Signed Firmware, Secure Boot 및 개인 키의 보안

Axis 제품의 사이버 보안 기능

7월 2020

목차

1 요약

본 문서에서는 사이버 위협을 완화하고 특정 유형의 공격에 대응하도록 Axis 제품에서 사용할 수 있는 몇 가지 기능에 대해 설명합니다. 기능은 다음과 같습니다.

- Signed Firmware
- Secure Boot
- TPM(신뢰할 수 있는 플랫폼 모듈)
- Axis device ID와 Axis Edge Vault

요약된 위협은 다음과 같습니다.

- 펌웨어 탬퍼링
- 공급망 탬퍼링
- 개인 키 추출
- 무단 장치 교체

1.1 Signed Firmware

Signed Firmware는 소프트웨어 공급업체가 개인 키로 펌웨어 이미지에 서명하여 구현됩니다. 펌웨어에 이 서명이 첨부되어 있으면 장치는 펌웨어 설치를 수락하기 전에 펌웨어의 유효성을 검사합니다. 장치에서 펌웨어 무결성이 손상되었음을 감지하면 펌웨어 업그레이드가 거부됩니다.

1.2 Secure Boot

Secure Boot는 변경 불가능 메모리(부팅 ROM)에서 시작하여 암호화로 검증된 소프트웨어의 손상되지 않은 체인으로 구성된 부팅 프로세스입니다. Signed Firmware 사용을 기반으로 하는 Secure Boot는 장치가 승인된 펌웨어로만 부팅할 수 있도록 합니다.

1.3 TPM

TPM은 무단 액세스로부터 정보를 보호하는 데 적합한 암호화 기능 집합을 제공하는 구성 요소입니다. 개인 키는 TPM에 저장되고 개인 키 사용이 필요한 모든 암호화 작업은 처리를 위해 TPM으로 전송됩니다. 이렇게 하면 보안 침입 시에도 인증서의 보안 부분이 안전하게 유지됩니다. 선택한 Axis 제품에 사용되는 TPM은 FIPS 140-2 요구 사항을 충족하는 것으로 인증되었습니다.

1.4 Axis device ID와 Axis Edge Vault

새 국제 표준 IEEE 802.1AR에는 네트워크 상에서 장치 식별을 자동화하고 보호하는 방법에 대한 절차가 설명되어 있습니다. Axis 제품의 이러한 보안 조치는 Axis Edge Vault 및 Axis device ID를 사용하여 구현됩니다. Edge Vault는 안전하게 보관된 인증서에 대해 작동하는 암호화 문제에 사용할 수 있습

니다. 인증서의 개인 부분은 사용되는 중일 때도 Edge Vault에 보관되어 있습니다. Axis device ID는 Axis 루트 인증서를 통해 서명된 인증서로 Edge Vault에 안전하고 영구적으로 보관되며, 이를 통해 제품 수명 주기 동안 새로운 수준의 장치 신뢰가 지원됩니다.

2 용어

인증서(Certificate) - 암호화에서 인증서는 키 쌍의 출처와 속성을 증명하는 서명된 문서입니다. 인증서는 인증 기관(CA)이 서명하고, 시스템에서 CA를 신뢰하는 경우 CA가 발행한 인증서도 신뢰합니다.

인증 기관(Certificate Authority, CA) - 인증서 체인의 신뢰 루트입니다. 기본 인증서의 신뢰성과 진실성을 증명하는 데 사용됩니다.

FIPS - Federal Information Processing Standard(연방 정보 처리 표준), 미국 NIST(National Institute of Standards and Technology, 미국 표준 기술 연구소)에서 발표한 데이터 암호화 및 데이터 보안을 위한 표준입니다.

변경 불가능 ROM(Immutable ROM) - 신뢰할 수 있는 공개 키와 서명을 비교하는 데 사용되는 프로그램을 안전하게 보관하여 덮어쓰지 않도록 합니다.

프로비저닝(Provisioning) - 네트워크용 장치를 준비하고 장착하는 과정입니다. 여기에는 중앙 지점의 구성 데이터 및 정책 설정을 장치에 전달하는 작업이 포함됩니다. 장치에 키 및 인증서가 제공됩니다.

공개 키 암호화(Public key cryptography) - 누구나 수신자의 *공개 키*를 사용하여 메시지를 암호화할 수 있지만, *개인 키*를 사용하는 수신자만 메시지를 해독할 수 있는 비대칭 암호화 시스템입니다. 이는 메시지를 암호화하고 서명하는 데 사용할 수 있습니다.

TLS - Transport Layer Security(전송 계층 보안), 네트워크 트래픽 보호를 위한 인터넷 표준입니다. TLS는 HTTPS에서 S(보안용)를 제공합니다.

3 소개

Axis는 사이버 위험에 대한 고객의 노출을 최소화하기 위해 제품의 보안 취약성을 관리하고 대응하는 업계 모범 사례를 따릅니다. 제품과 서비스가 악의적인 공격에 악용될 수 있는 결함이 없다고 보장할 방법이 없습니다. 이는 Axis에만 국한된 것이 아니라, 모든 네트워크 장치에 대한 일반적인 조건입니다. Axis가 보장할 수 있는 것은 Axis 장치 및 서비스와 관련해서 가능한 위험을 최소화하도록 가능한 모든 단계에서 항상 최선의 노력을 한다는 것입니다.

