已簽署的韌體、安全開機，以及私密金鑰的安全性

Axis 產品的網路安全功能

七月 2020

目錄

1 摘要

本文件說明 Axis 產品中可以減輕網路威脅並防範特定攻擊類型的部分功能。 功能包括：

- 已簽署的韌體
- 安全開機
- 信任平台模組 (TPM)
- Axis Edge Vault (利用 Axis 裝置 ID)。

概述的威脅包括：

- 韌體竄改
- 供應鏈竄改
- 擷取私密金鑰
- 未經授權的裝置更換。

1.1 已簽署的韌體

已簽署的韌體由使用私密金鑰簽署韌體映像的軟體廠商實作。 韌體附加簽章時，裝置將會在接受韌體安裝前驗證韌體。 如果裝置偵測到韌體完整性遭入侵，將會拒絕韌體升級。

1.2 安全開機

安全開機是一種開機程序，由未間斷的軟體 (以密碼編譯驗證) 鏈結組成，從不可變動的記憶體 (開機 ROM) 開始。 安全開機以簽署的韌體為基礎，確保裝置僅能使用授權的韌體開機。

1.3 TPM

TPM 是一項元件，提供用於保護資訊不被未經授權存取的密碼編譯功能組。 私密金鑰儲存於 TPM 內，且所有密碼編譯操作均需使用傳送至 TPM 處理的私密金鑰。 如此可確保憑證的密碼部分仍安全無虞，即使是出現安全性缺口。 用於所選 Axis 產品中的 TPM 經過認證，以符合 FIPS 140-2 的需求。

1.4 Axis Edge Vault (利用 Axis 裝置 ID)

新型國際標準 IEEE 802.1AR 說明如何自動化並保護網路上裝置識別的程序。 在 Axis 產品中，這些安全性措施是透過使用 Axis Edge Vault 和 Axis 裝置 ID 的方式實作。 Edge Vault 可以用於以安全儲存的憑證操作的密碼編譯盤問。 憑證的私密部分保留在 Edge Vault 內，即使正在使用中。 Axis 裝置 ID 會安全、永久地儲存於 Edge Vault 中，並作為 Axis 根憑證簽署的憑證，因此能在產品的生命週期內達到全新的裝置信任境界。

2 字彙表

憑證 — 在密碼編譯中，憑證是證明金鑰組來源和屬性的簽署文件。 憑證是由憑證授權單位 CA 簽署，且如果系統信任 CA，則也會信任其核發的憑證。

憑證授權單位 CA — 憑證鏈結的信任根目錄。 它用於證明基礎憑證的真確性和真實性。

FIPS — 聯邦資訊處理標準是用於資料加密和資料安全性的標準，是由 NIST (國家標準暨技術研究院) 在美國發佈。

不可變動的 ROM — 安全地儲存信任的公開金鑰和用於比較簽章的程式，因此無法被覆寫。

佈建 — 準備和配備網路裝置的程序。 此工作涉及從中心點提供組態資料和原則設定至裝置。 裝置隨附金鑰和憑證。

公開金鑰密碼編譯 — 對稱式密碼編譯，其中任何人都可使用接收者的*公開金鑰*加密訊息，但唯有使用*公開金鑰*的接收者可以將訊息解密。 可以用於加密和簽署訊息。

TLS — 傳輸層安全性，用於保護網路流量的網際網路標準。 TLS 在 HTTPS 提供 S (用於保護)。

3 簡介

Axis 依照業界管理並因應旗下產品中安全性弱點的最佳實務，以盡量減少客戶暴露於網路風險的機會。 沒有任何一種方式可以確保產品和服務毫無遭到惡意攻擊利用的瑕疵。 這不是 Axis 特有的狀況，而是所有網路裝置的一般狀況。 Axis 可以保證的是，我們始終在每個可能的階段齊心協力，以確保與您的 Axis 裝置和服務承受最小的相關風險。

如需產品安全性和發現的弱點詳細資訊，請參閱 *www.axis.com/support/product-security*。 如需您可以採取措施以減少常見威脅風險的詳細資訊，請從 *www.axis.com/cybersecurity* 下載 Axis 強化指南。

