排除WLC上的证书安装故障

目录

简介
先决条件
要求
使用的组件
背景信息
故障排除
场景 1.提供的用于解密私钥的密码不正确或未提供密码
场景 2：链中没有中间CA证书
场景 3：链中没有根CA证书
场景 4.链中没有CA证书
方案 5.无私钥
相关信息

简介

本文档介绍在无线局域网控制器(WLC)上使用第三方证书导致的问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 无线LAN控制器(WLC)
- 公用密钥基础结构 (PKI)
- X.509证书

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 固件版本为8.10.105.0的3504 WLC
- 用于命令行工具的OpenSSL 1.0.2p
- Windows 10计算机
- 来自专用实验室证书颁发机构(CA)的证书链，包含三个证书（枝叶、中级、根）
- 用于文件传输的简单文件传输协议(TFTP)服务器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在AireOS WLC上，您可以安装用于WebAuth和WebAdmin的第三方证书。安装时，WLC需要一个PEM(Privacy Enhanced Mail)格式化文件，文件链中的所有证书一直到根CA证书和私钥。有关此过程的详细信息记录在生成第三方证书的CSR并将链接证书下载到WLC中。

本文档将展开并更详细地显示最常见的安装错误，以及每个场景的调试示例和解决方案。本文档中使用的调试输出来自debug transfer all enable和debug pm pki enable，后者在WLC上启用。使用TFTP传输证书文件。

故障排除

场景 1.提供的用于解密私钥的密码不正确或未提供密码

<#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 check12


*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.
```

解决方案：确保提供正确的密码，以便WLC可以将其解码以进行安装。

场景 2：链中没有中间CA证书

<#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.
```

解决方案：验证WLC证书中的颁发者和X509v3授权密钥标识符字段，以验证签署证书的CA证书。如果中间CA证书由CA提供，则可用于进行验证。否则，请向您的CA申请证书。

此OpenSSL命令可用于验证每个证书的以下详细信息：

<#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:

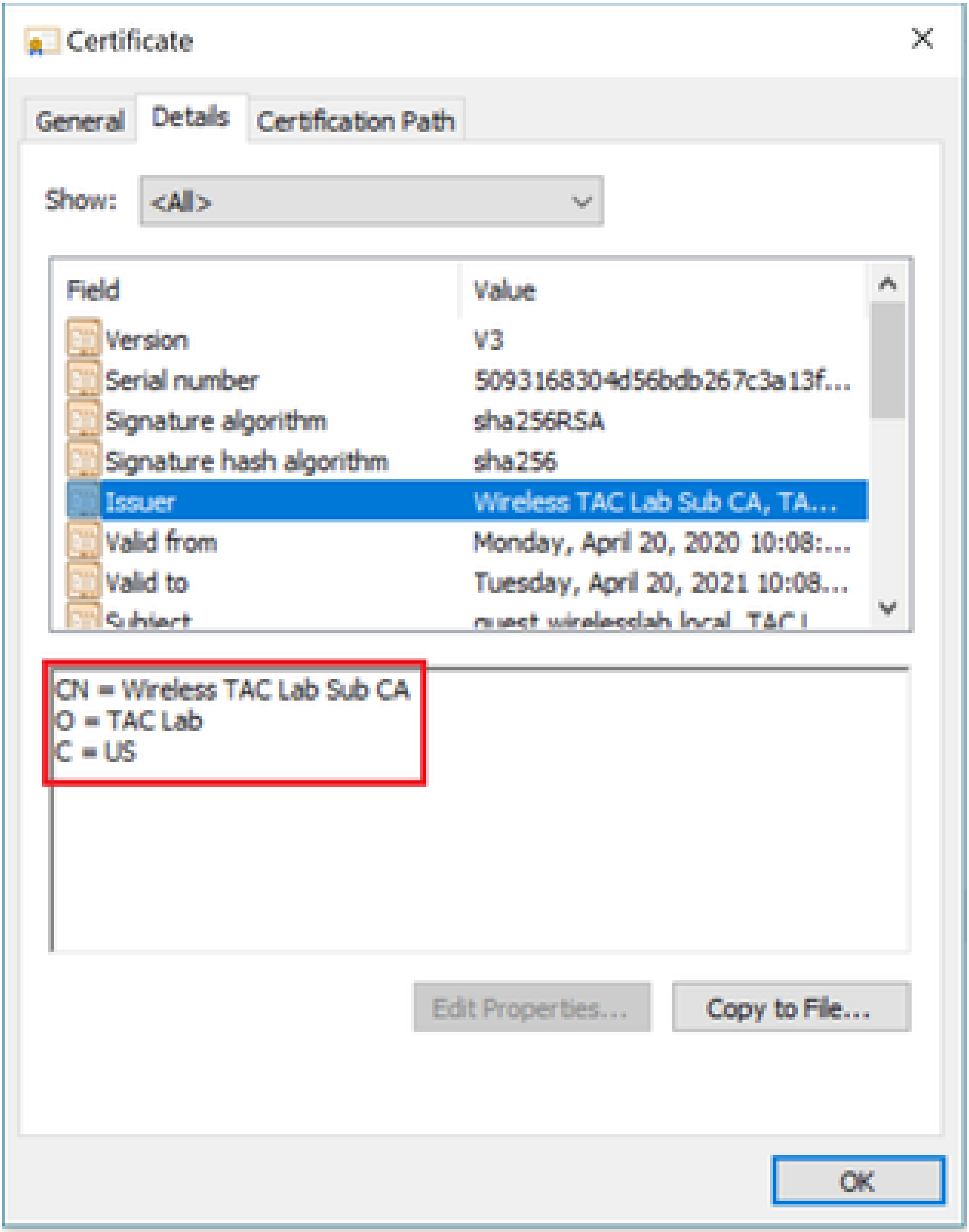
```
keyid:27:69:2E:C3:2F:20:5B:07:14:80:E1:86:36:7B:E0:92:08:4C:88:12
```

