ASA Smart Licensing-Fehler aufgrund von Zertifikatproblemen ermitteln

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie ASA Smart Licensing-Fehler ermitteln, die auf einen Handshake-Fehler des Zertifikats zurückzuführen sind.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In diesem Dokument wird beschrieben, wie Sie eine im März 2016 und Oktober 2018 eingetretene Änderung beheben können, bei der Webserver, die tools.cisco.com hosten, zu einem anderen Stammzertifikat der Zertifizierungsstelle (Certificate Authority, CA) migriert wurden. Nach dieser Migration stellen einige ASA-Geräte (Adaptive Security Appliance) keine Verbindung mit dem Smart Software Licensing Portal (das unter tools.cisco.com gehostet wird) her, wenn sie ein ID-Token registrieren oder versuchen, aktuelle Autorisierungen zu erneuern. Es wurde festgestellt, dass es sich um ein

zertifikatbezogenes Problem handelt. Das neue Zertifikat, das der ASA vorgelegt wird, wird von einer anderen zwischengeschalteten Zertifizierungsstelle signiert, als von der ASA erwartet und bereits vorinstalliert wurde.

Problem

Wenn versucht wird, eine ASAv im Smart Software Licensing-Portal zu registrieren, schlägt die Registrierung mit einem Verbindungs- oder Kommunikationsfehler fehl. Die Befehle **show license registration** und **call-home test profile license** zeigen diese Ausgaben an.

<#root>

ASAv#

show license registration

```
        Registration Status: Retry In Progress.
        Registration Start Time: Mar 22 13:25:46 2016 UTC
        Registration Status: Retry In Progress.
        Registration Start Time: Mar 22 13:25:46 2016 UTC
        Last Retry Start Time: Mar 22 13:26:32 2016 UTC.
        Next Scheduled Retry Time: Mar 22 13:45:31 2016 UTC.
        Number of Retries: 1.
        Last License Server response time: Mar 22 13:26:32 2016 UTC.
        Last License Server response message:
```

Communication message send response error

<#root>

ASAv#

call-home test profile License

```
INFO: Sending test message to DDCEService
ERROR: Failed:
```

CONNECT_FAILED(35)

Die ASAv kann jedoch tools.cisco.com auflösen und über den TCP-Port 443 eine Verbindung mit einem TCP-Ping herstellen.

Syslogs und Debug-Ausgabe

Die Syslog-Ausgabe auf der ASAv nach einem versuchten Registrierungsprozess kann Folgendes anzeigen:

<#root>

```
%ASA-3-717009: Certificate validation failed. No suitable trustpoints found to validate
 certificate serial number: 250CE8E030612E9F2B89F7058FD, subject name:
 cn=VeriSign Class 3 Public Primary Certification Authority - G5,ou=(c) 2006 VeriSign\, Inc.
 - For authorized use only,ou=VeriSign Trust Network,o=VeriSign\, Inc.,c=US, issuer name:
 ou=Class 3 Public Primary Certification Authority,o=VeriSign\, Inc.,c=US .
%ASA-3-717009: Certificate validation failed. No suitable trustpoints found to validate
```

```
 certificate serial number: 513FB9743870B73440418699FF, subject name:

 cn=Symantec Class 3 Secure Server CA - G4

,ou=Symantec Trust Network,o=Symantec
 Corporation,c=US, issuer name: cn=VeriSign Class 3 Public Primary Certification Authority
 - G5,ou=(c) 2006 VeriSign\, Inc. - For authorized use only,ou=VeriSign Trust Network,
 o=VeriSign\, Inc.,c=US .
```

Weitere Informationen erhalten Sie, wenn Sie diese Debug-Befehle ausführen, während Sie versuchen, eine weitere Registrierung durchzuführen. Es treten Fehler in Secure Socket Layer auf.

```
debug license 255
debug license agent all
debug call-home all
debug ssl 255
```

Diese Meldung wird als Teil der Ausgabe betrachtet:

```
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify
 failed@s3_clnt.c:1492
```

In der ASAv-Standardkonfiguration gibt es einen Vertrauenspunkt mit der Bezeichnung _SmartCallHome_ServerCA, für den ein Zertifikat geladen und mit dem Betreffnamen "cn=Verisign Class 3 Secure Server CA - G3" ausgestellt wurde.

