백서

# Axis Edge Vault

다음을 제공하여 Axis 장치를 보호하는 하드웨어 기반 사이버 보안 플랫폼:

— 공급망 보호

— 신뢰할 수 있는 장치 ID

— 안전한 키 보관

— 비디오 변조 감지

4월 2024

# 요약

Axis Edge Vault는 Axis 장치를 보호하는 하드웨어 기반 사이버 보안 플랫폼을 제공합니다. 이 플랫폼은 암호화 컴퓨팅 모듈(보안 요소 및 TPM) 및 SoC 보안(TEE 및 Secure Boot)의 강력한 기반에 의존하며, 에지 장치 보안에 대한 전문 지식이 결합되어 있습니다. Axis Edge Vault는 *Signed OS*("OS"는 운영 체제를 가리키는 것임)와 함께 *Secure Boot*를 통해 구축되는 강력한 신뢰 루트에 앵커 포인트를 두고 있습니다. 이러한 기능은 모든 보안 운영이 의존하는 신뢰 체인을 위해 암호학적으로 검증된 소프트웨어의 끊어지지 않는 체인을 가능하게 합니다.

Edge Vault가 포함된 Axis 장치는 중요한 정보의 도청 및 악의적인 유출을 방지하여 고객이 사이버 보안 위험에 노출되는 것을 최소화합니다. 또한 Axis Edge Vault를 사용하면 Axis 장치가 고객의 네트워크에서 신뢰할 수 있는 장치가 될 수 있습니다.

**Axis Edge Vault 사이버 보안 플랫폼**

| 암호화 컴퓨팅 모듈 | 특징 | 사용 사례 |
|---|---|---|
| • 보안 요소<br>• TPM 2.0<br>• SoC 보안(TEE) | • Secure Boot<br>• Signed OS<br>• Axis device ID<br>• 보안 키 저장소<br>• Signed Video<br>• 암호화된 파일 시스템 | • 공급망 보호<br>• 신뢰할 수 있는 장치 ID<br>• 안전한 키 보관<br>• 비디오 변조 감지 |

- **공급망 보호**: Axis Edge Vault는 신뢰의 루트 역할을 하는 안전한 기반이 필요합니다. Secure Boot 및 Signed OS의 도움 없이는 신뢰 체인의 루트를 확립할 수 없습니다. Secure Boot는 Signed OS와 함께 변경 불가능 메모리(부트 ROM)에서 시작하여 암호학적으로 검증된 소프트웨어의 끊어지지 않는 체인을 제공합니다. Secure Boot는 Signed OS로만 장치를 부팅할 수 있도록 하여 물리적 공급망 변조를 방지할 수 있습니다. Signed OS를 사용하면, 장치는 설치를 수락하기 전에 새 장치 소프트웨어를 검증할 수도 있습니다. 장치에서 무결성이 손상되었거나 Axis가 서명하지 않은 장치 소프트웨어가 감지되면 업그레이드가 거부됩니다. 이를 통해 장치를 소프트웨어 변조로부터 보호할 수 있습니다.
- **신뢰할 수 있는 장치 ID**: 장치의 출처를 확인할 수 있는 것은 장치 ID에 대한 신뢰를 구축하는 데 핵심적인 것입니다. 생산 과정에서 Axis Edge Vault가 설치된 장치에는 공장에서 프로비저닝된 고유하고 IEEE 802.1AR을 준수하는 Axis 장치 ID 인증서가 할당됩니다. 이는 장치의 출처를 증명하는 여권과 같은 역할을 합니다. 장치 ID는 Axis 루트 인증서로 서명된 인증서로 보안 키 저장소에 안전하고 영구적으로 저장됩니다. 장치 ID는 고객의 IT 인프라에서 자동화된 보안 장치 온보딩 및 보안 장치 식별을 위해 활용할 수 있습니다.

- **안전한 키 보관**: 보안 키 저장소는 하드웨어 기반의 변조 방지 암호화 정보 저장을 제공합니다. 보안 키 저장소는 Axis 장치 ID와 고객이 로드한 암호화 정보를 보호하고, 보안 침해 발생 시 무단 액세스 및 악의적인 추출을 방지합니다.
- **비디오 변조 감지**: Signed Video는 비디오 파일의 보관 연속성을 증명하지 않고도 비디오 증거가 변조되지 않은 것으로 검증될 수 있도록 합니다. 각 카메라는 보안 키 저장소에 안전하게 저장된 고유한 비디오 서명 키를 사용하여 비디오 스트림에 서명을 추가합니다. 비디오가 재생되면 Axis의 *파일 플레이어*는 비디오가 손상되지 않았는지 여부를 보여줍니다. Signed Video를 통해 비디오의 원본 촬영 카메라를 추적하고 비디오가 카메라를 떠난 후 변조되지 않았는지 확인할 수 있습니다.

# 목차

# 1 서론

Axis는 제품에 보안을 구현할 때 업계 모범 사례를 따릅니다. 이는 사이버 보안 위험에 대한 고객의 노출을 최소화하고 Axis 장치를 고객 네트워크에서 신뢰할 수 있는 장치로 만들기 위해 수행됩니다.

Axis Edge Vault는 Axis 장치를 보호하는 하드웨어 기반 사이버 보안 플랫폼을 제공합니다. 이 플랫폼은 암호화 컴퓨팅 모듈(보안 요소 및 TPM) 및 SoC 보안(TEE 및 Secure Boot)의 강력한 기반 위에 구축되며, 에지 장치 보안에 대한 전문 지식이 결합되어 있습니다.

이 백서에서는 Axis 에지 장치 보안의 다중 계층 접근 방식을 간략하게 설명하고 일반적인 위험과 이를 방지할 수 있는 방법을 제시합니다. Axis Edge Vault는 신뢰의 루트 역할을 하는 안전한 기반이 필요합니다. 따라서 Axis 장치의 공급망 보안 측면을 살펴보고 Signed OS(서명된 운영 체제)와 Secure Boot가 어떻게 소프트웨어 변조 및 물리적 공급망 변조에 대응하는 근본적인 조치인지 알아봅니다.

*https://www.axis.com/support/cybersecurity/resources*에서 제품 보안, 발견된 취약점 및 일반적인 위협의 위험을 줄이기 위해 취할 수 있는 조치에 대한 자세한 정보를 찾을 수 있습니다.

이 백서의 마지막 장에는 용어집이 포함되어 있습니다.

# 2 공급망 보호

Axis Edge Vault는 신뢰의 루트 역할을 하는 안전한 기반이 필요합니다. 신뢰 루트 확립은 장치의 부팅 프로세스에서 시작됩니다. Axis 장치에서 하드웨어 기반 메커니즘 *Secure Boot*는 장치가 부팅되는 운영 체제(AXIS OS)를 확인합니다. 그러면 빌드 프로세스 중에 AXIS OS가 *Signed OS*를 사용하여 암호화 서명됩니다.

Secure Boot와 Signed OS는 서로 연결되어 있습니다. 이 둘은 장치를 배포하기 전에 운영 체제 또는 장치 소프트웨어가 (장치에 물리적으로 액세스할 수 있는 사람에 의해) 변조되지 않았는지 확인하고, 배포 후에는 장치가 손상되거나 코드 서명되지 않은 소프트웨어 업데이트를 설치할 수 없는지 확인합니다. Secure Boot와 Signed OS를 함께 사용하면 모든 보안 작업이 의존하는 신뢰 체인을 위해 암호학적으로 검증된 소프트웨어의 끊어지지 않는 체인이 생성됩니다.

## 2.1 Secure Boot

Secure Boot 메커니즘은 변경 불가능 메모리(부팅 ROM)에서 시작하여 암호화로 검증된 소프트웨어의 손상되지 않은 체인으로 구성된 부팅 프로세스입니다. Secure Boot는 장치가 인증된 운영 체제에서만 부팅할 수 있도록 합니다.

부트 프로세스는 부트 로더의 유효성을 검사하는 부트 ROM에서 시작됩니다. 그런 다음 Secure Boot는 플래시 메모리에서 로드된 각 소프트웨어 구성 요소에 대해 내장된 서명을 실시간으로 확인합니다. 부팅 ROM은 신뢰 루트 역할을 수행하며 각 서명이 확인되는 경우 부팅 프로세스가

계속됩니다. 체인의 모든 부분은 다음 부분을 인증하여 궁극적으로 검증된 Linux 커널 및 검증된 루트 파일 시스템이 됩니다.

