wykonał usługi wstępnej konfiguracji. Mając fizyczny dostęp do urządzenia Axis, złośliwy podmiot może próbować uzyskać informacje z systemu plików przez odmontowanie pamięci flash i uzyskanie do niej dostępu za pomocą czytnika pamięci flash. Dlatego ochrona systemu plików dostępnego do odczytu i zapisu przed wykradaniem wrażliwych danych lub ingerowaniem w konfiguracje jest ważnym zabezpieczeniem na wypadek kradzieży urządzenia Axis lub włamania do systemu.

Bezpieczny magazyn kluczy zapobiega złośliwemu wyprowadzaniu danych i manipulowaniu konfiguracją przez wymuszanie silnego szyfrowania systemu plików. W przypadku odłączenia urządzenia Axis od zasilania dane dostępne w systemie plików są szyfrowane. Podczas uruchamiania urządzenia system plików dostępny do odczytu i zapisu jest odszyfrowywany za pomocą 256-bitowego klucza AES-XTS-Plain64, dzięki czemu może zostać zamontowany i być używany przez urządzenie Axis. Klucz szyfrowania systemu plików jest generowany specjalnie dla każdego urządzenia z osobna w ramach jego fabrycznego

konfigurowania i generowany ponownie po każdej aktualizacji oprogramowania, a zatem nie jest taki sam przez cały okres eksploatacji urządzenia.

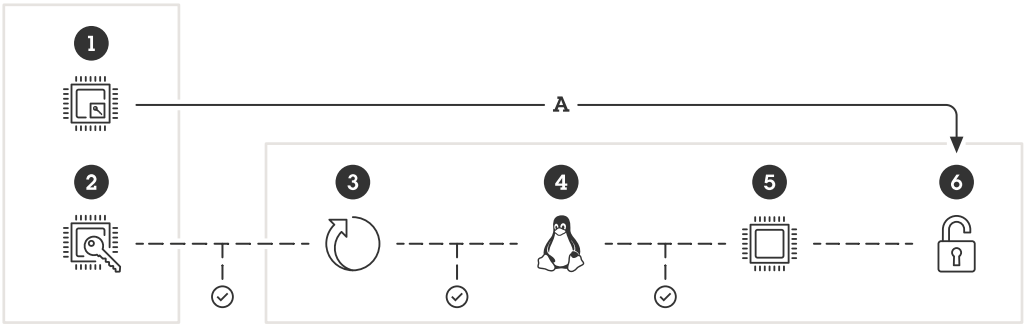

Figure 14. TEE (1) i rozruchowa pamięć ROM (2) są wbudowane w procesor SoC. Podczas uruchamiania urządzenia system plików dostępny do odczytu i zapisu (6) jest odszyfrowywany (przez TEE), dzięki czemu system plików może zostać zamontowany i być używany przez urządzenie Axis. Podczas uruchamiania każda część łańcucha — program inicjujący (3), jądro systemu Linux (4) i bazowy system plików (5) — zostaje zweryfikowana i uwierzytelnia kolejny podsystem w pamięci flash. Ostatecznym wynikiem tego procesu jest zweryfikowany bazowy system plików.

1 *TEE*
2 *Rozruchowa pamięć ROM*
3 *Program inicjujący*
4 *Jądro systemu Linux*
5 *Bazowy system plików*
6 *System plików dostępny do odczytu i zapisu*
A *TEE odszyfrowuje system plików dostępny do odczytu i zapisu.*

