Signierte Firmware, sicheres Hochfahren und sichere private Schlüssel

Cybersicherheitsfunktionen in Produkten von Axis

Juli 2020

AXIS COMMUNICATIONS

Inhalt

1 Zusammenfassung

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

- signierte Firmware
- sicheres Hochfahren
- Trusted Platform Module (TPM)
- Axis Edge Vault mit Axis Geräte-ID.

Zu den beschriebenen Bedrohungen gehören:

- Firmware-Manipulation
- Manipulation der Lieferkette
- Extraktion privater Schlüssel
- nicht autorisierter Geräteaustausch

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 die Installation der Firmware akzeptiert. Wenn das Gerät feststellt, dass die Integrität der Firmware beeinträchtigt ist, wird die Aktualisierung der Firmware abgelehnt.

1.2 Sicheres Hochfahren

Sicheres Hochfahren ist ein Bootvorgang, 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, wird sichergestellt, dass ein Gerät nur mit autorisierter Firmware booten kann.

1.3 TPM

Ein TPM ist eine Komponente mit einem bestimmten Satz von kryptographischen Merkmalen, die geeignet sind, Informationen vor unbefugtem Zugriff zu schützen. Private Schlüssel werden im TPM gespeichert, und 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 auch im Falle einer Sicherheitsverletzung sicher bleibt. Das in ausgewählten Produkten von Axis verwendete TPM ist gemäß den Anforderungen von FIPS 140-2 zertifiziert.

1.4 Axis Edge Vault mit Axis Geräte-ID

Der neue internationale Standard IEEE 802.1AR beschreibt ein Verfahren, wie die Identifizierung eines Geräts über ein Netzwerk automatisiert und gesichert werden kann. In den Produkten von Axis werden diese Sicherheitsmaßnahmen durch die Verwendung von Axis Edge Vault und der Axis Geräte-ID

implementiert. Edge Vault kann für kryptografische Herausforderungen verwendet werden, die auf sicher gespeicherten Zertifikaten ausgeführt werden. Der private Teil der Zertifikate verbleibt auch bei Verwendung im Edge Vault. Die Axis Geräte-ID wird sicher und dauerhaft in Edge Vault in Form eines von einem Axis Root-Zertifikat signierten Zertifikats gespeichert. Dies ermöglicht eine neue Ebene des Gerätevertrauens während des gesamten Lebenszyklus des Produkts.

2 Glossar

Zertifikat – In der Kryptographie ist ein Zertifikat ein signiertes Dokument, das Herkunft und Eigenschaften eines Schlüsselpaars bescheinigt. 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) – Die Wurzel der Sicherheitskette eines Zertifikats. Die Zertifizierungsstelle weist die Echtheit und Richtigkeit der zugrunde liegenden Zertifikate nach.

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

Unveränderliches ROM – Zur sicheren Speicherung der vertrauenswürdigen öffentlichen Schlüssel und des Programms, das zum Vergleich von Signaturen verwendet wird. Ein Überschreiben ist nicht möglich.

Bereitstellung – Prozess der Vorbereitung und Ausstattung eines Geräts für das Netzwerk. Dazu gehört die Bereitstellung von Konfigurationsdaten und Richtlinieneinstellungen für das Gerät von einer zentralen Stelle 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 kann, aber nur der Empfänger kann die Nachricht – unter Verwendung des *privaten Schlüssels* – entschlüsseln. Kann sowohl zum Verschlüsseln als auch zum Signieren von Nachrichten verwendet werden.

TLS (Transport Layer Security) – Internetstandard zum Schutz des Datenverkehr im Netzwerk. TLS stellt das S (für „secure") in HTTPS zur Verfügung.

3 Einführung

Axis hält sich bei der Verwaltung und Reaktion auf Sicherheitslücken in unseren Produkten an bewährte Vorgehensweisen der Branche, 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. Dies gilt nicht nur für Axis, sondern allgemein für alle Netzwerkgeräte. Axis garantiert jedoch, dass in jeder Phase stets konzertierte Anstrengungen unternommen werden, um sicherzustellen, dass Ihre Geräte und Dienste von Axis dem geringstmöglichen Risiko ausgesetzt sind.

Weitere Informationen über Produktsicherheit und entdeckte Schwachstellen finden Sie unter *www.axis.com/support/product-security*. Weitere Informationen über die Maßnahmen, die Sie ergreifen können, um die Risiken gängiger Bedrohungen zu verringern, finden Sie im Axis Hardening Guide unter *www.axis.com/cybersecurity*.

Dieses Whitepaper stellt einige plausible Cyberangriffe vor und erläutert, wie sie bei Produkten von Axis verhindert werden können. Es wird speziell beschrieben, wie durch signierte Firmware und sicheres Hochfahren die Manipulation der Firmware und der Lieferkette verhindert werden kann. TPM (Trusted Platform Module) und Axis Edge Vault, die beide zur Sicherung privater Schlüssel verwendet werden können, werden ebenfalls behandelt. Axis Edge Vault wird für eine sichere Speicherung der Axis Geräte-ID verwendet, was eine neue Ebene des Gerätevertrauens ermöglicht.

