WLC에서 인증서 설치 문제 해결

목차

소개

이 문서에서는 WLC(Wireless LAN Controller)에서 서드파티 인증서를 사용할 때 발생하는 문제를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 무선 LAN 컨트롤러(WLC)
- PKI(Public Key Infrastructure)
- X.509 인증서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 3504 WLC(펌웨어 버전 8.10.105.0 포함)
- 명령줄 도구용 OpenSSL 1.0.2p
- Windows 10 시스템
- 3개의 인증서(리프, 중간, 루트)가 있는 사설 랩 CA(Certificate Authority)의 인증서 체인
- 파일 전송을 위한 TFTP(Trivial File Transfer Protocol) 서버

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

AireOS WLC에서 WebAuth 및 WebAdmin에 사용할 타사 인증서를 설치할 수 있습니다. 설치 시 WLC는 단일 PEM(Privacy Enhanced Mail) 형식의 파일이며 체인의 모든 인증서가 루트 CA 인증서 및 개인 키까지 연결되어 있습니다. 이 절차에 대한 자세한 내용은 서드파티 인증서에 대한 CSR 생성 및 WLC에 체인으로 연결된 인증서 다운로드에 설명되어 있습니다.

이 문서에서는 각 시나리오에 대한 디버그 예제 및 확인과 함께 가장 일반적인 설치 오류를 더 자세히 보여 줍니다. 이 문서 전체에서 사용되는 디버그 출력은 WLC에서 활성화된 디버그 전송 모든 활성화 및 디버그 pm pki 활성화로부터 가져옵니다. TFTP는 인증서 파일을 전송하는 데 사용되었습니다.

문제 해결

시나리오 1. 개인 키의 암호를 해독하기 위해 제공한 암호가 올바르지 않거나 제공된 암호가 없습니다.

<#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.
```

해결 방법: WLC에서 설치를 위해 암호를 해독할 수 있도록 올바른 암호가 제공되었는지 확인하십시오.

시나리오 2. 체인에 중간 CA 인증서 없음

<#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.
```

해결 방법: WLC 인증서에서 Issuer 및 X509v3 Authority Key Identifier 필드를 확인하여 인증서에 서명한 CA 인증서를 검증합니다. CA에서 중간 CA 인증서를 제공한 경우, 이 인증서를 사용하여 유효성을 검사할 수 있습니다. 그렇지 않으면 CA에 인증서를 요청합니다.

이 OpenSSL 명령을 사용하여 각 인증서에서 이러한 세부사항을 검증할 수 있습니다.

<#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

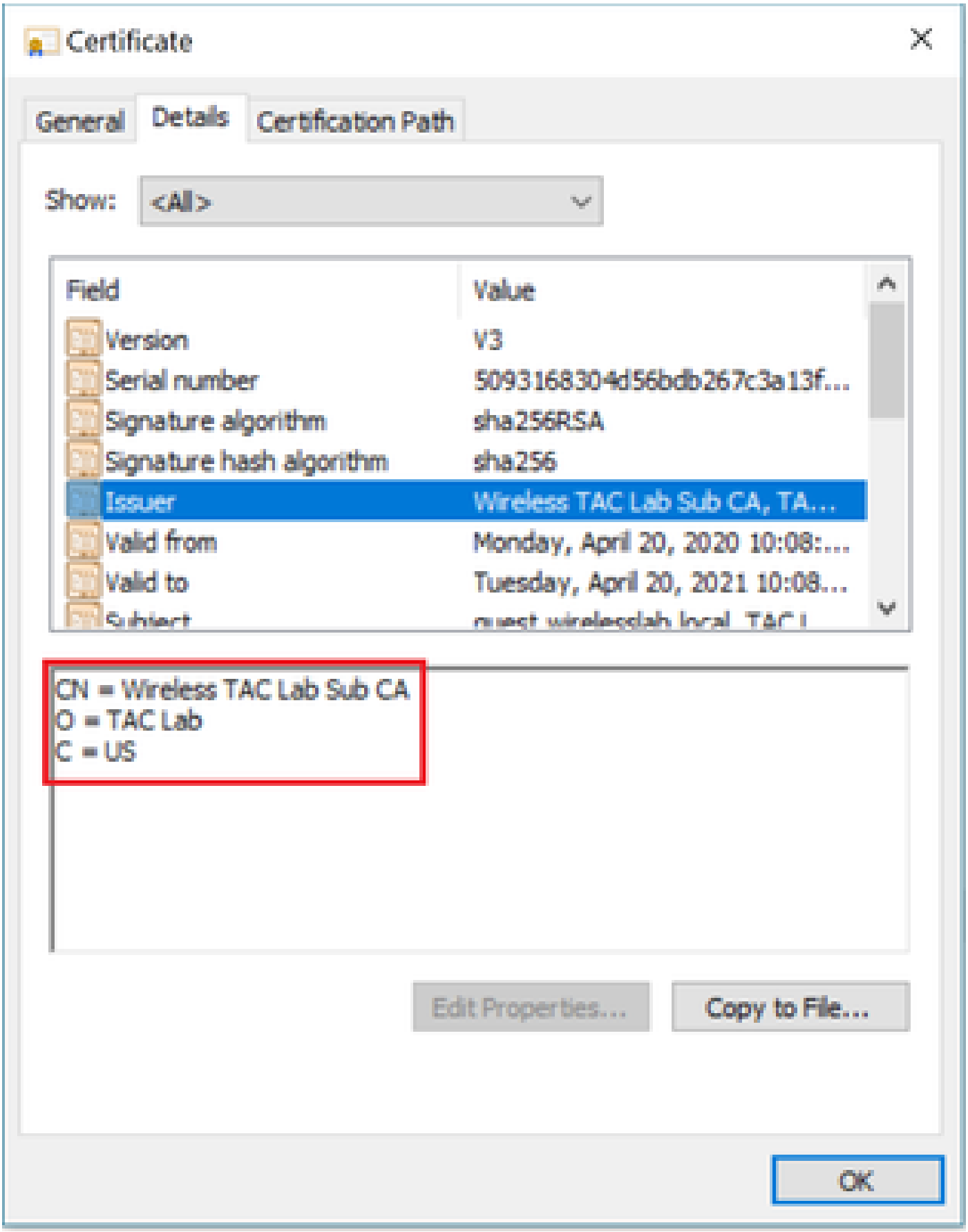
...