5 Ochrona przed manipulacją w materiale wizyjnym

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

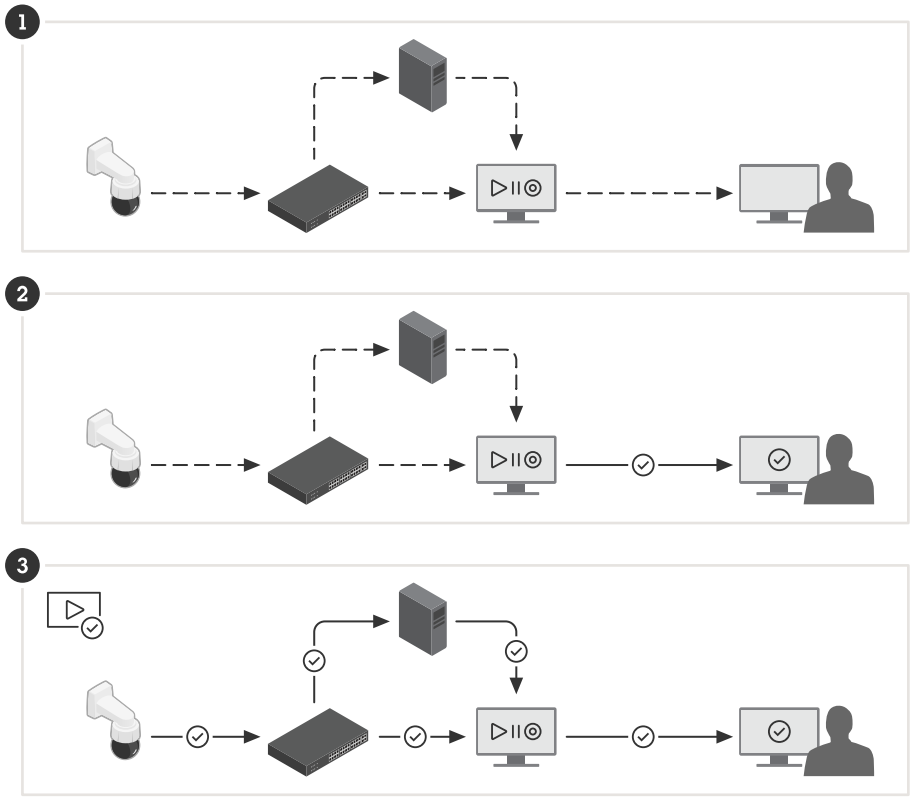

Figure 15. Weryfikacja autentyczności materiału wizyjnego.

1 *Materiał wizyjny przechodzi wiele etapów w drodze od kamery do osoby oglądającej nagranie. Wprawny przestępca może zmanipulować materiał wizyjny na każdym z tych etapów pośrednich.*
2 *Ponieważ podczas eksportu materiału system zarządzania materiałem wizyjnym dodaje do niego znak wody, na niektórych etapach jest dokonywana weryfikacja, ale nie daje ona gwarancji, że materiał wizyjny nie został wcześniej poddany manipulacji.*
3 *Podpis dodany do materiału wizyjnego zapewnia dostępność środków pozwalających na rzetelne ustalenie, czy materiał ten nie został poddany manipulacji na żadnym etapie drogi od kamery do osoby oglądającej wyeksportowane nagranie. Materiał wizyjny można prześledzić z powrotem do urządzenia, które go nagrało.*

5.1 Podpisany materiał wizyjny

Opracowana przez Axis funkcja podpisanego materiału wizyjnego, proaktywnie udostępniona na zasadach open source, pozwala na stosowanie podpisu w strumieniu wideo w celu zabezpieczenia go przed manipulacją i na potrzeby weryfikacji jego pochodzenia, czyli ustalenia, która kamera dany strumień wygenerowała. W ten sposób można dowieść autentyczności nagrania wideo bez konieczności odtwarzania całego łańcucha pochodzenia pliku wideo.

Po nagraniu incydentu przez kamerę z systemu dozorowego policja może otrzymać nagranie wideo w formie plików wyeksportowanych na urządzenie pamięci USB i zapisać je w systemie zarządzania materiałem dowodowym (evidence management system — EMS). W czasie eksportu materiału wizyjnego z kamery policjant widzi, czy materiał ten 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.

