WHITEPAPER

Axis Edge Vault

Die hardwaregestützte Cybersicherheitsplattform, die Axis Geräte durch folgende Maßnahmen schützt:

– Schutz der Lieferkette

– Vertrauenswürdige Geräteidentität

– Sichere Speicherung der Schlüssel

– Videomanipulationserkennung

April 2024

AXIS COMMUNICATIONS

Zusammenfassung

Axis Edge Vault stellt eine Hardware-basierte Cybersicherheitsplattform bereit, die das Axis Gerät schützt. Es sorgt für eine starke Grundlage kryptografischer Berechnungsmodule (Sicherheitselement und TPM) und SoC-Sicherheit (TEE und Secure Boot), die wir mit Expertise in Edge-Gerätesicherheit kombinieren. Axis Edge Vault ist ein starker Vertrauensanker, der durch *Secure Boot* in Verbindung mit *Signed OS* entsteht („OS" steht für Operating System=Betriebssystem). Diese Merkmale ermöglichen eine lückenlose Kette kryptografisch validierter Software für die Vertrauenskette, auf der sämtliche sicheren Operationen beruhen.

Axis Geräte mit Edge Vault minimieren Risiken für die Cybersicherheit bei den Kundinnen und Kunden, da sie das Abhören und die böswillige Verwendung sensibler Informationen verhindern. Axis Edge Vault macht Axis Geräte außerdem zu vertrauenswürdigen, zuverlässigen Geräten im Kundennetzwerk.

Axis Edge Vault Cybersicherheitsplattform

Kryptografische Berechnungsmodule	Merkmale	Anwendungsbeispiele
• Secure-Element • TPM 2.0 • SoC-Sicherheit (TEE)	• Sicheres Hochfahren • Signiertes Betriebssystem • Axis Geräte-ID • Sicherer Schlüsselspeicher • Signiertes Video • Verschlüsseltes Dateisystem	• Schutz der Lieferkette • Vertrauenswürdige Geräteidentität • Sichere Speicherung der Schlüssel • Videomanipulationserkennung

- **Schutz der Lieferkette:** Axis Edge Vault benötigt eine sichere Grundlage als Vertrauensanker. Ohne die Hilfe von Secure Boot und Signed OS kann die Vertrauensanker-Kette nicht entstehen. Secure Boot stellt zusammen mit Signed OS eine lückenlose Kette kryptografisch validierter Software bereit, beginnend im unveränderbaren Speicher (Boot-ROM). Secure Boot sorgt dafür, dass ein Gerät nur mit signiertem Betriebssystem gestartet werden kann. Das verhindert Manipulationen an der physischen Lieferkette. Ein Gerät mit signiertem Betriebssystem kann außerdem neue Geräte-Software validieren, bevor es zulässt, dass sie installiert wird. Erkennt das Gerät, dass die Integrität verletzt wurde oder die Geräte-Software nicht von Axis signiert wurde, weist es das Upgrade zurück. Das schützt Geräte vor Software-Manipulation.
- **Vertrauenswürdige Geräteidentität:** Den Ursprung eines Gerätes überprüfen zu können, ist der Schlüssel zum Vertrauen in die Geräteidentität. In der Produktion wird Geräten mit Axis Edge Vault ein eindeutiges, von der Fabrik bereitgestelltes und IEEE 802.1AR-kompatibles Zertifikat für die Axis Geräte-ID zugewiesen. Dies funktioniert wie ein Reisepass und weist den Ursprung des Gerätes nach. Die Geräte-ID wird sicher und permanent als vom Axis Root-Zertifikat signiertes Zertifikat im sicheren Schlüsselspeicher aufbewahrt. Daraufhin kann die Geräte-ID von der IT-Infrastruktur des Kunden für automatisiertes, sicheres Onboarding des Gerätes und zur sicheren Geräteidentifizierung genutzt werden.
- **Sichere Speicherung der Schlüssel:** Der sichere Schlüsselspeicher speichert kryptografische Daten Hardware-basiert und manipulationsgeschützt. Der sichere Schlüsselspeicher schützt die Axis Geräte-ID sowie von den Kundinnen und Kunden geladene kryptografische Daten und verhindert unbefugte Zugriffe und böswillige Extraktion bei einem Sicherheitsverstoß.

- **Videomanipulationserkennung:** Signiertes Video sorgt dafür, dass Videobeweise als nicht manipuliert verifiziert werden können, ohne die Produktkette der Videodatei überprüfen zu müssen. Jede Kamera hat ihren eigenen, eindeutigen Videosignierschlüssel, der zuverlässig im sicheren Schlüsselspeicher aufbewahrt wird und eine Signatur zum Videostream hinzufügt. Wenn das Video abgespielt wird, zeigt der *Dateiplayer* von Axis an, ob das Video intakt ist. Signiertes Video ermöglicht die Nachverfolgung des Videos bis zur Kamera und die Überprüfung, ob das Video nach der Aufzeichnung verfälscht wurde.

Inhalt

1 Einführung

Axis folgt hinsichtlich der Sicherheit bei unseren Produkten bewährten Branchenpraktiken. Damit möchten wir die Exposition der Kunden gegenüber Cybersicherheitsrisiken minimieren und dafür sorgen, dass Axis Geräten im Kundennetzwerk immer vertraut werden kann.

Axis Edge Vault stellt eine Hardware-basierte Cybersicherheitsplattform bereit, die das Axis Gerät schützt. Es sorgt für eine starke Grundlage kryptografischer Berechnungsmodule (Sicherheitselement und TPM) und SoC-Sicherheit (TEE und Secure Boot), die wir mit Expertise in Edge-Gerätesicherheit kombinieren.

Dieses Whitepaper beschreibt die mehrstufige Strategie der Axis Edge-Gerätesicherheit, zeigt häufige Risiken auf und beschreibt, wie man diese verhindert. Axis Edge Vault benötigt eine sichere Grundlage als Vertrauensanker. Deshalb gehen wir auch auf die Sicherheitsaspekte in der Lieferkette von Axis Geräten ein und zeigen, wie ein Signed OS (signiertes Betriebssystem) und Secure Boot (sicheres Hochfahren) als grundlegende Maßnahmen einer Manipulation der Firmware und der physischen Manipulationen der Lieferkette einen Riegel vorschieben.

Unter *https://www.axis.com/de-de/support/cybersecurity/resources* finden Sie weitere Informationen über die Produktsicherheit, erkannte Schwachstellen und Maßnahmen, mit denen Sie den Risiken häufiger Bedrohungen begegnen können.

Der letzte Teil dieses Whitepapers besteht aus einem Glossar.

2 Schutz der Lieferkette

Axis Edge Vault benötigt eine sichere Grundlage als Vertrauensanker. Die Grundlage für diesen Vertrauensanker beginnt beim Hochfahren des Gerätes. In Axis Geräten verifiziert der Hardware-basierte Mechanismus *Secure Boot* (sicheres Hochfahren) das Betriebssystem (AXIS OS), worüber das Gerät hochgefahren wird. AXIS OS wiederum wird während des Build-Prozesses mithilfe eines *signierten Betriebssystems* kryptografisch signiert.

Secure Boot und Signed OS sind miteinander verknüpft. Sie stellen sicher, dass das Betriebssystem oder die Geräte-Software vor dem Deployment nicht manipuliert wurde (durch jemandem mit physischem Zugriff auf das Gerät) und dass das Gerät auch danach keine verfälschten oder nicht mit einem Codeschlüssel versehenen Software-Updates installieren kann. Zusammen schaffen sicheres Hochfahren und signiertes Betriebssystem eine lückenlose Kette kryptografisch validierter Software und eine ununterbrochene Vertrauenskette, auf der sämtliche sicheren Operationen beruhen.

2.1 Sicheres Hochfahren

Secure Boot oder „Sicheres Hochfahren" ist ein Bootvorgang, der aus einer ununterbrochenen Kette von kryptografisch validierter Software besteht, die im unveränderbaren Speicher (Boot-ROM) beginnt. Sicheres Hochfahren stellt sicher, dass ein Gerät nur mit einem autorisierten Betriebssystem gestartet werden kann.

Der Bootvorgang wird durch das Boot-ROM eingeleitet, das den Bootloader validiert. Beim sicheren Hochfahren werden dann in Echtzeit die eingebetteten Signaturen für jede aus dem Flash-Speicher geladene Software-Komponente überprüft. Das Boot-ROM stellt einen Vertrauensanker dar: Der Bootvorgang wird nur fortgesetzt, wenn jede Signatur verifiziert wurde. Jeder Teil der Kette authentifiziert den jeweils

nächsten Teil, so dass am Ende ein verifizierter Linux-Kernel und ein verifiziertes Root-Dateisystem entstehen.