<#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，如果使用Windows，请为证书提供.crt扩展名，然后双击以验证这些详细信息。

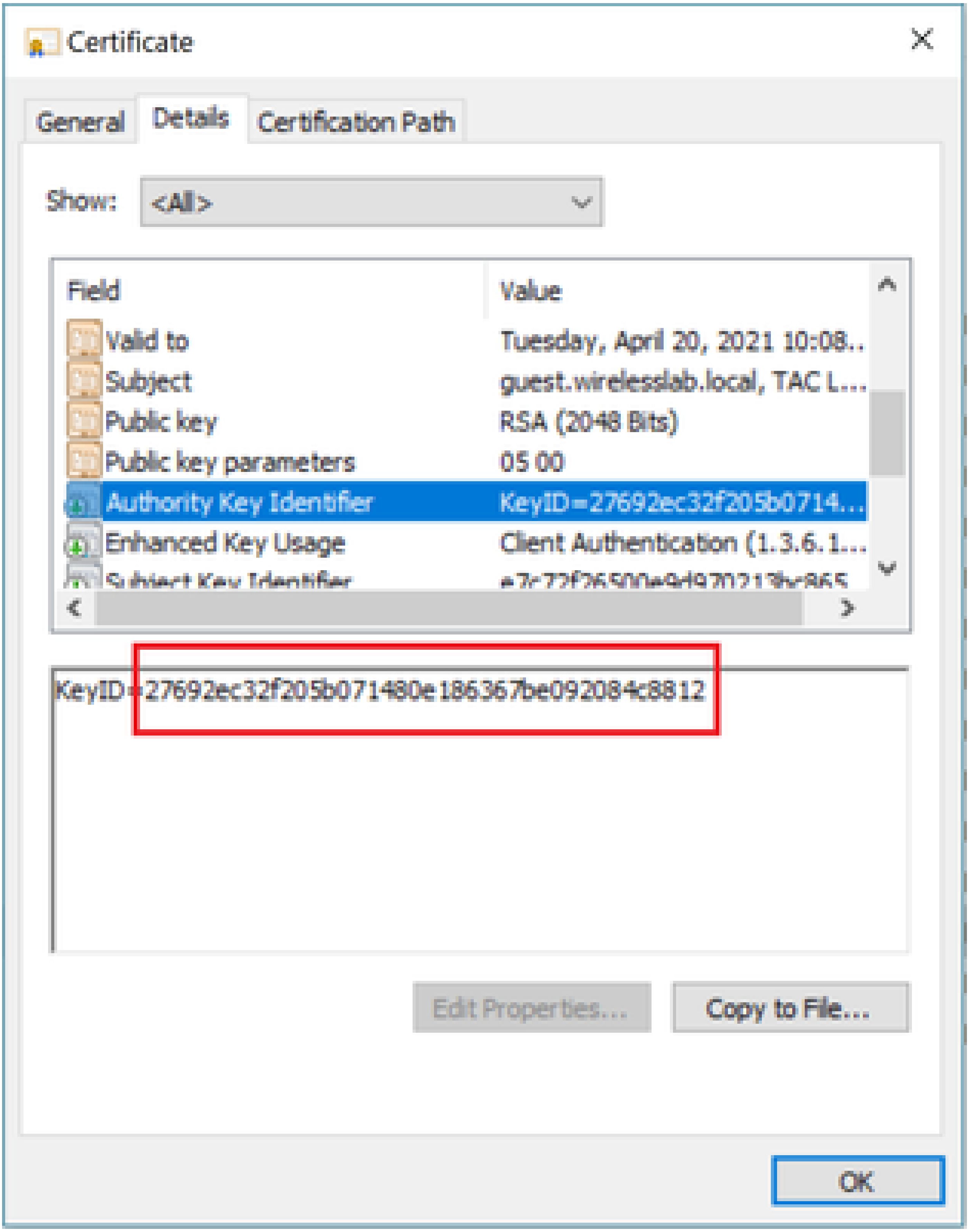
WLC证书：



Show: <All>

Field	Value
Version	V3
Serial number	509316830 4d56bdb267c3a13f...
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...
Subject	guest.wirelesslab.local, TAC L