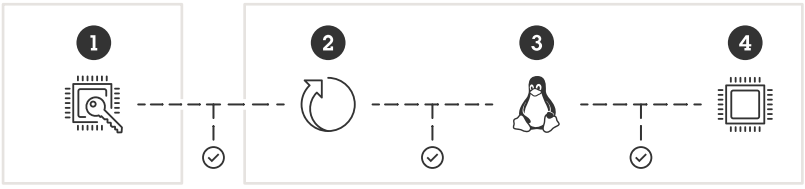


*Figure 1. Secure Boot 프로세스에서는 체인의 각 부분이 다음 부분을 인증합니다. 이를 통해 궁극적으로 루트 파일 시스템이 확인됩니다.*

1 *SoC의 부트 ROM(신뢰 루트)*
2 *부트로더*
3 *Linux 커널*
4 *루트 파일 시스템*

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 Boot 기능이 있는 장치의 경우, 플래시 메모리에 설치된 운영 체제는 수정되지 않도록 보호되지만 구성은 보호되지 않은 상태로 유지됩니다. Secure Boot는 공장 초기화 후에도 장치의 올바른 상태를 보장합니다. 그러나 Secure Boot가 작동하려면 부팅 시 운영 체제가 Axis에 의해 서명되었는지 확인해야 합니다.

## 2.2 Signed OS

Axis Signed OS에는 비밀로 유지되는 개인 키로 장치 소프트웨어 이미지에 Axis가 코드를 서명하는 것이 포함됩니다. 장치를 시작할 때 Axis 장치의 Secure Boot는 장치 소프트웨어가 서명되었는지 확인합니다. 장치 소프트웨어의 무결성이 손상된 것을 장치가 감지하면, 장치가 실행되지 않습니다. 장치 소프트웨어를 업그레이드할 때, 장치의 기존 Signed AXIS OS가 새 AXIS OS도 서명되었는지 자동으로 확인합니다. 그렇지 않은 경우 업그레이드가 거부됩니다.

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

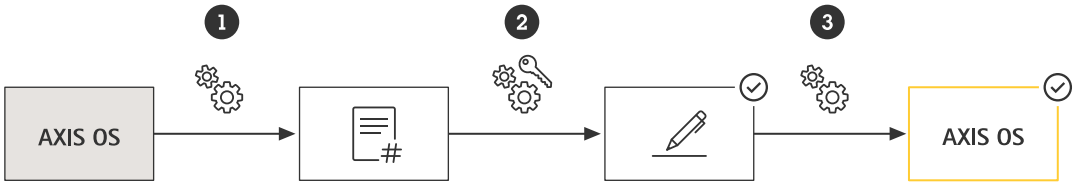


*Figure 2. OS 코드 서명 프로세스.*

1 *AXIS OS에 대한 암호화 해시 값이 생성됩니다.*
2 *서명은 해시와 개인 키를 결합하여 만들어집니다.*
3 *서명이 AXIS OS 버전 및 바이너리에 추가됩니다.*

업그레이드하기 전에 새 소프트웨어 업데이트의 진위 여부를 확인해야 합니다. 이를 위해 공개 키(Axis 제품에 포함되어 있음)를 사용하여 해시 값이 실제로 일치하는 개인 키로 서명되었는지 확인합니다. 또한 해시 값을 계산하고 서명에서 검증된 이 해시 값과 비교함으로써 무결성을 확인할 수 있습니다. 서명이 유효하지 않거나 AXIS OS 이미지가 변조된 경우, Axis 장치의 부팅 프로세스가 중단됩니다.

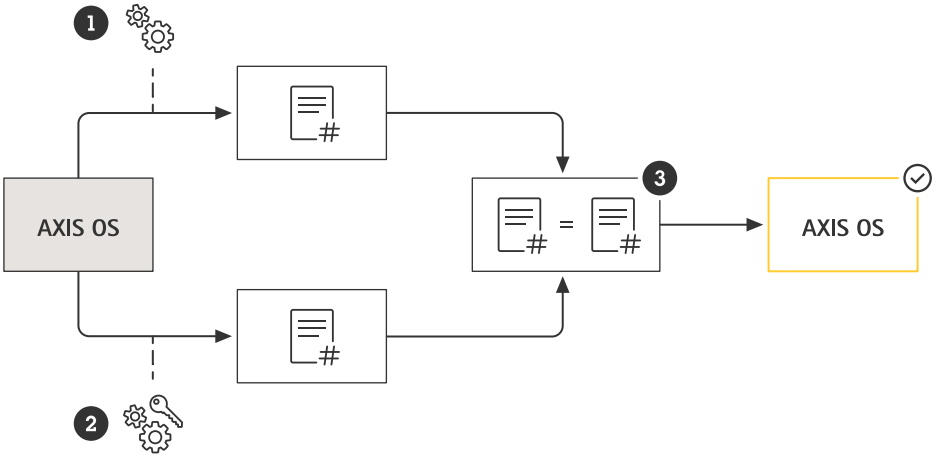


*Figure 3. Signed OS를 확인하는 프로세스입니다.*

1 *AXIS OS의 해시 값 계산*
2 *공개 키를 사용하여 서명에서 해시 값 확인*
3 *결과가 일치하는 경우에만 서명이 성공적으로 확인됩니다.*

Axis Signed OS는 업계에서 인정하는 RSA 공개 키 암호화 방법을 기반으로 합니다. 개인 키는 Axis에서 엄격한 보안 위치에 저장되며, 공개 키는 Axis 장치에 포함됩니다. 전체 소프트웨어 이미지의 무결성은 서명을 통해 보장됩니다. 기본 서명은 이미지의 압축을 풀 때 확인되는 여러 보조 서명을 확인합니다.

테스트 및 사용자 지정 빌드를 위해, Axis는 개별 장치가 비생산 이미지를 수락하도록 승인하는 메커니즘을 구현했습니다. 이 이미지는 소유자와 Axis의 승인을 받아 해당 용도의 전용 키를 사용하여 코드 서명되며, 이를 통해 사용자 지정 서명이 생성됩니다. 인증서는 승인된 장치에 설치되면 고유한 일련 번호와 칩 ID를 기반으로 승인된 장치에서만 실행할 수 있는 사용자 지정 이미지를 사용할 수 있습니다. 사용자 지정 인증서는 Axis가 서명할 키를 가지고 있기 때문에 Axis만 만들 수 있습니다.

# 3 신뢰할 수 있는 장치 ID

최신 제로 트러스트 보안 네트워크("절대 신뢰하지 않고 항상 확인")에서는 장치의 출처, 진위 여부, 연결 상태를 확인할 수 있는 기능이 기본적으로 필요합니다. 네트워크 장치는 공항에서 신원 확인을 위해 당국에 여권을 제시하는 것과 유사한 방식으로 무결성과 진위 여부를 확인할 수 있습니다.

## 3.1 Axis 장치 ID로 안전한 장치 식별

국제 표준 *IEEE 802.1AR*은 네트워크상에서 장치 식별을 자동화하고 보호하는 방법을 정의합니다. 통신이 내장 암호화 컴퓨팅 모듈로 전달되면 장치는 이 표준에 따라 신뢰할 수 있는 식별 응답을 반환할 수 있습니다. 이 신뢰할 수 있는 응답은 네트워크 인프라에서 초기 장치 구성 및 소프트웨어 업데이트를 위해 장치를 프로비저닝 네트워크에 자동으로 안전하게 온보딩하는 데 사용할 수 있습니다.

IEEE 802.1AR을 준수하기 위해 Axis는 대부분의 장치를 장치 고유의 공장 프로비저닝된 Axis 장치 ID 인증서(IEEE 802.1AR 초기 장치 식별자, IDevID)를 사용하여 제조합니다. Axis 장치 ID는 장치 자체의 암호화 컴퓨팅 모듈을 통해 제공되는 변조 방지 보안 키 저장소에 안전하게 저장됩니다. 이 ID는 각 Axis 장치마다 고유하며 장치의 출처를 증명하도록 설계되었습니다.

