WHITEPAPER

Cybersicherheitsfunktionen in Produkten von Axis

– Signierte Firmware

– Sicheres Booten

– Axis Edge Vault

– Axis Geräte-ID

– Signiertes Video

November 2021

AXIS COMMUNICATIONS

Inhalt

1 Zusammenfassung

Dieses Dokument beschreibt einige Funktionen in den Produkten von Axis, die Cyber-Bedrohungen eindämmen und bestimmten Arten von Angriffen entgegenwirken können. Die Merkmale sind:

- Signierte Firmware
- Sicheres Hochfahren
- Axis Edge Vault
- Axis Geräte-ID
- Signiertes Video

Folgende Bedrohungen werden beschrieben:

- Firmware-Manipulation
- Manipulation der Lieferkette
- Extraktion privater Schlüssel
- Nicht autorisierter Geräteaustausch
- Video-Manipulation

1.1 Signierte Firmware

Signierte Firmware wird vom Softwarehersteller implementiert, der das Firmware-Image mit einem privaten Schlüssel signiert. Wenn eine Firmware mit dieser Signatur versehen ist, validiert ein Gerät die Firmware, bevor es ihre Installation zulässt. Erkennt das Gerät, dass die Integrität der Firmware verletzt wurde, wird das Firmware-Upgrade abgelehnt.

1.2 Sicheres Hochfahren

Sicheres Hochfahren ist ein Boot-Prozess, der aus einer ununterbrochenen Kette von kryptografisch validierter Software besteht, die im unveränderlichen Speicher (Boot-ROM) beginnt. Da sicheres Hochfahren auf der Verwendung signierter Firmware basiert, ist sichergestellt, dass ein Gerät nur mit autorisierter Firmware booten kann.

1.3 Axis Edge Vault

Axis Edge Vault ist ein sicheres kryptografisches Berechnungsmodul zur Speicherung kryptographischer Operationen in sicher gespeicherten Zertifikaten. Edge Vault stellt einen manipulationsgeschützten Speicher bereit, mit dem jedes Gerät seine Geheimnisse bewahren kann. Es legt die Grundlage für eine sichere Implementierung fortschrittlicher Sicherheitsfunktionen.

1.4 Axis Geräte-ID

Die Axis Geräte-ID funktioniert wie ein digitaler Pass, der für jedes Gerät eindeutig ist. Sie wird sicher und dauerhaft in Edge Vault als ein vom Axis Stammzertifikat signiertes Zertifikat gespeichert.

Die Axis Geräte-ID ist so konzipiert, dass sie den Ursprung des Gerätes nachweisen kann, was die Vertrauenswürdigkeit des Gerätes während seiner gesamten Lebensdauer erhöht.

1.5 Signiertes Video

Signiertes Video sorgt dafür, dass Videobeweise als nicht manipuliert verifiziert werden können, ohne die Produktkette der Videodatei überprüfen zu müssen. Jede Kamera hat eine eindeutige Axis Geräte-ID in Axis Edge Vault, mit der sie eine Signatur in den Videostream einfügen kann. Beim Abspielen des Videos zeigt der Datei-Player an, ob das Video intakt ist. So ermöglicht signiertes Video die Nachverfolgung des Videos bis zur Kamera und die Überprüfung, ob das Video nach der Aufzeichnung verfälscht wurde.

2 Glossar

Zertifikat – In der Kryptographie ist ein Zertifikat ein signiertes Dokument, das Herkunft und Eigenschaften eines Schlüsselpaares bescheinigt. Das Zertifikat ist von einer Zertifizierungsstelle (Certificate Authority, CA) signiert. Vertraut das System der CA, 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.

FIPS (Federal Information Processing Standard) – Standards für Datenverschlüsselung und Datensicherheit, herausgegeben in den USA vom NIST (National Institute of Standards and Technology).

Unveränderliches ROM – Zur sicheren Speicherung der vertrauenswürdigen öffentlichen Schlüssel und des Programms zum Vergleichen von Signaturen, 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.

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

3 Einführung

Axis beachtet bei der Verwaltung und Reaktion auf Sicherheitslücken in unseren Produkten bewährte Branchenpraktiken, um die Gefährdung der Kunden durch Cyberrisiken zu minimieren. Es gibt keine Möglichkeit zu garantieren, dass Produkte und Dienste frei von Fehlern sind, die für böswillige Angriffe ausgenutzt werden können. Das gilt nicht nur für Axis, sondern grundsätzlich für alle Netzwerk-Geräte. Axis kann jedoch garantieren, dass wir in jeder möglichen Phase stets konzertierte Anstrengungen unternehmen, damit Ihre Geräte und Dienstleistungen von Axis für Sie möglichst frei von Risiken sind.

Weitere Informationen zur Produktsicherheit und zu erkannten Schwachstellen finden Sie unter *www.axis.com/de-de/support/product-security*. Weitere Informationen darüber, wie Sie selbst Risiken durch verbreitete Bedrohungen reduzieren können, finden Sie im Axis Hardening Guide, den Sie auf der gleichen Seite herunterladen können.

Dieses Whitepaper stellt einige nachvollziehbare Cyberattacken vor und zeigt, wie sie mit Produkten von Axis verhindert werden können. Insbesondere beschreiben wir, wie durch die signierte Firmware und sicheres Hochfahren die Manipulation der Firmware und der Lieferkette verhindert werden kann. Daneben erklären wir unser vertrauenswürdiges Plattformmodul (Trusted Platform Module, TPM) und Axis Edge Vault. Beide können zur Sicherung privater Schlüssel verwendet werden. Axis Edge Vault dient zum sicheren Speichern der Geräte-ID von Axis, was die Geräte besonders vertrauenswürdig macht. Axis Edge Vault und die Axis Geräte-ID ermöglichen außerdem den Einsatz signierter Videos. Diese Funktion kann überprüfen, ob Videos bei der Übertragung von der Kamera manipuliert wurden.