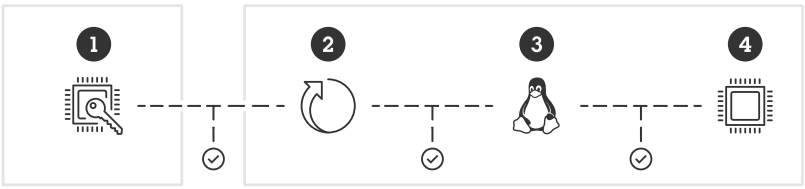

Figure 1. Beim sicheren Hochfahren authentifiziert jeder Teil der Kette die jeweils nachfolgende. Das ergibt am Ende ein verifiziertes Root-Dateisystem.

1 *Boot-ROM (Vertrauensanker) im SoC*
2 *Bootloader*
3 *Linux-Kernel*
4 *Root-Dateisystem*

Bei vielen Geräten ist es wichtig, dass die Low-Level-Funktionen nicht verändert werden können. Werden andere Sicherheitsmechanismen auf die Software der unteren Ebene aufgesetzt, dient das Secure Boot-Verfahren als sichere Basisschicht, die verhindert, dass diese Mechanismen umgangen werden. Bei Geräten mit Secure Boot ist das Betriebssystem im Flash-Speicher vor Veränderung geschützt, die Konfiguration hingegen bleibt ungeschützt. Sicheres Hochfahren garantiert den ordnungsgemäßen Zustand des Gerätes sogar nach einem Zurücksetzen auf Werkseinstellungen. Doch das kann nur funktionieren, wenn beim Booten verifiziert wird, dass das Betriebssystem von Axis signiert wurde.

2.2 Signiertes Betriebssystem

Um das Betriebssystem mit einer Code-Signatur zu versehen, signiert Axis ein Software-Image mit einem privaten Schlüssel, der geheim gehalten wird. Beim Start eines Axis Geräts überprüft Secure Boot, ob die Geräte-Software signiert ist. Erkennt das Gerät, dass die Integrität der Geräte-Software verletzt wurde, wird das Gerät nicht hochgefahren. Bei Aktualisierung der Geräte-Software überprüft das vorhandene, signierte AXIS OS automatisch, ob das neue AXIS OS ebenfalls signiert ist. Falls nicht, wird das Upgrade zurückgewiesen.

Die Vergabe der Code-Signatur für das Betriebssystem wird durch die Berechnung eines kryptographischen Hash-Wertes eingeleitet. Der Wert wird dann mit dem privaten Schlüssel eines privat/öffentlichen Schlüsselpaares signiert, bevor die Signatur an das AXIS OS Image angehängt wird.

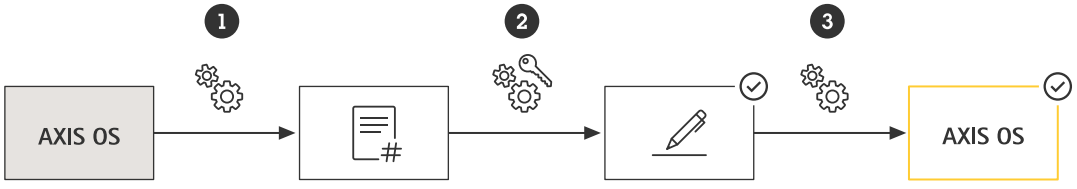

Figure 2. Versehen des OS mit einer Code-Signatur.

1 *Ein kryptographischer Hash-Wert für AXIS OS wird erzeugt.*
2 *Die Signatur wird als Kombination aus dem Hash-Wert und dem privaten Schlüssel erzeugt.*
3 *Die Signatur wird zur AXIS OS Version und zum Binärprogramm hinzugefügt.*

Vor einem Upgrade muss die Echtheit des neuen Software-Updates überprüft werden. Hierfür wird mithilfe des öffentlichen Schlüssels (im Lieferumfang des Axis Produkts enthalten) bestätigt, dass der Hashwert tatsächlich mit dem passenden privaten Schlüssel signiert wurde. Indem auch der Hash-Wert berechnet und mit diesem validierten Hash-Wert aus der Signatur verglichen wird, lässt sich die Integrität verifizieren. Das Boot-Verfahren von Axis Geräten wird abgebrochen, falls die Signatur ungültig ist oder das AXIS OS Image manipuliert wurde.

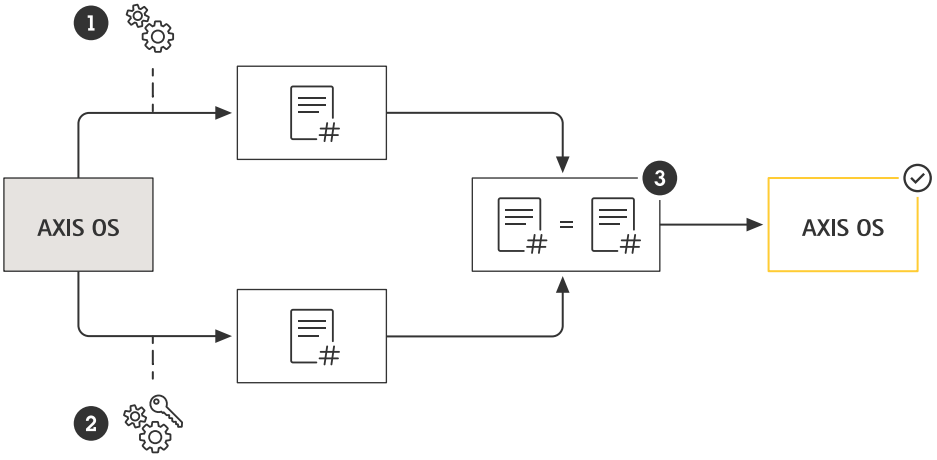

Figure 3. Überprüfung des signierten Betriebssystems.

1. *Berechnen des Hash-Wertes von AXIS OS*
2. *Überprüfung des Hash-Werts anhand des öffentlichen Schlüssels aus der Signatur*
3. *Nur wenn die Ergebnisse übereinstimmen, wird die Signatur erfolgreich bestätigt.*

Das Axis Signed OS basiert auf der von der Branche anerkannten Verschlüsselungsmethode RSA mit öffentlichem Schlüssel. Der private Schlüssel wird streng bewacht bei Axis gespeichert, nur der öffentliche Schlüssel ist in die Axis Geräte eingebettet. Die Integrität des gesamten Software-Image wird durch eine Signatur bestätigt. Eine primäre Signatur überprüft verschiedene sekundäre Signaturen, die während des Entpackens des Bildes überprüft werden.

Für Tests und benutzerspezifische Lösungen hat Axis einen Mechanismus entwickelt, nach dem einzelne Geräte Images von Dritten akzeptieren dürfen. Dieses Image wird mit einem für diesen Zweck reservierten speziellen Schlüsselcode signiert, mit Zustimmung der Besitzerin/des Besitzers und von Axis, woraus sich eine benutzerspezifische Signatur ergibt. Nach der Installation in den zugelassenen Geräten ermöglicht das Zertifikat die Nutzung eines benutzerspezifischen Images, das nur auf diesem Gerät läuft, abhängig von ihrer eindeutigen Seriennummer und Chip-ID. Benutzerspezifische Zertifikate können nur von Axis erstellt werden, da nur Axis über den Schlüssel zu ihrer Signierung verfügt.

3 Vertrauenswürdige Geräteidentität

In modernen Zero-Trust-Netzwerken („trau niemals, prüfe immer“) ist es unbedingt notwendig, den Ursprung des Gerätes, seine Echtheit und seine Verbindungen überprüfen zu können. Ein Netzwerk-Gerät kann seine Integrität und Echtheit auf ähnliche Weise nachweisen, wie man am Flughafen seinen Reisepass als Identitätsnachweis vorlegt.

3.1 Sichere Geräteidentifizierung mit der Axis Geräte-ID

Der internationale Standard *IEEE 802.1AR* legt ein Verfahren zur automatisierten und geschützten Identifizierung eines Geräts über ein Netzwerk fest. Wenn die Kommunikation in ein eingebettetes kryptografisches Berechnungsmodul weitergeleitet wird, kann das Gerät eine dem Standard entsprechende vertrauenswürdige Identifikationsantwort zurücksenden. Anhand dieser vertrauenswürdigen Antwort kann die Netzwerk-Infrastruktur das Gerät automatisiert und sicher zur anfänglichen Gerätekonfiguration und für Software-Updates in ein Bereitstellungsnetzwerk eingliedern.

Zur Erfüllung von IEEE 802.1AR produzieren wir die meisten unserer Geräte mit einem jeweils eindeutigen, ab Werk bereitgestellten Axis Geräte-ID-Zertifikat (IEEE 802.1AR Initial Device Identifier, IDevID). Die Axis Geräte-ID wird sicher im manipulationsgeschützten sicheren Schlüsselspeicher aufbewahrt, der über ein kryptografisches Berechnungsmodul im Gerät selbst bereitgestellt wird. Jedes Axis Gerät hat eine eigene, eindeutige Identität, die seine Herkunft belegt.

