Podpisane oprogramowanie sprzętowe, bezpieczne uruchamianie i bezpieczeństwo kluczy prywatnych

Funkcje cyberbezpieczeństwa w produktach Axis

Lipiec 2020

AXIS COMMUNICATIONS

Spis treści

1 **Podsumowanie** 3

1.1 Podpisane oprogramowanie sprzętowe 3

1.2 Bezpieczne uruchamianie 3

1.3 TPM 3

1.4 Axis Edge Vault z ID urządzenia Axis 3

2 **Słownik** 4

3 **Wprowadzenie** 5

4 **Wykrywanie sabotażu oprogramowania sprzętowego** 5

4.1 Podpisywanie oprogramowania sprzętowego 5

4.2 Podpisane oprogramowanie sprzętowe Axis 7

5 **Ochrona łańcucha dostaw przed sabotażem** 7

5.1 Bezpieczne uruchamianie 7

5.2 Bezpieczne uruchamianie Axis 8

5.3 Bezpieczne uruchamianie i niestandardowe certyfikaty oprogramowania sprzętowego 8

6 **Bezpieczeństwo kluczy prywatnych** 8

6.1 Bezpieczne przechowywanie klucza z modułem TPM (Trusted Platform Module) 9

6.2 Certyfikat FIPS 140-2 9

7 **IEEE 802.1AR — weryfikacja urządzeń z ID urządzenia Axis** 9

7.1 Moduł Axis Edge 12

7.2 ID urządzenia Axis 12

1 Podsumowanie

W tym dokumencie opisano niektóre funkcje dostępne w produktach Axis, które mogą zmniejszyć zagrożenia bezpieczeństwa cyfrowego i typy ataków swoistych dla licznika. Są to następujące funkcje:

- podpisane oprogramowanie sprzętowe
- bezpieczne uruchamianie
- moduł TPM (Trusted Platform Module)
- Axis Edge Vault z ID urządzenia Axis.

Poniżej wymieniono zagrożenia:

- sabotaż oprogramowania sprzętowego
- sabotaż łańcucha dostaw
- wyodrębnianie kluczy prywatnych
- nieautoryzowana wymiana urządzenia.

1.1 Podpisane oprogramowanie sprzętowe

Podpisane oprogramowanie sprzętowe jest wdrażane przez dostawcę oprogramowania podpisującego obraz oprogramowania sprzętowego za pomocą klucza prywatnego. Po dołączeniu tego podpisu urządzenie będzie sprawdzać oprogramowanie sprzętowe przed zaakceptowaniem jego instalacji. Jeżeli urządzenie wykryje naruszenie integralności oprogramowania sprzętowego, aktualizacja tego oprogramowania zostanie odrzucona.

1.2 Bezpieczne uruchamianie

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

1.3 TPM

Moduł TPM to składnik udostępniający zestaw funkcji kryptograficznych umożliwiający ochronę informacji przed nieupoważnionym dostępem. Klucze prywatne są przechowywane w module TPM, wszystkie operacje kryptograficzne wymagające użycia klucza prywatnego są wysyłane do niego w celu przetworzenia. Dzięki temu tajny element certyfikatu pozostaje bezpieczny nawet w przypadku naruszenia bezpieczeństwa. Moduł TPM używany w wybranych produktach Axis posiada certyfikat zgodności z normą FIPS 140-2.

1.4 Axis Edge Vault z ID urządzenia Axis

Nowa norma międzynarodowa IEEE 802.1AR zawiera opis procedury automatyzowania i zabezpieczania identyfikacji urządzenia w sieci. W produktach Axis te środki bezpieczeństwa są wdrażane za pomocą modułu Axis Edge Vault i ID urządzenia Axis. Edge Vault może być wykorzystywany do obsługi szyfrowania działającego na certyfikatach przechowywanych w bezpieczny sposób. Prywatne części certyfikatów

pozostają w Edge Vault nawet wtedy, gdy jest on używany. ID urządzenia Axis jest bezpiecznie i na stałe przechowywany w Edge Vault jako certyfikat oznaczony przez Axis jako certyfikat główny, co pozwala na osiągnięcie nowego poziomu bezpieczeństwa urządzeń w cyklu eksploatacji produktu.

2 Słownik

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 dla łańcucha certyfikatów. Służy ono do potwierdzania autentyczności i wiarygodności podstawowych certyfikatów.

FIPS — Federal Information Processing Standard, normy szyfrowania danych 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 służących do porównywania podpisów, tak aby nie można było ich nadpisywać.

Obsługa administracyjna — proces przygotowania i wyposażenia urządzenia w sieci. Wymaga to dostarczenia danych o konfiguracji i ustawień zasad do urządzenia z punktu centralnego. 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 go używać do szyfrowania i podpisywania wiadomości.

TLS — Transport Layer Security, standard internetowy służący do ochrony ruchu w sieci. Protokół TLS oznaczony jest literą S (od słowa secure — zabezpieczenie) w protokole HTTPS.