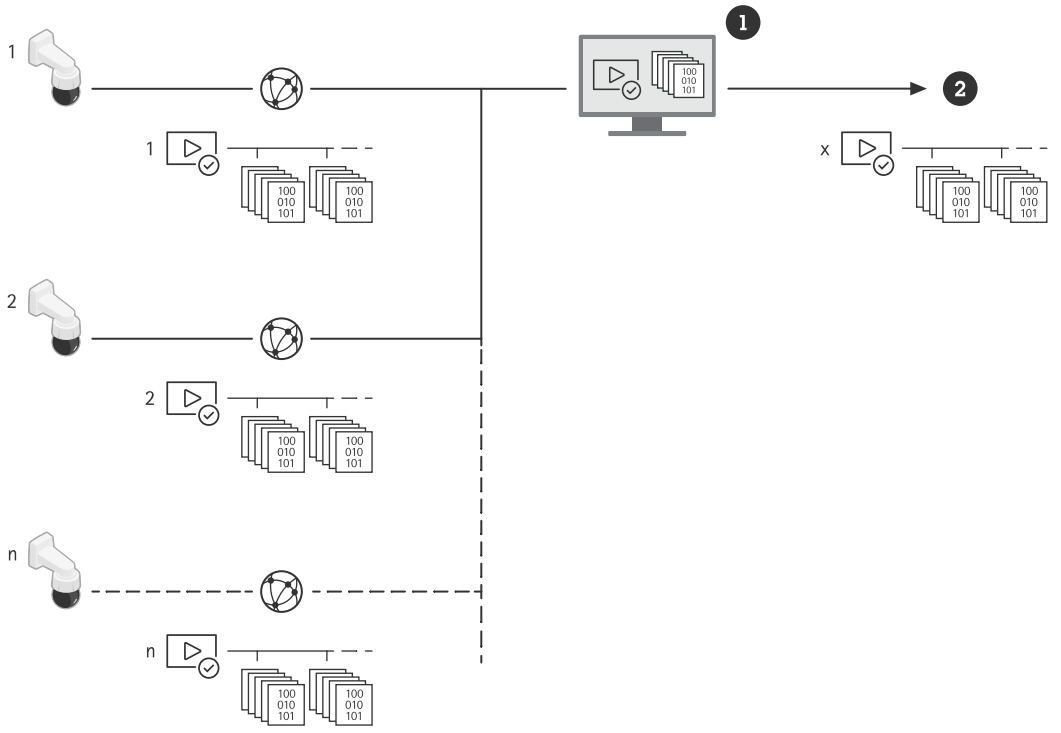

Figure 16. Podpis jest dodawany już w kamerze, co pozwala na weryfikację treści na każdym etapie: od źródła po ostateczne wykorzystanie materiału wizyjnego.

1 *VMS*
2 *Eksport materiału wizyjnego na płytę CD, pamięć USB bądź stronę internetową albo do poczty e-mail*

Każda kamera podpisuje materiał wizyjny za pomocą własnego unikatowego klucza, który jest przechowywany w bezpiecznym magazynie kluczy. W celu dodania podpisu do strumienia wideo kamera

oblicza skrót każdej klatki wideo, dodaje do niego metadane i podpisuje taki złożony skrót. Następnie podpis jest umieszczany w strumieniu, w przeznaczonych na niego polach metadanych (nagłówku SEI).

