疑難排解WLC上的憑證安裝

目錄

簡介

本檔案介紹在無線LAN控制器(WLC)上使用第三方憑證所造成的問題。

必要條件

需求

思科建議您瞭解以下主題：

- 無線區域網路控制器(WLC)
- 公開金鑰基礎架構 (PKI)
- X.509憑證

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 3504 WLC（韌體版本8.10.105.0）
- 用於命令列工具的OpenSSL 1.0.2p
- Windows 10電腦
- 來自專用實驗室證書頒發機構(CA)的證書鏈，包含三個證書（枝葉、中間、根）
- 簡單式檔案傳輸通訊協定(TFTP)伺服器，用於檔案傳輸。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在AireOS WLC上，您可以安裝將用於WebAuth和WebAdmin的第三方憑證。安裝時，WLC期望有一個PEM(Privacy Enhanced Mail)格式化檔案，其中包含鏈中的所有證書，一直到根CA證書和私鑰。有關此程式的詳細資訊記錄在產生第三方憑證的CSR，並將鏈結的憑證下載到WLC中。

本文檔將展開並詳細展示最常見的安裝錯誤，以及每個方案的調試示例和解決方案。本文檔中使用的調試輸出來自debug transfer all enable和debug pm pki enable（在WLC上啟用）。使用TFTP傳輸憑證檔案。

疑難排解

案例 1.為解密私鑰而提供的密碼不正確或沒有提供密碼

<#root>

```
*TransferTask: Apr 21 03:51:20.737:

Add ID Cert: Adding certificate & private key using password check123


*TransferTask: Apr 21 03:51:20.737:

Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert) to ID table using password check123


*TransferTask: Apr 21 03:51:20.737: Add Cert to ID Table: Decoding PEM-encoded Certificate (verify: YES)
*TransferTask: Apr 21 03:51:20.737: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking string l
*TransferTask: Apr 21 03:51:20.737: Decode & Verify PEM Cert: Cert/Key Length 6276 & VERIFY
*TransferTask: Apr 21 03:51:20.741: Decode & Verify PEM Cert: X509 Cert Verification return code: 1
*TransferTask: Apr 21 03:51:20.741: Decode & Verify PEM Cert: X509 Cert Verification result text: ok
*TransferTask: Apr 21 03:51:20.741:

Add Cert to ID Table: Decoding PEM-encoded Private Key using password check123


*TransferTask: Apr 21 03:51:20.799:

Decode PEM Private Key: Error reading Private Key from PEM-encoded PKCS12 bundle using password check123


*TransferTask: Apr 21 03:51:20.799: Add ID Cert: Error decoding / adding cert to ID cert table (verifyC
*TransferTask: Apr 21 03:51:20.799: Add WebAuth Cert: Error adding ID cert
*TransferTask: Apr 21 03:51:20.799:

RESULT_STRING: Error installing certificate.
```

解決方案：確保提供正確的密碼，以便WLC可以將其解碼以進行安裝。

案例 2.鏈中沒有中繼CA憑證

<#root>

```
*TransferTask: Apr 21 04:34:43.319: Add ID Cert: Adding certificate & private key using password Cisco1
*TransferTask: Apr 21 04:34:43.319: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert)
*TransferTask: Apr 21 04:34:43.319: Add Cert to ID Table: Decoding PEM-encoded Certificate (verify: YES
*TransferTask: Apr 21 04:34:43.319: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking string l
*TransferTask: Apr 21 04:34:43.319: Decode & Verify PEM Cert: Cert/Key Length 4840 & VERIFY
*TransferTask: Apr 21 04:34:43.321: Decode & Verify PEM Cert: X509 Cert Verification return code: 0
*TransferTask: Apr 21 04:34:43.321:
```

Decode & Verify PEM Cert: X509 Cert Verification result text: unable to get local issuer certificate

```
*TransferTask: Apr 21 04:34:43.321:
```

Decode & Verify PEM Cert: Error in X509 Cert Verification at 0 depth: unable to get local issuer certifi

```
*TransferTask: Apr 21 04:34:43.321: Add Cert to ID Table: Error decoding (verify: YES) PEM certificate
*TransferTask: Apr 21 04:34:43.321: Add ID Cert: Error decoding / adding cert to ID cert table (verifyC
*TransferTask: Apr 21 04:34:43.321: Add WebAuth Cert: Error adding ID cert
*TransferTask: Apr 21 04:34:43.321: RESULT_STRING: Error installing certificate.
```

解決方案：驗證WLC憑證中的Issuer和X509v3 Authority Key Identifier欄位，以驗證簽署憑證的CA憑證。如果中間CA憑證是由CA提供的，則此憑證可用於驗證。否則，請向您的CA請求證書。

此OpenSSL指令可用於驗證每個憑證的以下詳細資訊：

<#root>

>

openssl x509 -in

wlc.crt

-text -noout

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
50:93:16:83:04:d5:6b:db:26:7c:3a:13:f3:95:32:7e
Signature Algorithm: sha256WithRSAEncryption
```

Issuer: C=US, O=TAC Lab, CN=Wireless TAC Lab Sub CA

```
Validity
Not Before: Apr 21 03:08:05 2020 GMT
Not After : Apr 21 03:08:05 2021 GMT
Subject: C=US, O=TAC Lab, CN=guest.wirelesslab.local

...

