使用Expressway x15.5導航客戶端EKU日落

簡介

本文檔介紹使用Cisco Expressway x15.5導航客戶端EKU日落。

背景資訊

數位證書是由受信任的證書頒發機構(CA)頒發的電子憑證，通過確保身份驗證、資料完整性和機密性來保護伺服器和客戶端之間的通訊。這些證書包含定義其用途的擴展金鑰用法(EKU)欄位：

- 伺服器身份驗證EKU(id-kp-serverAuth)在伺服器出示證書以證明身份時使用。
- 客戶端身份驗證EKU(id-kp-clientAuth)在雙方TLS(mTLS)連線中使用，在該連線中雙方相互進行身份驗證。

傳統上，單個證書可以同時包含伺服器和客戶端身份驗證EKU，使其可用於雙重用途。這對於在不同連線場景中同時充當伺服器和客戶端的Cisco Expressway等產品尤為重要。

問題定義

Chrome根程式策略更改

自2026年6月起，Chrome根程式策略限制包含在Chrome根儲存中的根證書頒發機構(CA)證書，逐步停用多用途根來調整所有公共金鑰基礎結構(PKI)層次結構，以便僅使用TLS伺服器身份驗證使用案例。

主要政策要求

- 公共根CA必須宣告僅用於伺服器身份驗證(id-kp-serverAuth)的擴展金鑰使用(EKU)。
- 禁止在這些證書中包括客戶端身份驗證EKU。
- 沒有更多公共伺服器TLS證書的混合使用的根CA。
- 實施時間表：2026年6月

公共CA響應時間表

- 2025年10月：許多公共CA(DigiCert、Sectigo、SSL)預設開始頒發僅伺服器證書。
- 2026年5月：公共CA伺服器停止頒發客戶端身份驗證EKU證書
- 2026年6月：Chrome根計劃策略完全生效

附註：此策略僅適用於公共CA頒發的證書。私有PKI和自簽名證書不受此策略的影響。

如果您有興趣閱讀有關客戶端EKU設定對Expressway的影響，請參閱[在公共CA證書中準備Expressway客戶端身份驗證EKU失效。]

Expressway版本x15.5，帶解決方案

Expressway x15.5

Expressway x15.5提供了針對由於所有公共證書頒發機構對客戶端EKU的設定而引起的問題而提出的解決方案。這是一個全球性問題，影響選擇使用公共PKI證書的所有供應商/部署。

x15.4之前的版本中有一個CLI命令開關，允許管理員在Expressway E上上傳僅伺服器EKU證書（無客戶端EKU）。

xConfiguration XCP TLS證書CVS EnableServerEkuUpload:於

附註：此命令在x15.5上已棄用。

X15.5證書儲存新增

x15.5有兩個證書儲存區：

1.伺服器證書儲存

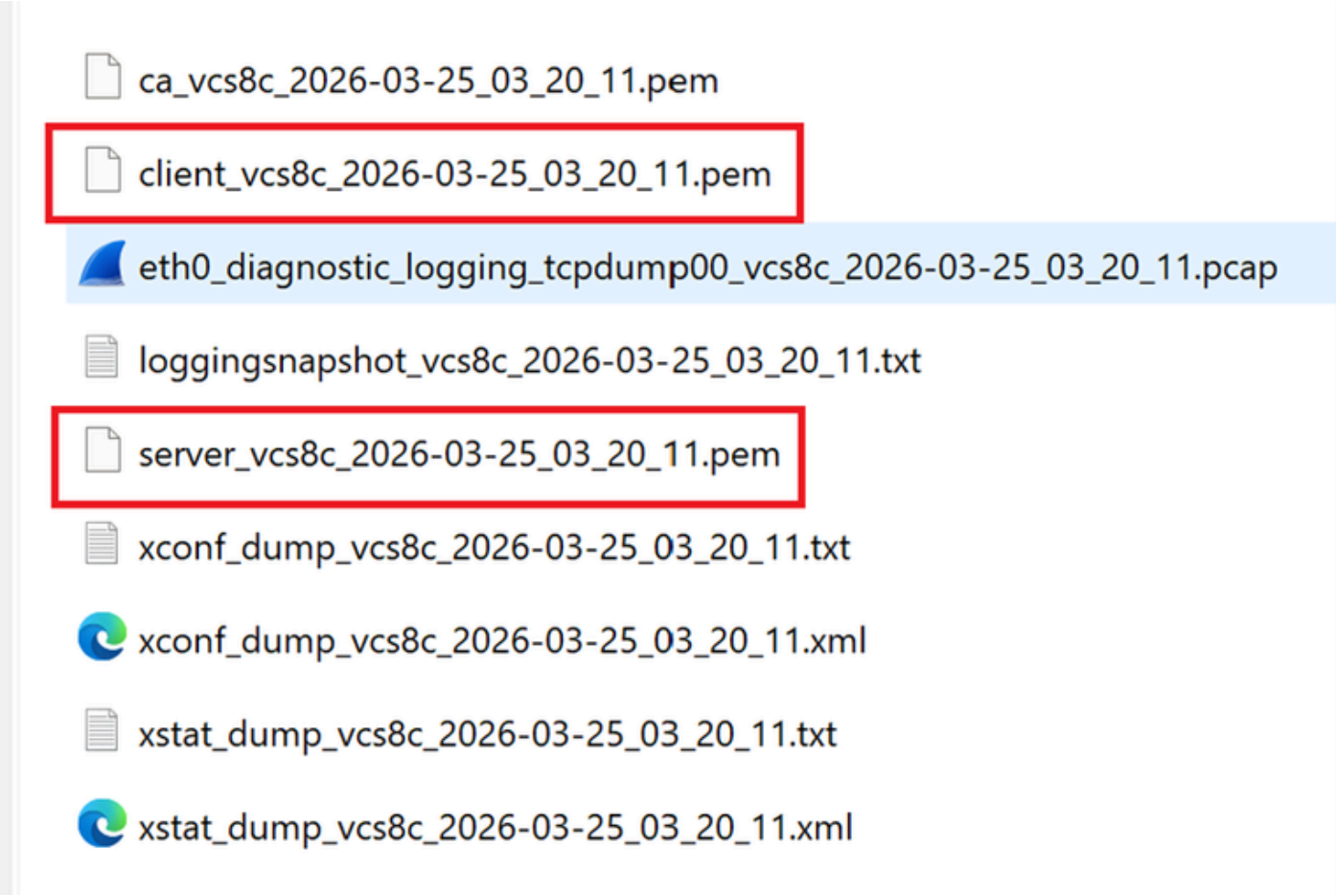
2.客戶端證書儲存

高速公路（單網絡卡或雙網絡卡）：兩個Expressway介面均可根據需要使用2個證書儲存。

範例：

- 當expressway在TLS握手期間充當客戶端時，將顯示客戶端證書。
- 當expressway在TLS握手期間充當伺服器時，將顯示伺服器證書。

附註：兩個證書儲存（客戶端和伺服器）使用相同的受信任CA庫。確保已在信任儲存上正確上載簽署伺服器和客戶端證書的CA。 診斷日誌現在包含PEM檔案格式的伺服器證書和客戶端證書。



從X15.4或早期版本升級到X15.5

執行升級時，來自x15.4或早期版本的伺服器證書會複製到x15.5上的客戶端證書儲存中。x15.5上的客戶端和伺服器證書儲存具有相同的證書。

螢幕截圖示例

15.4上的Expressway伺服器，當前伺服器證書序列號46:df:76:aa:00:00:00:00:00:29

證書：

版本:3(0x2)

