白皮书

安讯士产品网络安全功能

— 签名固件

— 安全启动

— Axis Edge Vault

— 安讯士设备ID

— 签名视频

十一月 2021

目录

1 概述 3

1.1 签名固件 3

1.2 安全启动 3

1.3 Axis Edge Vault 3

1.4 安讯士设备ID 3

1.5 签名视频 4

2 词汇表 4

3 引言 5

4 固件篡改侦测 5

4.1 固件签名 5

4.2 安讯士签名固件 6

5 供应链防篡改 6

5.1 安全启动 6

5.2 安讯士安全启动 7

5.3 安全启动和自定义固件证书 7

6 机密信息防篡改 7

6.1 安讯士设备ID 7

7 安全密钥存储 8

7.1 使用Axis Edge Vault安全存储证书 9

7.2 通过TPM (Trusted Platform Module) 进行的安全密钥存储 9

7.3 FIPS 140–2认证 9

8 IEEE 802.1AR – 使用安讯士设备ID进行设备验证 9

9 视频篡改侦测 12

9.1 签名视频 12

1 概述

本文档介绍了安讯士产品中的一些可降低网络威胁并应对特定攻击类型的功能。这些功能包括：

- 签名固件
- 安全启动
- Axis Edge Vault
- 安讯士设备ID
- 签名视频。

文中所述的威胁包括：

- 固件篡改
- 供应链篡改
- 私钥提取
- 未授权设备更换
- 视频篡改。

1.1 签名固件

固件签名由软件供应商执行，软件供应商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，则固件升级将被拒绝。

1.2 安全启动

安全启动是一种由加密验证软件的完整链组成的启动过程，始于不可变的内存（启动ROM）。安全启动基于签名固件的使用，可保证设备只能使用已授权的固件来启动。

1.3 Axis Edge Vault

Axis Edge Vault是一个安全加密计算模块，可用于对安全存储的证书执行加密操作。Edge Vault提供防篡改存储，让设备能够保护其机密信息。它为安全执行更先进的安全功能奠定坚实基础。

1.4 安讯士设备ID

安讯士设备ID的工作方式与数字护照相似，对设备而言具有唯一性。作为经安讯士根证书签名的证书，它被安全且永久地存储在Edge Vault中。安讯士设备ID旨在证明设备来源，保障产品寿命期内的高设备信任级别。

1.5 签名视频

签名视频能够在无需证明视频文件保管链的情况下，证实视频证据未遭到篡改。摄像机使用安全地保存在Axis Edge Vault中的唯一安讯士设备ID将签名添加到视频流中。播放视频时，文件播放器将显示视频是否完好。因此，签名视频让视频追溯可达源头摄像机，并让您能够确定视频在离开摄像机后未遭到篡改。

2 词汇表

证书 – 在加密中，证书是一个签名文档，用于证明是密钥对的来源和属性。证书由证书颁发机构 (CA) 签名，如果系统信任该 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，这些标准是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标准。

不可变ROM – 用于安全存储可信公钥，以及安全存储用于比较签名以使签名无法被覆盖的程序。

预处理 – 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集中提供给设备。设备随附有密钥和证书。

公钥加密 – 一种非对称加密系统，在这种系统中，谁都可以使用接收方的*公钥*来加密消息，但只有接收方才能（使用*私钥*来）解密消息。可用于加密和签名消息。

TLS – 传输层安全，它是一种用于保护网络通信的互联网标准。HTTPS中的S（安全）指的可以是TLS（安全传输层协议）。

3 引言

安讯士依据业界良好做法来管理并应对我们产品中的安全漏洞，尽可能地降低客户遭到攻击的风险。我们无法保证产品和服务毫无可被恶意攻击利用的漏洞。这不是安讯士产品的特有状况，而是网络设备的普遍状况。安讯士可以保证的是，我们在相关阶段通力合作，尽可能降低与安讯士设备和服务相关的风险。

有关产品安全和已发现漏洞的更多信息，请访问*www.axis.com/support/product-security*。如需详细了解针对常见威胁的降低风险措施，请从该网页下载“安讯士强化配置指南”。

本白皮书介绍了一些潜在网络攻击，并介绍了如何在安讯士产品中避免这些攻击。它详细介绍了签名固件和安全启动如何防止固件篡改和供应链篡改。其中还讨论了如何使用可用于保护私钥安全的Trusted Platform Module (TPM) 和Axis Edge Vault。Axis Edge Vault用于安全存储可提高设备信任级别的安讯士设备ID。Axis Edge Vault和安讯士设备ID还让您能够使用签名视频，以便确认视频在离开摄像机后未遭篡改。

4 固件篡改侦测

在以其他方式入侵系统失败后，攻击者可能利用的一种攻击方式是，让系统拥有者安装已遭篡改的应用、固件或其他软件模块。遭篡改的软件可能包含具有特定用途的恶意代码。通常建议从不安装来源不完全可信的软件。就视频系统而言，可能存在一个“中间环节的人”，这个人可能篡改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，攻击者需要技术娴熟且坚持不懈。他需要详细地了解安讯士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，则可能会存在这样的攻击者。针对他们，常见的对策是，软件供应商使用已签名的固件。