X509v3 extensions:
```

X509v3 Authority Key Identifier:

keyid:27:69:2E:C3:2F:20:5B:07:14:80:E1:86:36:7B:E0:92:08:4C:88:12

<#root>

>

openssl x509 -in

int-ca.crt

-text -noout

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
d1:ec:26:0e:be:f1:aa:65:7b:4a:8f:c7:d5:7f:a4:97
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=TAC Lab, CN=Wireless TAC Lab Root CA
Validity
Not Before: Apr 21 02:51:03 2020 GMT
Not After : Apr 19 02:51:03 2030 GMT

Subject: C=US, O=TAC Lab, CN=Wireless TAC Lab Sub CA

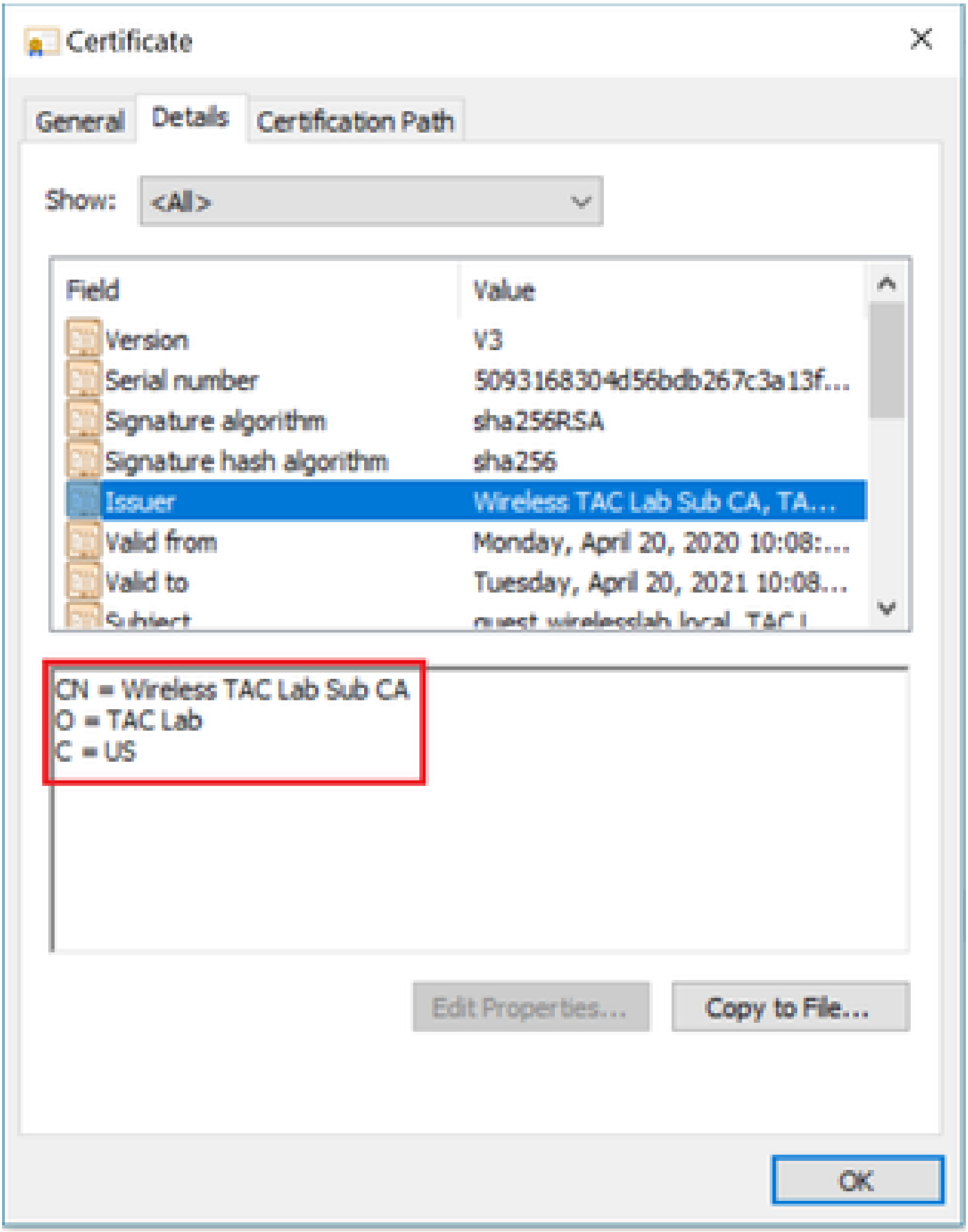
...

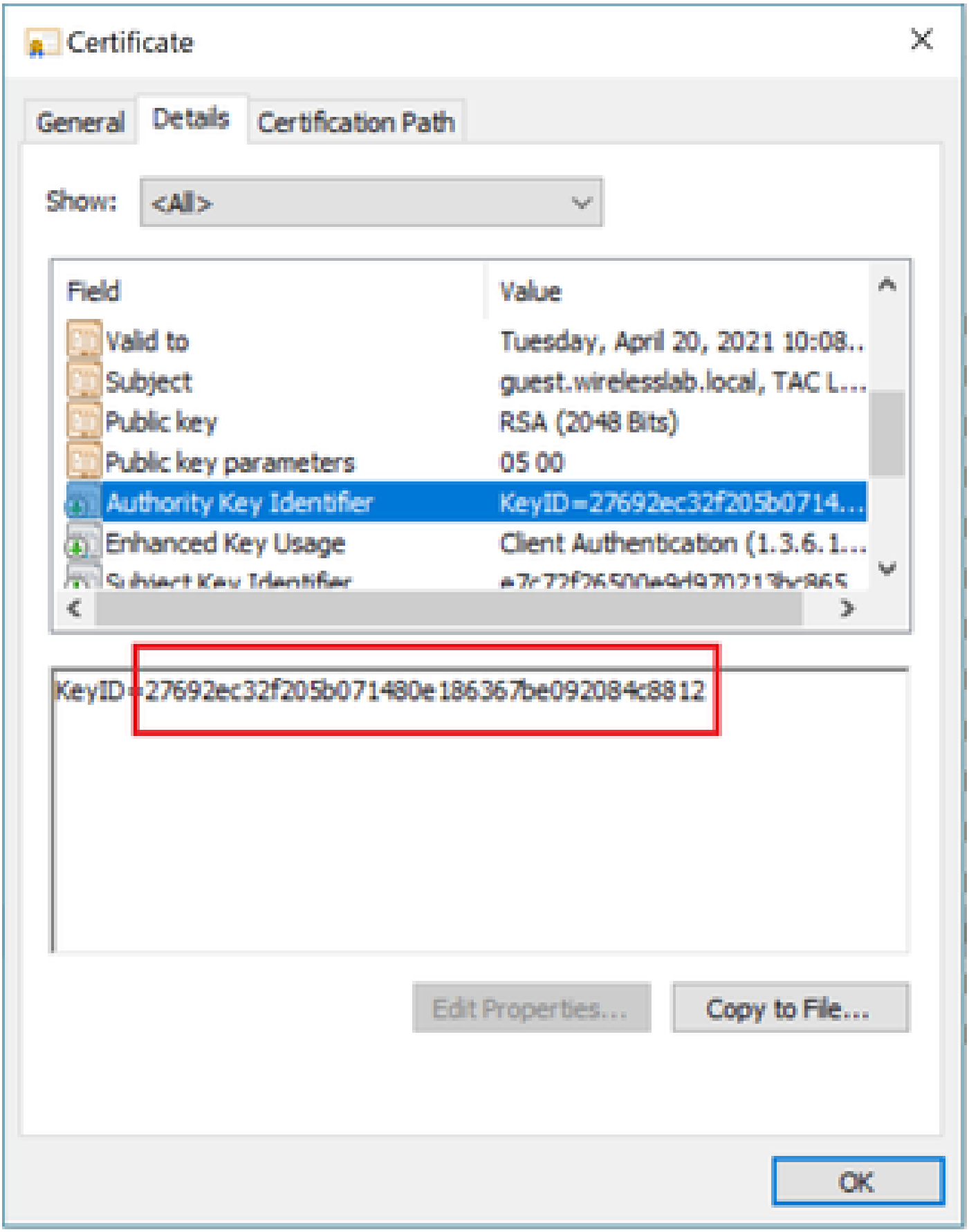
X509v3 Subject Key Identifier:

27:69:2E:C3:2F:20:5B:07:14:80:E1:86:36:7B:E0:92:08:4C:88:12

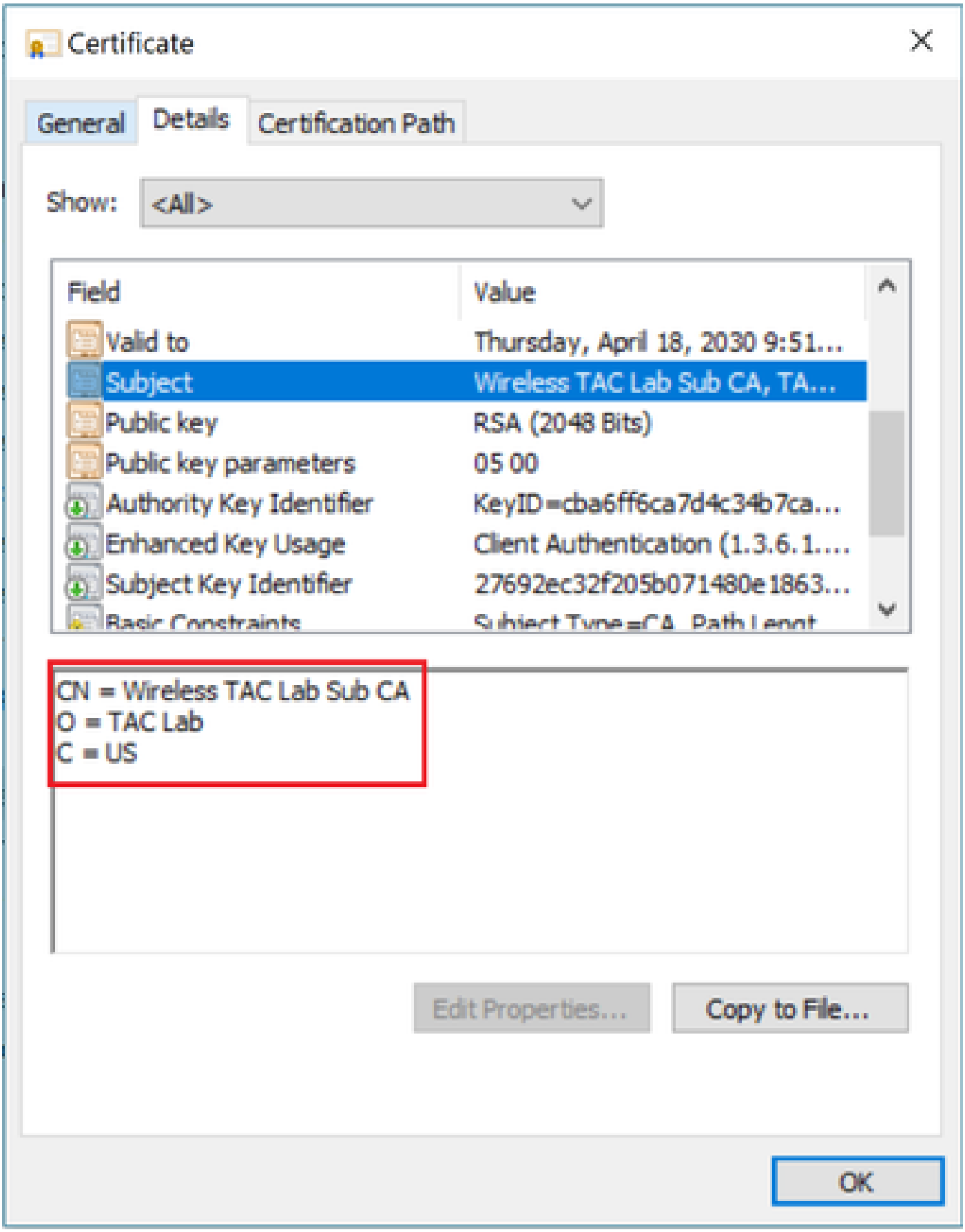
或者，如果您使用Windows，請為證書提供.crt副檔名，然後按兩下以驗證這些詳細資訊。

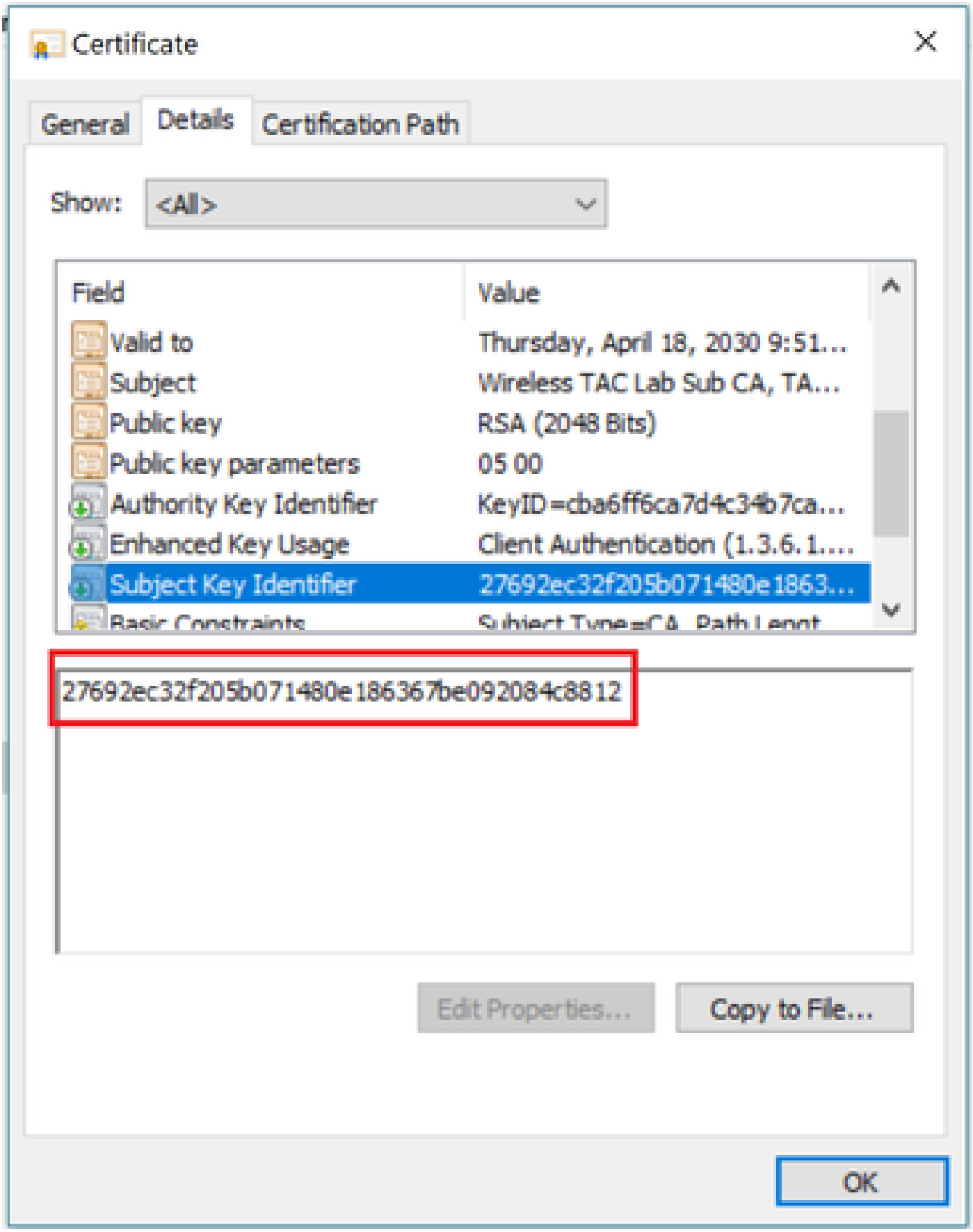
WLC憑證：


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
5093168304d56bdb267c3a13f...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
Wireless TAC Lab Sub CA, TA...
Valid from
