白皮书

Axis Edge Vault

基于硬件的网络安全平台，通过以下功能保护安讯士设备：

—供应链保护

—可信设备身份识别

—安全密钥存储

—视频篡改侦测

四月 2024

概述

Axis Edge Vault为保障安讯士设备安全提供了基于硬件的网络安全平台。它依托加密计算模块（安全元素和TPM）和SoC安全（TEE和安全启动）的强大基础，与前端设备安全的相关专业知识相结合。Axis Edge Vault定位于由*安全启动*和*签名OS*（“OS”指操作系统）共同建立的强大信任根。这些功能让安全操作所依赖的信任链能够拥有完整的加密验证软件链。

配备Edge Vault的安讯士设备可防止敏感信息被窃听和恶意提取，从而尽可能降低客户暴露于网络安全风险的几率。Axis Edge Vault还让安讯士设备能够成为客户网络上一个可信且可靠的单元。

Axis Edge Vault网络安全平台

密码计算模块	功能	应用场合
• 安全元素 • TPM 2.0 • SoC安全 (TEE)	• 安全启动 • 签名OS • 安讯士设备ID • 安全密钥库 • 签名视频 • 加密文件系统	• 供应链保护 • 可信设备身份识别 • 安全密钥存储 • 视频篡改侦测

- **供应链保护**：Axis Edge Vault需要一个作为信任根的安全基础。如不借助安全启动和签名OS，便无法建立信任链的信任根。安全启动与签名OS一起，从不可变ROM（启动ROM）开始，提供完整的加密验证软件链。安全启动可保证设备以签名OS启动，从而可防止物理供应链篡改。凭借签名OS，设备还能够先验证新设备软件，然后再同意进行安装。如果设备检测到完整性受损或者设备软件未经安讯士签名，则升级将会被拒绝。这可保护设备免遭软件篡改。
- **可信设备身份识别**：能够验证设备来源是建立设备身份信任的关键。在生产期间，配备AXIS Edge Vault的设备被分配到具有唯一性、由工厂预置且符合IEEE 802.1AR标准的安讯士设备ID证书。其原理与护照相似，旨在证明设备来源。设备ID作为经安讯士根证书签名的证书，安全且永久存储在安全密钥库中。设备ID可被客户的IT基础设施用于实现自动化安全设备配置入网以及安全设备识别。
- **安全密钥存储**：安全密钥库为加密信息提供基于硬件的防篡改存储。安全密钥库保护安讯士设备ID和客户加载的加密信息，防止在存在安全漏洞的情况下发生非法访问和恶意提取。
- **视频篡改侦测**：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。摄像机使用安全地存储在安全密钥库中的唯一签名密钥将签名添加到视频流中。播放视频时，安讯士*文件播放器*会显示视频是否完好无损。签名视频让视频追溯可达摄像机源头，并确定视频在离开摄像机后未遭到篡改。

目录

1 引言

安讯士遵循行业良好做法，保证我们产品的自身安全。这旨在尽可能减少客户暴露于网络安全风险的几率，让安讯士设备成为客户网络上的可信单元。

Axis Edge Vault为保障安讯士设备安全提供了基于硬件的网络安全平台。它依托加密计算模块（安全元素和TPM）和SoC安全（TEE和安全启动）的强大基础，与前端设备安全的相关专业知识相结合。

本白皮书将概述安讯士前端设备安全的多层方案，并对其常见风险以及如何加以防范进行介绍。Axis Edge Vault需要一个作为信任根的安全基础。因此，我们还将探讨安讯士设备的供应链安全方面，并了解签名OS（签名操作系统）和安全启动如何作为基础措施来抵御软件篡改和物理供应链篡改。

在*https://www.axis.com/support/cybersecurity/resources*中，更详细地介绍了产品安全、已发现的漏洞以及针对常见威胁的风险降低措施。

本白皮书的最后一章为术语表。

2 供应链保护

Axis Edge Vault需要一个作为信任根的安全基础。信任根的建立始于设备的启动过程。在安讯士设备中，基于硬件的机制*安全启动*会验证设备启动所使用的操作系统 (AXIS OS)。AXIS OS反过来又在构建过程中使用*签名OS*进行了加密签名。

安全启动和签名OS相互捆绑。它们可保证在部署设备前，操作系统或设备软件未被（能够实际接触到设备的人员）篡改，并可保证在部署后，设备无法安装已遭破坏或未经代码签名的软件更新。安全启动和签名OS共同为安全操作所依赖的信任链创建完整的加密验证软件链。

2.1 安全启动

安全启动机制是一种由完整的加密验证软件链组成的启动过程，始于不可变存储器（启动ROM）。安全启动可保证设备只能使用已授权的操作系统来启动。

启动ROM在验证启动程序时，发起启动过程。安全启动然后以实时的方式验证从闪存中加载的不同软件组件的嵌入式签名。启动ROM是信任根，只有在验证全部签名的情况下，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。

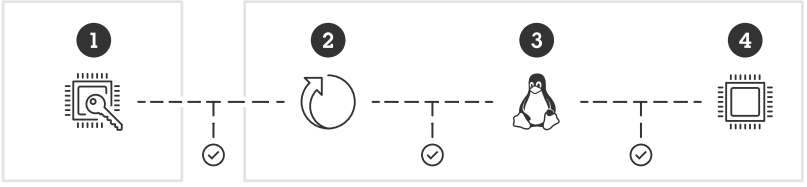

Figure 1. 在安全启动过程中，链的每个部分都会对下一部分执行身份验证。这最终会产生一个经过验证的根文件系统。

1 *SoC上的启动ROM（信任根）*
2 *启动程序*
3 *Linux内核*

4 根文件系统

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。对于拥有安全启动的设备，闪存中的已安装操作系统受到防篡改保护，而配置不受保护。即使在恢复出厂默认设置后，安全启动也能够保证设备处于正确状态。但要让安全启动功能正常工作，必须保证启动过程已验证操作系统由安讯士签名。