此白皮書提出部分合理的網路攻擊及如何在 Axis 產品中防止這些攻擊。 白皮書也具體說明功能如何簽署韌體且安全開機如何防止韌體竄改與供應鏈竄改。 我們也會討論信任平台模組 (TPM) 和 Axis Edge Vault 的使用，這兩者都可用於保護私密金鑰。 Axis Edge Vault 用於安全地儲存實現全新裝置信任境界的 Axis 裝置 ID。

4 韌體竄改偵測

在攻擊者未能順利侵入系統後可能會嘗試進行的一項攻擊特徵就是，讓系統擁有者安裝經過修改的應用程式、韌體或其他軟體模組。 修改過的軟體可能包括特定用途的惡意程式碼。 常見的建議是切勿安裝來自您無法完全信任之來源的任何軟體。 在視訊系統情境下，可能會有「中間人」修改裝置韌體並誘使一般使用者安裝該韌體。 這不容易做到，攻擊者需要技巧純熟並下定決心。 他需要極為了解 Axis 韌體設計，以及韌體在裝置中的運作方式。 若攻擊特定系統的價值不夠高，這些攻擊者也仍可能存在。 軟體廠商常見的對策就是使用簽署的韌體。

4.1 韌體簽署

簽署的韌體是由軟體廠商實作，以秘密保留的私密金鑰簽署韌體映像。 韌體附加簽章時，裝置將會在接受韌體安裝前驗證韌體。 如果裝置偵測到韌體完整性遭入侵，將會拒絕韌體升級。

簽署韌體的程序是透過密碼編譯雜湊值運算啟動。 在簽章附加到韌體映像之前，此值會以私密/公開金鑰組簽署。

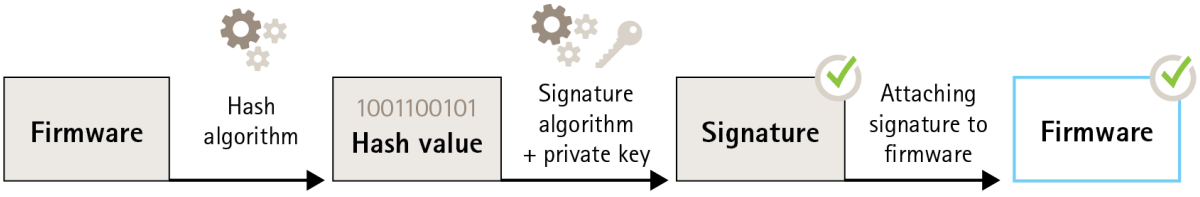

Figure 1. 簽署韌體的程序。

韌體升級前，必須先驗證新韌體。 為確保新韌體完好如初，公開金鑰 (Axis 產品隨附) 用於確認雜湊值確實是以相符的私密金鑰簽署。 也可運算韌體的雜湊值，然後將此值與簽章經過驗證的雜湊值進行驗證，來驗證韌體的完整性。

