WHITEPAPER

Axis Edge Vault

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

– Vertrauenswürdige Geräteidentität

– Sichere Speicherung der Schlüssel

– Videomanipulationserkennung

– Schutz der Lieferkette

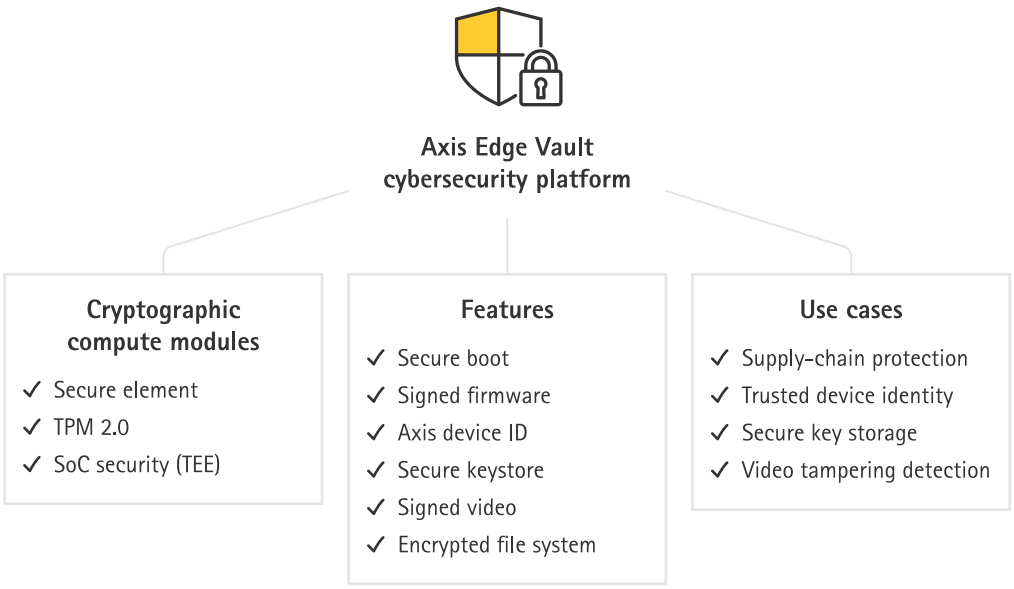
April 2023

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 *signierter Firmware* entsteht. Diese Merkmale ermöglichen eine lückenlose Kette kryptografisch validierter Software für die Vertrauenskette, auf der sämtliche sicheren Operationen beruhen.

Axis Geräte mit Axis Edge Vault minimieren die Exposition der Kunden gegenüber Cybersicherheitsrisiken, indem sie Lauschangriffe und die böswillige Extraktion sensibler Informationen verhindern. Axis Edge Vault macht Axis Geräte außerdem zu vertrauenswürdigen, zuverlässigen Geräten im Kundennetzwerk.



- **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 vom 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. Beim Abspielen des Videos zeigt der Datei-Player 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.

- **Schutz der Lieferkette:** Axis Edge Vault benötigt eine sichere Grundlage als Vertrauensanker. Ohne die Hilfe von Secure Boot und signierter Firmware kann die Vertrauensanker-Kette nicht entstehen. Secure Boot stellt zusammen mit signierter Firmware eine lückenlose Kette kryptografisch validierter Software bereit, beginnend im unveränderbaren Speicher (Boot-ROM). Secure Boot sorgt dafür, dass ein Gerät nur mit von Axis signierter Firmware gestartet werden kann. Das verhindert Manipulationen an der physischen Lieferkette. Mit signierter Firmware kann das Gerät außerdem neue Software validieren, bevor es zulässt, dass sie installiert wird. Erkennt das Gerät, dass die Firmware-Integrität verletzt wurde oder die Firmware nicht von Axis signiert wurde, wird das Firmware-Upgrade zurückgewiesen. Das schützt Geräte vor Firmware-Manipulation.

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 signierte Firmware 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 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 Netzwerkgerät kann seine Integrität und Echtheit auf ähnliche Weise nachweisen, wie man seine Identität Behörden gegenüber durch Vorzeigen seines Reisepasses am Flughafen nachweist.

2.1 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 Firmware-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.

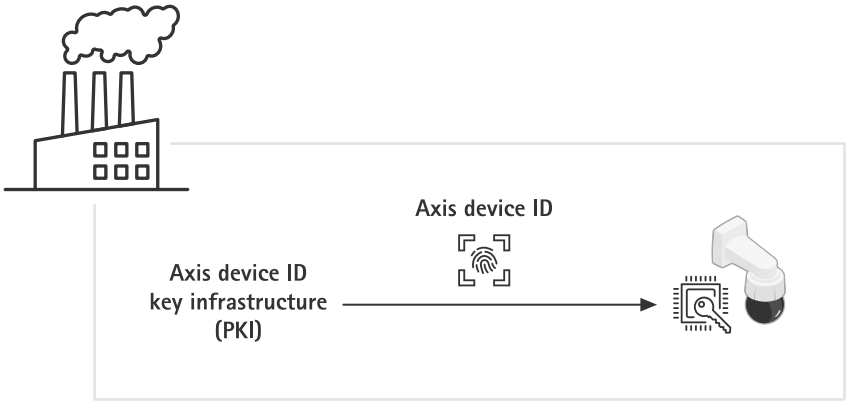


Figure 1. Während der Herstellung eines Geräts wird die eindeutige Axis Geräte-ID in seinem sicheren Schlüsselspeicher gespeichert.