4.1 固件签名

固件签名由软件供应商执行，软件供应商使用秘密保管的私钥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，则固件升级将被拒绝。

签名固件的过程通过计算加密哈希值来启动。然后，在将签名附加到固件映像之前，使用公私密钥对中的私钥来对这个值签名。

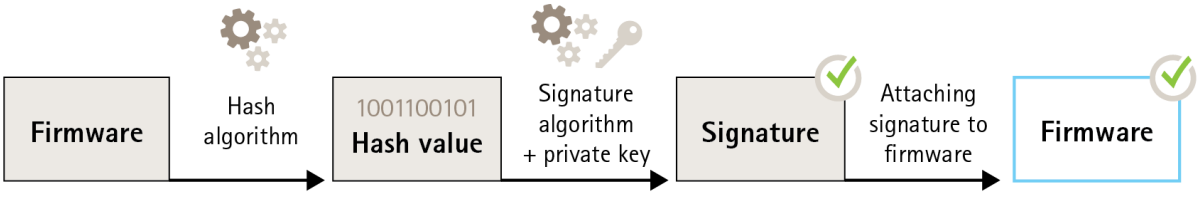

Figure 1. 固件签名过程。

在升级固件之前，必须验证新固件。为了确定新固件未遭到修改，因此使用了公钥（包含在安讯士产品中）来确认确实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。

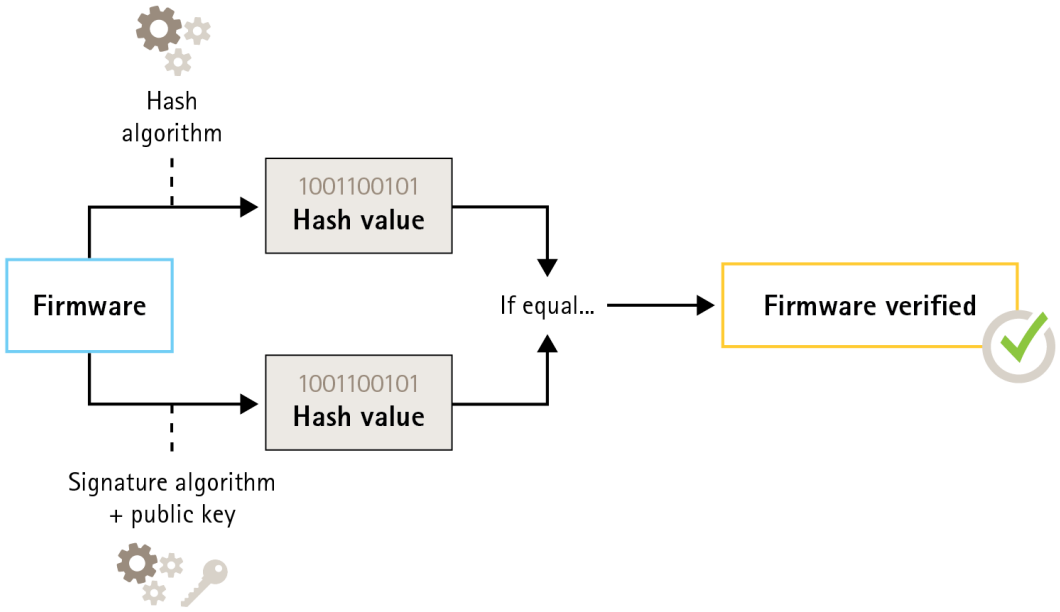

Figure 2. 验证已签名固件的过程。

4.2 安讯士签名固件

安讯士签名固件基于业界认可的RSA公钥加密方法。私钥存储在安讯士内部的受到严格监管的地方，而公钥则嵌入在安讯士设备中。整个固件映像的完整性通过图像内容的签名来保证。一次签名对多个二次签名进行验证，这种验证在图像解压时进行。

5 供应链防篡改

固件签名可在未来固件更新中保护设备免于安装不良固件。但是，如果在从供应商到最终用户的供应链中，有中间环节的人更改了设备，该怎么办呢？在运输期间能够切实接触到设备的攻击者可能会执行攻击，例如，破坏设备的启动分区，从而规避固件完整性检查，以便在部署设备之前安装经篡改的（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链组成的启动过程，始于不可变的内存（启动ROM）。安全启动基于签名固件的使用，可保证设备只能使用已授权的固件来启动。