3 Wprowadzenie

Axis stosuje najlepsze praktyki branżowe w celu zarządzania podatnością na ataki i reagowania na nią w swoich produktach w celu zminimalizowania ekspozycji klienta na zagrożenia cybernetyczne. Nie ma gwarancji, że produkty czy usługi będą wolne od wad, które mogą zostać wykorzystane do przeprowadzenia złośliwych ataków. Nie dotyczy to tylko firmy Axis, ale jest to raczej cecha wspólna wszystkich urządzeń sieciowych. Firma Axis może jednak zagwarantować, że zawsze podejmujemy wspólne wysiłki na każdym możliwym etapie, aby zapewnić, że ryzyko związane z urządzeniami i usługami Axis będzie jak najmniejsze.

Aby uzyskać więcej informacji dotyczących bezpieczeństwa produktów i odkrytych podatności na ataki, zobacz *www.axis.com/support/product-security*. Aby uzyskać więcej informacji na temat działań, które można podjąć w celu ograniczenia ryzyka wystąpienia częstych zagrożeń, należy pobrać Przewodnik po zabezpieczeniach Axis ze strony *www.axis.com/cybersecurity*.

Ten oficjalny dokument opisuje prawdopodobne cyberataki i możliwości zapobiegania im w produktach Axis. Opisuje on szczegółowo, w jaki sposób podpisane oprogramowanie sprzętowe i bezpieczne uruchamianie uniemożliwiają sabotaż oprogramowania sprzętowego oraz łańcucha dostaw. Omówiono również wykorzystanie modułu TPM (Trusted Platform Module) i Axis Edge Vault, które można wykorzystać do zabezpieczenia kluczy prywatnych. W Axis Edge Vault używany jest do bezpiecznego przechowywania ID urządzenia Axis, który pozwala na osiągnięcie nowego poziomu bezpieczeństwa urządzeń.

4 Wykrywanie sabotażu oprogramowania sprzętowego

Jednym z możliwych kierunków ataku, którego może próbować użyć przeciwnik po niepowodzeniu innych prób złamania zabezpieczeń systemu, jest sprawienie, aby właściciel systemu zainstalował zmienione aplikacje, oprogramowanie sprzętowe lub inne moduły oprogramowania. Zmienione oprogramowanie może zawierać szkodliwy kod o określonym przeznaczeniu. Powszechnym zaleceniem jest nieinstalowanie żadnego oprogramowania, które nie pochodzi z w pełni zaufanego źródła. W kontekście systemu wizyjnego może to być 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. Jednak ci przeciwnicy mogą zaistnieć wtedy, kiedy ataku na określony system ma wystarczająco wysoką wartość. Popularnym środkiem zaradczym jest używanie przez dostawcę oprogramowania podpisanego oprogramowania sprzętowego.

4.1 Podpisywanie oprogramowania sprzętowego

Podpisane oprogramowanie sprzętowe jest wdrażane przez dostawcę oprogramowania podpisującego obraz oprogramowania sprzętowego za pomocą klucza prywatnego, który nie jest ujawniany. Po dołączeniu tego podpisu urządzenie będzie sprawdzać oprogramowanie sprzętowe przed zaakceptowaniem jego instalacji. Jeżeli urządzenie wykryje naruszenie integralności oprogramowania sprzętowego, aktualizacja tego oprogramowania zostanie odrzucona.

Proces podpisywania oprogramowania sprzętowego rozpoczyna obliczenie wartości skrótu kryptograficznego. Następnie wartość jest podpisywana kluczem prywatnym pary klucza prywatnego/publicznego przed dołączeniem podpisu do obrazu oprogramowania sprzętowego.

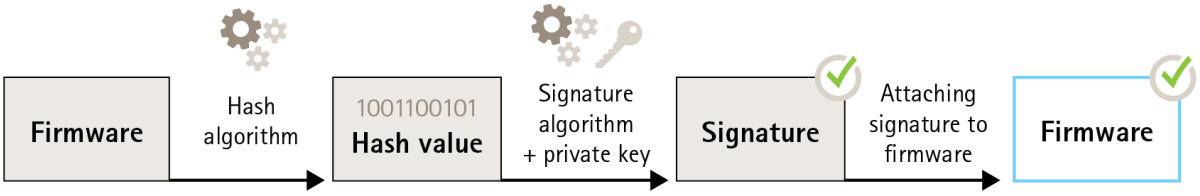

Figure 1. Proces podpisywania oprogramowania sprzętowego.

Przed aktualizacją oprogramowania sprzętowego należy zweryfikować nowe oprogramowanie sprzętowe. Aby upewnić się, że nowe oprogramowanie sprzętowe nie zostało zmienione, używany jest klucz publiczny (dostarczany z produktem Axis) w celu potwierdzenia, że wartość skrótu została rzeczywiście podpisana przy użyciu pasującego klucza prywatnego. Poprzez obliczenie wartości skrótu oprogramowania układowego i porównanie go z tą zwalidowaną wartością skrótu z podpisu można zweryfikować integralność oprogramowania sprzętowego.