제품 보안 및 발견된 취약성에 대한 자세한 내용은 *www.axis.com/support/product-security*를 참조하십시오. 일반적인 위협의 위험을 줄이기 위해 취할 수 있는 조치에 대한 자세한 내용을 보려면 *www.axis.com/cybersecurity*에서 Axis 보안 강화 가이드를 다운로드하십시오.

본 백서에서는 몇 가지 발생 가능한 사이버 공격과 Axis 제품에서 이를 예방할 수 있는 방법을 설명합니다. 본 백서에서는 특히 Signed Firmware 및 Secure Boot 기능이 펌웨어 탬퍼링과 공급망 탬퍼링을 방지할 수 있는 방법을 설명합니다. 또한 개인 키를 보호하는 데 사용할 수 있는 TPM(신뢰할 수 있는 플랫폼 모듈) 및 Axis Edge Vault의 사용에 대해 설명합니다. Axis Edge Vault는 새로운 수준의 장치 신뢰를 지원하는 Axis device ID를 안전하게 저장하는 데 사용됩니다.

4 펌웨어 탬퍼링 감지

공격자가 다른 시스템 침해 시도에 실패한 후 악용할 수 있는 한 가지 가능한 공격 벡터는 시스템 소유자가 변경된 애플리케이션, 펌웨어 또는 기타 소프트웨어 모듈을 설치하도록 유도하는 것입니다. 변경된 소프트웨어에는 특정 목적을 가진 악성 코드가 포함될 수 있습니다. 일반적인 권장 사항은 출처를 완전히 신뢰할 수 없는 소프트웨어는 절대 설치하지 않는 것입니다. 비디오 시스템 컨텍스트에는 장치 펌웨어를 변경하고 최종 사용자에게 이를 설치하도록 유도하는 "중간자"가 있을 수 있습니다. 이는 쉬운 작업이 아니며 공격자는 매우 능숙하고 과감해야 할 것입니다. 또한 Axis 펌웨어 설계와 펌웨어가 장치에서 작동하는 방식을 매우 상세히 알아야 할 것입니다. 그럼에도 특정 시스템 공격 시 얻을 가치가 충분히 높다면 이러한 공격자가 존재할 수 있습니다. 일반적인 대응 조치는 소프트웨어 공급업체가 Signed Firmware를 사용하는 것입니다.

4.1 펌웨어 서명

Signed Firmware는 소프트웨어 공급업체가 보안 유지되는 개인 키로 펌웨어 이미지에 서명하여 구현됩니다. 펌웨어에 이 서명이 첨부되어 있으면, 장치는 펌웨어 설치를 수락하기 전에 펌웨어의 유효성을 검사합니다. 장치에서 펌웨어 무결성이 손상되었음을 감지하면, 펌웨어 업그레이드가 거부됩니다.

펌웨어 서명 프로세스는 암호화 해시 값 계산을 통해 시작됩니다. 그런 다음 이 값은 서명이 펌웨어 이미지에 첨부되기 전에 개인/공개 키 쌍의 개인 키로 서명됩니다.

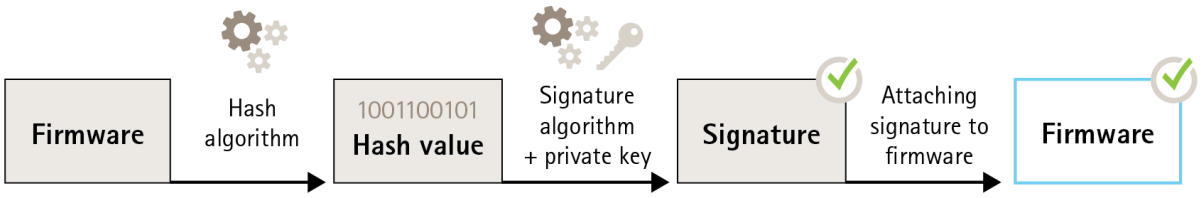

Figure 1. 펌웨어 서명 프로세스입니다.

펌웨어 업그레이드 전에 새 펌웨어를 확인해야 합니다. 새 펌웨어가 수정되지 않았는지 확인하기 위해, 공개 키(Axis 제품에 포함되어 있음)를 사용하여 해시 값이 실제로 일치하는 개인 키로 서명되었는지 확인합니다. 또한 펌웨어의 해시 값을 계산하고 이를 서명의 이 검증된 해시 값과 비교함으로써 펌웨어의 무결성을 확인할 수 있습니다.