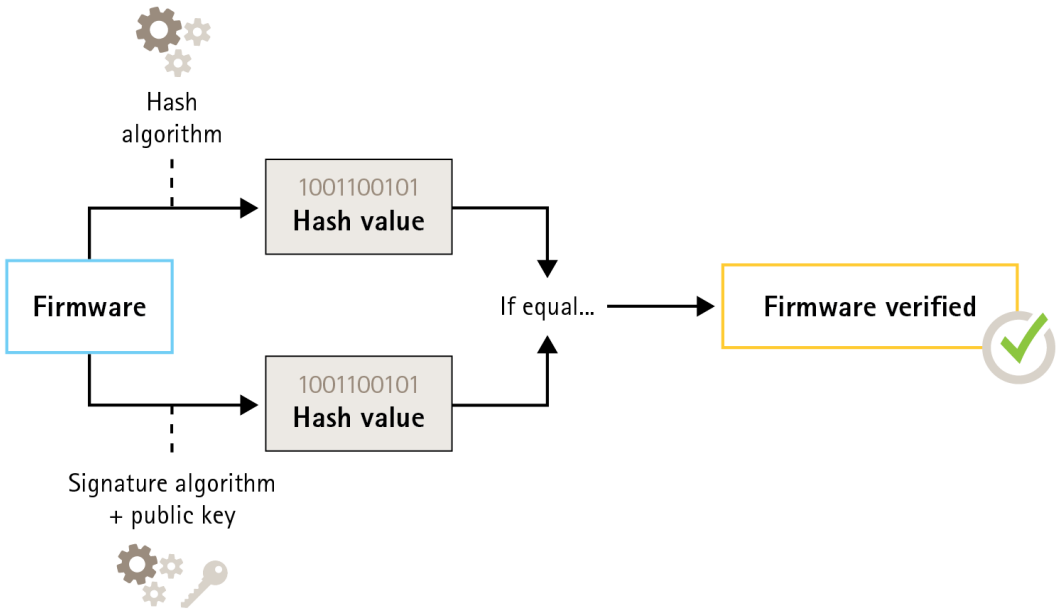

Figure 2. 驗證已簽署韌體的程序。

4.2 Axis 已簽署的韌體

Axis 已簽署的韌體是以業界接受的 RSA 公開金鑰加密方法為基礎。 私密金鑰儲存在 Axis 受到緊密保護的位置，同時公開金鑰內嵌於 Axis 裝置內。 整個韌體映像的完整性是以映像內容的簽章確保。 主要簽章驗證許多次要簽章，並在驗證時將映像解壓縮。

5 防止供應鏈竄改

韌體簽署可以在所有未來的韌體更新中防止裝置安裝遭入侵的韌體。 但如果有中間人在裝置從廠商提供給使用者的路上修改裝置？ 在運送期間可以拿取裝置的攻擊者便會執行此類攻擊，例如入侵裝置的開機分割區、繞過韌體完整性檢查，以在裝置部署前安裝經過修改的惡意韌體。

5.1 安全開機

安全開機是一種開機程序，由未間斷的軟體 (以密碼編譯驗證) 鏈結組成，從不可變動的記憶體 (開機 ROM) 開始。 安全開機以簽署的韌體為基礎，確保裝置僅能使用授權的韌體開機。

開機程序以驗證開機載入器的開機 ROM 啟動。 安全開機然後即時驗證從快閃記憶體載入之各韌體區塊的嵌入式簽章。 開機 ROM 做為信任跟目錄，然後唯有驗證每個簽章，才會

繼續進行開機程序。 鏈結的每個部分會驗證下一個部分，最終達成驗證的 Linux 核心和驗證的根檔案系統。

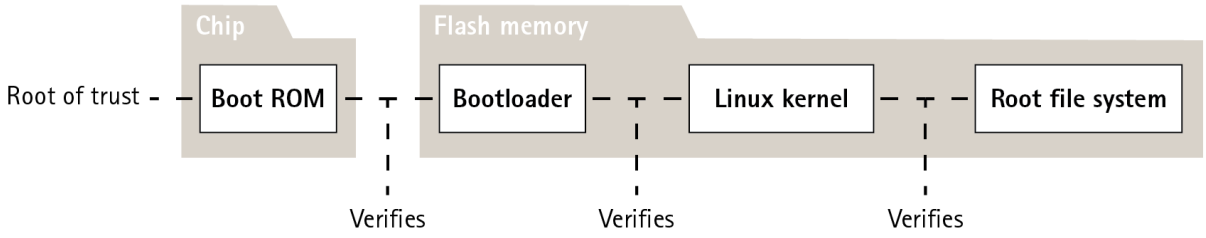

Figure 3. 安全開機程序。

5.2 Axis 安全開機

在許多裝置中，應無法修改低階功能。 當其他安全性機制是以下層軟體建置時，安全開機作為安全基礎層運作，防止這些機制遭到規避。

如果裝置設有安全開機功能，安裝於快閃記憶體的韌體會受到保護，無法修改。 出廠預設設定映像受到保護，同時組態仍未受到保護。 安全開機確保在出廠預設設定後，Axis 裝置完全不被可能的惡意程式碼侵入。

5.3 安全開機與自訂韌體憑證

雖然安全開機可以讓產品變得更安全，但確實也會降低不同韌體的彈性，因而讓載入任何臨時韌體的動作變得更複雜，例如將 Axis 的測試韌體或其他自訂韌體載入產品時。 然而，Axis 已實行核准個別裝置的機制，可接受此類非實際執行的韌體。 此韌體透過不同的方式簽署，並經過擁有者和 Axis 核准，因此會產生自訂韌體憑證。 安裝於核准的裝置時，憑證會根據其唯一的序號和晶片 ID，啟用僅可在核准的裝置上執行的自訂韌體。 由於 Axis 持有簽署憑證的金鑰，因此自訂韌體憑證僅可由 Axis 建立。