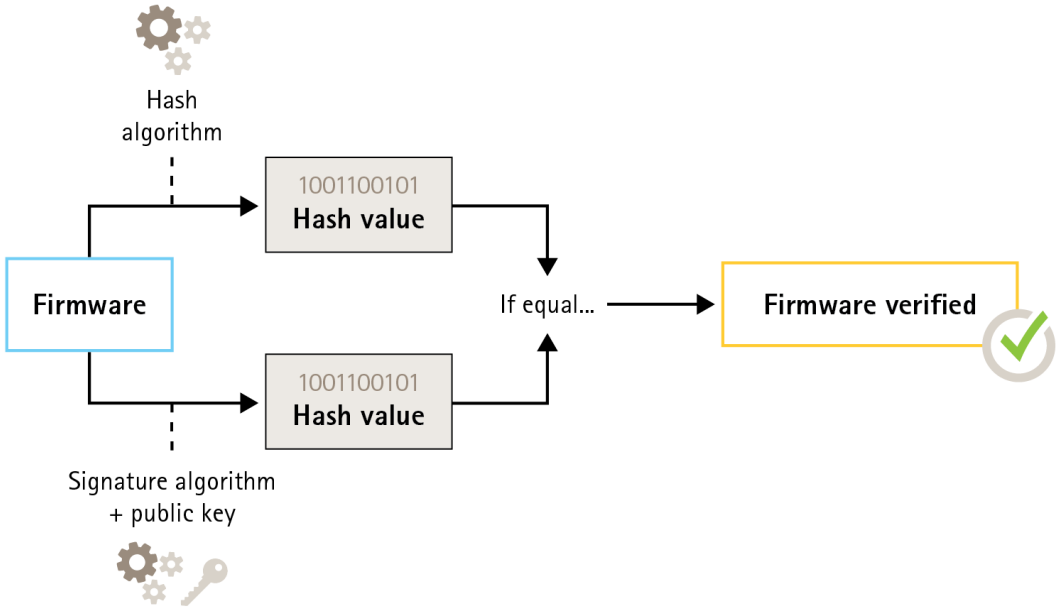

Figure 2. Proces weryfikacji podpisanego oprogramowania sprzętowego.

4.2 Podpisane oprogramowanie sprzętowe Axis

Podpisane przez firmę Axis oprogramowanie sprzętowe jest oparte na zweryfikowanej w branży metodzie szyfrowania RSA. 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 liczby podpisów dodatkowych po rozpakowaniu obrazu.

5 Ochrona łańcucha dostaw przed sabotażem

Podpisywanie oprogramowania sprzętowego chroni urządzenie we wszystkich przyszłych aktualizacjach oprogramowania sprzętowego przed zainstalowaniem uszkodzonego 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 przesyłania, mógłby przeprowadzić atak, na przykład poprzez wpłynięcie na partycję rozruchową urządzenia, omijając sprawdzanie integralności oprogramowania sprzętowego, aby zainstalować zmienione, złośliwe oprogramowanie sprzętowe przed wprowadzeniem urządzenia do użytku.

5.1 Bezpieczne uruchamianie

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

Proces uruchamiania jest inicjowany przez rozruchową pamięć ROM, która dokonuje walidacji programu inicjującego. Bezpieczne uruchamianie polega na sprawdzeniu w czasie rzeczywistym osadzonych podpisów dla każdego bloku oprogramowania sprzętowego ładowanego z pamięci flash. Rozruchowa pamięć ROM służy jako źródło zaufania, a proces uruchamiania działa tylko pod warunkiem, że każdy podpis zostanie zweryfikowany. Każdy element tego łańcucha uwierzytelnia następny element, co skutkuje zweryfikowanym jądrem systemu Linux i zweryfikowaniem systemu plików głównych.

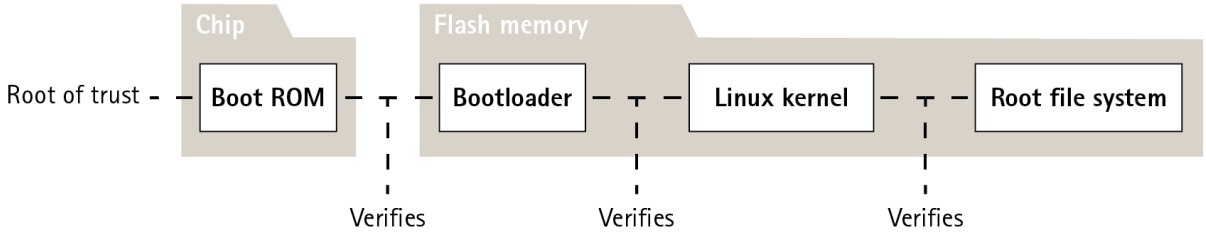

Figure 3. Proces bezpiecznego uruchamiania.

5.2 Bezpieczne uruchamianie Axis

W wielu urządzeniach ważne jest, że nie można zmieniać funkcji niskiego poziomu. Kiedy inne mechanizmy bezpieczeństwa są wbudowane na szczycie oprogramowania niższego poziomu, bezpieczne uruchamianie działa jak podstawowa tarcza bezpieczeństwa, która chroni te mechanizmy przed możliwością obejścia.

