白皮書

Axis Edge Vault (憑證伺服器)

這是防護安迅士設備的硬體網路安全平台，可提供：

— 信任的設備身分

— 安全金鑰儲存區

— 影像竄改偵測

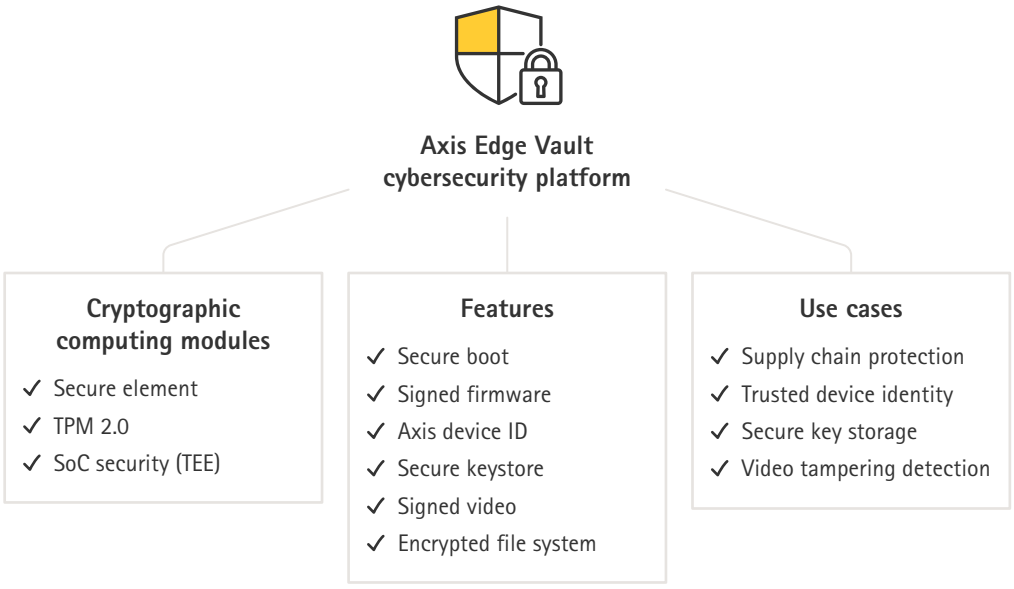
— 供應鏈防護

4 月 2023

總結

Axis Edge Vault (憑證伺服器)提供一個防護安迅士設備的硬體網路安全平台。其仰賴強大的密碼學運算模組(安全元件和TPM)與SoC安全(TEE和安全開機)基礎，並結合邊際設備安全的專業知識。Axis Edge Vault (憑證伺服器)具有自己的強大信任根源錨點，這是由*安全開機*搭配*已簽署的韌體*確立的。這些功能可建立堅固的密碼學驗證軟體鏈建構之信任鏈，這是所有安全操作的基礎。

安迅士設備搭配Axis Edge Vault (憑證伺服器)可透過預防竊聽和惡意提取敏感資訊，減少客戶接觸的網路安全風險。Axis Edge Vault (憑證伺服器)也讓安迅士設備成為客戶網路中可信任且可靠的裝置。



- 信任的設備身分：能夠驗證設備的來源，是在設備識別中建立信任的關鍵。生產期間，搭配Axis Edge Vault (憑證伺服器)的設備會被指派一個獨特、原廠佈建且符合IEEE 802.1AR的安迅士設備ID憑證。這可作為通行護照證明設備的來源。設備ID安全且永久儲存在安全金鑰儲存區內，作為以安迅士根憑證簽署的憑證。設備ID可由客戶的IT基礎架構用於自動化安全設備接入與安全設備識別。
- 安全金鑰儲存區：安全金鑰儲存區可用硬體防竄改方式儲存密碼學資訊。安全金鑰儲存區保護安迅士設備ID以及客戶載入的密碼學資訊，並可在發生安全侵駭事件時，防止非授權存取和惡意提取。
- 影像竄改偵測：已簽署的影像確保可驗證影像證據未經竄改，而不需要提供影像檔案的監管鏈。每台攝影機使用本身獨特的影像簽署金鑰，金鑰安全儲存在安全金鑰儲存區內，可將簽章加入影像串流中。播放影像時，檔案播放器會顯示影像是否完整。已簽署的影像可將影像回溯到來源攝影機，並驗證影像離開攝影機後並未遭受竄改。
- 供應鏈防護：Axis Edge Vault (憑證伺服器)要求可作為信任根源的安全基礎。若沒有安全開機和已簽署的韌體協助，就無法建立信任鏈的根源。安全開機搭配已簽署的韌體，可從不可變記憶體(開機ROM)開始，提供堅固的密碼學驗證軟體鏈。安全開機可確保設備只能使用安迅士已簽署的韌體開機，防止實體供應鏈竄改。藉由已簽署的韌體，設備也能在接受並安裝之前，先驗證新韌體。如果設備偵測到韌體完整性不足，或韌體並非由安迅士簽署，將拒絕韌體升級。這可防止設備遭受韌體竄改。

目錄

1 簡介

安迅士遵循業界最佳實務經驗，以在我們的產品中實作安全性。這樣做是為了減少客戶暴露到網路安全風險，並讓安迅士設備成為客戶網路上的可信裝置。

Axis Edge Vault (憑證伺服器)提供一個防護安迅士設備的硬體網路安全平台。其建立在強大的密碼學運算模組(安全元件和TPM)與SoC安全(TEE和安全開機)基礎上，並結合邊際設備安全的專業知識。

這份白皮書將摘述安迅士邊際設備安全的多層次方法，並呈現常見風險以及如何預防風險。Axis Edge Vault (憑證伺服器)要求可作為信任根源的安全基礎。因此，我們也會檢視安迅士設備的供應鏈安全層面，並了解已簽署的韌體和安全開機，如何作為防範韌體竄改以及實體供應鏈竄改的基本措施。

在*https://www.axis.com/support/cybersecurity/resources*，可找到有關產品安全、已發現安全漏洞、和您可以採取以降低常見威脅風險之措施的更多資訊。

本白皮書的最後一章包含字彙表。

2 信任的設備身分

在現代的零信任安全網路中(「絕不信任、始終驗證」)，能夠驗證設備來源、其真實性和連線的能力，是一項基本需求。網路設備驗證其完整性和真實性的方式，與您在機場出示護照向主管單位驗證您身分的方式類似。

2.1 以安迅士設備ID進行安全設備識別

國際標準*IEEE 802.1AR*定義如何自動化並保護網路上裝置識別的方法。如果通訊轉送到嵌入式密碼學運算模組，設備可根據標準傳回值得信任的識別回應。網路基礎架構可以使用這個可信任回應，以便將設備自動化並安全接入佈建網路進行初始設定和韌體更新。

為了符合IEEE 802.1AR，我們以設備特有且原廠提供的安迅士設備ID憑證(IEEE 802.1AR初始設備識別碼，IDevID)，製造我們大部分的設備。安迅士設備ID會安全儲存在，透過設備本身密碼學運算模組提供的防竄改安全金鑰儲存區中。每個安迅士設備的身分都是唯一的，設計用於證明設備的原產地。