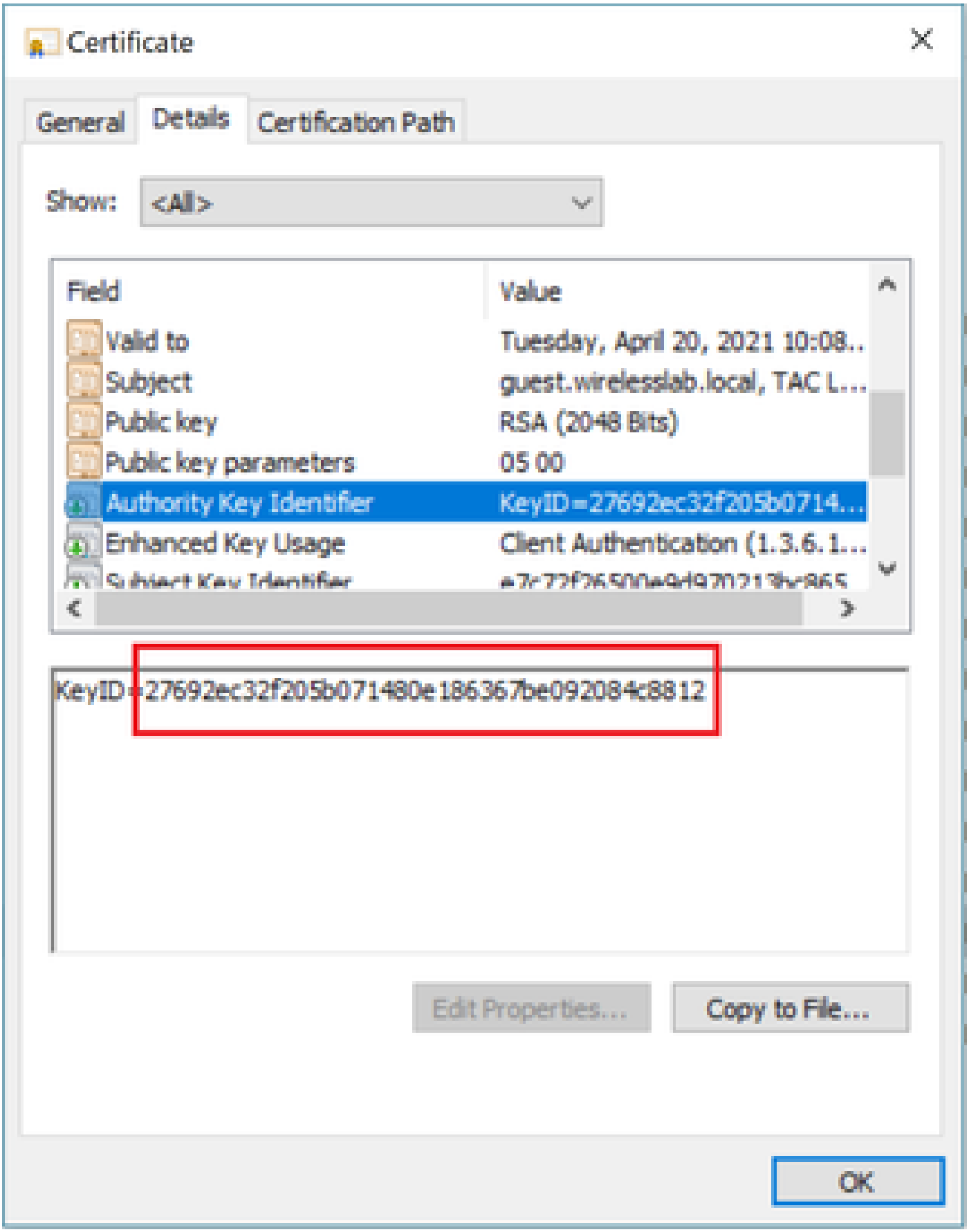
X509v3 Subject Key Identifier:

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

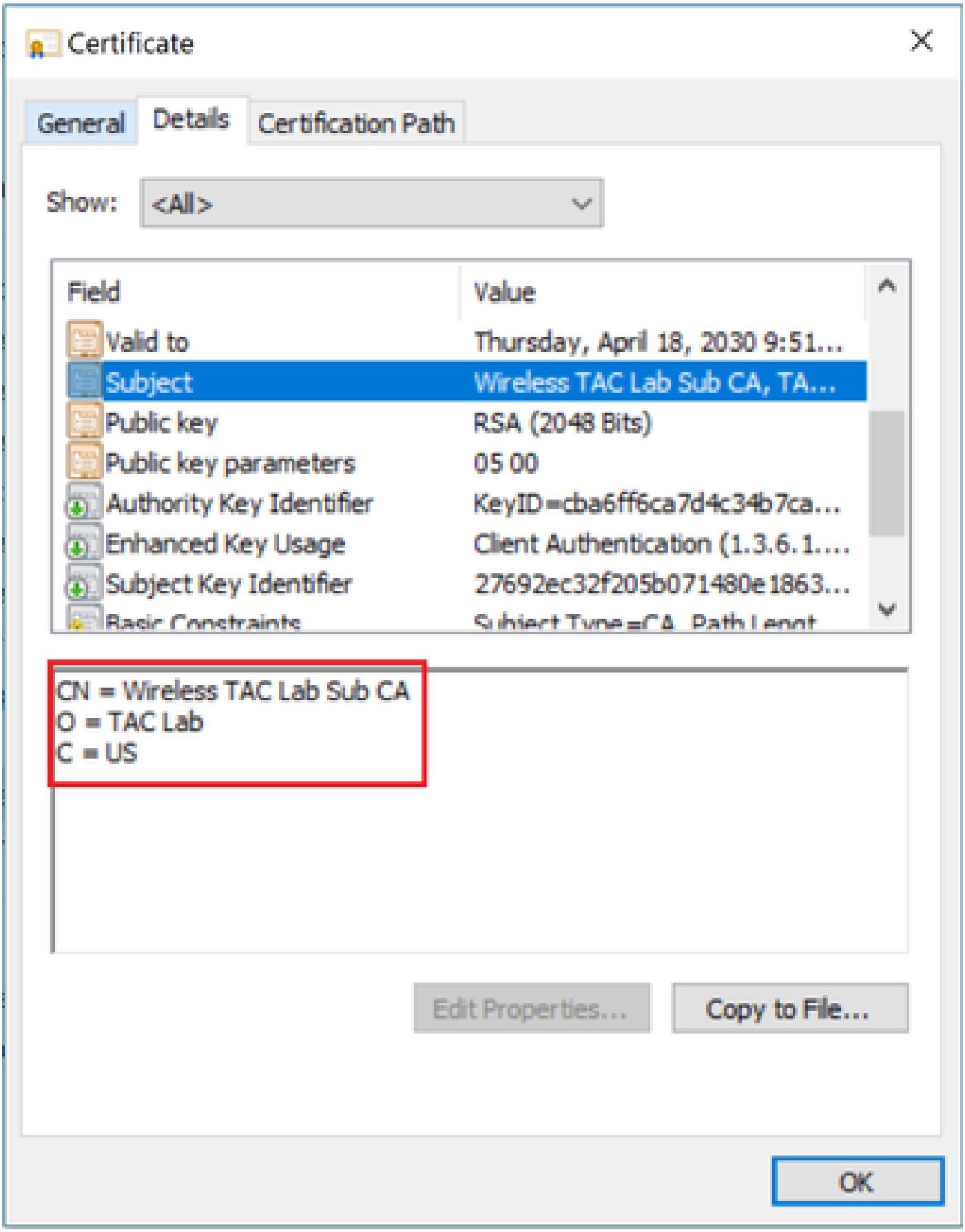
또는 Windows를 사용하는 경우 인증서에 .crt 확장명을 지정하고 두 번 클릭하여 이러한 세부 정보를 검증합니다.