Monday, April 20, 2020 10:08:...
Valid to
Tuesday, April 20, 2021 10:08...
CN = Wireless TAC Lab Sub CA
O = TAC Lab
C = US
Edit Properties...
Copy to File...
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Valid to
Tuesday, April 20, 2021 10:08..
Subject
guest.wirelesslab.local, TAC L...
Public key
RSA (2048 Bits)
Public key parameters
05 00
Authority Key Identifier
KeyID=27692ec32f205b0714...
Enhanced Key Usage
Client Authentication (1.3.6.1...
KeyID=27692ec32f205b071480e186367be092084c8812
Edit Properties...
Copy to File...
OK

中間CA證書：


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Valid to
Thursday, April 18, 2030 9:51...
Subject
Wireless TAC Lab Sub CA, TA...
Public key
RSA (2048 Bits)
Public key parameters
05 00
Authority Key Identifier
KeyID=cba6ff6ca7d4c34b7ca...
Enhanced Key Usage
Client Authentication (1.3.6.1....
Subject Key Identifier
27692ec32f205b071480e1863...
CN = Wireless TAC Lab Sub CA
O = TAC Lab
C = US
Edit Properties...
Copy to File...
OK



識別中繼CA憑證後，請相應地繼續鏈結並重新安裝。

案例 3.鏈中沒有根CA憑證

<#root>