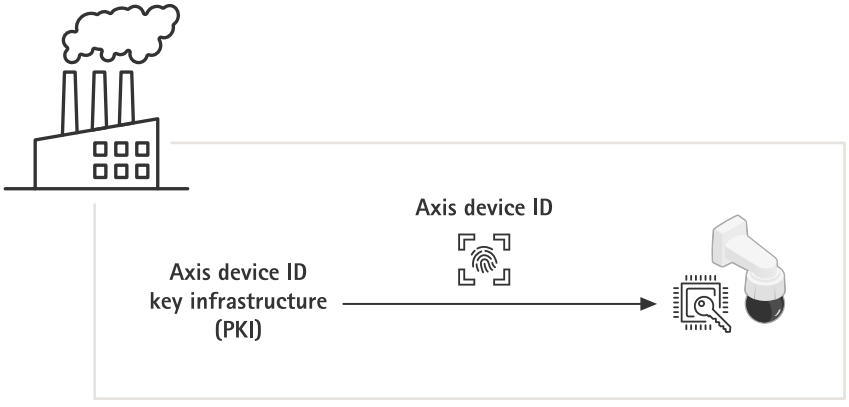


Figure 1. 在裝置的製造過程中，獨特的安迅士設備ID會儲存在裝置的安全金鑰儲存區中。

IEEE 802.1AR是基於用於網路存取管控的IEEE 802.1X標準，在預選安迅士設備ID的安迅士設備中會預設啟用。這可讓安迅士設備即使在原廠預設狀態下，也能透過具備802.1X能力的IT基礎架構，進行安全識別和身分驗證。

安迅士設備ID憑證可採用多種密碼學組態(2048位元RSA、4096位元RSA、ECC-P256)。這些會預設啟用，以便透過IEEE 802.1X網路存取管控與HTTPS，進行安全設備連線和識別。

安迅士管理其自有的專屬IEEE 802.1AR公開金鑰基礎架構(PKI)，以便在製造過程中由原廠佈建安迅士設備ID。安迅士設備ID由中間憑證簽署，其進而由安迅士根憑證簽署。根源CA和中間CA都安全儲存在地理區域分離的密碼學運算模組中。這可在安迅士生產設施發生安全侵駭事件時，防止惡意提取。有關安迅士PKI基礎架構的更多資訊，請參閱 *www.axis.com/support/public-key-infrastructure-repository*

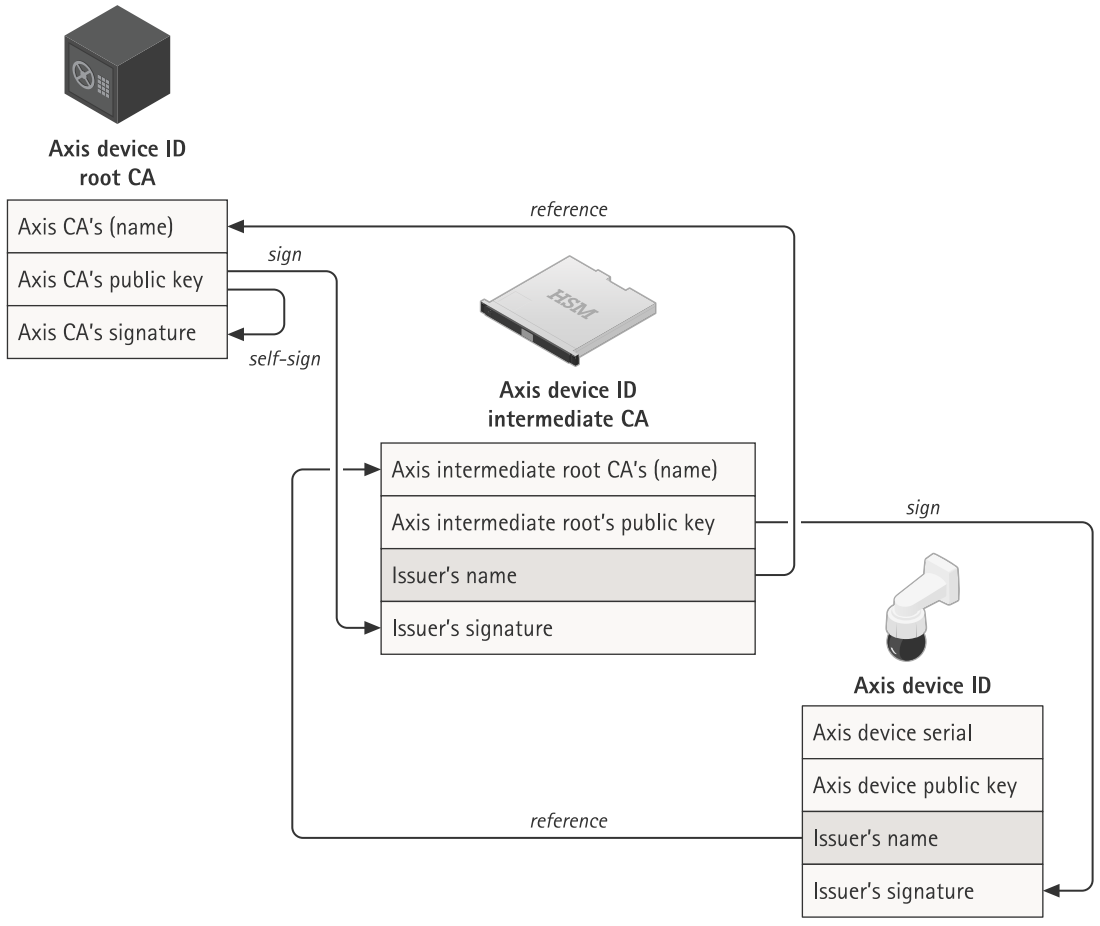


Figure 2. 在製造過程中，由原廠佈建安迅士設備ID的安迅士IEEE 802.1AR公開金鑰基礎架構(PKI)。安迅士設備ID是納入產品序號的憑證，由一個中間CA簽署，而中間CA由安迅士設備ID根源CA簽署。由於安迅士根源CA非常寶貴且需要儲存在安全處所，原廠佈建期間需要中間CA。

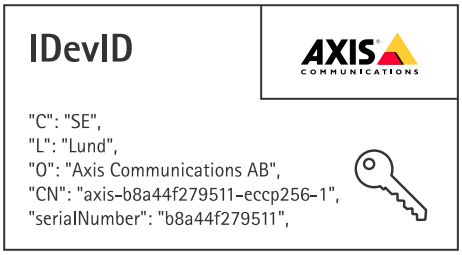


Figure 3. 安迅士設備ID範例。

2.2 安全接入網路

您購買安迅士設備時，可以在開始使用之前進行手動檢查。透過目視檢查設備並使用有關安迅士產品外觀的既有知識，您可以相信設備來自安迅士。不過您只能在實體接觸設備時，才能進行這類檢查。因此您在網路上與設備通訊時，要如何確認您與正確的設備通訊，並且能夠驗證其身分？伺服器上的連網設備或軟體都無法進行實物檢查。常見的安全性做法是在封閉式網路上先與新設備進行互動，以便在此安全地佈建設備。