2.2 签名OS

安讯士签名OS涉及安讯士使用保密的私钥对设备软件映像进行代码签名。设备启动时，安讯士设备的安全启动功能将检查设备软件是否已签名。如果检测到设备软件的完整性受损，设备将不会运行。在更新设备软件时，设备的现有已签名AXIS OS将自动检查新的AXIS OS是否也已签名。如未签名，将拒绝更新。

对OS进行代码签名的过程是通过计算加密哈希值来发起的。在将签名附加到AXIS OS映像之前，这个值使用私钥/公钥对的私钥进行签名。

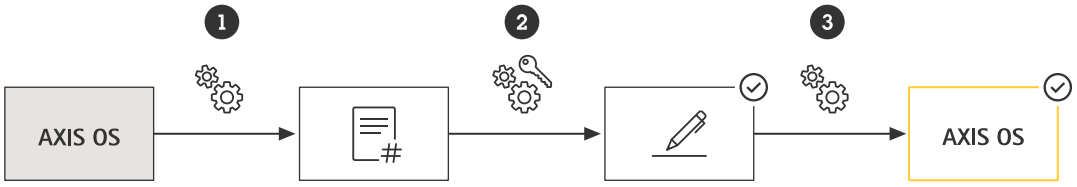

Figure 2. OS代码签名过程。

1 为AXIS OS创建加密哈希值。
2 签名是通过组合哈希值和私钥来创建的。
3 签名被添加到AXIS OS版本和二进制代码中。

升级前，必须验证新软件更新的真实性。为了保证这一操作，使用了公钥（安讯士产品随附）来确认是否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，可以验证完整性。如果签名无效，或者AXIS OS映像已被篡改，安讯士设备的启动过程将被中止。

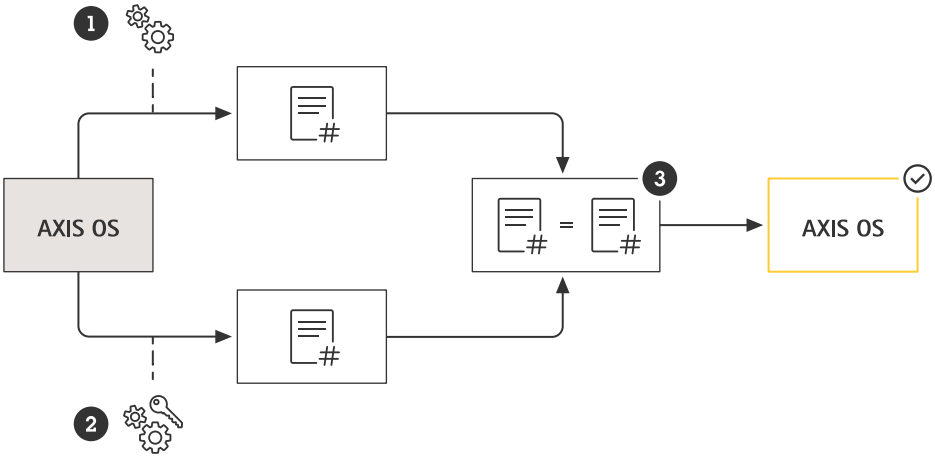

Figure 3. 签名OS验证过程。

1 *计算AXIS OS的哈希值*
2 *使用公钥确认签名的哈希值*
3 *仅当结果匹配时，签名才能成功验证。*

安讯士签名OS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。整个软件映像的完整性通过签名获得保证。主签名验证多个二次签名，在映像解压时加以验证。

对于测试和自定义版本，安讯士实施了相应的机制，用于审批具体的设备以接受非生产映像。此映像使用同时受所有者和安讯士认可的专用密钥进行代码签名，进而形成自定义签名。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映像。自定义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。

3 可信设备身份识别

在先进的零信任网络（“永不信任，始终验证”）中，验证设备来源及其真实性和连接的能力是一种基本需求。网络设备能够验证其完整性和真实性，这种验证方法类似于在机场通过出示护照以向相关机构提供自身身份验证。

3.1 利用安讯士设备ID安全识别设备

国际标准*IEEE 802.1AR*定义了一种方法，用于通过网络自动且安全地识别设备。如果将通信转发到嵌入式安全模块，则设备可根据此标准返回可信识别响应。这种可信响应可被网络基础设施使用，以便自动、安全地将设备并入预置网络中，进而执行初始设备配置和软件更新。

为了符合IEEE 802.1AR，大多数安讯士设备都拥有设备特有且由工厂预置的安讯士设备ID证书（IEEE 802.1AR初始设备标识符，即IDevID）。安讯士设备ID安全地存储在受到防篡

改保护的安全密钥库中，通过设备自身的加密计算模块提供。这个标识对于安讯士设备是唯一的，旨在证明设备的来源。

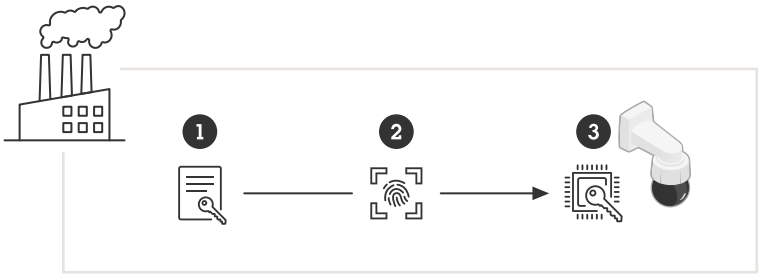

Figure 4. 在设备的制造过程中，这个唯一的安讯士设备ID (2) 存储在设备的安全密钥库中 (3)。

1 *安讯士设备ID基础设施 (PKI)*
2 *安讯士设备ID*
3 *安讯士设备ID安全地存储在受到防篡改保护的安全密钥库中，通过设备上的加密计算模块提供。*

IEEE 802.1AR的网络访问控制基于IEEE 802.1X标准，在预先选择了安讯士设备ID的安讯士设备中，已默认启用了此网络访问控制。由此，就能够通过支持802.1X的IT基础设施（甚至在工厂默认状态下），安全地识别并验证安讯士设备。