序列號：

46:df:76:aa:00:00:00:00:00:29

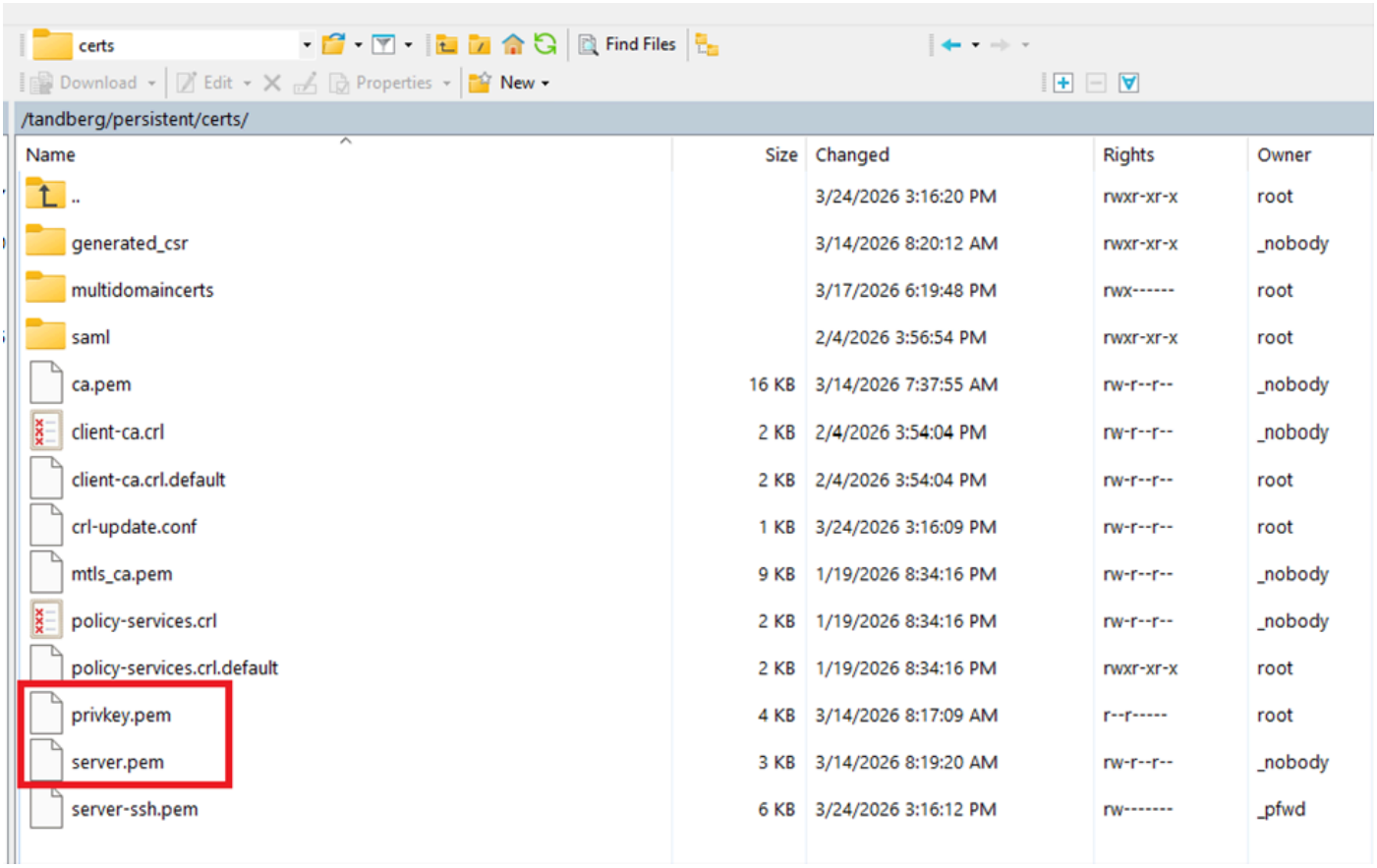
有效性

不早於：3月14日02:37:40 2026格林尼治標準時

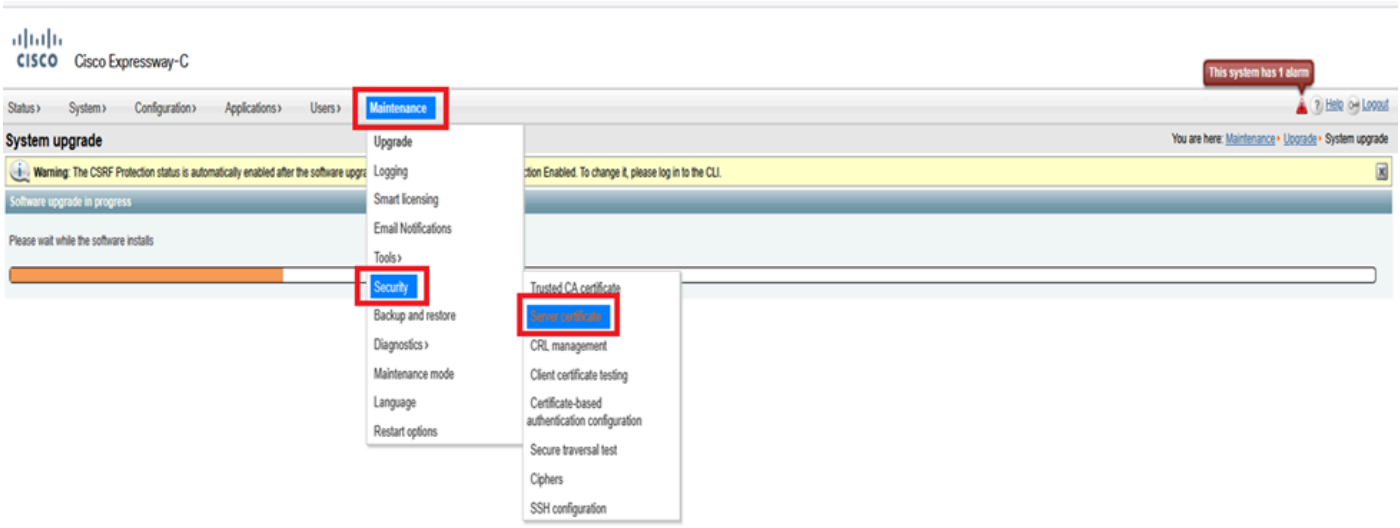
不晚於：3月14日02:47:40 2028格林尼治標準時

主題：C = IN、ST = KA、L = KA、O = Cisco、OU = TAc、CN = cluster.s.com

x15.4上的Expressway檔案系統永久/證書目錄：

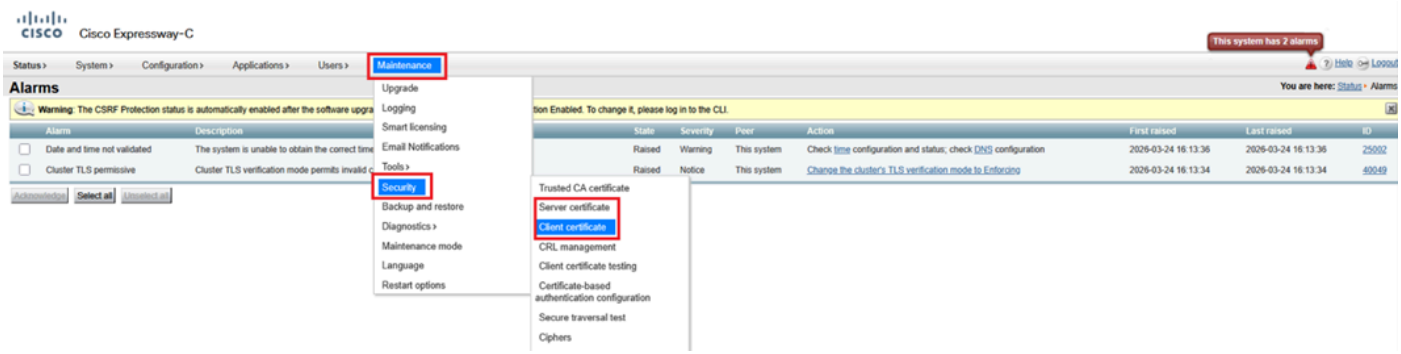


x15.4上的Expressway選單(「維護」>「安全」>「伺服器證書」)(僅存在伺服器證書欄位):