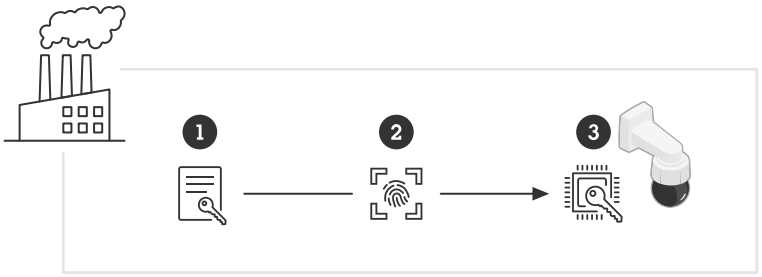

Figure 4. Bei der Herstellung eines Geräts wird die eindeutige Axis Geräte-ID (2) in seinem sicheren Schlüsselspeicher (3) gespeichert.

1 *Axis Geräte-ID Public Key Infrastructure (PKI)*
2 *Axis Geräte-ID*
3 *Die Axis Geräte-ID wird sicher im manipulationsgeschützten sicheren Schlüsselspeicher aufbewahrt, der über ein kryptografisches Berechnungsmodul im Axis Gerät bereitgestellt wird.*

IEEE 802.1AR basiert auf dem Standard IEEE 802.1X für die Netzwerkzugangskontrolle, das bei vorausgewählter Axis Geräte-ID standardmäßig in Axis Geräten aktiviert ist. Dies ermöglicht eine sichere Identifizierung und Authentifizierung des Axis Geräts über eine 802.1X-fähige IT-Infrastruktur, sogar nach dem Zurücksetzen auf Werkseinstellungen.

Das Axis Geräte-ID-Zertifikat gibt es in verschiedenen kryptografischen Konfigurationen (2048-Bit RSA, 4096-Bit RSA, ECC-P256). Diese sind standardmäßig aktiviert, um sichere Geräteverbindungen und Identifizierung über die IEEE 802.1X Netzwerkzugangskontrolle sowie HTTPS zu ermöglichen.

Axis verwaltet seine eigene IEEE 802.1AR Public Key Infrastructure (PKI) für die Bereitstellung der Axis Geräte-ID ab Werk bereits während der Herstellung. Die Axis Geräte-ID wird durch das Zwischenzertifikat signiert, das wiederum vom Axis Root-Zertifikat signiert wird. Beide, die Root-CA und die Zwischen-CA, werden sicher in kryptografischen Berechnungsmodulen gespeichert. Beide sind geographisch voneinander getrennt. Das verhindert eine böswillige Extraktion bei einem Sicherheitsverstoß an einer

Produktionsanlage von Axis. Weitere Informationen zur Infrastruktur der Axis PKI finden Sie unter *https://www.axis.com/de-de/support/public-key-infrastructure-repository*

Figure 5. Axis IEEE 802.1AR Public-Key Infrastructure (PKI) für die Bereitstellung der Axis Geräte-ID ab Werk der Herstellung. Die Axis Geräte-ID (1), ein Zertifikat mit der Seriennummer des Produkts, wird von einer Zwischen-CA (2) für die Axis Geräte-ID signiert, die vom Root CA (3) für die Axis Geräte-ID unterzeichnet wurde. Spezielle Hardware-Sicherheitsmodule (HSM) sorgen für eine sichere Bereitstellung ab Werk.

A Referenz
B Signieren

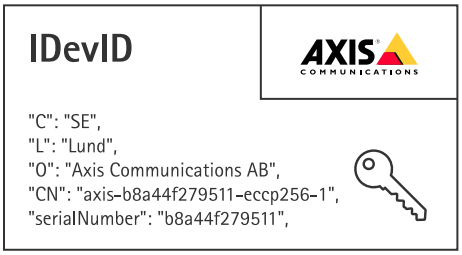

Figure 6. Beispiel einer Axis Geräte-ID

3.2 Sicheres Netzwerk-Onboarding

Wenn Sie ein Axis Gerät kaufen, können Sie es manuell überprüfen, bevor Sie es in Betrieb nehmen. Indem Sie das Gerät einer Sichtprüfung unterziehen und sich vorher mit dem Erscheinungsbild von Axis Produkten vertraut machen, können Sie sicher sein, dass das Gerät wirklich von Axis stammt. Eine solche Prüfung ist aber nur möglich, wenn Sie physischen Zugang zum Gerät haben. Wie können Sie also sicher sein, dass Sie bei der Kommunikation über ein Netzwerk mit dem richtigen Gerät kommunizieren, und wie können Sie seine Identität überprüfen? Weder Netzwerk-Geräte noch Software auf Servern können eine physische Inspektion durchführen. Als Sicherheitsmaßnahme wurde die Kommunikation mit einem neuen Gerät bisher üblicherweise zunächst über ein geschlossenes Netzwerk getestet, in dem es sicher bereitgestellt werden kann.

Die Axis Geräte-ID liefert Ihrem Netzwerk einen kryptografisch verifizierbaren Nachweis darüber, dass ein bestimmtes Gerät von Axis hergestellt wurde und dass die Netzwerkverbindung zu diesem Gerät tatsächlich von genau diesem Gerät bedient wird. Die Axis Geräte-ID kann bei der IEEE 802.1X-Netzwerkauthentifizierung eingesetzt werden, um Zugang zu einem Provisioning-Netzwerk zu erhalten, in dem weitere Software-Updates und eine Konfiguration des Axis Gerätes erfolgen, bevor dieses in das Produktionsnetzwerk verschoben wird.

Die Axis Geräte-ID kann die allgemeine Sicherheit erhöhen und die Installationsdauer der Geräte verkürzen, da mehr automatisierte und kosteneffiziente Kontrollen für die Geräteinstallation und -konfiguration eingesetzt werden können.

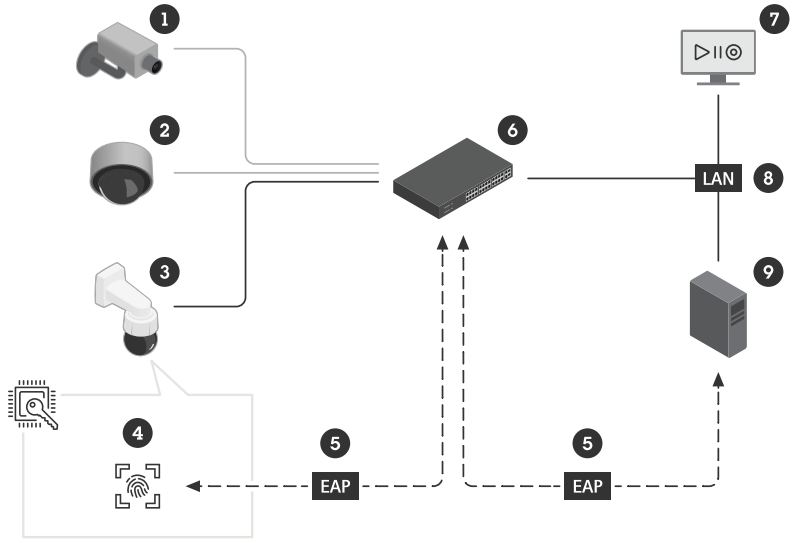

Figure 7. Sicheres Netzwerk-Onboarding. Der Authentifizierungsserver (9) kann angewiesen werden, Axis Geräte (3) im Netzwerk (8) und VMS (7) automatisch zu akzeptieren. Dies geschieht über die Seriennummern der Geräte und die Axis Geräte-ID (4) als Fingerabdruck oder Authentifizierung.

1 *Nicht autorisiertes Gerät (muss manuell eingegliedert werden)*
2 *Gerät eines anderen Herstellers*
3 *Axis Gerät*
4 *Axis Geräte-ID, sicher gespeichert im manipulationsgeschützten sicheren Schlüsselspeicher*
5 *802.1X EAP-TLS Netzwerk-Authentifizierung des Axis Geräts über ein Axis Geräte-ID-Zertifikat*
6 *Verwaltbarer Switch (Authentifizierer)*
7 *VMS (Geräteverifizierung)*
8 *LAN geschützt von 802.1X*
9 *RADIUS (Netzwerk-Authentifizierungsserver)*

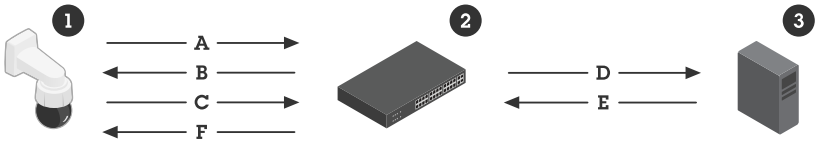

Figure 8. Ausführlichere Beschreibung des Onboarding-Verfahrens: IEEE 802.1AR legt zur sicheren Geräteidentifizierung ein Verfahren zur Identifizierung eines Gerätes (1) über Anfragen über das IEEE 802.1X EAP (EAP-TLS) unter Verwendung eines RADIUS-Servers (3) fest, um den Zugang zum Netzwerk zu gewähren.

