签名固件、安全启动和私钥提供的安全性

安讯士产品的网络安全功能

7月 2020

AXIS COMMUNICATIONS

目录

1 概要

本文档描述了可降低网络威胁和应对特定类型攻击的 Axis 产品中的一些可用功能。 这些功能包括：

- 签名固件
- 安全启动
- 受信任的平台模块（TPM）
- 带 Axis 设备 ID 的 Axis Edge Vault。

概述中的威胁包括：

- 固件篡改
- 供应链篡改
- 私钥提取
- 未授权设备更换。

1.1 签名固件

已签名的固件由软件供应商实施，并使用私钥对固件映像进行签名。 当固件附加有此签名时，设备将在接受安装前验证固件。 如果设备侦测到固件完整性受损，固件升级将被拒绝。

1.2 安全启动

安全启动是一种由加密验证软件的完整的链组成的引导过程，可从不可变的内存（引导 ROM）开始。 安全启动基于签名固件的使用，可确保设备仅能使用已授权的固件启动。

1.3 TPM

TPM 是一种提供加密功能集的组件，适用于保护信息以防未经授权的访问。 私钥存储在 TPM 中，需要使用私钥的加密操作都将发送到 TPM 进行处理。 这可确保即使在安全破坏的情况下，证书的机密部分也会保持安全。 在选定的 Axis 产品中使用的 TPM 经过认证，能够满足 FIPS 140–2 的要求。

1.4 带 Axis 设备 ID 的 Axis Edge Vault

新的国际标准 IEEE 802.1 AR 描述了如何通过网络对设备进行自动化和安全识别的过程。 在 Axis 产品中，通过使用 Axis Edge Vault 及 Axis 设备 ID 来实施这些安全措施。 Edge Vault 可用于安全存储的证书上运行的加密挑战。 证书的私有部分即使在使用时也会保留在 Edge Vault 中。 作为由 Axis 根证书签署的证书，Axis 设备 ID 安全且永久地存储在 Edge Vault 中，这可通过产品生命周期实现新的设备信任级别。

2 词汇表

证书– 在加密中，证书是一个签名的文档，以验证是密钥对的来源和属性。 证书由证书颁发机构（CA）签名，如果系统信任 CA，则它还将信任其颁发的证书。

证书颁发机构（CA） – 证书链的信任根。 它用于证明底层证书的真实性和正确性。

FIPS– 联邦信息处理标准、NIST（国家标准和技术协会）在美国发布的数据加密和数据安全的标准。

不可变 ROM– 安全存储受信任公钥和用于比较签名的程序，以使其不被覆盖。

资源调配 – 为网络准备和装配设备的过程。 这包括将配置数据和策略设置从一个中心点提供给设备。 设备随附有密钥和证书。

公钥加密 – 一种非对称加密系统，人人都可以使用接收者的*公钥*加密消息，但只有接收方*（使用私钥）*才能解密消息。 可用于加密和签名信息。

TLS – 传输层安全性，用于保护网络流量的互联网标准。 TLS 提供 HTTPS 中的 S（安全）。

3 简介

Axis 采用业界领先做法来管理和响应我们产品中的安全漏洞，以尽可能地降低客户的网络风险影响。 无法确保产品和服务不存在被恶意攻击利用的缺陷。 这并非 Axis 特有，而是网络设备的普遍状况。 Axis 可保证的是，我们在每个可能的阶段进行共同工作，以确保与您的 Axis 设备和服务相关的风险更小。

有关产品安全性和发现的漏洞信息，请参见 *www.axis.com/support/product-security* 。 有关您可以采取的降低常见威胁风险措施的更多信息，请从 *www.axis.com/cybersecurity* 下载 Axis 强化指南。

本白皮书提供了一些貌似真实的网络攻击以及如何在 Axis 产品中加以避免。 它具体描述功能签名固件和安全启动如何防止固件篡改和供应链篡改。 我们还讨论了如何使用均可用于保护私钥安全的受信任的平台模块（TPM）和 Axis Edge Vault。 Axis Edge Vault 用于安全存储 Axis 设备 ID，从而实现了新的设备信任级别。