安讯士设备ID证书拥有多种不同的加密配置（2048位RSA、4096位RSA、ECC–P256）。它们已默认启用，以便通过IEEE 802.1X网络访问控制和HTTPS安全连接并识别设备。

安讯士管理自己的专用IEEE 802.1AR公钥基础设施 (PKI)，以便在制造过程中由工厂预置安讯士设备ID。安讯士设备ID由中间证书签名，该中间证书由安讯士根证书签名。根CA和中间CA都安全地存储在地理上分开的加密计算模块中。这能够防止在安讯士生产设施处存在安全漏洞的情况下发生恶意提取事件。有关安讯士PKI基础设施的详情，请参阅 *www.axis.com/support/public-key-infrastructure-repository*

Figure 5. 安讯士IEEE 802.1AR公钥基础设施 (PKI)，用于在制造过程中由工厂预置安讯士设备ID。安讯士设备ID (1)（其为包含产品序列号的证书）由经安讯士设备ID根CA证书 (3) 签名的安讯士设备ID中间CA (2) 进行签名。专用硬件安全模块 (HSM) 用于进行安全出厂配置。

A *参考*
B *签名*

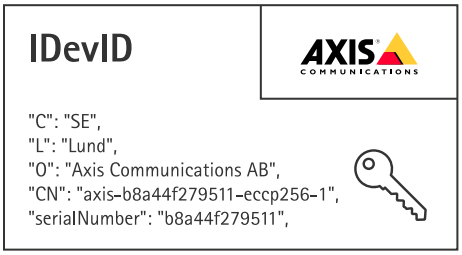

Figure 6. 安讯士设备ID示例。

3.2 安全网络配置入网

购买了安讯士设备后，在开始使用前，您可以执行手动检查。通过对设备的目视检查，并凭借先前对安讯士产品观感的了解，您可以确认该设备是否为安讯士正品。但执行此类检查的前提是，您亲自使用过这种设备。那么，在与设备进行网络通信时，您将如何保证与正确的设备通信，同时能够验证设备身份呢？网络设备和服务器上的软件均不能执行物理检查。一种常见的安全措施是，首次与新设备交互时，通过能够被安全预置的封闭式网络进行交互。

安讯士设备ID为您的网络提供了加密的可验证证据，证明特定设备是由安讯士生产的，并且与设备的网络连接确实是由该设备提供的。安讯士设备ID可用在IEEE 802.1X网络身份验证过程中，以访问预置网络；在该网络中，安讯士设备被移入生产网络之前，执行了进一步软件更新和安讯士设备配置。

借助安讯士设备ID，可提升总体安全性，减少设备部署时间，因为可使用自动化程度更高且成本效益更好的控制来实现设备的安装和配置。

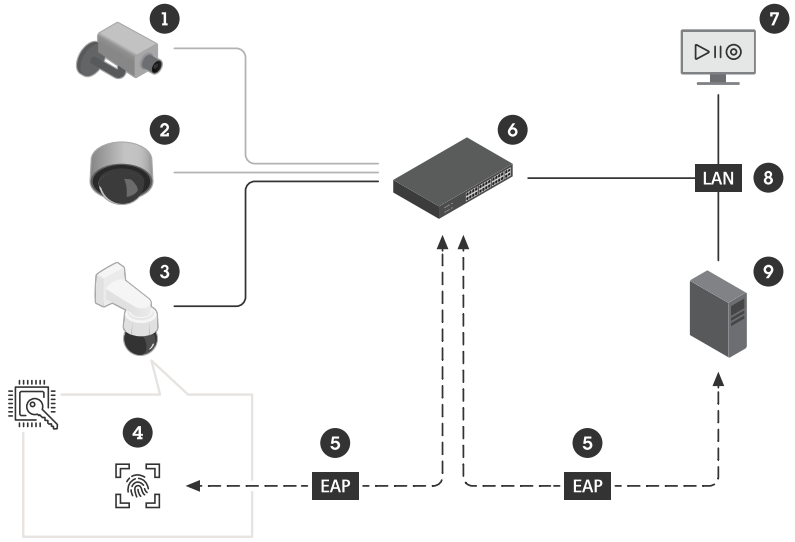

Figure 7. 安全网络配置入网。您可以指示身份验证服务器 (9) 自动接受连接到网络 (8) 和 VMS (7) 的安讯士设备 (3)。为此，可以使用设备序列号和安讯士设备ID (4) 作为指纹识别或身份验证。

1 *非授权设备（必须手动配置入网）*
2 *第三方设备*
3 *安讯士设备*
4 *安讯士设备ID，安全存储在防篡改的安全密钥库中*
5 *通过安讯士设备ID证书对安讯士设备进行802.1X EAP–TLS网络身份验证*
6 *管理型交换机（认证器）*
7 *VMS（设备验证）*
8 *受802.1X保护的局域网 (LAN)*
9 *RADIUS（网络身份验证服务器）*

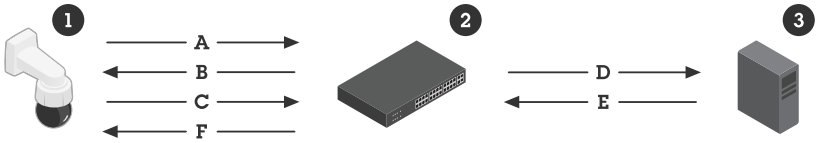

Figure 8. 更详细的配置入网说明。用于安全设备身份识别的IEEE 802.1AR定义了一种方法，旨在利用RADIUS服务器 (3)，通过IEEE 802.1X可扩展身份验证协议请求 (EAP–TLS) 来识别设备 (1)，从而获取设备对网络的访问权限。

1 *安讯士设备*
2 *管理型交换机（认证器）*
3 *RADIUS服务器（网络身份验证服务器）*
A *新建连接*
B *EAP–请求身份*
C *EAP响应身份，包括安讯士设备ID证书、IEEE 802.1AR IDevID*
D *RADIUS访问请求*
E *RADIUS访问询问*