启动ROM在验证启动程序时，发起启动过程。安全启动，然后实时验证从闪存加载的具体固件模块的嵌入式签名。启动ROM是可信根，只有在验证了全部签名后，才会继续执行启

动过程。链的每个部分都会对下一部分执行身份验证，进而得到经验证的Linux内核和经验证的根文件系统。

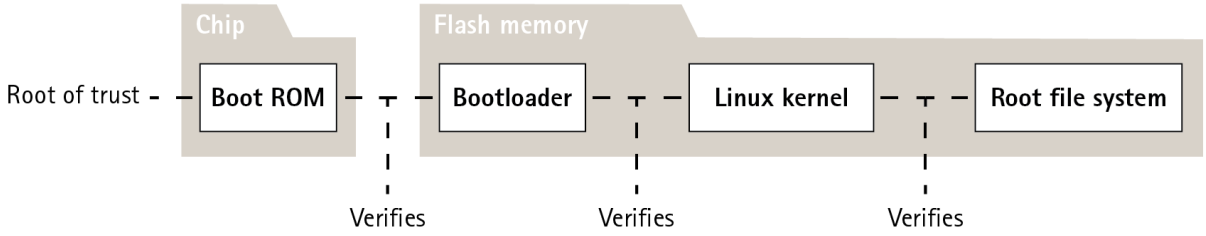

Figure 3. 安全启动过程。

5.2 安讯士安全启动

在许多设备中，低级功能应无法更改。当其他安全机制构建在较低级别的软件之上时，安全启动可用作安全基础层，以免这些机制遭到规避。

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，无法被修改。出厂默认图像受到保护，但配置依然不受保护。在出厂默认设置下，安全启动可保证安讯士设备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，但它同时也降低了在面对不同固件时的灵活适配能力，从而让在产品中加载临时固件（如测试固件或安讯士的其他自定义固件）的过程变得更复杂。不过，安讯士已经实施了一种机制，可批准单个设备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。在安装到经认可的设备中后，该证书让您能够基于唯一序列号和芯片ID来使用只能在这个经认可的设备上运行的自定义固件。自定义固件证书仅可由安讯士创建，因为只有安讯士才拥有相应的签名密钥。

6 机密信息防篡改

安全分布式系统的基本要求是，能够验证连接并防止窃取。这就要求设备使用防篡改安全存储机制来保护其机密信息。Axis Edge Vault就是这样的存储机制，基于这项工具，您能够安全地执行更先进的安全功能。

6.1 安讯士设备ID

在安讯士网络设备的生产期间，在设备的Axis Edge Vault中以安全的方式安装了一个“数字护照”，这个数字护照被称为安讯士设备ID。这个标识对于设备是唯一的，旨在证明设备的来源。安讯士设备ID是在模块的加密操作部分中使用的证书集合，用于以签名的方式证明嵌入式产品固件对Edge Vault所带来的挑战。这个操作的响应将发送回接收方，接收方可使用安讯士公钥来对响应进行身份验证。

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机构的签名相结合，以证实证书的有效性。证书层次结构是证明证书出处的一种方式。

下面来看看安讯士设备ID与护照之间的相似之处。如果您拥有护照，则您所在国家/地区的政府将保证您实际上是护照所声称的人。与此类似，安讯士设备ID证书由安讯士设备ID根CA证书进行签名背书。就像海关相信您的国家/地区政府正确无误地颁发您的护照一样，网络安全系统也相信安讯士设备ID根CA证书正确验证了联网设备的安讯士证书。