CN = Wireless TAC Lab Sub CA
O = TAC Lab
C = US

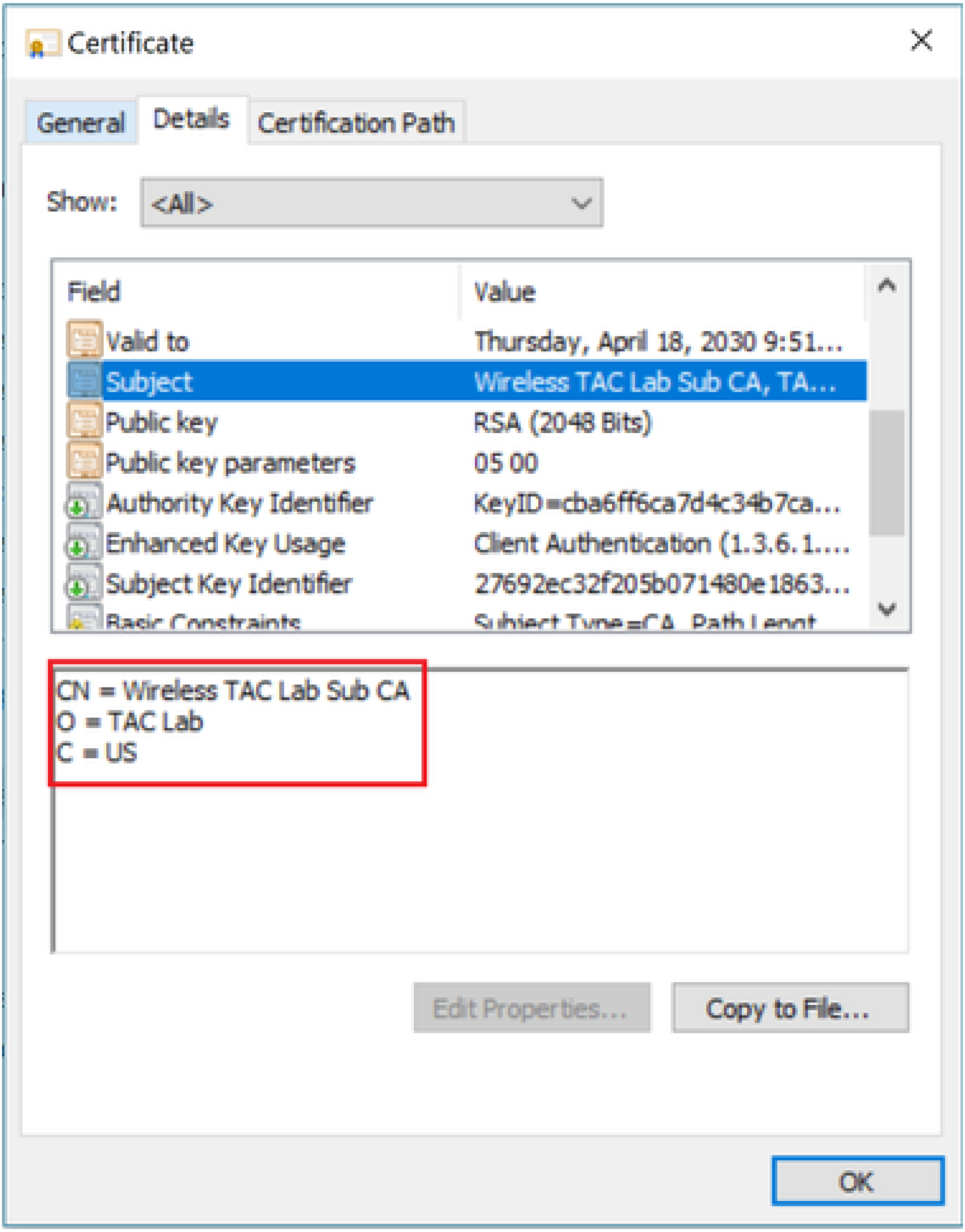


Show: <All>

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...
Subject Key Identifier	e7c72f26500e9d970213bc865

