Risoluzione dei problemi di installazione dei certificati sul WLC

Sommario

Introduzione

Questo documento descrive i problemi che si possono verificare quando si usa un certificato di terze parti sul controller WLC.

Contributo di Joel Torres, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Controller LAN wireless (WLC)
- PKI (Public Key Infrastructure)
- Certificati X.509

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 3504 WLC con firmware 8.10.105.0
- OpenSSL 1.0.2p per lo strumento da riga di comando
- computer Windows 10
- Catena di certificati da autorità di certificazione (CA) lab privata con tre certificati (foglia, intermedia, radice)

- Server TFTP (Trivial File Transfer Protocol) per il trasferimento di file.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, verificare di aver compreso l'impatto potenziale di qualsiasi passaggio.

Premesse

Sul WLC di AireOS, è possibile installare certificati di terze parti da utilizzare per WebAuth e WebAdmin. Al momento dell'installazione, il WLC prevede un singolo file in formato PEM (Privacy Enhanced Mail) con tutti i certificati della catena fino al certificato della CA radice e alla chiave privata. I dettagli relativi a questa procedura sono documentati in questo documento:

In questo documento vengono illustrati in dettaglio gli errori di installazione più comuni con esempi di debug e risoluzione per ogni scenario. Gli output di debug usati in questo documento provengono da **debug transfer all enable** e **debug pm pki enable** abilitato sul WLC. TFTP è stato utilizzato per trasferire il file dei certificati.

Risoluzione dei problemi

Scenario 1. La password fornita per decrittografare la chiave privata non è corretta oppure non è stata fornita alcuna password

```
*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 length instead
*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
(verifyChain: TRUE)
*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.
```

Soluzione: Accertarsi di aver fornito la password corretta in modo che il WLC possa decodificarla per l'installazione.

Scenario 2. Nessun certificato CA intermedio nella catena

```
*TransferTask: Apr 21 04:34:43.319: Add ID Cert: Adding certificate & private key using password
Cisco123
```

```
*TransferTask: Apr 21 04:34:43.319: Add Cert to ID Table: Adding certificate (name:
bsnSslWebauthCert) to ID table using password Cisco123
*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 length instead
*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 certificate
*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
(verifyChain: TRUE)
*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.
```

Soluzione: Convalidare i campi **Issuer** e **X509v3 Authority Key Identifier** dal certificato WLC per convalidare il certificato CA che lo ha firmato. Se il certificato CA intermedio è stato fornito dalla CA, può essere utilizzato per la convalida. In caso contrario, richiedere il certificato alla CA.

Questo comando OpenSSL può essere utilizzato per convalidare i seguenti dettagli su ciascun certificato:

```
> 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
```

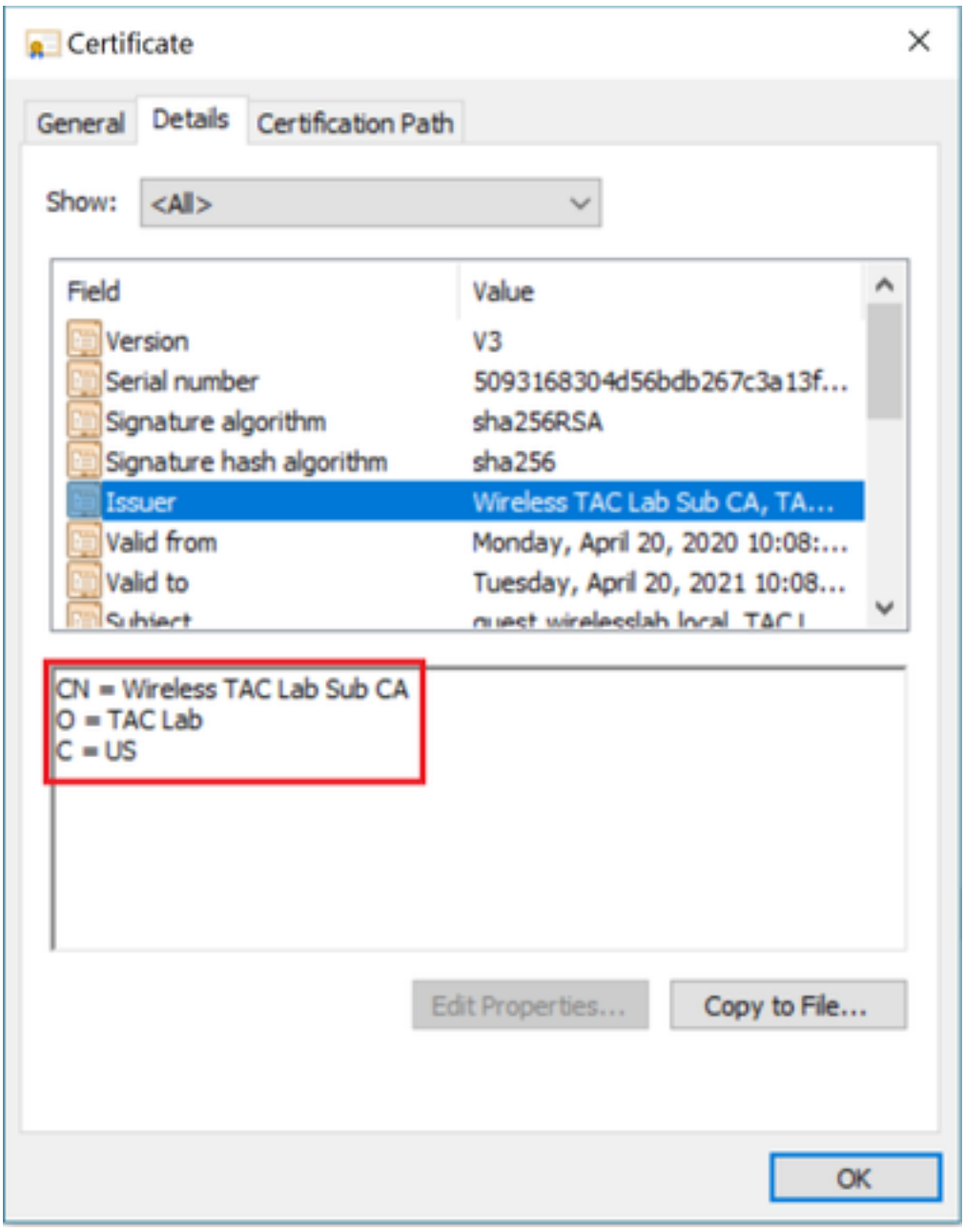
```
> openssl x509 -in int-ca.crt -text -noout

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
```