1 *Axis Gerät*
2 *Verwaltbarer Switch (Authentifizierer)*
3 *RADIUS-Server (Netzwerk-Authentifizierungsserver)*
A *Neue Verbindung*
B *EAP-Anfrage der Identität*

C EAP-Antwort: Identität inklusive Axis Geräte-ID-Zertifikat, IEEE802.1AR IDevID
D RADIUS-Zugriffsanfrage
E RADIUS Access-Challenge
F EAP-Erfolg

Die Axis Geräte-ID ist nicht nur eine zusätzliche, integrierte Vertrauensinstanz, sondern ermöglicht auch die Nachverfolgung der Geräte und eine periodische Verifizierung und Authentifizierung nach Zero-Trust-Netzwerkprinzipien.

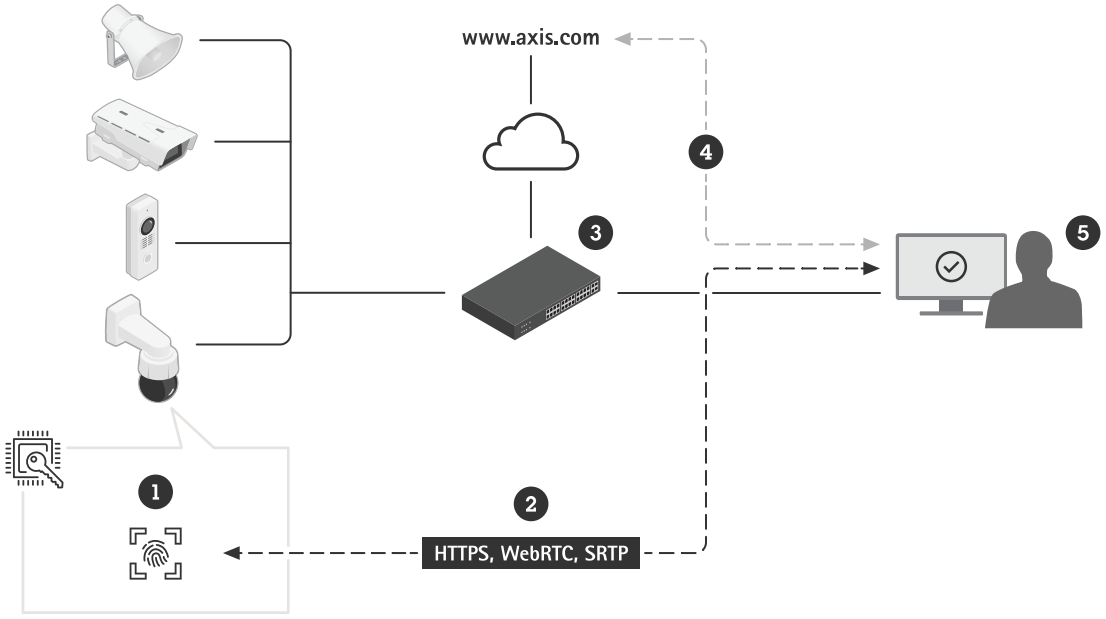

Figure 9. Ist ein Gerät einmal sicher eingegliedert, können Software-Anwendungen (5) in anderen Teilen des Systems das Gerät in verschiedenen TLS-basierten Kommunikationsszenarien (2) über die Axis Geräte-ID (1) und die kryptografischen Operationen überprüfen und authentifizieren. Die Axis Geräte-ID kann über das öffentlich verfügbare Axis Geräte-ID Root-CA-Zertifikat (4) überprüft werden.

1 Axis Geräte-ID, sicher gespeichert im manipulationsgeschützten sicheren Schlüsselspeicher
2 TLS-basierte Kommunikation (HTTPS, WebRTC, SRTP)
3 Verwaltbarer Switch
4 Axis Geräte-ID Root-CA-Zertifikat (zum Download unter www.axis.com/support/public-key-infrastructure-repository
5 VMS oder andere Software (Geräteverifizierung)

4 Sichere Speicherung der Schlüssel

Klassischerweise werden sensible kryptografische X.509-Daten (private Schlüssel) im Dateisystem eines Gerätes gespeichert. Sie werden nur durch die Zugangsrichtlinien für die Benutzerkonten gesichert. Diese bieten einen Basisschutz, weil das Benutzerkonto nicht leicht zu knacken ist. Doch im Falle eines Sicherheitsverstoßes wären diese kryptografischen Daten ungeschützt und für den Gegner einsehbar.

Aus Sicherheitsaspekten ist der sichere Schlüsselspeicher kritisch für die Speicherung und den Schutz kryptografischer Daten. Nicht nur werden die sensiblen kryptografischen Daten in der Axis Geräte-ID und

dem signierten Video im sicheren Schlüsselspeicher aufbewahrt, sondern auf die gleiche Weise können auch vom Kunden geladene Informationen geschützt werden.

4.1 Sicherer Schlüsselspeicher

Sensible kryptografische Daten (private Schlüssel) werden im Hardware-basierten, manipulationsgeschützten sicheren Schlüsselspeicher gespeichert. Das verhindert eine böswillige Extraktion sogar bei einem Sicherheitsverstoß. Außerdem bleiben die privaten Schlüssel im sicheren Schlüsselspeicher geschützt, sogar während sie verwendet werden. Eventuelle Angreifer haben keinen Zugriff auf den sicheren Schlüsselspeicher und können den Netzwerkverkehr nicht belauschen, über IEEE 802.1X-Schlüssel Zugang zum Netzwerk erhalten oder andere private Schlüssel extrahieren.

Der sichere Schlüsselspeicher wird über ein Hardware-basiertes kryptografisches Berechnungsmodul bereitgestellt. Je nach Sicherheitsanforderungen kann ein Axis Gerät über ein oder mehrere solcher Module verfügen, wie z. B. ein TPM 2.0 (Trusted Platform Module) oder ein sicheres Element, und/oder ein Trusted Execution Environment (TEE).

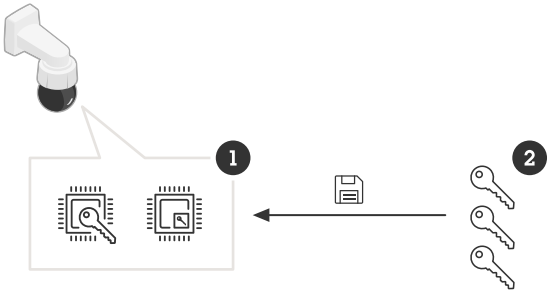

Figure 10. Die sicheren Schlüsselspeicher (1) schützen private Schlüssel (2) und sichern die Ausführung kryptografischer Operationen.

1 *Sichere Schlüsselspeicher; dies kann ein Sicherheitselement, ein TPM oder eine TEE (im SoC) sein*
2 *Private Schlüssel, wie eine Axis Geräte-ID, ein Video-Signierschlüssel, Schlüssel zur Zutrittskontrolle, Dateisystemschlüssel und vom Kunden geladene Schlüssel (z. B. IEEE 802.1X und HTTPS)*

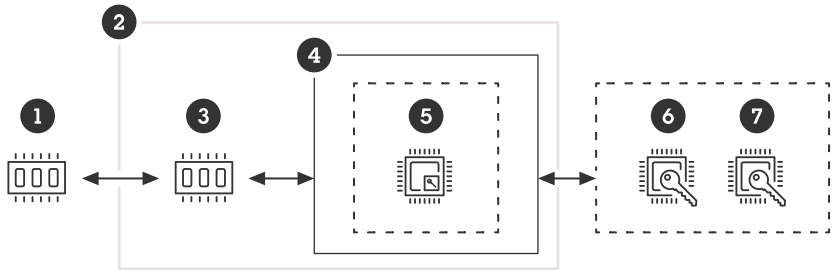

Figure 11. Geräte mit Axis Edge Vault enthalten kryptographische Hardware-Berechnungsmodule (Sicherheitselement (6) und TPM (7)), die direkt neben dem Hauptprozessor des SoC (4) auf der Leiterplatte angeordnet sind. Die TEE (5) ist ein sicherer Bereich im Hauptprozessor des SoC selbst. Das in den SoC integrierte Boot-ROM (3) führt die Verfahren für sicheres Hochfahren aus und stellt sicher, dass zum

Hochfahren des Gerätes nur signierte Betriebssystem-Software-Images aus dem Flash-Speicher (1) verwendet werden.