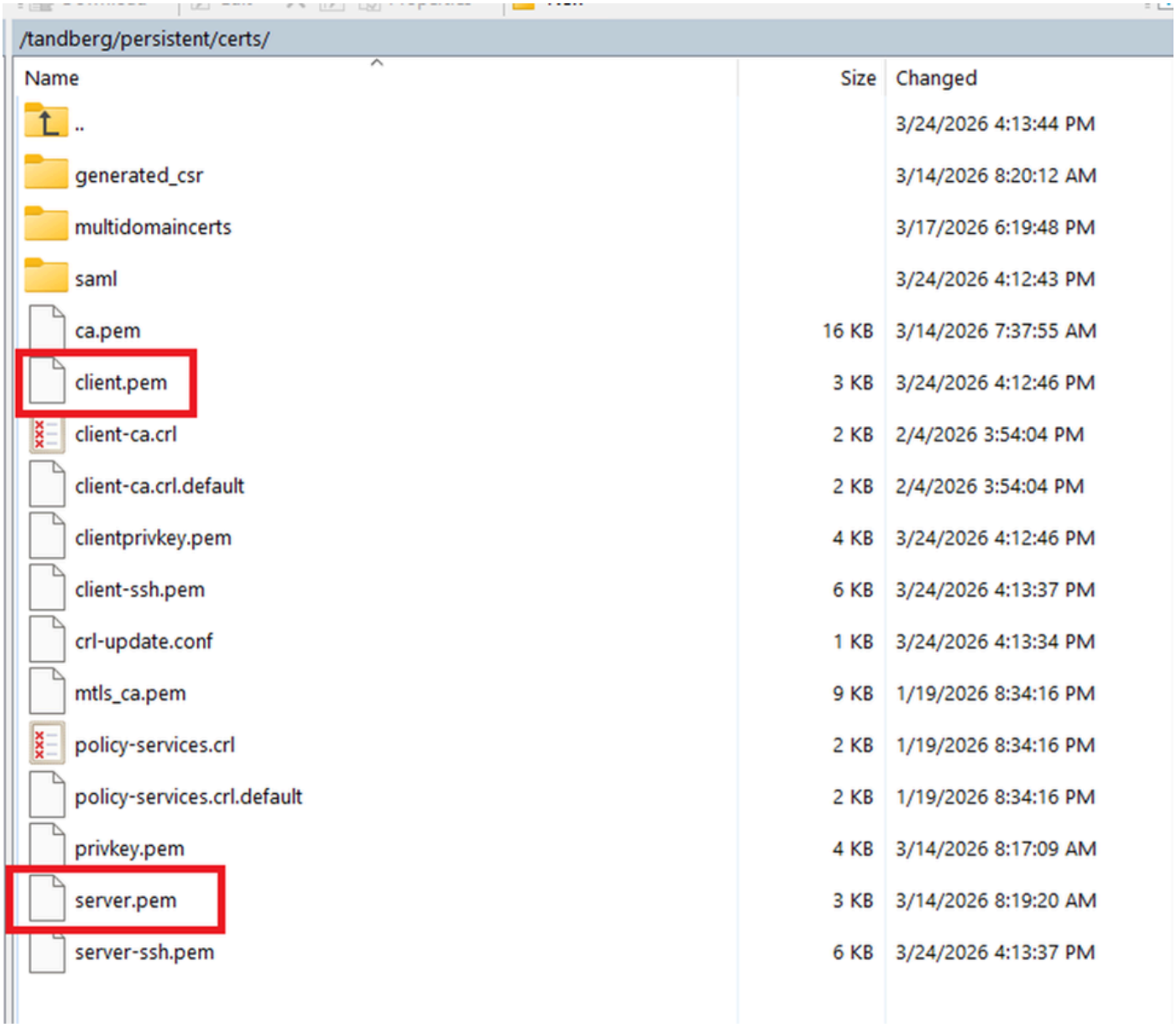
成功升級到x15.5後

在此,您會看到維護>安全>客戶端證書和伺服器證書下有2個證書選項。升級到x15.5後,Web admin上的伺服器和客戶端證書門戶顯示相同的證書,因為來自x15.4的伺服器證書已複製到x15.5上的客戶端證書儲存中。



升級到x15.5的現有證書和私鑰已被複製到客戶端證書儲存中。

x15.5上的Expressway檔案系統永續性/證書目錄:



在TLS握手期間進行X15.5 EKU檢查

在x15.5上，引入了新的CLI命令來檢查TLS握手期間的擴展金鑰使用(EKU)。預設值為「ON」。 命令集在Expressway核心和邊緣上有效。

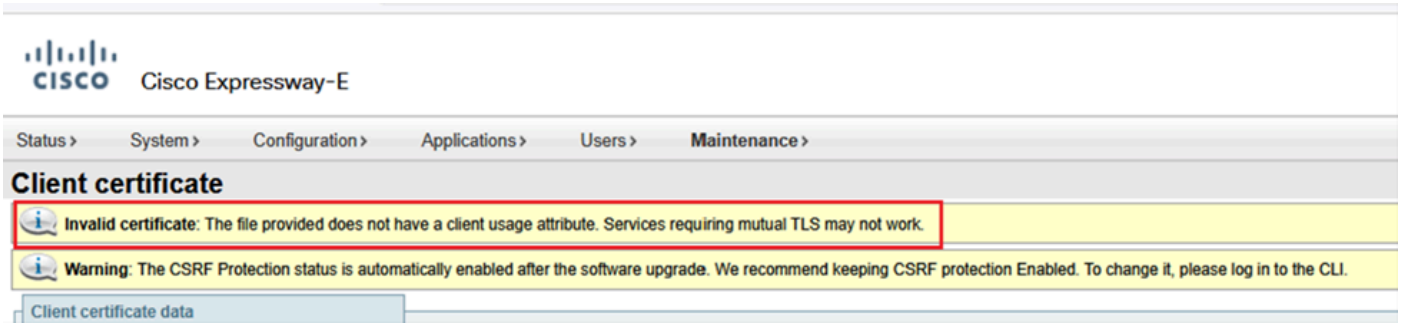
命令集觸發檢查所有到Expressway的入站SIP TLS連線。（入站客戶端hello/提供的證書）。 如果設定為「ON」，則檢查TLS發起方提供的證書在證書中是否包含客戶端EKU。如果關閉，則繞過檢查；但是，會檢查伺服器EKU是否存在於證書中。

xconfiguration SIP TLS Certificate ExtendedKeyUsage檢查模式：開/關：

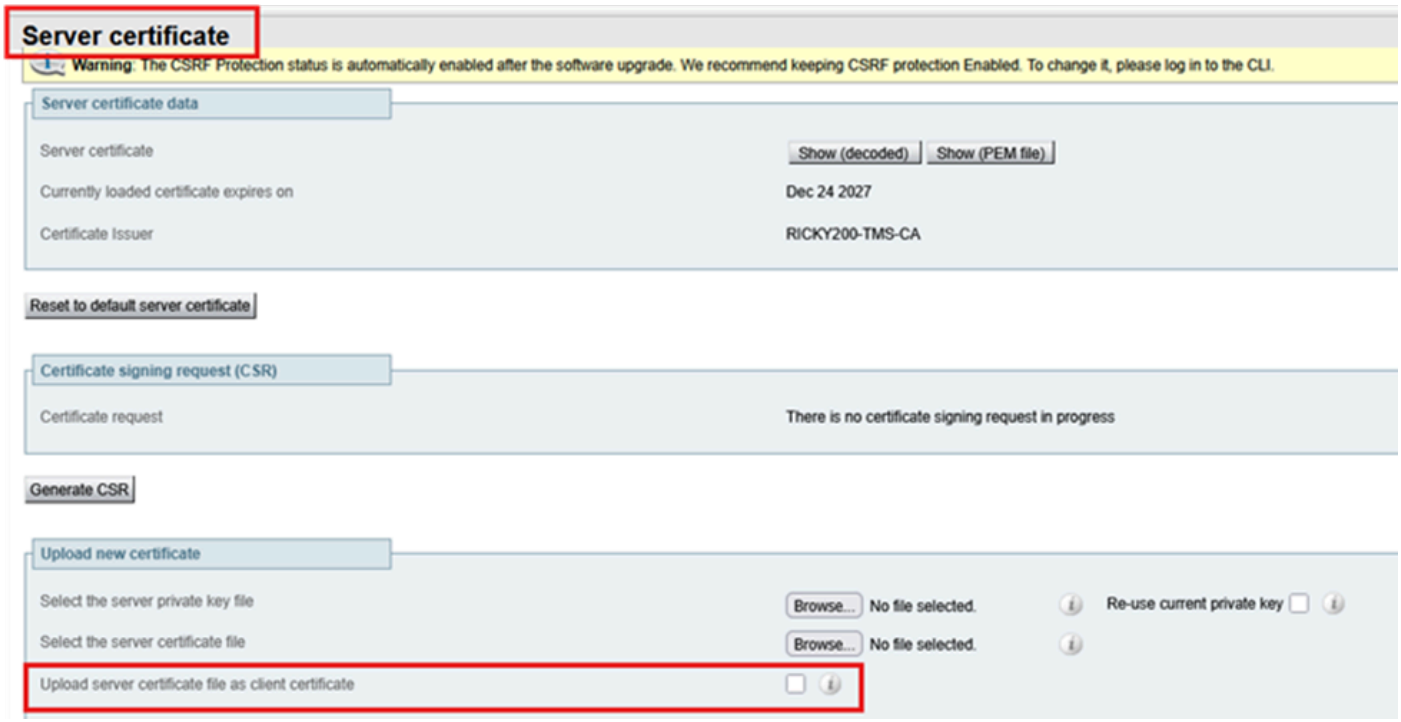
附註：如果生成客戶端證書，並對不包含客戶端EKU的CSR進行簽名（公共CA簽名證書的

示例），則無法在客戶端證書儲存上手動上載此證書。因此，您需要確保通過簽署CSR生成的證書始終包含客戶端EKU（可以使用專用CA插入客戶端EKU）。

提示：當您嘗試從客戶端證書儲存中上傳CSR簽名證書（缺少客戶端EKU）時，此錯誤變得明顯。



但是，如果選擇通過伺服器證書儲存上傳僅具有伺服器EKU（無客戶端EKU）的證書，並選擇上傳伺服器證書檔案作為客戶端證書，則證書將複製到客戶端證書儲存中。如果管理員不想在Expressway-Edge上使用私有CA簽名的證書，可以選擇僅將伺服器EKU從伺服器證書儲存複製到客戶端證書儲存。

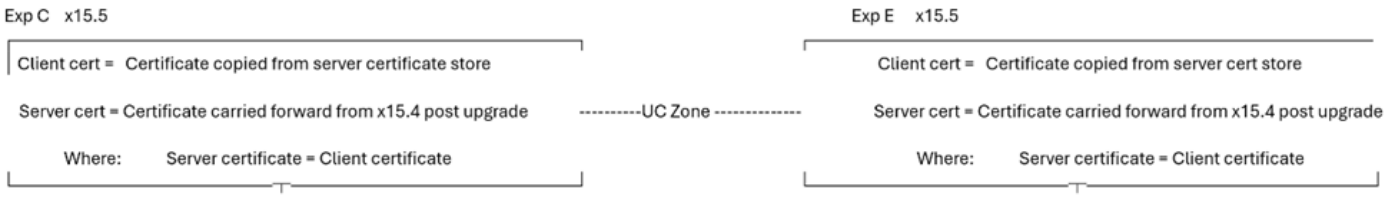


多個證書儲存，多個部署方案

由於現在在Expressway上有兩個證書儲存，因此存在多個證書儲存方案。

條件1:升級

當Expressway從x15.4或x15.5之前的版本升級時，此情況為真。x15.4版本的現有證書被複製到兩(2)個證書儲存中。在x15.5客戶端和伺服器上，證書是相同的。