KeyID=27692ec32f205b071480e186367be092084c8812

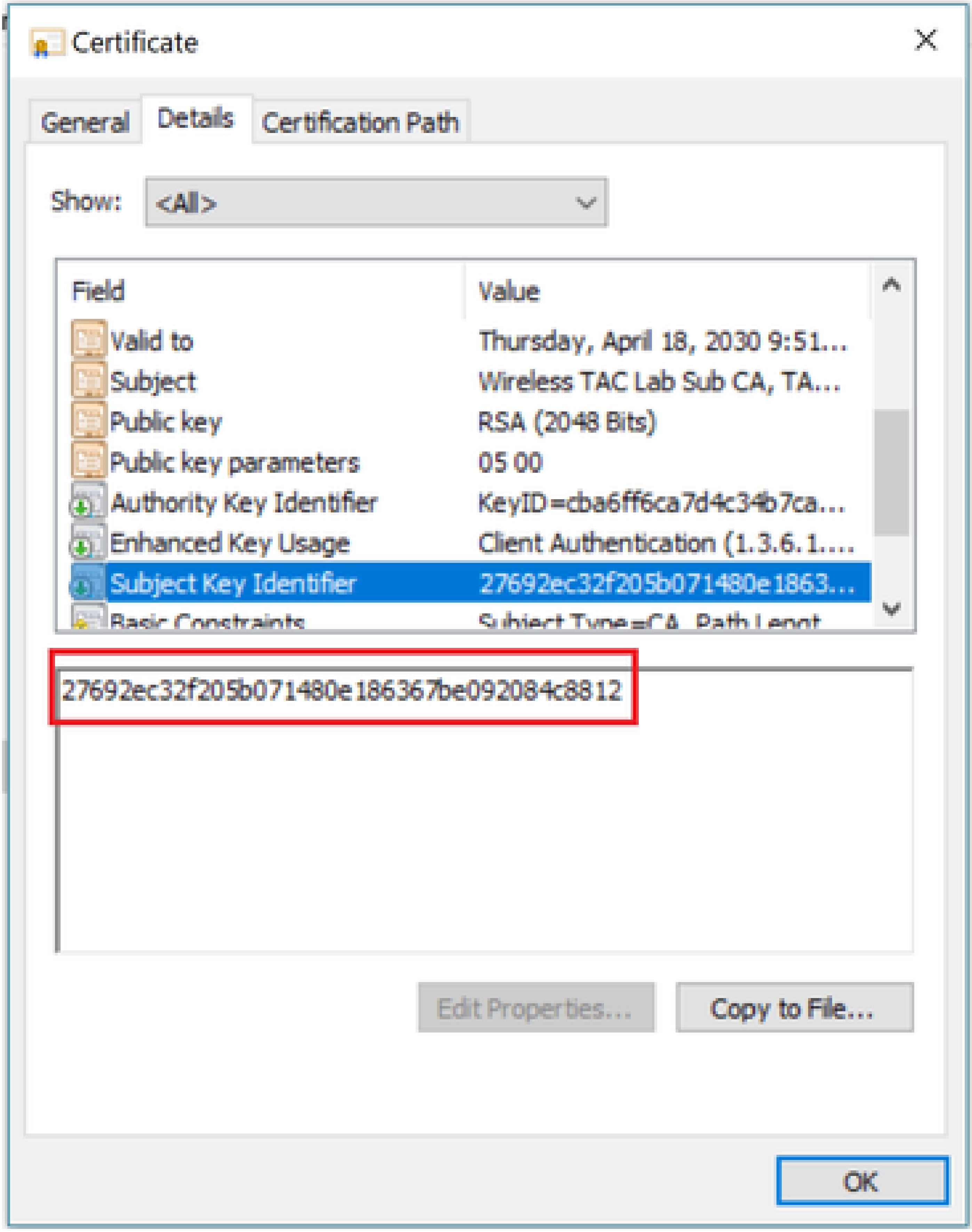
中间CA证书：



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...
Basic Constraints	Subject Type=CA, Path Lengt

CN = Wireless TAC Lab Sub CA
O = TAC Lab
C = US



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...
Basic Constraints	Subject Type=CA, Path Lengt

27692ec32f205b071480e186367be092084c8812

确定中间CA证书后，相应地继续链并重新安装。

场景 3：链中没有根CA证书

```
<#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
```

解决方案：此方案与方案2类似，但这次针对的是验证颁发者（根CA）时的中间证书。在中间CA证书上执行Issuer和X509v3 Authority Key Identifier字段验证以验证根CA，可以遵循相同的说明。