4 Erkennung von Firmware-Manipulationen

Wenn alle anderen Eindringversuche in das System fehlgeschlagen sind, könnte ein Angreifer versuchen, den Systemeigentümer dazu zu bringen, geänderte Anwendungen, Firmware oder andere Softwaremodule zu installieren. Die geänderte Software kann einen schädlichen Code enthalten, der einen bestimmten Zweck erfüllen soll. Deshalb sollte man grundsätzlich niemals Software von einer Quelle installieren, der man nicht völlig vertraut. Im Kontext eines Videosystems könnte ein „Man in the Middle" (Mittelsmann) die Firmware eines Geräts verändern und Endbenutzer dazu verleiten, sie zu installieren. Das ist allerdings nicht leicht. Der Gegner muss dafür sehr geschickt und entschlossen sein. Außerdem müsste er genauestens mit dem Axis Firmware-Design und der Funktionsweise der Firmware in einem Gerät vertraut sein. Je größer die Gewinne, die ein erfolgreicher Angriff auf ein bestimmtes System verspricht, desto höher ist auch die Gefahr, dass derartige Angriffe tatsächlich durchgeführt werden. Die übliche Gegenmaßnahme liegt in der Verwendung signierter Firmware seitens der Softwarehersteller.

4.1 Firmware-Signierung

Signierte Firmware wird vom Softwarehersteller implementiert, der das Firmware-Image mit einem geheim gehaltenen privaten Schlüssel signiert. Wenn eine Firmware mit dieser Signatur versehen ist, validiert ein Gerät die Firmware, bevor es ihre Installation zulässt. 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.

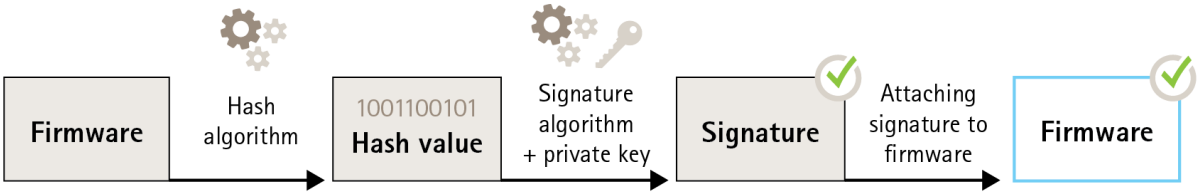

Figure 1. Signieren von Firmware – Ablauf

Vor einem Firmware-Upgrade muss die neue Firmware verifiziert werden. Um sicherzustellen, dass die neue Firmware nicht verändert wurde, wird mit dem öffentlichen Schlüssel (mit dem Axis Produkt geliefert) überprüft, ob der Hashwert tatsächlich mit dem zugehörigen 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.

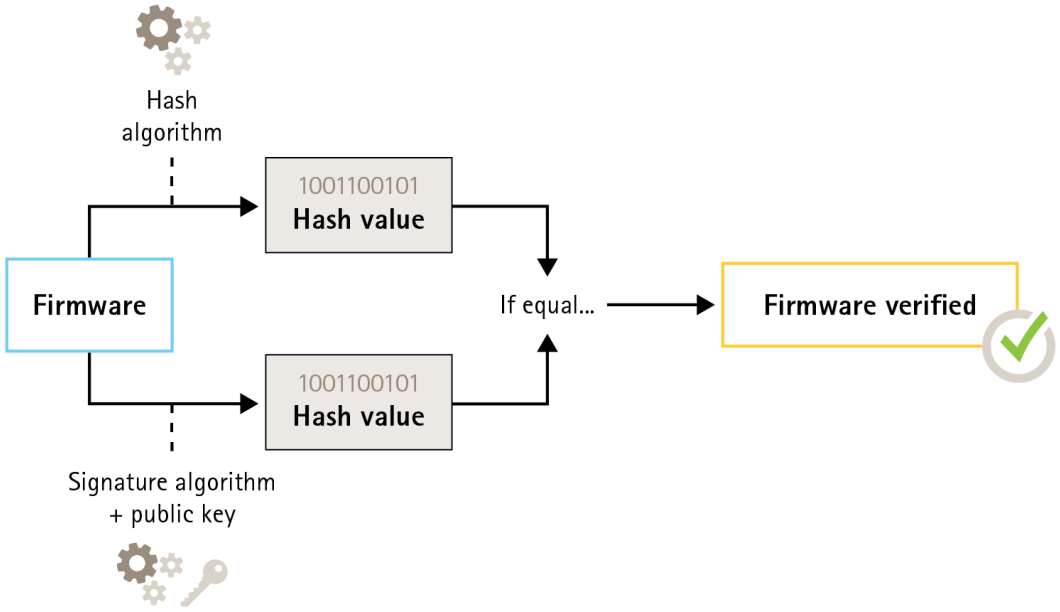

Figure 2. Verifizierung signierter Firmware – Ablauf

4.2 Signierte Firmware bei Axis

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 eine Reihe sekundärer Signaturen, die beim Entpacken des Images überprüft werden.

5 Manipulationsschutz in der Lieferkette

Die Firmware-Signierung schützt ein Gerät bei allen zukünftigen Firmware-Updates vor der Installation einer kompromittierten Firmware. Was aber, wenn ein Mittelsmann das Gerät auf dem Weg zwischen Anbieter und Endnutzer verändert? Ein Angreifer, der während der Übertragung physischen Zugriff auf das Gerät hat, könnte z. B. die Boot-Partition des Geräts kompromittieren und die Firmware-Integritätsprüfung umgehen, um eine geänderte, bösartige Firmware zu installieren, bevor das Gerät in Betrieb genommen wird.

5.1 Sicheres Hochfahren

Sicheres Hochfahren ist ein Boot-Prozess, der aus einer ununterbrochenen Kette von kryptografisch validierter Software besteht, die im unveränderlichen Speicher (Boot-ROM) beginnt. Da sicheres Hochfahren auf der Verwendung signierter Firmware basiert, ist sichergestellt, dass ein Gerät nur mit autorisierter Firmware booten 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 dient als Vertrauensanker, und der Boot-Prozess dauert nur so lange, wie jede Signatur überprüft wird. Jeder Teil der Kette authentifiziert den jeweils nächsten Teil, so dass am Ende ein verifizierter Linux-Kernel und ein verifiziertes Root-Dateisystem entstehen.