```
*TransferTask: Apr 21 04:28:09.643: Add ID Cert: Adding certificate & private key using password Cisco1
*TransferTask: Apr 21 04:28:09.643: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert)
*TransferTask: Apr 21 04:28:09.643: Add Cert to ID Table: Decoding PEM-encoded Certificate (verify: YES)
*TransferTask: Apr 21 04:28:09.643: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking string l
*TransferTask: Apr 21 04:28:09.643: Decode & Verify PEM Cert: Cert/Key Length 4929 & VERIFY
*TransferTask: Apr 21 04:28:09.645: Decode & Verify PEM Cert: X509 Cert Verification return code: 0
*TransferTask: Apr 21 04:28:09.645:
```

Decode & Verify PEM Cert: X509 Cert Verification result text: unable to get issuer certificate

```
*TransferTask: Apr 21 04:28:09.645:
```

Decode & Verify PEM Cert: Error in X509 Cert Verification at 1 depth: unable to get issuer certificate

```
*TransferTask: Apr 21 04:28:09.646: Add Cert to ID Table: Error decoding (verify: YES) PEM certificate
*TransferTask: Apr 21 04:28:09.646: Add ID Cert: Error decoding / adding cert to ID cert table (verifyC
```

解決方案：此案例與案例2類似，但這次針對的是驗證頒發者（根CA）時的中間憑證。在中間CA證書上執行Issuer和X509v3 Authority Key Identifier欄位驗證以驗證根CA時，可以遵循相同的說明。

此OpenSSL指令可用於驗證每個憑證的以下詳細資訊：

<#root>

>

openssl x509 -in

int-ca.crt

-text -noout

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
d1:ec:26:0e:be:f1:aa:65:7b:4a:8f:c7:d5:7f:a4:97
Signature Algorithm: sha256WithRSAEncryption
```

Issuer: C=US, O=TAC Lab, CN=Wireless TAC Lab Root CA

```
Validity
Not Before: Apr 21 02:51:03 2020 GMT
Not After : Apr 19 02:51:03 2030 GMT
Subject: C=US, O=TAC Lab, CN=Wireless TAC Lab Sub CA

...

X509v3 extensions:
```