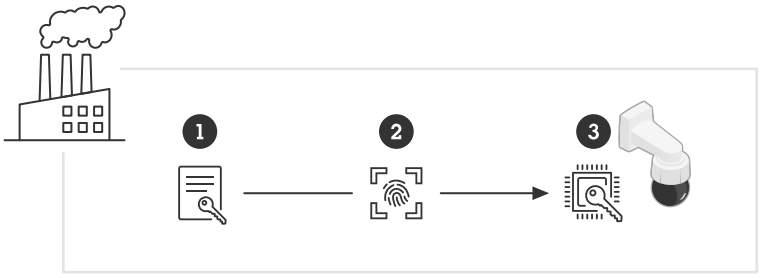


*Figure 4. 장치의 제조 프로세스 중에 고유한 Axis 장치 ID(2)가 장치의 보안 키 저장소(3)에 저장됩니다.*

1 *Axis 장치 ID key infrastructure(PKI)*
2 *Axis device ID*
3 *Axis 장치 ID는 Axis 장치의 암호화 컴퓨팅 모듈을 통해 제공되는 변조 방지 보안 키 저장소에 안전하게 저장됩니다.*

IEEE 802.1AR은 네트워크 접근 제어를 위한 IEEE 802.1X 표준을 기반으로 하며, 이 표준은 Axis 장치 ID가 사전 선택된 Axis 장치에서 기본적으로 활성화됩니다. 따라서 공장 출하 시 기본 설정 상태에서도 802.1X 지원 IT 인프라를 통해 Axis 장치를 안전하게 식별하고 인증할 수 있습니다.

Axis 장치 ID 인증서는 다양한 암호화 구성(2048 비트 RSA, 4096 비트 RSA, ECC-P256)으로 제공됩니다. 이러한 암호화 구성은 기본적으로 활성화되어 있으며, IEEE 802.1X 네트워크 접근 제어와 HTTPS를 통해 장치를 안전하게 연결하고 식별할 수 있도록 합니다.

Axis는 제조 프로세스 중에 Axis 장치 ID를 공장 프로비저닝하기 위해 자체 전용 IEEE 802.1AR 공개 키 인프라(PKI)를 관리합니다. Axis 장치 ID는 중간 인증서에 의해 서명되며, 중간 인증서는 다시 Axis 루트 인증서에 의해 서명됩니다. 루트 CA와 중간 CA는 모두 지리적으로 분리된 암호화 컴퓨팅 모듈에 안전하게 저장됩니다. 이를 통해 Axis 생산 시설에서 보안 침해가

발생할 경우 악의적인 추출을 방지할 수 있습니다. Axis PKI 인프라에 대한 자세한 정보는 *www.axis.com/support/public-key-infrastructure-repository*에서 확인할 수 있습니다.


*Figure 5. 제조 프로세스 중에 Axis 장치 ID를 공장 프로비저닝하기 위한 Axis IEEE 802.1AR 공개 키 인프라(PKI). 제품의 일련 번호가 포함된 인증서인 Axis 장치 ID(1)는 Axis 장치 ID 루트 CA(3)에서 서명한 Axis 장치 ID 중간 CA(2)에 의해 서명됩니다. 전용 하드웨어 보안 모듈(HSM)이 안전한 공장 프로비저닝에 사용됩니다.*

*A 참조*
*B 서명*

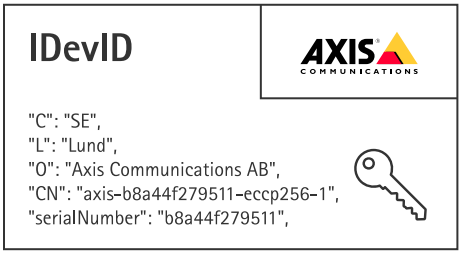


*Figure 6. Axis 장치 ID의 예.*

## 3.2 보안 네트워크 온보딩

Axis 장치를 구입하면 사용을 시작하기 전에 수동 검사를 수행할 수 있습니다. 장치를 육안으로 검사하고 Axis 제품의 모양과 느낌에 대한 사전 지식을 활용하면, 해당 장치가 Axis에서 제공한 제품임을 확신할 수 있습니다. 그러나 이러한 유형의 검사는 장치에 물리적으로 액세스할 수 있는 경우에만 수행할 수 있습니다. 그렇다면 네트워크를 통해 장치와 통신할 때 올바른 장치와 통신하고 있는지 어떻게 확신하고 ID를 확인할 수 있습니까? 네트워크로 연결된 장비나 서버에 있는 소프트웨어는 물리적 검사를 수행할 수 없습니다. 보안 조치로 먼저 안전하게 프로비저닝할 수 있는 폐쇄형 네트워크를 통해 새 장치와 상호 작용하는 것이 일반적입니다.

Axis 장치 ID는 특정 장치가 Axis에서 생산되었으며 해당 장치에 대한 네트워크 연결이 실제로 해당 장치에서 제공된다는 암호화 확인 가능한 증거를 네트워크에 제공합니다. Axis 장치 ID는 IEEE 802.1X 네트워크 인증 프로세스 중에 Axis 장치를 생산 네트워크로 이동하기 전에 추가 소프트웨어 업데이트 및 Axis 장치 구성이 수행되는 프로비저닝 네트워크에 액세스하는 데 사용할 수 있습니다.

Axis 장치 ID를 사용하면, 장치 설치 및 구성에 더 자동화되고 비용 효율적인 제어 기능을 사용할 수 있으므로 전반적인 보안을 강화하고 장치 배포 시간을 줄일 수 있습니다.

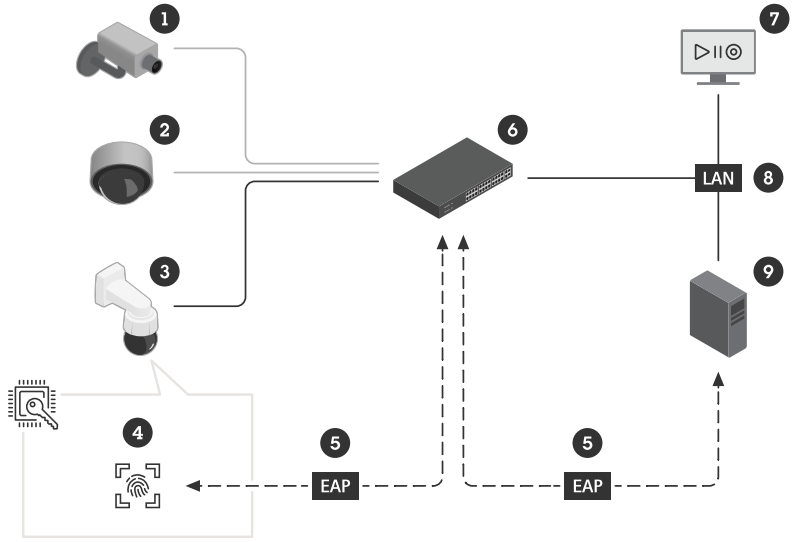


*Figure 7. 보안 네트워크 온보딩. 인증 서버(9)에 Axis 장치(3)를 네트워크(8) 및 VMS(7)에 자동으로 수락하도록 지시할 수 있습니다. 이는 장치 일련 번호와 Axis 장치 ID(4)를 지문 또는 인증으로 사용하여 가능해집니다.*

*1 승인되지 않은 장치(수동으로 온보딩해야 함)*
*2 타사 장치*
*3 Axis 장치*
*4 변조 방지 보안 키 저장소에 안전하게 저장된 Axis 장치 ID*
*5 Axis 장치 ID 인증서를 통한 Axis 장치의 802.1X EAP-TLS 네트워크 인증*
*6 관리 지원 스위치(인증자)*
*7 VMS(장치 검증)*
*8 802.1X로 보호되는 LAN*
*9 RADIUS(네트워크 인증 서버)*

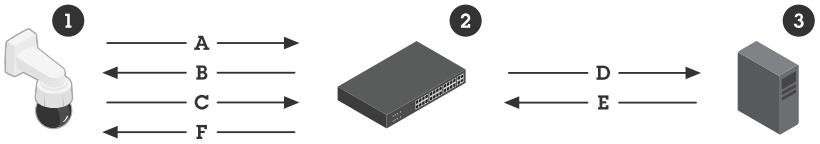


*Figure 8. 온보딩 프로세스에 대한 더 자세한 설명. 보안 장치 ID를 위한 IEEE 802.1AR은 장치에 네트워크 액세스 권한을 부여하기 위해 RADIUS 서버(3)를 사용하여 IEEE 802.1X EAP 요청(EAP-TLS)을 통해 장치(1)를 식별하는 방법을 정의합니다.*

*1 Axis 장치*
*2 관리 지원 스위치(인증자)*
*3 RADIUS 서버(네트워크 인증 서버)*
*A 새로운 연결*
*B EAP 요청 ID*
*C Axis 장치 ID 인증서, IEEE 802.1AR IDevID를 포함한 EAP 응답 ID*

*D RADIUS 액세스 요청*
*E RADIUS 액세스 챌린지*
*F EAP 성공*

Axis 장치 ID는 추가적인 기본 제공 신뢰 소스를 제공하는 것 외에도 장치를 추적할 수 있는 수단을 제공하고 제로 트러스트 네트워킹 원칙에 따라 주기적인 확인 및 인증을 허용합니다.