安迅士設備ID將能以密碼學驗證的證明提供給網路，用於證明特定設備是由安迅士生產，且確實是由該設備進行網路連線。IEEE 802.1X網路身分驗證流程中可使用安迅士設備ID存取佈建網路，先在其中進行後續韌體更新和安迅士設備設定，再將安迅士設備移到生產網路中。

透過使用安迅士設備ID，可提升整體安全並縮短設備佈建時間，因為可以將更自動化且具成本效益的管控用於設備安裝和設定。

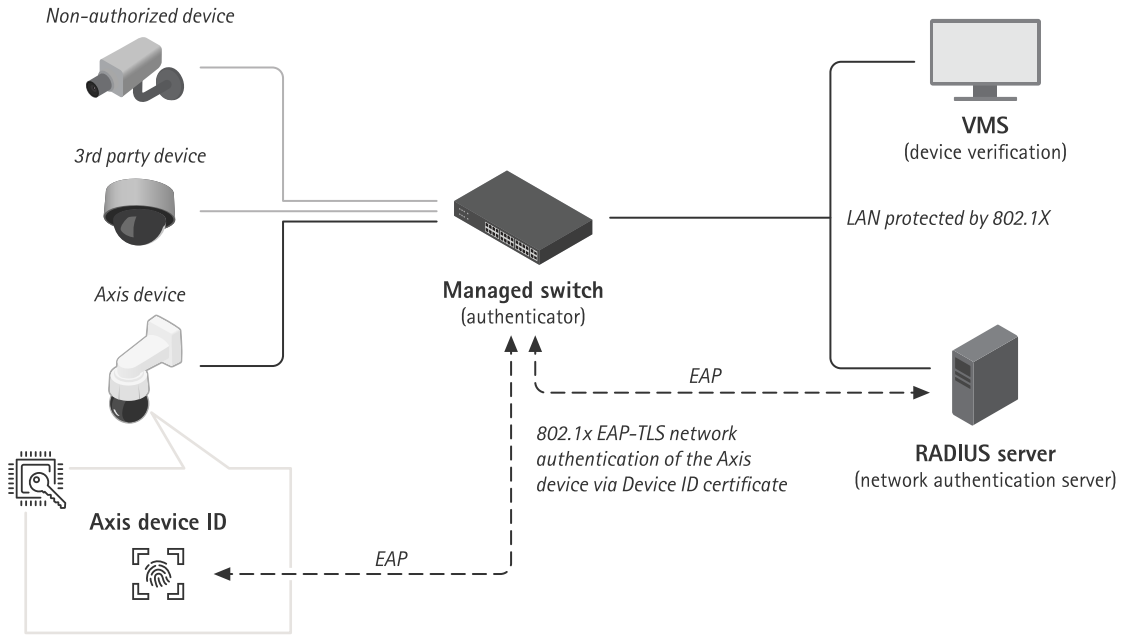


Figure 4. 安全接入網路。您可以指示身分驗證伺服器，使用設備序號和安迅士設備ID，自動接受網路上的安迅士設備。安迅士設備ID可用來作為指紋，確保將設備安全且自動接入網路。未授權設備必須手動接入網路。

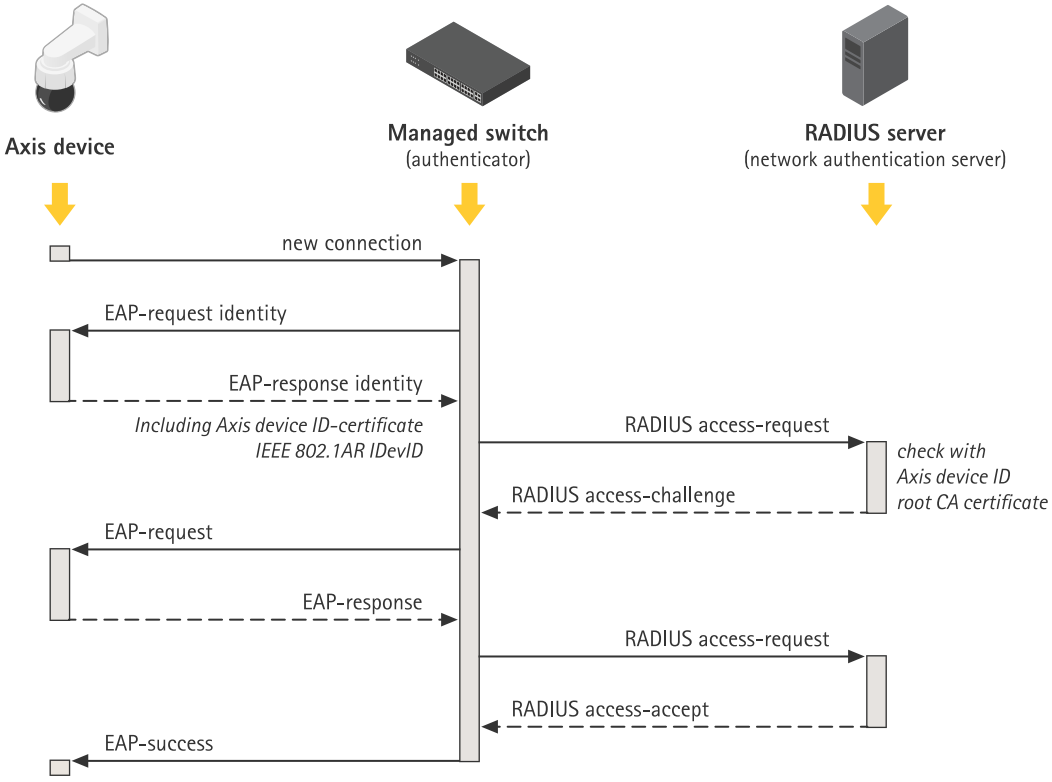


Figure 5. 接入流程的更詳細說明。用於安全設備識別的IEEE 802.1AR，定義如何使用遠端身分驗證撥接使用者服務(RADIUS)伺服器，透過IEEE 802.1X可擴展身分驗證協定要求(EAP-TLS)，識別設備以授予設備存取網路權限的方法。