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*

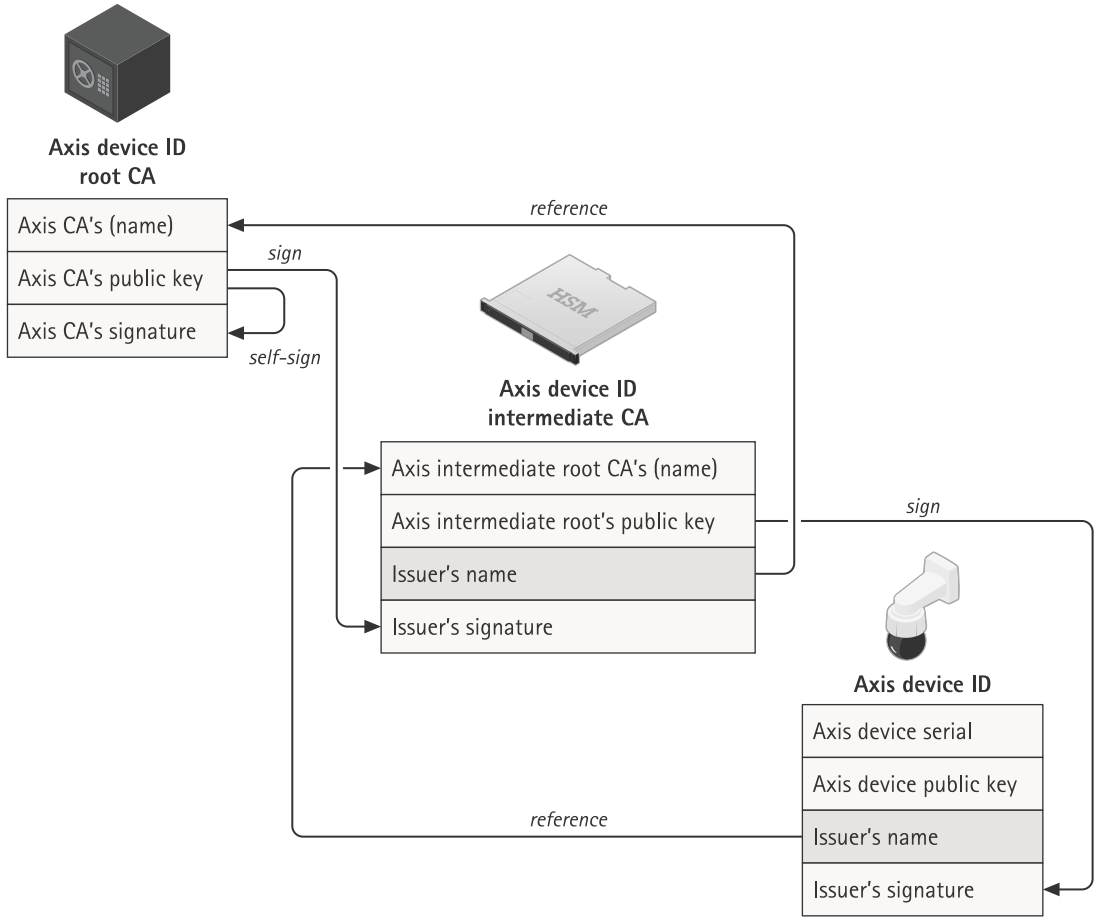


Figure 2. Axis IEEE 802.1AR Public-Key Infrastructure (PKI) für die Bereitstellung der Axis Geräte-ID ab Werk der Herstellung. Die Axis Geräte-ID (ein Zertifikat mit der Seriennummer des Produkts) wird von einer Zwischen-CA zertifiziert, die wiederum von der Axis Geräte-ID Root-CA signiert wurde. Da die Axis Root-CA sehr wertvoll ist und in einem Safe aufbewahrt werden muss, wird die Zwischen-CA bei der Bereitstellung im Werk benötigt.

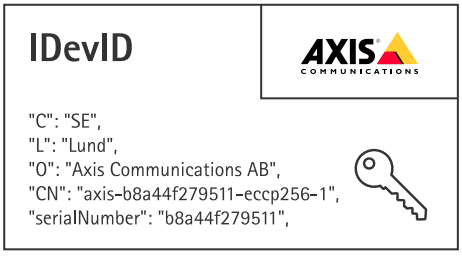


Figure 3. Beispiel einer Axis Geräte-ID

2.2 Sicheres Netzwerk-Onboarding

Wenn Sie ein Axis Gerät kaufen, können Sie es vor der Nutzung manuell überprüfen. 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 dazu verwendet werden, um Zugang zu einem Provisioning-Netzwerk zu erhalten, in dem weitere Firmware-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.