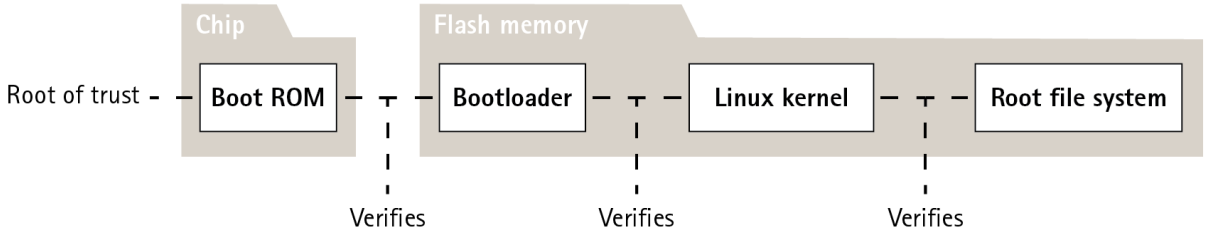

Figure 3. Sicheres Hochfahren – Ablauf

5.2 Axis Secure Boot

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, dass das Axis Gerät nach Zurücksetzen auf die Werkseinstellung vollständig frei von eventueller Malware ist.

5.3 Sicheres Booten und kundenspezifische Firmware-Zertifikate

Sicheres Hochfahren erhöht zwar die Produktsicherheit, reduziert aber die Flexibilität bei Verwendung unterschiedlicher Firmware, weil es das Laden temporärer Firmware wie Test-Firmware oder anderer benutzerdefinierter Firmware von Axis in das Produkt erschwert. Deshalb hat Axis ein Verfahren entwickelt, mit dem die verschiedenen Einzelgeräte diese produktionsfremde Firmware zulassen können. 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 Geheimnisse vor Manipulation geschützt

Eine Grundanforderung jedes gesicherten verteilten Systems ist die Fähigkeit, Verbindungen zu verifizieren und heimliches Mithören zu verhindern. Hierfür muss jedes Gerät seine Geheimnisse in einem manipulationsgeschützten sicheren Speicher aufbewahren. Axis Edge Vault ist ein solcher Speicher, auf dessen Grundlage erweiterte Sicherheitsfunktionen auf sichere Weise umgesetzt werden können.

6.1 Axis Geräte-ID

Während der Produktion jeder Axis Netzwerk-Geräteeinheit wird ein „digitaler Pass" namens Axis Geräte-ID sicher im Axis Edge Vault des Geräts installiert. Jedes Gerät hat eine eigene, eindeutige Identität, die die Herkunft des Geräts belegt. Die Geräte-ID von Axis ist eine Sammlung von Zertifikaten, die im kryptografischen Teil des Moduls verwendet wird, um Anforderungen zu signieren, die von der eingebetteten Produktfirmware an Edge Vault gestellt werden. Die Antwort darauf wird an den Empfänger zurückgesendet, der mithilfe der öffentlichen Schlüssel von Axis die Authentifizierung der Antwort validieren kann.

Ein Zertifikat ist ein kleiner Datensatz, der einen öffentlichen Schlüssel und Metadaten zur Beschreibung des Schlüssels mit einer Signatur des Ausstellers kombiniert, die die Gültigkeit des Zertifikats bestätigt. Eine Zertifikatshierarchie ist eine Möglichkeit, um die Herkunft des Zertifikats nachzuweisen.

Vergleichen wir als Beispiel die Axis Geräte-ID mit einem Reisepass. Wenn Sie einen Reisepass besitzen, versichert die Regierung Ihres Landes, dass Sie tatsächlich die Person sind, die in Ihrem Reisepass angegeben ist. Auf ähnliche Weise werden alle Geräte-ID-Zertifikate von Axis durch ein Axis Geräte-ID-Root-CA-Zertifikat bestätigt. So wie ein Zollbeamter darauf vertraut, dass die Regierung Ihres Landes Ihren Reisepass korrekt ausgestellt hat, vertraut ein Netzwerk-Sicherheitssystem darauf, dass

das Axis Geräte-ID-Root-CA-Zertifikat das Axis Zertifikat eines mit dem Netzwerk verbundenen Geräts korrekt verifiziert hat.