4 固件篡改侦测

攻击者在其他入侵系统尝试失败后可能利用的攻击媒介之一，是让系统拥有者安装更改过的应用、固件或其他软件模块。 修改后的软件可能包含具有特定用途的恶意代码。 我们的一个常见建议是不安装来源不完全信任的软件。 在视频系统上下文中，可能有一个“中间人”，可改变设备固件并引诱终端用户进行安装。 这不是一种简单的操作，攻击者需要具有技能且很坚决。 他需要详细地了解 Axis 固件设计以及固件如何在设备上运行。 但是，如果攻击特定系统的价值足够高，则可能会存在这些攻击者。 常见的计数器测量值是供软件供应商使用已签名的固件。

4.1 固件签名

签名固件由软件供应商实施，它使用私钥（密码）来对固件映像进行签名。 当固件附加有此签名时，设备将在接受安装前验证固件。 如果设备侦测到固件完整性受损，固件升级将被拒绝。

签名固件的过程是通过计算加密哈希值来启动的。 在将签名附加到固件图像之前，该值使用私钥/公钥对的私钥进行签名。

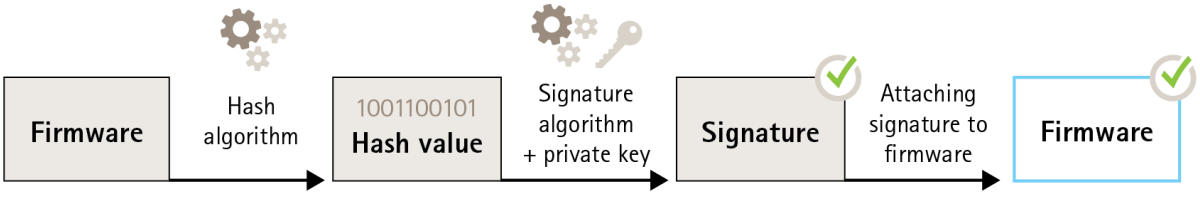

Figure 1. 签名固件的过程。

在升级固件之前，必须验证新固件。 为了确保新固件不被修改，公钥（包含在 Axis 产品中）用于确认是否已使用匹配的私钥对哈希值进行了签名。 此外，通过计算固件的哈希值，并将其与签名中经过验证的哈希值进行比较，可以验证固件的完整性。

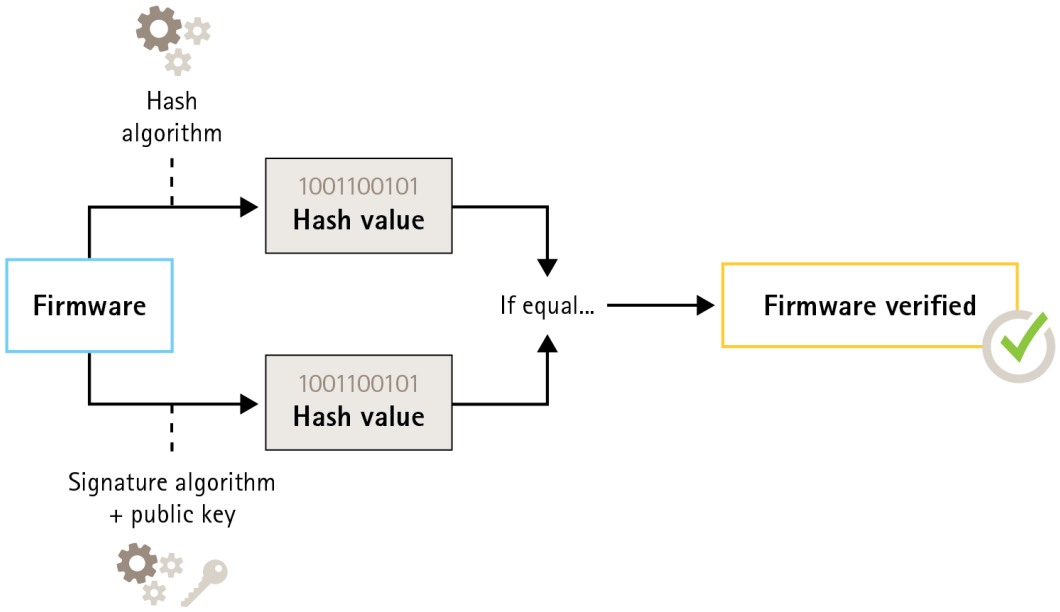

Figure 2. 验证已签名固件的过程。

4.2 Axis 的签名固件

Axis 签名固件基于业界认可的 RSA 公钥加密方法。 当公钥嵌入安讯士设备时，私钥存储在安讯士密切保护的位置。 对图像内容的签名可确保整个固件图像的完整性。 主签名验证多个二次签名，在图像解压缩时加以验证。