1 *Flash-Speicher (für signiertes Betriebssystem, lesbares/beschreibbares Dateisystem)*
2 *SoC*
3 *Boot ROM (für sicheres Hochfahren)*
4 *CPU*
5 *TEE (für sicheren Schlüsselspeicher)*
6 *Sicherheitselement (für sicheren Schlüsselspeicher)*
7 *TPM (für sicheren Schlüsselspeicher)*

TPM, Sicherheitselement und TEE bieten alle Schutz für private Schlüssel und eine sichere Ausführung kryptografischer Operationen. Bei einem Sicherheitsverstoß werden unberechtigter Zugriff und böswillige Extrahierung verhindert.

4.2 Common Criteria und FIPS 140

Kryptografische Berechnungsmodule können nach den Common Criteria Evaluation Levels (CC EAL) sowie nach den Compliance Levels (1–4) von FIPS 140 zertifiziert werden. Diese Zertifizierungen dienen dazu, die Richtigkeit und Integrität der kryptografischen Operationen festzustellen und verschiedene Manipulationsschutzmaßnahmen wie Selbstüberprüfung, Manipulationssicherheit usw. zu überprüfen. Informationen zur Zertifizierung finden Sie auf dem Datenblatt des jeweiligen Axis Geräts oder im *Axis Product Selector*. Axis verlangt für die in seine Hardware integrierten kryptografischen Berechnungsmodule eine Zertifizierung mindestens nach Common Criteria EAL4 und/oder FIPS 140-2/3 Level 2/3.

4.2.1 Common Criteria

Common Criteria (CC) (Common Criteria for Information Technology Security Evaluation) ist ein internationaler Standard (ISO/IEC 15408) für die Zertifizierung der Sicherheit von IT-Produkten. Common Criteria stellt Herstellern und Implementierern ein Framework zur Festlegung der Aspekte der Funktionalität und Vertrauenswürdigkeit als so genannte „Security Targets" bereit, die zu Schutzprofilen zusammengefasst werden können.

Die angegebenen Security Targets werden daraufhin von unabhängigen, zertifizierten Prüflaboren evaluiert, bevor sie als zertifizierte Produkte in der Common Criteria Database gelistet werden. Die Anforderungen und Tiefe der Evaluierung des Testlabors werden über eine EAL-Bewertung (Evaluation Assurance Level) angegeben, von Stufe EAL 1 – funktionell getestet, bis Stufe EAL 7 – formal verifizierter Entwurf und getestet. Common Criteria können also alles – von Betriebssystemen und Firewalls bis hin zu TPMs und Pässen – umfassen.

Weitere Informationen zu den Zertifizierungsanforderungen der Common Criteria finden Sie auf der Common Criteria-Website unter *www.commoncriteriaportal.org/*

4.2.2 FIPS 140

FIPS (Federal Information Processing Standards) 140-2 und 140-3 sind Datenschutzstandards für kryptografische Berechnungsmodule und die Verwendung kryptografischer Algorithmen, die vom NIST (National Institute of Standards and Technology) herausgegeben wurden und deren Verwendung von der US-amerikanischen und kanadischen Regierung vorgeschrieben ist. FIPS 140-3 ist die aktualisierte Version von FIPS 140-2, das es 2019 ersetzte. Die Validierung durch ein NIST-zertifiziertes Testlabor garantiert, dass das Modulsystem und die Kryptographie des Moduls ordnungsgemäß implementiert

wurden. Die Zertifizierung erfordert die Beschreibung, Spezifizierung und Verifizierung des kryptografischen Berechnungsmoduls, zugelassener Algorithmen, zugelassener Betriebsarten und Einschalttests.

So können die Kundinnen und Kunden sicher sein, dass ihre Produkte gemäß Regierungsvorgaben betrieben werden können. Dies gibt ihnen Sicherheit im Hinblick auf Audits von Regierungsbehörden. Firmen, die nicht FIPS 140-reguliert sind, können sicher sein, dass ihre Produkte den von der Regierung vorgegebenen Standards entsprechen. Weitere Details zu den Zertifizierungsanforderungen für FIPS 140-2 und FIPS 140-3 finden Sie auf der NIST-Website *www.nist.gov*

Damit ein komplettes System FIPS 140-konform ist, muss jede einzelne Komponente des Systems FIPS 140 entsprechen. Das heißt, dass das Video Management System, der Aufzeichnungsserver sowie die angeschlossenen Geräte wie z. B. Kameras konform sein müssen. Ein Gerät ist FIPS 140-konform, wenn mindestens ein Software-zertifiziertes oder Hardware-zertifiziertes Modul verwendet wird.

Axis Geräte mit AXIS OS Version 12 oder höher sind mit dem FIPS 140-zertifizierten, Software-basierten (OpenSSL) kryptografischen Modul von Axis ausgestattet. Die meisten neuen Geräte von Axis enthalten sowohl ein FIPS 140-zertifiziertes kryptografisches Hardware-Modul als auch das Software-basierte kryptografische Modul. Dies ergibt eine optimale Lösung: Das Software-zertifizierte Modul schützt Software-basierte Anwendungen wie HTTPS und IEEE 802.1X auf Betriebssystemebene, das Hardware-zertifizierte Modul stellt einen sicheren Schlüsselspeicher bereit.

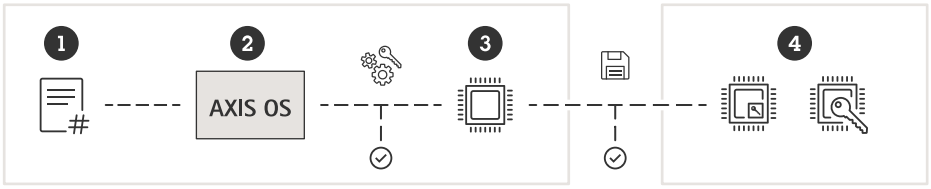

Figure 12. Verwendung der FIPS 140-konformen kryptografischen Software- und Hardware-Module in einem Axis Gerät. Anwendungen (1) werden über das in das AXIS OS (2) des Axis Gerätes integrierte kryptografische Modul von Axis gesichert. Das kryptografische Modul von Axis führt symmetrische und asymmetrische kryptografische Operationen aus, wobei es den SoC (3) und/oder die integrierten Hardware-basierten kryptografischen Rechenmodule (4) als sicheren Schlüsselspeicher verwendet.

1. *Anwendungen, die eine Verschlüsselung benötigen oder TLS-basiert sind (wie HTTPS, webRTC und 802.1X)*
2. *AXIS OS mit integriertem Software-basiertem kryptografischem Modul (NIST-Zertifikat: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4621*
3. *SoC*
4. *Eingebettete Hardware-basierte kryptografische Rechenmodule*

4.3 Schutz privater Schlüssel

Schafft es ein Angreifer, den privaten Schlüssel zu extrahieren, könnte er damit HTTPS-verschlüsselten Netzwerkverkehr belauschen oder sich als das andere Gerät ausgeben und dadurch den Zugang zu einem 802.1X-geschützten Netzwerk erschleichen.

Axis Geräte unterstützen verschiedene TLS-basierte (TLS=Transport Layer Security) Protokolle zur sicheren Kommunikation. Axis Geräte-ID (IEEE 802.1AR), HTTPS (Netzwerk-Verschlüsselung) und 802.1X (Netzwerkzugangskontrolle) basieren auf kryptografischem X.509-Datenschutz.

Die digitalen TLS-Zertifikate nach X.509 ermöglichen die Kommunikation zwischen zwei Hosts im Netzwerk über ein Zertifikat und ein zugehöriges öffentliches und privates Schlüsselpaar. Der private Schlüssel

verbleibt dauerhaft im sicheren Schlüsselspeicher, sogar während es zur Entschlüsselung von Daten eingesetzt wird. Das jeweilige Zertifikat und der öffentliche Schlüssel sind bekannt, können vom Axis Gerät geteilt werden und dienen zum Verschlüsseln der Daten.

4.4 Schutz der Schlüssel für die Zutrittskontrolle

Ein weiteres Beispiel dafür, warum ein durch die Hardware geschützter Schlüsselspeicher so wichtig ist, ist der Schutz der kryptografischen Daten, die von den Axis Lösungen zur Zutrittskontrolle, beispielsweise Open Supervised Device Protocol (OSDP) Secure Channel, verwendet werden.

OSDP Secure Channel ist ein weit verbreitetes AES-128-basiertes Verschlüsselungs- und Authentifizierungssystem zum Schutz der Kommunikation zwischen Tür-Steuerungen und Peripheriegeräten wie Kartenlesern.

Der gemeinsame symmetrische AES-Schlüssel, Secure Channel Base Key (SCBK), von Tür-Steuerung und Lesegerät initiiert die gegenseitige Authentifizierung und erzeugt in der Folge einen Satz von Sitzungsschlüsseln zur Verschlüsselung der Kommunikationsdaten zwischen den Tür-Steuerungen und Lesegeräten.