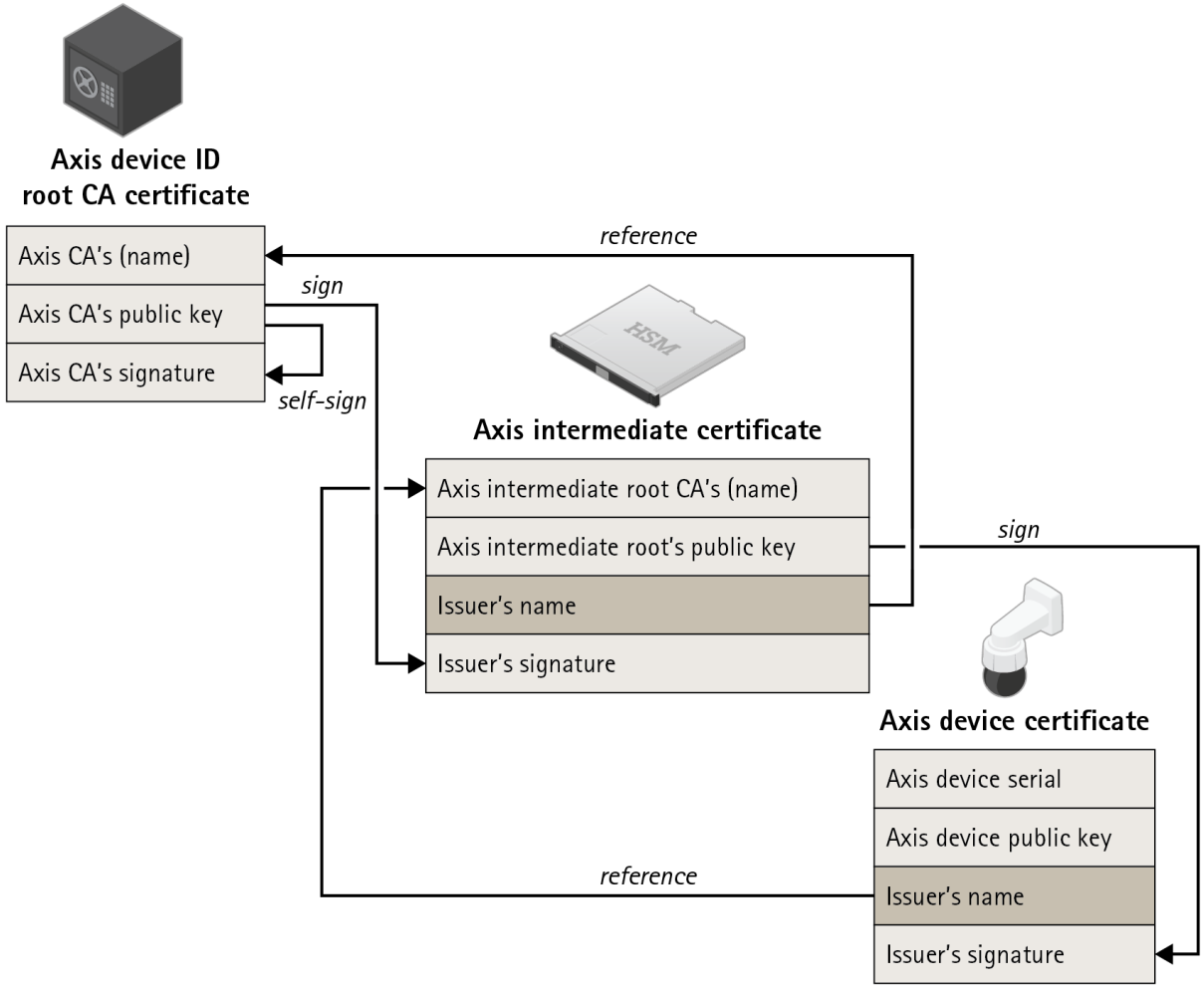

Figure 4. Die Geräte-ID von Axis, ein Zertifikat mit der Seriennummer des Produkts, wird von einem Zwischenzertifikat signiert, das vom Axis Stammzertifikat unterzeichnet wurde. Da das wertvolle Axis Stammzertifikat in einem Safe aufbewahrt werden muss, benötigt man für die Bereitstellung im Werk dieses Zwischenzertifikat.

7 Sichere Speicherung der Schlüssel

Die Geräte von Axis unterstützen HTTPS (Netzwerk-Verschlüsselung) und 802.1X (Netzwerk-Zugangskontrolle), die beide TLS (Transport Layer Security) verwenden. Die digitalen Zertifikate von TLS verwenden ein öffentlich/privates Schlüsselpaar. Der private Schlüssel wird auf dem Gerät gespeichert, während der öffentliche Schlüssel im Zertifikat enthalten ist. Hier ist anzumerken, dass keine Schlüssel geschützt werden müssen, wenn weder HTTPS noch 802.1X verwendet wird.

Ein Angreifer könnte versuchen, den privaten Schlüssel und das Zertifikat aus dem Gerät zu extrahieren und auf einem angreifenden Computer zu installieren. Im Fall von HTTPS könnte mithilfe dieses privaten Schlüssels verschlüsselter Netzwerk-Datenverkehr zwischen dem Gerät und dem VMS gelesen werden. Oder im Fall von Spoofing könnte der angreifende Computer Zugang zum VMS erhalten, indem er vorgibt, ein

legitimes Gerät zu sein. Im Fall von 802.1X könnte der Gegner den privaten Schlüssel verwenden, um Zugriff auf ein 802.1X-geschütztes Netzwerk zu erhalten, indem er sich als vertrauenswürdiges Gerät ausgibt.

Zertifikate und private Schlüssel werden im Allgemeinen im Dateisystem eines Geräts gespeichert, durch die Kontozugriffsrichtlinie geschützt und in der normalen Computerumgebung verwendet. In den meisten Fällen ist dies auch ausreichend, da es sehr schwer ist, das Konto zu kompromittieren. Zertifikate können auch widerrufen werden, wenn eine Verletzung vermutet wird. Damit wird der private Schlüssel unbrauchbar.

Bei einigen Endbenutzern kritischer Systeme besteht ein erhöhtes Risiko, dass entschlossene und qualifizierte Angreifer versuchen, das Gerät zu knacken, um den privaten Schlüssel zu extrahieren. Mit Axis Edge Vault kann der Schlüssel so gespeichert werden, dass er praktisch unmöglich extrahiert werden kann, sogar wenn das Gerät kompromittiert wird.

7.1 Sichere Speicherung von Zertifikaten mit Axis Edge Vault

Axis Edge Vault ist ein sicheres kryptografisches Berechnungsmodul in Form eines Chips auf der Leiterplatte im Inneren des Produkts. Edge Vault kann Zertifikate sicher speichern und dafür verwendet werden, um kryptographische Operationen an sicher gespeicherten Zertifikaten auszuführen.

Die in Edge Vault gespeicherten Zertifikate müssen diesen sicheren Speicherort nicht verlassen, um im Gerät verwendet werden zu können. Sie verbleiben auch bei Verwendung sicher im Edge Vault, da die kryptografische Hardware, die mit dem Schlüssel arbeitet, auf demselben physischen Chip installiert ist.

7.2 Sichere Schlüsselspeicherung mit einem TPM (Trusted Platform Module)

Ein TPM ist eine Komponente, die einen bestimmten Satz von kryptographischen Merkmalen bereitstellt, die geeignet sind, um Informationen vor unbefugtem Zugriff zu schützen. Der private Schlüssel wird im TPM gespeichert, wo er dauerhaft bleibt. Alle kryptographischen Operationen, die eine Verwendung des privaten Schlüssels erfordern, werden zur Verarbeitung an das TPM gesendet. Dadurch wird sichergestellt, dass der geheime Teil des Zertifikats niemals die sichere Umgebung innerhalb des TPM verlässt und auch im Falle eines Sicherheitsverstoßes sicher bleibt.