5 供应链篡改预防

固件签名可在未来固件更新中保护设备免于安装受损固件。 但是，如果中间人在供应商和终端用户之间改变了设备，该怎么办呢？ 在传输期间能够物理访问设备的攻击者可能会执行攻击，例如，降低设备的启动分区，从而绕过固件完整性检查，以便在部署设备之前安装已更改的恶意固件。

5.1 安全启动

安全启动是一种由加密验证软件的完整的链组成的引导过程，可从不可变的内存（引导 ROM）开始。 安全启动基于签名固件的使用，可确保设备仅能使用已授权的固件启动。

启动 ROM 验证启动程序时启动引导过程。 安全引导，然后以实时的方式验证从闪存中加载的每个固件块的嵌入式签名。 启动 ROM 是信任的根，仅在验证每个签名时，才会继续执行启动过程。 链的每个部分都验证下一部分，导致已验证的 Linux 内核和经验证的根文件系统。

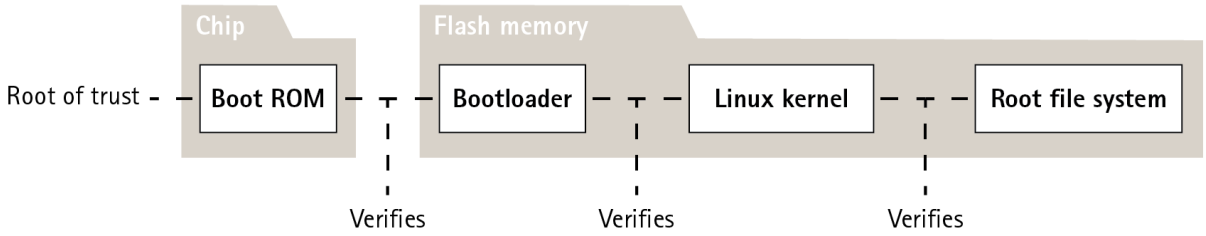

Figure 3. 安全启动过程。

5.2 Axis 安全启动

在许多设备中，低级功能不可能改变，这一点很重要。 当其他安全机制构建在较低级别软件之上时，安全启动可用作安全基层，以保护这些机制避免被规避。

对于具有安全启动功能的设备，闪存中已安装的固件会受到保护，无法进行修改。 出厂默认图像受保护，而配置仍保持不受保护。 在出厂默认设置下，安全启动可保证 Axis 设备完全远离可能的恶意软件。

5.3 安全启动和自定义固件证书

尽管安全启动使产品更加安全，但它同时降低了其他固件的灵活性，从而让在产品中加载临时固件（如测试固件或 Axis 的其他自定义固件）的过程变得更复杂。 不过，安讯士已经实施了一种机制，可批准各个单元来接受此类非生产固件。 此固件以不同方式签名，由拥有者和安讯士审批，生成自定义固件证书。 当安装在已批准的单元中时，证书支持使用仅可在获批单元上运行的自定义固件（根据其唯一序列号和芯片 ID）。 自定义固件证书只能由安讯士创建，因为安讯士持有对其进行签名的密钥。

6 私有密钥的安全性

Axis 设备支持 HTTPS（网络加密）和 802.1X（网络访问控制），两者均使用 TLS（传输层安全）。 TLS 的数字证书使用公共/专用密钥对。 私钥存储在设备中，而公钥则包含在证书中。请注意，如果不使用 HTTPS 或 802.1X，则没有要保护的密钥。

攻击者可尝试从设备提取私钥和证书，并将其安装在攻击计算机上。 对于 HTTPS，该私钥可用于窃取设备和 VMS 之间加密网络流量。 或者，在进行网络欺骗，攻击电脑可通过假装成为合法设备来获得对 VMS 的访问权。 在 802.1X 的情况下，攻击者可使用私钥获得对 802.1X 保护网络的访问权限，并伪装成受信任的设备。