<#root>

```
ASAv#

show crypto ca certificate

CA Certificate
  Status: Available
  Certificate Serial Number: 6ecc7aa5a7032009b8cebc2d491
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
    cn=VeriSign Class 3 Public Primary Certification Authority - G5
    ou=(c) 2006 VeriSign\, Inc. - For authorized use only
    ou=VeriSign Trust Network
    o=VeriSign\, Inc.
    c=US
  Subject Name:

    cn=VeriSign Class 3 Secure Server CA - G3

    ou=Terms of use at https:// verisign /rpa (c)10
    ou=VeriSign Trust Network
    o=VeriSign\, Inc.
    c=US
```

```
  OCSP AIA:
    URL: http://ocsp verisign
  CRL Distribution Points:
    [1]  http://crl verisign/pca3-g5.crl
  Validity Date:
    start date: 00:00:00 UTC Feb 8 2010
    end   date: 23:59:59 UTC Feb 7 2020
  Associated Trustpoints: _SmartCallHome_ServerCA
```

In den vorherigen Syslogs gibt die ASA jedoch an, dass sie ein Zertifikat vom Smart Software Licensing-Portal erhält, das von einem Zwischenprodukt mit der Bezeichnung "cn=Symantec Class 3 Secure Server CA - G4" signiert wird.

> **Hinweis**: Die Betreffnamen sind ähnlich, unterscheiden sich aber in zwei Punkten: Verisign vs. Symantec am Anfang und G3 vs. G4 am Ende.

Lösung

Die ASAv muss einen Trustpool herunterladen, der die richtigen Zwischen- und/oder Stammzertifikate enthält, um die Kette zu validieren.

In Version 9.5.2 und höher ist der Vertrauenspool für den automatischen Import um 22:00 Uhr Ortszeit des Geräts konfiguriert:

<#root>

```
ASAv#
```

sh run crypto ca trustpool

```
crypto ca trustpool policy
 auto-import
ASAv#
```

sh run all crypto ca trustpool

```
crypto ca trustpool policy
 revocation-check none
 crl cache-time 60
 crl enforcenextupdate
 auto-import
 auto-import url http://www.cisco.com/security/pki/trs/ios_core.p7b
 auto-import time 22:00:00
```

Wenn es sich um eine Erstinstallation handelt und die DNS-Suche (Domain Name System) und die Internetverbindung zu diesem Zeitpunkt noch nicht aktiv waren, war der automatische Import nicht erfolgreich und muss manuell durchgeführt werden.

Bei älteren Versionen, z. B. 9.4.x, ist der automatische Trustpool-Import nicht auf dem Gerät konfiguriert und muss manuell importiert werden.

Bei jeder Version importiert dieser Befehl den Trustpool und die entsprechenden Zertifikate:

```
<#root>

ASAv#

crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

Root file signature verified.
You are about to update the current trusted certificate pool
with the 17145 byte file at http://www.cisco.com/security/pki/trs/ios_core.p7b
Do you want to continue? (y/n)
Trustpool import:
   attempted:  14
   installed:  14
   duplicates: 0
   expired:    0
   failed:     0
```

Überprüfung

Sobald der Trustpool durch den manuellen Befehl oder nach 22:00 Uhr (Ortszeit) importiert wurde, überprüft dieser Befehl, ob im Trustpool Zertifikate installiert sind:

```
<#root>

ASAv#

show crypto ca trustpool policy
14 trustpool certificates installed

Trustpool auto import statistics:
    Last import result: FAILED
    Next scheduled import at 22:00:00 UTC Wed Mar 23 2016
Trustpool Policy
   Trustpool revocation checking is disabled
   CRL cache time: 60 seconds
   CRL next update field: required and enforced
   Automatic import of trustpool certificates is enabled
   Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
   Download time: 22:00:00
   Policy Overrides:
      None configured
```