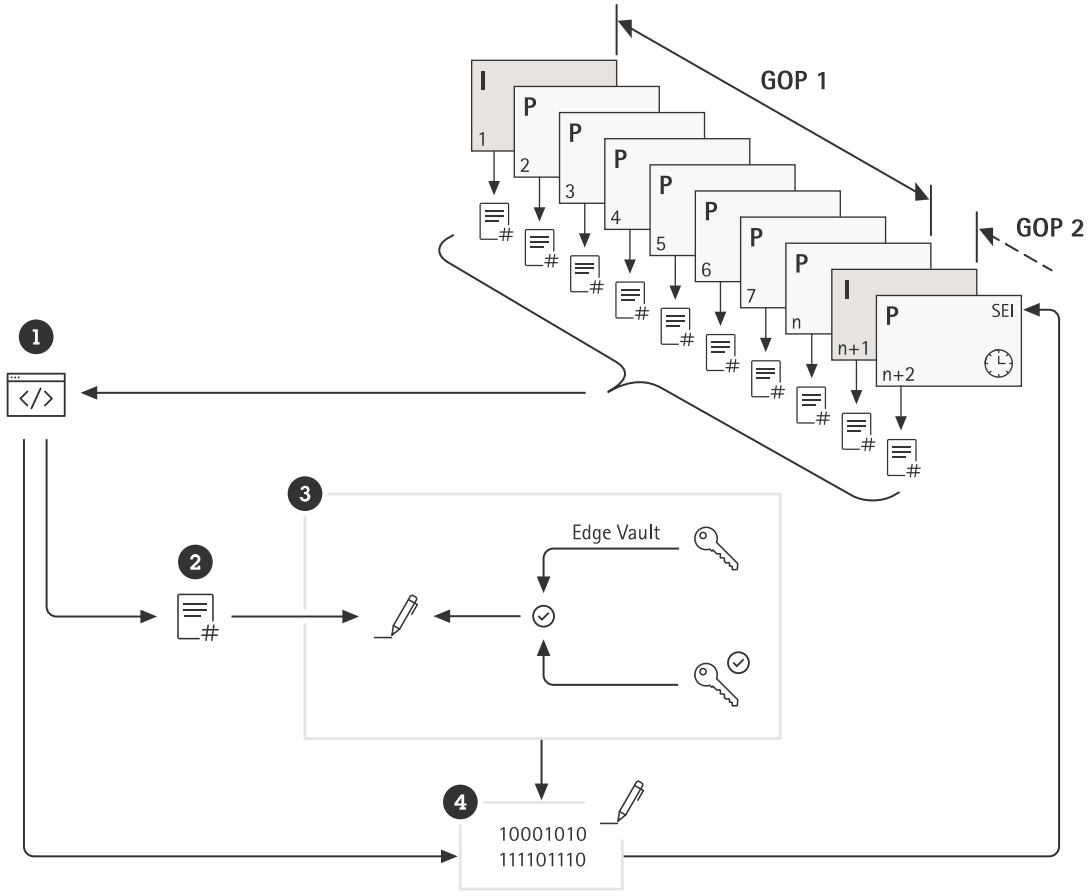

Figure 17. Ilustracja sposobu dodawania podpisu do strumienia wideo. Skrót zawartości każdej klatki grupy obrazów (group of pictures — GOP) jest łączony ze skrótem metadanych (1). Powstaje w ten sposób skrót GOP (2), który jest podpisywany w Edge Vault (3) przy użyciu unikatowego dla urządzenia klucza do podpisywania materiału wizyjnego i klucza poświadczającego. Następnie podpis cyfrowy (4) i metadane (1) są dodawane do tworzonego później nagłówka SEI przekazywanego razem ze strumieniem.

1 *Unikatowe dla urządzenia metadane (identyfikator sprzętu, wersja systemu AXIS OS, numer seryjny i raport o poświadczeniu*) oraz metadane strumienia (licznik GOP i skróty klatek)*
2 *Skrót GOP*
3 *Axis Edge Vault*
4 *Podpis cyfrowy*

* *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.*

Rzeczywiste podpisanie odbywa się przy użyciu unikatowego dla danego urządzenia klucza do podpisywania materiału wizyjnego, który jest poświadczany za pomocą unikatowego dla danego urządzenia klucza poświadczającego. Raport o poświadczeniu jest dołączany do strumienia na początku, a potem w pewnych odstępach czasowych, zazwyczaj raz na godzinę. Ponieważ metadane zawierają skrót każdej klatki, można weryfikować poprawność poszczególnych klatek. Aby podpisanie było kompletne, należy chronić strukturę grupy obrazów (group of pictures — GOP) materiału wizyjnego. To zabezpieczenie polega na umieszczeniu w

podpisie skrótu pierwszej klatki kluczowej następnej grupy GOP. Wyklucza ono możliwość niezauważonych usunięć lub zmian kolejności klatek. W mało prawdopodobnym przypadku utraty klatek podczas przesyłania strumieniowego lub ich uszkodzenia podczas przechowywania zostaną one podobnie wykryte i zgłoszone.