4 Erkennung von Firmware-Manipulationen

Wenn andere Versuche, in das System einzudringen, fehlgeschlagen sind, setzen Angreifer möglicherweise auf andere Angriffsmethoden. Beispielsweise versuchen sie, 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. Allgemein wird empfohlen, niemals Software von Quellen zu installieren, denen Sie nicht völlig vertrauen. Bei einem Videosystem versucht möglicherweise ein „Mann in der Mitte", die Firmware eines Geräts zu ändern und Endbenutzer zur Installation zu verleiten. Das ist selbstverständlich nicht einfach. Angreifer bedienen sich jedoch sehr ausgefeilter Taktiken. Ein Angreifer benötigt detaillierte Kenntnisse vom Design der Axis Firmware und deren Funktionsweise. Wenn der Gewinn durch einen erfolgreichen Angriff hoch genug ist, leisten Angreifer jedoch die notwendige Vorarbeit. Um dieser Gefahr vorzubeugen, verwenden Softwareanbieter in der Regel signierte Firmware.

4.1 Firmware-Signierung

Signierte Firmware wird vom Softwarehersteller implementiert, indem er 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 die Installation der Firmware akzeptiert. Wenn das Gerät feststellt, dass die Integrität der Firmware beeinträchtigt ist, wird die Aktualisierung der Firmware abgelehnt.

Die Signierung der Firmware wird durch die Berechnung eines kryptographischen Hashwerts eingeleitet. Der Wert wird dann mit dem privaten Schlüssel eines privaten/öffentlichen Schlüsselpaars signiert, bevor die Signatur an das Firmware-Image angehängt wird.

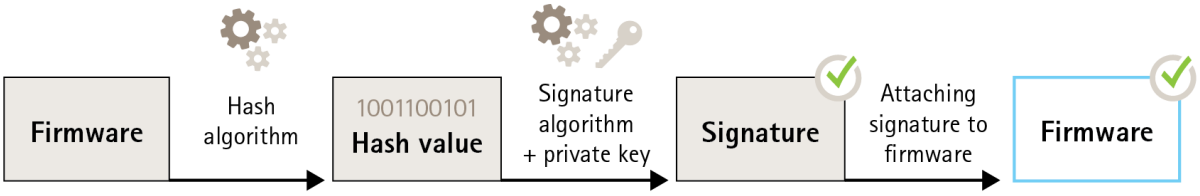

Figure 1. Die Signierung von Firmware.

Vor einer Aktualisierung der Firmware muss die neue Firmware verifiziert werden. Um sicherzustellen, dass die neue Firmware unverändert ist, 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 dem validierten Hashwert aus der Signatur verglichen wird, kann die Integrität der Firmware verifiziert werden.

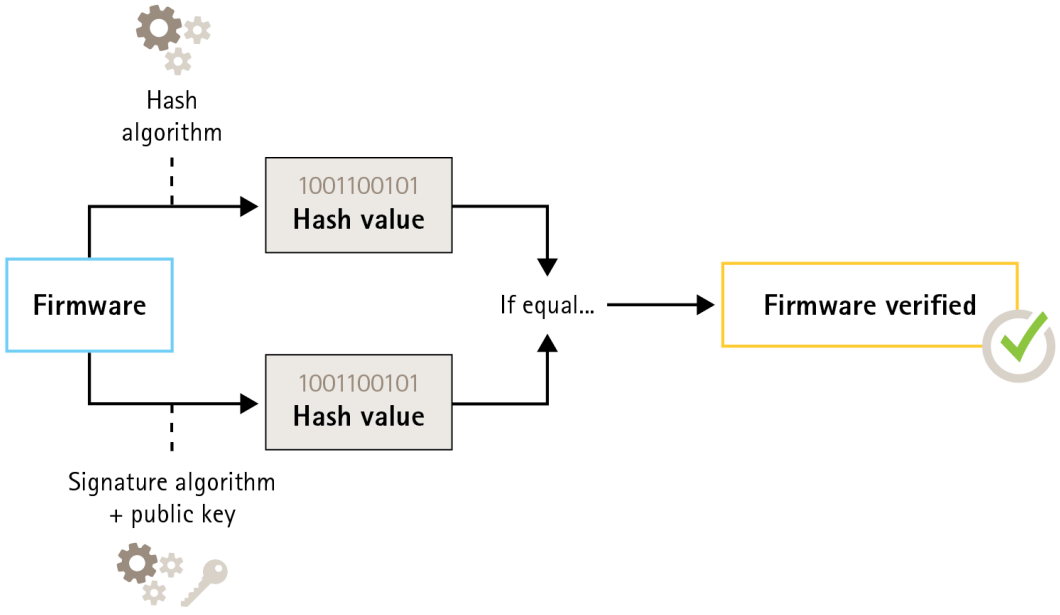

Figure 2. Die Verifizierung signierter Firmware.