7.3 FIPS 140-2-Zertifizierung

Bei manchen Produkten und Anwendungsfällen könnte ein TPM für den Schutz der Daten gesetzlich vorgeschrieben sein, manchmal in Verbindung mit der Forderung nach Kompatibilität mit FIPS 140-2. FIPS (Federal Information Processing Standard) 140-2 ist ein Informationssicherheitsstandard für kryptographische Module, der in den USA vom NIST (National Institute of Standards and Technology) herausgegeben wird.

Die Validierung durch ein NIST-zertifiziertes Testlabor garantiert, dass das Modulsystem und die Kryptographie des Moduls ordnungsgemäß implementiert wurden. Kurz gesagt: Die Zertifizierung erfordert die Beschreibung, Spezifikation und Verifizierung des kryptografischen Moduls, zugelassene Algorithmen, zugelassene Betriebsarten und Einschalttests.

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

7.3.1 Zertifiziertes TPM in Axis Produkten

Das in ausgewählten Axis Produkten verwendete TPM ist für die Erfüllung der Anforderungen von FIPS 140-2 zertifiziert, bzw. genauer gesagt für Security Level 2 des Standards, was bedeutet, dass das TPM unter anderem auch die Anforderungen für rollenbasierte Authentifizierung und Originalitätssicherung erfüllt.

8 IEEE 802.1AR – Geräteverifizierung mit der Geräte-ID von Axis

Der Käufer eines Netzwerk-Geräts von Axis kann vor der Inbetriebnahme eine manuelle Prüfung durchführen. Der Kunde kann das Produkt visuell untersuchen und sich aufgrund seines Vorwissens über das Aussehen und die Handhabung von Axis Produkten überzeugen, dass das Produkt tatsächlich von Axis stammt. Das ist natürlich nur möglich, wenn man physischen Zugang zum Produkt hat. Wenn Sie also über ein Netzwerk mit einem nicht bereitgestellten Produkt kommunizieren, wie können Sie dann sicher sein, mit dem richtigen Gerät zu kommunizieren? Woher wissen Sie, dass das Gerät nicht unautorisiert ausgetauscht wurde? Weder Netzwerk-Geräte noch Software auf Servern können eine physische Inspektion durchführen. Als Sicherheitsmaßnahme war es bisher üblich, mit einem neuen Produkt zunächst über ein geschlossenes Netzwerk zu interagieren, in dem das Gerät sicher bereitgestellt werden kann.

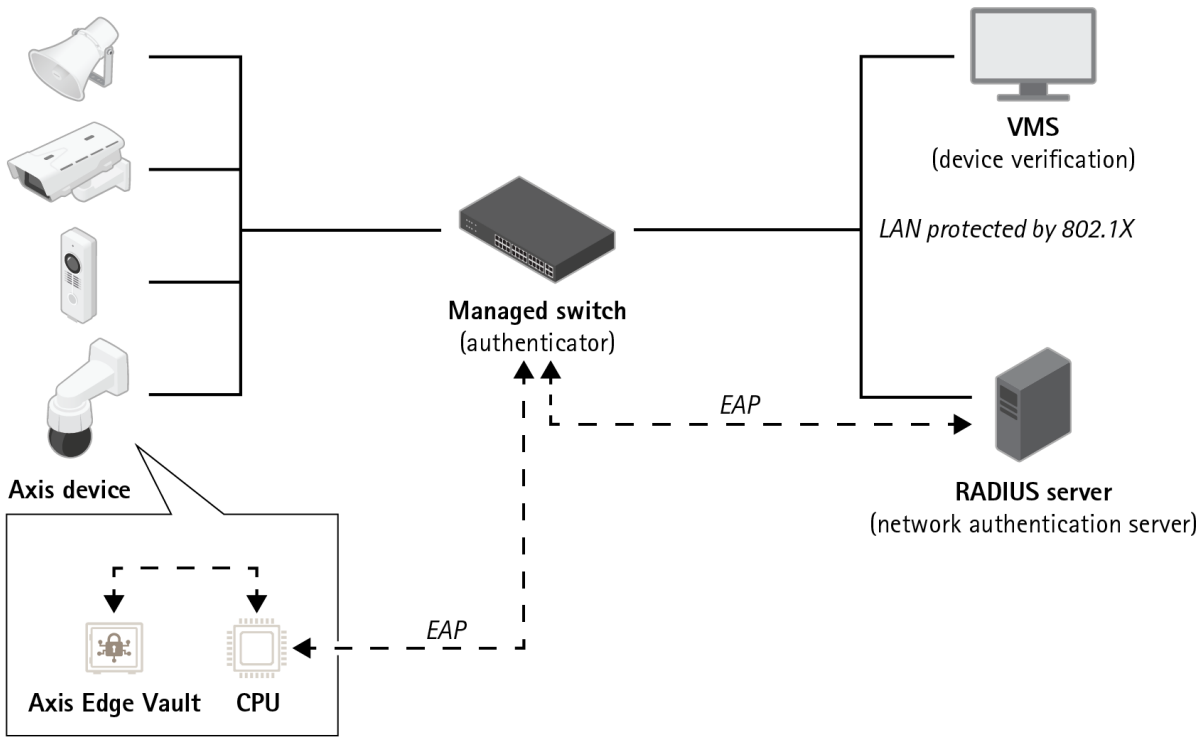

Figure 5. Die Kunden können ihren Authentifizierungsserver anweisen, gekaufte Axis Produkte unter Verwendung der Geräteseriennummern und der Axis Geräte-ID automatisch im Netzwerk zu akzeptieren.

Der neue internationale Standard IEEE 802.1AR (*https://1.ieee802.org/security/802-1ar/*) legt ein Verfahren zur Autorisierung und Sicherung der Identifizierung eines Geräts über ein Netzwerk fest. Wenn die

Kommunikation in ein eingebettetes Sicherheitsmodul weitergeleitet wird, kann die Einheit eine dem Standard entsprechende vertrauenswürdige Identifikationsantwort zurücksenden.