除了提供額外、內建的信任來源以外，安迅士設備ID也提供追蹤設備的方式，並可依據零信任網路原則，定期進行驗證和身分驗證。

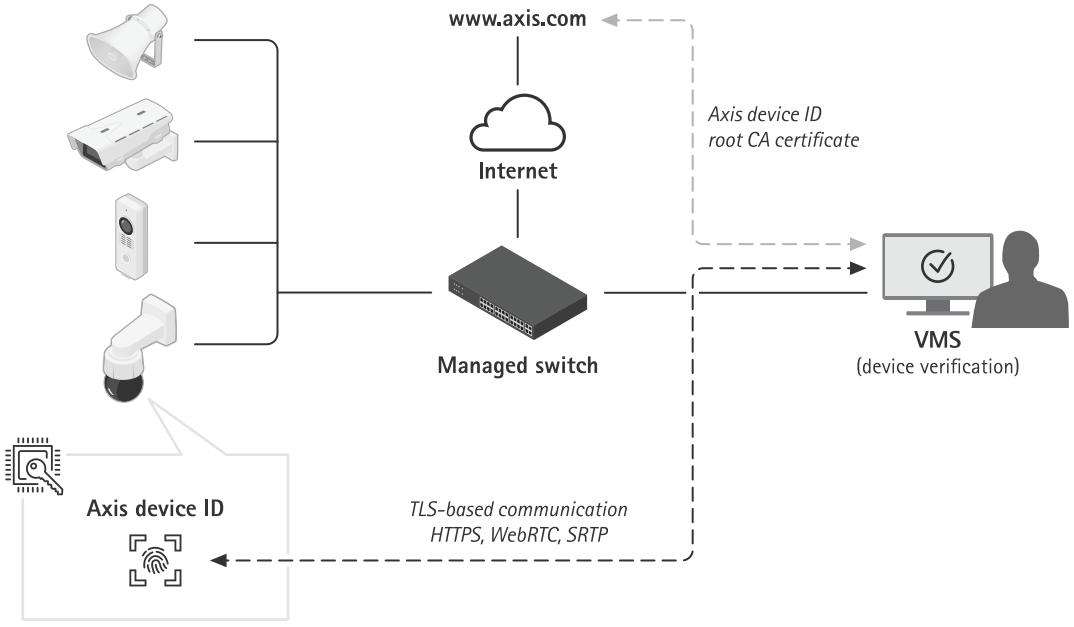


Figure 6. 設備安全接入網路後，系統其他部分中的軟體應用程式，可以使用安迅士設備ID和密碼學操作，在多項基於TLS的通訊中驗證設備。安迅士設備ID可以由公開可用的安迅士設備ID根源CA憑證驗證，此憑證可從axis.com下載。

3 安全金鑰儲存區

傳統上，敏感的X.509密碼學資訊(私密金鑰)會儲存在設備的檔案系統內。僅受到使用者帳戶存取原則保護，這能夠提供基本的保護，因為使用者帳戶不會輕易遭受突破。不過如果發生安全侵駭事件，這些密碼學資訊將不再受到保護，且能被不法份子取得。

從安全觀點看來，安全金鑰儲存區對於儲存和保護密碼學資訊非常關鍵。安全金鑰儲存區不僅儲存包含在安迅士設備ID和已簽署的影像中的敏感密碼學資訊，客戶載入的資訊也可以使用相同方式保護。

3.1 安全金鑰儲存區

敏感的密碼學資訊(私密金鑰)儲存在設備的硬體防竄改安全金鑰儲存區中。這可在出現安全侵駭事件時，防止惡意提取。還有，私密金鑰即便使用時，也會在安全金鑰儲存區中持續受到保護。潛在不法份子將無法存取安全金鑰儲存區，且無法竊聽網路流量、透過IEEE 802.1X金鑰存取網路，或提取其他私密金鑰。

安全金鑰儲存區是透過硬體密碼學運算模組提供的。取決於安全要求，安迅士設備可能具備一個或多重此類模組，例如TPM 2.0 (信任平台模組)或安全元件，和/或TEE (信任執行環境)。

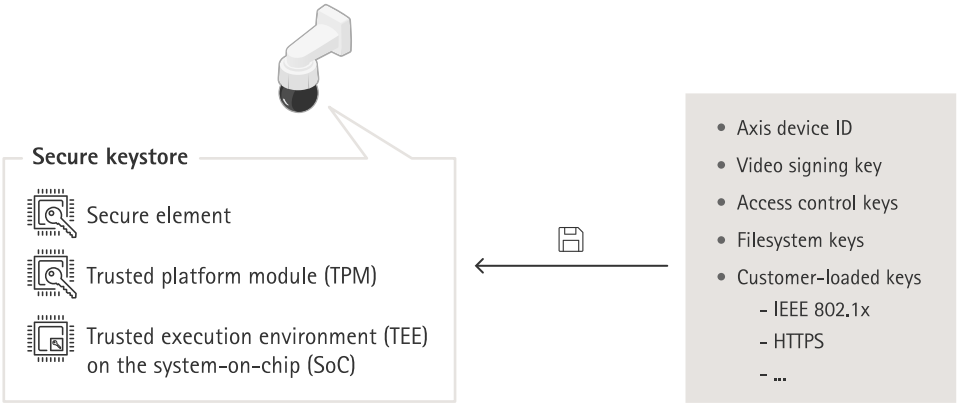


Figure 7. 安迅士設備中配備的安全金鑰儲存區，可採用安全元件、TPM或TEE。它們都可以防護私密金鑰，並安全執行密碼學操作。

TPM和安全元件是硬體密碼學運算模組，安裝在SoC主要處理器旁的電路板上。TEE是SoC主要處理器本身的安全區。

TPM、安全元件和TEE都能防護私密金鑰，並安全執行密碼學操作。若出現安全侵駭事件，可防止未授權存取和惡意提取。

3.2 共同準則與FIPS 140

密碼學運算模組可以使用共同準則評估等級(CC EAL)以及FIPS 140合規等級(1-4)驗證。這些認證用於判斷密碼學操作的正確性與完整性，並驗證多項防竄改措施，例如自我驗證、防竄改和其他防範措施。您可以在安迅士設備的型錄上或在安迅士產品選擇工具中，找到有關認證的資訊。安迅士要求其納入的硬體密碼學運算模組，必須至少通過共同準則EAL4和/或FIPS 140-2/3等級2的認證。

3.2.1 共同準則

共同準則(CC) (也稱為資訊安全評估的共同準則)，是IT產品安全認證的國際標準(ISO/IEC 15408)。共同準則為製造商和實作者提供一個框架，將安全功能性和保證要求列為「安全目標」，這些目標則可分組為「保護設定檔」。

這些宣稱的安全目標接著會先由認證獨立測試實驗室評估，才能在共同準則資料庫中列為認證產品。測試實驗室評估的要求與完整性，會透過指定的EAL (評估保證等級)傳達，涵蓋從測試過功能性的EAL 1，到正式驗證過設計並測試的EAL 7。這表示共同準則可以涵蓋作業系統和防火牆，到TPM與通行護照。

有關共同準則認證要求的更多詳細資訊，可查閱共同準則網站*www.commoncriteriaportal.org/*

3.2.2 FIPS 140

FIPS (聯邦資訊處理標準) 140-2和140-3，是密碼學運算模組的資訊安全標準，由美國NIST (國家標準與技術研究院)發佈。FIPS 140-3在2019年取代FIPS 140-2作為其更新版本。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學皆正確實作。簡而言之，認證需要密碼學運算模組、核准演算法、核准操作模式、和開機測試的描述、規格與驗證。

有關FIPS 140-2和FIPS 140-3認證要求的更多詳細資訊，可查詢NIST網站*www.nist.gov*。

3.3 私密金鑰的保護

對於不法份子而言，擷取私密金鑰將可讓他們竊聽HTTPS加密網路流量，或者偽裝成實際設備並進入受到802.1X保護的網路。

安迅士設備支援多種基於TLS (傳輸層安全)的協定，以達成安全的通訊。這些仰賴X.509密碼學資訊保護，例如安迅士設備ID (IEEE 802.1AR)、HTTPS (網路加密)、802.1X (網路存取管控)和其他。