4.2 Signierte Firmware von Axis

Die von Axis signierte Firmware basiert auf der von der Branche anerkannten Verschlüsselungsmethode RSA mit öffentlichem Schlüssel. Der private Schlüssel wird an einem genau bewachten Ort bei Axis gespeichert.

Der öffentliche Schlüssel ist in die Axis Geräte eingebettet. Die Integrität des gesamten Firmware-Bildes wird durch Signieren des Bildinhalts gewährleistet. Eine primäre Signatur überprüft eine Reihe sekundärer Signaturen, die während des Entpackens des Images überprüft werden.

5 Manipulationsschutz in der Lieferkette

Die Firmware-Signierung sorgt dafür, dass ein Gerät bei allen zukünftigen Aktualisierungen der Firmware vor der Installation einer kompromittierten Firmware geschützt ist. Was geschieht, wenn das Gerät bei einem Man-in-the-Middle-Angriff auf dem Weg zwischen Verkäufer und Endbenutzer geändert wird? Angreifer, die während des Transports physischen Zugriff auf das Gerät erlangen, könnten einen Angriff durchführen und z. B. die Boot-Partition des Geräts durch eine Umgehung der Firmware-Integritätsprüfung kompromittieren, um vor der Bereitstellung des Geräts eine geänderte, schädliche Firmware zu installieren.

5.1 Sicheres Hochfahren

Sicheres Hochfahren ist ein Bootvorgang, 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, wird sichergestellt, dass ein Gerät nur mit autorisierter Firmware booten kann.

Der Bootvorgang wird durch das Boot-ROM eingeleitet, das den Bootloader validiert. Beim sicheren Hochfahren werden dann in Echtzeit die eingebetteten Signaturen für jeden aus dem Flash-Speicher geladenen Firmwareblock verifiziert. Das Boot-ROM stellt die Wurzel der Sicherheitskette dar, und der Bootvorgang wird nur so lange fortgesetzt, bis jede Signatur verifiziert wurde. Jeder Teil der Kette authentifiziert den nächsten Teil, was letztendlich zu einem verifizierten Linux-Kernel und einem verifizierten Root-Dateisystem führt.

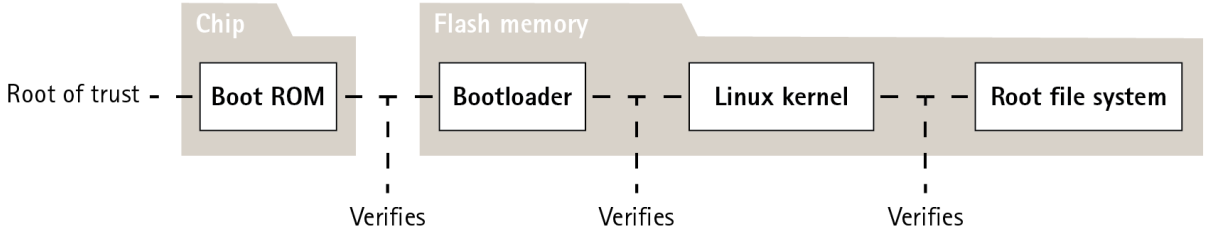

Figure 3. Der sichere Bootvorgang.

5.2 Axis Secure Boot

Bei vielen Geräten ist es wichtig, dass die Funktionen niederer Ebene nicht verändert werden können. Wenn andere Sicherheitsmechanismen auf der Software niederer Ebene basieren, dient der sichere Bootvorgang als sichere Basisschicht, die diese Mechanismen vor Umgehung schützt.

Bei einem Gerät mit sicherem Bootvorgang ist die installierte Firmware im Flash-Speicher vor Änderungen geschützt. Das werksseitige Standard-Image ist geschützt, während die Konfiguration ungeschützt bleibt. Ein sicherer Bootvorgang gewährleistet, dass das Axis Gerät nach dem Zurücksetzen auf die Werkseinstellungen vollständig von möglicher Malware gereinigt ist.

5.3 Sicheres Hochfahren und kundenspezifische Firmwarezertifikate

Ein sicherer Bootvorgang macht das Produkt zwar sicherer, verringert aber auch die Flexibilität bei unterschiedlicher Firmware, wodurch es komplizierter wird, temporäre Firmware, wie z. B. Test-Firmware oder andere kundenspezifische Firmware von Axis, in das Produkt zu laden. Axis hat jedoch einen Mechanismus implementiert, der einzelnen Einheiten die Genehmigung erteilt, solche nicht serienmäßige Firmware zu akzeptieren. Diese Firmware wird auf andere Weise protokolliert, wobei sowohl der Besitzer als auch Axis die Freigabe durchführen und ein benutzerdefiniertes Firmware-Zertifikat erstellen. Nach dem Installieren auf den zugelassenen Geräten ermöglicht das Zertifikat das Verwenden von benutzerdefinierter Firmware, die nur auf der zugelassenen Einheit ausgeführt werden kann. Verwendet werden dabei die eindeutige Seriennummer und die Chip-ID. Benutzerdefinierte Firmwarezertifikate können nur von Axis erstellt werden, da Axis den Schlüssel zum Signieren besitzt.