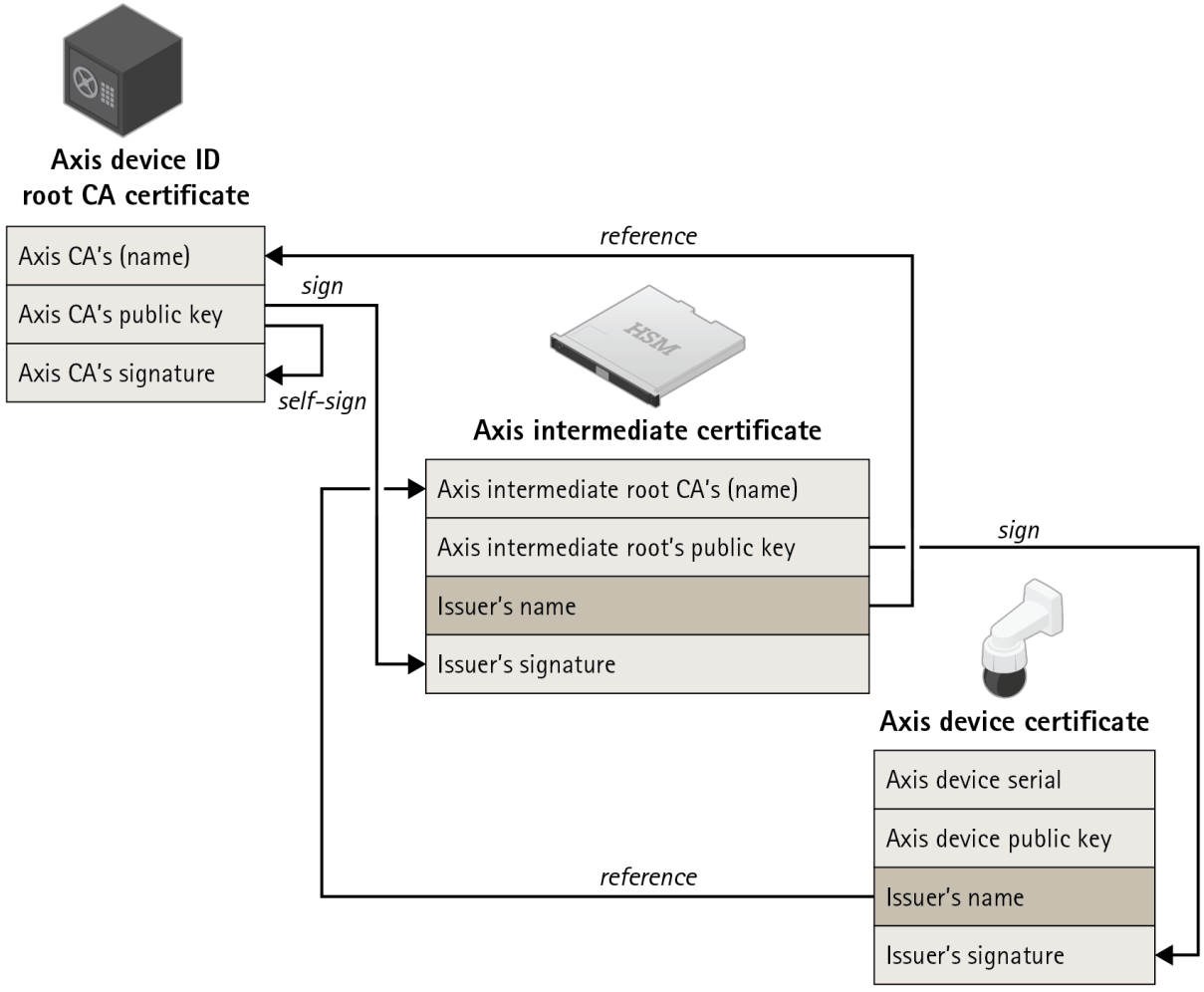

Figure 4. 安讯士设备ID（其为包含产品序列号的证书）由经安讯士根证书签名的中间证书进行签名。由于安讯士根证书非常重要，需要安全地存储，因此在工厂预处理期间需要使用中间证书。

7 安全密钥存储

安讯士设备支持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的数字证书使用公私密钥对。私钥存储在设备中，而公钥则包含在证书中。请注意，如果既不使用HTTPS，也不使用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。在HTTPS环境中，私钥可用于窃听设备与VMS之间的加密网络通信。或者，利用电子欺骗网络，攻击计算机可伪

装成合法设备，从而能够访问VMS。在802.1X环境中，攻击者可使用私钥获得对802.1X保护网络的访问权限，并伪装成可信设备。

证书和私钥通常存储在设备的文件系统中，依据帐户访问策略进行保护，并在正常计算环境下使用。在大多数情况下，其安全性是足够的，因为帐户不会轻易受到破坏。请注意，如果怀疑遭到破坏，则可能撤销证书，从而使私钥毫无用处。

关键系统的某些最终用户可能遭遇较大风险，即，有坚持不懈且技术娴熟的攻击者试图侵入设备以提取私钥。Axis Edge Vault可用于以特定方式存储密钥，从而使设备即便遭到破坏，攻击者也无法提取密钥。

7.1 使用Axis Edge Vault安全存储证书

Axis Edge Vault是一个安全加密计算模块，其形式为安装在产品内部的PCB上的一个芯片。Edge Vaul有可能安全地存储证书，并可用于对安全存储的证书执行加密操作。

存储在Edge Vault中的证书无需离开Edge Vault，便可供设备使用。由于通过密钥运行的加密硬件安装在同一个物理芯片上，因此即使在使用证书时，证书也能够安全地保留在Edge Vault中。

7.2 通过TPM (Trusted Platform Module) 进行的安全密钥存储

TPM是一个提供特定加密功能的组件，适用于保护信息以防未经授权的访问。私钥存储在TPM中，且从不离开TPM。需要使用私钥的加密操作都将发送到TPM进行处理。这保证证书的机密部分不离开TPM中的安全环境，即使是存在安全漏洞的情况下，依然能够保持安全。

7.3 FIPS 140–2认证

对于某些产品和用例，法律法规可能要求使用TPM来保护信息，有时甚至还需要额外遵守FIPS 140–2的要求。FIPS（联邦信息处理标准）140–2是面向加密模块的信息安全标准，由NIST（国家标准和技术协会）在美国发布。

经NIST认证的测试实验室对产品进行检验，保证了模块系统和模块的加密能够正确实施。简言之，要通过认证，必须提供加密模块的描述、规格和验证，以及认可的算法、认可的工作模式和电源测试。

有关FIPS 140–2认证要求的更多详情，请访问NIST网站*www.nist.gov*

7.3.1 安讯士产品中的认证 TPM

安讯士产品中所使用的TPM通过FIPS 140–2认证。具体来讲，已经通过了该标准的2级安全认证，这就意味着，TPM也满足在基于角色的授权和篡改证据等方面的要求。

8 IEEE 802.1AR – 使用安讯士设备ID进行设备验证

购买安讯士网络设备的人可在开始使用之前执行手动检查。通过目检产品，并根据对安讯士产品外观的了解，客户可以确信产品确实来自安讯士。但是，这种类型的检查只能由可切实接触到产品的人来完成。因此，当通过网络与未经预处理的产品进行通信时，该如何保证正在与正