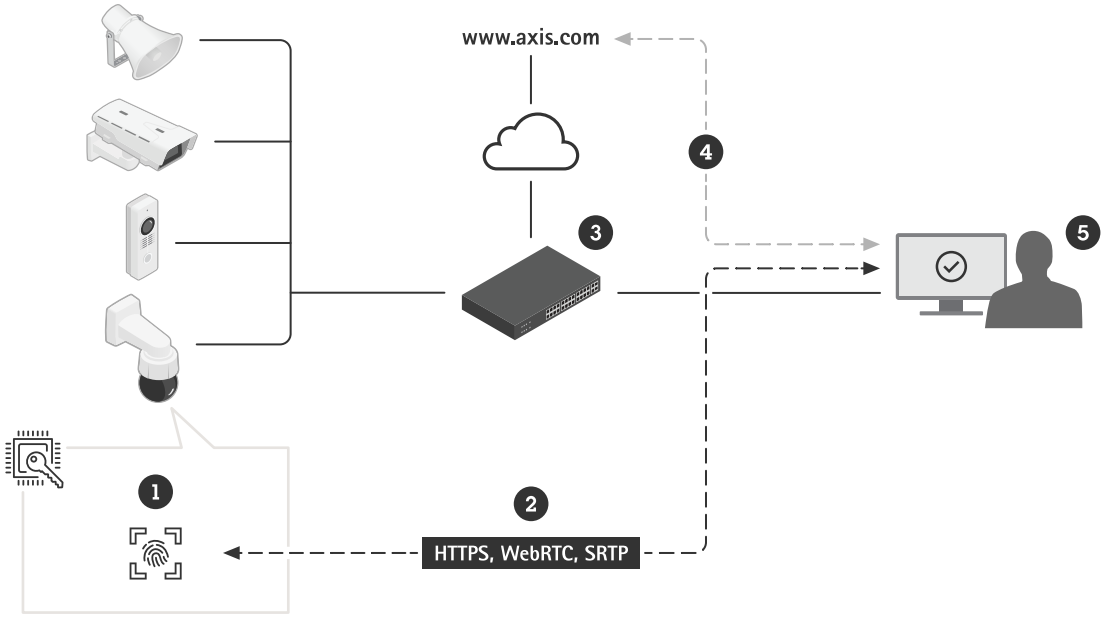


*Figure 9. 장치가 안전하게 온보딩되면 시스템의 다른 부분에 있는 소프트웨어 애플리케이션(5)이 Axis 장치 ID(1) 및 암호화 작업을 사용하여 다양한 TLS 기반 통신(2)에서 장치를 확인하고 인증할 수 있습니다. Axis 장치 ID는 공개적으로 사용 가능한 Axis 장치 ID 루트 CA 인증서(4)로 확인할 수 있습니다.*

*1 변조 방지 보안 키 저장소에 안전하게 저장된 Axis 장치 ID*
*2 TLS 기반 통신(HTTPS, WebRTC, SRTP)*
*3 관리 지원 스위치*
*4 Axis 장치 ID 루트 CA 인증서(www.axis.com/support/public-key-infrastructure-repository에서 다운로드 가능)*
*5 VMS 또는 기타 소프트웨어(장치 검증)*

# 4 안전한 키 보관

일반적으로 민감한 X.509 암호화 정보(개인 키)는 장치의 파일 시스템에 저장됩니다. 사용자 계정이 쉽게 손상되지 않기 때문에 기본적인 보호 기능을 제공하는 사용자 계정 액세스 정책으로만 보호됩니다. 그러나 보안 침해가 발생할 경우, 이 암호화 정보는 보호되지 않고 공격자가 액세스할 수 있습니다.

보안 측면에서 볼 때, 보안 키 저장소는 암호화 정보를 저장하고 보호하는 데 매우 중요합니다. Axis 장치 ID 및 Signed Video에 포함된 민감한 암호화 정보가 보안 키 저장소에 저장될 뿐만 아니라 고객이 로드한 정보도 동일한 방식으로 보호할 수 있습니다.

## 4.1 보안 키 저장소

민감한 암호화 정보(개인 키)는 장치의 하드웨어 기반, 변조 방지 보안 키 저장소에 저장됩니다. 따라서 보안 침해가 발생하더라도 악의적인 추출을 방지할 수 있습니다. 또한 개인 키는 사용 중에도 보안 키 저장소에 보호된 상태로 유지됩니다. 잠재적인 공격자는 보안 키 저장소에 액세스할 수 없으며, 네트워크 트래픽을 도청하거나 IEEE 802.1X 키를 통해 네트워크에 액세스하거나 다른 개인 키를 추출할 수 없습니다.

보안 키 저장소는 하드웨어 기반 암호화 컴퓨팅 모듈을 통해 제공됩니다. 보안 요구 사항에 따라 Axis 장치에는 TPM 2.0(Trusted Platform Module) 또는 보안 요소 및/또는 TEE(Trusted Execution Environment)와 같은 모듈이 하나 또는 여러 개 있을 수 있습니다.

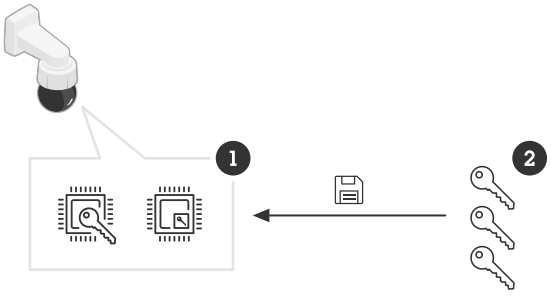


*Figure 10. 보안 키 저장소(1)는 개인 키(2)를 보호하고 암호화 작업을 안전하게 실행합니다.*

1 *보안 요소, TPM 또는 TEE(SoC에 내장)일 수 있는 보안 키 저장소*
2 *Axis 장치 ID, 비디오 서명 키, 접근 제어 키, 파일 시스템 키 및 고객 로드 키(예: IEEE 802.1X 및 HTTPS)와 같은 개인 키*

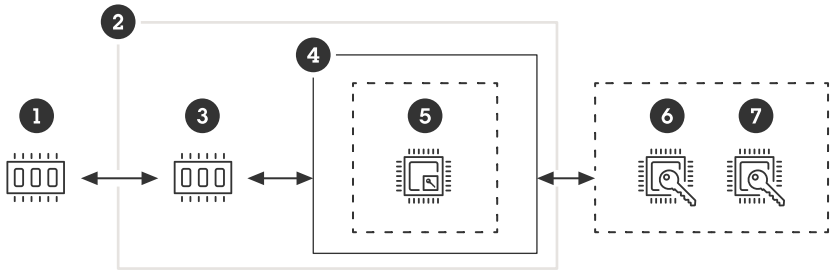


*Figure 11. Axis Edge Vault가 설치된 장치에는 SoC의 메인 프로세서(4) 바로 옆에 PCB에 실장되어 있는 하드웨어 암호화 컴퓨팅 모듈(보안 요소(6) 및 TPM(7))이 있습니다. TEE(5)는 SoC의 메인 프로세서 자체의 보안 영역입니다. SoC에 내장된 부트 ROM(3)은 Secure Boot 절차를 실행하고 플래시 메모리(1)에서 Signed OS 소프트웨어 이미지만 장치 부팅에 사용되도록 하는 역할을 담당합니다.*

1 *플래시 메모리(Signed OS, 읽기-쓰기 파일 시스템용)*

2 *SoC*
3 *부트 ROM(Secure Boot용)*
4 *CPU*
5 *TEE(보안 키 저장소용)*
6 *보안 요소(보안 키 저장소용)*
7 *TPM(보안 키 저장소용)*

TPM, 보안 요소 및 TEE는 모두 개인 키를 보호하고 암호화 작업을 안전하게 실행합니다. 보안 침해가 발생하는 경우 무단 액세스 및 악의적인 추출이 방지됩니다.