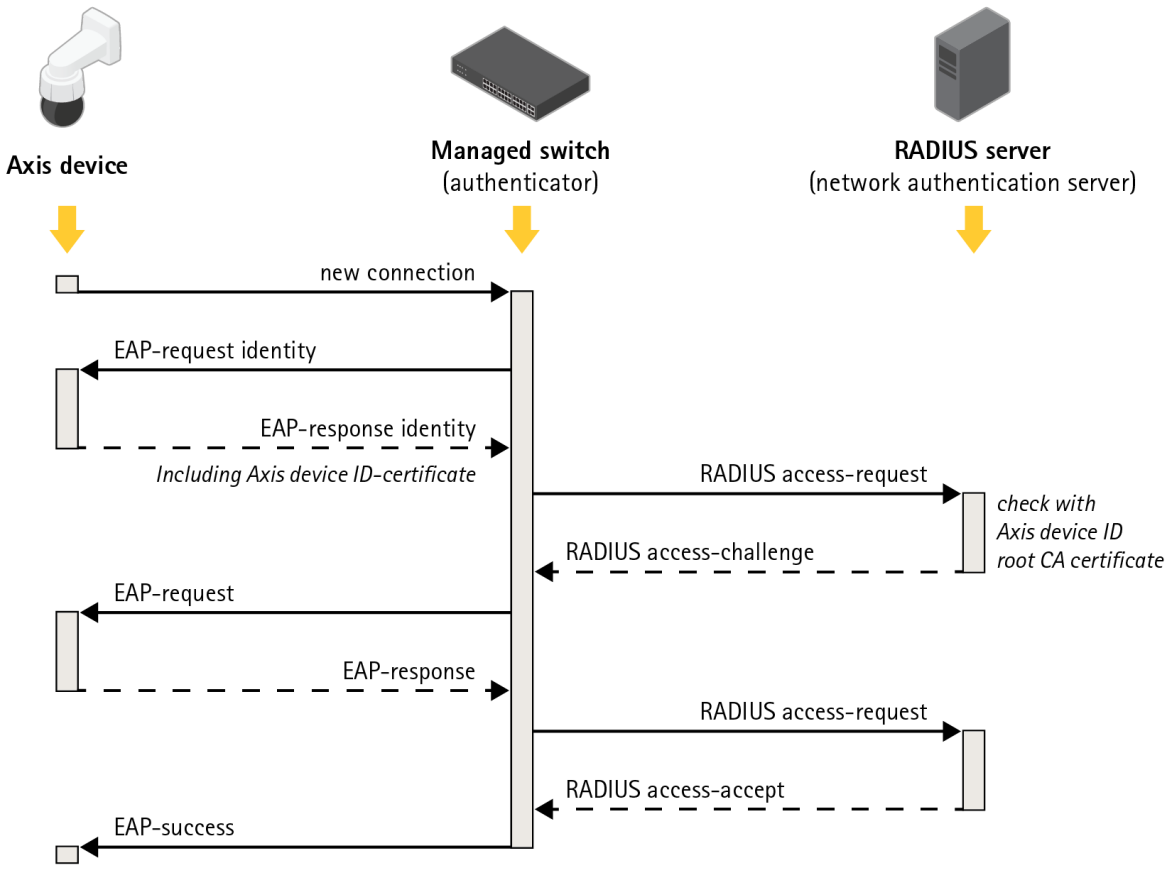

Figure 6. IEEE 802.1AR definiert ein Verfahren für die Identifizierung eines Geräts über ein Netzwerk mit einem Protokoll. Das Protokoll sendet EAP-Anforderungen (Extensible Authentication Protocol) an den Switch, der mithilfe von RADIUS-Anforderungen (Remote Authentication Dial-In User Service) Zugriff gewährt.

Axis setzt diese Sicherheitsmaßnahmen in seinen Produkten über Axis Edge Vault und die Axis Geräte-ID um. Axis Edge Vault ist ein sicheres Modul, in dem die Axis Geräte-ID (eine Sammlung von Zertifikaten zur Verifizierung der Geräteidentifizierung) installiert ist. Diese Funktionen liefern Ihrem Netzwerk einen kryptografisch überprüfbaren Nachweis, dass ein bestimmtes Gerät tatsächlich von Axis hergestellt wurde und dass die Netzwerk-Verbindung zu diesem Gerät tatsächlich von ihm bedient wird.

Ein Gerät mit der Geräte-ID von Axis wurde im Werk bereitgestellt (mit Schlüsseln und Zertifikaten). Anhand dieser Bereitstellung kann später ein Kunde das Gerät vor Ort zusätzlich mit anderen Schlüsseln und/oder Zertifikaten ausstatten, die ihm den Zugriff auf bestimmte Netzwerk-Ressourcen ermöglichen.

Durch die Identifizierung des Geräts mit der Geräte-ID von Axis kann die Zeit für die Bereitstellung von Geräten verkürzt werden, da die Installation und Konfiguration des Geräts im vorgesehenen Netzwerk mit weniger Arbeit verbunden ist. Ein weiterer Vorteil ist, dass die Geräte-ID von Axis nicht nur einen

zusätzlichen, integrierten Vertrauensnachweis bereitstellt, sondern auch die Möglichkeit, die Geräte in einem großen System zu verfolgen.