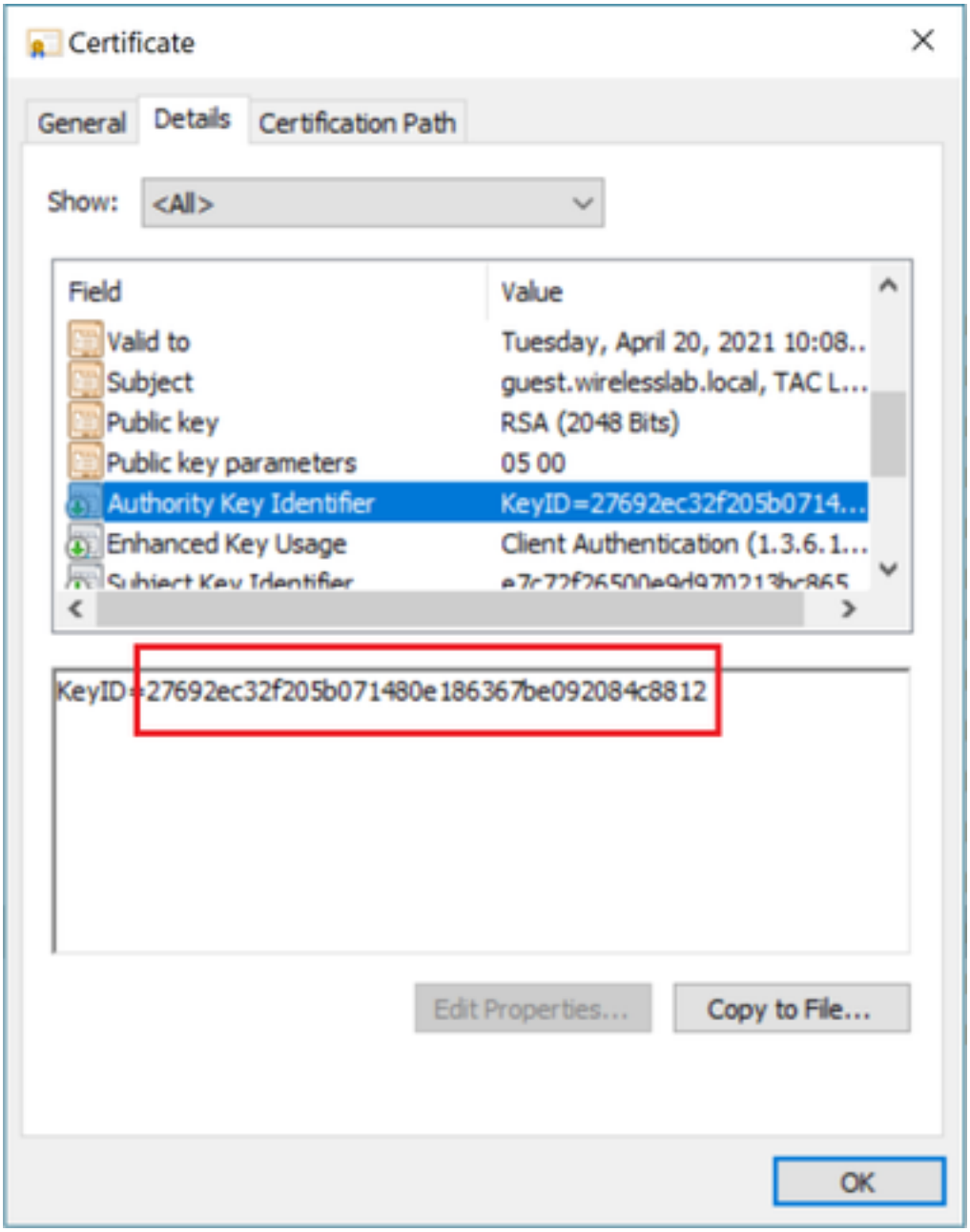
...