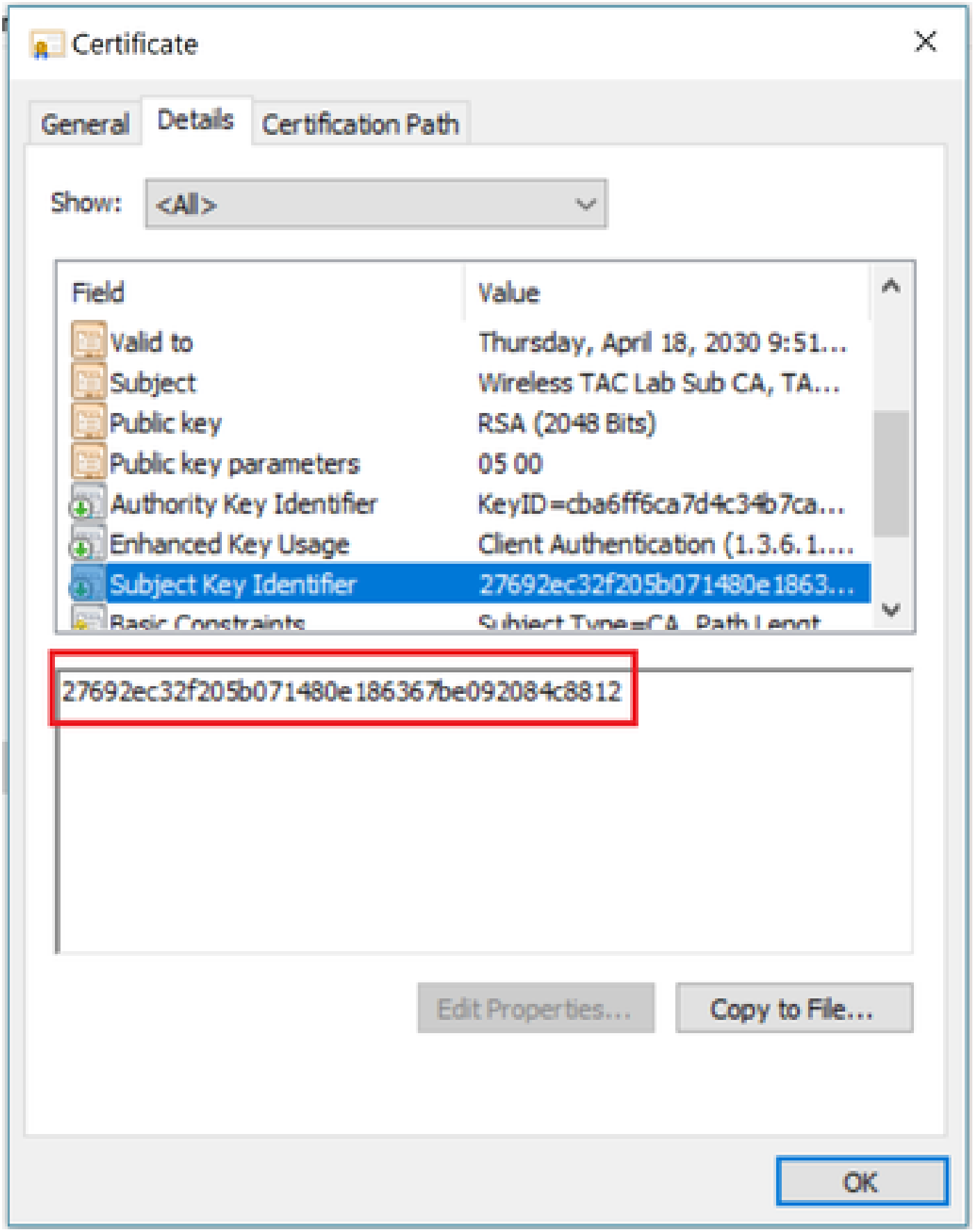
WLC 인증서:


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

중간 CA 인증서:


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



Intermediate CA 인증서가 식별되면 그에 따라 체인을 진행하고 다시 설치합니다.