## 4.2 공통 평가 기준 및 FIPS 140

암호화 컴퓨팅 모듈은 공통 평가 기준 평가 레벨(CC EAL)과 FIPS 140 준수 레벨(1~4)을 사용하여 인증될 수 있습니다. 이러한 인증은 암호화 작업의 정확성과 무결성을 확인하고 자체 검증, 변조 방지 및 기타 방지 조치와 같은 다양한 변조 방지 대책을 검증하는 데 사용됩니다. 인증에 대한 정보는 Axis 장치의 데이터시트 또는 *Axis 제품 선택기*에서 찾을 수 있습니다. Axis는 통합 하드웨어 암호화 컴퓨팅 모듈이 최소한 Common Criteria EAL4 및/또는 FIPS 140-2/3 Level 2/3에 따라 인증을 받을 것을 요구합니다.

### 4.2.1 공통 평가 기준

공통 평가 기준(CC)(정보 기술 보안 평가를 위한 공통 평가 기준이라고도 함)은 IT 제품 보안 인증을 위한 국제 표준(ISO/IEC 15408)입니다. 공통 평가 기준은 제조업체와 구현자가 보안 기능 및 보증 요구 사항을 보안 목표로 지정할 수 있는 프레임워크를 제공하며, 이를 보호 프로필로 그룹화할 수 있습니다.

이러한 주장된 보안 목표는 인증된 독립 시험 기관에서 평가한 후 공통 평가 기준 데이터베이스에 인증 제품으로 등재됩니다. 시험 기관의 평가 요구 사항과 평가의 철저함은 기능 테스트인 EAL 1부터 공식적 설계 검증 및 테스트인 EAL 7에 이르기까지 할당된 평가 보증 레벨(Evaluation Assurance Level: EAL)을 통해 전달됩니다. 즉, 공통 평가 기준은 운영 체제 및 방화벽에서 TPM 및 여권에 이르기까지 다양한 분야에 적용될 수 있습니다.

공통 평가 기준의 인증 요건에 대한 자세한 내용은 공통 평가 기준 웹사이트 (*www.commoncriteriaportal.org/*)에서 확인할 수 있습니다.

### 4.2.2 FIPS 140

FIPS(연방 정보 처리 표준) 140-2 및 140-3은 NIST(National Institute of Standards and Technology)에서 발행하고 미국 및 캐나다 연방 정부에서 요구 사항으로 채택한 암호 컴퓨팅 모듈 및 암호 알고리즘 사용에 대한 정보 보안 표준입니다. 2019년에 업데이트된 버전인 FIPS 140-3이 FIPS 140-2를 대체합니다. NIST 인증 테스트 연구소에서 수행하는 검증은 모듈 시스템 및 모듈의 암호화가 올바르게 구현되었는지 확인하는 것입니다. 간단히 말해 인증에는 암호화 컴퓨팅 모듈, 승인된 알고리즘, 승인된 운영 모드 및 전원 공급 테스트에 대한 설명, 사양 및 검증이 필요합니다.

고객은 정부 사양에 따라 제품을 운영할 수 있다고 확신할 수 있습니다. 이를 통해 고객은 정부 기관의 감사를 받을 때 안심할 수 있습니다. FIPS 140 규제를 받지 않는 조직은 제품이 정부 정

의 표준을 준수하는지 확인합니다. FIPS 140-2 및 FIPS 140-3의 인증 요구사항에 대한 자세한 내용은 NIST 웹사이트 *www.nist.gov*에서 확인할 수 있습니다.

전체 시스템이 FIPS 140에 부합하려면 시스템의 모든 구성 요소가 FIPS 140을 준수해야 합니다. 예를 들어, 비디오 관리 시스템, 녹화 서버는 물론 카메라와 같은 연결된 장치도 이를 준수해야 합니다. 적어도 소프트웨어 인증 또는 하드웨어 인증 모듈 중 하나 이상을 사용하는 경우 장치는 FIPS 140에 부합합니다.

AXIS OS 버전 12 이상이 설치된 Axis 장치에는 FIPS 140 인증을 받은 소프트웨어 기반(OpenSSL) Axis 암호화 모듈이 탑재되어 있습니다. 대부분의 새로운 Axis 장치에는 FIPS 140 인증을 받은 하드웨어 암호화 모듈과 소프트웨어 기반 암호화 모듈이 모두 통합되어 있습니다. 따라서 운영 체제 수준에서 HTTPS 및 IEEE 802.1X와 같은 소프트웨어 기반 애플리케이션을 제공하기 위해 소프트웨어 인증을 받은 모듈과 안전한 키 저장을 위해 하드웨어 인증을 받은 모듈을 함께 사용하는 최적의 솔루션이 가능합니다.

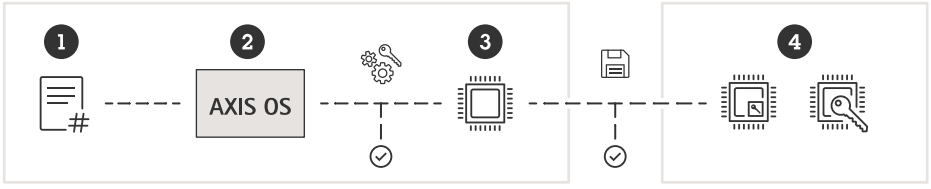


*Figure 12. Axis 장치에서 FIPS 140에 부합하는 암호화 소프트웨어 및 하드웨어 모듈 사용. 애플리케이션(1)은 Axis 장치의 AXIS OS(2)에 내장된 Axis 암호화 모듈을 통해 제공됩니다. Axis 암호화 모듈은 보안 키 저장을 위해 SoC(3) 및/또는 임베디드 하드웨어 기반 암호화 컴퓨팅 모듈(4)을 사용하여 대칭 및 비대칭 암호 작업을 수행합니다.*

1 *암호화가 필요하거나 TLS 기반인 애플리케이션(예: HTTPS, webRTC 및 802.1X)*
2 *임베디드 소프트웨어 기반 암호화 모듈이 탑재된 AXIS OS(NIST 인증서: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4621*
3 *SoC*
4 *임베디드 하드웨어 기반 암호화 컴퓨팅 모듈*

## 4.3 개인 키 보호

공격자의 경우, 개인 키를 추출하면 HTTPS로 암호화된 네트워크 트래픽을 도청하거나 실제 장치인 것처럼 가장하여 802.1X로 보호되는 네트워크에 액세스할 수 있습니다.

Axis 장치는 보안 통신을 위해 다양한 TLS(Transport Layer Security) 기반 프로토콜을 지원합니다. Axis 장치 ID(IEEE 802.1AR), HTTPS(네트워크 암호화) 및 802.1X(네트워크 액세스 제어)는 X.509 암호화 정보 보호에 의존합니다.

TLS의 X.509 디지털 인증서는 네트워크의 두 호스트가 통신할 수 있도록 인증서와 해당 공개 및 개인 키 쌍을 사용합니다. 개인 키는 보안 키 저장소에 저장되며 데이터 복호화에 사용되는 동안에도 저장소를 떠나지 않습니다. 실제 인증서와 공개 키는 알려져 있고, Axis 장치에서 공유할 수 있으며, 데이터를 암호화하는 데 사용됩니다.

## 4.4 접근 제어 키의 보호

Open Supervised Device Protocol(OSDP) Secure Channel과 같은 Axis 접근 제어 솔루션에 사용되는 암호화 정보의 보호는 하드웨어로 보호되는 키 저장이 중요한 이유를 보여주는 또 다른 예입니다.

OSDP Secure Channel은 도어 컨트롤러와 리더와 같은 주변 장치 간의 통신을 보호하기 위해 널리 사용되는 AES-128 기반 암호화 및 인증 방법입니다.

도어 컨트롤러와 리더가 공유하는 AES 대칭 키 SCBK(Secure Channel Base Key)는 상호 인증을 시작하고 나중에 도어 컨트롤러와 리더 간의 통신 데이터를 암호화하는 세션 키 세트를 생성하는 데 사용됩니다.