Für echte End-to-End-Sicherheit müssen der Master Key (MK) und der SCBK unzugänglich im sicheren Schlüsselspeicher des Axis Netzwerk-Tür-Controllers gespeichert sein. Der Master Key leitet einen eindeutigen SCBK-Schlüssel über den angeschlossenen Axis Kartenleser ab. Ebenso muss auch der individuelle SCBK, der während der Installation sicher an ein Axis Lesegerät übermittelt wurde, im sicheren Schlüsselspeicher des Lesegeräts gespeichert werden. Das Lesegerät ist besonders kritisch, da es normalerweise auf der unsicheren Seite der Tür installiert ist.

Auf diese Weise sind die OSDP Secure Channel-Schlüssel an beiden Enden in einer Hardware-geschützten Umgebung sicher aufbewahrt. Das verhindert eine böswillige Extraktion sogar bei einem Sicherheitsverstoß.

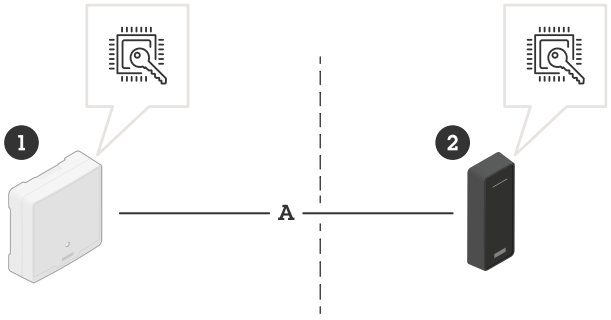

Figure 13. End-to-End-Sicherheit mit einem sicheren Schlüsselspeicher bei der Zutrittskontrolle. Der Master Key und der individuelle Secure Channel Base Key (SCBK) werden beide in sicheren Schlüsselspeichern in Geräten auf beiden Seiten der Tür aufbewahrt.

1 Axis Tür-Steuerung, installiert auf der sicheren Seite der Tür
2 Axis Kartenleser, installiert auf der unsicheren Seite der Tür
A OSDP Secure Channel Kommunikation

4.5 Schutz der Dateisystemschlüssel

Während der Verwendung enthält ein Axis Gerät eine kundenspezifische Konfiguration und Daten. Das gilt auch, während das Axis Gerät von einem Händler oder Systemintegrator, der es vorkonfiguriert hat,

zum Kunden transportiert wird. Ein Angreifer könnte physischen Zugang zum Axis Gerät erzwingen und versuchen, durch Ausbau des Flash-Speichers und Ablesen mit einem Flash-Reader Informationen aus dem Dateisystem zu extrahieren. Daher ist der Schutz des lesbaren und beschreibbaren Dateisystems vor der Extraktion sensibler Daten oder unbefugten Änderungen der Konfiguration des Axis Geräts eine wichtige Schutzmaßnahme für den Fall eines Diebstahls oder Einbruchs.

Der sichere Schlüsselspeicher verhindert das böswillige Herausschleusen von Informationen und Veränderungen der Konfiguration, indem es eine starke Verschlüsselung des Dateisystems erzwingt. Beim Ausschalten des Axis Geräts werden die Informationen im Dateisystem verschlüsselt. Beim Hochfahren wird das lesbare/beschreibbare Dateisystem mit einem AES-XTS-Plain64 256-Bit-Schlüssel verschlüsselt, so dass es angeschlossen und vom Axis Gerät genutzt werden kann. Der Codierschlüssel für das Dateisystem wird ab Werk gerätespezifisch in die Werkseinstellungen integriert und bei jedem folgenden Software-Update neu generiert. Der Schlüssel ändert sich also zwangsläufig während der Nutzungsdauer des Gerätes.

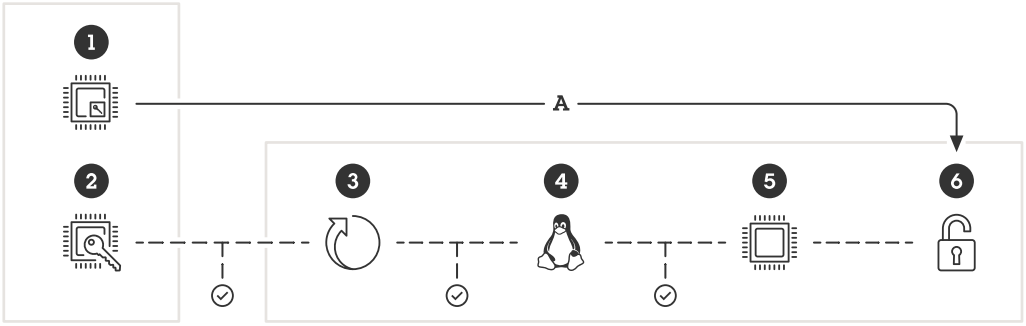

Figure 14. TEE (1) und Boot-ROM (2) sind in den SoC integriert. Beim Booten wird das lesbare/beschreibbare Dateisystem (6) (von der TEE) verschlüsselt, so dass das Dateisystem angeschlossen und vom Axis Gerät genutzt werden kann. Während des Bootens wird jeder Teil der Kette – Bootloader (3), Linux-Kernel (4) und Root-Dateisystem (5) – verifiziert und authentifiziert das jeweils nächste Sub-System im Flash-Speicher. Das ergibt am Ende ein verifiziertes Root-Dateisystem.

1 TEE
2 Boot-ROM
3 Bootloader
4 Linux-Kernel
5 Root-Dateisystem
6 Lesbares/beschreibbares Dateisystem
A Die TEE entschlüsselt das lesbare/beschreibbare Dateisystem.

5 Videomanipulationsschutz

Eine Grundannahme in der Überwachungsbranche ist, dass Videos von Überwachungskameras authentisch und vertrauenswürdig sind. Die Funktion Signiertes Video wurde entwickelt, um die Vertrauenswürdigkeit von Videos als Beweismaterial zusätzlich zu stärken. Indem sie die Echtheit eines Videos verifiziert, kann diese Funktion sicherstellen, dass es nicht etwa nach der Übertragung von der Kamera bearbeitet oder modifiziert wurde.

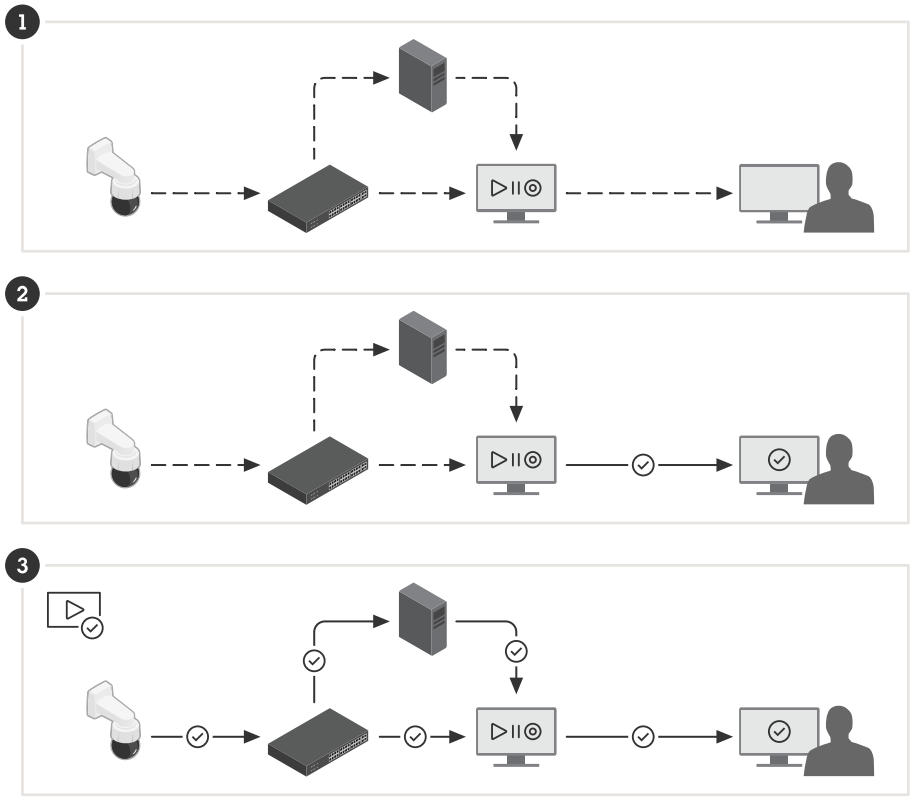

Figure 15. Verifizierung der Echtheit des Videos

1. *Ein Video durchläuft auf seinem Weg von der Kamera bis zum Betrachter der Aufzeichnung viele Stationen. Ein geschickter Angreifer kann das Video an jeder dieser Stationen verfälschen.*
2. *Beim Export zum Video hinzugefügte VMS-Wasserzeichen verifizieren einige Schritte, garantieren aber nicht, dass das Video nicht bereits davor manipuliert wurde.*
3. *Signiertes Video ist eine Möglichkeit, um sicherzustellen, dass das Video in keinem Schritt von der Kamera bis zur Person, die die exportierte Aufzeichnung betrachtet, manipuliert wurde. Das Video kann bis zum Gerät zurückverfolgt werden, mit dem es aufgenommen wurde.*

5.1 Signiertes Video

Die von Axis entwickelte Funktion „Signiertes Video“, die proaktiv als Open-Source-Software entwickelt wurde, stellt über eine Signatur im Videostream die Unversehrtheit des Videos sicher und verfolgt seinen Ursprung bis zur Kamera zurück, aus der es stammt. So kann die Echtheit des Videos nachgewiesen werden, ohne die gesamte Produktkette der Videodatei überprüfen zu müssen.