시나리오 3. 체인에 루트 CA 인증서 없음

<#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
```

해결 방법: 이 시나리오는 시나리오 2와 비슷하지만, 발급자(루트 CA)를 검증할 때 중간 인증서에 대해 이 시나리오를 수행합니다. 중간 CA 인증서에서 Issuer 및 X509v3 Authority Key Identifier 필드를 확인하여 루트 CA를 검증할 때도 동일한 지침을 따를 수 있습니다.

이 OpenSSL 명령을 사용하여 각 인증서에서 이러한 세부사항을 검증할 수 있습니다.

<#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

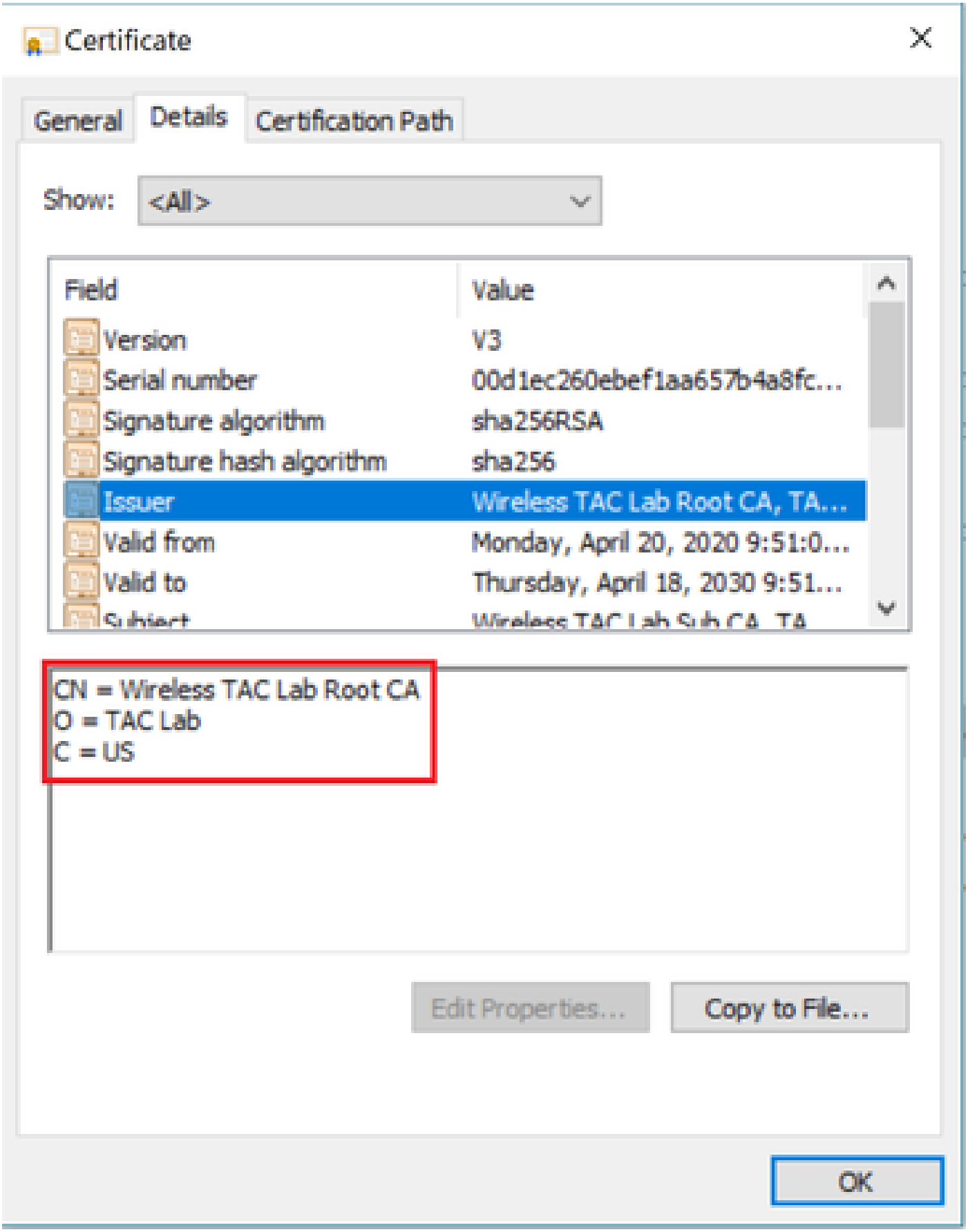
Subject: C=US, O=TAC Lab, CN=Wireless TAC Lab Root CA

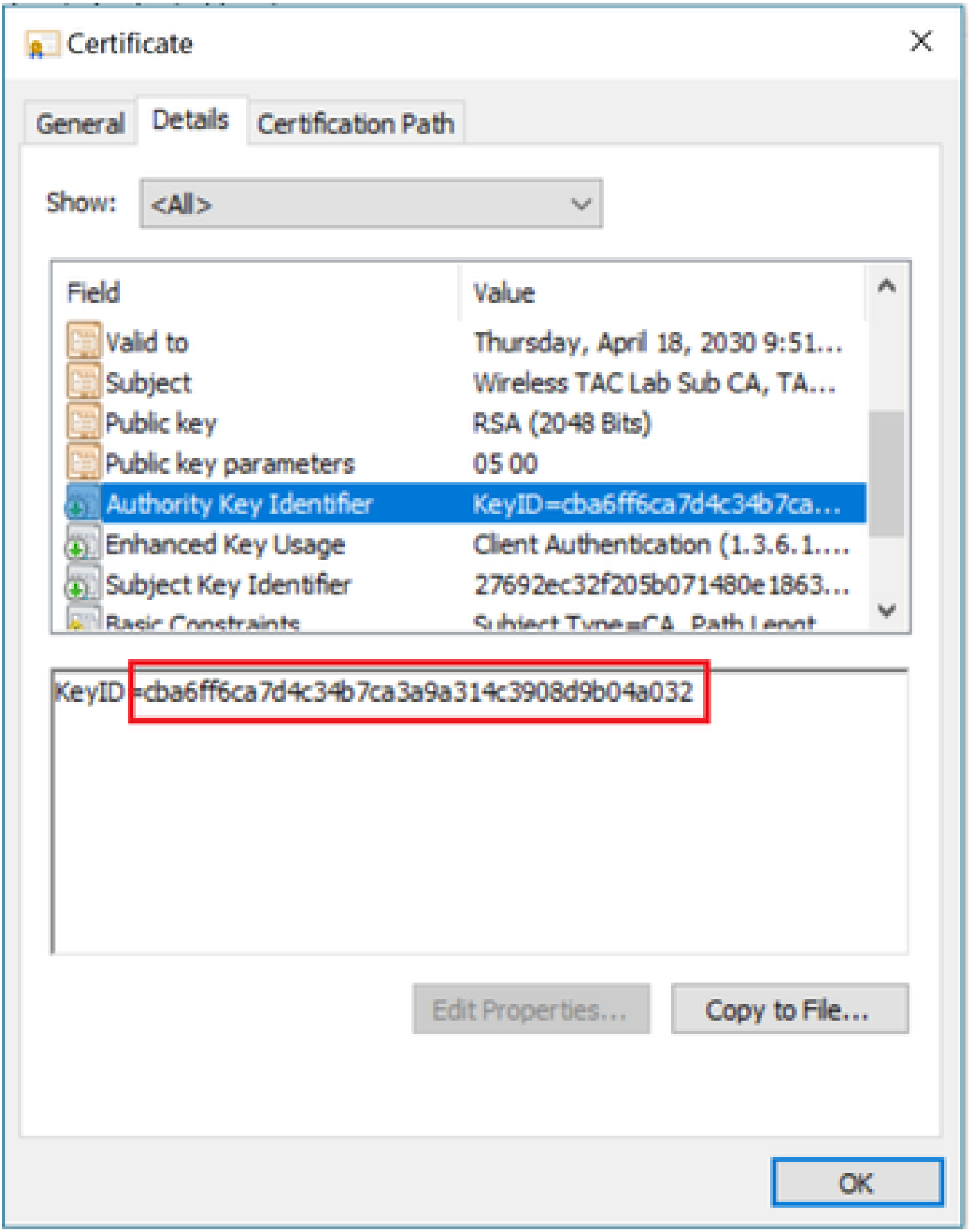