6 私密金鑰的安全性

Axis 裝置支援使用 TLS (傳輸層安全性) 的 HTTPS (網路加密) 和 802.1X (網路存取控制)。 TLS 的數位憑證使用公開/私密金鑰組。 私密金鑰儲存於裝置中，而公開金鑰則包含在憑證中。 請注意，如果未使用 HTTPS 或 802.1X，便無金鑰要保護。

攻擊者可能會嘗試從裝置擷取私密金鑰和憑證，然後安裝於攻擊電腦上。 若採用 HTTPS，該私密金鑰可用於竊聽裝置與 VMS 之間的加密網路流量。 或者，如果欺騙網路，則攻擊電腦可以佯裝是合法裝置來存取 VMS。 如果是 802.1X，攻擊者則可能使用私密金鑰存取受 802.1X 保護的網路，充當受信任的裝置。

憑證和私密金鑰一般儲存在裝置的檔案系統中，並以帳戶存取原則保護並用於一般運算環境中。 在大多數情況下，由於該帳戶不容易遭盜用侵，因此此做法足以足夠。 請注意，如果疑似遭盜用，則可撤銷憑證，讓私密金鑰毫無用武之地。

關鍵系統的部分使用者可能會因攻擊者訓練有素且下定決心要嘗試入侵裝置，以擷取私密金鑰，而致使風險提高。 信任平台模組 (TPM) 會以近乎無法擷取的方式儲存金鑰，即使裝置遭到入侵。

6.1 使用 TPM (信任平台模組) 進行安全金鑰儲存

TPM 是一項元件，提供用於保護資訊不被未經授權存取的某種密碼編譯功能組。 私密金鑰儲存 TPM 之中，且絕不會從 TPM 離去。 所有密碼編譯操作均需使用傳送至 TPM 處理的私密金鑰。 如此可確保憑證的密碼部分絕不會離開 TPM 內的安全環境並仍安全無虞，即使是出現安全性缺口。

6.2 FIPS 140-2 認證

對於某些產品和使用案例而言，法規可能要求要將 TPM 用於保護資訊，有時會加上 FIPS 140-2 法務遵循需求。 FIPS (聯邦資訊處理標準) 140-2 是密碼編譯模組的資安標準，是由 NIST (國家標準暨技術研究院) 在美國發佈。

經過 NIST 認證測試實驗室驗證後，即可確保模組系統和模組的密碼編譯皆正確實作。 簡而言之，認證需要密碼編譯模組的描述、規格和驗證、核准的演算法、核准的操作模式和開機測試。

如需 FIPS 140-2 認證需求的詳細資訊，請參閱 NIST 網站
https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards

6.2.1 Axis 產品中的認證 TPM

用於所選 Axis 產品中的 TPM 經過認證，以符合 FIPS 140-2 的需求。 更具體來說，它已通過標準的安全性等級 2 認證，這意味著 TPM 也滿足角色型授權和竄改證據等需求。

7 IEEE 802.1AR - 使用 Axis 裝置 ID 的裝置驗證

購買 Axis 網路裝置的人員可以在開始使用前進行手動檢查。 客戶可以透過先前對於 Axis 產品外觀和風格的理解目視檢查產品，認為該產品確實是來自 Axis。 然而，此類檢查僅可由能夠實際拿取產品的人員完成。 因此，當您與網路上非佈建產品進行通訊息，您如何確定自己與正

確的單元進行通訊？未經授權就更換裝置嗎？伺服器上的連網設備或軟體都無法進行實物檢查。常見的安全性措施是在封閉式網路上先與新產品進行互動，以便在此處安全地佈建單元。