6 Słownik pojęć

Identyfikator urządzenia Axis — unikatowy dla urządzenia certyfikat oraz powiązane z nim klucze, za pomocą których można potwierdzić autentyczność urządzenia Axis. Urządzenie Axis jest fabrycznie wyposażone w identyfikator urządzenia Axis, który jest przechowywany w bezpiecznym magazynie kluczy. Identyfikator urządzenia Axis jest zgodny z międzynarodowym standardem IEEE 802.1AR (Initial device identifier, IDevID — pierwszy identyfikator urządzenia), w którym określono metodę automatycznej, bezpiecznej identyfikacji.

Axis Edge Vault — sprzętowa platforma cyberbezpieczeństwa chroniąca urządzenie Axis. Rozwiązanie to bazuje na mocnych podstawach zapewnianych przez kryptograficzne moduły obliczeniowe (bezpieczny element i TPM) oraz zabezpieczenia procesora SoC (TEE i bezpieczny start), a także na specjalistycznej wiedzy z zakresu bezpieczeństwa urządzeń brzegowych.

Certyfikat — podpisany dokument, który poświadcza pochodzenie i właściwości pary kluczy: publicznego i prywatnego. Certyfikat jest podpisany przez urząd certyfikacji i jeśli dany urząd certyfikacji jest dla systemu wiarygodny, wiarygodne będą też wystawione przez niego certyfikaty.

Urząd certyfikacji — źródło zaufania dla łańcucha certyfikatów. Służy do potwierdzania autentyczności i wiarygodności bazowych certyfikatów.

Common Criteria — międzynarodowy standard certyfikacji bezpieczeństwa produktów IT. Znany jest też pod nazwą Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408.

FIPS 140 — grupa amerykańskich standardów bezpieczeństwa rozwiązań komputerowych, które służą do zatwierdzania kryptograficznych modułów obliczeniowych. FIPS (Federal Information Processing Standard — federalny standard przetwarzania informacji) 140 określa wymogi dotyczące sposobów projektowania i wdrażania modułu kryptograficznego w celu obniżenia ryzyka manipulacji w module.

Niezmienna pamięć ROM (read-only memory — pamięć operacyjna tylko do odczytu) — pamięć operacyjna, w której są bezpiecznie przechowywane zaufane klucze publiczne, i program używany do porównywania podpisów, aby nie można było ich podmienić.

Inicjowanie obsługi administracyjnej — 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 klucza publicznego — system kryptografii asymetrycznej, w którym dowolna osoba może zaszyfrować wiadomość za pomocą *klucza publicznego* odbiorcy, ale tylko odbiorca może tę wiadomość odszyfrować za pomocą swojego *klucza prywatnego*. Można używać tego systemu do szyfrowania i podpisywania wiadomości.

Bezpieczny start — funkcja zapobiegająca ładowaniu nieautoryzowanego oprogramowania podczas uruchamiania urządzenia. Funkcja bezpiecznego startu korzysta z podpisanego systemu operacyjnego, gwarantując, że w celu uruchomienia urządzenia będzie używane tylko autoryzowane oprogramowanie Axis.

Bezpieczny element — kryptograficzny moduł obliczeniowy, który zapewnia sprzętowe, zabezpieczone przed manipulacją przechowywanie kluczy prywatnych i bezpieczne wykonywanie operacji kryptograficznych. W odróżnieniu od modułu TPM interfejsy sprzętowe oraz programowe bezpiecznego elementu nie są zestandaryzowane, więc różnią się w zależności od producenta.