...

X509v3 Subject Key Identifier:

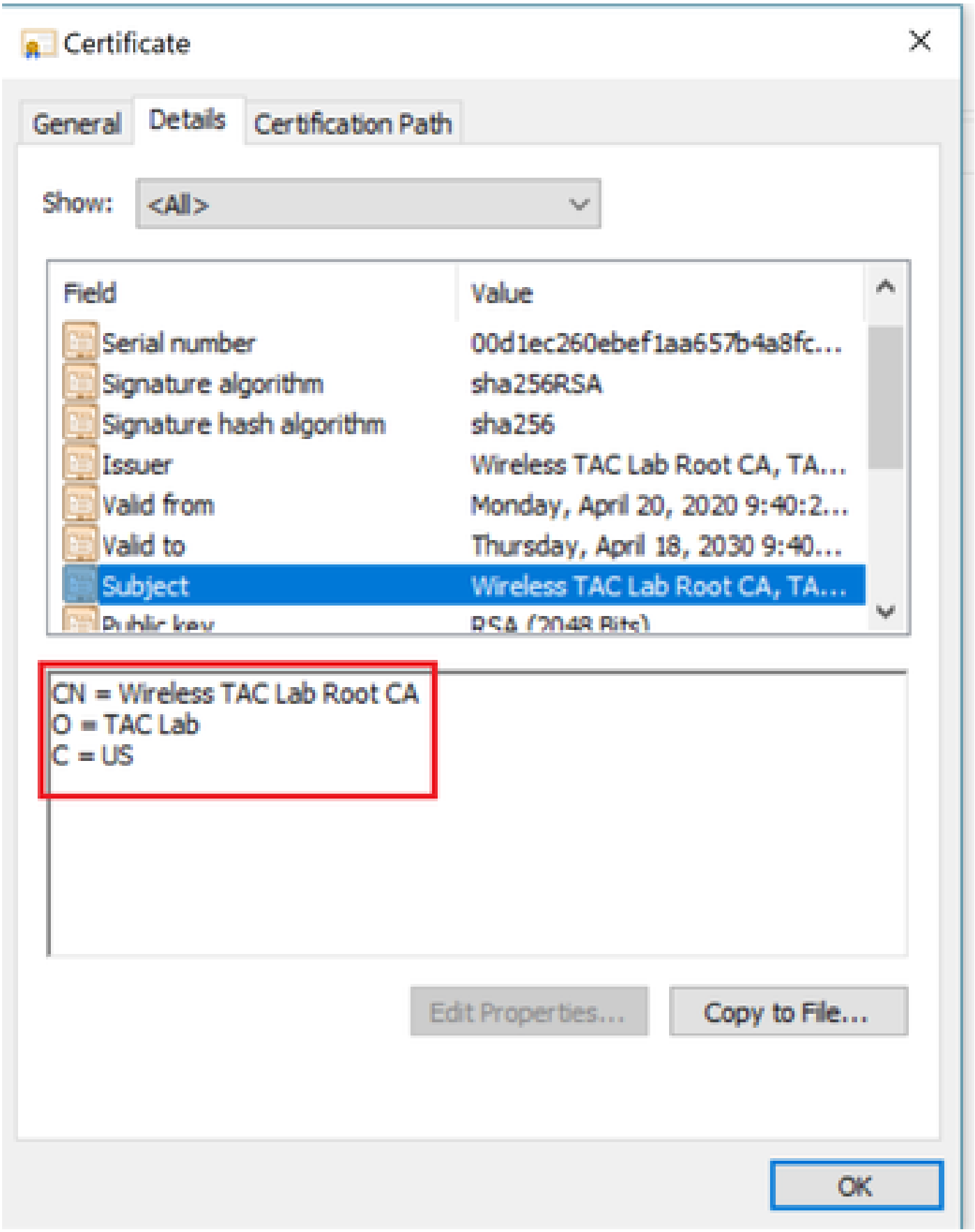
CB:A6:FF:6C:A7:D4:C3:4B:7C:A3:A9:A3:14:C3:90:8D:9B:04:A0:32

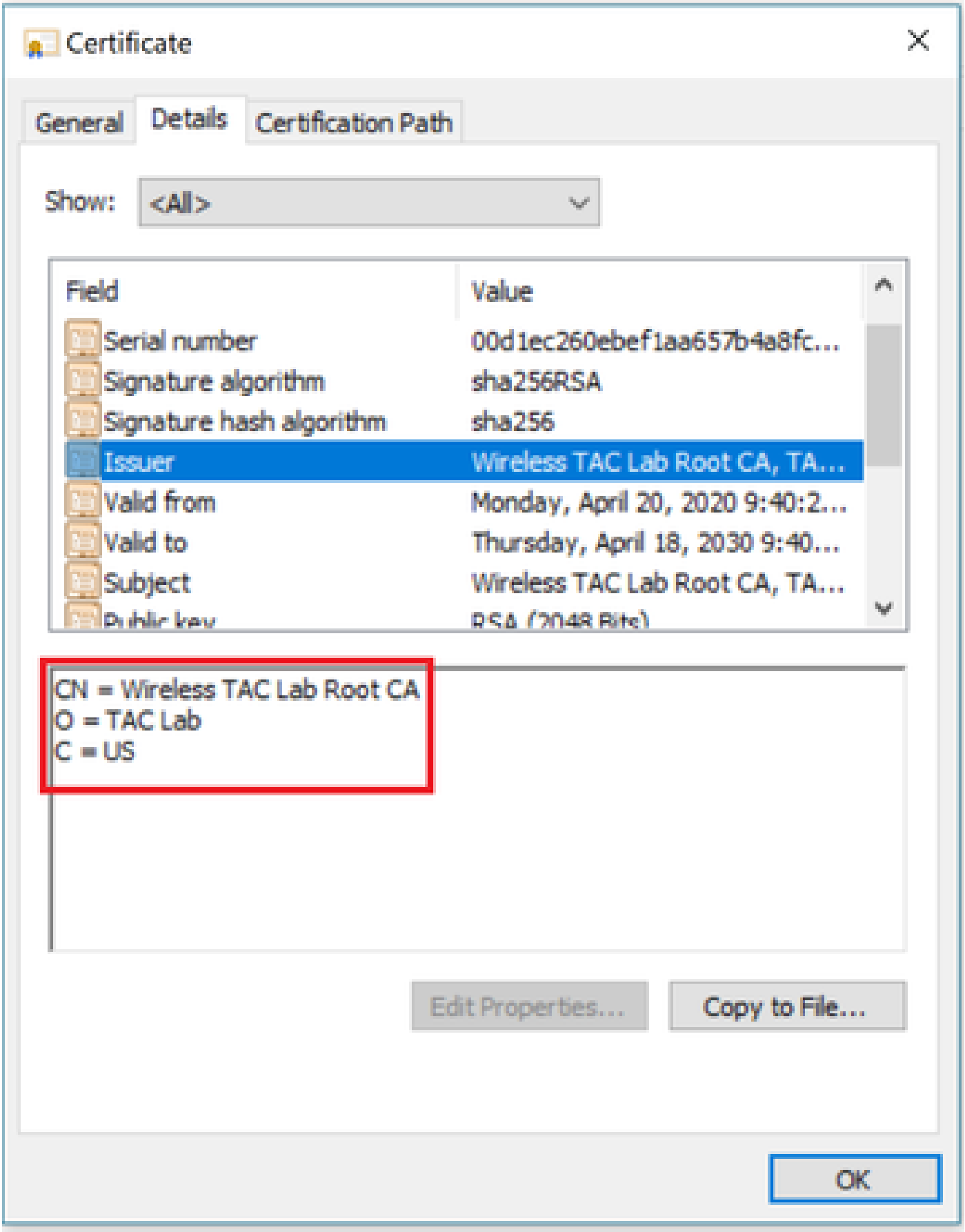
중간 CA 인증서

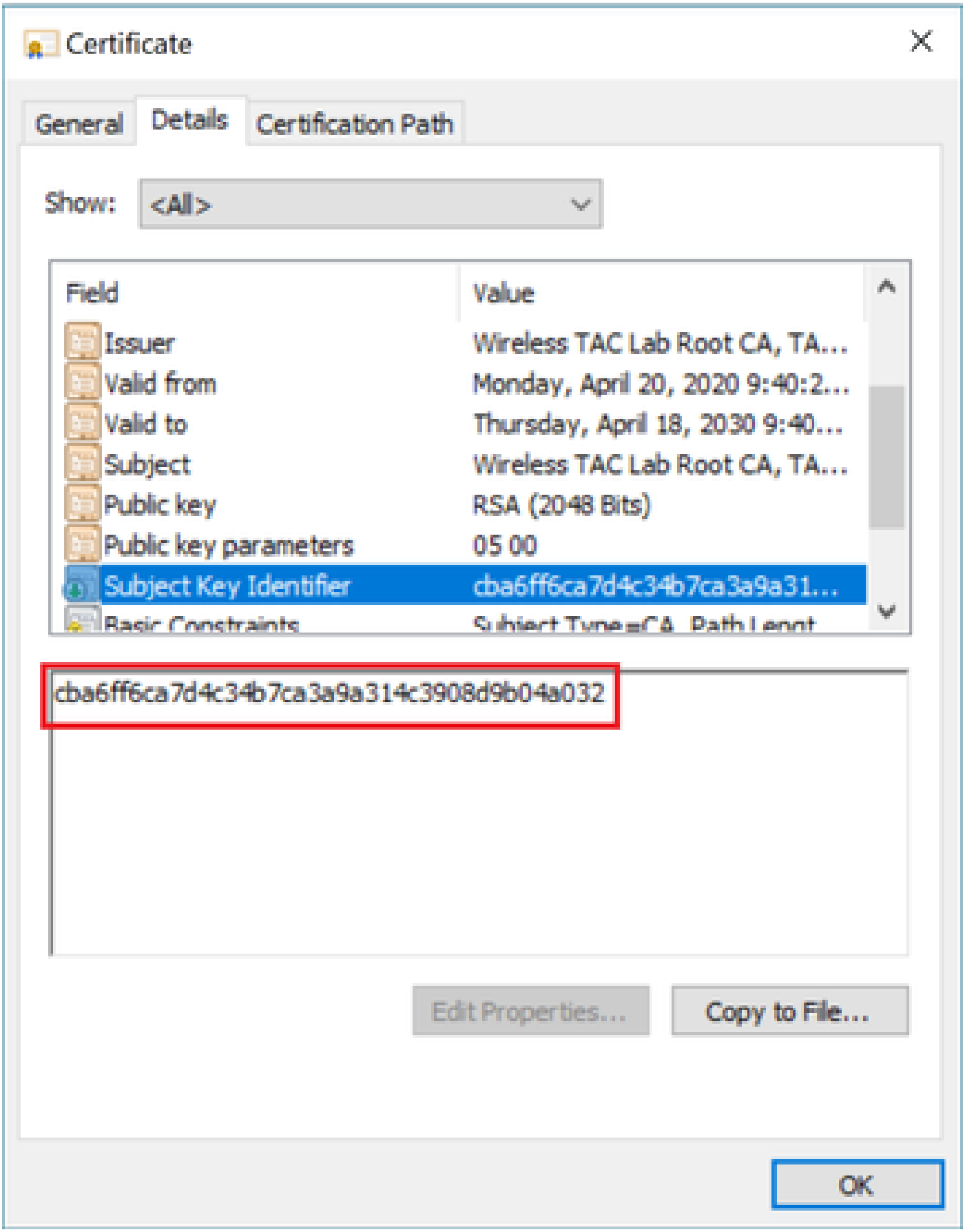

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
00d1ec260ebef1aa657b4a8fc...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
Wireless TAC Lab Root CA, TA...
Valid from
Monday, April 20, 2020 9:51:0...
Valid to
Thursday, April 18, 2030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