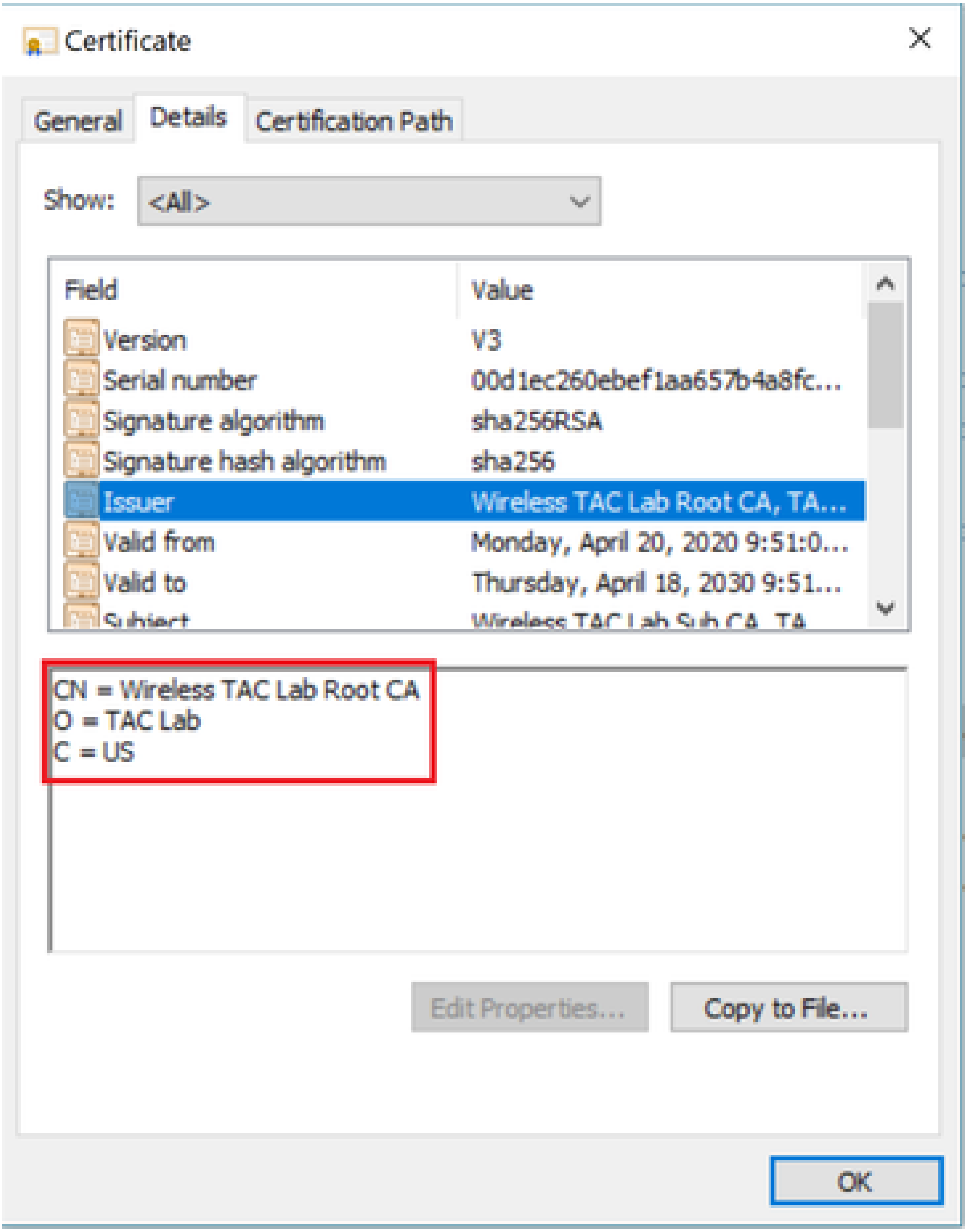
此OpenSSL命令可用于验证每个证书的以下详细信息：

```
<#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
```

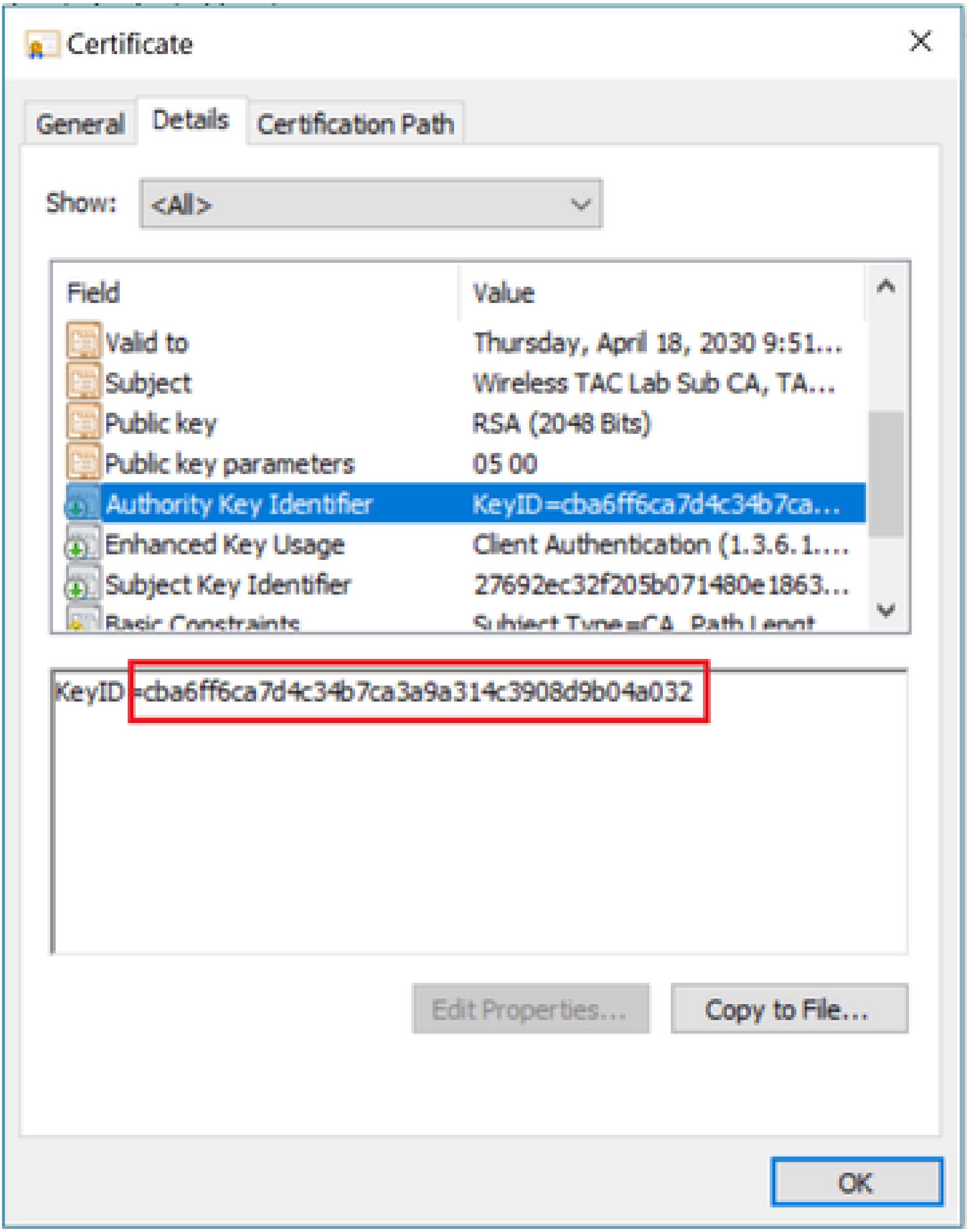
<#root>

```
>

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
```