X509v3 Authority Key Identifier:

keyid:CB:A6:FF:6C:A7:D4:C3:4B:7C:A3:A9:A3:14:C3:90:8D:9B:04:A0:32

<#root>

>

openssl x509 -in

root-ca.crt

-text -noout

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
d1:ec:26:0e:be:f1:aa:65:7b:4a:8f:c7:d5:7f:a4:96
Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, O=TAC Lab, CN=Wireless TAC Lab Root CA

Validity
Not Before: Apr 21 02:40:24 2020 GMT
Not After : Apr 19 02:40:24 2030 GMT

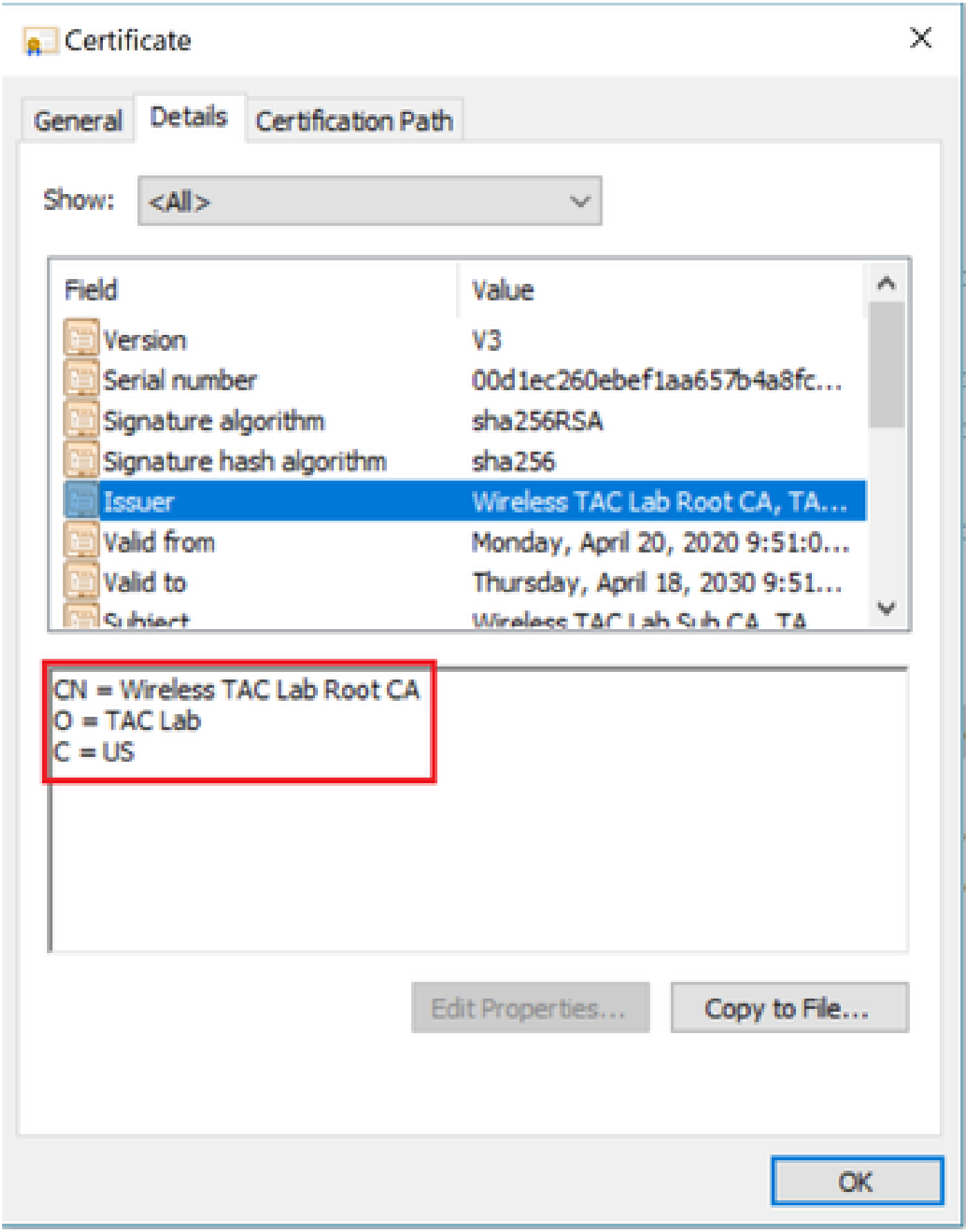
Subject: C=US, O=TAC Lab, CN=Wireless TAC Lab Root CA

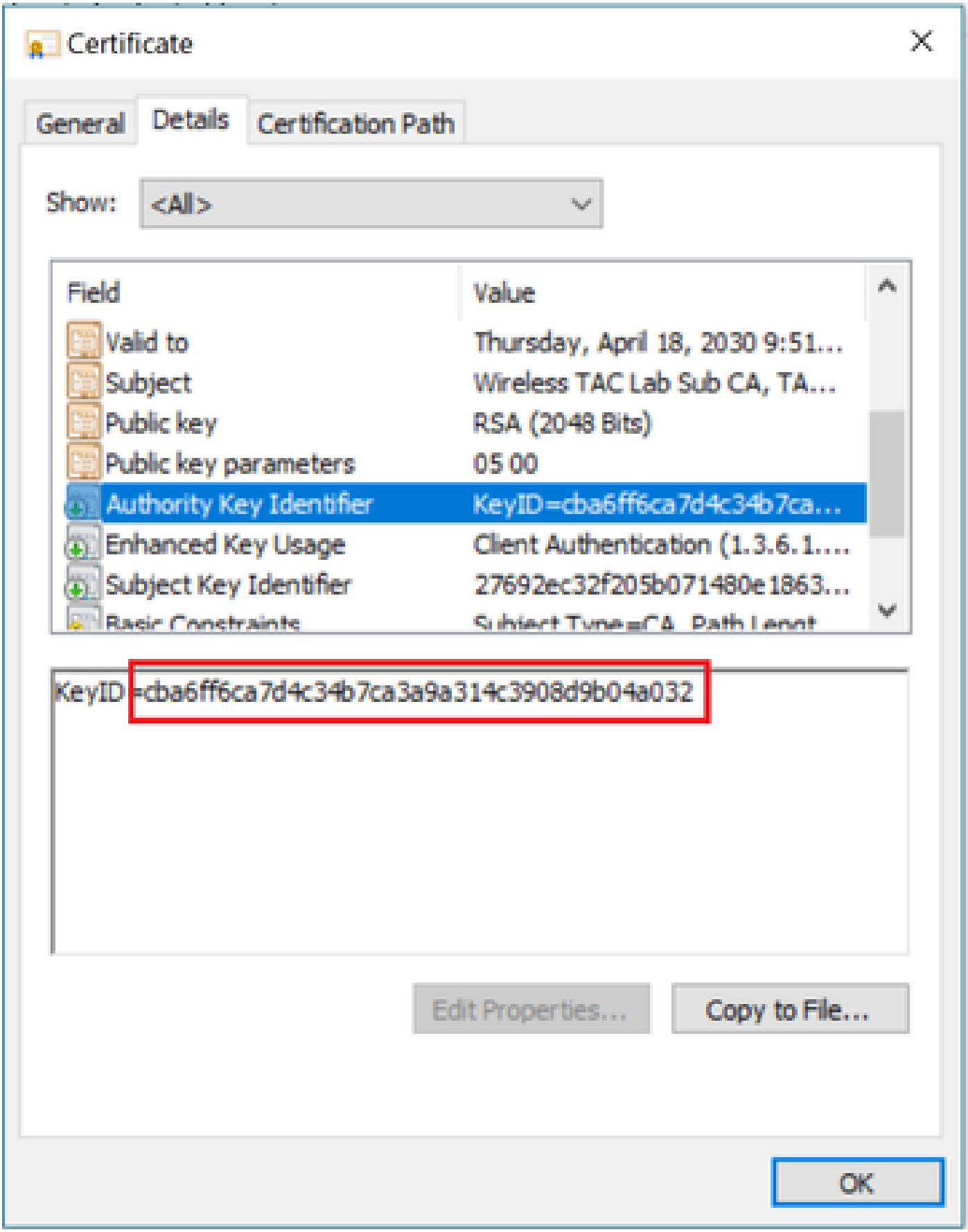
...