> **Hinweis**: In der vorherigen Ausgabe ist der letzte automatische Update-Import fehlgeschlagen, da DNS beim letzten automatischen Versuch nicht betriebsbereit war. Daher wird das letzte Auto-Import-Ergebnis weiterhin als fehlgeschlagen angezeigt. Es wurde jedoch ein manuelles Trustpool-Update ausgeführt, bei dem der Trustpool erfolgreich aktualisiert wurde (weshalb 14 Zertifikate installiert sind).

Nach der Installation des Trustpools kann der Befehl zur Tokenregistrierung erneut ausgeführt werden, um die ASAv beim Smart Software-Lizenzierungsportal zu registrieren.

<#root>

ASAv#

license smart register idtoken *id_token* force

Wenn die ASAv bereits beim Smart Software-Lizenzierungsportal registriert war, die Autorisierung jedoch fehlgeschlagen ist, können diese auch manuell versucht werden.

<#root>

ASAv#

license smart renew auth

Änderung des Stammzertifikats der Zertifizierungsstelle - Oktober 2018

Das Stammzertifikat der Zertifizierungsstelle für tools.cisco.com wurde am Freitag, den 5. Oktober 2018 geändert.

Die aktuell bereitgestellte ASAv Version 9.6(2) und höher sowie die Firepower 2100, auf der ASA ausgeführt wird, können von dieser Änderung nicht betroffen werden, wenn die Kommunikation mit http://www.cisco.com/security/pki/trs/ios_core.p7b nicht zulässig ist. Es gibt eine Funktion für den automatischen Zertifikatimport, die standardmäßig auf allen zuvor erwähnten ASA Smart Licensed-Plattformen aktiviert ist. Die Ausgabe von "show crypto ca trustpool" enthält das Zertifikat "QuoVadis Root CA 2":

```
CA Certificate
  Fingerprint: 5e397bddf8baec82e9ac62ba0c54002b
  Issuer Name:
    cn=QuoVadis Root CA 2
    o=QuoVadis Limited
    c=BM
  Subject Name:
    cn=QuoVadis Root CA 2
    o=QuoVadis Limited
    c=BM
```

Bei neuen Bereitstellungen können Sie den Befehl "crypto ca trustpool import default" ausgeben und das Cisco Standard-Zertifikatspaket herunterladen, das das QuoVadis-Zertifikat enthält. Wenn das nicht funktioniert, können Sie das Zertifikat manuell installieren:

```
asa(config)# crypto ca trustpoint QuoVadisRootCA2
asa(config-ca-trustpoint)# enrollment terminal
asa(config-ca-trustpoint)# crl configure
asav(config-ca-crl)# crypto ca authenticate QuoVadisRootCA2
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9W
YWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----

quit

INFO: Certificate has the following attributes:
Fingerprint:     5e397bdd f8baec82 e9ac62ba 0c54002b
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

4100/9300-Plattformen mit ASA

Dieses Problem betrifft etwa 4100/9300 vor Ort, auf denen ASA ausgeführt wird, die Smart Licensing-Informationen über das FirePOWER eXtensible Operating System (FXOS) bereitstellt:

Betroffene Einheit:

<#root>

```
FP9300-1-A-A-A /license # show license all

Smart Licensing Status
======================
```

```
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: TAC Cisco Systems, Inc.
  Virtual Account: CALO
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jul 01 18:37:38 2018 UTC
  Last Renewal Attempt: FAILED on Oct 09 17:32:59 2018 UTC
```

Failure reason: Failed to authenticate server

Lösungsschritte

Um dies zu beheben, müssen Sie einen neuen Vertrauenspunkt erstellen und die Zertifikatdaten in FXOS eingeben:

<#root>