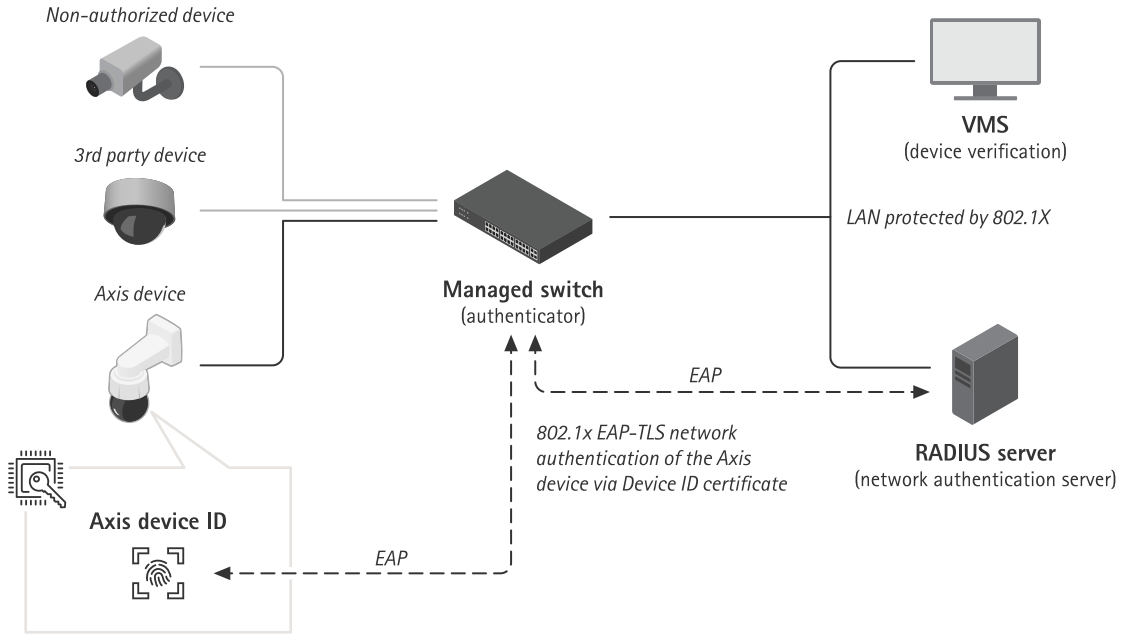


Figure 4. Sicheres Netzwerk-Onboarding. Sie können Ihren Authentifizierungsserver anweisen, Axis Geräte unter Verwendung der Seriennummern der Geräte und der Axis Geräte-ID automatisch im Netzwerk zu akzeptieren. Die Axis Geräte-ID dient als Fingerabdruck, der das sichere und automatische Onboarding der Geräte sicherstellt. Nicht autorisierte Geräte müssen manuell eingegliedert werden.

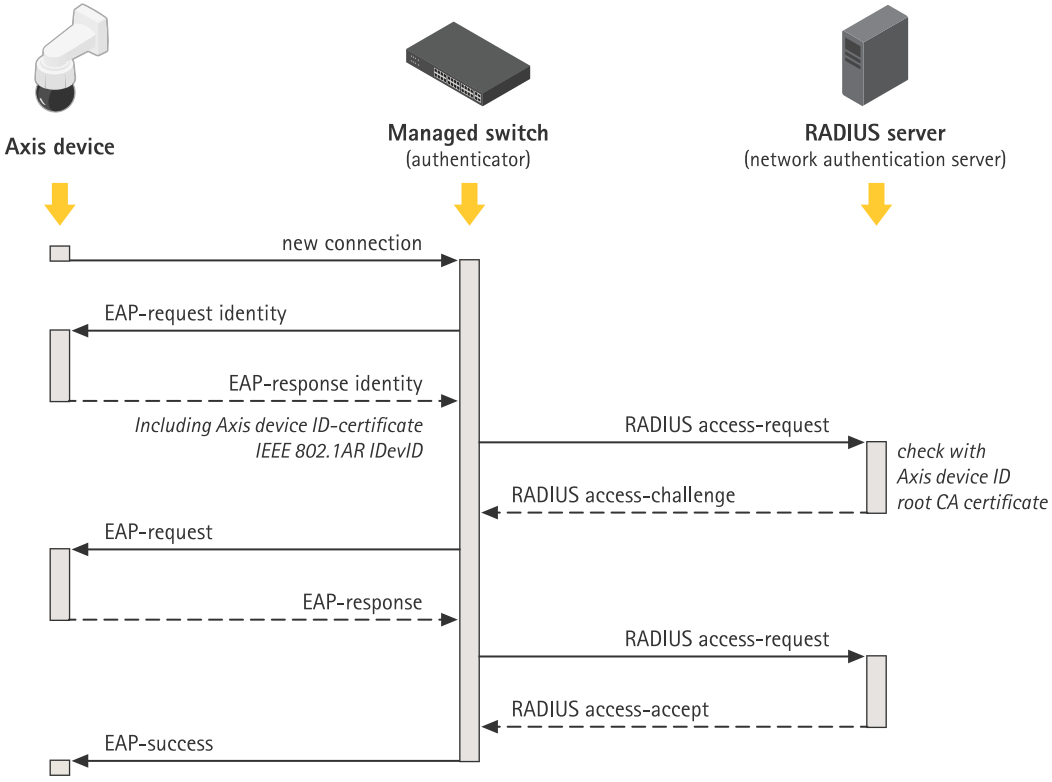


Figure 5. Ausführlichere Beschreibung des Onboarding-Verfahrens. IEEE 802.1AR legt zur sicheren Geräteidentifizierung ein Verfahren für die Identifizierung eines Gerätes über Anfragen über das IEEE 802.1X Extensible Authentication Protocol (EAP-TLS) unter Verwendung eines Remote Authentication Dial-In User Service (RADIUS) Server fest, um den Zugang zum Netzwerk zu gewähren.