F EAP–成功

除提供额外的内置受信源之外，安讯士设备ID还让您能够持续跟踪设备，根据零信任网络原则进行定期核实和身份验证。

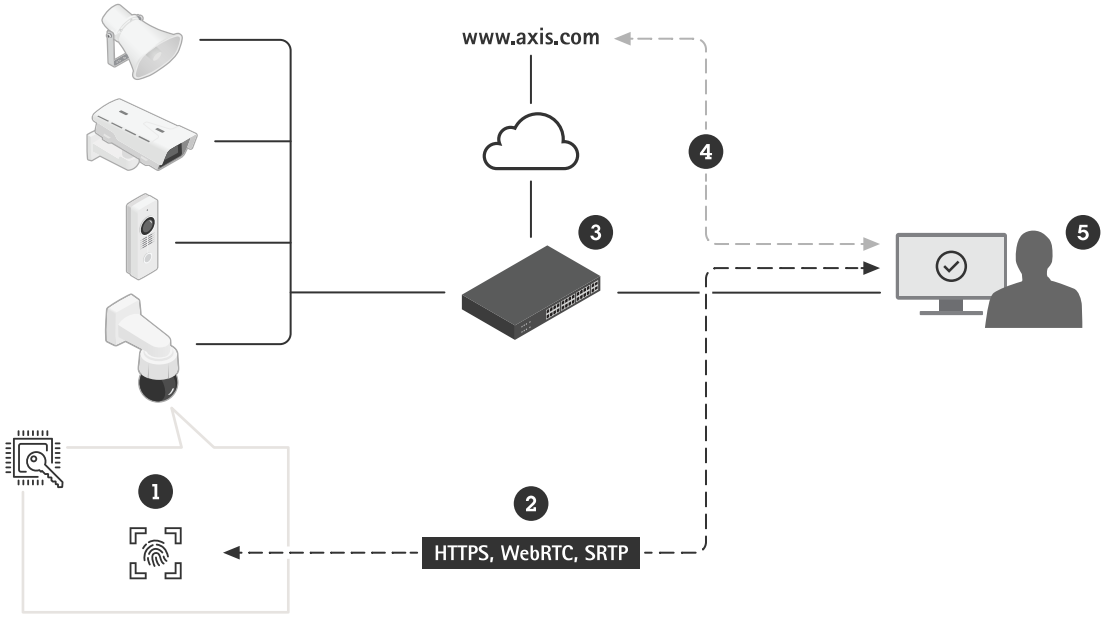

Figure 9. 在设备安全配置入网后，系统其他部分中的软件应用 (5) 可使用安讯士设备ID(1) 和加密操作对参与TLS通信 (2) 的设备进行核实与身份验证。安讯士设备ID可通过公开的安讯士设备ID根CA证书 (4) 来验证。

1 *安讯士设备ID，安全存储在防篡改的安全密钥库中*
2 *基于TLS的通信（HTTPS、WebRTC、SRTP）*
3 *管理型交换机*
4 *安讯士设备ID根CA证书（下载网址：www.axis.com/support/public-key-infrastructure-repository）*
5 *VMS或其他软件（设备验证）*

4 安全密钥存储

传统上，X.509加密敏感信息（私钥）存储在设备的文件系统中。它仅受到用户账户访问策略的保护，但这种访问策略提供的是基本保护，旨在保证用户账户不容易被盗用。然而，在存在安全漏洞的情况下，此加密信息将无法受到保护，并可能遭到敌手访问。

就安全方面而言，安全密钥库对于存储和保护加密信息具有重要意义。不仅包含在安讯士设备ID和签名视频中以及存储在安全密钥库中的加密敏感信息能够受到保护，而且客户加载的信息也能够同样受到保护。

4.1 安全密钥库

加密敏感信息（私钥）存储在设备基于硬件的防篡改安全密钥库中。由此，即使存在安全漏洞，也可防止这些信息遭到恶意提取。另外，私钥即便在使用时，仍在安全密钥库中受到持

续保护。潜在敌手将无法访问安全密钥库，且无法窃听网络通信，无法通过IEEE 802.1X 密钥访问网络，亦无法提取其他私钥。

安全密钥库通过基于硬件的加密计算模块来提供。根据安全要求，安讯士设备可配备一个或多个这样的模块，比如TPM 2.0（可信平台模块）、或安全元素、和/或TEE（可信执行环境）。

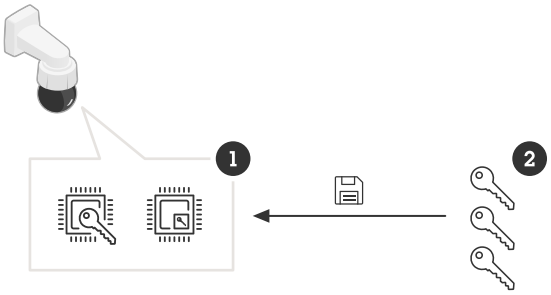

Figure 10. 安全密钥库 (1) 提供私钥 (2) 保护和安全执行加密操作。

1 *安全密钥库，可以是安全元素、TPM或TEE（在SoC上）*
2 *私钥，例如安讯士设备ID、视频签名密钥、访问控制密钥、文件系统密钥和客户加载的密钥（例如IEEE 802.1X和HTTPS）*

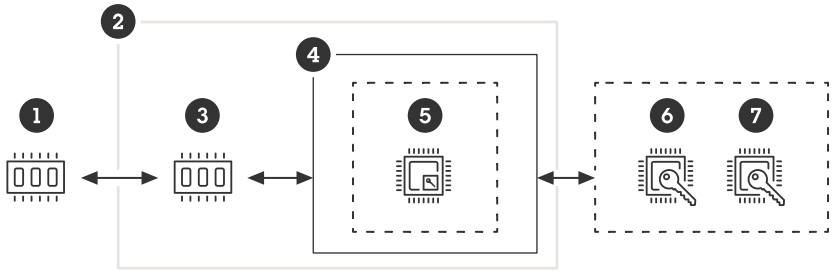

Figure 11. 配备Axis Edge Vault的设备拥有硬件加密计算模块（安全元素 (6) 和TPM (7)），这些模块安装在PCB上，靠近系统级芯片 (SoC) 的主处理器 (4)。TEE (5) 是SoC主处理器自身的安全区域。SoC嵌入式启动ROM (3) 负责执行安全启动程序，保证仅使用来自闪存 (1) 的签名OS软件映像来启动设备。