6 Sicherheit privater Schlüssel

Die Geräte von Axis unterstützen HTTPS (Netzwerkverschlüsselung) und 802.1X (Netzwerkzugangskontrolle), die beide TLS (Transport Layer Security) verwenden. Die digitalen Zertifikate von TLS verwenden ein öffentliches/privates Schlüsselpaar. Der private Schlüssel wird auf dem Gerät gespeichert, während der öffentliche Schlüssel im Zertifikat enthalten ist. Wenn weder HTTPS noch 802.1X verwendet wird, sind keine zu schützenden Schlüssel vorhanden.

Ein Angreifer könnte versuchen, den privaten Schlüssel und das Zertifikat aus dem Gerät zu extrahieren und auf einem angreifenden Computer zu installieren. Im Falle von HTTPS könnte dieser private Schlüssel verwendet werden, um verschlüsselten Datenverkehr über das Netzwerk zwischen dem Gerät und dem VMS abzuhören. Beim Netzwerk-Spoofing könnte der angreifende Computer Zugang zum VMS erhalten, indem er vorgibt, ein legitimes Gerät zu sein. Im Fall von 802.1X könnte der Angreifer den privaten Schlüssel verwenden, um Zugriff auf ein 802.1X-geschütztes Netzwerk zu erhalten, wobei 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 ausreichend, da das Konto nicht leicht kompromittiert werden kann. Zertifikate können widerrufen werden, wenn eine Kompromittierung vermutet wird, wodurch der private Schlüssel unbrauchbar wird.

Bei einigen Endbenutzern kritischer Systeme besteht ein erhöhtes Risiko, dass Angreifer durch ausgefeilte Taktiken versuchen, das Gerät zu knacken, um den privaten Schlüssel zu extrahieren. Ein TPM speichert den Schlüssel so, dass es nahezu unmöglich ist, ihn zu extrahieren, selbst wenn das Gerät kompromittiert ist.

6.1 Sichere Speicherung von Schlüsseln mit einem TPM (Trusted Platform Module)

Ein TPM ist eine Komponente mit einem bestimmten Satz von kryptographischen Merkmalen, die geeignet sind, Informationen vor unbefugtem Zugriff zu schützen. Der private Schlüssel wird im TPM gespeichert und verbleibt dauerhaft im TPM. 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 TPMs verlässt und auch im Falle einer Sicherheitsverletzung sicher bleibt.

6.2 FIPS 140-2-Zertifizierung

Für einige Produkte und Anwendungsfälle gelten möglicherweise gesetzliche Bestimmungen, ein TPM zum Schutz von Informationen zu verwenden. Teilweise muss zusätzlich FIPS 140-2 eingehalten werden. 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 stellt sicher, dass das Modulsystem und die Kryptographie des Moduls korrekt implementiert sind. Die Zertifizierung erfordert die Beschreibung, Spezifizierung und Verifizierung des kryptografischen Moduls, zugelassener Algorithmen, zugelassener Betriebsarten und Einschalttests.

Ausführliche Informationen über die Zertifizierungsanforderungen von FIPS 140-2 finden Sie auf der NIST-Website unter *https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards*.

6.2.1 Zertifiziertes TPM in Axis Produkten

Das in ausgewählten Produkten von Axis verwendete TPM ist gemäß den Anforderungen von FIPS 140-2 zertifiziert. Das TPM verfügt über die Sicherheitsstufe 2 des Standards und erfüllt unter anderem auch die Anforderungen für rollenbasierte Autorisierung und Manipulationsschutz.

7 IEEE 802.1AR – Geräteverifizierung mit der Axis Geräte-ID

Eine Person, die ein Netzwerkgerät von Axis kauft, kann dieses vor der Inbetriebnahme manuell prüfen. Durch eine Sichtprüfung des Produkts kann sich der Kunde aufgrund von Vorkenntnissen über das Aussehen und die Handhabung von Axis Produkten davon überzeugen, dass das Produkt tatsächlich von Axis stammt. Diese Art der Inspektion kann jedoch nur durchgeführt werden, wenn die Person physischen Zugang zum Produkt hat. Wenn Sie über ein Netzwerk mit einem nicht bereitgestellten Produkt kommunizieren, wie können Sie sicher sein, dass Sie mit dem richtigen Gerät kommunizieren? Wie können Sie sicher sein, dass das Gerät nicht unautorisiert ausgetauscht wurde? Eine physische Inspektion kann weder über Netzwerkgeräte noch über auf Servern befindliche Software durchgeführt werden. Als

Sicherheitsmaßnahme wurde die Kommunikation mit einem neuen Produkt bisher zunächst über ein geschlossenes Netzwerk, in dem das Gerät sicher bereitgestellt werden kann, getestet.