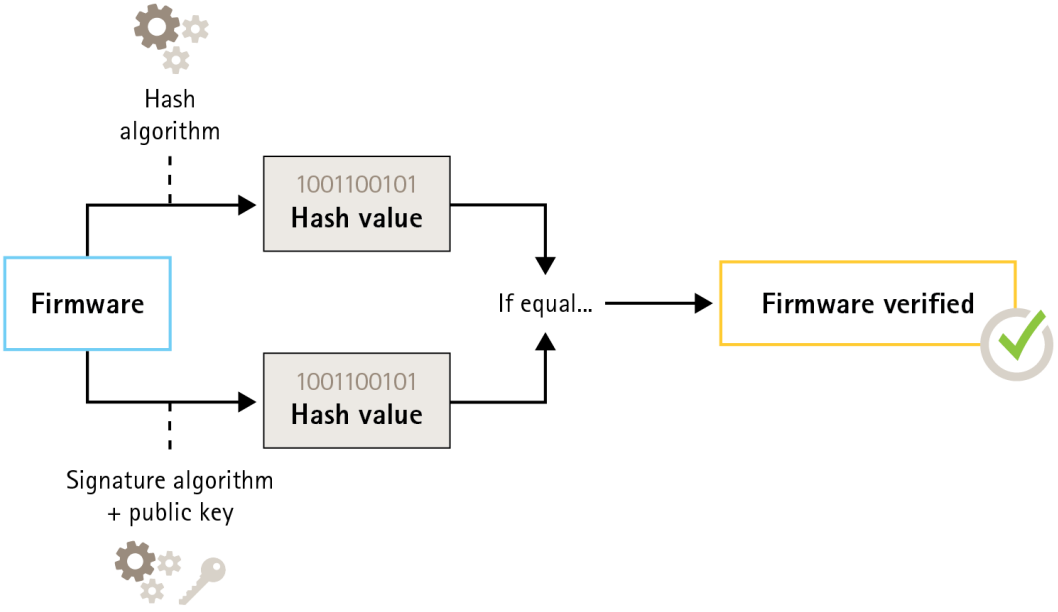

Figure 2. Signed Firmware를 확인하는 프로세스입니다.

4.2 Axis의 Signed Firmware

Axis의 Signed Firmware는 업계에서 승인된 RSA 공개 키 암호화 방법을 기반으로 합니다. 개인 키는 Axis에서 극비의 위치에 저장되며, 공개 키는 Axis 장치에 포함됩니다. 전체 펌웨어 이미지의 무결

성은 이미지 내용의 서명으로 보장됩니다. 기본 서명은 이미지의 압축을 풀 때 확인되는 여러 가지 보조 서명을 확인합니다.

5 공급망 탬퍼링 방지

펌웨어 서명은 향후 모든 펌웨어 업데이트에서 손상된 펌웨어를 설치하지 못하도록 장치를 보호합니다. 그러나 중간자가 공급업체와 최종 사용자 사이의 장치를 변경하면 어떻게 될까요? 전송 중 장치에 실제로 접근하는 공격자는 장치가 배포되기 전에 변경된 악성 펌웨어를 설치하기 위해 장치의 부팅 파티션을 손상시키고 펌웨어 무결성 검사를 우회하는 등의 공격을 수행할 수 있습니다.

5.1 Secure Boot

Secure Boot는 변경 불가능 메모리(부팅 ROM)에서 시작하여 암호화로 검증된 소프트웨어의 손상되지 않은 체인으로 구성된 부팅 프로세스입니다. Signed Firmware 사용을 기반으로 하는 Secure Boot는 장치가 승인된 펌웨어로만 부팅할 수 있도록 합니다.

부팅 프로세스는 부트 로더의 유효성을 검사하는 부팅 ROM에서 시작됩니다. 그런 다음 Secure Boot는 플래시 메모리에서 로드된 각 펌웨어 블록에 대해 내장 서명을 실시간으로 확인합니다. 부팅 ROM은 신뢰의 루트 역할을 수행하며 각 서명이 확인되는 동안에만 부팅 프로세스가 계속됩니다. 체인의 모든 부분은 다음 부분을 인증하여 궁극적으로 검증된 Linux 커널 및 검증된 루트 파일 시스템이 됩니다.

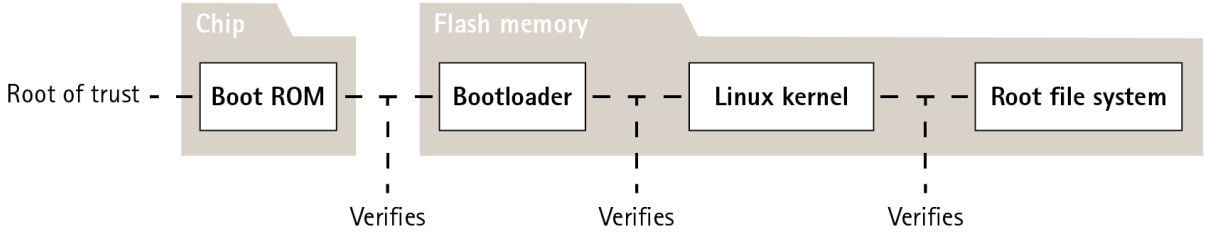

Figure 3. Secure Boot 프로세스입니다.

5.2 Axis Secure Boot

대부분의 장치에서는 낮은 수준의 기능은 변경할 수 없다는 것이 중요합니다. 하위 수준 소프트웨어 위에 다른 보안 메커니즘이 구축된 경우, Secure Boot는 이러한 메커니즘이 우회되지 않도록 보호하는 안전한 기본 계층 역할을 수행합니다.