X509v3 Subject Key Identifier:
27:69:2E:C3:2F:20:5B:07:14:80:E1:86:36:7B:E0:92:08:4C:88:12

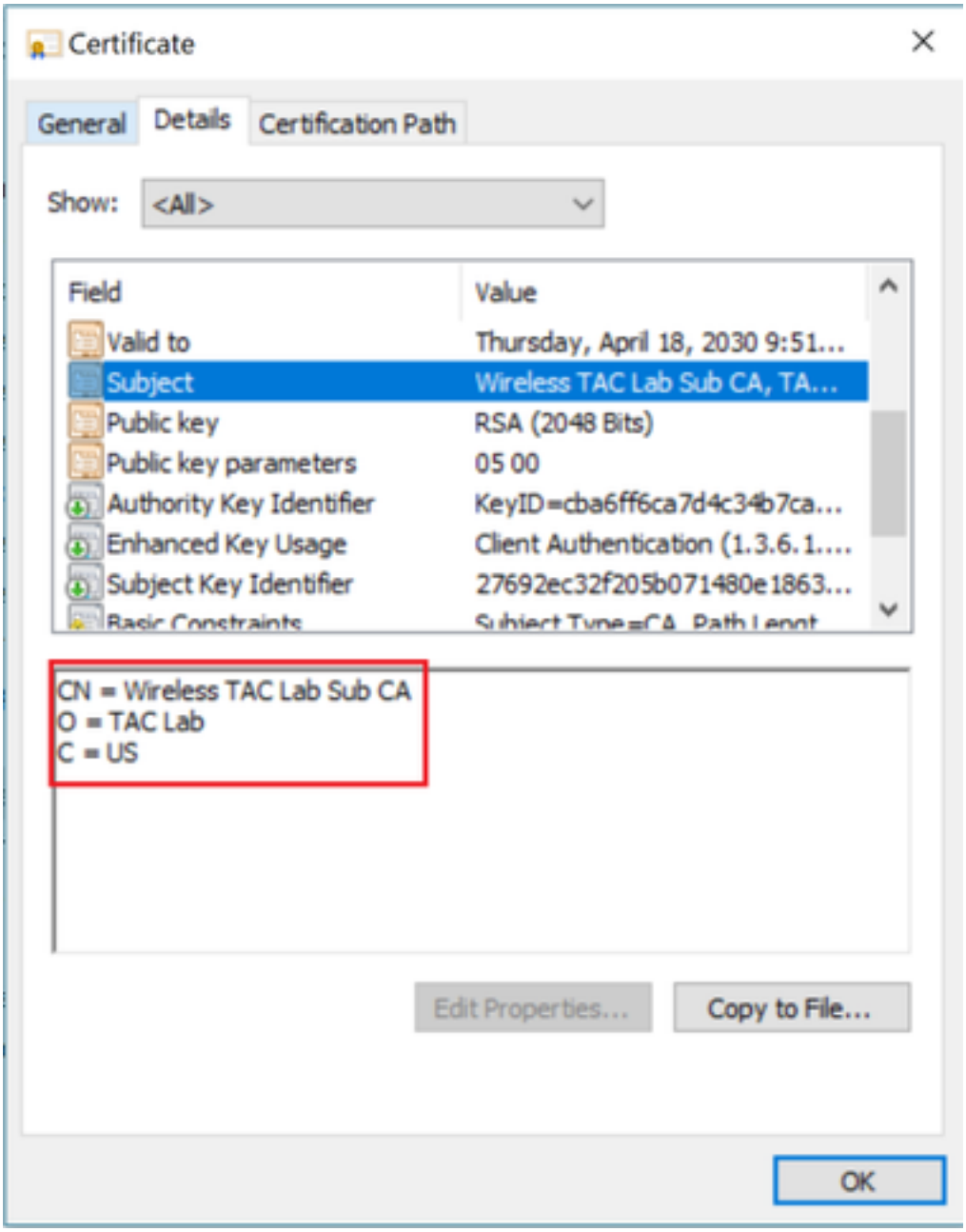
In alternativa, se si utilizza Windows, assegnare al certificato l'estensione **.crt** e fare doppio clic per convalidare i dettagli seguenti:

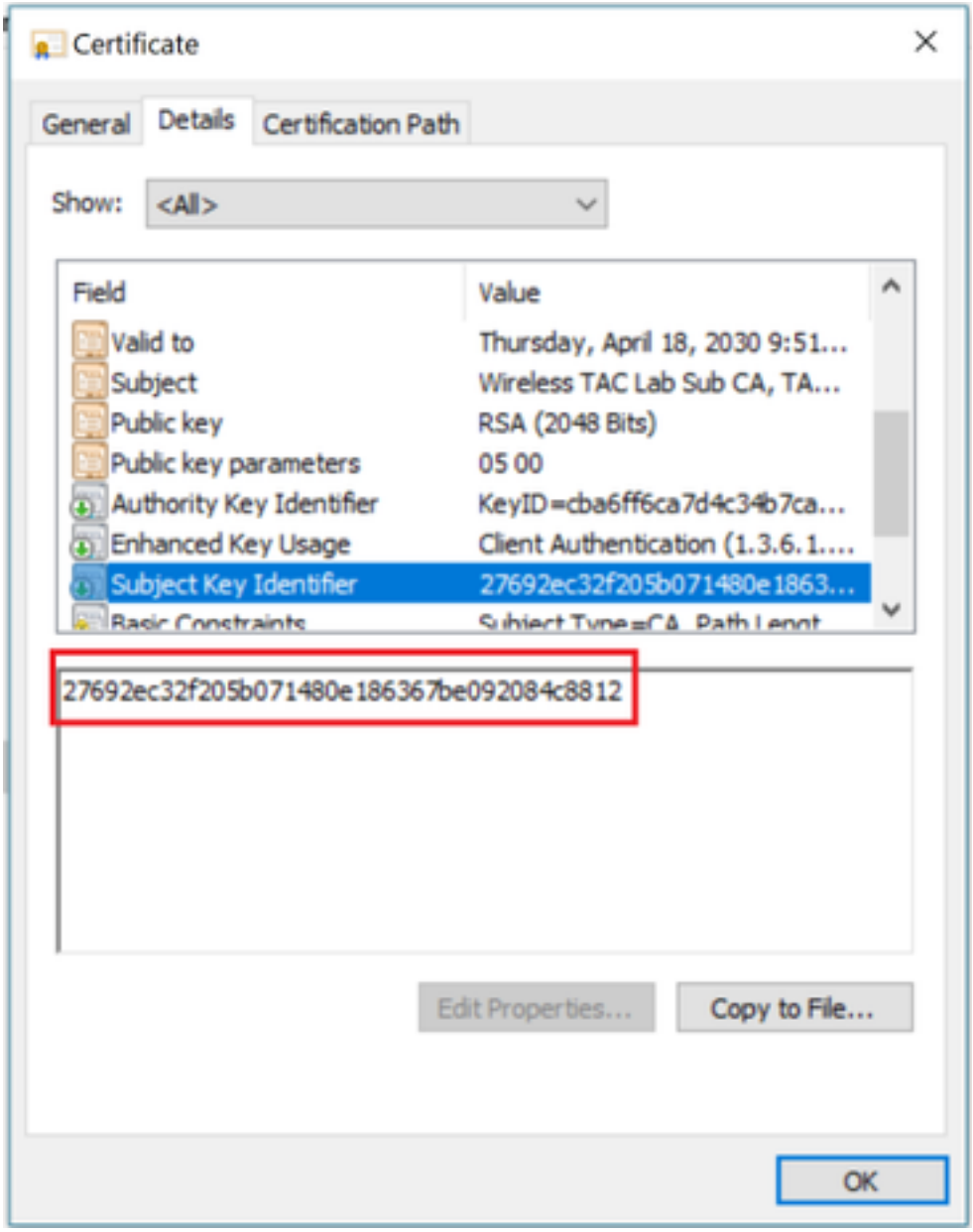
Certificato WLC:





Certificato CA intermedio:


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



Una volta identificato il certificato CA intermedio, procedere con la catena e reinstallare.

Scenario 3. Nessun certificato CA radice nella catena

```
*TransferTask: Apr 21 04:28:09.643: Add ID Cert: Adding certificate & private key using password
Cisco123
*TransferTask: Apr 21 04:28:09.643: Add Cert to ID Table: Adding certificate (name:
bsnSslWebauthCert) to ID table using password Cisco123
*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 length instead
*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
```