Bezpieczny magazyn kluczy — zabezpieczone przed manipulacją środowisko do ochrony kluczy prywatnych i bezpiecznego wykonywania operacji kryptograficznych. Zapobiega nieautoryzowanemu dostępowi i złośliwemu wykradaniu w przypadku włamania do systemu. W zależności od wymogów bezpieczeństwa urządzenie Axis może mieć jeden lub kilka sprzętowych modułów kryptograficznych, które udostępniają chroniony sprzętowo bezpieczny magazyn kluczy.

Podpisany system operacyjny: oprogramowanie urządzenia, którego kod obraz pliku został cyfrowo podpisany przez zaufany podmiot. Podpisany system operacyjny jest niezbędny w procesie bezpiecznego startu — zapewnia, że urządzenie zostanie uruchomione tylko przy użyciu zaufanego obrazu oprogramowania. W przypadku produktów z systemem operacyjnym AXIS OS urządzenie weryfikuje integralność i autentyczność obrazu oprogramowania urządzenia przed dokonaniem aktualizacji.

Podpisany materiał wizyjny — funkcja, która podtrzymuje i wzmacnia wiarygodność materiału wizyjnego jako dowodu. Podpis dodany do materiału wizyjnego umożliwia detekcję manipulacji w materiale wizyjnym i potwierdzanie autentyczności takiego materiału, stanowi gwarancję, że dany materiał wizyjny nie został naruszony, a także umożliwia powiązanie materiału z konkretną kamerą Axis. Klucze do podpisywania materiału wizyjnego znajdują się w bezpiecznym magazynie kluczy urządzenia Axis.

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

Trusted Execution Environment (TEE) — środowisko zapewniające sprzętowe, zabezpieczone przed manipulacją przechowywanie kluczy prywatnych i bezpieczne wykonywanie operacji kryptograficznych. W odróżnieniu od bezpiecznego elementu i modułu TPM środowisko TEE jest bezpiecznym, odizolowanym sprzętowo obszarem głównego procesora SoC (system-on-chip).

Trusted Platform Module (TPM) — kryptograficzny moduł obliczeniowy, który zapewnia sprzętowe, zabezpieczone przed manipulacją przechowywanie kluczy prywatnych i bezpieczne wykonywanie operacji kryptograficznych. TPM to zestandaryzowane na poziomie międzynarodowym (TPM 1.2, TPM 2.0) podzespoły komputerowe zgodne ze specyfikacją określoną przez *Trusted Computing Group (TCG)*.

Bezpieczeństwo oparte na zerowym zaufaniu — nowoczesne podejście do kwestii bezpieczeństwa środowisk IT, w którym połączone urządzenia i infrastruktura IT (sieci, komputery, serwery, usługi w chmurze, aplikacje itd.) muszą się nawzajem identyfikować, weryfikować i uwierzytelniać, co pozwoli uzyskać wysoki poziom kontroli bezpieczeństwa.

O firmie Axis Communications

Axis umożliwia tworzenie mądrzejszego i bezpieczniejszego świata, tworząc rozwiązania zwiększające bezpieczeństwo i wydajność biznesową. Jako firma z branży technologicznej będąca liderem na rynku, Axis oferuje systemy dozoru wizyjnego, kontroli dostępu, domofonowe i rozwiązania audio. Rozwiązania te są wzbogacone o inteligentne aplikacje analityczne i wysokiej jakości szkolenia

Firma Axis zatrudnia około 4000 zaangażowanych pracowników w ponad 50 krajach i współpracuje z partnerami z sektora technologii oraz integracji systemów na całym świecie, aby dostarczać rozwiązania dla klientów. Firma Axis powstała w 1984 roku, a jej siedziba znajduje się w Lund w Szwecji