```
FPR-2-A /license # scope security
FPR-2-A /security # enter trustpoint QuoVadisRootCA2
FPR-2-A /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:    (THIS PART NEEDS TO BE COPY/PASTED)
>
-----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9W
YWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
```

```
-----END CERTIFICATE-----
>ENDOFBUF
```

<---manually type this on a new line after the ----END OF CERTIFICATE---- line and press ENTER

Bestätigen Sie dann die Änderung, und verlängern Sie die Lizenz:

```
FPR-2-A /security/trustpoint* # comm
FPR-2-A /security/trustpoint # scope license
FPR-2-A /license # scope licdebug
FPR-2-A /license/licdebug # renew
```

Überprüfen Sie nun, ob die Lizenz erneuert wurde:

<#root>

```
FP9300-1-A-A-A /license/licdebug # show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: TAC Cisco Systems, Inc.
  Virtual Account: CALO
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jul 01 18:37:38 2018 UTC
  Last Renewal Attempt: SUCCEEDED on Oct 09 17:39:07 2018 UTC
  Next Renewal Attempt: Apr 07 17:39:08 2019 UTC
  Registration Expires: Oct 09 17:33:07 2019 UTC

License Authorization:
  Status: AUTHORIZED on Oct 09 17:39:12 2018 UTC
  Last Communication Attempt: SUCCESS on Oct 09 17:39:12 2018 UTC
  Next Communication Attempt: Nov 08 17:39:12 2018 UTC
  Communication Deadline: Jan 07 17:33:11 2019 UTC
```

ASA-Softwareinstallationen, die FIPS-Konformität (Federal Information Processing Standards) erfordern

Bei ASA-basierten Plattformen, die die FIPS-Konformität erfordern, kann der Import des QuoVadis Root CA 2-Zertifikats fehlschlagen, wenn die kryptografischen Anforderungen der Signatur nicht erfüllt werden. Diese Meldung kann angezeigt werden:

```
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate is not FIPS compliant.
% Error in saving certificate: status = FAIL
```

Importieren Sie als Workaround für FIPS-konforme ASA-Installationen das Zwischenzertifikat HydrantID SSL ICA G2. Das HydrantID SSL ICA G2-Zertifikat wird als Nächstes angezeigt und erfüllt die Anforderungen des sha256WithRSAEncryption-Signaturalgorithmus. Informationen zum Laden des Zertifikats auf Basis Ihrer Plattform finden Sie in der Dokumentation zu diesem Artikel:

```
-----BEGIN CERTIFICATE-----
MIIGxDCCBKygAwIBAgIUdRcWd4PQQ361VsNXlG5FY7jr06wwDQYJKoZIhvcNAQEL
BQAwRTELMAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZ
BgNVBAMTElF1b1ZhZGlzIFJvb3QgQ0EgMjAeFw0xMzEyMTcxNDI1MTBaFw0yMzEy
MTcxNDI1MTBaMF4xCzAJBgNVBAYTAlVTMTAwLgYDVQQKEydIeWRyYW50SUQgKEF2
YWxhbmNoZSBDbG91ZCBDb3Jwb3JhdGlvbikxHTAbBgNVBAMTFEh5ZHJhbnRJRCBT
U0wgSUNBIEcyMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA9p1ZOA9+
H+tgdln+STF7bdOxvnOERYyjo8ZbKumzigNePSwbQYVWuso76GI843yjaX2rhn0+
Jt0NVJM41jVctf9qwacVduR7CEi0qJgpAUJyZUuB9IpFWF1Kz14O3Leh6URuRZ43
RzHaRmNtzkxttGBuOtAg+ilOuwiGAo9VQLgdONlqQFcrbp97/fO8ZIqiPrbhLxCZ
fXkYi3mktZVRFKXG62FHAuH1sLDXCKba3avDcUR7ykG4ZXcmp6kl14UKa8JHOHPE
NYyr0R6oHELOGZMox1nQcFwuYMX9sJdAUU/9SQVXyA6u6YtxlpZiC8qhXM1IE00T
Q9+q5ppffSUDMC4V/5If5A6snKVP78M8qd/RMVswcjMUMEnov+wykwCbDLD+IReM
A57XX+HojN+8XFTL9Jwge3z3ZlMwL7E54W3cI7f6cxO5DVwoKxkdk2jRIg37oqSl
SU3z/bA9UXjHcTl/6BoLho2p9rWm6oljANPeQuLHyGJ3hc19N8nDo2IATp70klGP
kd1qhIgrdkki7gBpanMOK98hKMpdQgs+NY4DkaMJqfrHzWR/CYkdyUCivFaepaFS
K78+jVu1oCMOFOnucPXL2fQa3VQn+69+7mA324frjwZj9NzrHjd0a5UP7waPpd9W
2jZoj4b+g+l+XU1SQ+9DWiuZtvfDW++k0BMCAwEAAaOCAZEwggGNMBIGA1UdEwEB
/wQIMAYBAf8CAQAweAYDVR0gBHEwbzAIBgZngQwBAgEwCAYGZ4EMAQICMA4GDCsG
AQQBvlgAAmQBAjBJBgwrBgEEAb5YAAOHBAAwOTA3BggrBgEFBQcCARYraHR0cDov
L3d3dy5oeWRyYW50aWQuY29tL3N1cHBvcnQvcmVwb3NpdG9yeTByBggrBgEFBQcB
AQRmMGQwKgYIKwYBBQUHMAGGHmh0dHA6Ly9vY3NwLnF1b3ZhZGlzZ2xvYmFsLmNv
bTA2BggrBgEFBQcwAoYqaHR0cDovL3RydXN0LnF1b3ZhZGlzZ2xvYmFsLmNvbS9x
dnJjYTIuY3J0MA4GA1UdDwEB/wQEAwIBBjAfBgNVHSMEGDAWgBQahGK8SEwzJQTU
7tD2A8QZRtGUazA5BgNVHR8EMjAwMC6gLKAqhihodHRwOi8vY3JsLnF1b3ZhZGlz
Z2xvYmFsLmNvbS9xdnJjYTIuY3JsMB0GA1UdDgQWBBSYarYtLr+nqp/299YJr9WL
V/mKtzANBgkqhkiG9w0BAQsFAAOCAgEAlraik8EDDUkpAnIOajO9/r4dpj/Zry76
6SH1oYPo7eTGzpDanPMeGMuSmwdjUkFUPALuWwkaDERfz9xdyFL3N8CRg9mQhdtT
3aWQUv/iyXULXT87EgL3b8zzf8fhTS7r654m9WM2W7pFqfimx9qAlFe9XcVlZrUu
9hph+/MfWMrUju+VPL5U7hZvUpg66mS3BaN15rsXv2+Vw6kQsQC/82iJLHvtYVL/
LwbNio18CsinDeyRE0J9wlYDqzcg5rhD0rtX4JEmBzq8yBRvHIB/023o/vIO5oxh
83Hic/2Xgwksf1DKS3/z5nTzhsUIpCpwkN6nHp6gmA8JBXoUlKQz4eYHJCq/ZyC+
BuY2vHpNx6101J5dmy7ps7J7d6mZXzguP3DQN84hjtfwJPqdf+/9RgLriXeFTqwe
snxbk2FsPhwxhiNOH98GSZVvG02v10uHLVaf9B+puYpoUiEqgm1WG5mWW1PxHstu
Ew9jBMcJ6wjQc8He9rSUmrhBr0HyhckdC99RgEvpcZpV2XL4nPPrTI2ki/c9xQb9
kmhVGonSXy5aP+hDC+Ht+bxmc4wN5x+vB02hak8Hh8jIUStRxOsRfJozU0R9ysyP
EZAHFZ3Zivg2BaD4tOISO8/T2FDjG7PNUv0tgPAOKw2t94B+1evrSUhqJDU0Wf9c
9vkaKoPvX4w=
-----END CERTIFICATE-----
```

Zugehörige Informationen

- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.