Secure Boot가 있는 장치의 경우, 플래시 메모리에 설치된 펌웨어가 수정되지 않도록 보호됩니다. 공장 출하 시 기본 설정 이미지는 보호되지만, 구성은 보호되지 않습니다. Secure Boot는 Axis 장치가 공장 출하 시 기본 설정 후 발생 가능한 맬웨어로부터 완벽하게 보호되도록 보장합니다.

5.3 Secure Boot 및 사용자 정의 펌웨어 인증서

Secure Boot를 사용하면 제품이 더 안전하지만, 다른 펌웨어와의 유연성도 감소되어 Axis에서 제품으로 임시 펌웨어(예: 테스트 펌웨어 또는 다른 사용자 정의 펌웨어)를 로드하는 것이 더 복잡해집니다. 그러나 Axis는 개별 유닛에서 이러한 비 프로덕션 펌웨어를 수락하도록 승인하는 메커니즘을 구현했습니다. 이 펌웨어는 소유자와 Axis가 모두 승인하는 다른 방식으로 서명되며, 사용자 정의 펌웨어 인증서가 생성됩니다. 승인된 유닛에 설치된 경우, 인증서는 고유한 일련 번호 및 칩 ID에 따라 승인된 유닛에서만 실행할 수 있는 사용자 지정 펌웨어를 사용할 수 있습니다. Axis가 사용자 정의 펌웨어 인증서에 서명할 수 있는 키를 보유하므로, Axis만 해당 인증서를 생성할 수 있습니다.

6 개인 키의 보안

Axis 장치는 TLS(전송 계층 보안)를 사용하는 HTTPS(네트워크 암호화) 및 802.1X(네트워크 액세스 제어)를 지원합니다. TLS의 디지털 인증서는 공개/개인 키 쌍을 사용합니다. 개인 키는 장치에 저장되고 공개 키는 인증서에 포함됩니다. HTTPS와 802.1X가 모두 사용되지 않는 경우에는 보호할 키가 없습니다.

공격자가 장치에서 개인 키와 인증서를 추출하고 공격하는 컴퓨터에 설치하는 작업을 시도할 수 있습니다. HTTPS의 경우, 해당 개인 키를 사용하여 장치와 VMS 간의 암호화된 네트워크 트래픽을 도청할 수 있습니다. 또는 네트워크를 스푸핑하는 경우, 공격하는 컴퓨터는 합법적인 장치인 것처럼 가장하여 VMS에 액세스할 수 있습니다. 802.1X의 경우, 공격자는 개인 키를 사용하여 신뢰할 수 있는 장치로 위장하여 802.1X로 보호된 네트워크에 액세스할 수 있습니다.

인증서와 개인 키는 일반적으로 장치의 파일 시스템에 저장되고, 계정 액세스 정책으로 보호되며 일반 컴퓨팅 환경에서 사용됩니다. 대부분의 경우 계정이 쉽게 손상되지 않으므로 이것으로 충분합니다. 손상이 의심되는 경우 인증서를 철회하여 개인 키를 사용할 수 없도록 만들 수 있습니다.

중요 시스템의 일부 최종 사용자는 개인 키를 추출하기 위해 장치를 침해하려는 과감하고 능숙한 공격자의 위협이 늘어가는 것을 경험할 수도 있습니다. TPM(신뢰할 수 있는 플랫폼 모듈)은 장치가 손상된 경우에도 추출이 거의 불가능한 방식으로 키를 저장합니다.

6.1 TPM(신뢰할 수 있는 플랫폼 모듈)을 사용한 안전한 키 저장

TPM은 무단 액세스로부터 정보를 보호하는 데 적합한 특정 암호화 기능 집합을 제공하는 구성 요소입니다. 개인 키는 TPM에 저장되며 TPM에 항상 남아 있습니다. 개인 키를 사용해야 하는 모든 암호화 작업은 처리를 위해 TPM으로 전송됩니다. 이렇게 하면 인증서의 보안 부분이 TPM 내의 보안 환경에 항상 남아 있으며 보안 침입 시에도 안전하게 유지됩니다.

6.2 FIPS 140-2 인증

일부 제품 및 사용 사례의 경우 정보 보호를 위해 TPM을 사용하는 것이 규정 요구 사항일 수 있으며, FIPS 140-2 규정 준수 요구 사항을 함께 충족해야 하는 경우도 있습니다. FIPS(Federal Information Processing Standard, 연방 정보 처리 표준) 140-2는 미국 NIST(National Institute of Standards and Technology, 미국 표준 기술 연구소)에서 발표한 암호화 모듈에 대한 정보 보안 표준입니다.

NIST 인증 테스트 연구소에서 수행하는 검증은 모듈 시스템 및 모듈의 암호화가 올바르게 구현되었는지 확인하는 것입니다. 간단히 말해 인증에는 암호화 모듈, 승인된 알고리즘, 승인된 작업 모드 및 전원 공급 테스트에 대한 설명, 사양 및 확인이 필요합니다.

FIPS 140-2의 인증 요구 사항에 대한 자세한 내용은 NIST 웹 사이트 (*https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards*)에서 찾을 수 있습니다.

6.2.1 Axis 제품의 인증 TPM

선택한 Axis 제품에 사용되는 TPM은 FIPS 140-2 요구 사항을 충족하는 것으로 인증되었습니다. 보다 구체적으로, TPM은 이 표준의 보안 수준 2로 인증되었습니다. 이는 TPM이 다른 요구 사항 중에서도 역할 기반 승인 및 탬퍼 증거에 대한 요구 사항도 충족함을 의미합니다.