中间CA证书



CN = Wireless TAC Lab Root CA
O = TAC Lab
C = US

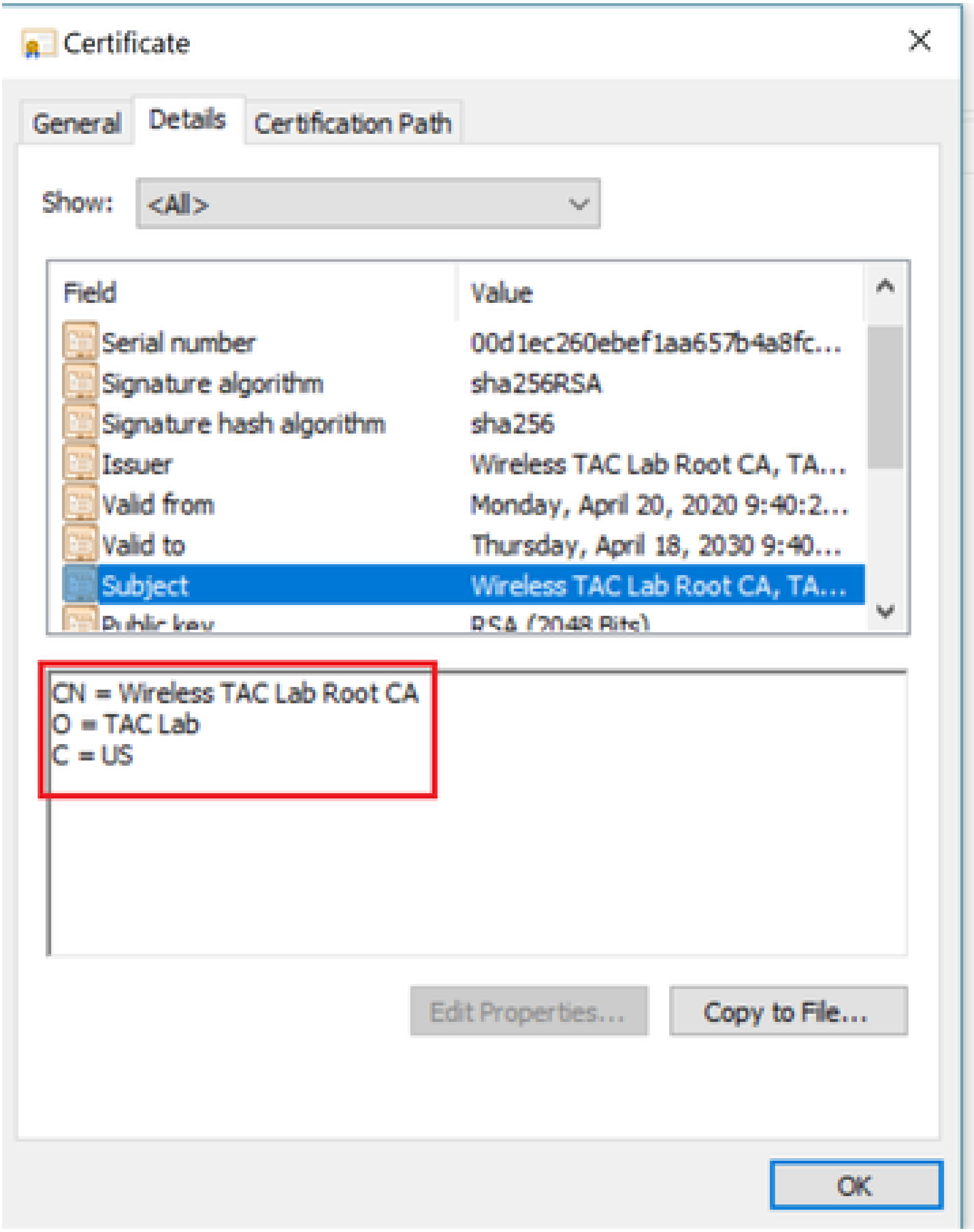


Show: <All>

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...
Basic Constraints	Subject Type=CA, Path Lengt