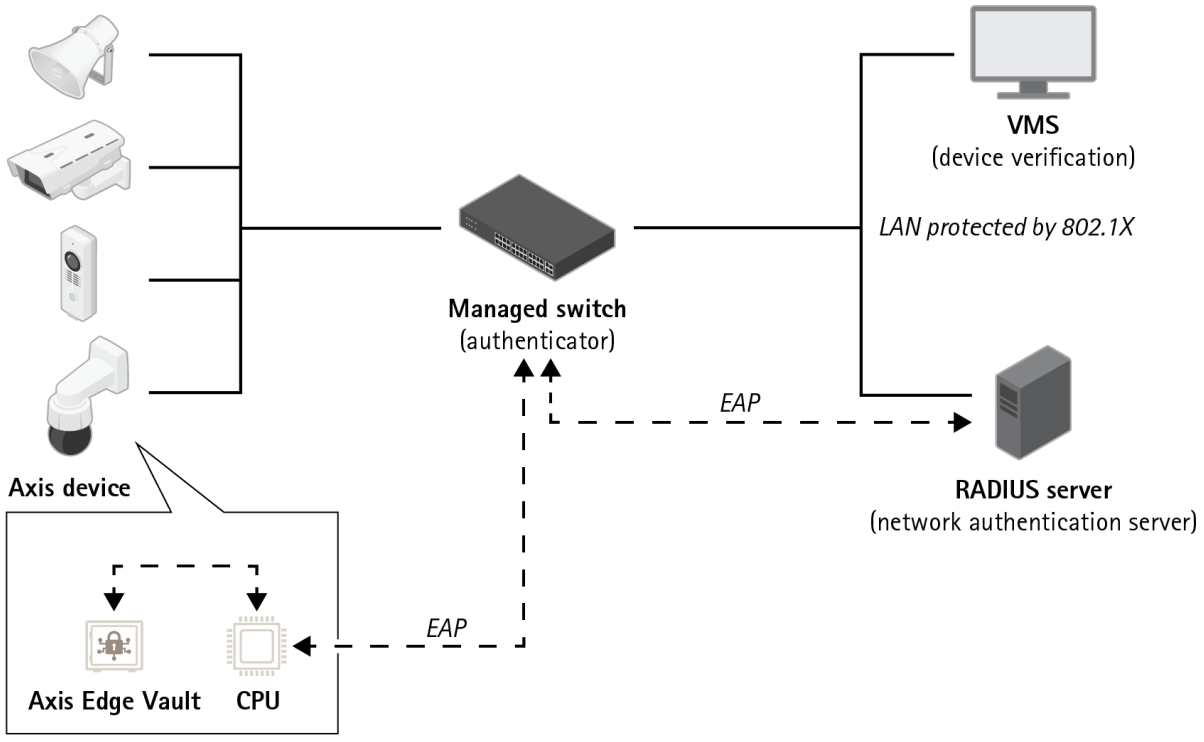

Figure 4. 客戶可以指示其驗證伺服器使用裝置序號和 Axis 裝置 ID 自動網路上購買的 Axis 產品。

新的國際標準 IEEE 802.1AR (*https://1.ieee802.org/security/802-1ar/*) 定義如何自動化和確保網路上裝置識別的方法。 如果通訊轉送到內嵌式安全模組，單元則可根據標準傳回值得信任的識別回應。