证书和私钥通常存储在设备的文件系统中，由帐户访问策略保护并在正常计算环境下使用。在大多数情况下，这是足够的，因为帐户不会轻易受到损害。 请注意，如果怀疑有安全漏洞，则可吊销证书，从而使私钥毫无用处。

一些关键系统的终端用户可能会带来更大的风险，即坚决并熟练的攻击者试图破坏设备以提取私钥。 受信任的平台模块（TPM）以接近无法解压缩的方式存储密钥，即使设备遭到破坏。

6.1 采用 TPM（受信任的平台模块）的安全密钥存储

TPM 是一种提供特定加密功能集的组件，适用于保护信息以防未经授权的访问。 私钥存储在 TPM 中，不会离开 TPM。 需要使用私钥的加密操作都将发送到 TPM 进行处理。 这可确保证书的机密部分不会离开 TPM 中的安全环境，即使在发生安全破坏时也保持安全。

6.2 FIPS 140–2 认证

对于某些产品和使用案例，使用 TPM 来保护信息可能是监管要求，有时还与符合 FIPS 140–2 要求相结合 。 FIPS（联邦信息处理标准）140–2是一个由 NIST（美国国家标准和技术协会）在美国发布的加密模块的信息安全标准。

通过 NIST 认证的测试实验室进行验证，确保了模块系统和模块的加密能够正确实施。 简而言之，认证要求加密模块的描述、规格和验证、批准算法、批准的操作模式和电源测试。

有关 FIPS 140–2 认证要求的更多详细信息，请参阅 NIST 网站 *https://csrc.nist.gov/projects/cryptographic–module–validation–program/standards*

6.2.1 Axis 产品中已认证的 TPM

在选定的 Axis 产品中使用的 TPM 经过认证，能够满足 FIPS 140–2 的要求。 更具体地说，它经过了标准安全级别 2 的认证，这意味着 TPM 还满足了基于角色的授权和篡改证据的要求，以及其他要求。

7 IEEE 802.1AR – 具有 Axis 设备 ID 的设备验证

购买 Axis 网络设备的人可在开始使用之前执行手动检查。 通过以视觉方式检查产品并使用有关 Axis 产品外观知识，客户可以确信产品确实源于 Axis。 但是，这种类型的检查只能由对产品有物理访问权限的人来完成。 因此，当您通过网络与未配备的产品通信时，如何确保您能够与正确的设备单元进行通信？ 是否未经授权更换设备？ 网络设备或服务器