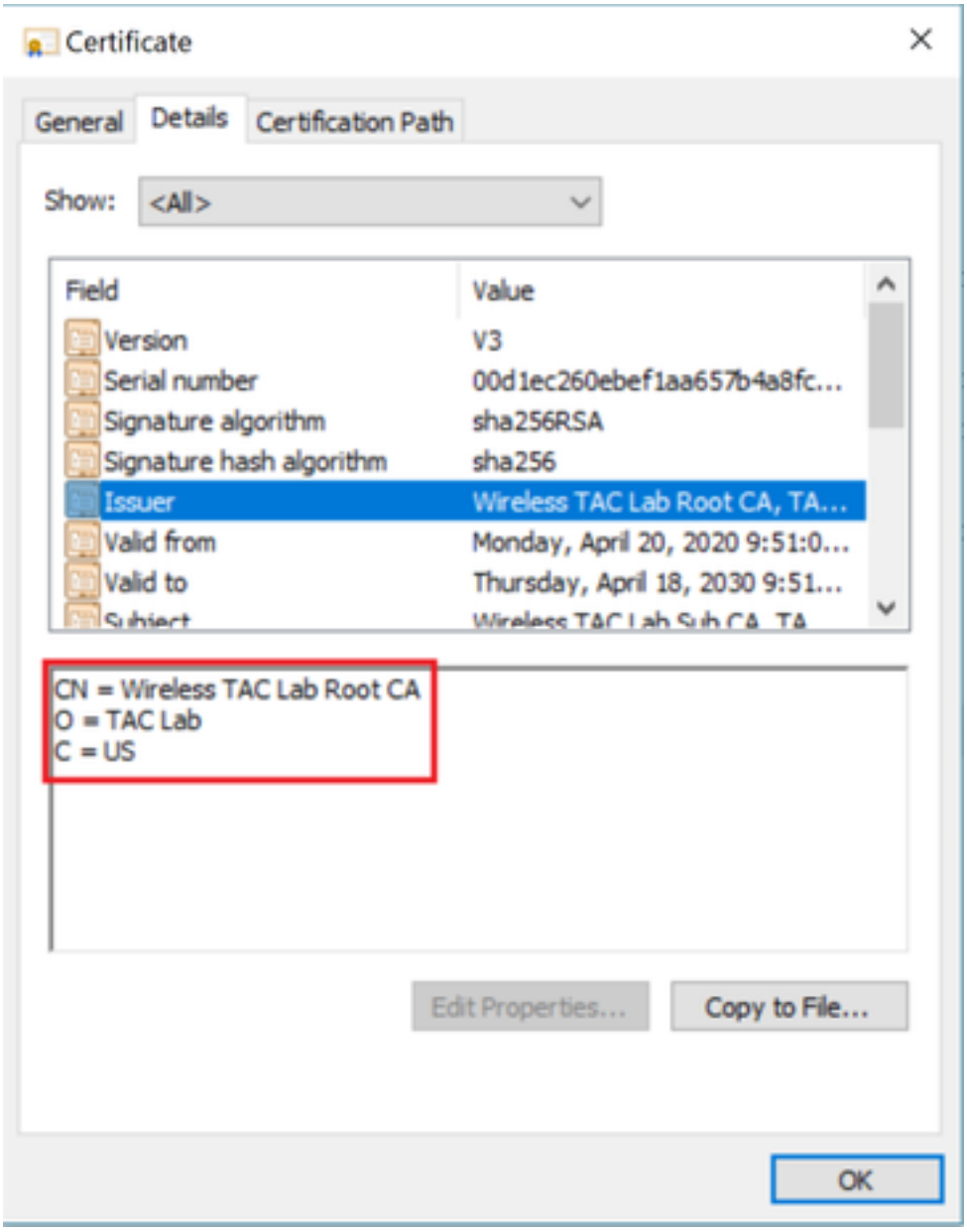
```
*TransferTask: Apr 21 04:28:09.646: Add ID Cert: Error decoding / adding cert to ID cert table
(verifyChain: TRUE)
```

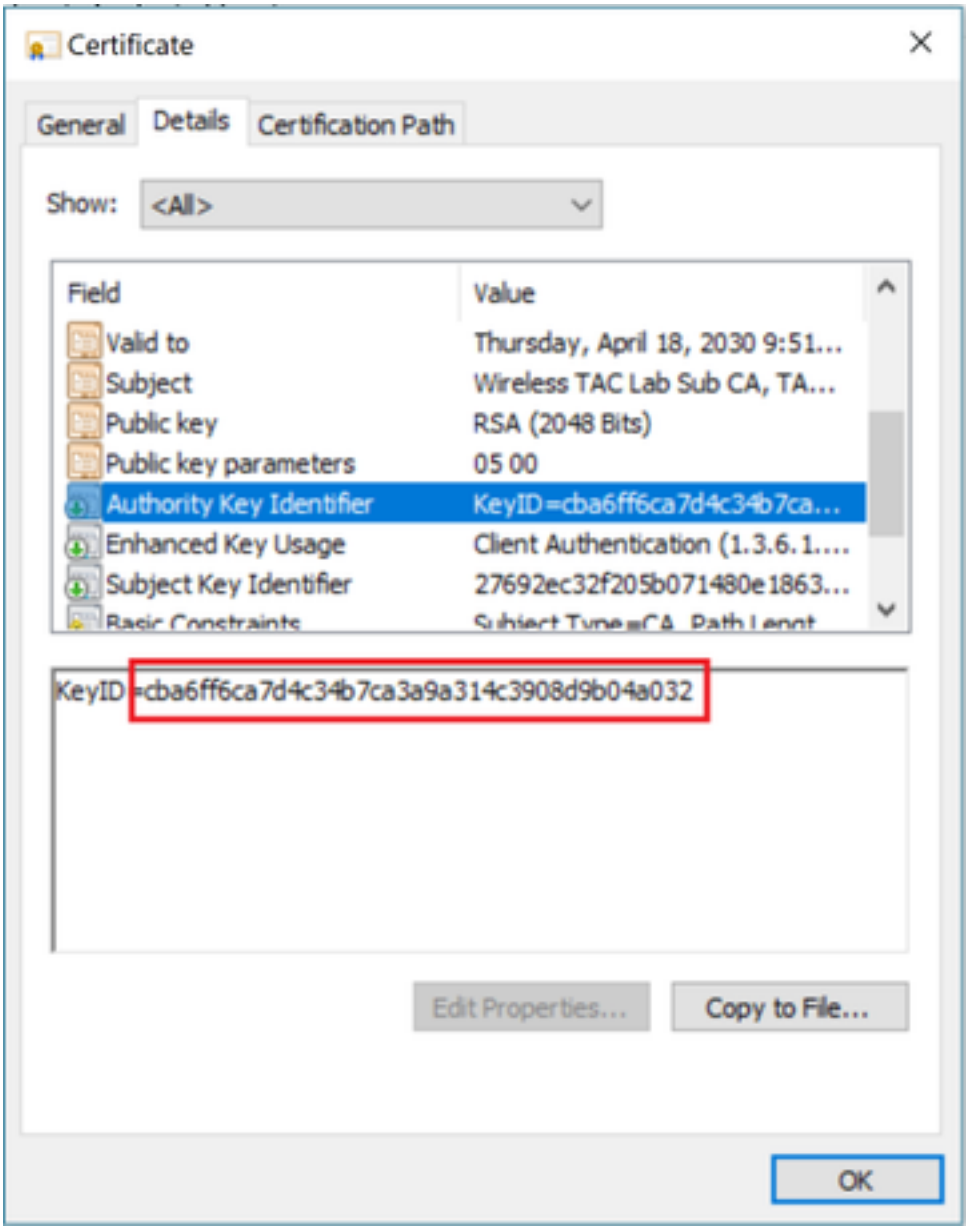
Soluzione: questo scenario è simile allo scenario 2, ma questa volta rispetto al certificato intermedio durante la convalida dell'autorità emittente (CA radice). Le stesse istruzioni possono essere seguite con la verifica dei campi **Issuer** e **X509v3 Authority Key Identifier** sul certificato CA intermedio per convalidare la CA radice.