7 IEEE 802.1AR - Axis device ID를 사용하는 장치 확인

Axis 네트워크 장치를 구입한 사람은 사용하기 전에 수동 검사를 수행할 수 있습니다. 고객은 제품을 육안으로 검사하고 Axis 제품의 모양과 느낌에 대한 사전 지식을 활용하여 제품이 실제 Axis 제품인지 확신할 수 있습니다. 그러나 이러한 유형의 검사는 제품에 실제로 접근할 수 있는 사람만 수행할 수 있습니다. 그러면 프로비저닝되지 않은 제품을 네트워크상에서 통신할 때, 올바른 유닛과 통신하고 있는지 어떻게 확신할 수 있을까요? 장치가 무단으로 교체되지 않았을까요? 네트워크로 연결된 장비나 서

버에 있는 소프트웨어는 물리적 검사를 수행할 수 없습니다. 일반적인 보안 조치는 유닛을 안전하게 프로비저닝할 수 있는 폐쇄 네트워크를 통해 새 제품과 먼저 상호 작용해 보는 것이었습니다.

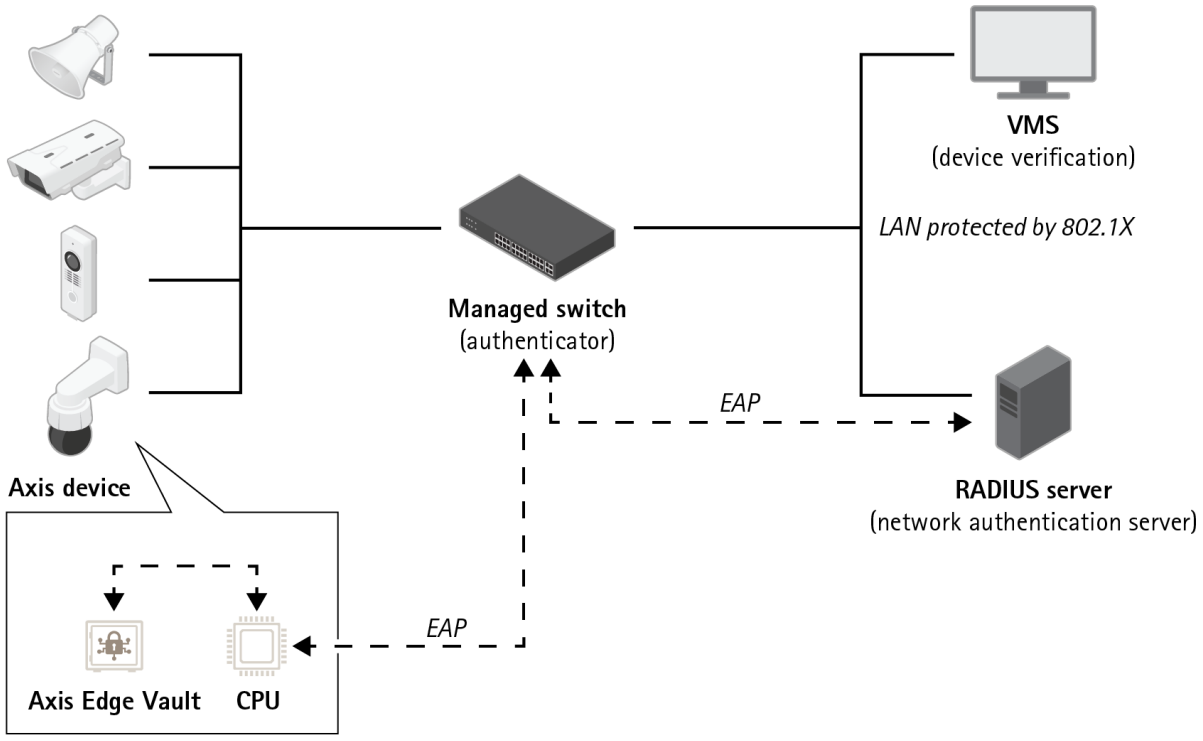

Figure 4. 고객은 자신의 인증 서버가 장치 일련 번호 및 Axis device ID를 사용하여 구입한 Axis 제품을 네트워크상에서 자동으로 수락하도록 지시할 수 있습니다.

새 국제 표준 IEEE 802.1AR(*https://1.ieee802.org/security/802-1ar/*)은 네트워크상에서 장치의 식별을 자동화하고 보호하는 방법을 정의합니다. 통신이 내장 보안 모듈로 전달되면 유닛은 이 표준에 따라 신뢰할 수 있는 식별 응답을 반환할 수 있습니다.