上的软件均不能执行物理检查。作为一种安全措施，在关闭的网络上首次与新产品进行交互是很常见的，即可安全地设置单元。

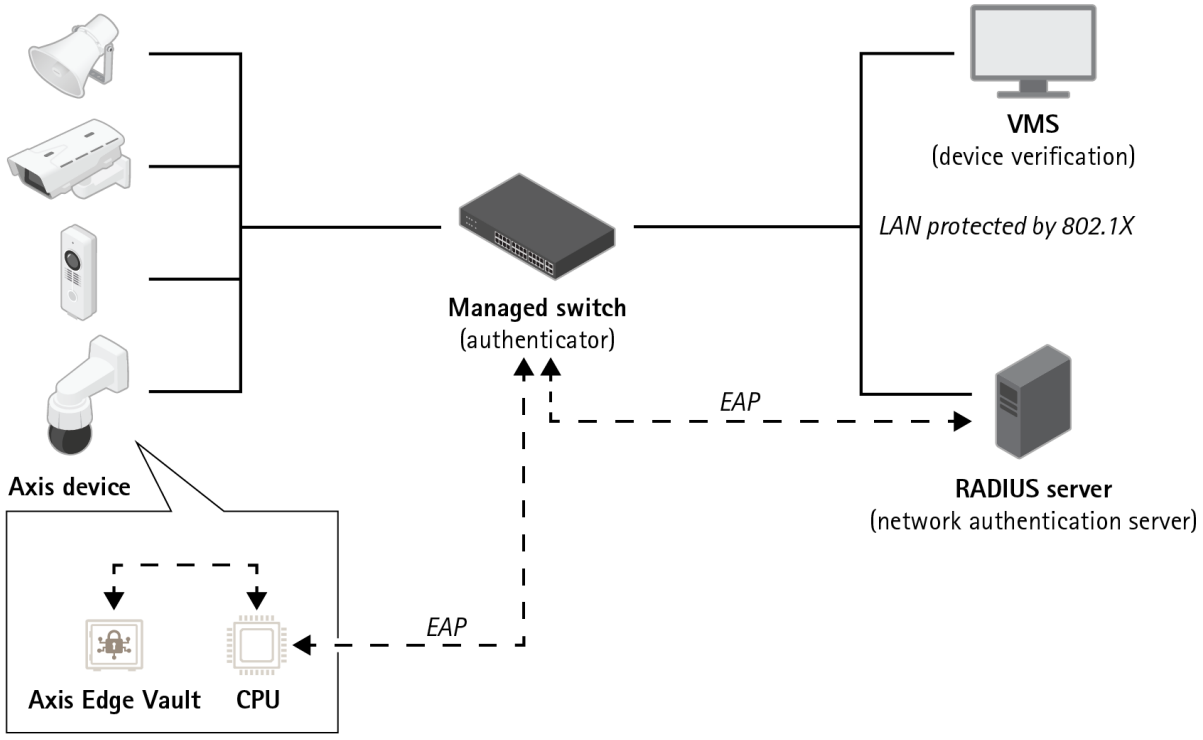

Figure 4. 客户可指示他们的验证服务器使用设备序列号和 Axis 设备 ID 自动接受购买的 Axis 产品连接至网络。

新的国际标准 IEEE 802.1AR（*https://1.ieee802.org/security/802-1ar/*）定义了一种方法，让您能够通过网络自动实现设备的安全识别。 如果将通信转发到嵌入式安全模块，则该单元可根据标准返回可信识别响应。