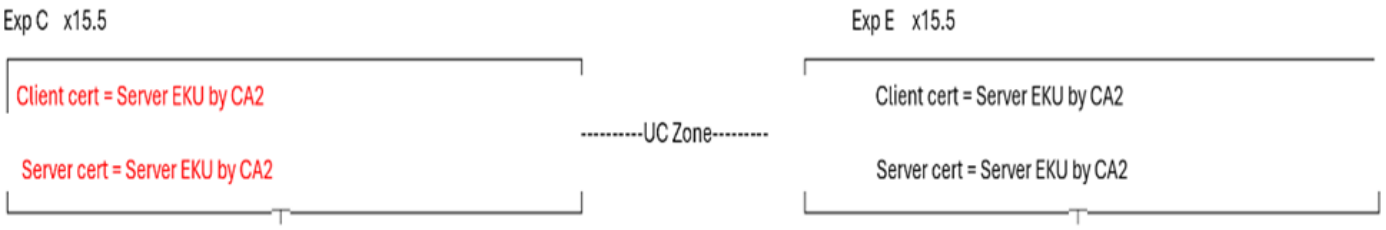


條件2:管理員在x15.5上安裝新證書時（現有證書已過期）

CA 1 =內部CA

CA 2 =公共CA

在下一圖中，Expressway核心具有僅由CA 2簽署的伺服器EKU的客戶端證書（公共CA）和僅由CA 2簽署的伺服器EKU的伺服器證書（公共CA）。 同樣，Expressway E具有包含由CA2簽名的伺服器EKU的客戶端證書（公共CA）和包含僅由CA 2簽名的伺服器EKU的伺服器證書（公共CA）。



如果Expressway核心伺服器證書沒有客戶端EKU、統一通訊遍歷區域、MRA，則WebRTC代理不起作用。確保Expressway核心伺服器證書具有客戶端EKU。 這是使用者選擇對來自公共CA的所有憑證進行簽名的常見使用案例。由於公共CA在證書中不包括客戶端EKU，因此統一通訊遍歷區域將變為活動狀態。

要啟用UC區域，快速修複方法是關閉Expressway E上的EKU檢查。這將顯示UC區域。但是，SSH隧道保持非活動狀態。從今天起，2222上的SSH隧道通訊需要驗證客戶端EKU。

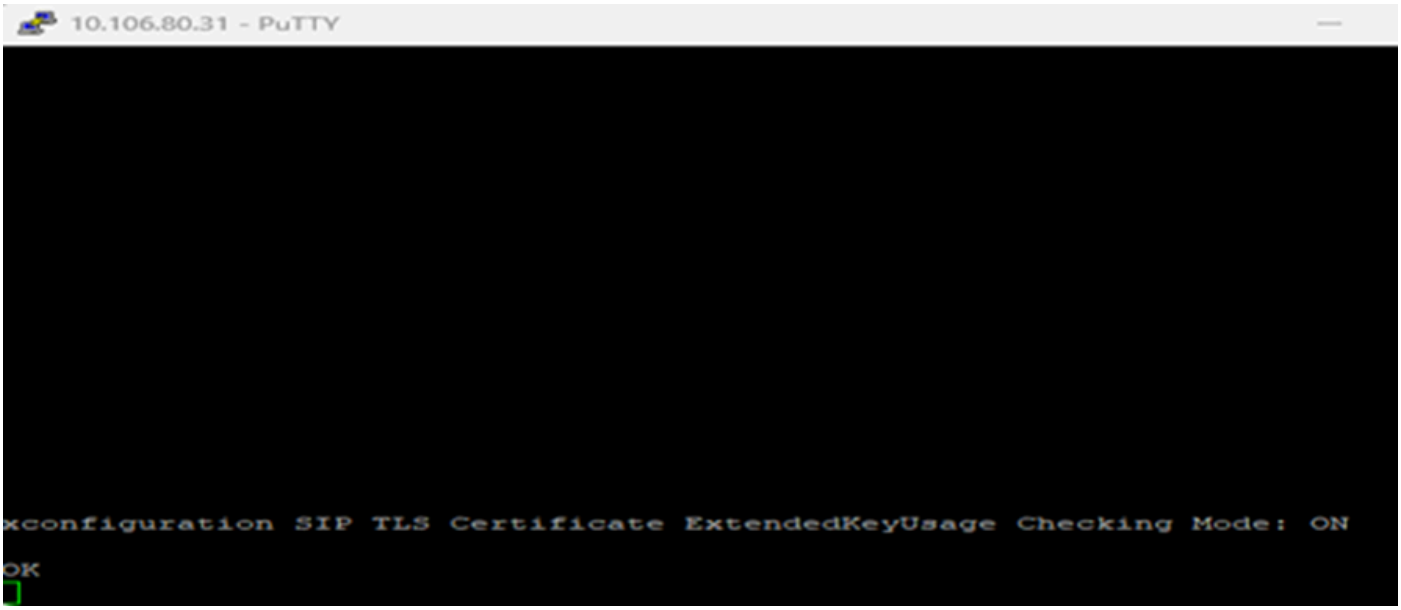
MRA客戶端登入和WebRTC代理功能無法正常工作。您可能不得不求助於私有CA。

測試用例1

- 當Expressway E上的EKU檢查為「ON」時
- 當Expressway核心上的客戶端和伺服器證書僅具有伺服器EKU時
- UC區域狀態失敗

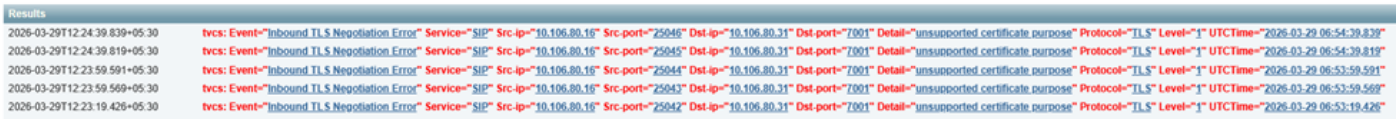
開啟Expressway-Edge ExtendedKeyUsage。

xconfiguration SIP TLS Certificate ExtendedKeyUsage檢查模式：於:



統一通訊區域故障：

Expressway E日誌顯示，其中10.106.80.16 = Expressway核心，10.106.80.31 = Expressway邊緣：

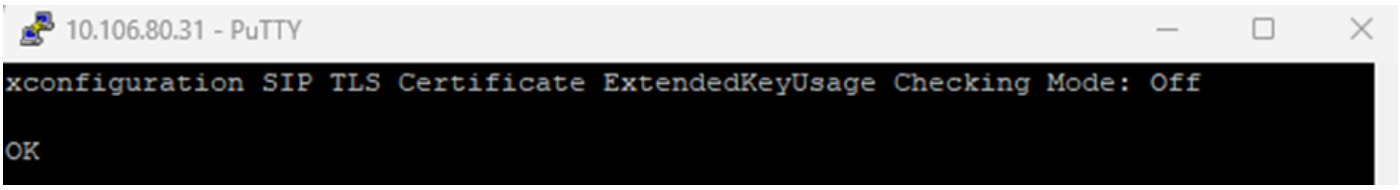


測試用例2

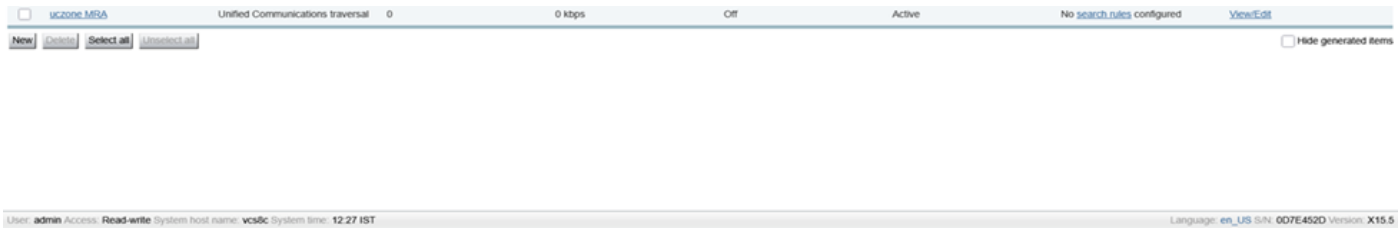
- Expressway E上的EKU檢查處於關閉狀態時
- 當Expressway核心上的客戶端和伺服器證書僅具有伺服器EKU時
- UC區域狀態為「活動」