Nachdem ein Videosicherheitssystem einen Vorfall aufgezeichnet hat, kann das Video als Videodatei auf einen USB-Stick exportiert, an die Polizei weitergeleitet und in einem EMS (Beweismittel-Verwaltungssystem) gespeichert werden. Beim Export des Videos aus der Kamera sieht der Beamte, dass das Video ordnungsgemäß signiert wurde. Wird es später in einem Prozess verwendet, kann das Gericht kontrollieren und überprüfen, wann das Video aufgezeichnet wurde, von welcher Kamera und

ob Videoframes verändert oder gelöscht wurden. Mit dem *File Player* von Axis kann jeder mit einer Kopie des Videos diese Informationen sehen.

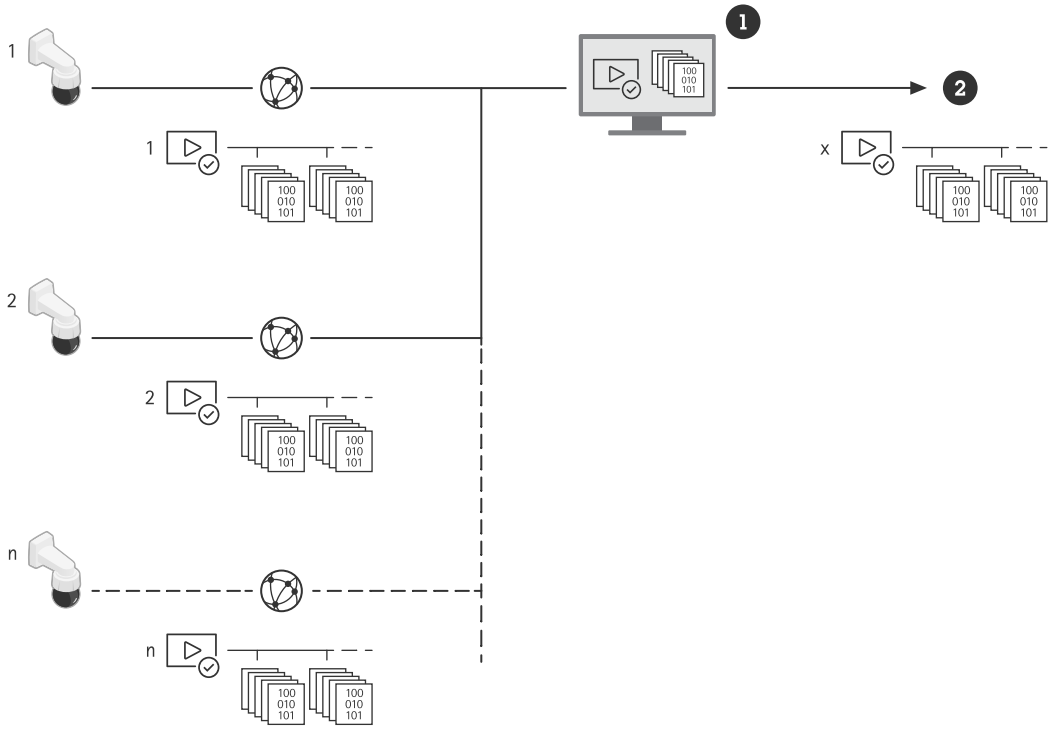

Figure 16. Die Signatur wird bereits in der Kamera eingefügt, so dass der Inhalt in jedem Schritt von der Quelle bis zur Verwendung des Videos überprüft werden kann.

1 VMS
2 Export der Videos auf CD/USB/Web/E-Mail

Jede Kamera hat ihren eigenen, eindeutigen Videosignierschlüssel, der im sicheren Schlüsselspeicher aufbewahrt wird und eine Signatur zum Videostream hinzufügt. Hierfür wird ein Hashwert für jeden

Videoframe einschließlich der Metadaten berechnet, und der kombinierte Hashwert wird signiert. Die Signatur wird daraufhin in speziellen Metadatenfeldern (dem SEI-Header) im Stream gespeichert.

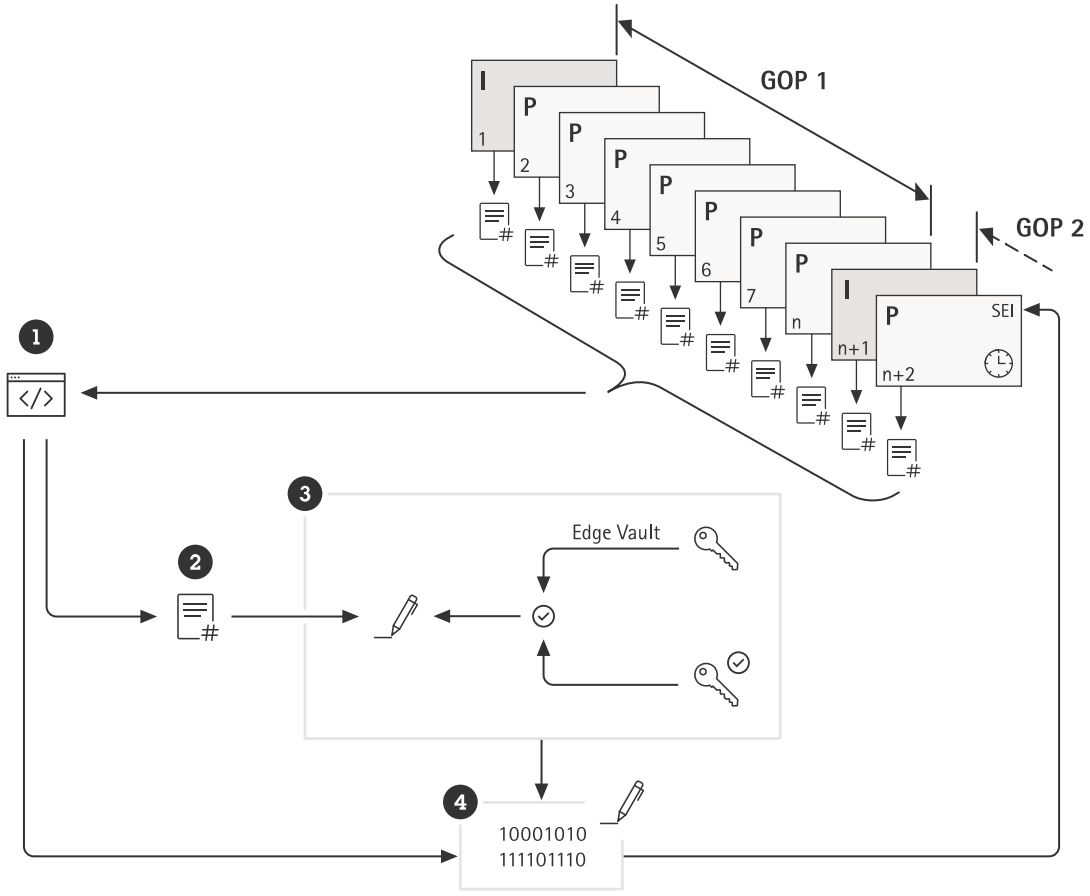

Figure 17. Eine grafische Darstellung, wie eine Signatur zum Videostream hinzugefügt wird. Der Inhalt jedes Frames einer Bildergruppe (Group of Pictures, GOP) wird zusammen mit einem Hashwert der Kamera-Metadaten abgebildet (1). Das ergibt den GOP-Hashwert (2), der in Edge Vault (3) mit dem gerätespezifischen Videosignierschlüssel und Bestätigungsschlüssel signiert wird. Die digitale Signatur (4) und die Metadaten (1) werden danach zu einem SEI-Header hinzugefügt, der zusammen mit dem Stream übertragen wird.