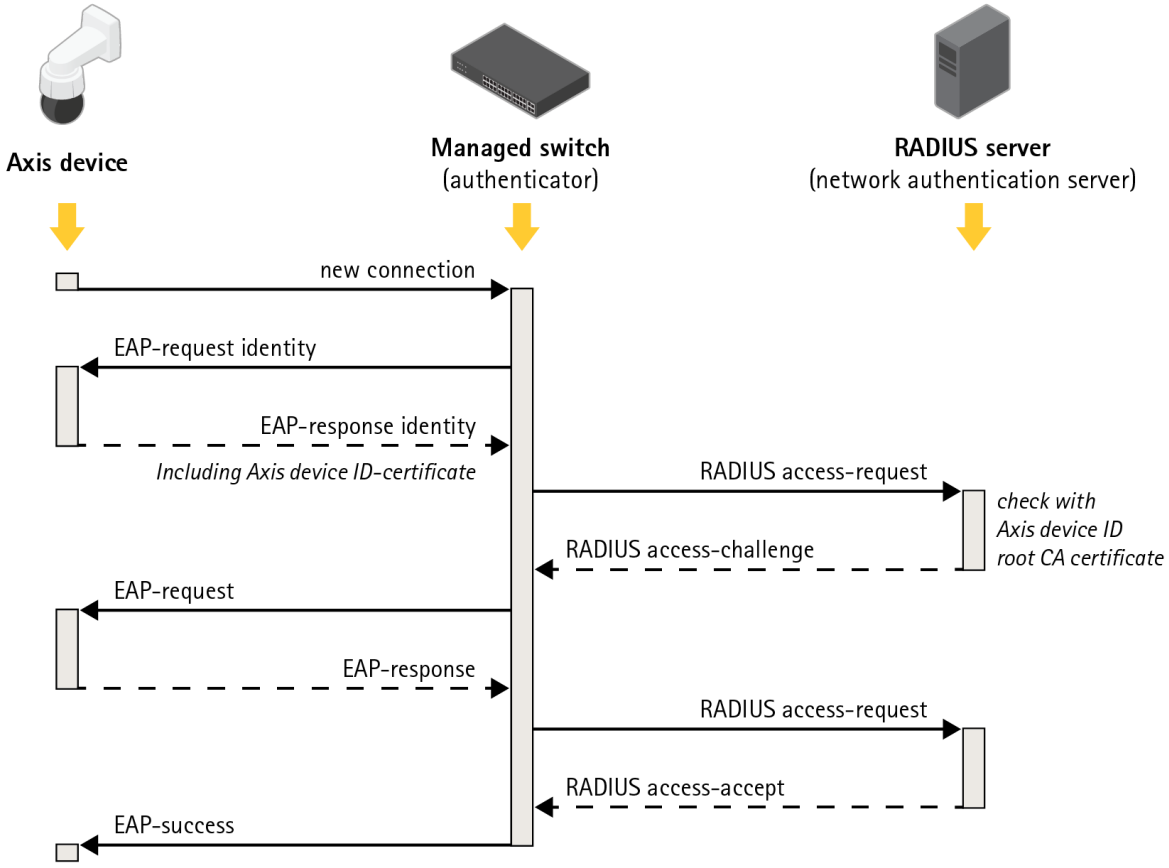

Figure 5. IEEE 802.1AR 通过将可扩展身份验证协议请求（AEP）发送到使用远程身份验证拨入用户服务（RADIUS）请求以授予访问权限的交换机，定义了如何通过网络识别设备的方法。

在 Axis 产品中，通过使用 Axis Edge Vault 及 Axis 设备 ID 来实施这些安全措施。 Axis Edge Vault 是一个安全模块，其中 Axis 设备 ID（用于验证设备识别的证书集合）已安装。 这些功能为您的网络提供了加密的可验证证据，即是由 Axis 生产的特定单元，并且与设备的网络连接确实是由该单元提供的。

出厂时已设置了具有 Axis 设备 ID 的设备（包含密钥和证书）。 该供应可供客户稍后用于使用其他密钥和/或证书进一步调配该设备，让其能够访问客户的某些网络资源。

通过识别具有 Axis 设备 ID 的设备，可降低设备部署时间，因为在预定网络上安装和配置设备之前，需要在设备上完成的工作减少。 另一个优点是 AXIS 设备 ID，除了提供一个额外的内置信任来源外，还提供了一种跟踪大型系统中的设备的方法。

7.1 Axis Edge Vault

Axis Edge Vault 是一种安全加密计算模块，其形式为安装在产品内部的 PCB 上的一个芯片。Edge Vault 有可能安全地存储证书，并可用于安全存储的证书上的加密操作。

存储在 Edge Vault 中的证书无需保留，即可供设备使用。 由于在密钥上操作的加密硬件安装在同一个物理芯片上，因此即使在使用时，它们也会在 Edge Vault 中保持安全。

7.2 Axis 设备 ID

在生产每个 Axis 网络设备单元的过程中，称为 Axis 设备 ID 的”数字护照“会安全地安装在装置的 Axis Edge Vault 中。 该标识对于每个单元都是唯一的，旨在证明设备的来源。 Axis 设备 ID 是在模块的加密操作部分中使用的证书集合，用于签署嵌入式产品固件至 Edge Vault 所呈现的挑战。 此操作的响应将发送回接收器，该接收器可使用 Axis 公钥来验证响应的身份验证。