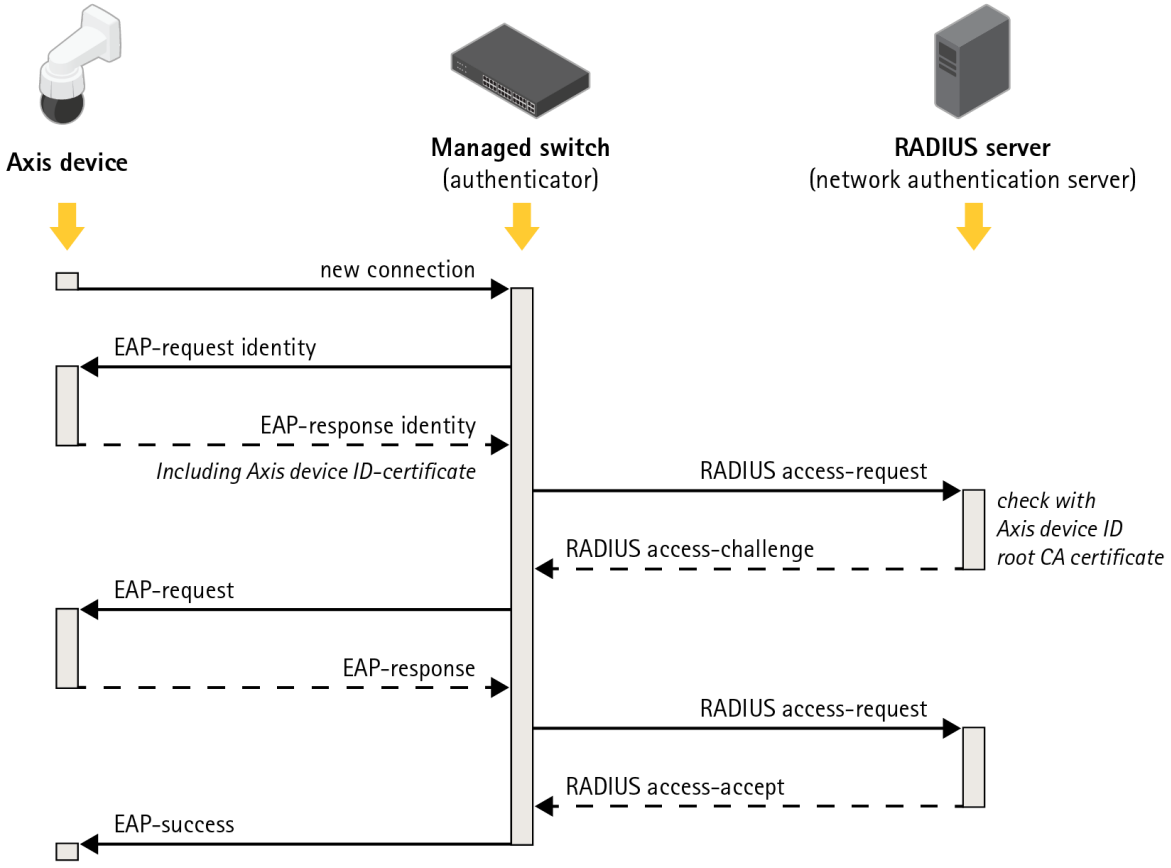

Figure 5. IEEE 802.1AR 定義如何透過以下方式識別網路上裝置的方法：遵循傳送可延伸的驗證通訊協定要求 (AEP) 至使用遠端驗證撥入使用者服務 (RADIUS) 之交換器的通訊協定 - 要求授與存取權。

在 Axis 產品中，這些安全性措施是透過使用 Axis Edge Vault 和 Axis 裝置 ID 的方式實作。 Axis Edge Vault 是安全模組，其中會安裝 Axis 裝置 ID (用於驗證裝置識別的集合)。 這些功能提供網路能以密碼編譯方式驗證的證明，用於證明特定單元是由 Axis 生產且確實是由該單元進行網路連線。

包含 Axis 裝置 ID 的裝置已佈建於原廠 (包含金鑰和憑證)。 此佈建之後可供客戶用於在現場使用其他金鑰和/或憑證進一步佈建裝置，以便存取客戶的部分網路資源。

識別包含 Axis 裝置 ID 的單元後，即可減少裝置部署時間，這是因為在預期網路上安裝和設定裝置前，裝置所需的工作會變少。 另一項好處是，先不說提供其他內建的信任來源，Axis 裝置 ID 也提供在大型系統中記錄裝置的方式。

7.1 Axis Edge Vault

Axis Edge Vault 是安全密碼編譯運算模組，以安裝於產品內 PCB 上的晶片形式呈現。 Edge Vault 可以安全地儲存憑證，並用於安全儲存之憑證的密碼編譯操作。

儲存於 Edge Vault 的憑證無須送出，以便供裝置使用。 憑證會安全地保留在 Edge Vault，即使正在使用憑證時，這是因為以金鑰操作的密碼編譯硬體安裝於相同的實體晶片上。

7.2 Axis 裝置 ID

在生產每台 Axis 網路裝置單元的期間，稱為 Axis 裝置 ID 的「數位護照」已安全地安裝於單元的 Axis Edge Vault 之中。 每個單元的身分都是唯一的，用於證明裝置的原產地。 Axis 裝置 ID 是用於模組密碼編譯操作部分的憑證集合，用於簽署嵌入式產品韌體向 Edge Vault 提出的盤問。 此操作的回應會傳回可使用 Axis 公用金鑰驗證回應驗證的接收器。