1 *闪存（供签名OS使用，读写文件系统）*
2 *SoC*
3 *启动ROM（用于安全启动）*
4 *CPU*
5 *TEE（用于安全密钥库）*
6 *安全元素（用于安全密钥库）*
7 *TPM（用于安全密钥库）*

TPM、安全元素和TEE都能够保护私钥，并安全执行加密操作。在存在安全漏洞的情况下，可防止非法访问和恶意提取。

4.2 “通用标准”与FIPS 140

加密计算模块可以依据“通用标准”评估等级 (CC EAL) 和FIPS 140合规等级 (1–4) 进行认证。这些认证旨在确定加密操作的正确性和完整性，并验证防篡改措施，如自动验证、防篡改以及其他防护措施。关于认证的相关信息，请参阅安讯士设备数据表或*安讯士产品选择向导*。安讯士要求至少根据“通用标准”EAL4和/或FIPS 140–2/3 2/3级对产品中的硬件加密计算模块进行认证。

4.2.1 通用标准

“通用标准”(CC)（又称为信息技术安全评估通用标准）是一种面向IT产品安全认证的国际标准 (ISO/IEC 15408)。“通用标准”为制造商和部署商指定安全功能和保证要求以作为安全目标（可分为若干保护类型）提供了框架。

然后由经认证的独立测试实验室评估这些声称的安全目标，之后，产品方可作为认证产品被列入“通用标准”数据库中。测试实验室的评估要求和评估完整性通过所评定的EAL（评估保证等级）来体现，该EAL的范围为EAL 1（功能测试）至EAL 7（形式验证设计和测试）。这就意味着，“通用标准”的覆盖范围广泛，从操作系统和防火墙乃至TPM和通行证。

有关“通用标准”认证要求的更多详情，请访问“通用标准”网站 *www.commoncriteriaportal.org/*

4.2.2 FIPS 140

FIPS（联邦信息处理标准）140–2和140–3是面向加密计算模块和加密算法使用的信息安全标准，由NIST（国家标准和技术协会）在美国发布，被美国和加拿大联邦政府采纳为法定要求。FIPS 140–3是FIPS 140–2的更新版本，于2019年取代后者。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。简而言之，认证要求加密计算模块的描述、规格和验证、批准算法、批准的操作模式和电源测试。

客户可以确定自己产品的运行能够符合政府规定。因此，在面临政府相关部门的审查时，他们也能够安枕无忧。非FIPS 140管制企业也能够保证自己的产品符合政府规定的相关标准。有关FIPS 140–2和FIPS 140–3认证要求的更多详情，请访问NIST网站*www.nist.gov*。

如要保证整套系统符合FIPS 140的要求，那么系统的各组件就需要符合FIPS 140的相关要求。比如，视频管理系统、录像服务器以及所连接的设备（如摄像机）需要符合其相关要求。当设备至少使用了软件认证或硬件认证模块时，此设备即符合FIPS 140。

搭载AXIS OS V12或更高版本的安讯士设备配有经FIPS 140认证且基于软件 (OpenSSL) 的安讯士加密模块。大多数新款安讯士设备同时配有经FIPS 140认证的硬件加密模块和基于软件的加密模块。这就能够打造理想的解决方案，即，使用软件认证模块来提供基于软件的

应用程序，比如操作系统层级上的HTTPS和IEEE 802.1X，同时又使用硬件认证模块来保证安全的密钥存储。

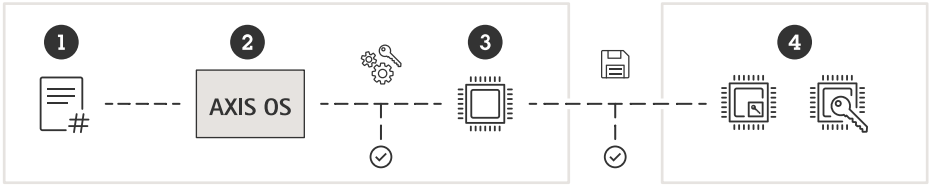

Figure 12. 在安讯士设备中使用符合FIPS 140的加密软硬件模块。应用程序 (1)通过安讯士加密模块提供，嵌入在安讯士设备的AXIS OS (2) 中。安讯士加密模块执行加密操作（包括对称和非对称加密），其中使用SoC (3) 和/或基于硬件的嵌入式加密计算模块 (4) 来保证安全密钥存储。

1 *需要加密或基于TLS（如HTTPS、webRTC和802.1X）的应用程序*
2 *AXIS OS，带基于软件的嵌入式加密模块（NIST证书：https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4621）*
3 *SoC*
4 *基于硬件的嵌入式加密计算模块*

4.3 私钥保护

对于敌手而言，通过提取私钥，他们能够窃听经HTTPS加密的网络通信，或者伪装成实际设备并获取对802.1X保护网络的访问权限。

安讯士设备支持使用多种基于TLS（传输层安全）的协议来实现安全通信。安讯士设备ID (IEEE 802.1AR)、HTTPS（网络加密）和802.1X（网络访问控制）依赖于X.509加密信息保护。

TLS的X.509数字证书使用证书以及相应的公钥私钥对来实现网络中两个主机之间的通信。私钥永久存储在安全密钥库中，即使在用于解密数据时，也不会离开设备。实际证书和公钥是已知的，可由安讯士设备共享，用于加密数据。

4.4 保护访问控制密钥

安讯士访问控制解决方案（如开放式监控设备协议 (OSDP) 安全通道）中使用的加密信息保护是体现硬件保护密钥存储重要性的另一示例。

OSDP安全通道是一种应用广泛且基于AES-128的加密和身份验证方案，用于保护门禁控制器与周边设备（如读卡器）之间的通信。

由门禁控制器和读卡器共享的AES对称密钥（安全通道基本密钥 (SCBK)）用于发起相互的身份验证，并在稍后生成一组会话密钥，用于加密门禁控制器与读卡器之间的通信数据。