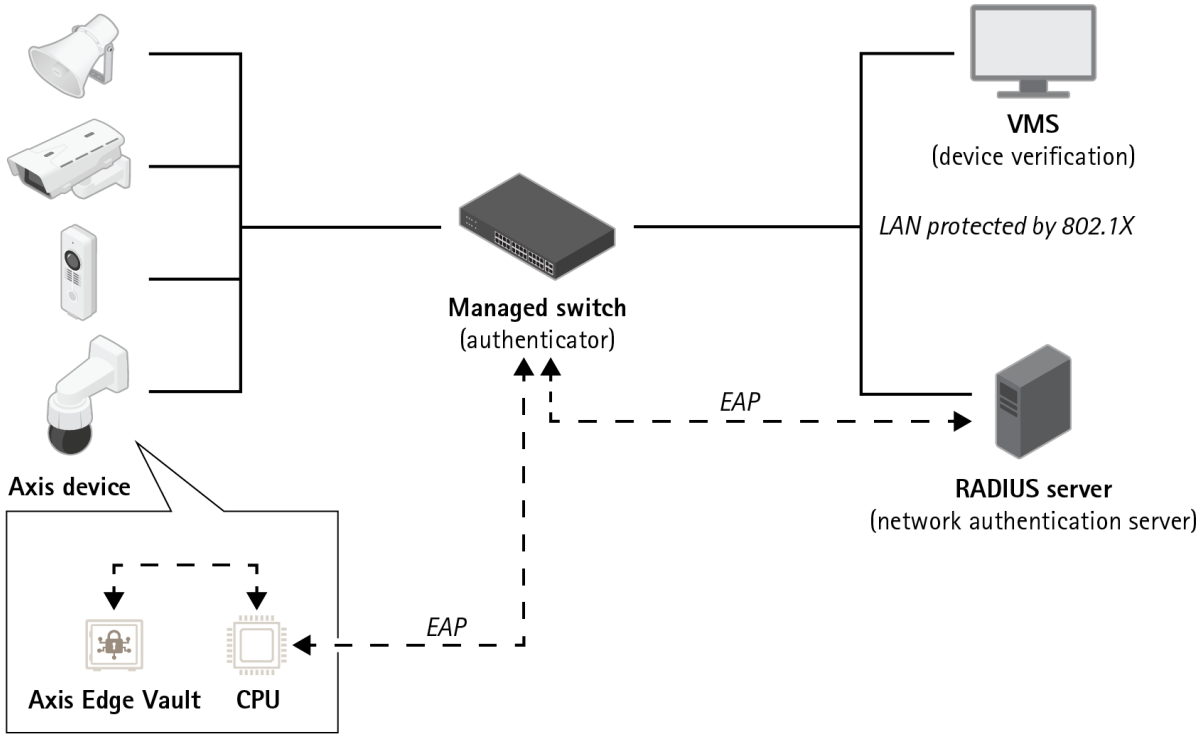

Figure 4. Kunden können ihren Authentifizierungsserver anweisen, gekaufte Axis Produkte unter Verwendung der Geräteseriennummern und der Axis Geräte-ID automatisch im Netzwerk zu akzeptieren.

Der neue internationale Standard IEEE 802.1AR (*https://1.ieee802.org/security/802-1ar/*) definiert ein Verfahren, wie die Identifizierung eines Geräts über ein Netzwerk automatisiert und gesichert werden kann.