TLS的X.509數位憑證，使用憑證和相應的公開與私密金鑰對，讓網路上的兩台主機可進行通訊。私密金鑰儲存在安全金鑰儲存區內，且絕對不會暴露在外，即使用於解密資料時也一樣。實際的憑證和公開金鑰已知，可由安迅士設備分享並用於加密資料。

3.4 門禁管制金鑰的保護

安迅士門禁管制解決方案中使用的密碼學資訊保護，例如開放監督設備協定(OSDP)安全頻道，是硬體保護金鑰儲存區很重要的另一個範例。

OSDP安全頻道是廣泛使用的AES-128加密和身分驗證方式，可保護門禁控制器和讀卡機等周邊設備之間的通訊。

門禁控制器和讀卡機共用的AES對稱金鑰，安全頻道基礎金鑰(SCBK)，會用於發起相互身分驗證，並在之後產生一組工作階段金鑰，加密門禁控制器和讀卡機之間的通訊。

為了達到真正的端對端安全性，主要金鑰(MK)和SCBK需要安全儲存在安迅士網路門禁控制器的安全金鑰儲存區內。主要金鑰會用於為每個連線的安迅士讀卡機產生獨特的SCBK金鑰。還有，在安迅士讀卡機安裝階段中安全分發的個別SCBK，需要安全儲存在讀卡機的安全金鑰儲存區內。讀卡機更關鍵，因為通常會安裝在門戶的不安全側。

透過這個方式，兩端都可在硬體保護環境中，保護OSDP安全頻道金鑰。這可在出現安全侵駭事件時，防止惡意提取。

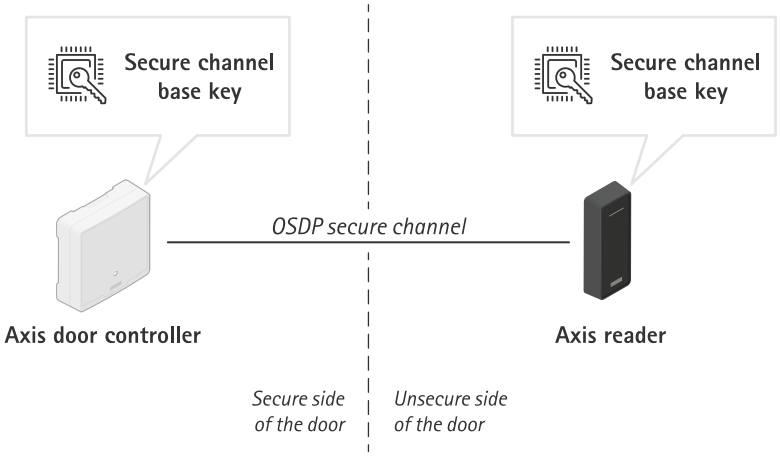


Figure 8. 在門禁管制中，以安全金鑰儲存區達成端對端安全。主要金鑰和個別安全頻道基礎金鑰(SCBK)，都儲存在門戶每一側設備中的安全金鑰儲存區內。

3.5 檔案系統金鑰的保護

操作中的安迅士設備帶有客戶專屬的設定和資訊。從提供預先設定服務的代理商或系統整合業者，將安迅士設備送交客戶時也同樣帶有這些設定。能夠實體接觸到安迅士設備時，惡意不法份子可透過解焊快閃記憶體並透過快閃記憶體讀取設備存取，嘗試從檔案系統提取資訊。因此，防止從可讀寫的檔案系統提取敏感資訊或設定竄改，是安迅士設備遭竊或遭受侵入時的一項重要保護措施。

安全金鑰儲存區可透過針對檔案系統實行強固加密，防止惡意外滲資訊並預防設定竄改。安迅士設備關閉電源時，檔案系統上的資訊會加密。在開機期間，可讀寫檔案系統會以AES-XTS-Plain64 256位元金鑰解密，以便掛載檔案系統並由安迅士設備使用。檔案系統加密金鑰是在出廠預設設定時為每個設備獨特產生，並會在後續每次韌體更新時重新產生，表示在整個設備生命週期中，金鑰不會維持不變。

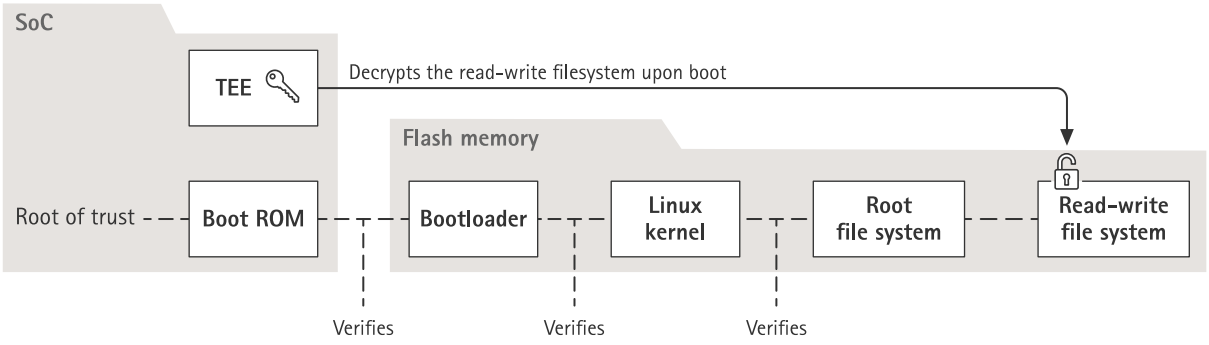


Figure 9. SoC內的TEE保存用於解密根目錄檔案系統的金鑰。

4 影像竄改保護

安全監控產業的基本前提是，監控攝影機錄製的影像真實並且可信任。研發已簽署的影像功能是為了維持並近一步強化將影像作為證據之信心。透過驗證影像真實性，此功能可確保影像離開攝影機後，並未遭受編輯或竄改。