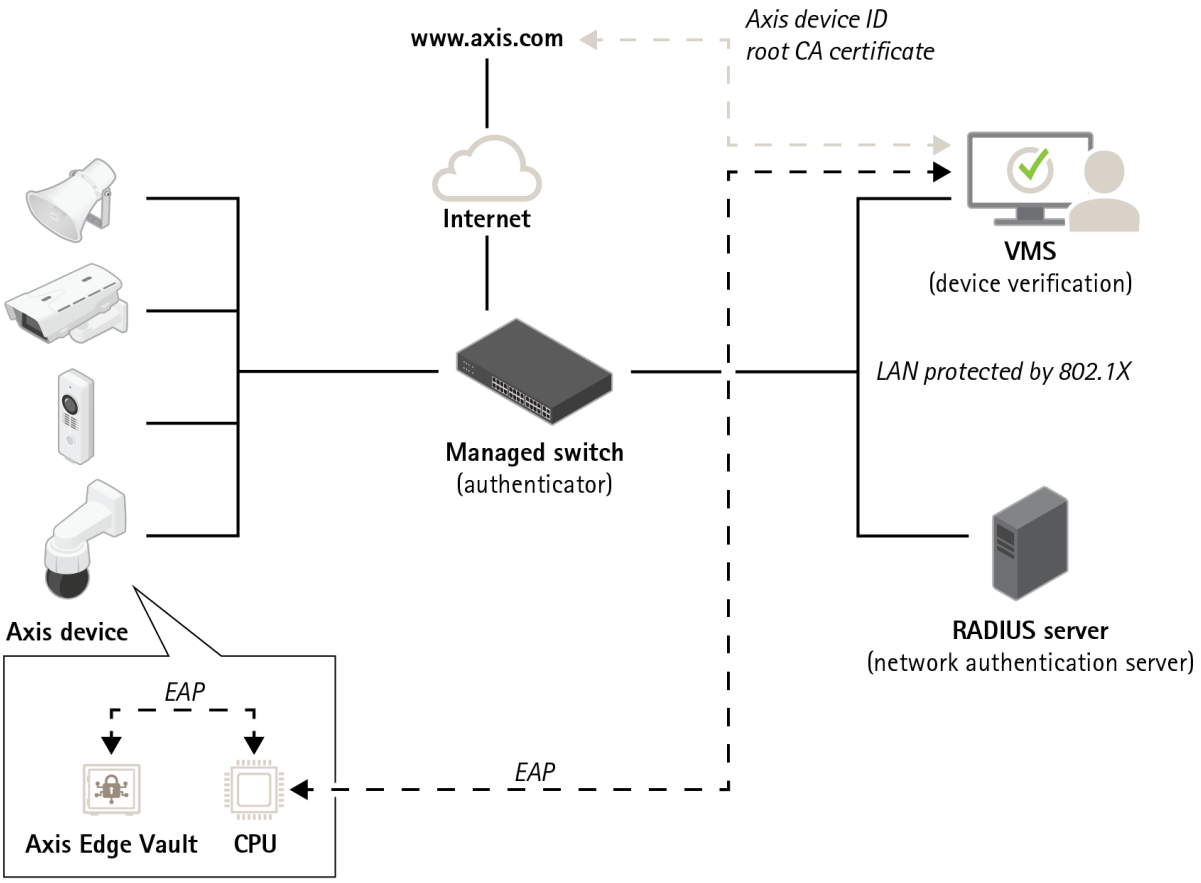

Figure 7. Softwareanwendungen in anderen Teilen des Systems können anhand der Axis Geräte-ID und kryptografischen Operationen überprüfen, mit wem sie kommunizieren. Die Geräte-ID von Axis wurde durch das öffentliche Axis Geräte-ID-Root-CA-Zertifikat von axis.com verifiziert.

9 Videomanipulationserkennung

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.

9.1 Signiertes Video

Die Funktion „Signiertes Video" von Axis stellt über eine Signatur im Videostream sicher, dass das Video intakt ist, 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 die Polizei das Video als Videodatei auf einen USB-Stick exportieren und in einem EMS (Beweismittel-Verwaltungssystem)

speichern. 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.

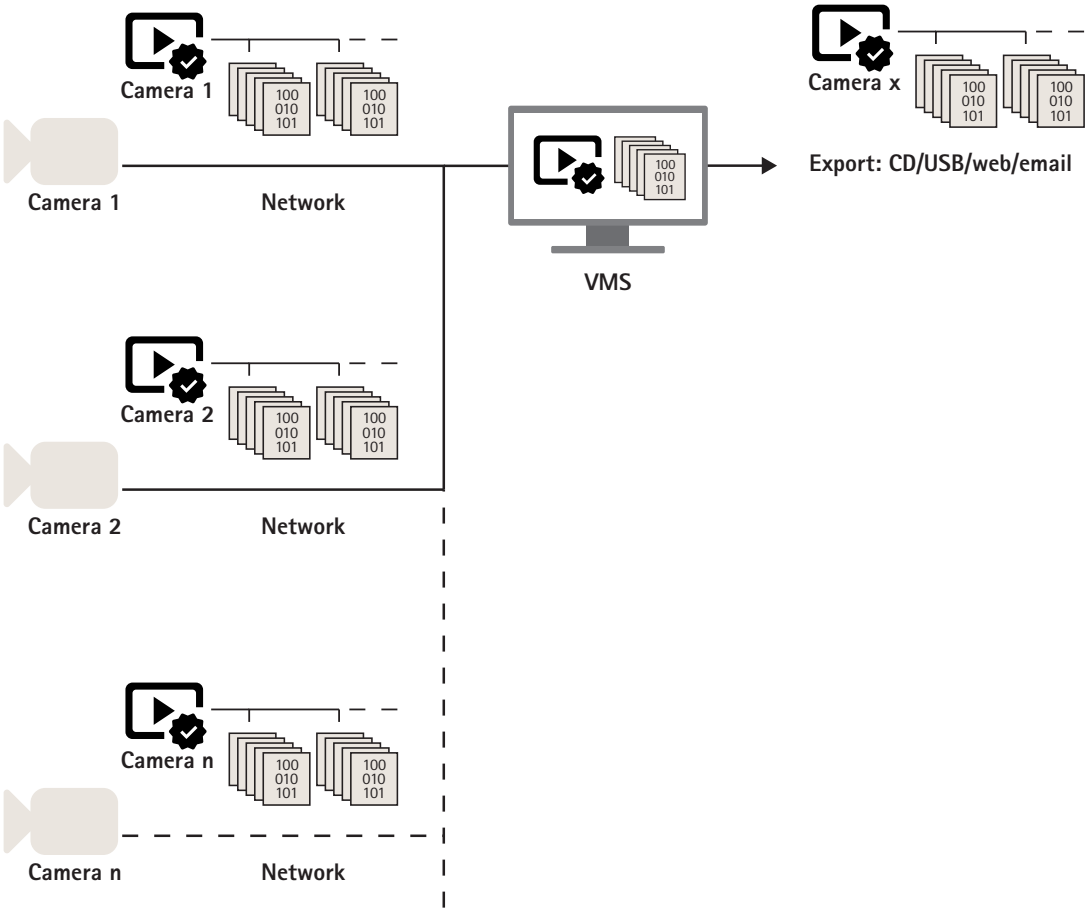

Figure 8. Die Signatur wird bereits in der Kamera eingefügt, so dass der Inhalt in jedem Schritt von der Quelle bis zur Verwendung des Videos überprüft werden kann.