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

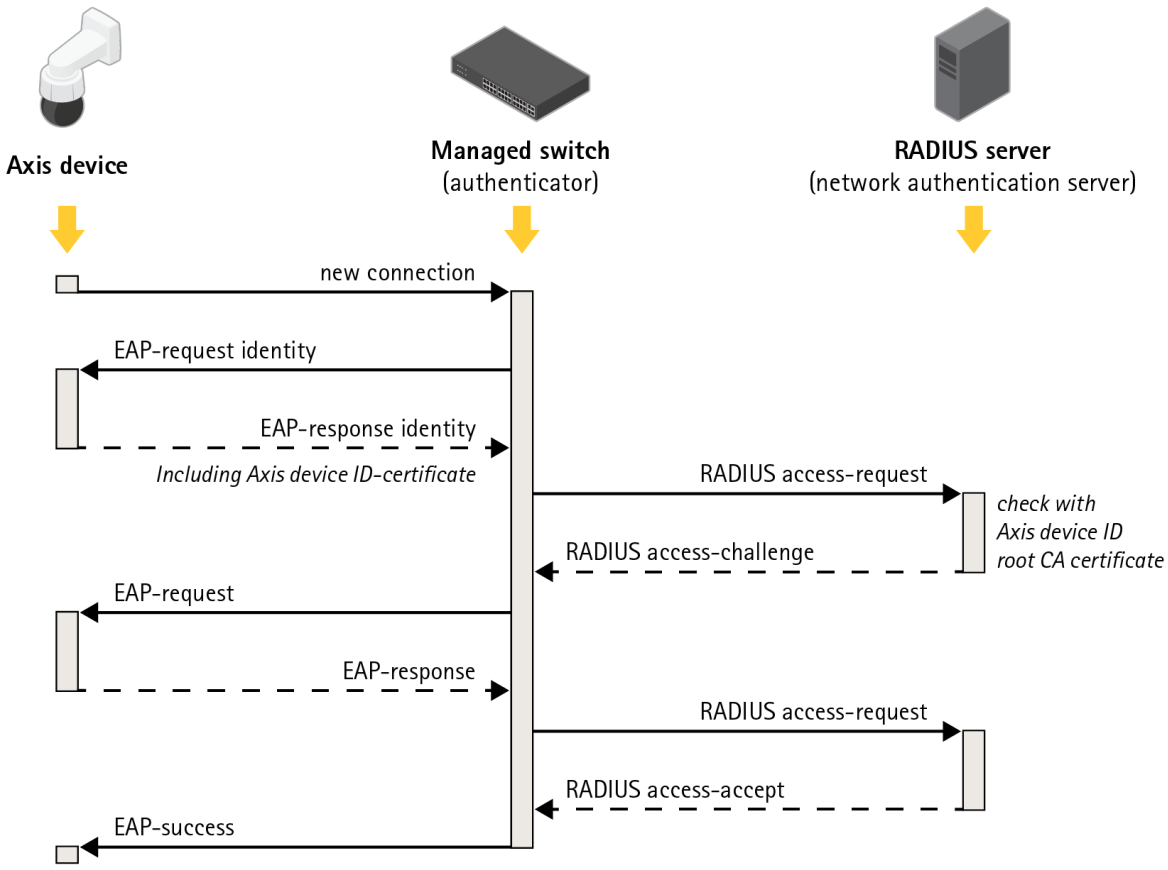

Figure 5. IEEE 802.1AR definiert ein Verfahren für die Identifizierung eines Geräts über ein Netzwerk mit einem Protokoll. Das Protokoll sendet EAP-Anforderungen (Extensible Authentication Protocol) an den Switch, der mithilfe von RADIUS-Anforderungen (Remote Authentication Dial-In User Service) Zugriff gewährt.

In den Produkten von Axis werden diese Sicherheitsmaßnahmen durch die Verwendung von Axis Edge Vault und der Axis Geräte-ID implementiert. Axis Edge Vault ist ein sicheres Modul, in dem die Axis Geräte-ID, eine Sammlung von Zertifikaten zur Verifizierung der Geräteidentifikation, gespeichert ist. Diese Funktionen liefern Ihrem Netzwerk einen kryptografisch verifizierbaren Nachweis, dass ein bestimmtes Gerät von Axis hergestellt wurde und dass die Netzwerkverbindung zu diesem Gerät tatsächlich von genau diesem Gerät bedient wird.

Ein Gerät mit Axis Geräte-ID wurde im Werk bereitgestellt (mit Schlüsseln und Zertifikaten). Über diese Bereitstellung kann der Kunde später das Gerät vor Ort mit anderen Schlüsseln und/oder Zertifikaten ausstatten, die ihm den Zugriff auf einige der Netzwerkressourcen des Kunden ermöglichen.

Durch die Identifizierung des Geräts mit der Axis Geräte-ID kann die Zeit für die Bereitstellung von Geräten verkürzt werden, da vor der Installation und Konfiguration des Geräts im vorgesehenen Netzwerk weniger Arbeiten an dem Gerät durchgeführt werden müssen. Ein weiterer Vorteil ist, dass die Axis Geräte-ID nicht nur eine zusätzliche, integrierte Vertrauensquelle darstellt, sondern auch die Möglichkeit bietet, die Geräte in einem großen System zu verfolgen.

7.1 Axis Edge Vault

Axis Edge Vault ist ein sicheres kryptografisches Berechnungsmodul in Form eines Chips, der auf der Leiterplatte des Produkts montiert ist. Edge Vault hat die Möglichkeit, Zertifikate sicher zu speichern und kann für kryptographische Operationen in sicher gespeicherten Zertifikaten verwendet werden.

In Edge Vault gespeicherte Zertifikate müssen diesen sicheren Speicherort bei einer Verwendung durch das Gerät nicht verlassen. Sie verbleiben auch bei einer Verwendung sicher im Edge Vault, da die kryptografische Hardware, die mit dem Schlüssel arbeitet, auf demselben physischen Chip installiert ist.