關閉Expressway E上的EKU檢查。

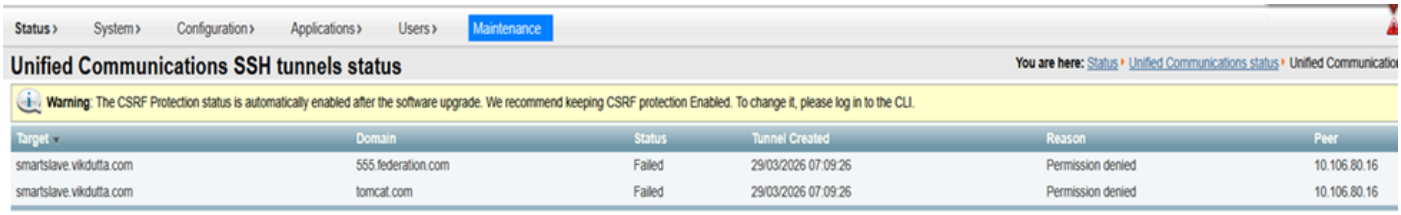
xconfiguration SIP TLS Certificate ExtendedKeyUsage檢查模式：Off



統一通訊區活動：



但是，ssh隧道仍然失敗：



Expressway事件日誌：

Results

2026-03-29T12:33:12.384+05:30 ssh: Detail="ssh: connect to host smartslavsrtsarts 22222port 2222: Connection timed out" Level="ERROR"

2026-03-29T12:31:56.811+05:30 ssh: Detail="ssh: connect to host smartslavsmartst 22222port 2222: Connection timed out" Level="ERROR"

2026-03-29T12:28:56.519+05:30 ssh: Detail="ssh: connect to host smartslavsmartst 22222port 2222: Connection timed out" Level="ERROR"

2026-03-29T12:28:24.476+05:30 ssh: Detail="ssh: connect to host smartslavsmartst 22222: port 2222: Connection timed out" Level="ERROR"

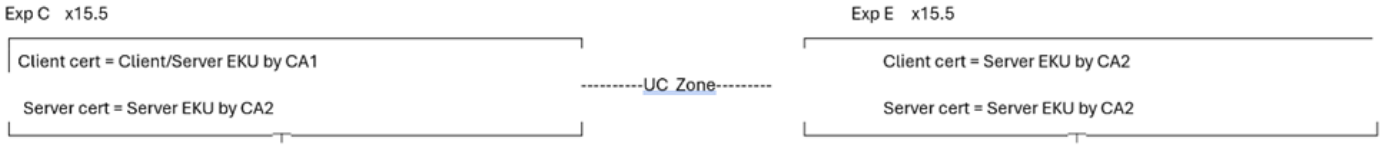
2026-03-29T12:27:52.445+05:30 ssh: Detail="ssh: connect to host smartslavslast smt 2222: port 2222: Connection timed out" Level="ERROR"

條件2.1:成功案例

CA 1 =內部CA

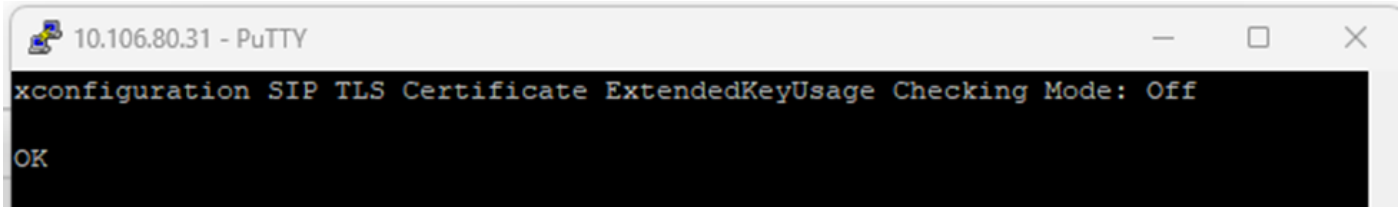
CA 2 =公共CA

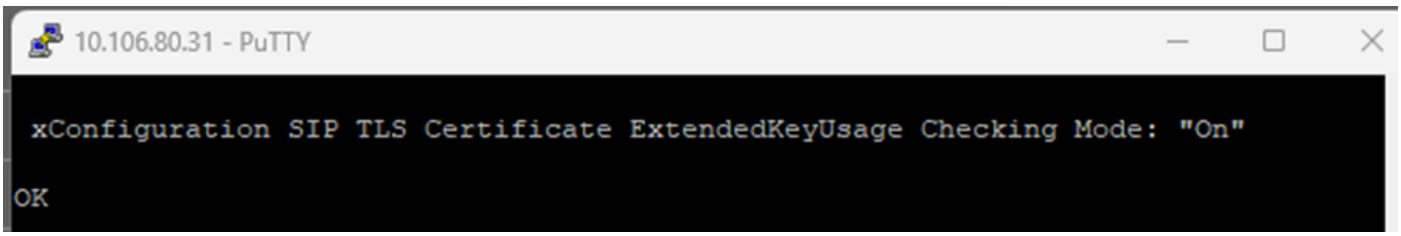
- 其中Expressway核心客戶端證書由CA 1（內部CA）簽名並包括，客戶端/伺服器EKU都包括。
- Expressway核心伺服器證書由CA 2公共CA簽署，僅包括伺服器EKU。
- Expressway邊緣伺服器證書由CA 2公共CA簽署，僅包括伺服器EKU。
- Expressway邊緣客戶端證書由CA 2公共CA簽署，僅包括伺服器EKU。



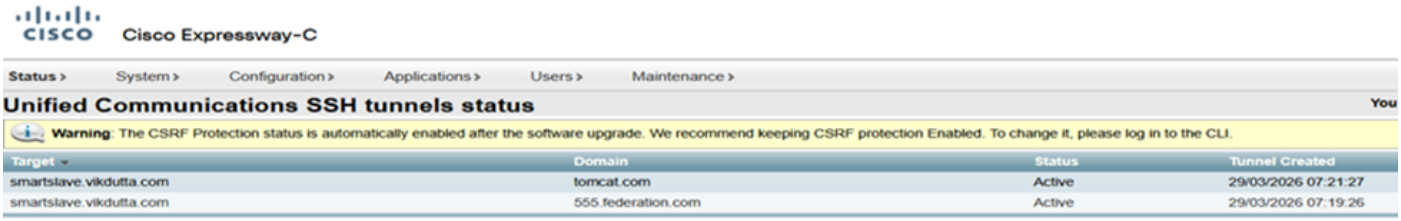
此條件是一個成功案例。 無論EKU檢查模式是否為ON/OFF，統一通訊區域和SSH隧道都變為活動狀態。MRA客戶端工作。

Expressway邊緣EKU檢查是關閉還是開啟並不重要。Expressway核心客戶端證書包含客戶端EKU:

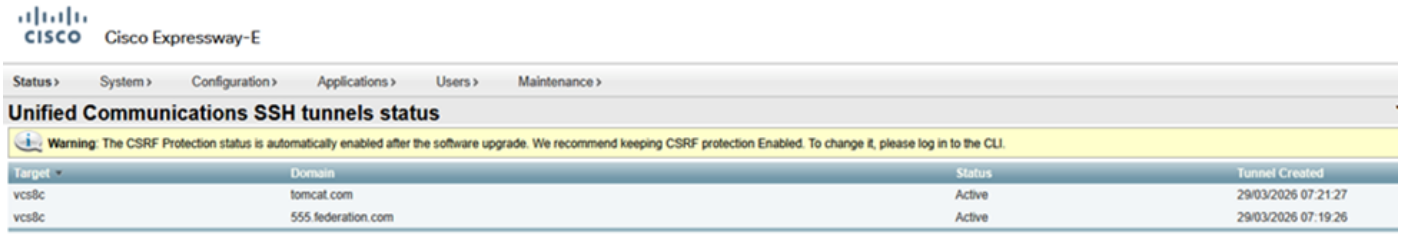




Expressway核心活動狀態上的SSH隧道：

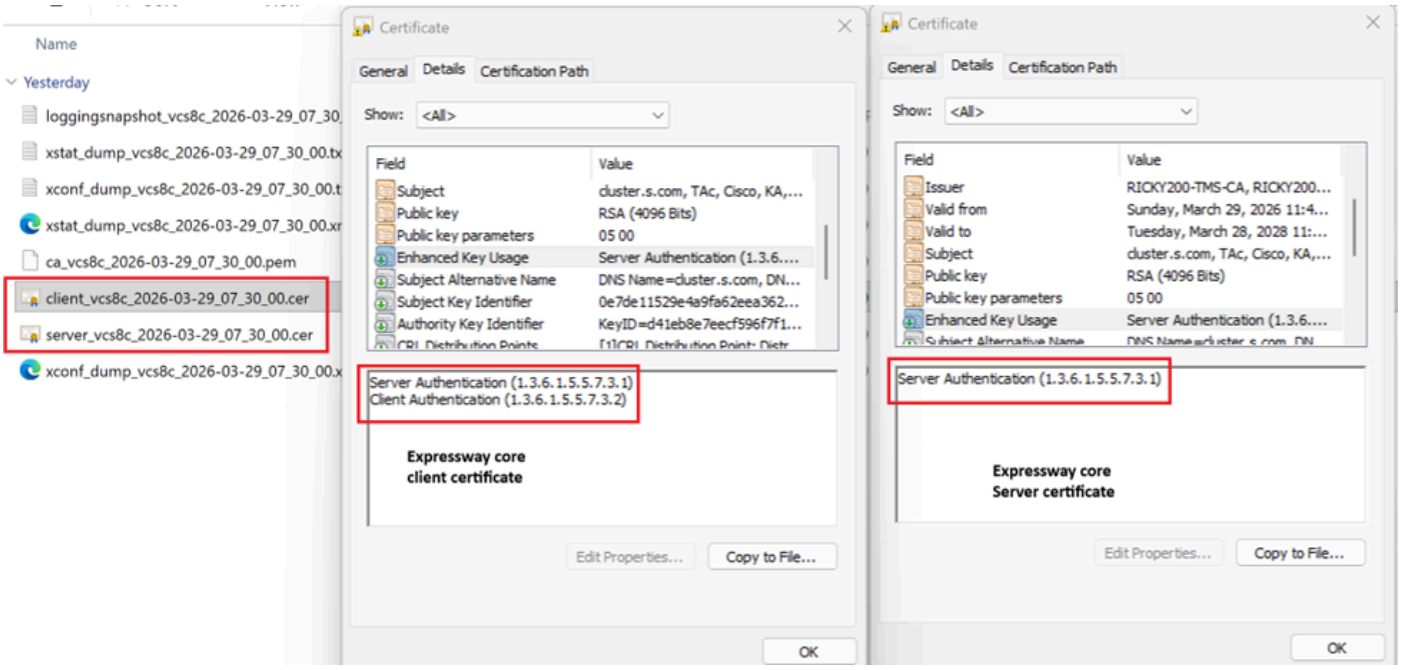


Expressway邊緣上處於活動狀態的SSH隧道：

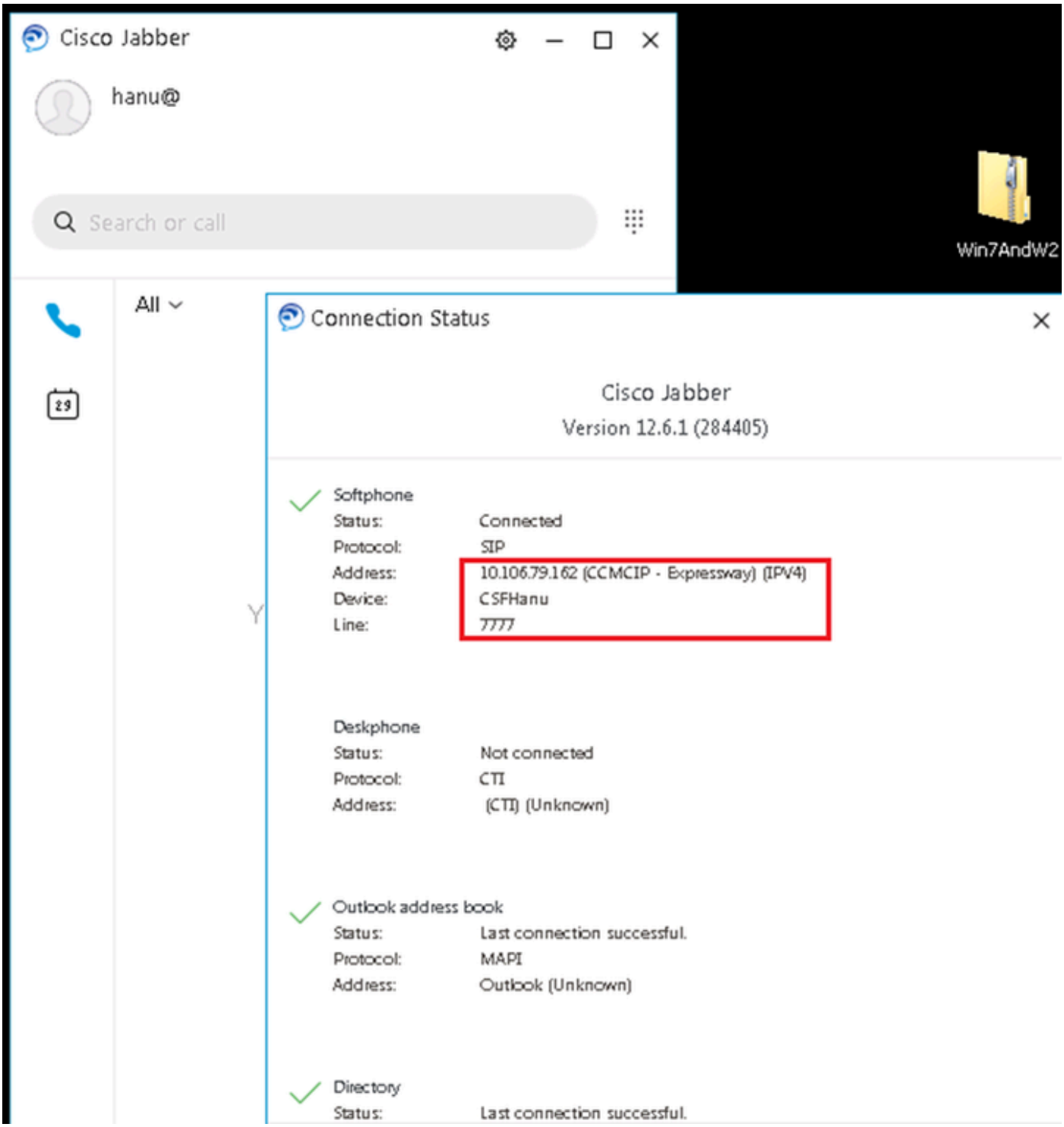


統一通訊MRA區域狀態處於活動狀態：

- Expressway-Core客戶端證書具有伺服器EKU和客戶端EKU。
- Expressway核心伺服器證書只有伺服器EKU。



MRA客戶端登入並註冊：

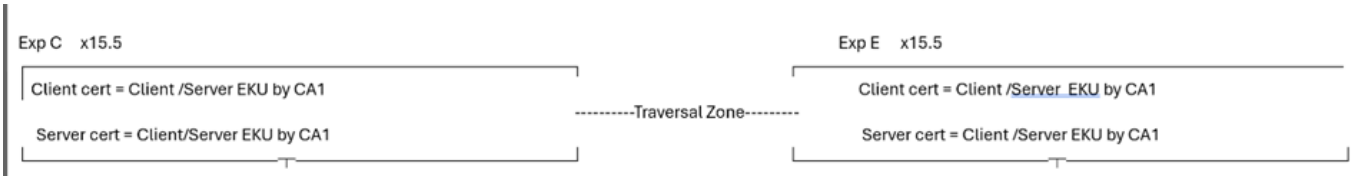


附註：比較並注意MRA和WebRTC代理在證書中存在的EKU。它是工作部署和非工作部署的比較。

條件3:使用私有CA簽署所有憑證

CA 1 =內部CA

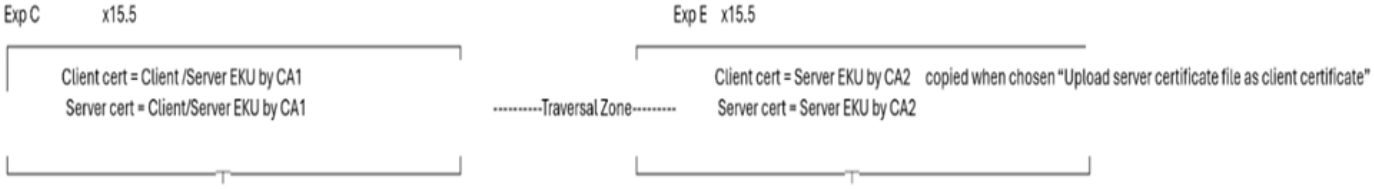
CA 2 =公共CA



在條件3中，所有憑證皆由內部CA(CA1)簽署。

- 當Expressway-E發出TLS連線時，CA 1根/中間需要與遠端實體交換。如果遠端沒有功能或不允許上傳私有CA證書，則TLS連線不成功。
- 如果私有證書不在OS信任儲存中，MRA客戶端將獲得證書以接受彈出視窗。

條件4:Expressway邊緣具有公共證書（僅包含伺服器EKU）



在條件4中，Expressway核心客戶端和伺服器證書是(CA1)內部CA簽名，並且客戶端和伺服器EKU都存在。Expressway E伺服器證書為公共CA簽名，並且只有伺服器EKU。將伺服器證書複製到客戶端證書儲存中，選擇上傳伺服器證書檔案作為客戶端證書。

在條件4中，當與遠端建立TLS連線時，如果Expressway -E傳送TLS客戶端hello，則遠端必須禁用客戶端EKU檢查（因為客戶端證書沒有客戶端身份驗證EKU），否則TLS連線不成功。

根據使用者部署和使用案例，在現場可以有更多的條件或情景，但由於我的思路有限，無法涵蓋所有情況。然而，需要記住的要點是：

- #如果在TLS握手期間Expressway成為客戶端，則客戶端證書將呈現給對等體。
- #IF Expressway在TLS握手期間成為伺服器；伺服器證書呈現給對等體。

該推理已結合這些測試用例進行確立。

案例 1

對於此情況，Expressway會在與Webex進行MTLS握手期間顯示客戶端證書。

Webex會議的視訊通話：

呼叫流Jabber -à CUCM -à Exp Core —à Exp Edge —à Webex示例

10.106.80.31= Expressway Edge

163.129.37.33 = Webex

2026-03-24T11:54:26.106+00:00 smartslave tvcs:UTCTime="2026-03-24 11:54:26,106" Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="10.106.80.31" Local-port="25002" Dst-ip="163.129.37.33" Dst-port="5061"