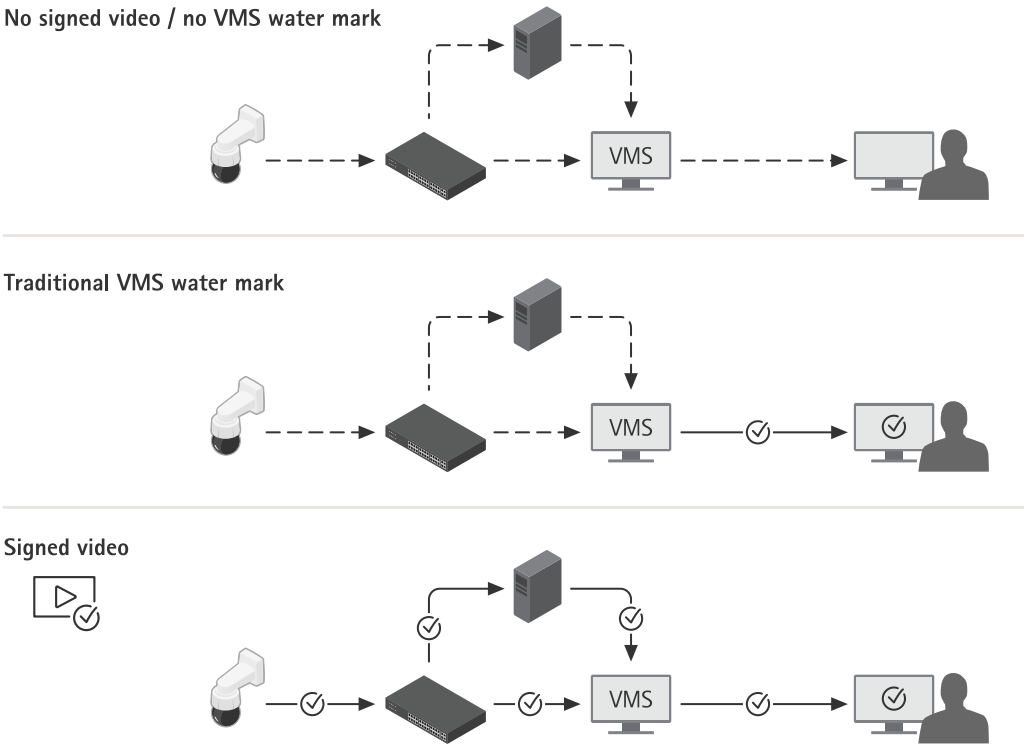


Figure 10. 驗證影像真實性。

上方：影像從攝影機到檢視錄影的人員過程中，會通過許多步驟。技能高超的攻擊者，可在上述任何轉換過程中竄改影像。

中間：匯出時添加到影像上的VMS浮水印可以驗證某些步驟，但無法保證影像並未在先前階段中遭受竄改。

下方：已簽署的影像可保證從攝影機到檢視匯出錄影人員的任何步驟中，影像均未遭受竄改。影像可回溯到錄製影像的設備。

4.1 已簽署的影像

藉由安迅士研發且主動開源之已簽署的影像功能，影像串流中的簽章可用於確保影像完整，並藉由回溯產生影像的攝影機以驗證影像來源。如此可證明影像真實性，而不需要證明影像檔案的監督鏈。

安全監控攝影機系統錄製事件後，警方可能收到USB隨身碟上的匯出影像檔案，並儲存到EMS (證據管理系統)內。從攝影機匯出影像時，警官可看到影像已正確簽署。如果之後在起訴流程中使用該影像，法庭可監控並確認影像在什麼時間錄製、由哪台攝影機錄製，以及

是否曾經改變或移除任何影格。藉由使用安迅士提供的檔案播放器，取得影像副本的任何人都可以看到這些資訊。

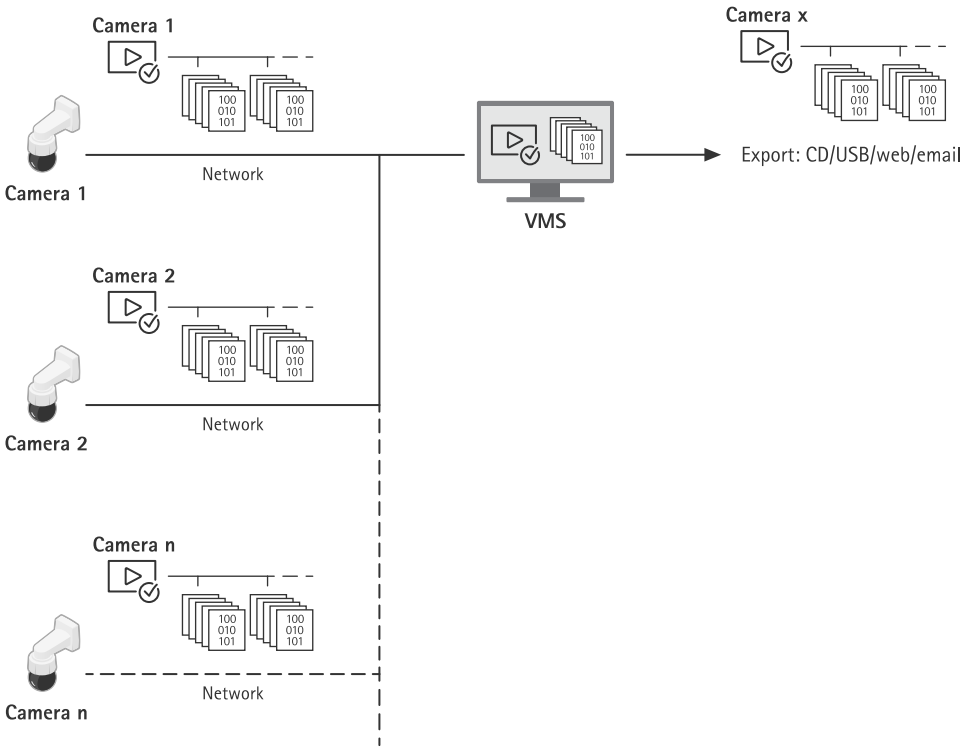


Figure 11. 簽章已經加入攝影機內，因此在從來源到最終使用影像的每個步驟中，都能夠驗證內容。

每台攝影機使用本身獨特的影像簽署金鑰，金鑰儲存在安全的金鑰儲存區內，可將簽章加入影像串流中。這是透過計算每個影格的雜湊，包括元資料，並簽署合併的雜湊而達成。簽章接著會儲存在串流中專屬的元資料欄位內(SEI標頭)。