진정한 엔드 투 엔드 보안을 달성하려면 마스터 키(MK)와 SCBK를 Axis 네트워크 도어 컨트롤러의 보안 키 저장소 내에 안전하게 저장해야 합니다. 마스터 키는 연결된 Axis 리더마다 고유한 SCBK 키를 추출합니다. 또한 설치 단계에서 Axis 리더에 안전하게 배포되는 개별 SCBK는 리더의 보안 키 저장소에 안전하게 저장되어야 합니다. 리더는 일반적으로 도어의 안전하지 않은 쪽에 설치되어 있기 때문에 더 중요합니다.

이러한 방식으로 OSDP Secure Channel 키는 하드웨어로 보호되는 환경에서 양쪽에서 보호됩니다. 따라서 보안 침해가 발생하더라도 악의적인 추출을 방지할 수 있습니다.

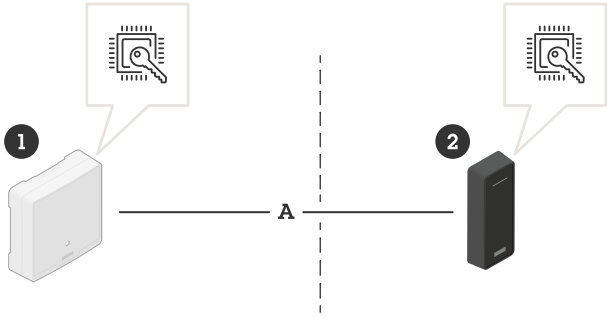


*Figure 13. 접근 제어에서 보안 키 저장소를 사용하여 엔드 투 엔드 보안을 달성합니다. 마스터 키와 개별 보안 채널 기본 키(SCBK)는 모두 보안 키 저장소에 저장되며, 도어의 양쪽의 장치에 저장됩니다.*

*1 도어의 안전한 곳에 설치된 Axis 도어 컨트롤러*
*2 도어의 안전하지 않은 곳에 설치된 Axis 리더*
*A OSDP 보안 채널 통신*

## 4.5 파일 시스템 키 보호

작동 중인 Axis 장치는 고객별 구성 및 정보를 전달합니다. 사전 구성 서비스를 제공한 총판 또는 시스템 통합업체에서 Axis 장치가 고객에게 배송되는 중일 때도 마찬가지입니다. Axis 장치에 대한 물리적 액세스가 성공하면 악의적인 공격자가 플래시 메모리를 분리하고 플래시 리더 장치를 통해 액세스하여 파일 시스템에서 정보를 추출하려고 시도할 수 있습니다. 따라서 읽기/쓰기 가능한 파일 시스템을 민감한 정보 추출 또는 구성 변조로부터 보호하는 것은 Axis 장치를 도난당하거나 침입을 당했을 때 중요한 보호 수단입니다.

보안 키 저장소는 파일 시스템에 강력한 암호화를 적용하여 악의적인 정보 유출을 방지하고 구성 변조를 방지합니다. Axis 장치의 전원이 꺼지면, 파일 시스템의 정보가 암호화됩니다. 부팅 프로세스 중에, 읽기-쓰기 파일 시스템은 AES-XTS-Plain64 256 비트 키로 복호화되어, Axis 장치가 파일 시스템을 마운트하고 사용할 수 있습니다. 파일 시스템 암호화 키는 공장 출하 시 장치별로 고유하게 생성되며, 소프트웨어를 업데이트할 때마다 다시 생성되므로, 장치 수명 주기 동안 키가 동일하지 않습니다.

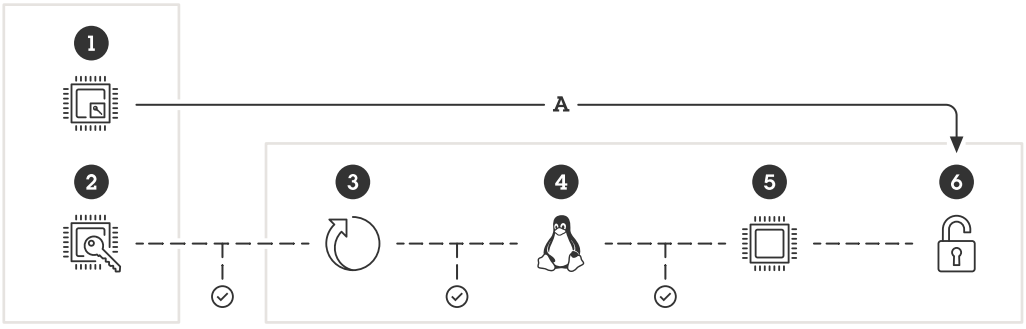


*Figure 14. TEE(1) 및 부트 ROM(2)은 SoC에 내장되어 있습니다. 부트 프로세스 중에 TEE에 의해 읽기-쓰기 파일 시스템(6)이 복호화되어 Axis 장치에서 파일 시스템을 마운트하고 사용할 수 있도록 합니다. 부팅 프로세스에서 체인의 각 부분(부트로더(3), Linux 커널(4) 및 루트 파일 시스템(5))이 확인되고 플래시 메모리에서 다음 하위 시스템을 인증합니다. 이를 통해 궁극적으로 루트 파일 시스템이 확인됩니다.*

*1 TEE*
*2 부트 ROM*
*3 부트로더*
*4 Linux 커널*
*5 루트 파일 시스템*
*6 읽기-쓰기 파일 시스템*
*A TEE는 읽기-쓰기 파일 시스템을 복호화합니다.*

# 5 비디오 변조 방지

보안 산업의 기본 전제는 감시 카메라로 녹화된 영상이 진본이며 신뢰할 수 있다는 것입니다. Signed Video는 증거로서 영상의 신뢰도를 유지하고 더욱 강화하기 위해 개발된 기능입니다. 이 기능은 영상의 진위를 확인함으로써 영상이 카메라를 떠난 후 편집되거나 변조되지 않았는지 확인하는 수단을 제공합니다.

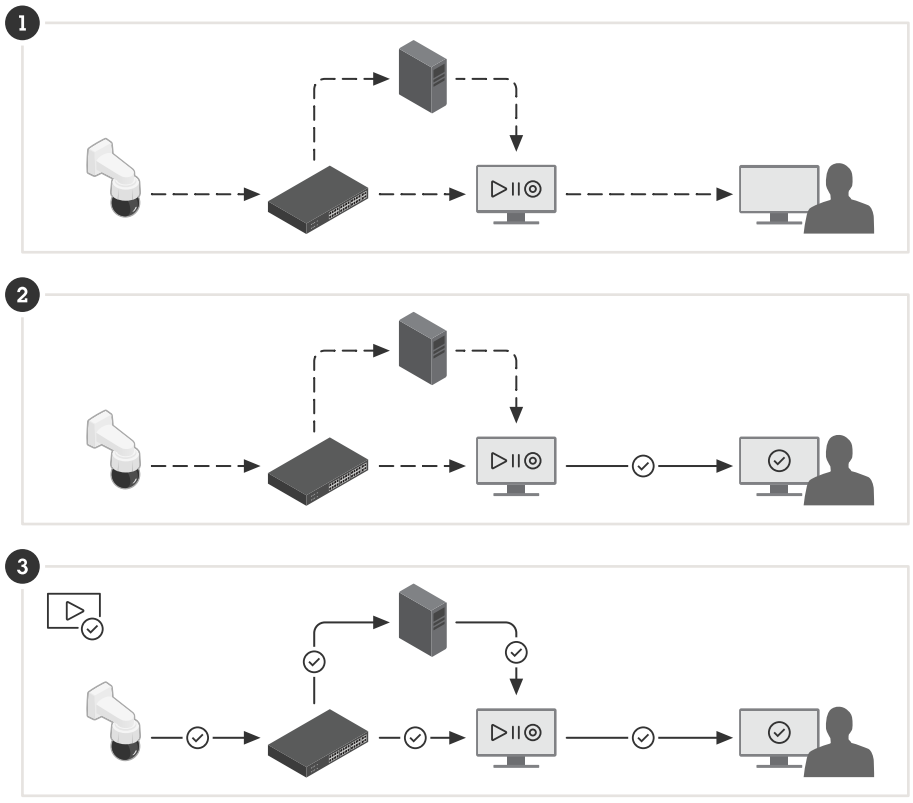

*Figure 15. 비디오 진위 여부 확인:*

1. *비디오는 카메라에서 녹화물을 보는 사람에게 전달되기까지 여러 단계를 거칩니다. 숙련된 공격자는 이러한 전달 과정에서 비디오를 변조할 수 있습니다.*
2. *내보내기 중에 비디오에 VMS 워터마크를 추가하면 일부 단계가 확인되지만, 이전 단계에서 동영상이 변조되지 않았다는 보장은 없습니다.*
3. *Signed Video는 카메라에서 내보낸 녹화물을 보는 사람에게 전달되는 모든 단계에서 비디오가 변조되지 않았는지 확인하기 위한 수단을 제공합니다. 비디오를 녹화한 장치를 추적할 수 있습니다.*

## 5.1 Signed Video

Axis가 개발한 signed video 기능을 사용하면 비디오 스트림의 서명을 사용하여 비디오가 손상되지 않도록 보호하고 비디오 스트림을 생성한 카메라로 다시 추적하여 원본을 확인할 수 있습니다. 이를 통해 비디오 파일의 보관의 연속성을 증명할 필요 없이 비디오 진위를 증명할 수 있습니다.