X509v3 Subject Key Identifier:

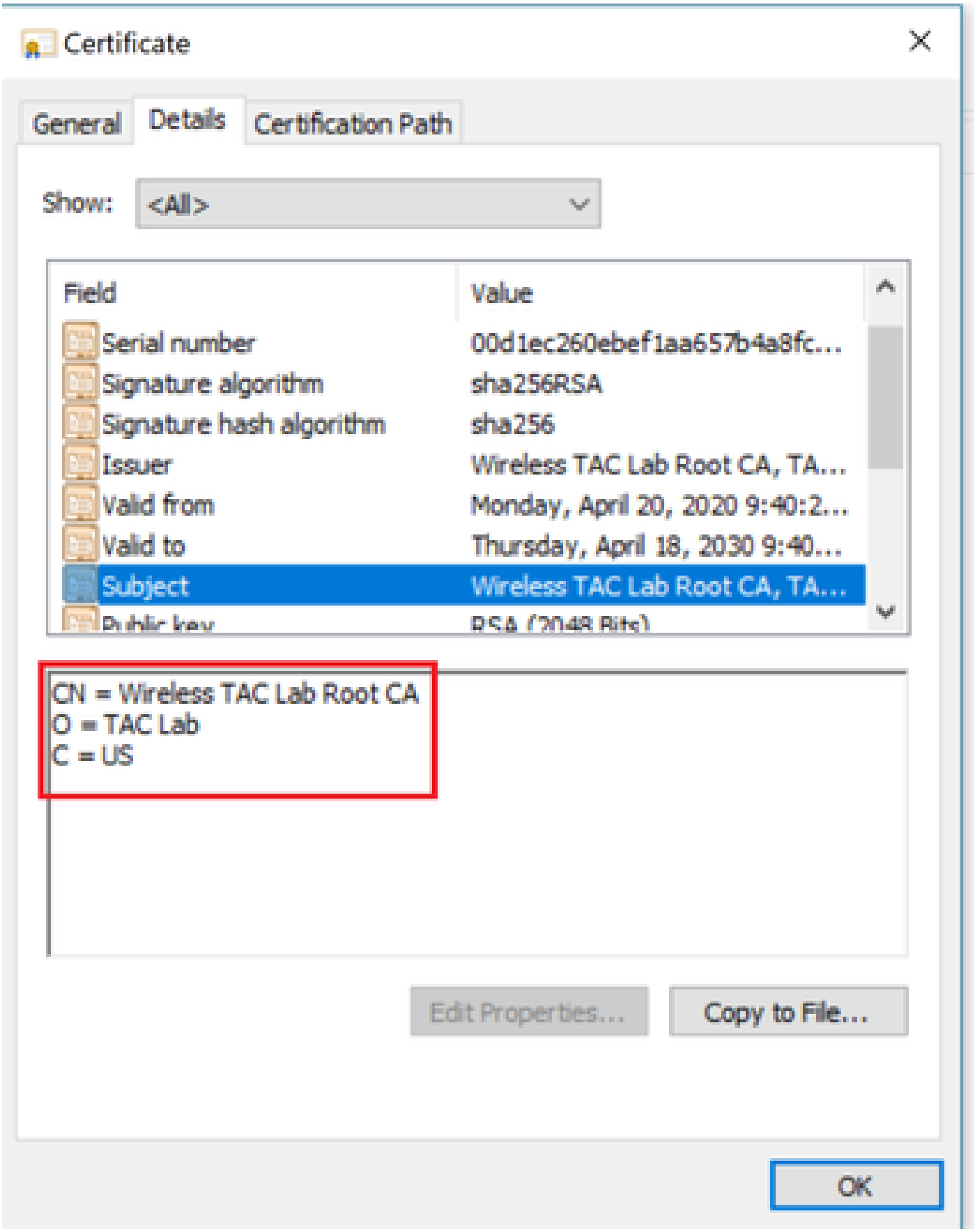
CB:A6:FF:6C:A7:D4:C3:4B:7C:A3:A9:A3:14:C3:90:8D:9B:04:A0:32