确的设备通信呢？是否未经授权更换了设备？网络设备和服务器上的软件均不能执行物理检查。一个常用的安全措施是，先通过能够安全地完成设备预处理的闭环网络与新产品交互。

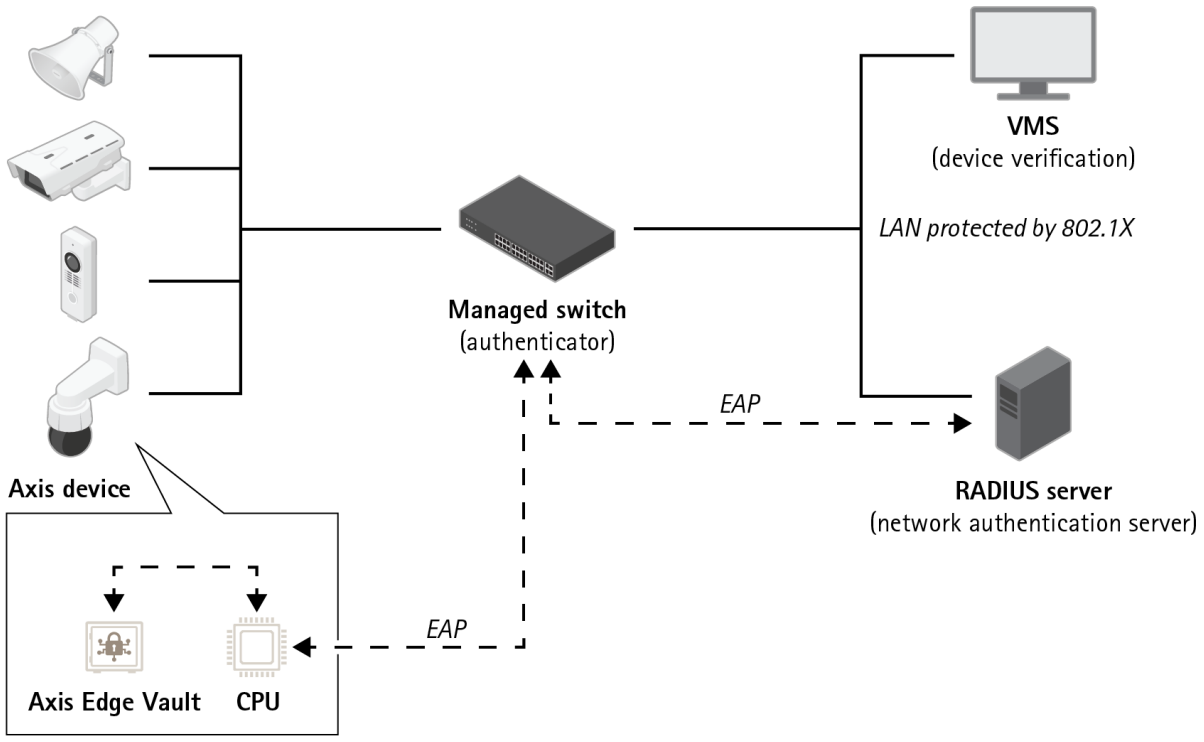

Figure 5. 客户可指示其身份验证服务器使用设备序列号和安讯士设备ID来自动允许所购买的安讯士产品连接至网络。

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

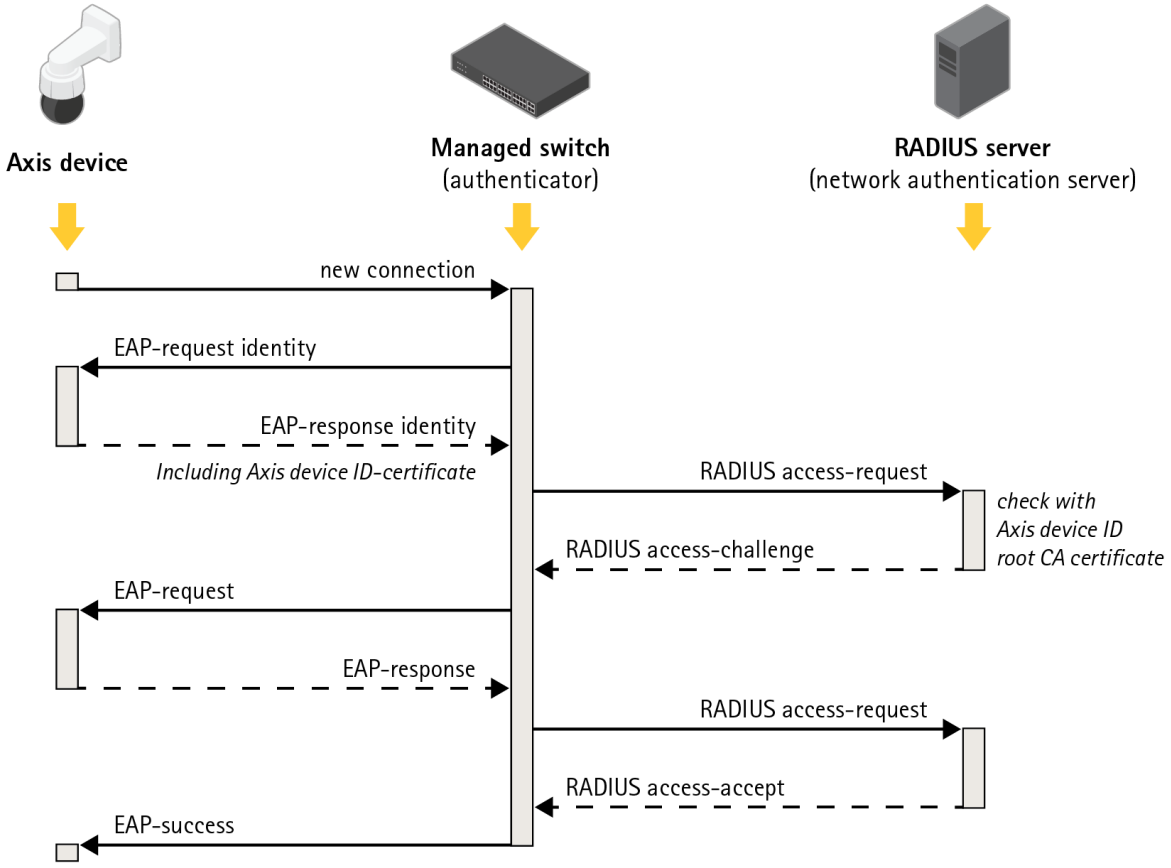

Figure 6. IEEE 802.1AR依据特定协议定义通过网络识别设备的方法，该协议可将可扩展身份验证协议请求 (EAP) 发送到使用远程身份验证拨入用户服务 (RADIUS) 请求来授予访问权限的交换机。