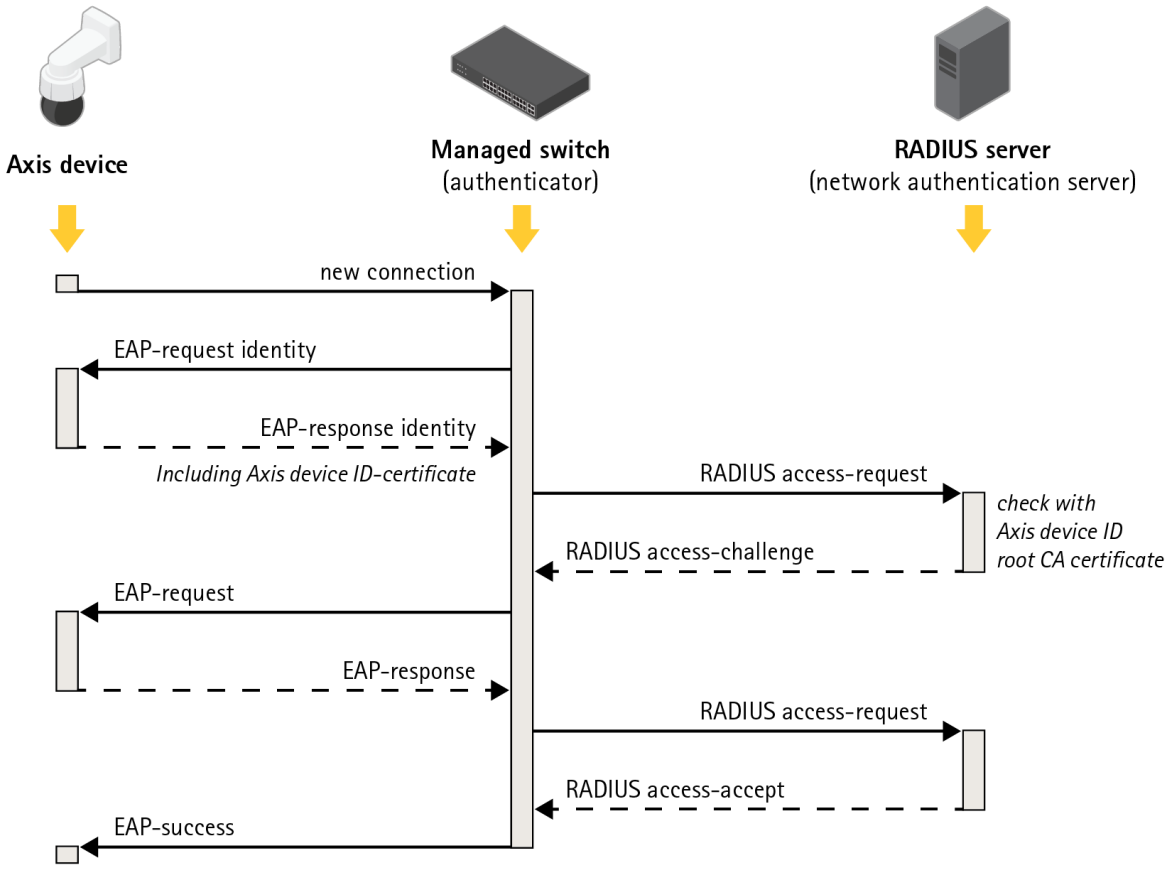

Figure 5. IEEE 802.1AR은 RADIUS(Remote Authentication Dial-In User Service)(액세스 허용 요청)를 사용하는 스위치에 AEP(Extensible Authentication Protocol) 요청을 전송하는 프로토콜을 따라 네트워크상에서 장치를 식별하는 방법을 정의합니다.

Axis 제품의 이러한 보안 조치는 Axis Edge Vault 및 Axis device ID를 사용하여 구현됩니다. Axis Edge Vault는 장치 식별을 확인하는 인증서 모음인 Axis device ID가 설치되는 보안 모듈입니다. 이러한 기능은 특정 유닛이 Axis에서 생산되었고 해당 유닛에 대한 네트워크 연결이 실제로 해당 유닛에서 제공된다는 암호화 확인 가능한 증거를 네트워크에 제공합니다.

Axis device ID가 있는 장치가 키 및 인증서와 함께 공장에서 프로비저닝되었습니다. 이 프로비저닝은 나중에 고객이 일부 고객의 네트워크 리소스에 액세스할 수 있도록 허용하는 다른 키 및/또는 인증서로 현장에서 장치를 추가로 프로비저닝하는 데 사용할 수 있습니다.

Axis device ID로 유닛을 식별함으로써, 원하는 네트워크에 장치를 설치하고 구성하기 전에 장치에 대해 수행해야 하는 작업이 줄어들기 때문에 장치 배포 시간을 줄일 수 있습니다. 또 다른 이점은 Axis device ID가 추가 내장 신뢰 소스를 제공하는 것 외에도 대규모 시스템에서 장치를 추적할 수 있는 수단도 제공한다는 것입니다.

7.1 Axis Edge Vault

Axis Edge Vault는 제품 내부의 PCB에 장착된 칩 형태의 안전한 암호화 컴퓨팅 모듈입니다. Edge Vault는 인증서를 안전하게 보관할 수 있으며 안전하게 보관된 인증서에 대한 암호화 작업에 사용할 수 있습니다.

Edge Vault에 보관된 인증서를 장치에서 사용해도 Edge Vault에 항상 남아 있습니다. 키에서 작동하는 암호화 하드웨어가 동일한 물리적 칩에 설치되기 때문에, 인증서가 사용되는 중일 때도 Edge Vault에 안전하게 보관되어 있습니다.