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.

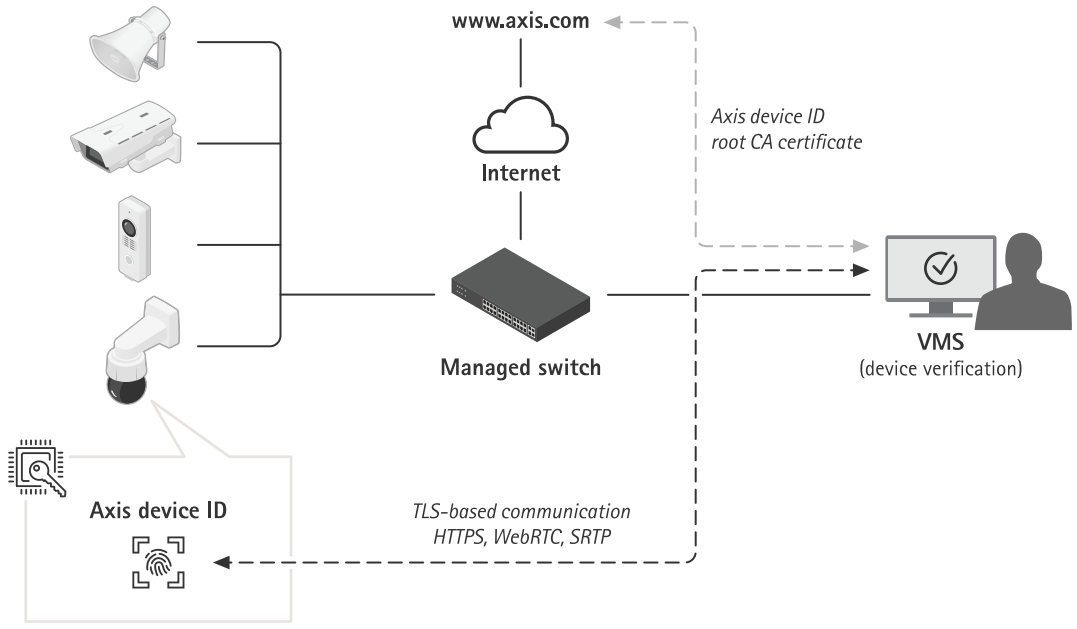


Figure 6. Ist ein Gerät einmal sicher eingegliedert, können Software-Anwendungen in anderen Teilen des Systems das Gerät in verschiedenen TLS-basierten Kommunikationsszenarien über die Axis Geräte-ID und die kryptografischen Operationen überprüfen. Die Axis Geräte-ID kann über das öffentlich verfügbare, von axis.com herunterladbare Axis Geräte-ID Root CA-Zertifikat verifiziert werden.

3 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.

3.1 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. Ein Axis Gerät kann je nach Sicherheitsanforderungen eines oder mehrere dieser Module enthalten, wie ein TPM 2.0 (Trusted Platform Module), ein Sicherheitselement (Secure Element, SE) und/oder eine TEE (Trusted Execution Environment).

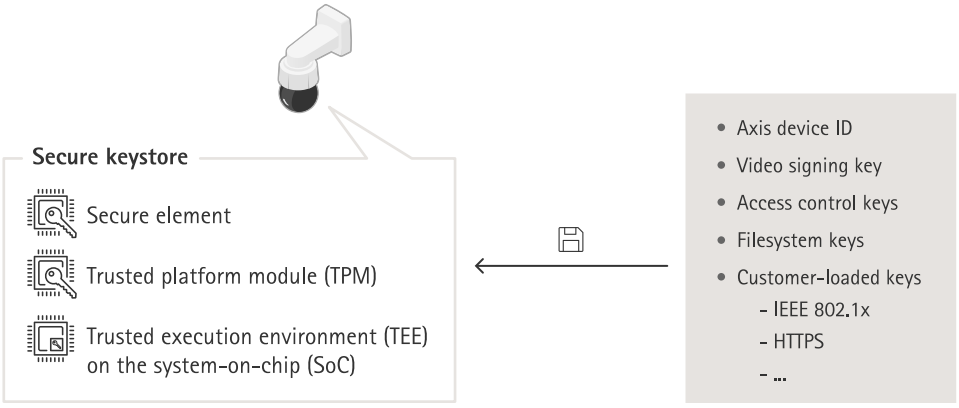


Figure 7. Die sichere Schlüsselspeicherfunktion in Axis Geräten kann ein Sicherheitselement, ein TPM oder eine TEE nutzen. Sie alle schützen private Schlüssel und sorgen für eine sichere Ausführung kryptografischer Operationen.

TPMs und Sicherheitselemente sind kryptografische Hardwaremodule im Computerbereich, die auf der Hauptplatine direkt neben dem Hauptprozessor des SoC angeordnet sind. Die TEE ist ein sicherer Bereich im Hauptprozessor des SoC selbst.

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.

3.2 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 eines 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.

3.2.1 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/*

3.2.2 FIPS 140

FIPS (Federal Information Processing Standard) 140-2 und 140-3 sind Datensicherheitsstandards für kryptografische Berechnungsmodule, die in den USA vom NIST (National Institute of Standards and Technology) ausgegeben werden. FIPS 140-3 ersetzte 2019 FIPS 140-2 und ist dessen aktualisierte Version. 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.