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

5.3 Bezpieczne uruchamianie i niestandardowe certyfikaty oprogramowania sprzętowego

Bezpieczny rozruch sprawia, że produkt jest bezpieczniejszy, zmniejsza ryzyko zastosowania innego oprogramowania sprzętowego, dzięki czemu trudniej jest wczytać tymczasowe oprogramowanie sprzętowe, takie jak testowa wersja oprogramowania sprzętowego lub inne niestandardowe oprogramowanie sprzętowe Axis. Firma Axis wdrożyła mechanizm zatwierdzający pojedyncze urządzenia w celu akceptacji takiego oprogramowania sprzętowego. To oprogramowanie sprzętowe jest podpisywane w inny sposób, po zatwierdzeniu zarówno przez właściciela, jak i Axis; użycie tej opcji powoduje utworzenie niestandardowego certyfikatu oprogramowania sprzętowego. Po zainstalowaniu w zatwierdzonych urządzeniach, certyfikat umożliwia użycie niestandardowego oprogramowania sprzętowego, które można uruchomić wyłącznie na zatwierdzonym urządzeniu, na podstawie jego unikatowego numeru seryjnego i identyfikatora procesora. Niestandardowe certyfikaty oprogramowania sprzętowego może utworzyć tylko firma Axis, ponieważ przechowuje klucze do ich podpisywania.

6 Bezpieczeństwo kluczy prywatnych

Urządzenia Axis obsługują protokoły HTTPS (szyfrowanie sieciowe) i 802.1X (kontrola dostępu do sieci), które wykorzystują protokół TLS (Transport Layer Security). Cyfrowe certyfikaty TLS wykorzystują parę kluczy publiczny/prywatny. Klucz prywatny jest przechowywany w urządzeniu, natomiast klucz publiczny jest dołączony do certyfikatu. Trzeba pamiętać, że jeżeli nie jest używany żaden protokół HTTPS ani 802.1X, nie ma kluczy do ochrony.

Przeciwnik może próbować wyodrębnić klucz prywatny i certyfikat z urządzenia i zainstalować je na zaatakowanym komputerze. W przypadku protokołu HTTPS klucz prywatny może służyć do podsłuchu szyfrowanego ruchu sieci pomiędzy urządzeniem a VSM. Lub też, w przypadku podrobienia adresu nadawcy sieci, komputer atakujący może uzyskać dostęp do VMS, podszywając się pod legalne 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 dostać się do konta. Należy pamiętać, że certyfikaty można odwołać w przypadku podejrzenia wystąpienia naruszenia, dzięki czemu klucz prywatny staje się bezużyteczny.

Niektórzy użytkownicy systemów o decydującym znaczeniu mogą być narażeni na zwiększone ryzyko ataku zdeterminowanych i dobrze wyszkolonych przeciwników, którzy próbują dostać się do urządzenia, aby wyodrębnić klucz prywatny. Trusted Platform Module (TPM) przechowuje klucz w taki sposób, żeby nie można go było wyodrębnić, nawet po włamaniu się do urządzenia.

6.1 Bezpieczne przechowywanie klucza z modułem TPM (Trusted Platform Module)

Moduł TPM to składnik udostępniający zestaw określonych funkcji kryptograficznych umożliwiający ochronę informacji przed nieupoważnionym dostępem. Klucz prywatny jest przechowywany w module TPM i nigdy go nie opuszcza. Wszystkie operacje kryptograficzne wymagające użycia klucza prywatnego są wysyłane do modułu TPM w celu przetworzenia. Gwarantuje to, że tajny element certyfikatu nigdy nie opuszcza bezpiecznego środowiska w module TPM i pozostaje bezpieczny nawet w przypadku naruszenia bezpieczeństwa.

6.2 Certyfikat FIPS 140-2

W niektórych produktach i przypadkach użycia mogą obowiązywać wymogi regulacyjne dotyczące stosowania TPM do ochrony informacji, czasami w połączeniu z wymaganiami dotyczącymi zgodności z normą FIPS 140-2. FIPS (Federal Information Processing Standard) 140-2 to norma bezpieczeństwa dla modułów kryptograficznych, wydana w USA przez instytut NIST (National Institute of Standards and Technology).

Zatwierdzenie przez laboratorium certyfikowane przez NIST gwarantuje prawidłowe wdrożenie systemu modułu i kryptografii modułu. Podsumowując, certyfikacja wymaga opisu, specyfikacji i weryfikacji modułu kryptograficznego, zatwierdzonych algorytmów, zatwierdzonych trybów pracy oraz testów zasilania.

Więcej informacji o wymaganiach certyfikacyjnych standardu FIPS 140-2 można znaleźć na stronie NIST *https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards*

6.2.1 Certyfikowany moduł TPM w produktach Axis

Moduł TPM używany w wybranych produktach Axis posiada certyfikat zgodności z normą FIPS 140-2. Jest on certyfikowany do poziomu ochrony 2 normy, co oznacza, że moduł TPM spełnia również wymogi dotyczące autoryzacji opartej między innymi na rolach i dowodach sabotażu.