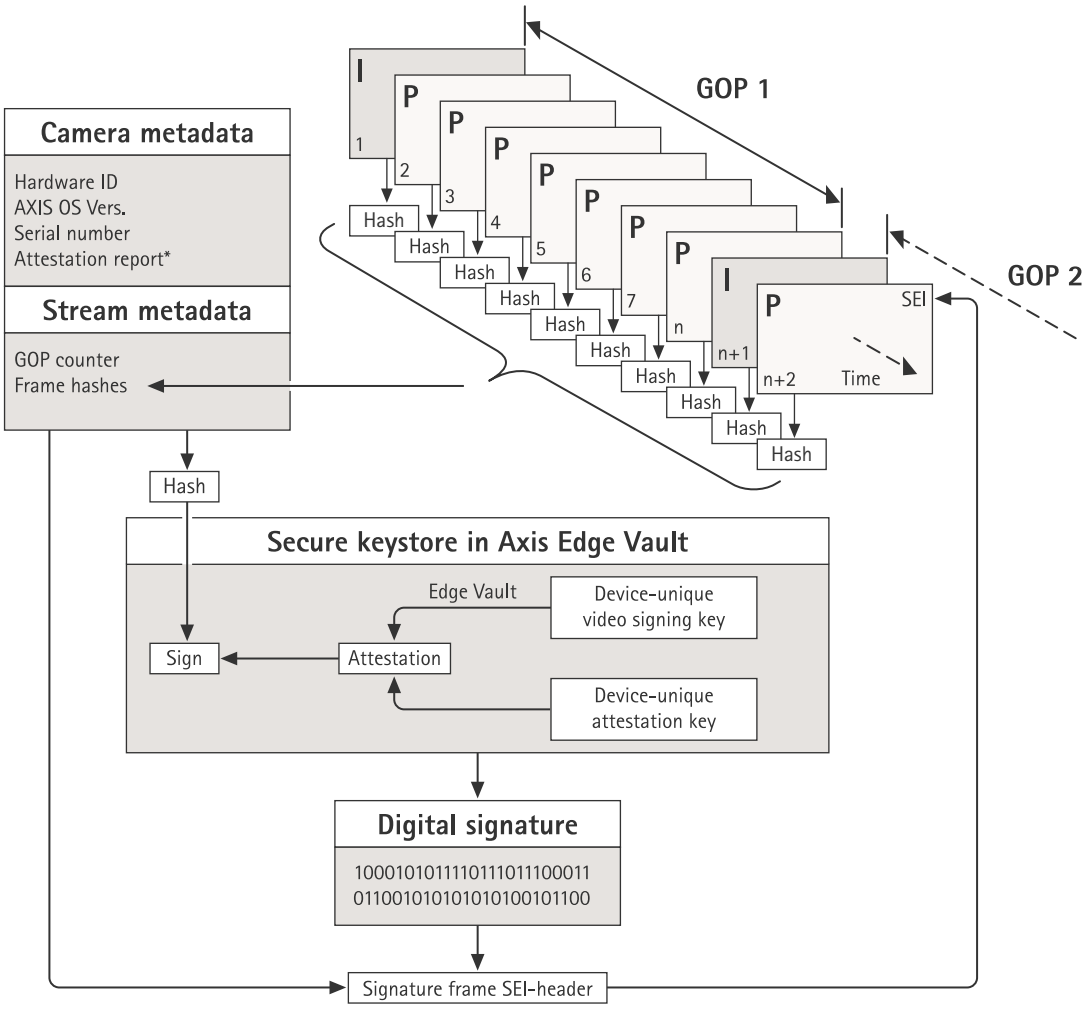


Figure 12. 如何將簽章加入影像元資料的示意圖。圖片群組(GOP)的每個影格內容，會與攝影機元資料和串流元資料的雜湊混雜在一起。這會形成GOP雜湊，並在Edge Vault內簽署。簽章和元資料接著會加入之後隨串流一起傳送的SEI標頭。

** 證明報告可用來確認用於簽署的金鑰對之來源和出處。透過驗證金鑰證明，可確保金鑰安全儲存在特定設備硬體中。此做法可確保影像的來源。*

實際的簽署是透過設備特有的影像簽署金鑰進行的，這個金鑰可以使用設備特有的證明金鑰證明。證明報告會在串流開頭和固定間隔附上，通常每小時一次。由於元資料包含每個個別影格雜湊，可以偵測個別影格是否正確。為了讓簽署完整，必須保護影像的圖片群組(GOP)。這是透過在簽章中納入下一個GOP之第一個I-frame的雜湊而達成。這可防止無法偵測出來的影格剪接或重新排序。串流期間遺失影格或儲存期間內容損壞的極低機率事件，也會以相同方式標記出來。

5 供應鏈防護

Axis Edge Vault (憑證伺服器)要求可作為信任根源的安全基礎。建立信任根源，從設備的開機程序開始。在安迅士設備中，硬體機制*安全開機*驗證設備用於開機的作業系統(AXIS OS)。而AXIS OS會在組建過程中以密碼學簽署(*已簽署的韌體*)。

安全開機和已簽署的韌體彼此緊密結合。可確保設備佈建之前，韌體並未受到(可實體接觸到設備的任何人)竄改，且佈建後設備無法安裝不安全的韌體更新。安全開機和已簽署的韌體之組合，可建立堅固的密碼學驗證軟體鏈建構之信任鏈，這是所有安全操作的基礎。

5.1 安全開機

安全開機是一種開機機制，包含從不可變記憶體(開機ROM)開始，堅固的密碼學驗證軟體鏈。安全開機確保設備只能以授權韌體開機。

開機程序從開機ROM驗證開機啟動程式(bootloader)開始。安全開機接著會即時驗證，從快閃記憶體載入之韌體每個區塊的內嵌簽章。開機ROM可作為信任根源，僅在驗證過每個簽章後才會繼續進行開機程序。鏈的每個部分會驗證下一個部分，最終得到驗證過的Linux核心和驗證過的檔案系統根目錄。

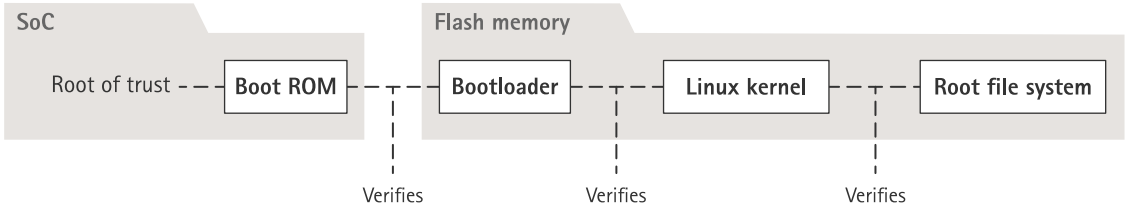


Figure 13. 在安全開機過程中，鏈的每個部分會驗證下一個部分。最終會得到驗證過的檔案系統根目錄。

在許多設備中，不允許改變低階功能非常重要。由於其他安全性機制以低階軟體建置，安全開機可作為安全基礎層，防止規避這些機制。如果設備具有安全開機功能，安裝於快閃記憶體的韌體會受到保護，無法修改。出廠預設設定映像檔會受到保護，同時設定不受保護。即使在回復出廠預設設定後，安全開機也可保證設備的正確狀態。不過若要讓安全開機正確運作，必須確保開機驗證韌體由安迅士簽署。

5.2 已簽署的韌體

安迅士已簽署的韌體涉及由安迅士以祕密保存的私密金鑰簽署韌體映像檔。韌體附加此簽章時，設備將先驗證韌體再接受韌體安裝。如果設備偵測到韌體完整性不足，將拒絕韌體升級。

簽署韌體的程序是透過計算密碼學雜湊值開始。在簽章附加到韌體映像檔之前，會以私密/公開金鑰對簽署這個數值。

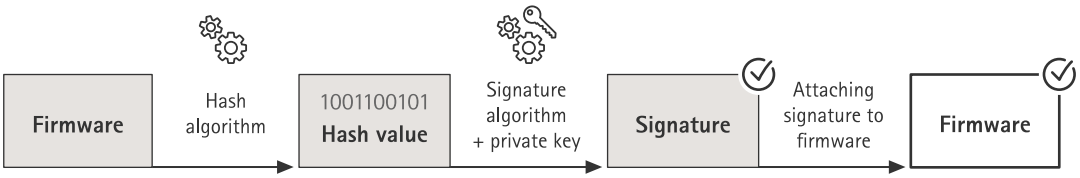


Figure 14. 簽署韌體的程序。

韌體升級前，必須先驗證新韌體的真實性。為確保這一點，公開金鑰(隨附在安迅士產品內)會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，然後將此值與簽章中經過驗證的雜湊值比較，驗證韌體的完整性。如果韌體簽章無效或韌體映像檔曾遭受竄改，安迅士設備的開機程序將中止。