Expressway邊緣具有使用此序列號(2f0000004c869c77c8981becde00000000004c)的客戶端證書。

Expressway Edge在TLS協商期間向'Webex'傳送客戶端hello，然後傳送客戶端證書。

序列號2f0000004c869c77c8981becde00000000004c:

1.在mTLS協商期間，Expressway Edge將客戶端hello(pkt= 13699)傳送到「Webex」。

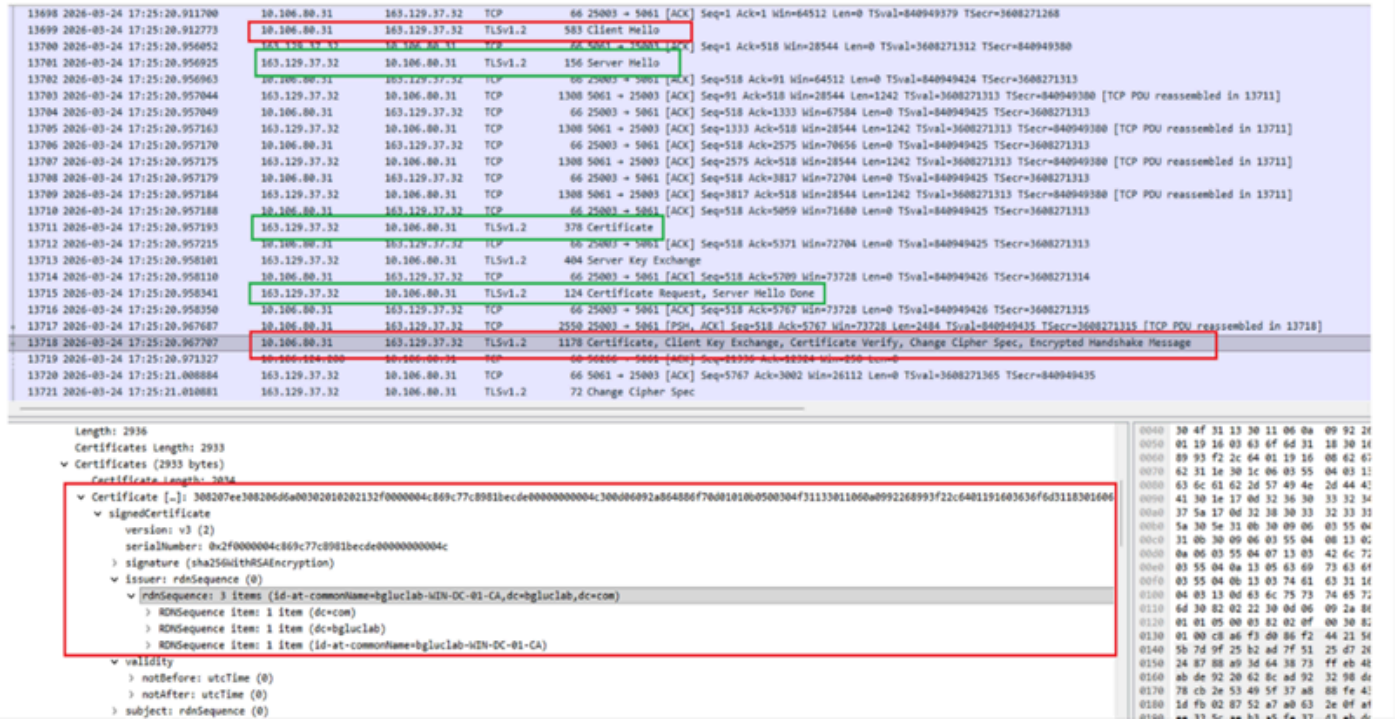
2. Webex向Expressway Edge(pkt=13701)傳送伺服器hello。

3. Webex將其憑證傳送到Expressway Edge(pkt=13711)。

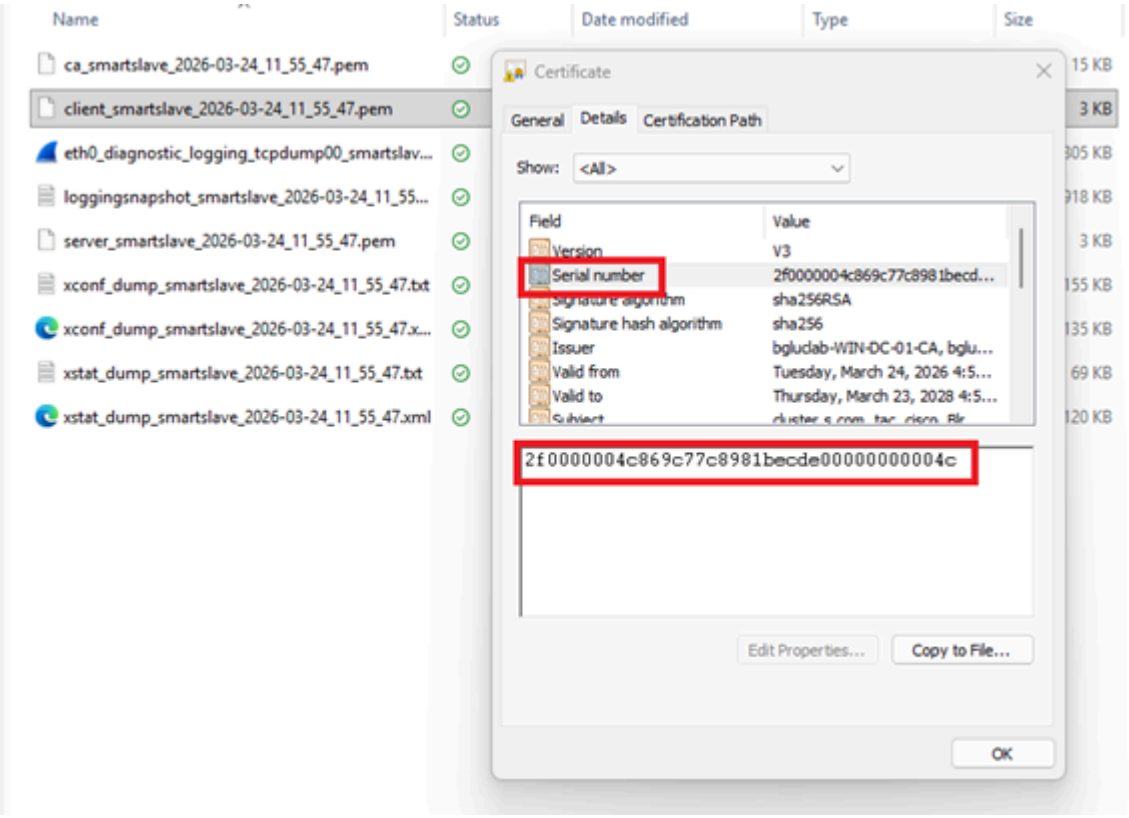
4. Webex請求Expressway邊緣證書「CertificateRequest」(pkt=13715)。

5. Expressway Edge將其證書傳送到Webex(pkt=13718)。

(螢幕截圖)



來自Expressway邊緣的客戶端證書：



案例 2

Expressway在mTLS握手期間成為伺服器實體，並顯示其伺服器證書：

當Expressway提供伺服器證書時，Expressway具有超過5061的安全鄰居區域，其驗證名稱為ON。

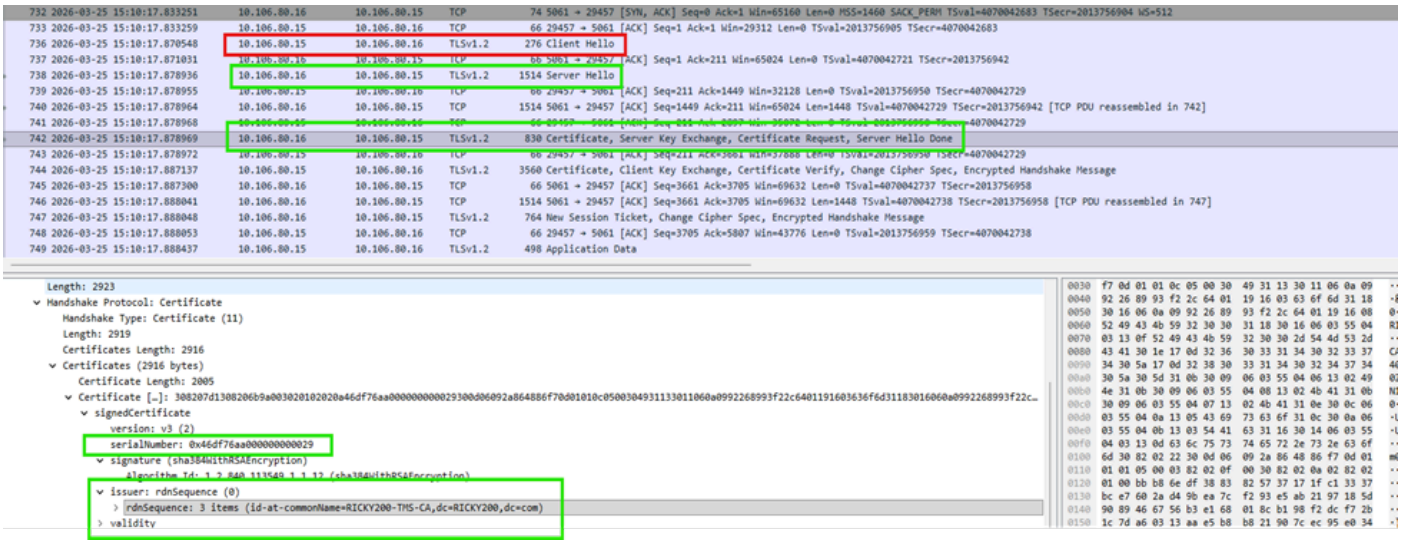
Expressway節點x15.5和Expressway節點x8.11.4之間的安全鄰居區域：