1 *Gerätespezifische Metadaten (Hardware-ID, AXIS OS-Version, Seriennummer und Bestätigungsbericht*) und Stream-Metadaten (GOP-Zähler und Frame-Hashwerte)*
2 *GOP-Hashwert*
3 *Axis Edge Vault*
4 *Digitale Signatur*

* *Anhand des Bestätigungsberichts lassen sich der Ursprung und die Herkunft des für die Signatur verwendeten Schlüsselpaares feststellen. Durch Überprüfung der Schlüsselbestätigung kann man sicherstellen, dass der Schlüssel sicher in der Hardware eines bestimmten Gerätes gespeichert ist. Dadurch wird der Ursprung des Videos geschützt.*

Die eigentliche Signierung erfolgt anhand eines für jedes Gerät eindeutigen Videosignierschlüssels, der mit einem gerätespezifischen Bestätigungsschlüssel bestätigt wird. Der Bestätigungsbericht wird zu Beginn und dann in periodischen Abständen, meist einmal pro Stunde, an den Stream angehängt. Da die Metadaten den Hashwert für jeden einzelnen Frame enthalten, kann man die Richtigkeit jedes einzelnen

Frames feststellen. Zur Fertigstellung der Signatur muss die Struktur der Group of Pictures (GOP) im Video geschützt werden. Dies geschieht, indem man den Hashwert des ersten I-Frame der nächsten Bildergruppe in die Signatur einfügt. So werden unentdeckte Schnitte oder Umstellungen der Frames verhindert. Im unwahrscheinlichen Fall, dass Frames beim Streamen verloren gehen oder im Speicher beschädigt werden, kann dies auf die gleiche Weise markiert werden.

6 Glossar

Axis Geräte-ID: Für das Gerät eindeutiges Zertifikat mit zugehörigen Schlüsseln zum Nachweis der Echtheit eines Axis Geräts. Das Axis Gerät ist ab Werk mit einer Axis Geräte-ID versehen, die im sicheren Schlüsselspeicher gespeichert ist. Die Axis Geräte-ID basiert auf dem internationalen Standard IEEE 802.1AR (IDevID, Initial Device Identifier), der ein Verfahren zur automatisierten, sicheren Identifizierung festlegt.

Axis Edge Vault: eine Hardware-basierte Cybersicherheitsplattform, die das Axis Gerät schützt. Es sorgt für eine starke Grundlage kryptografischer Berechnungsmodule (Sicherheitselement und TPM) und SoC-Sicherheit (TEE und Secure Boot), die wir mit Expertise in Edge-Gerätesicherheit kombinieren.

Zertifikat: ein signiertes Dokument, das den Ursprung und die Eigenschaften eines öffentlichen/privaten Schlüsselpaares bestätigt. Das Zertifikat wird von einer Zertifizierungsstelle (Certificate Authority, CA) signiert, und wenn das System der CA vertraut, vertraut es auch den von ihr ausgestellten Zertifikaten.

Zertifizierungsstelle (Certificate Authority, CA): der Vertrauensanker für eine Zertifikatskette. Wird verwendet, um die Echtheit und Richtigkeit der zugrunde liegenden Zertifikate nachzuweisen.

Common Criteria (CC): ein internationaler Standard für die Sicherheitszertifizierung von IT-Produkten. Wird auch als „Common Criteria for Information Technology Security Evaluation", ISO/IEC 15408, bezeichnet.

FIPS 140: eine Reihe von US-Computersicherheitsstandards zur Genehmigung kryptografischer Berechnungsmodule. FIPS (Federal Information Processing Standard) 140 legt die Anforderungen für Aufbau und Implementierung kryptografischer Module fest, um die Gefahr einer Manipulation der Module auszuräumen.

Unveränderbarer ROM (schreibgeschützter Speicher): der schreibgeschützte Speicher, in dem die vertrauenswürdigen öffentlichen Schlüssel und das Vergleichsprogramm für die Signaturen gespeichert ist, damit diese nicht überschrieben werden können.

Bereitstellung: Vorbereitung und Ausstattung eines Geräts für das Netzwerk. Dazu gehört auch die Bereitstellung von Konfigurationsdaten und Richtlinieneinstellungen für das Gerät von einem zentralen Punkt aus. Das Gerät wird mit Schlüsseln und Zertifikaten geliefert.

Kryptographie mit öffentlichem Schlüssel: ein asymmetrisches Kryptographiesystem, bei dem jede Person eine Nachricht mit dem *öffentlichen Schlüssel* des Empfängers verschlüsseln, aber nur der Empfänger (mithilfe des *privaten Schlüssels*) die Nachricht entschlüsseln kann. Kann sowohl zum Verschlüsseln als auch zum Signieren von Nachrichten verwendet werden.

Secure Boot (sicheres Hochfahren): eine Funktion, die das Laden unberechtigter Software beim Hochfahren des Gerätes verhindert. Secure Boot nutzt ein signiertes Betriebssystem, das dafür sorgt, dass das Gerät nur mit autorisierter Axis Software hochgefahren werden kann.

Sicherheitselement: ein kryptografisches Berechnungsmodul, das einen Hardware-basierten, manipulationsgeschützten Speicher für private Schlüssel und die sichere Ausführung kryptografischer Operationen bereitstellt. Im Gegensatz zum TPM sind die Hardware- und Softwareschnittstellen von Sicherheitselementen nicht standardisiert, sondern herstellerspezifisch.

Sicherer Schlüsselspeicher: eine manipulationsgeschützte Umgebung für den Schutz privater Schlüssel und die sichere Ausführung kryptografischer Operationen. Verhindert unbefugte Zugriffe und böswillige Extraktion im Falle eines Sicherheitsverstoßes. Je nach Sicherheitsbedarf kann ein Axis Gerät einen oder mehrere kryptografische Berechnungsmodule haben, die einen durch die Hardware geschützten sicheren Schlüsselspeicher bereitstellen.

Signed OS oder signiertes Betriebssystem: Geräte-Software, deren Datei-Image von einer vertrauenswürdigen Instanz mit einer digitalen Code-Signatur versehen wurde. Signed OS ist eine Voraussetzung für sicheres Hochfahren. Es stellt sicher, dass das Gerät nur von einem vertrauenswürdigen Software-Image hochgefahren wird. Bei Produkten mit AXIS OS überprüft das Gerät die Integrität und Echtheit des Gerätesoftware-Image, bevor es ein Update ausführt.

Signiertes Video: eine Funktion, die das Vertrauen in Video als Beweismaterial bewahrt und stärkt. Signiertes Video ermöglicht eine Erkennung von Videomanipulationen und bestätigt die Echtheit des Videos. Es dient zum Nachweis, dass das Video intakt und einer bestimmten Axis Kamera zuzuordnen ist. Die Signierschlüssel für signiertes Video sind im sicheren Schlüsselspeicher des Axis Geräts gespeichert.

Transport Layer Security (TLS): ein Internetstandard zum Schutz des Netzwerkverkehrs. TLS sorgt für das S (für „secure", sicher) in HTTPS.

Trusted Execution Environment (TEE): stellt Hardware-basierten, manipulationsgeschützten Speicher oder private Schlüssel bereit und sorgt für die sichere Ausführung kryptografischer Operationen. Im Gegensatz zu Sicherheitselementen und einem TPM ist die TEE ein sicherer, in der Hardware isolierter Bereich des Hauptprozessors des System-on-Chip (SoC).

Trusted Platform Module (TPM): ein kryptografisches Berechnungsmodul, das einen Hardware-basierten, manipulationsgeschützten Speicher für private Schlüssel und die sichere Ausführung kryptografischer Operationen bereitstellt. TPMs sind international standardisierte (TPM 1.2, TPM 2.0) Computerkomponenten, die von der *Trusted Computing Group (TCG)* festgelegt werden.

Zero-Trust-Sicherheit: eine moderne Strategie bei der IT-Sicherheit, bei der die angebundenen Geräte und die IT-Infrastruktur (Netzwerke, Computer, Server, Cloud-Services, Anwendungen usw.) sich wiederholt gegenseitig identifizieren, validieren und authentifizieren müssen, um zuverlässige Sicherheitskontrollen zu erreichen.

T10190380/DE/M3.5/2404

Über Axis Communications

Axis ermöglicht eine intelligente und sichere Welt durch Lösungen zur Verbesserung der Sicherheit und Geschäftsperformance. Als Unternehmen für Netzwerktechnologie und Branchenführer bietet Axis Lösungen in den Bereichen Videosicherheit, Zutrittskontrolle sowie Intercoms und Audiosysteme. Sie werden verstärkt durch intelligente Analyseanwendungen und unterstützt durch gute Schulungen.

Axis beschäftigt rund 4.000 engagierte Mitarbeiter in über 50 Ländern und arbeitet weltweit mit Technologie- und Systemintegrationspartnern zusammen, um den Kunden Lösungen anbieten zu können. Axis wurde 1984 gegründet und der Hauptsitz befindet sich in Lund, Schweden