보안 카메라 시스템에 사건이 녹화된 후 경찰은 USB 메모리에 내보낸 비디오 파일로 비디오를 수신하여 EMS(Evidence Management System)에 저장할 수 있습니다. 카메라에서 비디오를 내보내는 동안 경찰관은 비디오가 올바르게 서명되었는지 확인할 수 있습니다. 추후 기소 과정에서 사용될 경우 법원은 비디오가 녹화된 시간, 비디오를 녹화한 카메라, 비디오 프레임의 변경 또는 제거

여부 등을 통제하고 검증할 수 있습니다. Axis의 *파일 플레이어*를 사용하면 비디오 사본이 있는 모든 사람이 이 정보를 볼 수 있습니다.

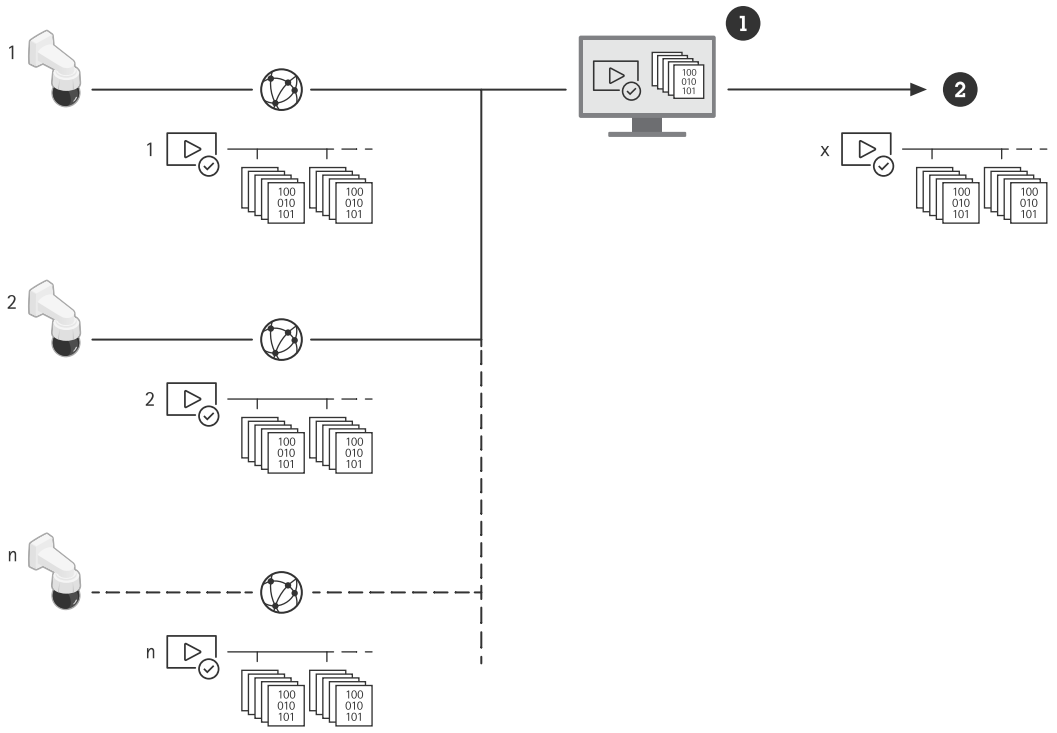


*Figure 16. 서명은 이미 카메라에 추가되어 소스에서 비디오의 최종 사용까지 모든 단계에서 콘텐츠를 확인할 수 있습니다.*

*1 VMS*
*2 CD/USB/웹/이메일로 비디오 내보내기*

각 카메라는 보안 키 저장소에 저장된 고유한 비디오 서명 키를 사용하여 비디오 스트림에 서명을 추가합니다. 이는 메타데이터를 포함하여 각 비디오 프레임의 해시를 계산하고 결합된 해시에 서명하여 수행됩니다. 그런 다음 서명은 전용 메타데이터 필드(SEI 헤더)의 스트림에 보관됩니다.

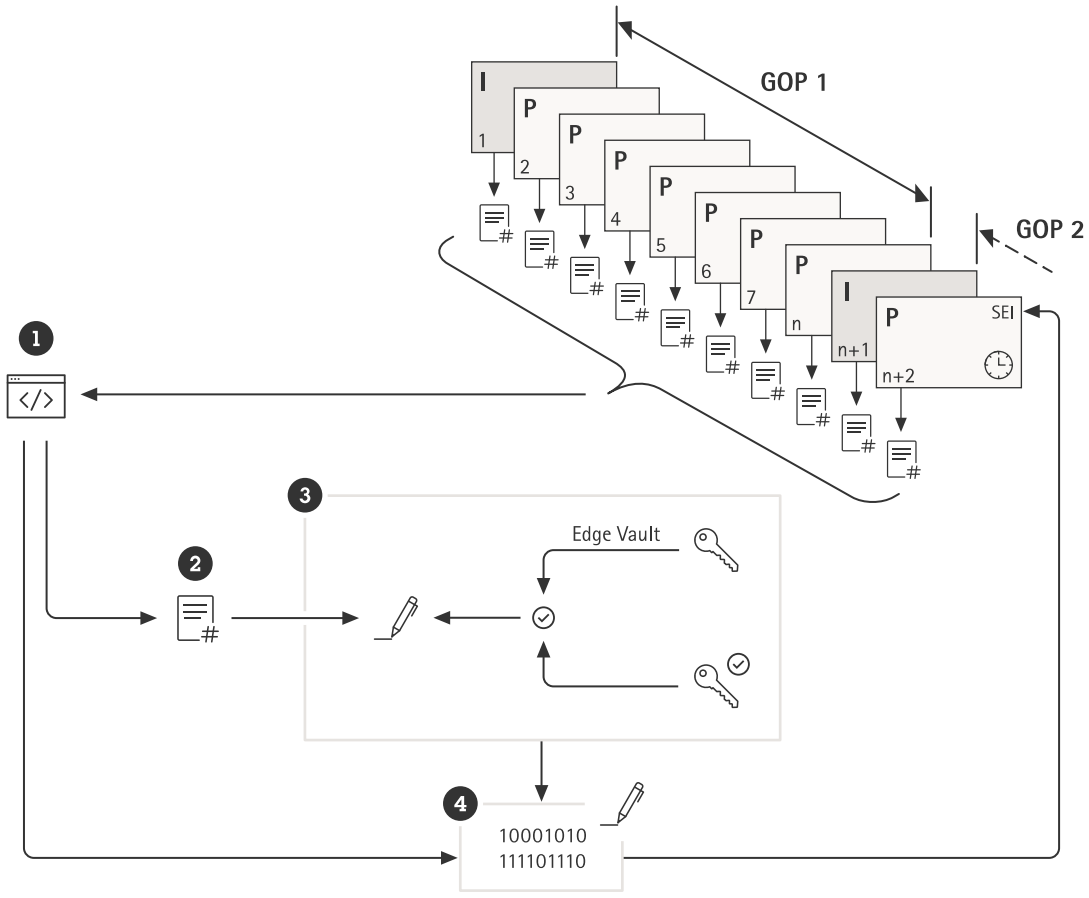


*Figure 17. 비디오 스트림에 서명이 추가되는 방식을 그래픽으로 표현한 것입니다. GOP(Group of Pictures)의 각 프레임 콘텐츠는 메타데이터 해시(1)와 함께 해시됩니다. 이를 통해 장치 고유 비디오 서명 키 및 증명 키를 사용하여 Edge Vault(3)에 서명되는 GOP 해시(2)가 형성됩니다. 그런 다음 디지털 서명(4)과 메타데이터(1)가 스트림을 따라 전송되는 이후의 SEI 헤더에 추가됩니다.*