7.2 Axis Geräte-ID

Während der Produktion eines Axis Netzwerkgeräts wird ein „digitaler Pass", die Axis Geräte-ID, sicher im Axis Edge Vault des Geräts installiert. Diese Identität ist für jedes Gerät eindeutig und soll die Herkunft des Geräts belegen. Die Axis Geräte-ID ist eine Sammlung von Zertifikaten, die im kryptografischen Teil des Moduls verwendet wird, um Herausforderungen, die durch die eingebettete Produktfirmware entstehen, an Edge Vault zu signieren. Die Antwort von diesem Vorgang wird an den Empfänger zurückgesendet, der die öffentlichen Schlüssel von Axis verwenden kann, um die Authentifizierung der Antwort zu validieren.

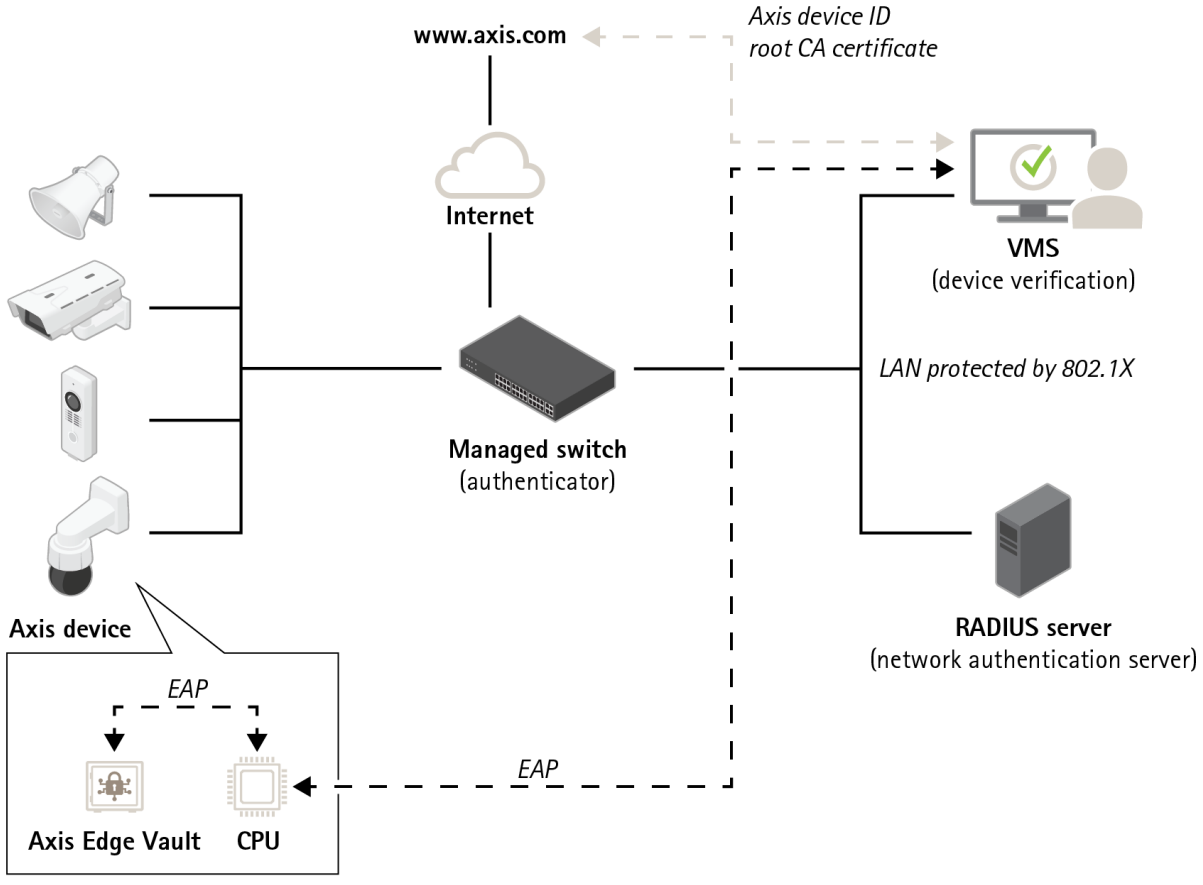

Figure 6. Softwareanwendungen in anderen Teilen des Systems können die Axis Geräte-ID und kryptografische Operationen verwenden, um zu überprüfen, mit wem sie kommunizieren. Die Axis Geräte-ID wurde durch das öffentliche Axis Geräte-ID-Root-CA-Zertifikat von axis.com verifiziert.

7.2.1 Zertifikatshierarchien

Ein Zertifikat ist ein kleiner Datensatz, das einen öffentlichen Schlüssel und Metadaten mit einer Beschreibung des Schlüssels zusammen mit einer Signatur des Ausstellers zur Bestätigung der Gültigkeit des Zertifikats kombiniert.