为了实现真正的端到端安全，需要将主密钥 (MK) 和SCBK安全地存储在安讯士网络门禁控制器的安全密钥库内。主密钥为连接的安讯士读卡器分别派生唯一的SCBK。此外，在安装期间安全地分发给安讯士读卡器的具体SCBK需要安全地存储在读卡器的安全密钥库中。读卡器通常安装在门的非安全侧，所以非常重要。

由此，OSDP安全通道密钥在硬件保护环境中两端都受保护。由此，即使存在安全漏洞，也可防止这些信息遭到恶意提取。

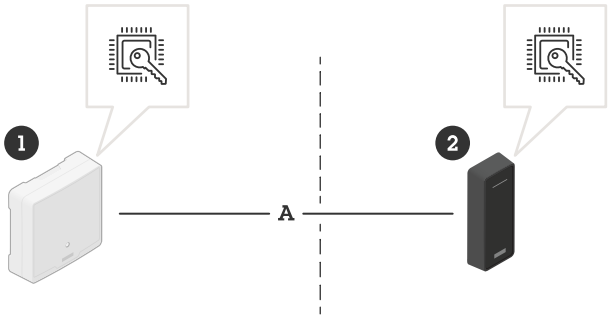

Figure 13. 在访问控制中，利用安全密钥库实现端到端安全。主密钥和个体安全通道基本密钥 (SCBK) 均存储在（位于门的两侧的）设备的安全密钥库中。

1 安讯士门禁控制器安装在门的安全侧
2 安讯士读卡器安装在门的非安全侧
A OSDP安全通道通信

4.5 保护文件系统密钥

投入运行的安讯士设备承载着客户特有的配置和信息。当从提供预配置服务的经销商或系统集成商将安讯士设备运送至客户时，同样如此。在能够实际接触到安讯士设备时，恶意的敌手可能拆下闪存并通过闪存读取设备以访问闪存，由此从文件系统中提取信息。因此，如果安讯士设备失窃或发生了入侵，则保护可读写文件系统以防敏感信息遭到提取或配置遭到篡改，就变得非常重要。

安全密钥库可通过对文件系统实施强效加密，以防止恶意信息提取和配置篡改。安讯士设备断电后，文件系统上的信息就被加密。在启动期间，读写型文件系统通过AES–XTS–Plain64 256位密钥来解密，使此文件系统能够被安讯士设备加载和使用。文件系统加密密钥具有唯一性，由工厂为每台设备分别默认生成，后续每更新一次软件，便重新生成一次：这就意味着，在设备的整个寿命期内，密钥均不相同。

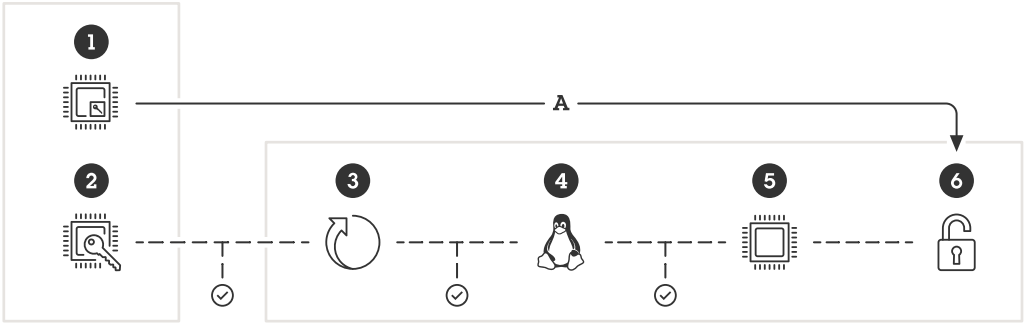

Figure 14. TEE (1) 和启动ROM (2) 嵌入在SoC上。在启动过程中，读写文件系统 (6) 被解密（通过TEE），以便安讯士设备可以加载和使用该文件系统。在启动过程中，链的每个部分（启动程序 (3)、Linux内核 (4) 和根文件系统 (5)）都经过验证，并随之对闪存中的下一个子系统进行身份验证。这最终会产生一个经过验证的根文件系统。