Weitere Details zu den Zertifizierungsanforderungen für FIPS 140-2 und FIPS 140-3 finden Sie auf der NIST-Website *www.nist.gov*.

3.3 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. Diese schützen die kryptografischen Daten nach X.509-Standard, unter anderem mit der Axis Geräte-ID (IEEE 802.1AR), HTTPS (Netzwerkverschlüsselung), 802.1X (Netzwerkzugangskontrolle).

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.

3.4 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.

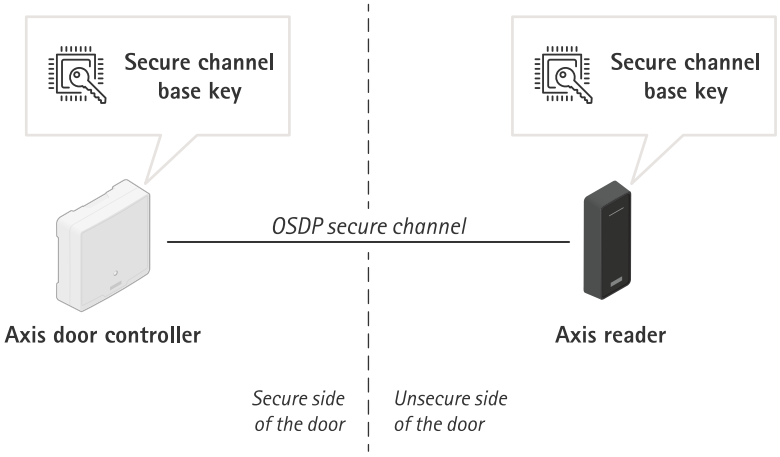


Figure 8. End-to-End-Sicherheit mit einem sicheren Schlüsselspeicher bei der Zutrittskontrolle. Der Master Key und der individuelle Secure Channel Base Key (SCBK) werden beide in sicheren Schlüsselspeichern in Geräten auf beiden Seiten der Tür aufbewahrt.

3.5 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 Firmware-Update neu generiert. Der Schlüssel ändert sich also zwangsläufig während der Nutzungsdauer des Gerätes.

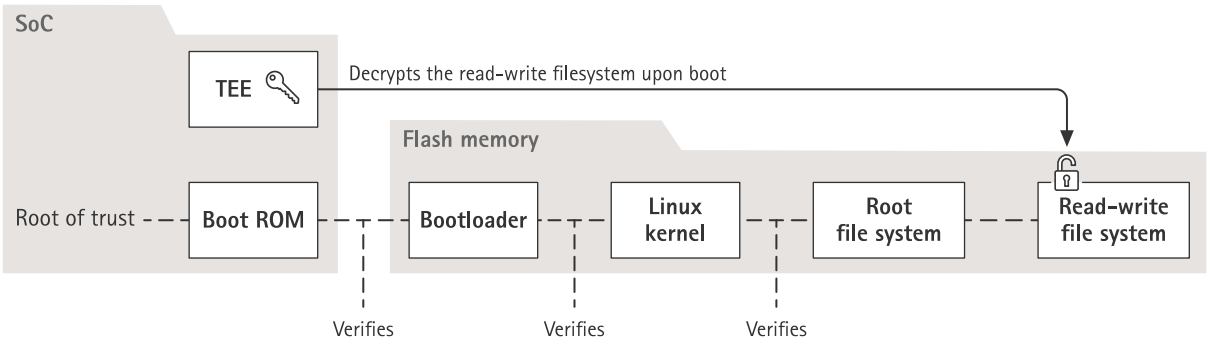


Figure 9. Die TEE im SoC enthält den Schlüssel für die Entschlüsselung des Dateisystems.

4 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.