7 IEEE 802.1AR — weryfikacja urządzeń z ID urządzenia Axis

Po zakupie urządzenia sieciowego Axis można przeprowadzić ręczne sprawdzenie przed rozpoczęciem korzystania z niego. Dzięki wzrokowej kontroli produktu i wykorzystaniu z wcześniejszej wiedzy o wyglądzie i działaniu produktów Axis klient może przekonać się, że jest to rzeczywiście produkt Axis. Taką kontrolę może jednak wykonać tylko osoba, która ma fizyczny dostęp do produktu. Zatem skąd można mieć pewność, że podczas komunikacji z nieobsługiwanym produktem za pośrednictwem sieci komunikujemy się z właściwą jednostką? Że urządzenie nie zostało zastąpione w nieautoryzowany sposób? Ani sprzęt sieciowy, ani oprogramowanie na serwerach nie mogą przeprowadzać kontroli fizycznej. Ze względów

bezpieczeństwa powszechny jest pierwszy kontakt z nowym produktem za pośrednictwem zamkniętej sieci, w której urządzenie może być bezpiecznie obsługiwane.

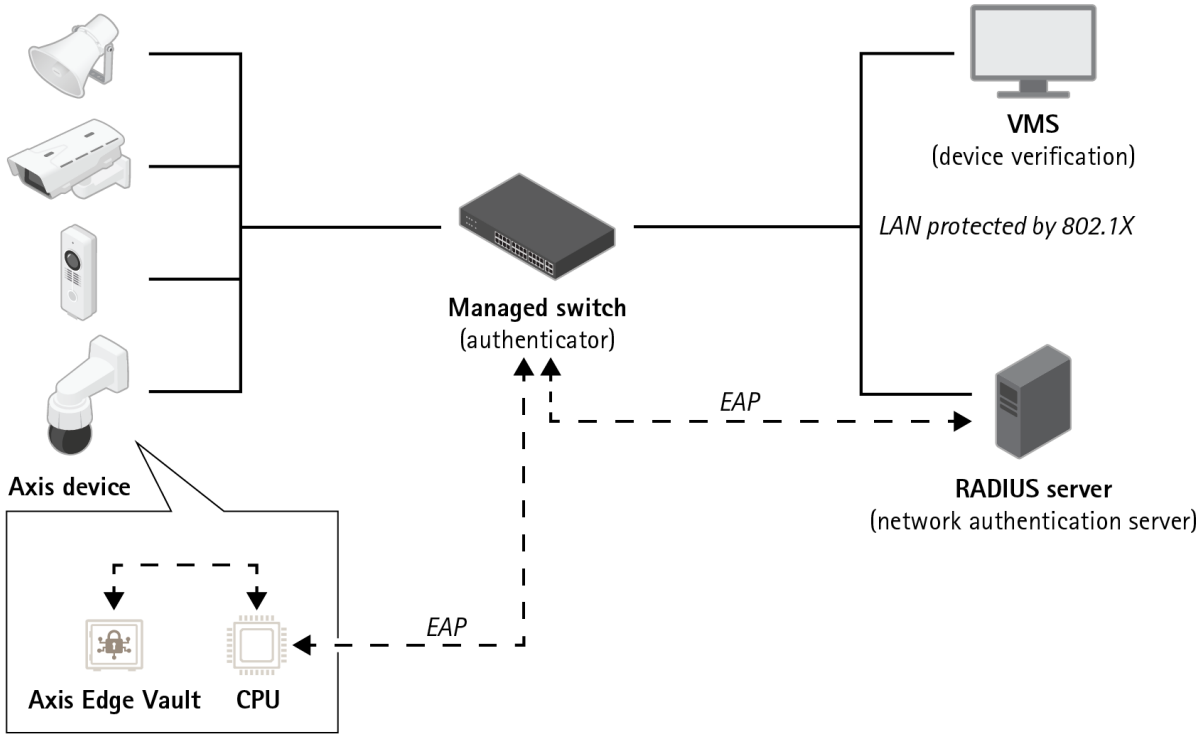

Figure 4. Klienci mogą tak ustawić serwer uwierzytelniania, aby automatycznie akceptował zakupione produkty Axis w sieci przy użyciu numerów seryjnych urządzeń i ID urządzenia Axis.

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

osadzonego bezpiecznego modułu, jednostka może zwrócić zaufaną odpowiedź identyfikującą zgodnie ze standardem.