1 TEE
2 启动ROM

3 启动程序
4 Linux内核
5 根文件系统
6 读写文件系统
A TEE解密读写文件系统。

5 视频篡改保护

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。

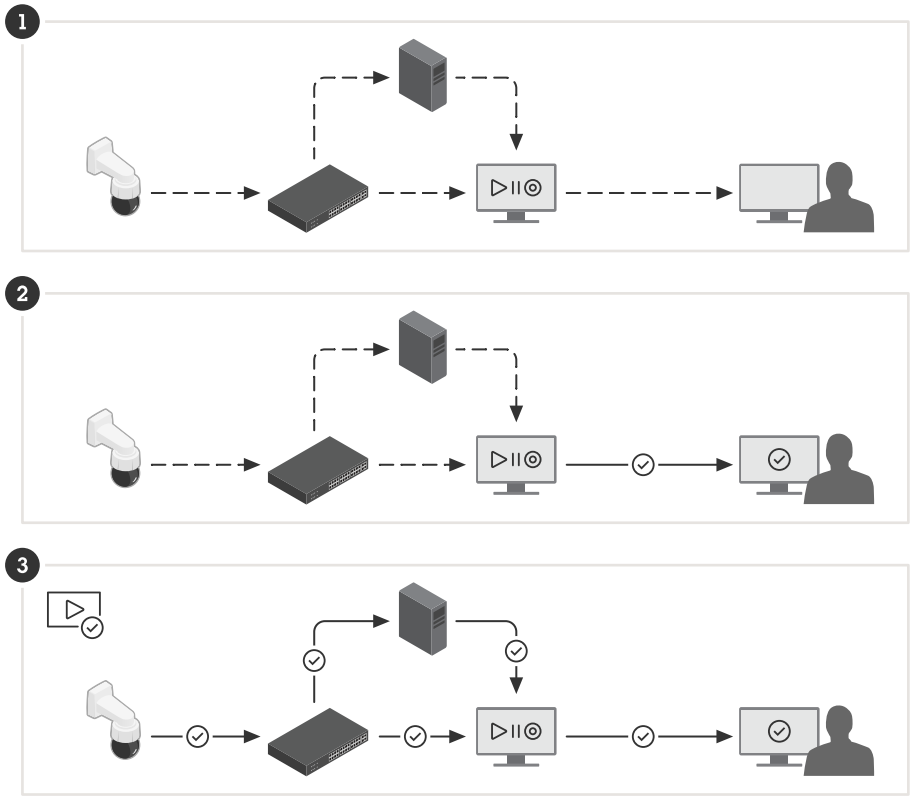

Figure 15. 验证视频真实性。

1 视频从摄像机途经多个环节到达录像观看者。娴熟的攻击者能够在视频传输途中篡改视频。
2 通过在导出期间为视频添加VMS水印，可以验证某些环节，但无法保证视频在更早的阶段中未遭到过篡改。
3 签名视频可保证视频在从摄像机传输至导出至录像观看者的过程中未遭到过篡改。视频可回溯至其记录设备。

5.1 签名视频

得益于安讯士开发的开源签名视频功能，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，来验证视频来源。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盘的方式接收视频，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。