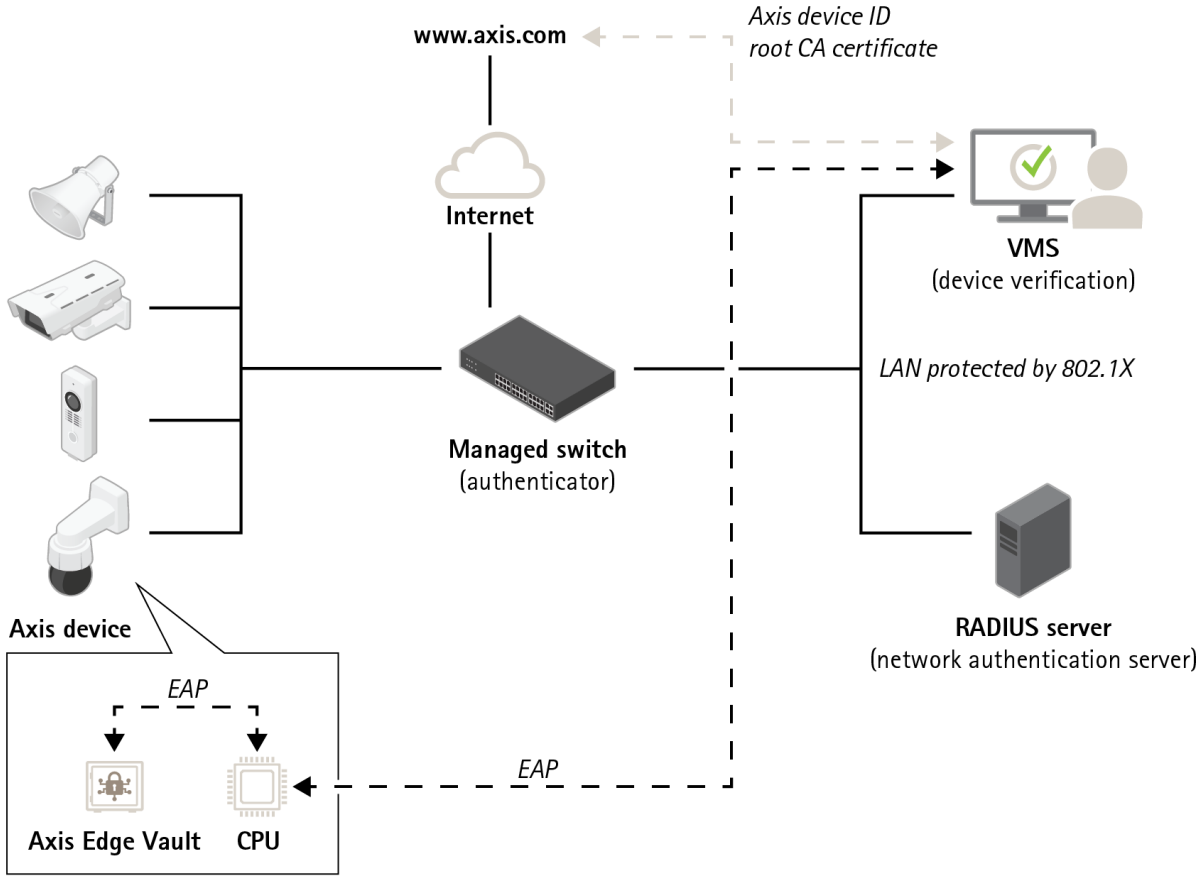

Figure 6. 系統其他部分中的軟體應用程是可以使用 Axis 裝置 ID 和密碼編譯操作驗證進行通訊的對象。 Axis 裝置 ID 是以來自 axis.com 公用 Axis 裝置 ID 根 CA 憑證驗證。

7.2.1 憑證階層

憑證是一小撮資料，其中結合公開金鑰與中繼資料 (描述金鑰和簽發者的簽章)，以證明憑證的有效性。

憑證階層是證明憑證來源的方式。 接著請思考一下 Axis 裝置 ID與護照之間的比喻。 如果您持有護照，則表示您所在國家/地區的政府提供保證，證明您是護照上所聲稱之人。 同樣地，所有 Axis 裝置 ID 憑證皆有 Axis 裝置 ID 根 CA 憑證的背書。 正如海關關員信任您的