Questo comando OpenSSL può essere utilizzato per convalidare i seguenti dettagli su ciascun certificato:

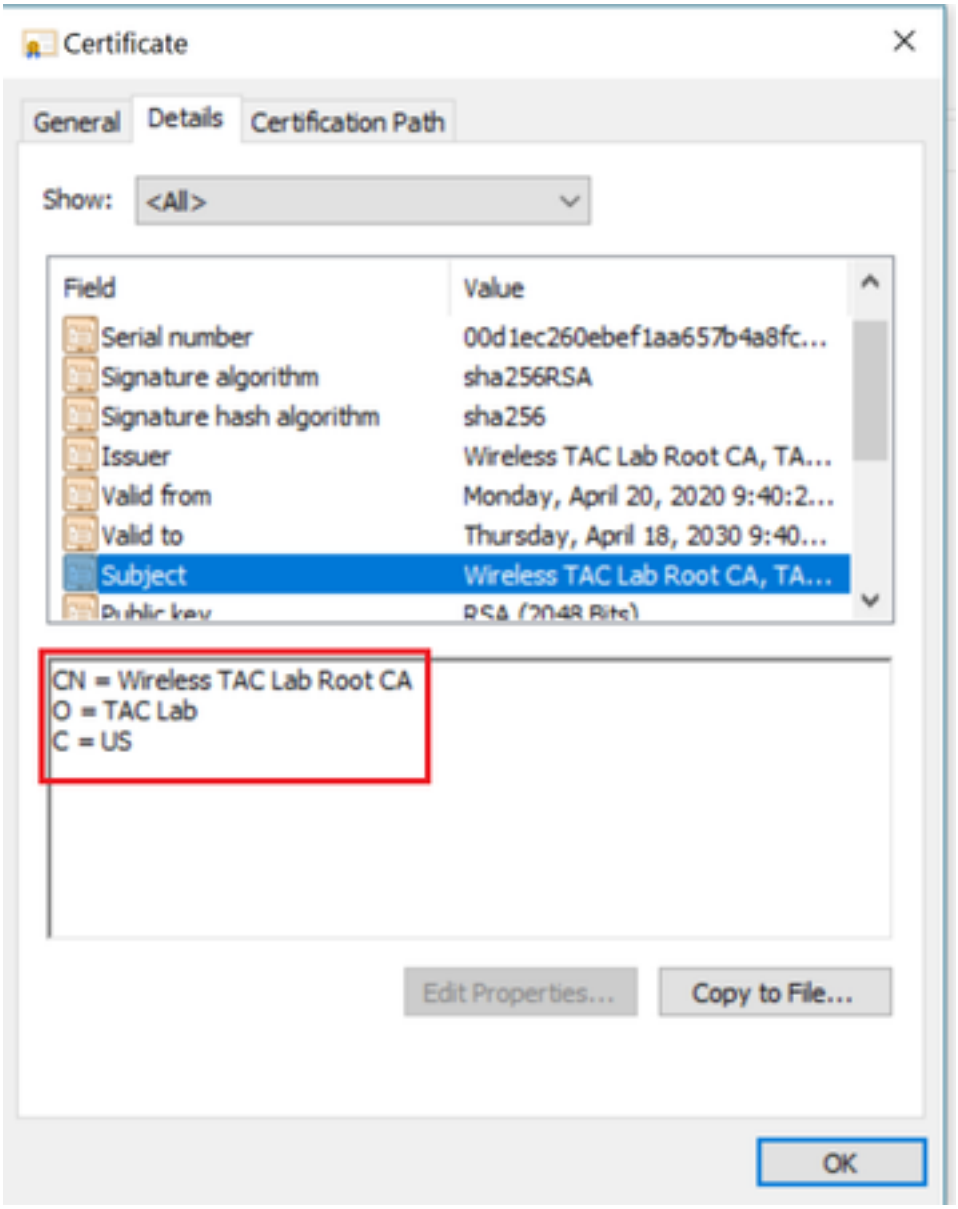
```
> openssl x509 -in int-ca.crt -text -noout

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

> 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
```