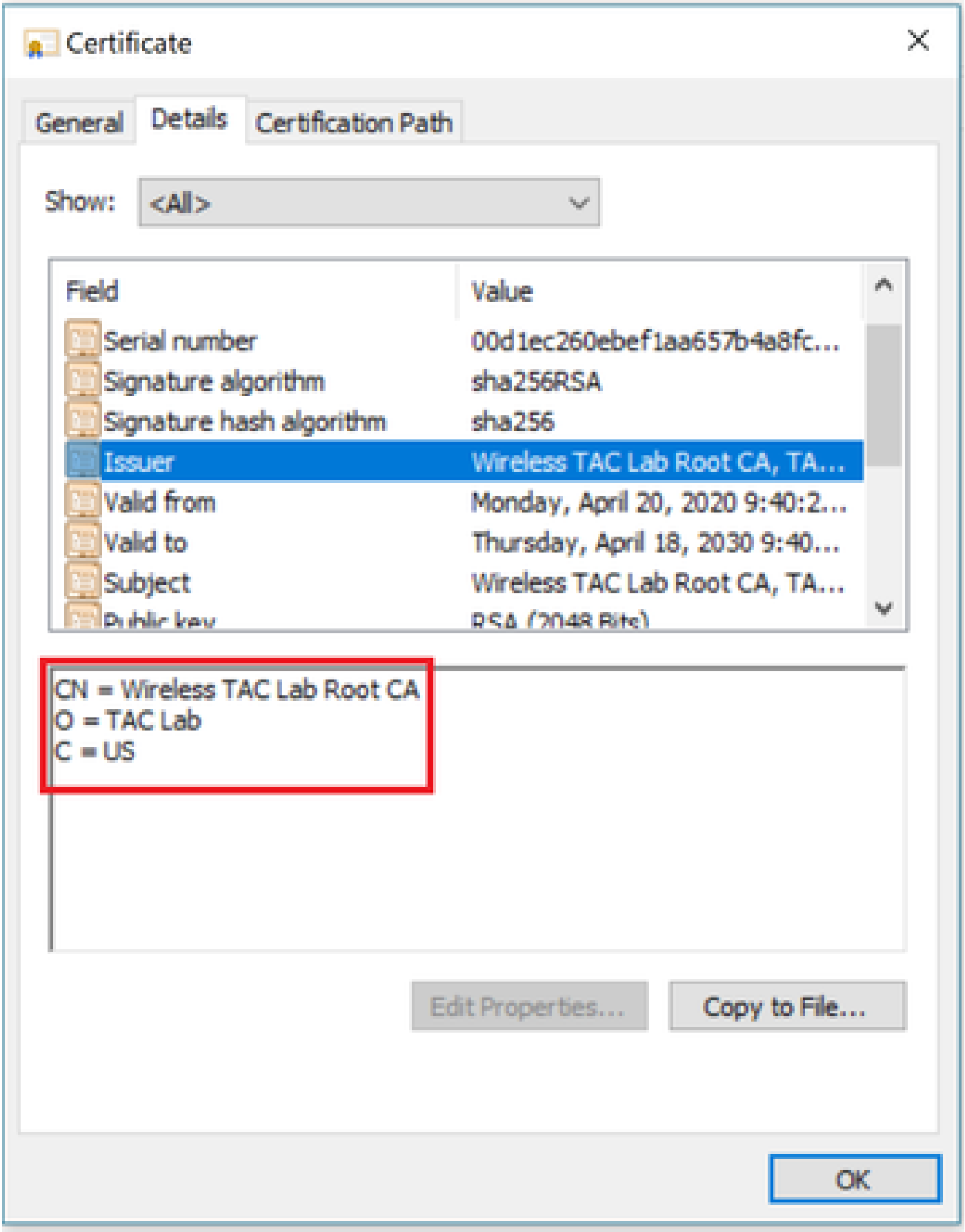
中間CA證書

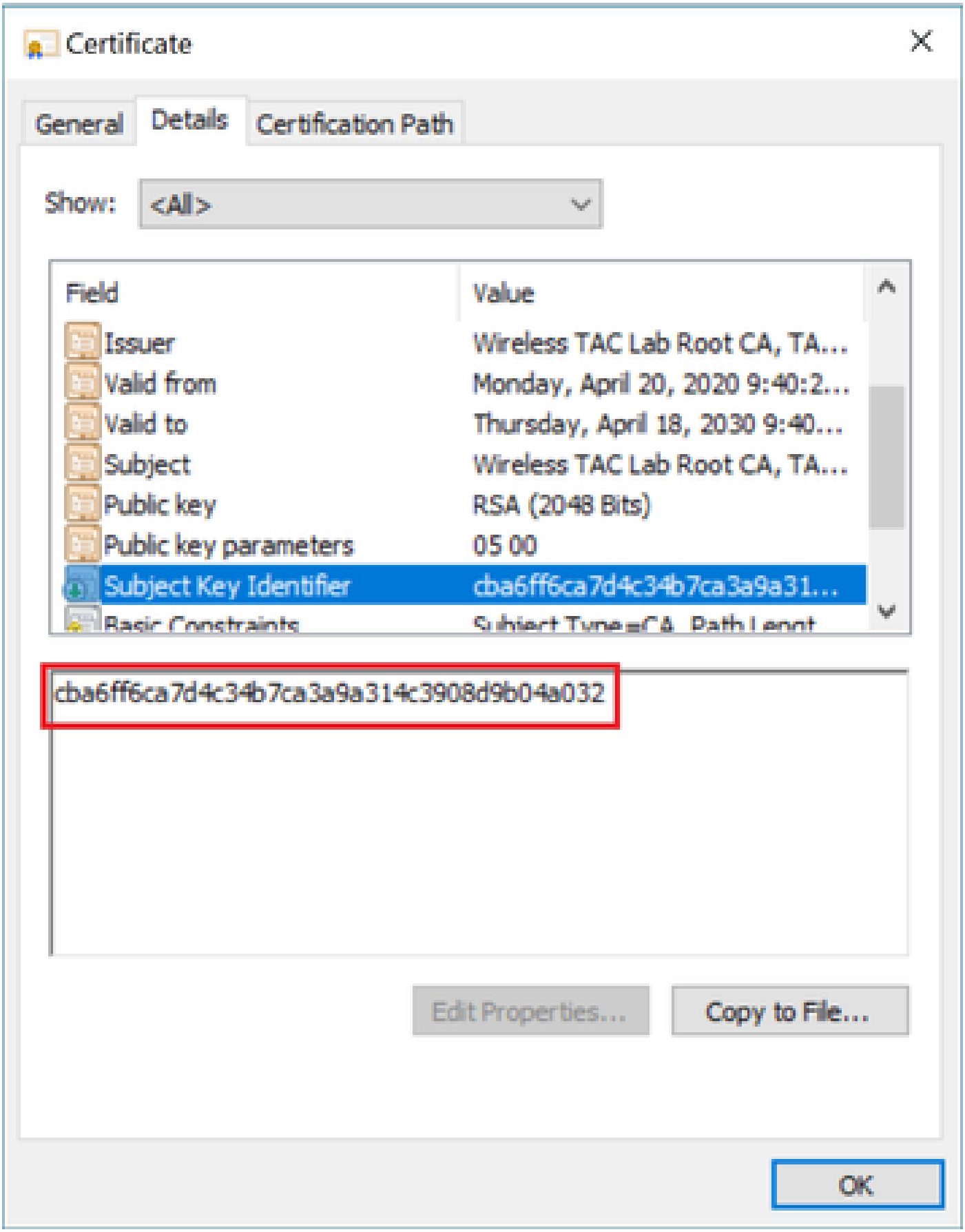

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
00d1ec260ebef1aa657b4a8fc...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
Wireless TAC Lab Root CA, TA...
Valid from
Monday, April 20, 2020 9:51:0...
Valid to
Thursday, April 18, 2030 9:51...
CN = Wireless TAC Lab Root CA
O = TAC Lab
C = US
Edit Properties...
Copy to File...
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Valid to
Thursday, April 18, 2030 9:51...
Subject
Wireless TAC Lab Sub CA, TA...
Public key
RSA (2048 Bits)
Public key parameters
05 00
Authority Key Identifier
KeyID=dba6ff6ca7d4c34b7ca...
Enhanced Key Usage
Client Authentication (1.3.6.1....
Subject Key Identifier
27692ec32f205b071480e1863...
KeyID=dba6ff6ca7d4c34b7ca3a9a314c3908d9b04a032
Edit Properties...
Copy to File...
OK

根CA證書：


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Serial number
00d1ec260ebef1aa657b4a8fc...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
Wireless TAC Lab Root CA, TA...
Valid from
Monday, April 20, 2020 9:40:2...
Valid to
Thursday, April 18, 2030 9:40...
Subject
Wireless TAC Lab Root CA, TA...
CN = Wireless TAC Lab Root CA
O = TAC Lab
C = US
Edit Properties...
Copy to File...
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Serial number
00d1ec260ebef1aa657b4a8fc...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
Wireless TAC Lab Root CA, TA...
Valid from
Monday, April 20, 2020 9:40:2...
Valid to
Thursday, April 18, 2030 9:40...
Subject
Wireless TAC Lab Root CA, TA...
CN = Wireless TAC Lab Root CA
O = TAC Lab
C = US
Edit Properties...
Copy to File...
OK



識別根CA證書後（頒發者和使用者相同），相應地繼續鏈並重新安裝。

註：本文檔使用三個證書鏈（枝葉、中間CA和根CA），這是最常見的情況。可能會發生涉及

2個中間CA證書的情況。在找到根CA證書之前，可以使用此方案中的同一准則。

案例 4.鏈中沒有CA憑證

<#root>

```
*TransferTask: Apr 21 04:56:50.272: Add ID Cert: Adding certificate & private key using password Cisco1
*TransferTask: Apr 21 04:56:50.272: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert)
*TransferTask: Apr 21 04:56:50.272: Add Cert to ID Table: Decoding PEM-encoded Certificate (verify: YES
*TransferTask: Apr 21 04:56:50.272: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking string l