10.106.80.15 (x8.11.4) sends a client hello to 10.106.80.16 (x15.5) (pkt=736)

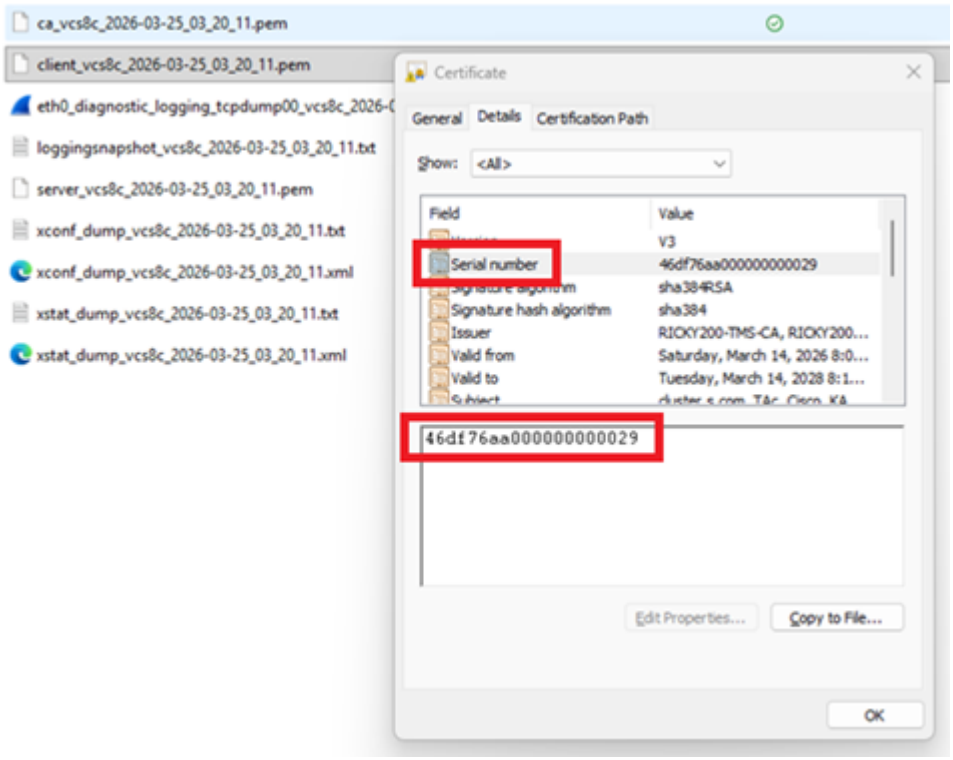
10.106.80.16 sends a server hello to 10.106.80.15 (pkt=738)

10.106.80.16 (x15.5) presents its server cert during TLS handshake (pkt=742) and requests client's cert

10.106.80.15 (x8.11.4) sends client certificate (pkt=744)



此螢幕截圖顯示序列號匹配的伺服器證書：

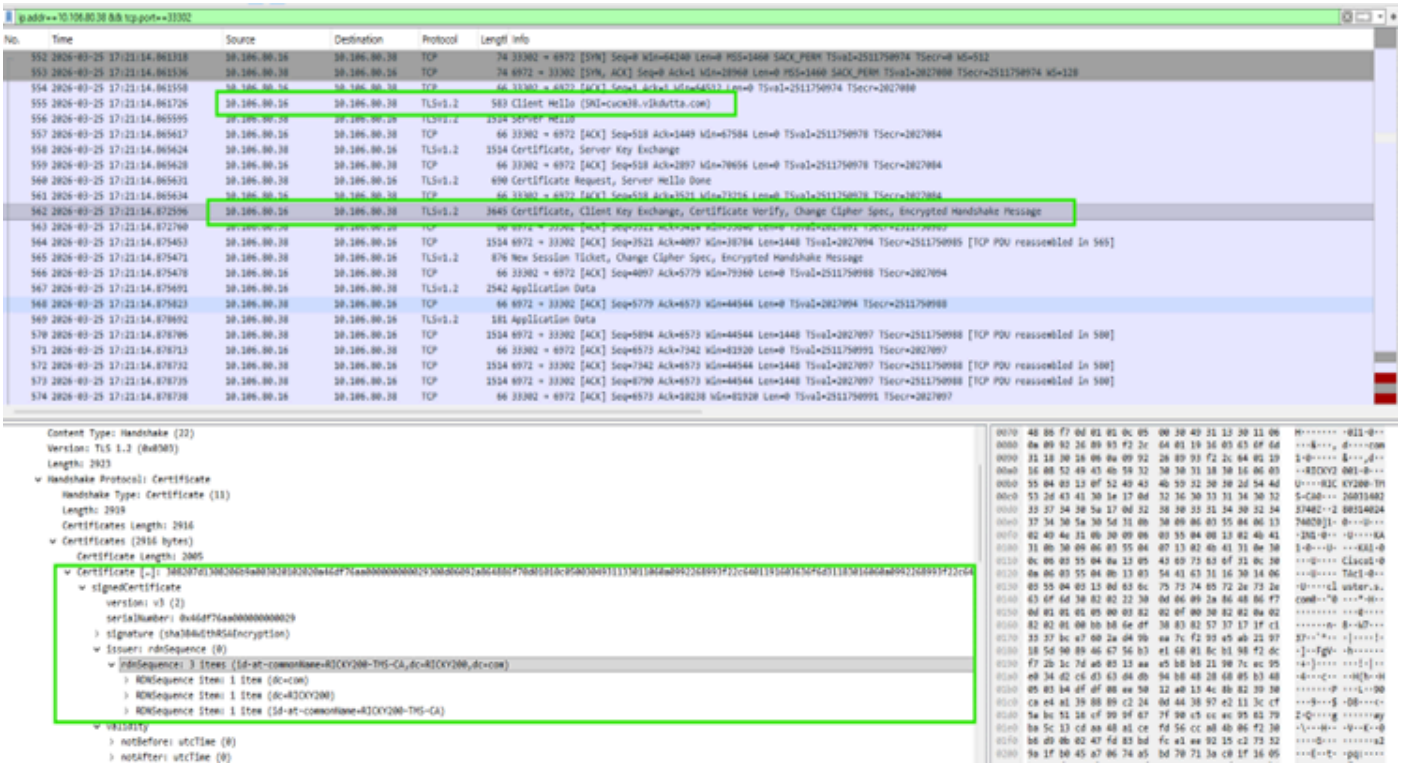


測試案例3:MRA客戶端已設定為登入，工作流包括Expressway核心與CUCM之間的流量伺服器證書驗證。

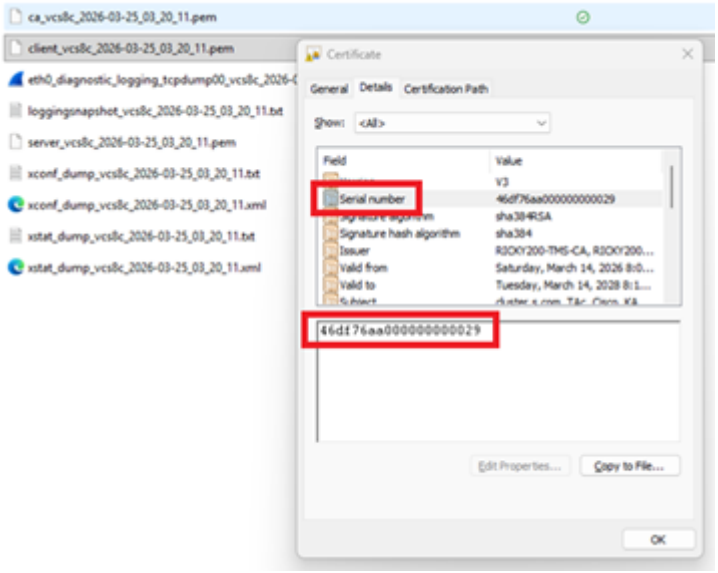
10.106.80.16 = Expressway核心x15.5

10.106.80.38 = CUCM

- Exp C 16在6972 TFTP上傳送客戶端hello。
- Exp C 16在TLS握手期間傳送客戶端證書。



Expressway核心客戶端證書：



關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。