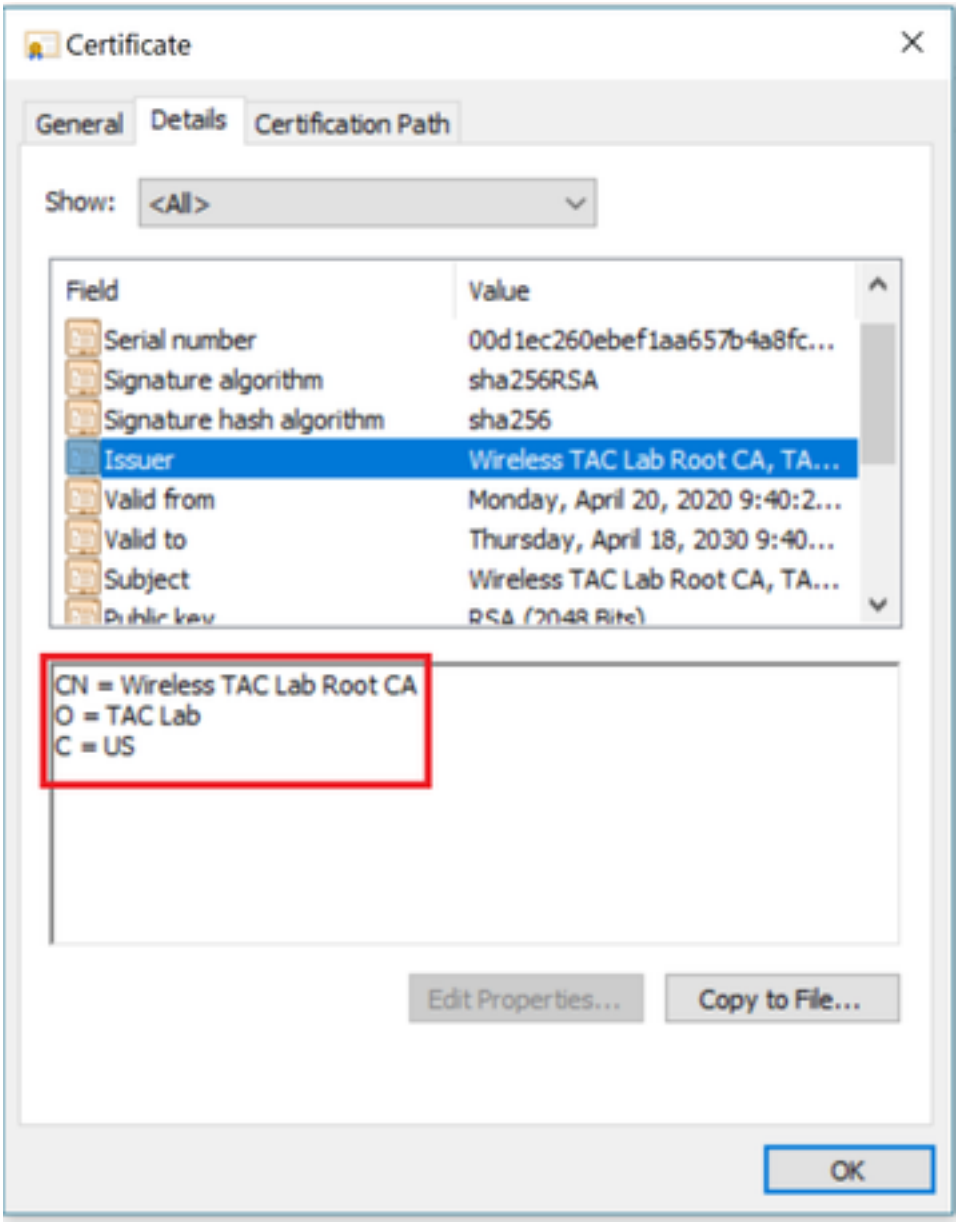
Certificato CA intermedio

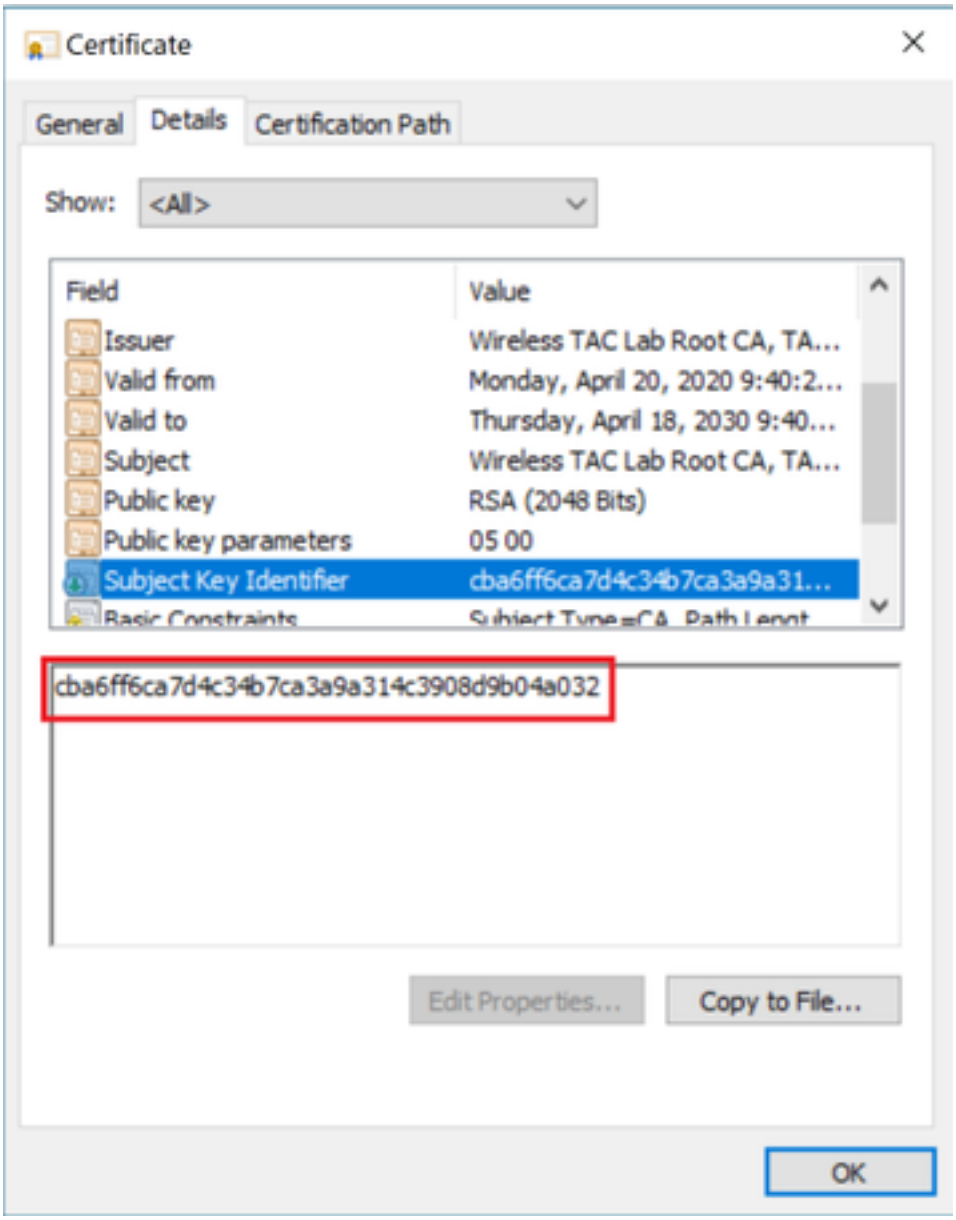

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
00d1ec260ebef1aa657b4a8fc...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
Wireless TAC Lab Root CA, TA...
Valid from
Monday, April 20, 2020 9:51:0...
Valid to
Thursday, April 18, 2030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



Certificato CA radice


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



Una volta identificato il certificato CA radice (emittente e soggetto sono gli stessi), procedere con la catena e reinstallare.

> **Nota:** Questo documento utilizza tre catene di certificati (foglia, CA intermedia, CA radice), che è lo scenario più comune. In alcuni casi possono essere interessati 2 certificati CA intermedi. È possibile utilizzare le stesse linee guida di questo scenario finché non viene trovato il certificato CA radice.

Scenario 4. Nessun certificato CA nella catena

```
*TransferTask: Apr 21 04:56:50.272: Add ID Cert: Adding certificate & private key using password
Cisco123
*TransferTask: Apr 21 04:56:50.272: Add Cert to ID Table: Adding certificate (name:
bsnSslWebauthCert) to ID table using password Cisco123
*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 length instead
*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 certificate
*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.
```

Soluzione: Se nel file non sono presenti altri certificati oltre al certificato WLC, la convalida non riesce alla verifica con una profondità pari a 0. Il file può essere aperto in un editor di testo per essere convalidato. È possibile seguire le linee guida dello scenario 2 e 3 per identificare la catena fino alla CA radice e ripetere il concatenamento e reinstallare.

Scenario 5. Nessuna chiave privata

```
*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) to ID table using password
*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 length instead
*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
password
*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
(verifyChain: TRUE)
*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.
```

Soluzione: Il WLC prevede che la chiave privata venga inclusa nel file se la richiesta di firma del certificato (CSR) è stata generata esternamente e deve essere concatenata nel file. Se la CSR è stata generata nel WLC, verificare che il WLC non venga ricaricato prima dell'installazione, in caso contrario la chiave privata viene persa.