루트 CA 인증서:


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



루트 CA 인증서가 식별되면(발급자와 주체가 동일함) 그에 따라 체인을 계속 진행하고 다시 설치합니다.

참고: 이 문서에서는 가장 일반적인 시나리오인 3개의 인증서 체인(leaf, Intermediate CA, Root CA)을 사용합니다. 2개의 중간 CA 인증서가 관련된 시나리오가 있을 수 있습니다. 루트 CA 인증서를 찾을 때까지 이 시나리오의 동일한 지침을 사용할 수 있습니다.

시나리오 4. 체인에 CA 인증서 없음

<#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 le
*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.
```

해결 방법: 파일에 WLC 인증서 이외의 다른 인증서가 없으면 0개 깊이에서 확인에서 검증이 실패합니다. 텍스트 편집기에서 파일을 열어 유효성을 검사할 수 있습니다. 시나리오 2와 3의 지침을 따라 루트 CA까지 체인을 식별하고 그에 따라 다시 체인을 구성한 다음 다시 설치할 수 있습니다.

시나리오 5. 개인 키 없음

<#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 le
*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.
```

해결 방법: CSR(Certificate Signing Request)이 외부에서 생성되어 파일에서 체인으로 연결해야 하는 경우 WLC는 개인 키가 파일에 포함될 것으로 기대합니다. CSR이 WLC에서 생성된 경우, 설치 전에 WLC가 다시 로드되지 않았는지 확인합니다. 그렇지 않으면 개인 키가 손실됩니다.

관련 정보

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.