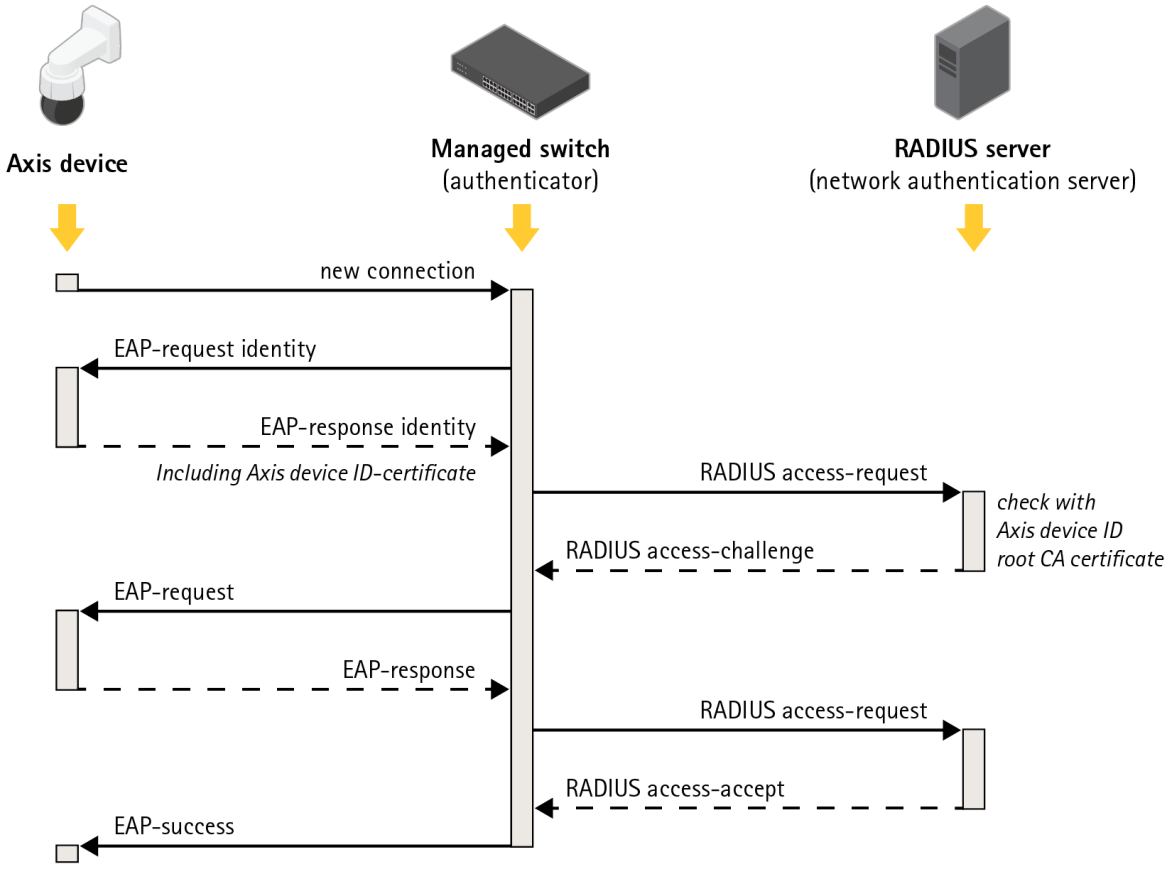

Figure 5. Norma IEEE 802.1 AR definiuje sposób identyfikacji urządzenia w sieci przy postępowaniu zgodnie z protokołem wysyłającym żądania protokołu Extensible Authentication Protocol (AEP) do przełącznika, który korzysta z usługi zdalnego uwierzytelniania użytkowników, którzy wdzwaniają się do systemu telefonii (RADIUS) — żądania udzielenia dostępu.

W produktach Axis te środki bezpieczeństwa są wdrażane za pomocą modułu Axis Edge Vault i ID urządzenia Axis. Axis Edge Vault to bezpieczny moduł, w którym zainstalowano ID urządzenia Axis, zbiór certyfikatów służących do weryfikacji identyfikacji urządzeń. Funkcje te dostarczają sieci możliwy do weryfikacji kryptograficznej dowód tego, że konkretna jednostka została wyprodukowana przez Axis oraz że połączenie sieciowe z tą jednostką jest faktycznie przez nią obsługiwane.

Urządzenie z ID urządzenia Axis zostało wyposażone podczas produkcji (w klucze i certyfikaty). To wyposażenie może później zostać wykorzystane przez klienta do dalszego wyposażenia urządzenia za pomocą innych kluczy i/lub certyfikatów umożliwiających mu dostęp do niektórych zasobów sieciowych klienta.

Dzięki identyfikacji jednostki z ID urządzenia Axis można zmniejszyć czas wprowadzania urządzeń do użytku, ponieważ przed zainstalowaniem i skonfigurowaniem urządzenia w zamierzonej sieci konieczne będzie wykonanie mniejszej ilości pracy. Inną korzyścią jest to, że ID urządzenia Axis, oprócz zapewniania dodatkowego, wbudowanego źródła zaufania, daje możliwość śledzenia urządzeń w dużym systemie.

7.1 Moduł Axis Edge

Axis Edge Vault to bezpieczny kryptograficzny moduł obliczeniowy w postaci układu scalonego umieszczonego na PCB produktu. Edge Vault może bezpiecznie przechowywać certyfikaty i można go używać do operacji kryptograficznych w bezpiecznie przechowywanych certyfikatach.

Certyfikaty przechowywane w Edge Vault nie muszą być w nim pozostawiane, aby urządzenie ich używało. Pozostają bezpieczne w Edge Vault, nawet gdy są używane, ponieważ sprzęt kryptograficzny działający na kluczu jest zainstalowany na tym samym układzie scalonym.