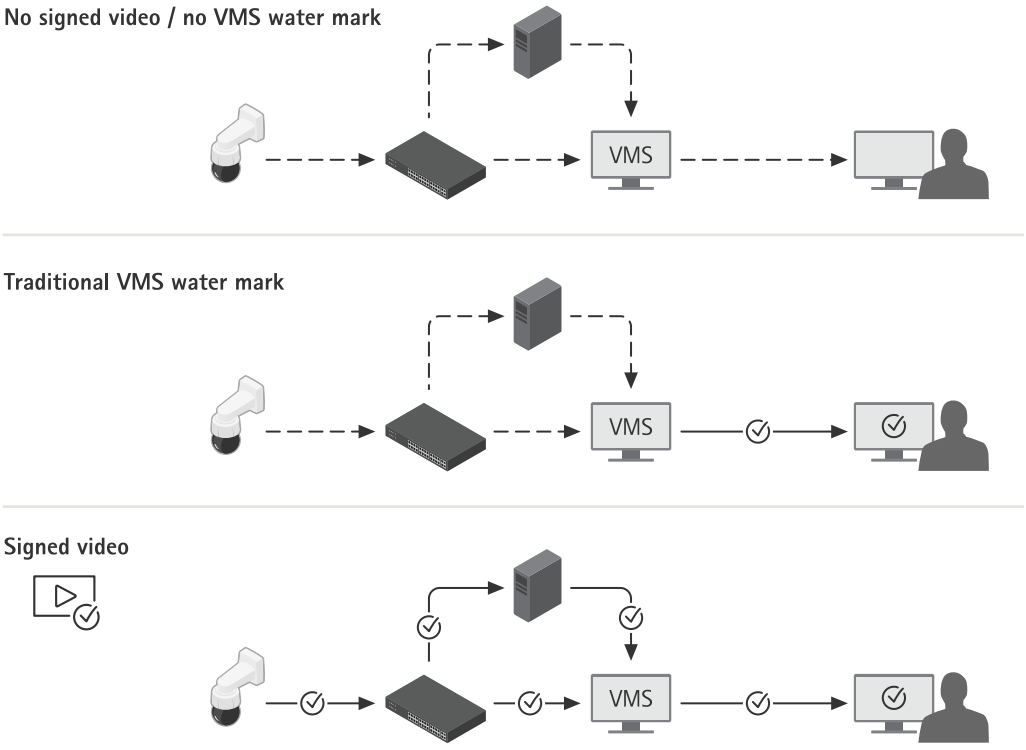


Figure 10. Verifizierung der Echtheit des Videos

Oben: 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.

Mitte: Beim Export zum Video hinzugefügte VMS-Wasserzeichen verifizieren einige Schritte, garantieren aber nicht, dass das Video nicht bereits davor manipuliert wurde.

Unten: Signiertes Video garantiert, dass das Video in keinem Schritt von der Kamera bis zum Betrachter der exportierten Aufzeichnung manipuliert wurde. Das Video kann bis zum Gerät zurückverfolgt werden, mit dem es aufgenommen wurde.

4.1 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.

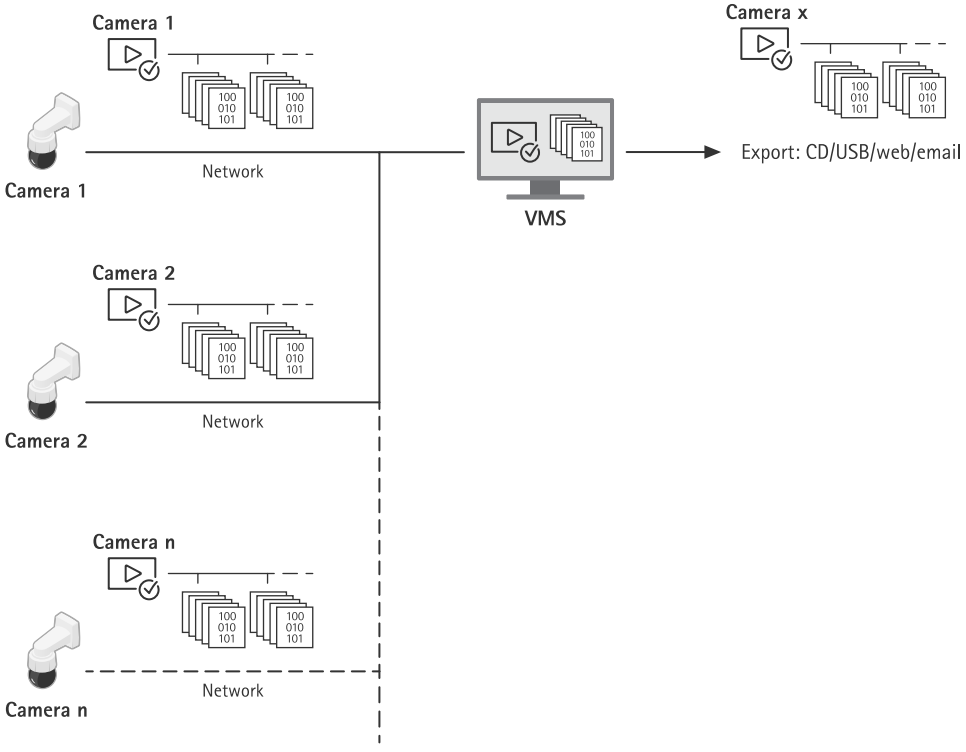


Figure 11. Die Signatur wird bereits in der Kamera eingefügt, so dass der Inhalt in jedem Schritt von der Quelle bis zur Verwendung des Videos überprüft werden kann.

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.