在安讯士产品中，这些安全措施借助Axis Edge Vault和安讯士设备ID来实现。Axis Edge Vault是一个安装有安讯士设备ID（一系列用于验证设备身份的证书）的安全模块。这些功能为您的网络提供了加密的可验证证据，证明特定单元是由安讯士生产的，并且与该设备的网络连接确实由该设备提供。

出厂时，已（使用密钥和证书）对包含安讯士设备ID的设备进行了预处理。这种预处理让客户能够在后期使用其他密钥和/或证书进一步预处理该设备，以便能够访问客户的某些网络资源。

通过使用安讯士设备ID来识别设备，可减少设备部署时间，因为在预期网络上安装和配置该设备之前，需要在设备上完成的工作减少了。另一个优点是，除提供额外的内置信任源之外，安讯士设备ID还让您能够跟踪大型系统中的设备。

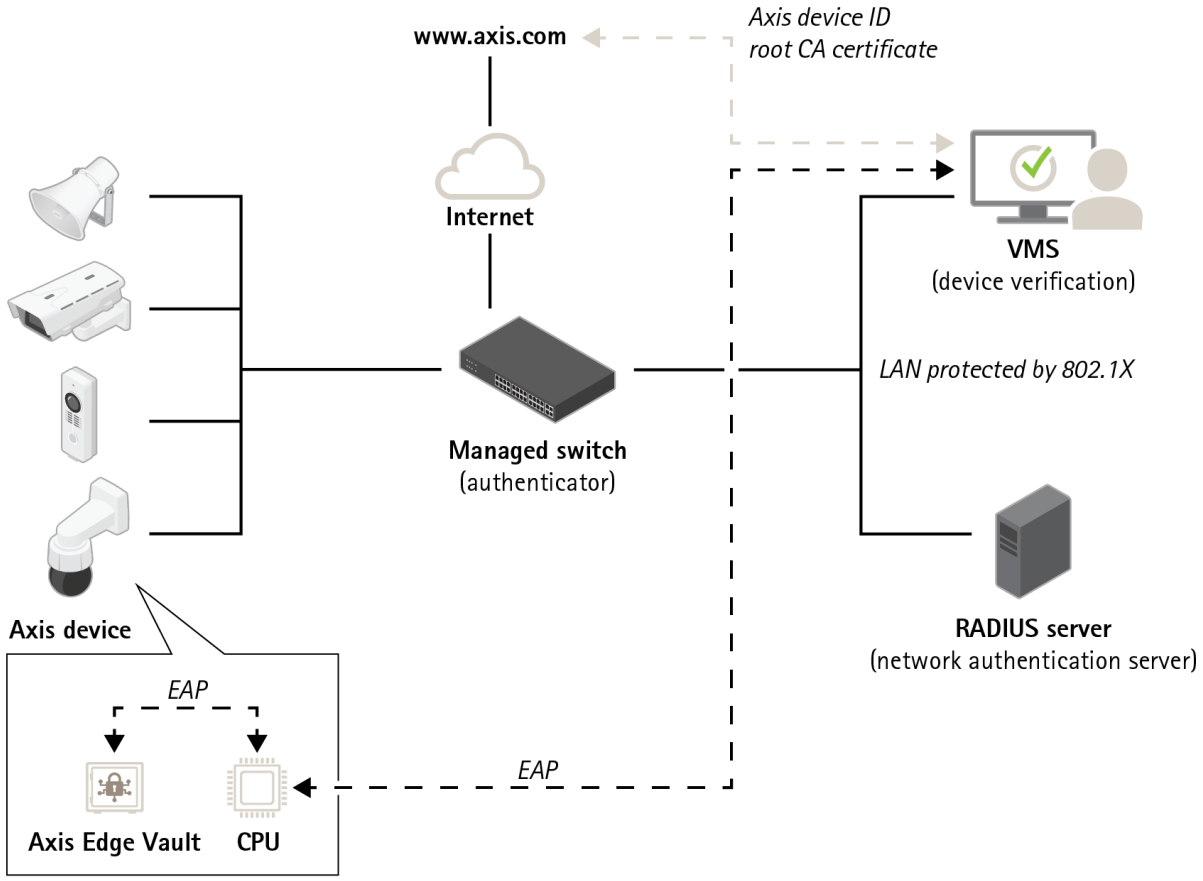

Figure 7. 系统其他部分中的软件应用可以利用安讯士设备ID和加密操作来验证通讯对方。安讯士设备ID由axis.com中的公共安讯士设备ID根CA证书验证。