7.2 ID urządzenia Axis

Podczas produkcji każdej jednostki urządzenia sieciowego Axis bezpiecznie instalowany jest „paszport cyfrowy" zwany ID urządzenia Axis w Axis Edge Vault jednostki. Ta identyfikacja jest unikatowa dla każdej jednostki i została zaprojektowana tak, aby można było ustalić źródło pochodzenia urządzenia. ID urządzenia Axis to zbiór certyfikatów używanych w części operacji kryptograficznej modułu do podpisywania wyzwań prezentowanych Edge Vault przez osadzone oprogramowanie sprzętowe produktu. Odpowiedź będąca wynikiem tej operacji jest odsyłana do odbiorcy, który może użyć kluczy publicznych Axis do potwierdzenia uwierzytelnienia odpowiedzi.

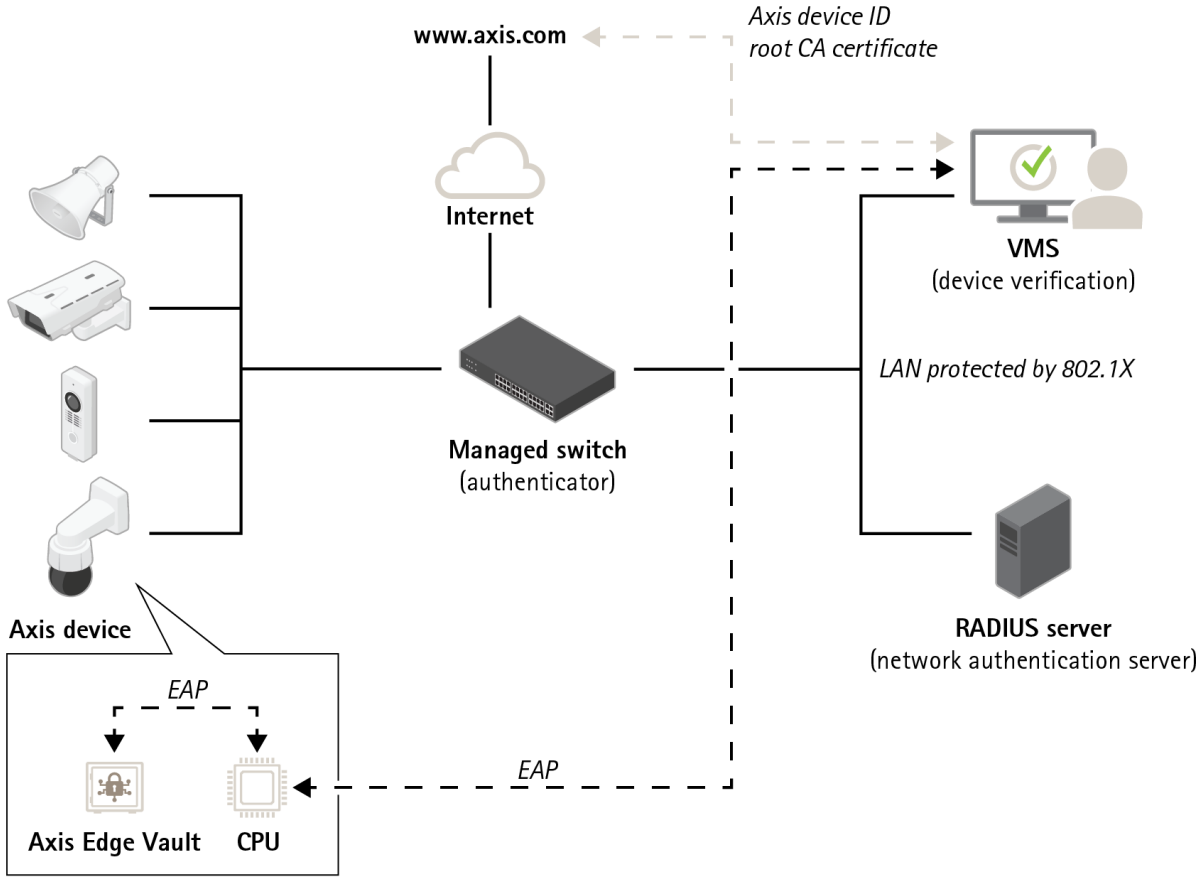

Figure 6. Aplikacje w innych częściach systemu mogą używać ID urządzenia Axis i operacji kryptograficznych, aby sprawdzić, z kim jest nawiązywana komunikacja. ID urządzenia Axis został zweryfikowany za pomocą publicznego certyfikatu głównego CA urządzenia Axis ze strony axis.com.

7.2.1 Hierarchie certyfikatów

Certyfikat to niewielka część danych, która służy do połączenia klucza publicznego z metadanymi opisującymi klucz wraz z podpisem wystawcy potwierdzającym ważność certyfikatu.

Hierarchia certyfikatów to sposób na udowodnienie pochodzenia certyfikatu. Można stworzyć analogię między ID urządzenia Axis a paszportem. Jeśli dana osoba dysponuje paszportem, rząd kraju, z którego ona pochodzi, daje gwarancję, że jest to osoba, której dane znajdują się w paszporcie. W podobny sposób certyfikaty ID urządzenia Axis są zatwierdzane przez główny certyfikat CA ID urządzenia Axis. Podobnie jak w przypadku, gdy urząd celny wierzy, że rząd kraju, poprawnie wystawił paszport, system bezpieczeństwa sieci wierzy, że główny certyfikat CA ID urządzenia, prawidłowo zweryfikował certyfikat jednostki Axis podłączonej do sieci.