Eine Zertifikatshierarchie ist eine Möglichkeit, die Herkunft des Zertifikats nachzuweisen. Lassen Sie uns als Beispiel die Axis Geräte-ID mit einem Reisepass vergleichen. Wenn Sie einen Reisepass besitzen, versichert die Regierung Ihres Landes, dass Sie tatsächlich die Person sind, für die der Reisepass Sie ausgibt. Auf ähnliche Weise werden alle Axis Geräte-ID-Zertifikate 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 Netzwerksicherheitssystem darauf, dass das Axis Geräte-ID-Root-CA-Zertifikat das Axis Zertifikat eines mit dem Netzwerk verbundenen Geräts korrekt verifiziert hat.

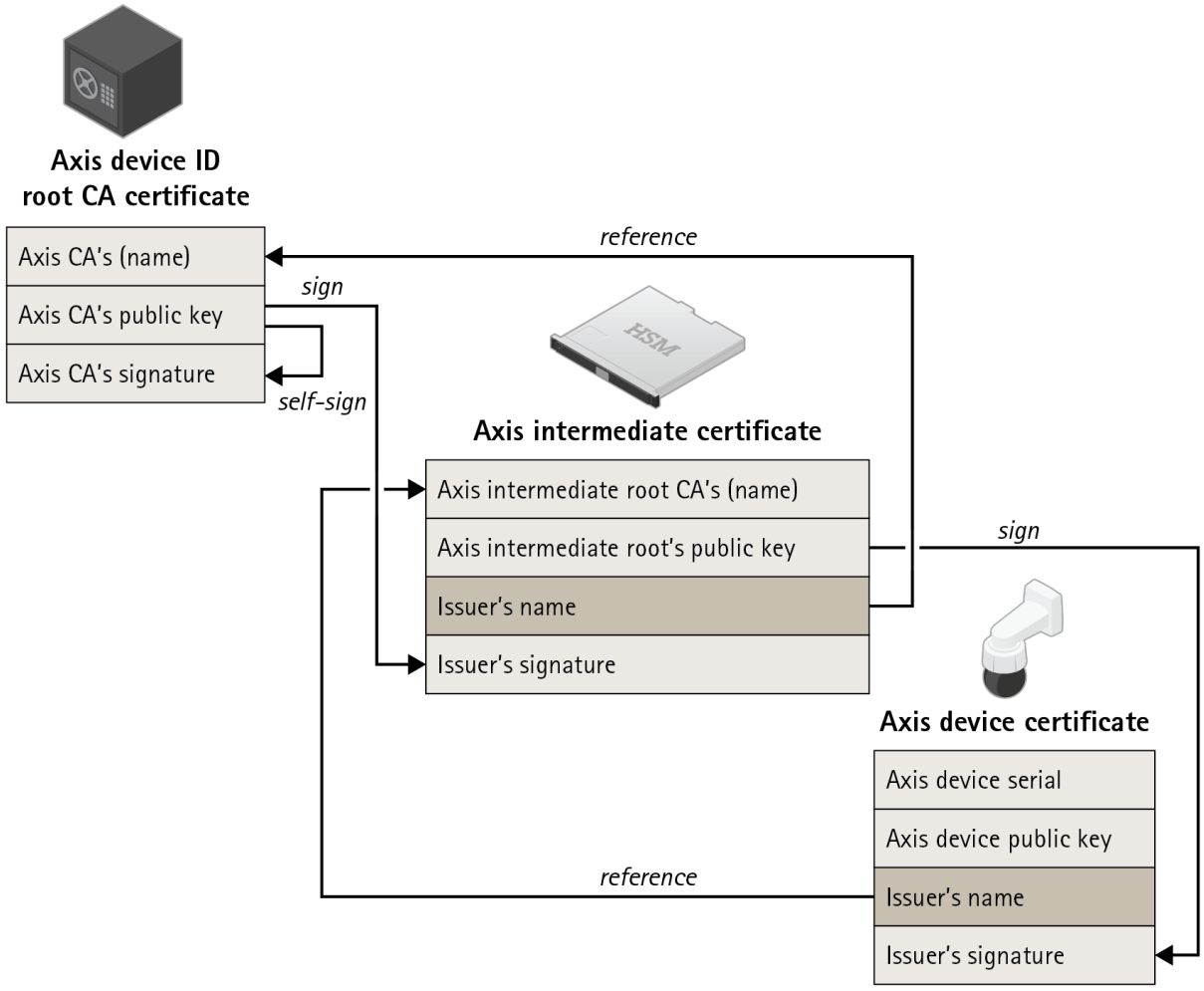

Figure 7. Die Axis Geräte-ID, bei der es sich um ein Zertifikat mit der Seriennummer des Produkts handelt, wird von einem Zwischenzertifikat signiert, das vom Axis Root-Zertifikat unterzeichnet wurde. Da das Axis Root-Zertifikat sehr wertvoll ist und in einem Safe aufbewahrt werden muss, wird das Zwischenzertifikat bei der Bereitstellung im Werk benötigt.

T10154694/DE/M1.8/2007

Informationen zu 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 über Axis finden Sie unter *axis.com*.

AXIS COMMUNICATIONS