國家/地區政府已正確核發您的護照，網路安全性系統也信任 Axis 裝置 ID 根 CA 憑證已正確驗證連網單元的 Axis 憑證。

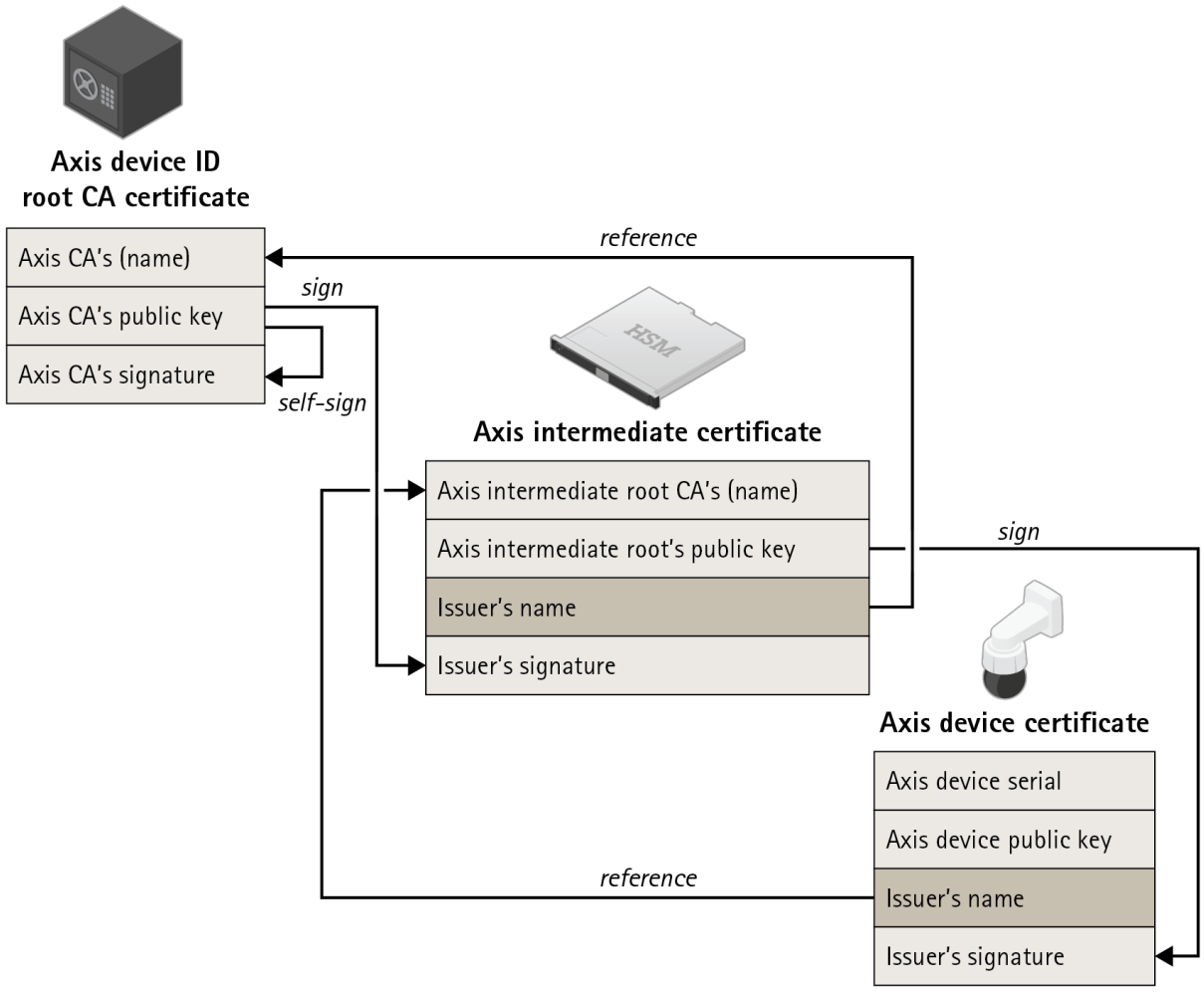

Figure 7. Axis 裝置 ID 是加入產品序號的憑證並由中繼憑證簽署，而中繼憑證則是由 Axis 根憑證簽署。由於 Axis 根憑證非常寶貴，且須要儲存於安全之處，因此在原廠佈建期間須則使用中繼憑證。

關於安迅士

安迅士透過打造網路解決方案，協助改善安全與創新企業營運模式，，讓世界變得更聰明且更安全。身為網路影像產業領導者，安迅士提供影像監控與分析、門禁管理及音訊系統產品與服務。

安迅士在50多個國家擁有超過3,500名專職員工，並與全球合作夥伴合作提供客戶解決方案。安迅士成立於1984年，總部位在瑞典隆德市

關於安迅士的更多資訊，請參閱本公司網站 *axis.com*