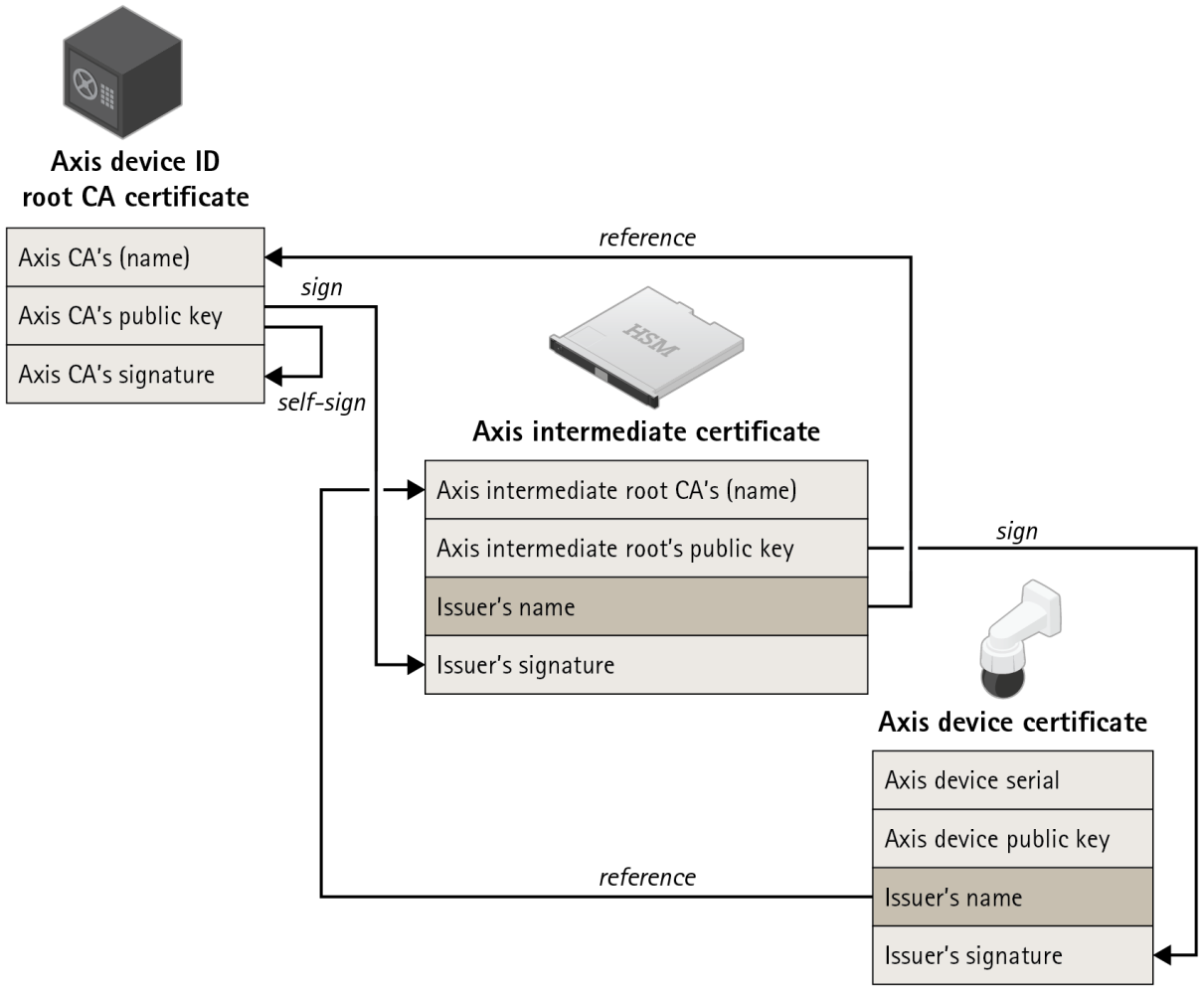

Figure 7. ID urządzenia Axis, który jest certyfikatem zawierającym numer seryjny produktu, podpisywany jest certyfikatem pośredniczącym podpisanym przez główny certyfikat Axis. Ponieważ główny certyfikat Axis jest bardzo cenny i musi być bezpiecznie przechowywany, certyfikat pośredni jest potrzebny podczas obsługi w fabryce.

O firmie Axis Communications

Axis wspiera rozwój inteligentnego oraz bezpiecznego świata poprzez tworzenie rozwiązań sieciowych, które dostarczają wiedzę umożliwiającą poprawę bezpieczeństwa i wdrażanie nowych sposobów prowadzenia działalności. Jako lider rynku sieciowych systemów wizyjnych Axis oferuje produkty i usługi z zakresu dozoru wizyjnego i analiz wideo, kontroli dostępu oraz systemów audio.

Axis to firma mająca ponad 3500 pracowników w ponad 50 krajach, która współpracuje z partnerami na całym świecie w celu dostarczania rozwiązań klientom. Firma została założona w 1984 roku; ma siedzibę w Lund, w Szwecji.

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

AXIS COMMUNICATIONS