KeyID=cba6ff6ca7d4c34b7ca3a9a314c3908d9b04a032

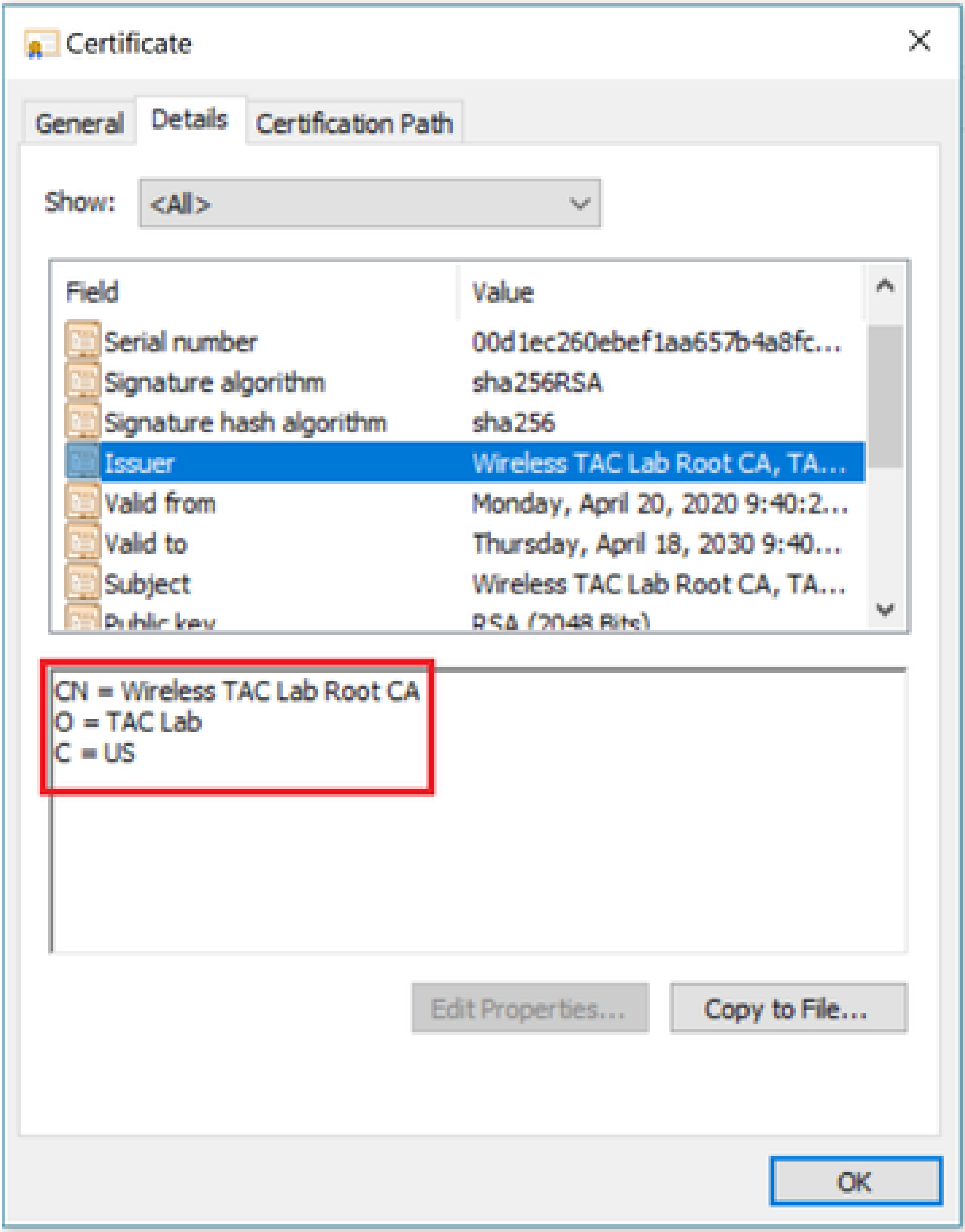
根CA证书：



Show: <All>

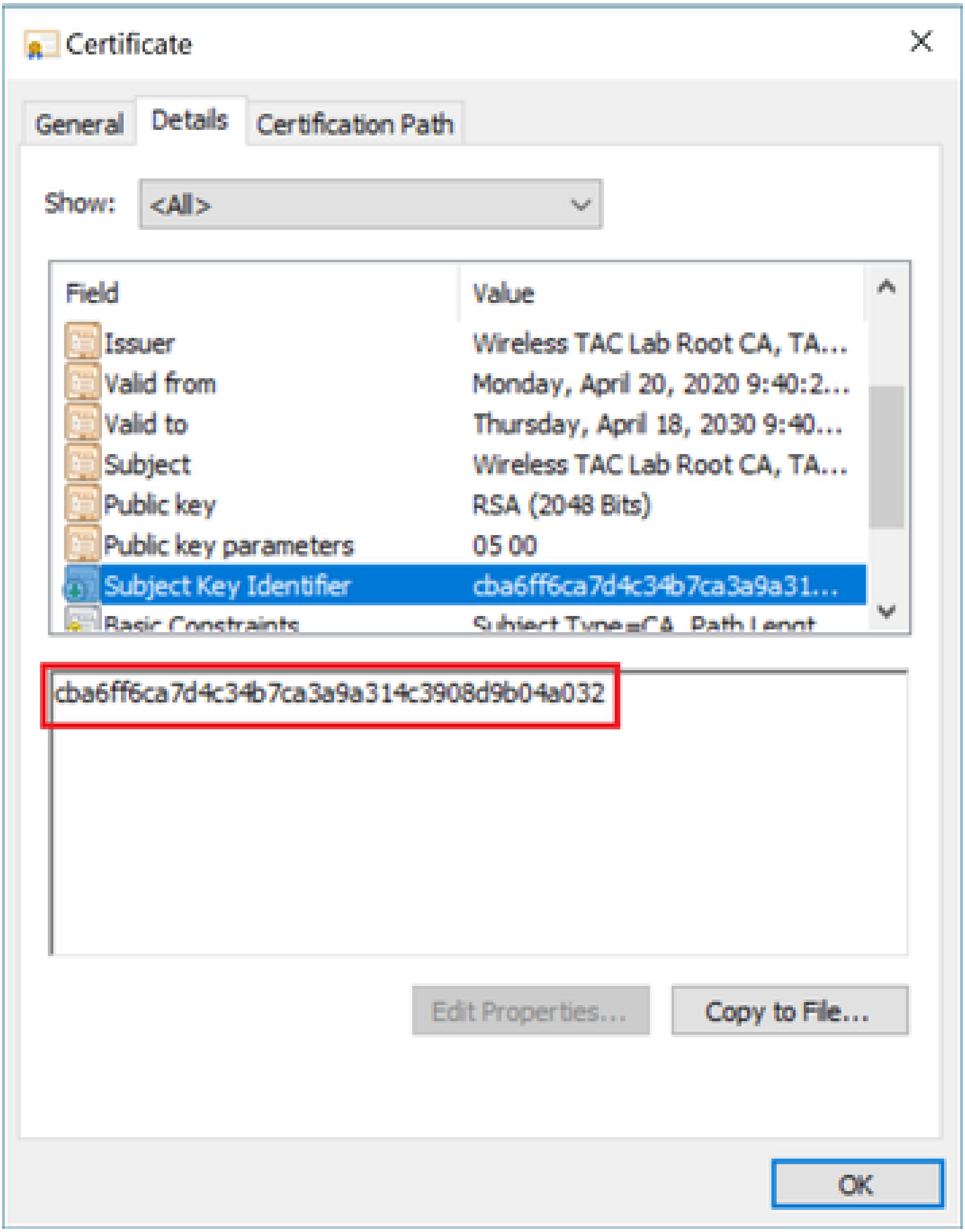
Field	Value
Serial number	00d1ec260ebef1aa657b4a8fc...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Wireless TAC Lab Root CA, TA...
Valid from	Monday, April 20, 2020 9:40:2...
Valid to	Thursday, April 18, 2030 9:40...
Subject	Wireless TAC Lab Root CA, TA...
Public key	RSA (2048 Bits)

CN = Wireless TAC Lab Root CA
O = TAC Lab
C = US



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...
Public key	RSA (2048 Bits)

CN = Wireless TAC Lab Root CA
O = TAC Lab
C = US



Field	Value
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...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Subject Key Identifier	cba6ff6ca7d4c34b7ca3a9a31...
Basic Constraints	Subject Type=CA, Path Lengt

cba6ff6ca7d4c34b7ca3a9a314c3908d9b04a032

确定根CA证书后（颁发者和主题相同），相应地继续链并重新安装。

注意：本文档使用三个证书链（枝叶、中间CA、根CA），这是最常见的场景。可能会出现涉

及2个中间CA证书的情况。在找到根CA证书之前，可以使用此方案的相同指南。

场景 4.链中没有CA证书

<#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 certif


*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.
```

解决方案：如果文件中除WLC证书外没有其他证书，验证在0深度处的验证失败。可在文本编辑器中打开该文件以进行验证。可以按照场景2和场景3的指导确定到根CA的整个链并相应地重新建立链并重新安装。

方案 5.无私钥

<#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.
```

解决方案：如果证书签名请求(CSR)是在外部生成的，并且需要在文件中链接，则WLC期望在文件中包含私钥。如果CSR是在WLC中生成的，请确保在安装之前不会重新加载WLC，否则会丢失私钥。

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。