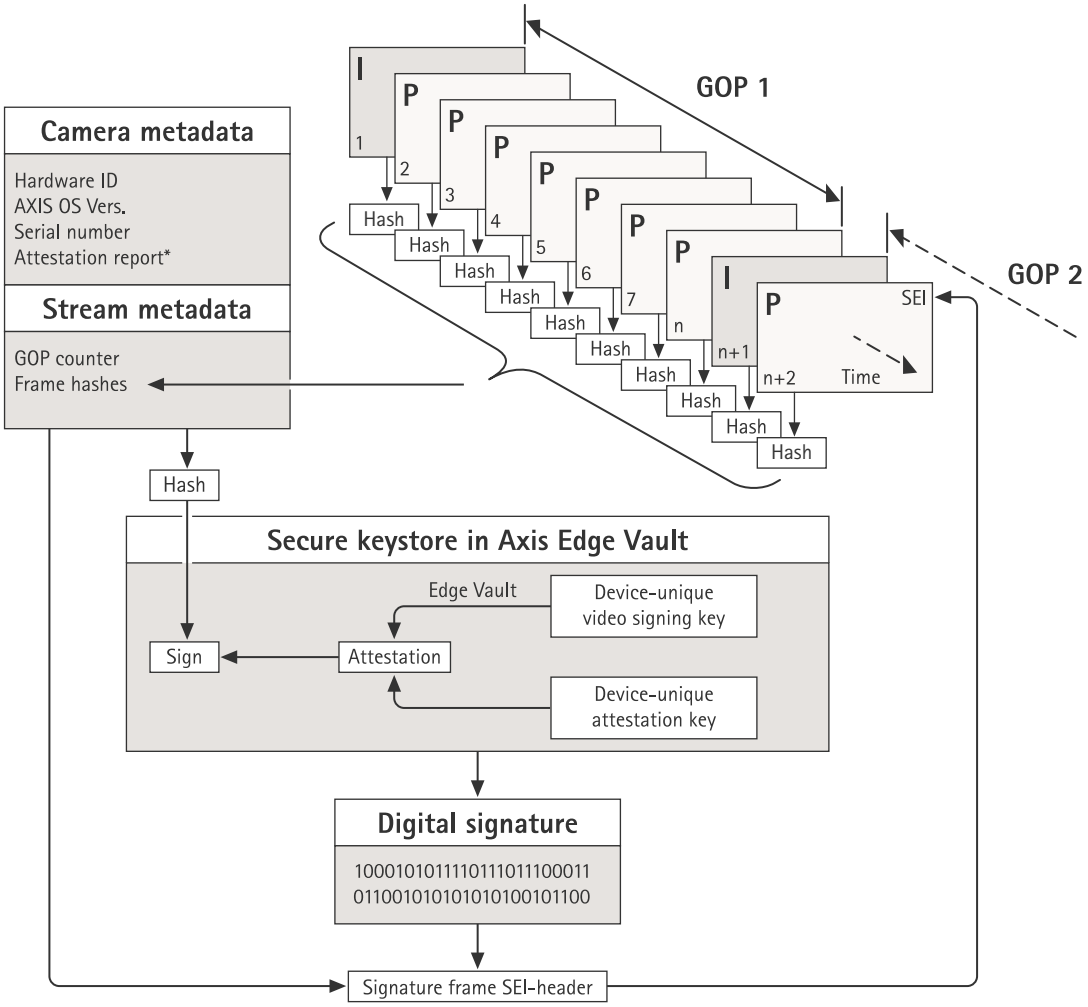


Figure 12. Grafische Darstellung der Hinzufügung einer Signatur zu den Video-Metadaten. Der Inhalt jedes Frames einer Bildergruppe (Group of Pictures, GOP) wird zusammen mit einem Hashwert der Kamera-Metadaten und Stream-Metadaten gehasht. So entsteht der Hashwert der Bildergruppe, der in Edge Vault signiert wird. Die Signatur und die Metadaten werden nun zu einem späteren SEI-Header hinzugefügt, der zusammen mit dem Stream übertragen wird.

* *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. Auf die gleiche Weise werden auch unwahrscheinliche Ereignisse wie verlorene Frames beim Streamen oder beschädigte Inhalte bei der Speicherung markiert.

5 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 kryptografisch signiert (*signierte Firmware*).

Secure Boot und signierte Firmware greifen ineinander. Sie stellen sicher, dass die Firmware vor dem Deployment nicht manipuliert wurde (durch jemandem mit physischem Zugriff auf das Gerät) und dass das Gerät auch danach keine verfälschten Firmware-Updates installieren kann. Zusammen schaffen sicheres Hochfahren und signierte Firmware eine lückenlose Kette kryptografisch validierter Software für die Vertrauenskette, auf der sämtliche sicheren Operationen beruhen.

5.1 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 sorgt dafür, dass ein Gerät nur mit autorisierter Firmware gestartet werden kann.

Der Bootvorgang wird durch das Boot-ROM eingeleitet, das den Bootloader validiert. Danach werden beim Hochfahren in Echtzeit die eingebetteten Signaturen für jeden aus dem Flash-Speicher geladenen Firmware-Block 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.

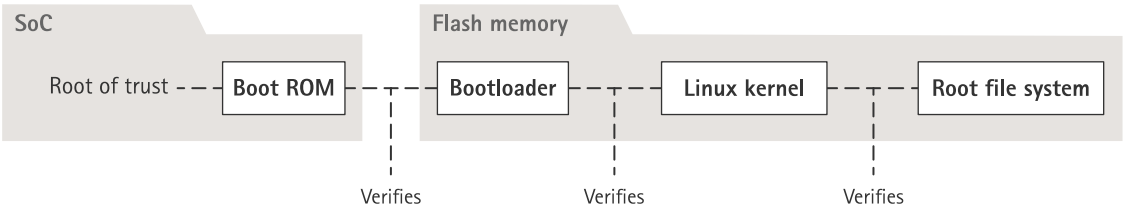


Figure 13. Beim sicheren Hochfahren authentifiziert jeder Teil der Kette die jeweils nachfolgende. Das ergibt am Ende ein verifiziertes Root-Dateisystem.

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 einem Gerät mit Axis Secure Boot ist die installierte Firmware im Flash-Speicher vor Änderungen geschützt. Das werkseitige Standard-Image ist geschützt, während die Konfiguration weiterhin ungeschützt ist. 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 die Firmware von Axis signiert wurde.

5.2 Signierte Firmware

Zur Signierung der Firmware signiert Axis ein Firmware-Image mit einem privaten Schlüssel, der geheim gehalten wird. Wenn eine Firmware mit dieser Signatur versehen ist, validiert ein Gerät die Firmware, bevor es die Installation der Firmware akzeptiert. Erkennt das Gerät, dass die Integrität der Firmware verletzt wurde, wird das Firmware-Upgrade abgelehnt.