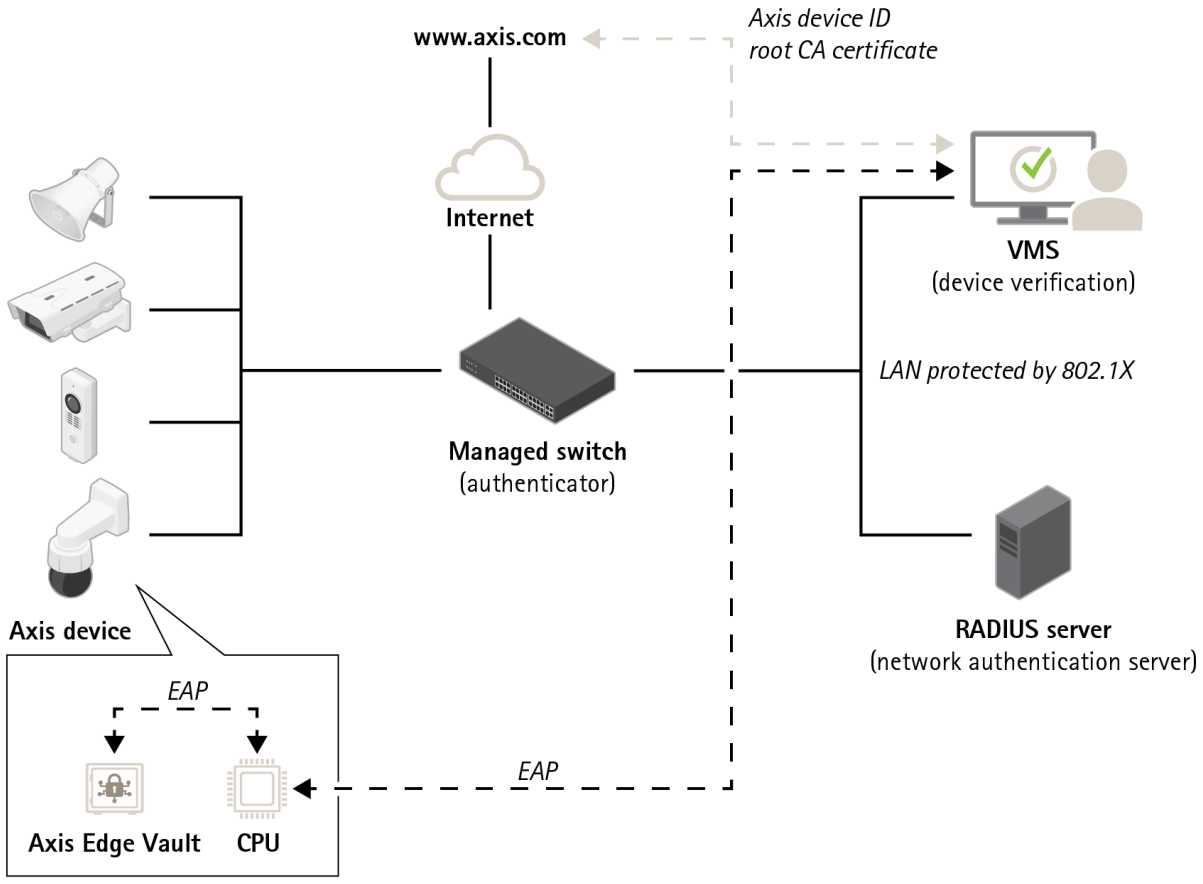

Figure 6. 系统其他部分中的软件应用可使用 Axis 设备 ID 和加密操作来验证与之通信的人员。 Axis 设备 ID 由 axis.com 的公共 Axis 设备 ID 根 CA 证书验证。

7.2.1 证书层次结构

证书是一小部分数据，它将公钥和描述密钥的元数据以及颁发者的签名结合起来证实证书的有效性。

证书层次结构是证明证书出处的一种方式。 让我们考虑一下 Axis 设备 ID 和护照之间的类比 。 如果您拥有护照，则您所在国家/地区的政府保证您实际上是护照所声称的人。 与此类似，Axis 设备 ID 证书由 AXIS 设备 ID 根 CA 证书进行认可。 就像海关信任您的国家/地