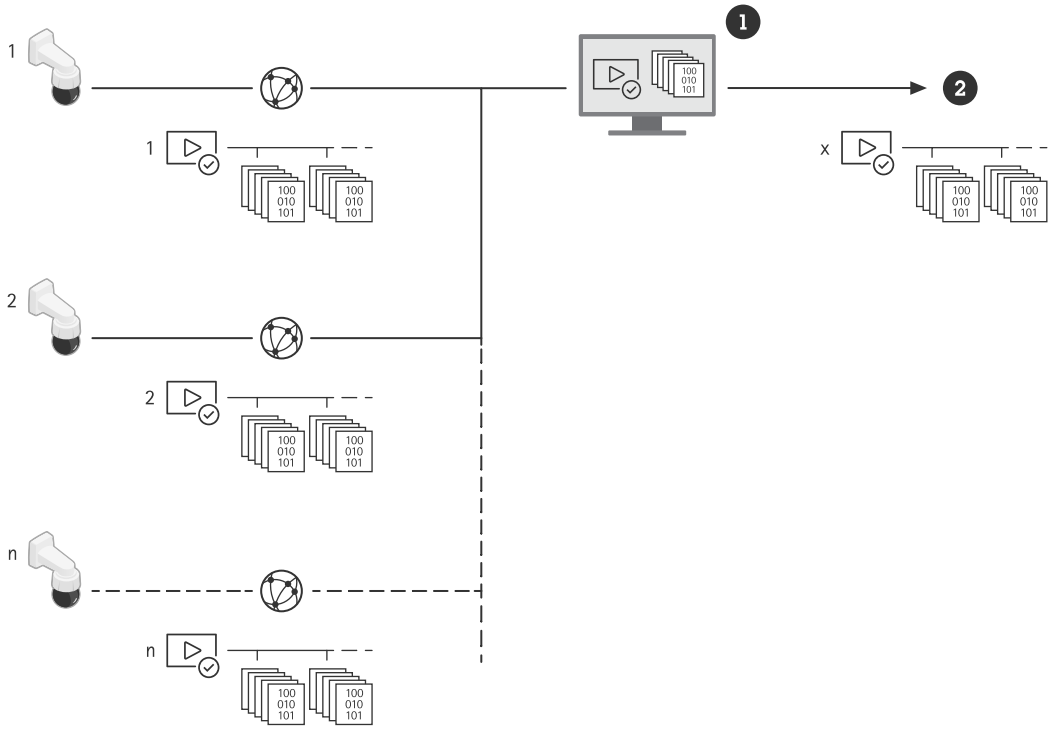

Figure 16. 签名已在摄像机中完成添加，这就能够在从视频来源到最终使用的不同环节验证视频内容。

1 *VMS*
2 *将视频导出至CD/USB/网页/电子邮件*

摄像机使用保存在安全密钥库中的唯一签名密钥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。

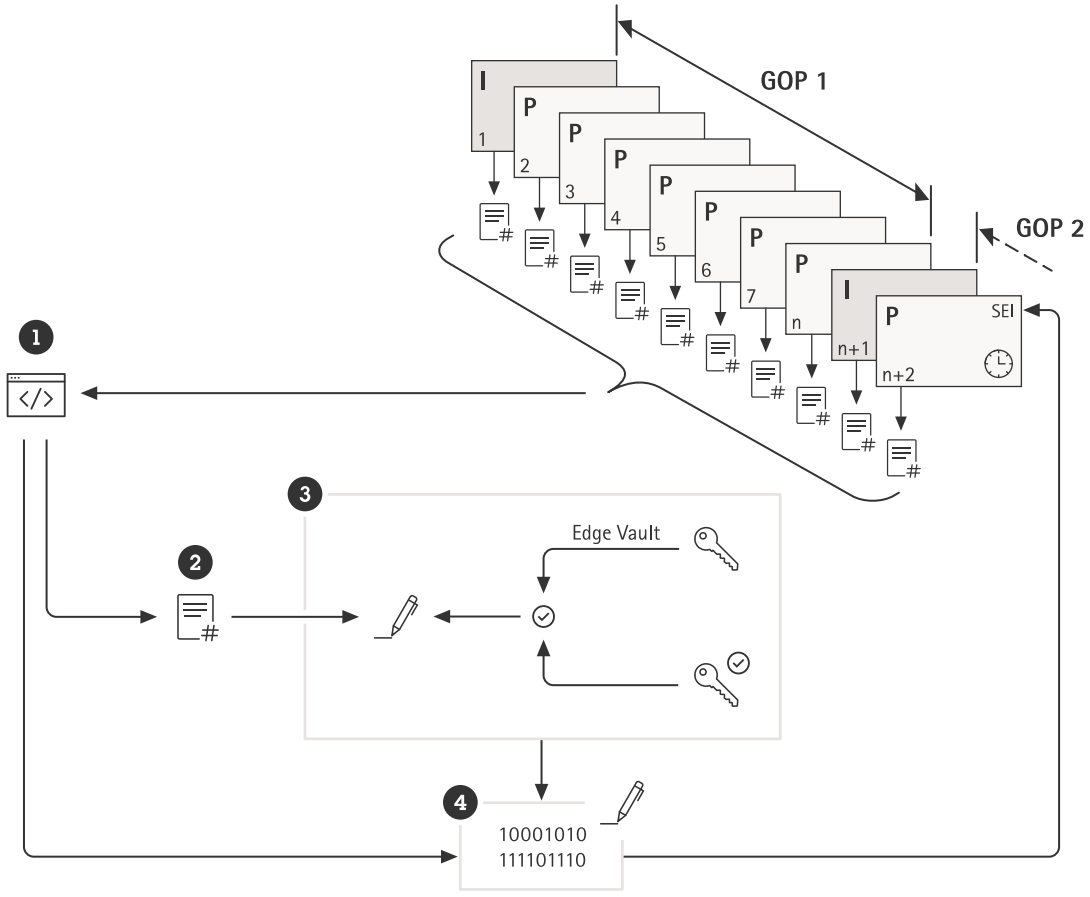

Figure 17. 将签名添加到视频流的示意图。图片组 (GOP) 的每帧内容与元数据 (1) 的哈希一起执行哈希处理。这会构成GOP哈希 (2)，该GOP哈希在Edge Vault (3) 中使用设备唯一的视频签名密钥和证明密钥进行签名。数字签名 (4) 和元数据 (1) 随后被添加到与视频流一起传输的SEI标头。

1. *设备唯一的元数据（硬件ID、AXIS OS版本、序列号和证明报告*）和流元数据（GOP计数器和帧哈希）*
2. *GOP哈希*
3. *Axis Edge Vault*
4. *数字签名*

** 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。*

实际签名通过设备唯一的视频签名密钥来完成，而视频签名密钥则通过设备唯一的证明密钥加以证明。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，必须保护视频的图片组 (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。当发生在流处理期间丢帧或者在存储期间帧受损的低概率事件时，也可以同样的方式进行标记。

6 词汇表

安讯士设备ID：设备唯一的证书，包含能够证明安讯士设备真实性的相应密钥。安讯士设备出厂预置有安讯士设备ID，此ID存储在安全密钥库中。安讯士设备ID基于国际标准IEEE 802.1AR（IDevID，初始设备标识符），此标准定义了用于执行自动安全识别的方法。

Axis Edge Vault：基于硬件的网络安全平台，用于保障安讯士设备安全。它依托加密计算模块（安全元素和TPM）和SoC安全（TEE和安全启动）的强大基础，与前端设备安全的相关专业知识相结合。

证书：一种签名文档，用于证明公钥/私钥对的来源和属性。证书由证书颁发机构 (CA) 签名，如果系统信任此 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。

通用标准 (CC)：一种面向IT产品安全认证的国际标准。又称为信息技术安全评估通用标准 (ISO/IEC 15408)。

FIPS 140：一系列美国计算机安全标准，用于认证加密计算模块。FIPS（联邦信息处理标准）140就应该如何设计和实施加密模块以降低模块篡改风险定义了相关要求。

不可变ROM（只读存储器）：只读存储器安全地存储可信公钥以及用于比较签名的程序，使它们无法被覆写。

预置：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。

安全启动：此功能用于在设备启动期间防止加载未授权软件。安全启动使用签名OS，可保证使用经授权的安讯士软件来启动设备。

安全元素：一种加密计算模块，提供基于硬件的防篡改私钥存储，并安全执行加密操作。与TPM不同，安全元素的软硬件接口是非标准化接口，因制造商而异。

安全密钥库：一种防篡改环境，用于保护私钥并安全执行加密操作。在存在安全漏洞的情况下，它可防止非法访问和恶意提取。根据安全要求，安讯士设备可配备一个或多个基于硬件的加密计算模块，用于提供硬件保护型安全密钥库。

签名OS或签名操作系统：设备软件，其文件映像已被可信方进行过数字代码签名。签名OS是安全启动过程的要求之一，旨在保证仅从信任的软件映像启动设备。在基于AXIS OS的产品中，设备在执行更新前，会先验证设备软件映像的完整性和真实性。

签名视频：此功能用于保持并增强视频作为证据的可信度。签名视频提供视频篡改侦测和真实性验证，用于保证视频完好无损以及可回溯至具体的安讯士摄像机。签名视频的签名密钥保存在安讯士设备的安全密钥库内。

传输层安全 (TLS)：一种用于保护网络通信的互联网标准。HTTPS中的S（安全）就是由TLS提供的。

可信执行环境 (TEE)：提供基于硬件的防篡改私钥存储，并安全执行加密操作。与安全元素和TPM不同，TEE是系统级芯片 (SoC) 主处理器中隔离硬件的安全区域。

可信平台模块 (TPM)：一种加密计算模块，提供基于硬件的防篡改私钥存储，并安全执行加密操作。TPM是由*可信计算组织 (TCG)*定义的国际标准化计算机组件（TPM 1.2、TPM 2.0）。

零信任安全：一种先进的IT安全策略，其中已连接的设备和IT基础设施（如网络、计算机、服务器、云服务和应用程序）需要循环地对彼此进行识别、确认和身份验证，以实现高安全性控制。

T10190380/zh/M3.5/2404

关于 Axis Communications

Axis 通过打造解决方案，不断提供改善 以提高安全性和业务绩效。 作为网络技术 公司和行业领导者，Axis 提供视频监控解决方案， 访问控制、对讲以及音频系统的相关产品和服务。 并通过 智能分析应用实现增强，通过高品质培训提供支持。

Axis 在 50 多个国家/地区拥有约 4,000 名敬业的员工 并与全球的技术和系统集成合作伙伴合作 为客户带来解决方案。 Axis 成立于 1984 年，总部 在瑞典隆德