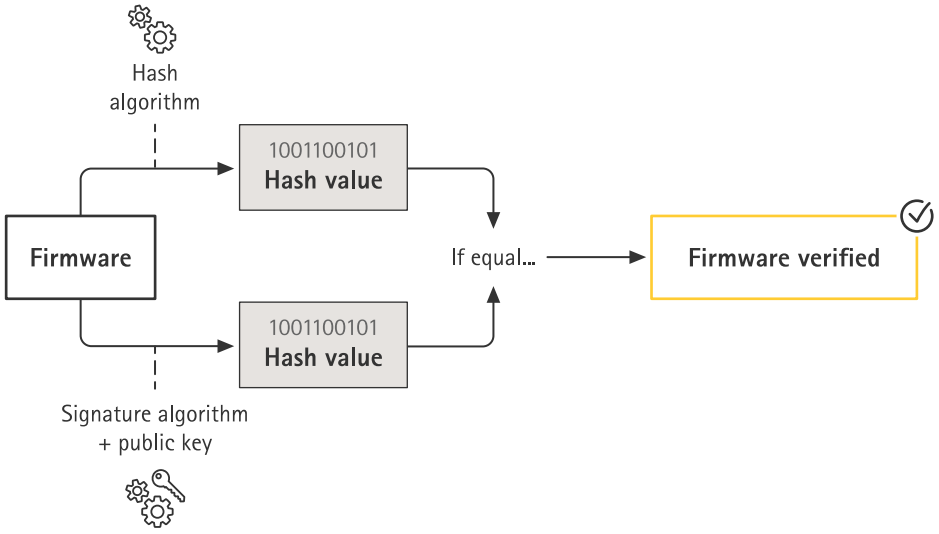


Figure 15. 驗證已簽署的韌體之程序。

安迅士已簽署的韌體是以業界公認的RSA公開金鑰加密方法為基礎。私密金鑰儲存在安迅士嚴密防護的地點，而公開金鑰內嵌於安迅士設備內。整個韌體映像檔的完整性，是以映像檔內容的簽章保證。主要簽章驗證數個次要簽章，並在映像檔解壓縮時驗證。

針對測試和自訂韌體組建，安迅士實行一個機制，核准個別設備接受非生產韌體。此韌體透過不同的方式簽署，並經過擁有者和安迅士核准，因此會產生自訂韌體憑證。安裝在核准的設備中時，憑證允許使用基於獨特序號和晶片ID，僅能在核准設備上運行的自訂韌體。自訂韌體憑證只能由安迅士建立，因為安迅士持有簽署這些韌體的金鑰。

6 字彙表

安迅士設備ID：設備特有的憑證，包含相應金鑰，可證明安迅士設備的真實性。安迅士設備會由原廠佈建儲存在安全金鑰儲存區內的安迅士設備ID。安迅士設備ID是基於國際標準IEEE 802.1AR (IDevID，初始設備識別碼)，其定義一個自動化安全識別方法。

Axis Edge Vault (憑證伺服器)：防護安迅士設備的硬體網路安全平台。其建立在強大的密碼學運算模組(安全元件和TPM)與SoC安全(TEE和安全開機)基礎上，並結合邊際設備安全的專業知識。

憑證：已簽署的文件，可證明公開/私密金鑰對的來源和屬性。憑證是由憑證授權中心(CA)簽署，若系統信任CA，也將信任其核發的憑證。

憑證授權中心(CA)：憑證鏈的信任根源。用於證明基礎憑證的真確性和真實性。

共同準則(CC)：IT產品安全認證的國際標準。也稱為資訊技術安全評估共同準則，ISO/IEC 15408。

FIPS 140：一系列的美國電腦安全標準，用於核准密碼學運算模組。FIPS (聯邦資訊處理標準) 140定義如何設計和實作密碼學模組，以減輕模組竄改風險的要求。

不可變ROM (唯讀記憶體)：安全儲存可信任公開金鑰和用於比較簽章之程式的唯讀記憶體，令其無法被覆寫。

佈建：為網路準備和配備設備的程序。此工作涉及從中心點提供組態資料和原則設定至設備。設備隨附金鑰和憑證。

公開金鑰密碼學：非對稱式密碼學系統，其中任何人都可使用接收者的*公開金鑰*加密訊息，但唯有接收者能夠使用*私密金鑰*將訊息解密。可以用於加密和簽署訊息。

安全開機：防止設備開機期間載入未授權軟體的一項功能。安全開機使用已簽署的韌體，確保僅使用授權安迅士軟體為設備開機。

安全元件：一個密碼學運算模組，以硬體防竄改方式儲存私密金鑰，並安全執行密碼學操作。和TPM不同，安全元件的硬體和軟體介面並未標準化，且為製造商專用。

安全金鑰儲存區：一個防竄改環境，可保護私密金鑰並安全執行密碼學操作。可在出現安全侵駭事件時，防止未授權存取和惡意提取。取決於安全要求，安迅士設備可以具有一個或多重硬體密碼學運算模組，其提供硬體防護安全金鑰儲存區。

已簽署的韌體：已由信任方數位簽署的韌體。安迅士設備進行韌體更新之前，會驗證韌體映像檔的真實性。已簽署的是安全開機程序中的一項要求。

已簽署的影像：維持並強化將影像作為證據之信心的一項功能。已簽署的影像提供影像竄改偵測與真實性，並且用於確保影像完整並可回溯到特定安迅士攝影機。已簽署的影像之簽署金鑰位於安迅士設備的安全金鑰儲存區內。

傳輸層安全(TLS)：用於保護網路流量的一項網際網路標準。TLS提供HTTPS內的S (代表安全)。

信任執行環境(TEE)：以硬體防竄改方式儲存私密金鑰，並安全執行密碼學操作。TEE和安全元件及TPM不同，是晶片系統(SoC)主要處理器的一個安全、硬體隔離區。

信任平台模組(TPM)：一個密碼學運算模組，以硬體防竄改方式儲存私密金鑰，並安全執行密碼學操作。TPM是*信任運算小組(TCG)*定義的國際標準化(TPM 1.2、TPM 2.0)電腦組件。

零信任安全：IT安全的一個現代做法，其中連線設備和IT基礎架構(例如網路、電腦、伺服器、雲端服務和應用程式)需要彼此重複識別、驗證和身分驗證，以達到高度安全管控。

關於 Axis Communications

Axis 透過建立解決方案讓世界更聰明和更安全，以提高安全性和業務績效。 做為網路技術 公司和產業領導者，Axis 提供影像監控、門禁管制、對講機和音訊系統的解決方案。 它們透過 智慧分析應用程式獲得強化，並得到高品質訓練的支援。

Axis 在全球 50 多個國家/地區雇用 4,000 多名專職員工，並與全球的技術和系統整合合作夥伴合作 交付客戶解決方案。 Axis 成立於 1984 年，總部 位於瑞典隆德