9 视频篡改侦测

安防行业中的一个基本要求是，监控摄像机记录的视频应真实可信。签名视频旨在保持并进一步增强视频作为证据的可信度。通过验证视频的真实性，这个功能可保证视频在离开摄像机后未遭到编辑或篡改。

9.1 签名视频

得益于安讯士推出的签名视频功能，您可使用视频流中的签名来保证视频完好，并通过回溯到生成视频的摄像机，以验证视频来源。这就能够轻松证实视频的真实性，而无需证实视频文件的保管链。

在安防摄像机系统录制某个事件后，警察可以通过将视频文件导出至U盘的方式提取视频，并将视频保存到EMS（证据管理系统）中。从摄像机导出视频时，警察可以看到视频带有正确签名。如果视频在后期用于诉讼程序，则法庭可以控制并验证视频录制时间、录

制视频的摄像机、以及视频帧是否被篡改或删除。使用安讯士文件播放器，拥有视频副本的人都可以看到该信息。

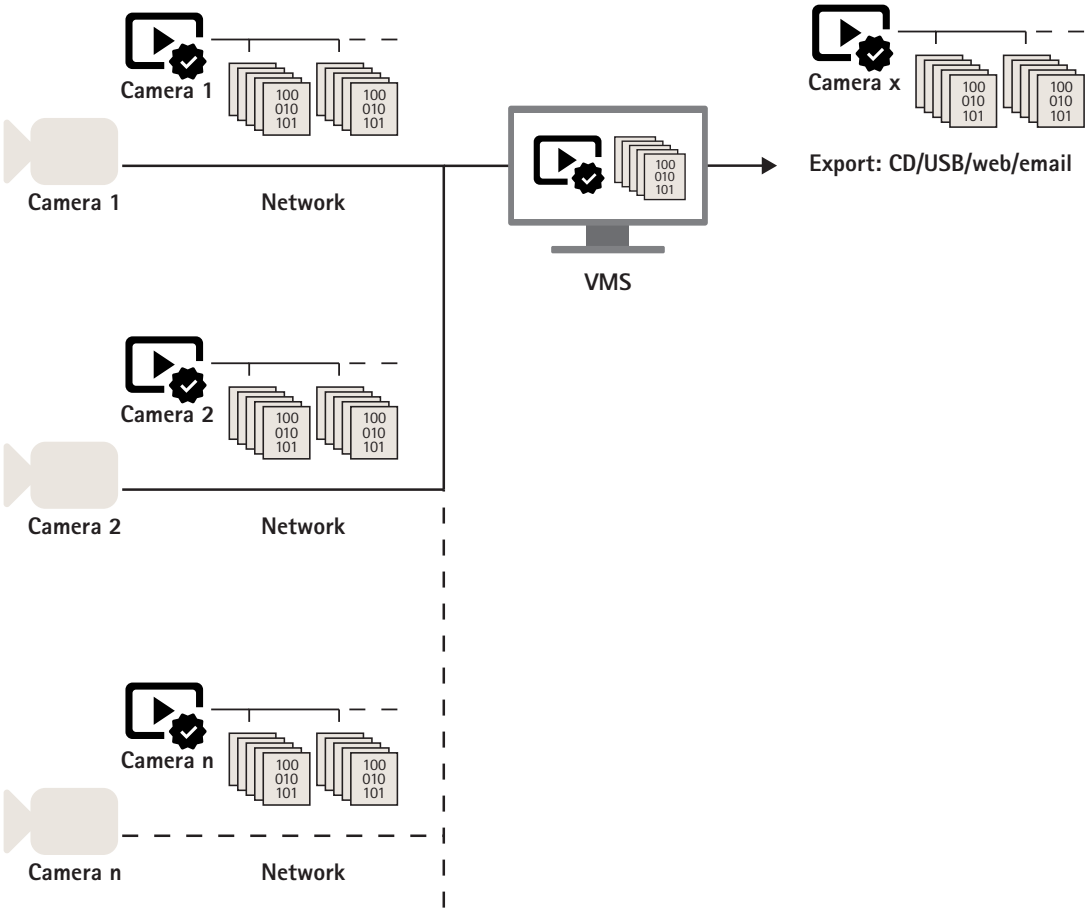

Figure 8. 签名已在摄像机中完成添加，这就能够在从视频来源到最终使用的不同环节验证视频内容。

摄像机使用Axis Edge Vault中的唯一安讯士设备ID将签名添加到视频流中。这通过计算每个视频帧的哈希值（包含元数据）以及在Edge Vault中对组合哈希进行签名来实现。签名随后保存在专用元数据字段（SEI标头）的数据流中。