Jede Kamera hat dabei eine eindeutige Axis Geräte-ID in Axis Edge Vault, mit der sie eine Signatur in den Videostream einfügen kann. Hierfür wird ein Hashwert für jeden Videoframe berechnet, einschließlich der

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

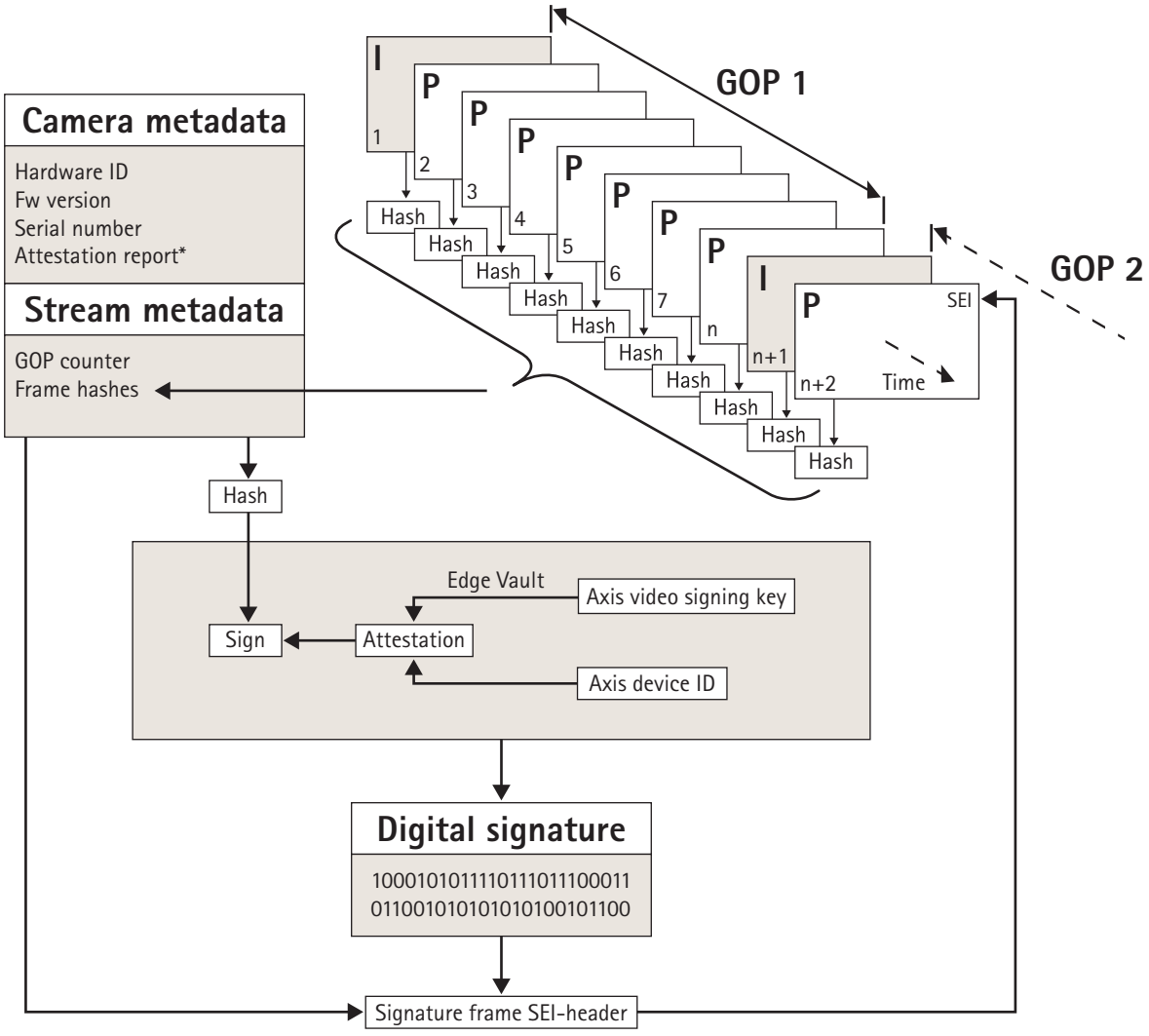

Figure 9. Grafische Darstellung der Hinzufügung einer Signatur zu den Video-Metadaten. Der Inhalt jedes Frames einer Bildergruppe wird zusammen mit einem Hashwert der Kamera-Metadaten und Stream-Metadaten gehasht. So entsteht der Hashwert der Bildergruppe, der in Edge Vault signiert wird. Die Signatur und 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 geschieht mithilfe eines gerätespezifischen Videosignierschlüssels, der für die eindeutige Axis Geräte-ID bestätigt wurde. Der Bestätigungsbericht wird am Anfang und danach in

regelmäßigen Zeitabständen in den Stream eingefügt, meist einmal pro Stunde. 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 Bildergruppe 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.

T10154694/DE/M3.2/2111

Über Axis Communications

Axis ermöglicht eine smarte und sichere Welt durch die Entwicklung von Netzwerk-Lösungen. Diese bieten Erkenntnisse, um die Sicherheit und Geschäftsmethoden zu verbessern. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte und Dienstleistungen für die Videoüberwachung/-analyse und Zutrittskontrolle sowie Sprechanlagen und Audiosysteme. Das 1984 gegründete schwedische Unternehmen beschäftigt mehr als 3.800 engagierte Mitarbeiter in über 50 Ländern. Gemeinsam mit seinen Partnern auf der ganzen Welt bietet das Unternehmen kundenspezifische Lösungen an.

Weitere Informationen zu Axis bietet Ihnen unsere Webseite *axis.com*.