Das Signieren von Firmware wird durch die Berechnung eines kryptographischen Hashwertes eingeleitet. Dieser Wert wird mit dem privaten Schlüssel eines privat/öffentlichen Schlüsselpaares signiert, bevor die Signatur an das Firmware-Image angehängt wird.

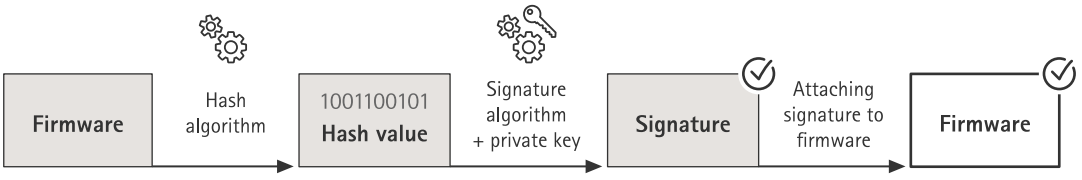


Figure 14. Signieren von Firmware – Ablauf

Vor einer Aktualisierung der Firmware muss die Echtheit der neuen Firmware verifiziert 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 Hashwert der Firmware berechnet und mit diesem validierten Hashwert aus der Signatur verglichen wird, kann die Integrität der Firmware verifiziert werden. Das Boot-Verfahren von Axis Geräten wird abgebrochen, falls die Firmware-Signatur ungültig ist oder das Firmware-Image manipuliert wurde.

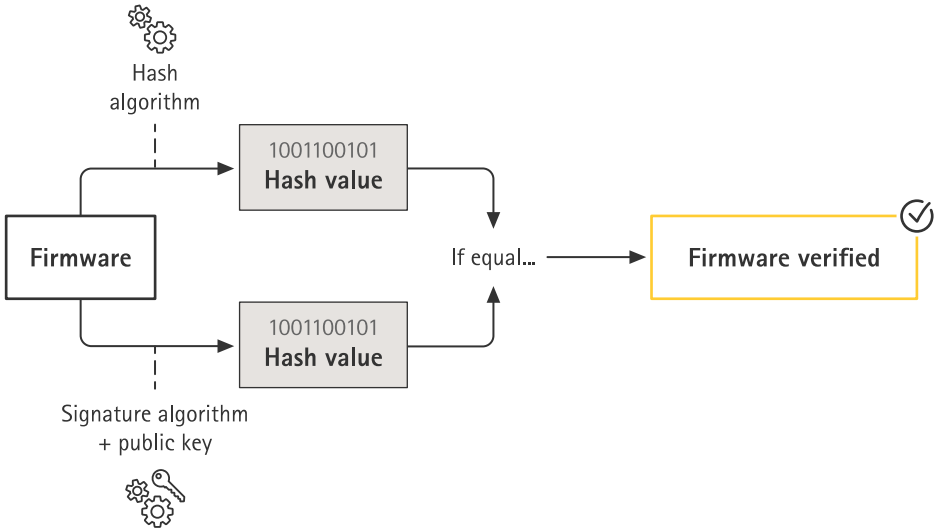


Figure 15. Verifizierung signierter Firmware – Ablauf

Die von Axis signierte Firmware basiert auf dem in der Branche anerkannten Public-Key-Verschlüsselungsverfahren RSA. Der private Schlüssel wird streng bewacht bei Axis gespeichert, nur der öffentliche Schlüssel ist in die Axis Geräte eingebettet. Die Integrität des gesamten Firmware-Image wird durch Signieren des Image-Inhalts gewährleistet. Eine primäre Signatur überprüft verschiedene sekundäre Signaturen, die während des Entpackens des Bildes überprüft werden.

Für Tests und benutzerspezifische Firmware hat Axis einen Mechanismus entwickelt, nach dem einzelne Geräte Firmware akzeptieren dürfen, die nicht aus eigener Produktion stammt. Diese Firmware wird auf eine andere Weise signiert und sowohl vom Besitzer als auch von Axis freigegeben. So erhält man ein benutzerdefiniertes Firmware-Zertifikat. Nach der Installation in den zugelassenen Geräten ermöglicht das Zertifikat die Nutzung einer benutzerspezifischen Firmware, die nur auf diesem Gerät läuft, abhängig von ihrer eindeutigen Seriennummer und Chip-ID. Benutzerspezifische Firmware-Zertifikate können nur von Axis erstellt werden, da nur Axis über den Schlüssel zu ihrer Signierung verfügt.

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 signierte Firmware, die 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.

Signierte Firmware: Firmware, die von einer vertrauenswürdigen Partei digital signiert wurde. Das Axis Gerät überprüft die Echtheit des Firmware-Image, bevor es ein Firmware-Update ausführt. Signierte Firmware ist im Secure-Boot-Verfahren vorgeschrieben.

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/M1.9/2304

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

©2023 Axis Communications AB AXIS COMMUNICATIONS, AXIS, ARTPEC und VAPIX sind unter diversen Rechtssystemen eingetragene Marken der Axis AB. Alle anderen Marken sind Eigentum der jeweiligen Inhaber. Das Recht auf Änderungen ohne Vorankündigung ist vorbehalten.