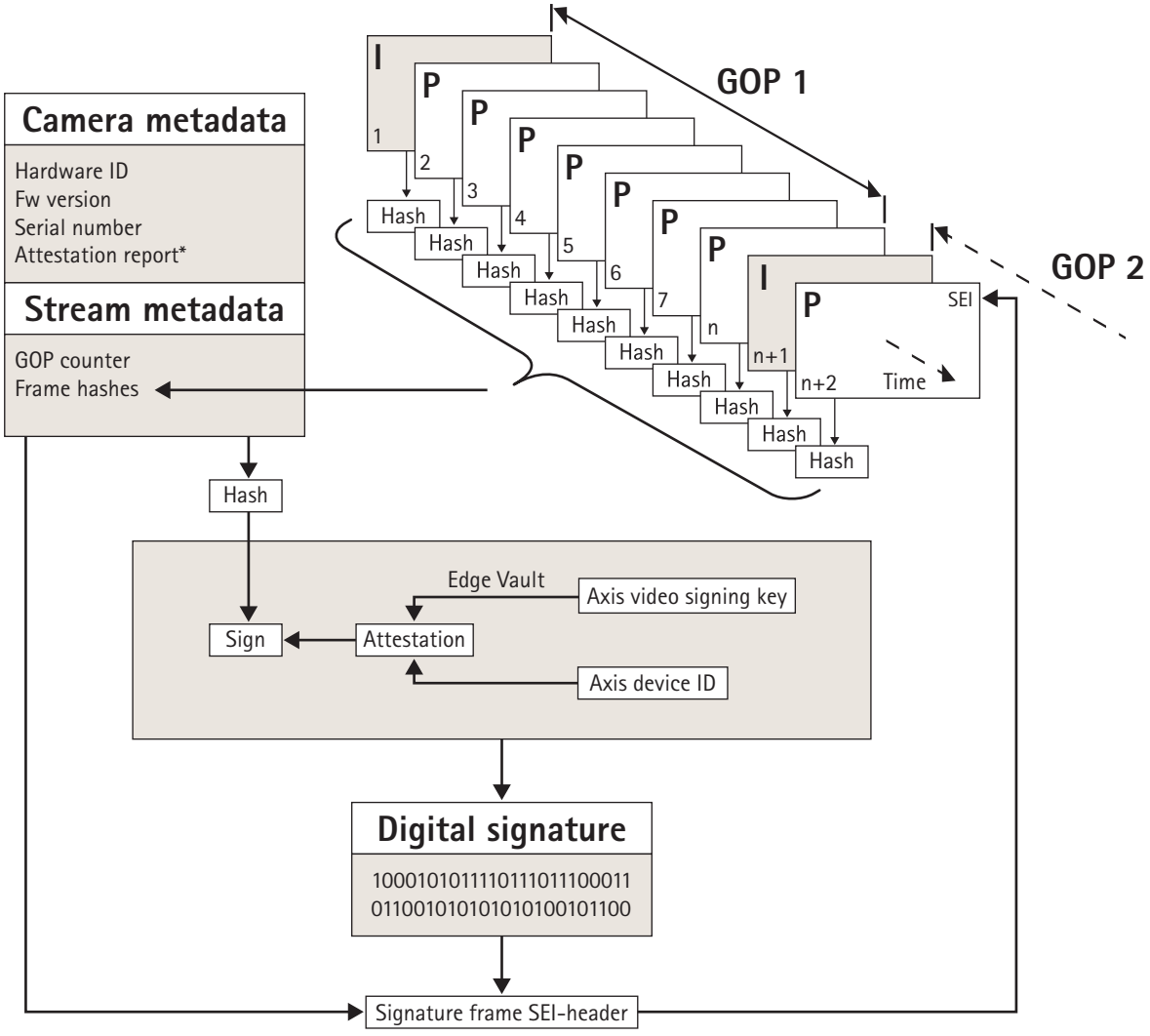

Figure 9. 将签名添加到视频元数据的图示。GOP的每帧内容与摄像机元数据和流元数据的组合哈希一起执行哈希处理。这就形成了在Edge Vault中进行签名的GOP哈希。签名和元数据随后被添加到与视频流一起传输的SEI标头。

** 证明报告可用于验证签名密钥对的来源和出处。通过验证密钥证明，可以保证密钥安全存储在特定设备的硬件中。这就保障了视频来源的安全性。*

实际签名通过因设备而异的视频签名密钥来完成，该密钥则通过设备唯一的安讯士设备ID来证明。证明报告附加到视频流开头，然后以特定时间间隔周期性地附加，通常是每小时附加一次。由于元数据包含具体的帧哈希，因此能够检测哪个帧是正确的。为了获得完整的签名，必须保护视频的GOP结构。这通过在签名中包含下一个GOP的第一个I帧的哈希来实现。

由此，帧就能够避免遭到无法被检测到的移除或重新排序。同样，这还将标记在流处理期间丢帧或者在存储时内容受损的异常事件。

T10154694/zh/M3.2/2111

关于 Axis Communications

Axis 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，Axis 致力于 推出视频监控和分析应用、访问 控制、内通系统以及音频系统的相关产品和服务。 Axis 在全球 50 多 个国家和地区设有办事机构，拥有超过 3800 名专职员工，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。 Axis 创立于 1984 年 总部位于瑞典隆德。

有关 Axis 的更多信息，请访问我们的网站 *axis.com*.