7.2 Axis device ID

각 Axis 네트워크 장치 유닛을 생산하는 동안 Axis device ID라는 "디지털 패스포트"가 유닛의 Axis Edge Vault에 안전하게 설치됩니다. 이 ID는 각 유닛마다 고유하며 장치의 출처를 증명하도록 설계되었습니다. Axis device ID는 내장 제품 펌웨어에서 발생하는 문제를 Edge Vault에 서명하도록 모듈의 암호화 작업 부분에 사용되는 인증서 모음입니다. 이 작업의 응답은 Axis 공개 키를 사용하여 해당 응답의 인증을 검증할 수 있는 수신자에게 다시 전송됩니다.

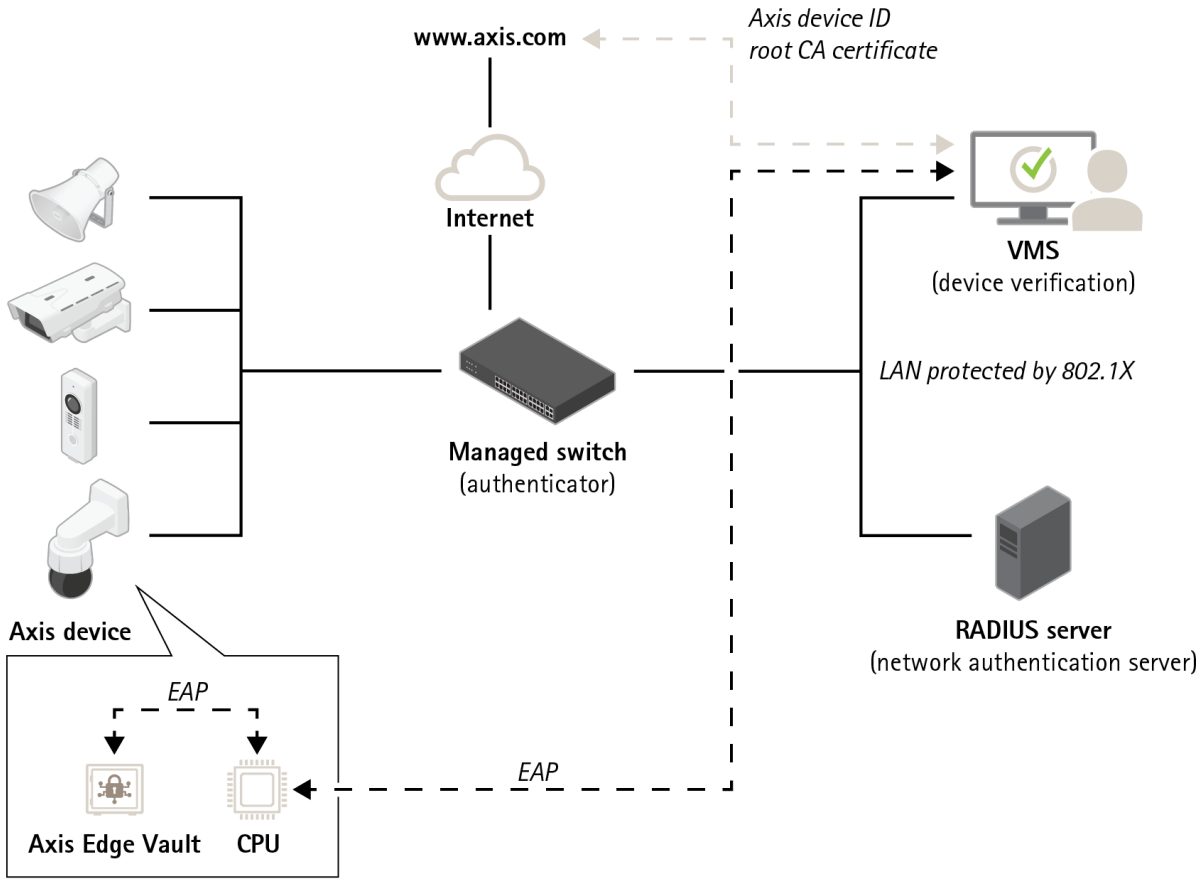

Figure 6. 시스템의 다른 부분에 있는 소프트웨어 애플리케이션은 Axis device ID 및 암호화 작업을 사용하여 통신 중인 사람을 확인할 수 있습니다. Axis device ID는 axis.com의 공개 Axis device ID 루트 CA 인증서로 확인되었습니다.

7.2.1 인증서 계층 구조

인증서는 인증서의 유효성을 증명하는 발급자의 서명과 함께 키를 설명하는 메타데이터 및 공개 키를 결합한 작은 데이터 조각입니다.

인증서 계층 구조는 인증서의 출처를 증명하는 방법입니다. Axis device ID와 여권 간의 유사점을 살펴볼까요. 여권을 갖고 있다면, 이는 한 국가의 정부가 여권에 명시된 사람의 신원을 보증해 주는 것입니다. 마찬가지로 모든 Axis device ID 인증서는 Axis device ID 루트 CA 인증서로 보증됩니다. 이는 세관 직원이 한 국가의 정부가 해당 여권을 올바르게 발급했다고 신뢰하는 것처럼, 네트워크 보안 시스템에서 Axis device ID 루트 CA 인증서가 네트워크로 연결된 유닛의 Axis 인증서를 올바르게 확인했다고 신뢰하는 것입니다.