*TransferTask: Apr 21 04:56:50.272: Decode & Verify PEM Cert: Cert/Key Length 3493 & VERIFY
*TransferTask: Apr 21 04:56:50.273: Decode & Verify PEM Cert: X509 Cert Verification return code: 0
*TransferTask: Apr 21 04:56:50.273:
```

Decode & Verify PEM Cert: Error in X509 Cert Verification at 0 depth: unable to get local issuer certifi

```
*TransferTask: Apr 21 04:56:50.274: Add Cert to ID Table: Error decoding (verify: YES) PEM certificate
*TransferTask: Apr 21 04:56:50.274: Add WebAuth Cert: Error adding ID cert
*TransferTask: Apr 21 04:56:50.274: RESULT_STRING: Error installing certificate.
```

解決方案：如果檔案中除了WLC證書之外沒有其他證書，驗證將在驗證時失敗，驗證深度為0。可在文本編輯器中開啟該檔案以進行驗證。可以按照案例2和案例3中的指導原則來識別到根CA的鏈條，然後相應地重新鏈條並重新安裝。

案例 5.無私鑰

<#root>

```
*TransferTask: Apr 21 05:02:34.764: Add WebAuth Cert: Adding certificate & private key using password
*TransferTask: Apr 21 05:02:34.764: Add ID Cert: Adding certificate & private key using password
*TransferTask: Apr 21 05:02:34.764: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert)
*TransferTask: Apr 21 05:02:34.764: Add Cert to ID Table: Decoding PEM-encoded Certificate (verify: YES
*TransferTask: Apr 21 05:02:34.764: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking string l
*TransferTask: Apr 21 05:02:34.764: Decode & Verify PEM Cert: Cert/Key Length 3918 & VERIFY
*TransferTask: Apr 21 05:02:34.767: Decode & Verify PEM Cert: X509 Cert Verification return code: 1
*TransferTask: Apr 21 05:02:34.767: Decode & Verify PEM Cert: X509 Cert Verification result text: ok
*TransferTask: Apr 21 05:02:34.768: Add Cert to ID Table: Decoding PEM-encoded Private Key using passwo
*TransferTask: Apr 21 05:02:34.768:
```

Retrieve CSR Key: can't open private key file for ssl cert.

```
*TransferTask: Apr 21 05:02:34.768:
```

Add Cert to ID Table: No Private Key

```
*TransferTask: Apr 21 05:02:34.768: Add ID Cert: Error decoding / adding cert to ID cert table (verifyC
*TransferTask: Apr 21 05:02:34.768: Add WebAuth Cert: Error adding ID cert
*TransferTask: Apr 21 05:02:34.768: RESULT_STRING: Error installing certificate.
```

解決方案：如果憑證簽署請求(CSR)是從外部產生的，且需要鏈結在檔案中，WLC預期會在檔案中包含私密金鑰。在WLC中產生CSR的情況下，請確保安裝前未重新載入WLC，否則私人金鑰會遺失。

相關資訊

- 思科技術支援與下載

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）。