区政府正确无误地颁发您的护照一样，网络安全系统信任 Axis 设备 ID 根 CA 证书正确验证了网络连接单元的 Axis 证书。

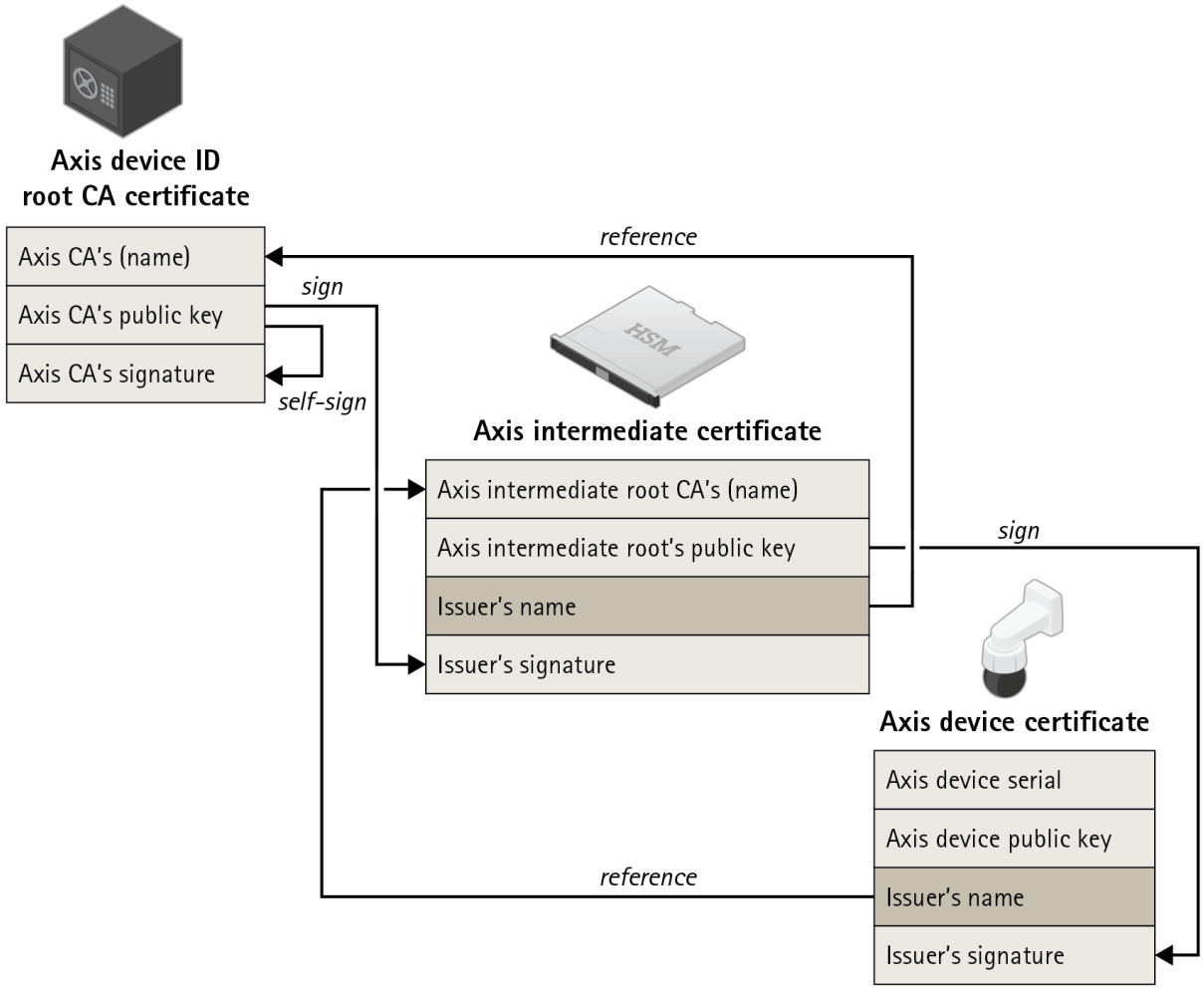

Figure 7. Axis 设备 ID（包含产品序列号的证书）由 Axis 根证书签名的中间证书进行签名。由于 Axis 根证书很重要，需要安全的存储，因此在工厂预配期间需要中间证书。

关于安讯士(Axis Communications)

安讯士通过打造网络解决方案，不断提供改善安防技术的独特见解并引入创新业务模式，旨在创造一个更加智能、安全的世界。作为网络视频行业的领导者，安讯士致力于推出视频监控和分析应用、访问控制以及音频系统的相关产品和服务。

安讯士在全球50多个国家和地区设有办事机构，拥有超过3,500名尽职的员工，并与遍布世界各地的合作伙伴携手并进，为客户带来高价值的解决方案。安讯士创立于1984年，总部位于瑞典。

关于安讯士的更多信息，请访问我们的网站：*axis.com*

©2020 Axis Communications AB. AXIS COMMUNICATIONS、 AXIS 和 VAPIX 均为 Axis AB 的注册商标或正在申请的商标，安讯士公司对其拥有各类管辖权。其它的公司名称和产品均为其各自公司的商标或注册商标。我们保留在未预先通知的情况下提出修改的权利。