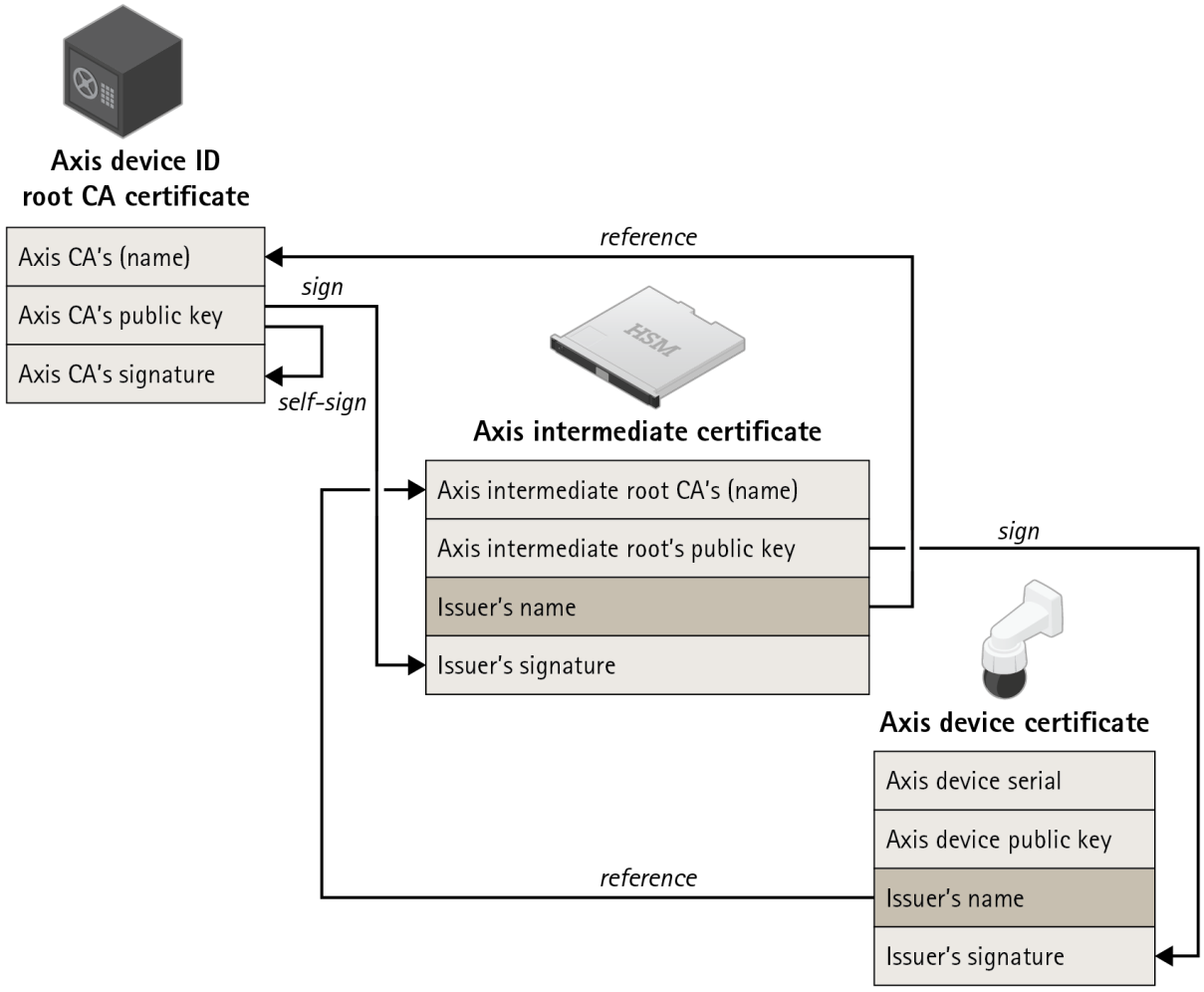

Figure 7. 제품의 일련 번호를 통합하는 인증서인 Axis device ID는 Axis 루트 인증서로 서명된 중간 인증서로 서명됩니다. Axis 루트 인증서는 매우 중요하며 안전한 곳에 보관해야 하므로, 공장에서 프로비저닝하는 동안 중간 인증서가 필요합니다.

T10156858/KO/M1.2/2007

Axis Communications에 대하여

Axis는 보안 개선과 새로운 비즈니스 수행 방식에 대한 통찰력을 제공하는 네트워크 솔루션을 개발하여 보다 스마트하고 안전한 세상을 만들 수 있도록 지원합니다. 네트워크 비디오 업계의 선도 기업인 Axis는 비디오 감시 및 분석, 접근 제어, 오디오 시스템 분야의 제품과 서비스를 제공합니다

50개 이상의 국가에서 3,500명이 넘는 Axis 임직원이 파트너와 협력하여 전세계 고객에게 최적의 솔루션을 제공하고 있습니다. 1984년에 설립된 Axis는 스웨덴에 본사를 두고 있습니다.

Axis에 대한 자세한 정보는 *axis.com*에서 확인하실 수 있습니다.