1 *장치 고유 메타데이터(하드웨어 ID, AXIS OS 버전, 일련 번호 및 증명 보고서*) 및 스트림 메타데이터(GOP 카운터 및 프레임 해시)*
2 *GOP 해시*
3 *Axis Edge Vault*
4 *디지털 서명*

* *증명 보고서는 서명에 사용된 키 쌍의 출처 및 기원을 확인하는 데 사용할 수 있습니다. 키 증명을 확인하면 키가 특정 장치의 하드웨어에 안전하게 보관되어 있는지 확인할 수 있습니다. 이것은 비디오의 출처를 보호합니다.*

실제 서명은 장치 고유의 증명 키를 사용하여 증명되는 장치 고유의 비디오 서명 키를 사용하여 이루어집니다. 증명 보고서는 시작 시 스트림에 첨부된 다음 정기적인 간격(일반적으로 한 시간에 한 번)으로 첨부됩니다. 메타데이터에는 각 개별 프레임 해시가 포함되어 있으므로 어떤 개별 프레임이 올바른지 감지할 수 있습니다. 서명을 완료하려면 비디오의 GOP(Group of Pictures) 구조를

보호해야 합니다. 이것은 서명에 다음 GOP의 첫 번째 I-프레임의 해시를 포함하여 수행됩니다. 이렇게 하면 감지할 수 없는 절단이나 프레임 재정렬을 방지할 수 있습니다. 혹시라도 스트리밍 중에 프레임이 손실되거나 저장 중에 손상될 경우, 동일한 방법으로 플래그를 지정할 수 있습니다.

# 6 용어집

**Axis 장치 ID**: Axis 장치의 진위 여부를 증명할 수 있는 해당 키가 포함된 장치 고유 인증서입니다. Axis 장치는 보안 키 저장소에 저장된 Axis 장치 ID로 공장 출하 시 프로비저닝됩니다. Axis 장치 ID는 자동화된 보안 식별 방법을 정의하는 국제 표준 IEEE 802.1AR(IDevID, 초기 장치 식별자)을 기반으로 합니다.

**Axis Edge Vault**: Axis 장치를 보호하는 하드웨어 기반 사이버 보안 플랫폼입니다. 이 플랫폼은 암호화 컴퓨팅 모듈(보안 요소 및 TPM) 및 SoC 보안(TEE 및 Secure Boot)의 강력한 기반 위에 구축되며, 에지 장치 보안에 대한 전문 지식이 결합되어 있습니다.

**인증서**: 공개/개인 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.

**공통 평가 기준(Common Criteria: CC)**: IT 제품 보안 인증을 위한 국제 표준입니다. 정보 기술 보안 평가에 대한 공통 평가 기준(Common Criteria for Information Technology Security Evaluation), ISO/IEC 15408이라고도 합니다.

**FIPS 140**: 암호화 컴퓨팅 모듈을 승인하는 데 사용되는 일련의 미국 컴퓨터 보안 표준입니다. 연방 정보 처리 표준(Federal Information Processing Standard: FIPS) 140은 모듈 변조 위험을 완화하기 위해 암호화 모듈을 어떻게 설계하고 구현해야 하는지에 대한 요구 사항을 정의합니다.

**변경 불가능 ROM(읽기 전용 메모리)**: 신뢰할 수 있는 공개 키와 서명을 비교하는 데 사용되는 프로그램을 덮어쓸 수 없도록 안전하게 저장하는 읽기 전용 메모리입니다.

**프로비저닝**: 네트워크를 위해 장치를 준비하고 장착하는 과정입니다. 여기에는 중앙 지점의 구성 데이터 및 정책 설정을 장치에 전달하는 작업이 포함됩니다. 장치에 키 및 인증서가 제공됩니다.

**공개 키 암호화**: 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.

**Secure Boot**: 장치를 시작하는 동안 승인되지 않은 소프트웨어의 로딩을 방지하는 기능입니다. Secure Boot는 Signed OS를 사용하여 승인된 Axis 소프트웨어만 장치를 부팅하는 데 사용되도록 합니다.

**보안 요소**: 하드웨어 기반의 변조 방지된 개인 키 저장 및 암호화 작업의 안전한 실행을 제공하는 암호화 컴퓨팅 모듈입니다. TPM과 달리 보안 요소의 하드웨어 및 소프트웨어 인터페이스는 표준화되어 있지 않고 제조업체마다 다릅니다.

**보안 키 저장소**: 개인 키를 보호하고 암호화 작업을 안전하게 실행하기 위한 변조 방지 환경입니다. 보안 침해 발생 시 무단 액세스 및 악의적인 추출을 방지합니다. 보안 요구 사항에 따라, Axis

장치에는 하드웨어로 보호되는 보안 키 저장소를 제공하는 하드웨어 기반 암호화 컴퓨팅 모듈이 하나 또는 여러 개 있을 수 있습니다.

**Signed OS(서명된 운영 체제)**: 신뢰할 수 있는 당사자가 파일 이미지에 디지털 코드 서명을 한 장치 소프트웨어입니다. Signed OS는 Secure Boot 프로세스에서 신뢰할 수 있는 소프트웨어 이미지로부터만 장치가 부팅되도록 하기 위한 요구 사항입니다. AXIS OS 기반 제품에서는, 업데이트를 수행하기 전에 장치가 장치 소프트웨어 이미지의 무결성과 진위 여부를 확인합니다.

**Signed Video**: 증거로서 비디오의 신뢰성을 유지하고 강화하는 기능입니다. Signed Video는 비디오 변조 감지 및 진위 여부 판정을 제공하며, 비디오가 온전하고 특정 Axis 카메라로 역추적할 수 있도록 보호하는 데 사용됩니다. Signed Video의 서명 키는 Axis 장치의 보안 키 저장소에 있습니다.

**Transport Layer Security(TLS)**: 네트워크 트래픽을 보호하기 위한 인터넷 표준입니다. TLS는 HTTPS에서 보안을 위한 S(보안용)를 제공합니다.

**Trusted Execution Environment(TEE)**: 하드웨어 기반의 변조 방지 개인 키 저장소 및 암호화 작업의 안전한 실행을 제공합니다. 보안 요소 및 TPM과 달리 TEE는 시스템 온 칩(SoC) 메인 프로세서의 안전한 하드웨어 격리 영역입니다.

**Trusted Platform Module(TPM)**: 하드웨어 기반의 변조 방지 개인 키 저장 및 암호화 작업의 안전한 실행을 제공하는 암호화 컴퓨팅 모듈입니다. TPM은 *TCG(Trusted Computing Group)*에서 정의한 국제적으로 표준화된(TPM 1.2, TPM 2.0) 컴퓨터 구성 요소입니다.

**제로 트러스트 보안**: 연결된 장치와 IT 인프라(네트워크, 컴퓨터, 서버, 클라우드 서비스, 애플리케이션 등)가 서로를 반복적으로 식별, 검증, 인증하여 높은 보안 제어를 달성해야 하는 IT 보안에 대한 최신 접근 방식입니다.

# Axis Communications 정보

Axis는 보안 및 새로운 비즈니스 성과를 개선하기 위한 솔루션을 창조하여 더 스마트하고 안전한 세상을 가능하게 합니다. 네트워크 기술 회사이자 업계 리더인 Axis는 비디오 감시, 접근 제어, 인터콤, 오디오 시스템 솔루션을 제공합니다. 이러한 솔루션은 지능형 분석 애플리케이션으로 향상되고, 고품질 교육의 지원을 받습니다.

Axis에서는 50개 이상의 나라에 약 4,000명의 전담 직원이 있으며 전 세계 기술 및 시스템 통합 파트너와 협력하여 고객 솔루션을 제공합니다. Axis는 1984년에 설립되었으며 본사는 스웨덴 룬드에 있습니다