Konfigurieren der ASA: Installation und Verlängerung digitaler SSL-Zertifikate

Inhalt

Einleitung

Dieses Dokument beschreibt die Installation eines vertrauenswürdigen SSL-Zertifikats von Drittanbietern auf der ASA für Clientless-SSL-VPN- und AnyConnect-Verbindungen.

Hintergrundinformationen

In diesem Beispiel wird ein GoDaddy-Zertifikat verwendet. Jeder Schritt enthält die ASDM-Prozedur (Adaptive Security Device Manager) und die CLI-Entsprechung.

Voraussetzungen

Anforderungen

Für die Registrierung von Zertifikaten ist der Zugriff auf eine vertrauenswürdige Zertifizierungsstelle (Certificate Authority, CA) eines Drittanbieters erforderlich. Zu den Anbietern von CA-Lösungen von Drittanbietern gehören u. a. Baltimore, Cisco, Entrust, Geotrust, G, Microsoft, RSA, Thawte und VeriSign.

Überprüfen Sie vor dem Start, ob die ASA über die richtige Uhrzeit, das richtige Datum und die richtige Zeitzone verfügt. Bei der Zertifikatsauthentifizierung wird empfohlen, zur Synchronisierung der Uhrzeit auf der ASA einen NTP-Server (Network Time Protocol) zu verwenden. Im Konfigurationsleitfaden für die CLI-Konfiguration der Cisco ASA-Serie 9.1 werden die Schritte beschrieben, die zur richtigen Zeit- und Datumseinstellung auf der ASA erforderlich sind.

Verwendete Komponenten

In diesem Dokument wird eine ASA 5500-X verwendet, auf der die Softwareversion 9.4.1 und ASDM Version 7.4(1) ausgeführt werden.

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 verstehen.

Konfigurieren

Das SSL-Protokoll schreibt vor, dass der SSL-Server dem Client ein Serverzertifikat zur Verfügung stellt, damit der Client die Serverauthentifizierung durchführt. Cisco rät von der Verwendung eines selbstsignierten Zertifikats ab, da ein Benutzer möglicherweise versehentlich einen Browser so konfigurieren könnte, dass ein Zertifikat von einem nicht autorisierten Server vertrauenswürdig ist. Bei der Verbindung mit dem sicheren Gateway müssen Benutzer außerdem unnötig auf eine Sicherheitswarnung reagieren. Es wird empfohlen, vertrauenswürdige CAs von Drittanbietern zu verwenden, um der ASA zu diesem Zweck SSL-Zertifikate auszustellen.

Der Lebenszyklus eines Drittanbieterzertifikats auf der ASA erfolgt im Wesentlichen mit den folgenden Schritten:

CSR-Generierung

Die CSR-Generierung ist der erste Schritt im Lebenszyklus jedes digitalen X.509-Zertifikats.

Sobald der Private/Public Rivest-Shamir-Adleman (RSA) oder der Elliptic Curve Digital Signature Algorithm (ECDSA)-Tastenblock generiert wurde (Anhang A beschreibt den Unterschied zwischen der Verwendung von RSA oder ECDSA), wird eine Zertifikatsanforderung (Certificate Signing Request, CSR) erstellt.

Ein CSR ist eine PKCS10-formatierte Nachricht, die den öffentlichen Schlüssel und die Identitätsinformationen des Hosts enthält, der die Anforderung sendet. PKI-Datenformate erläutert die verschiedenen Zertifikatsformate, die auf ASA und Cisco IOS anwendbar sind.®.

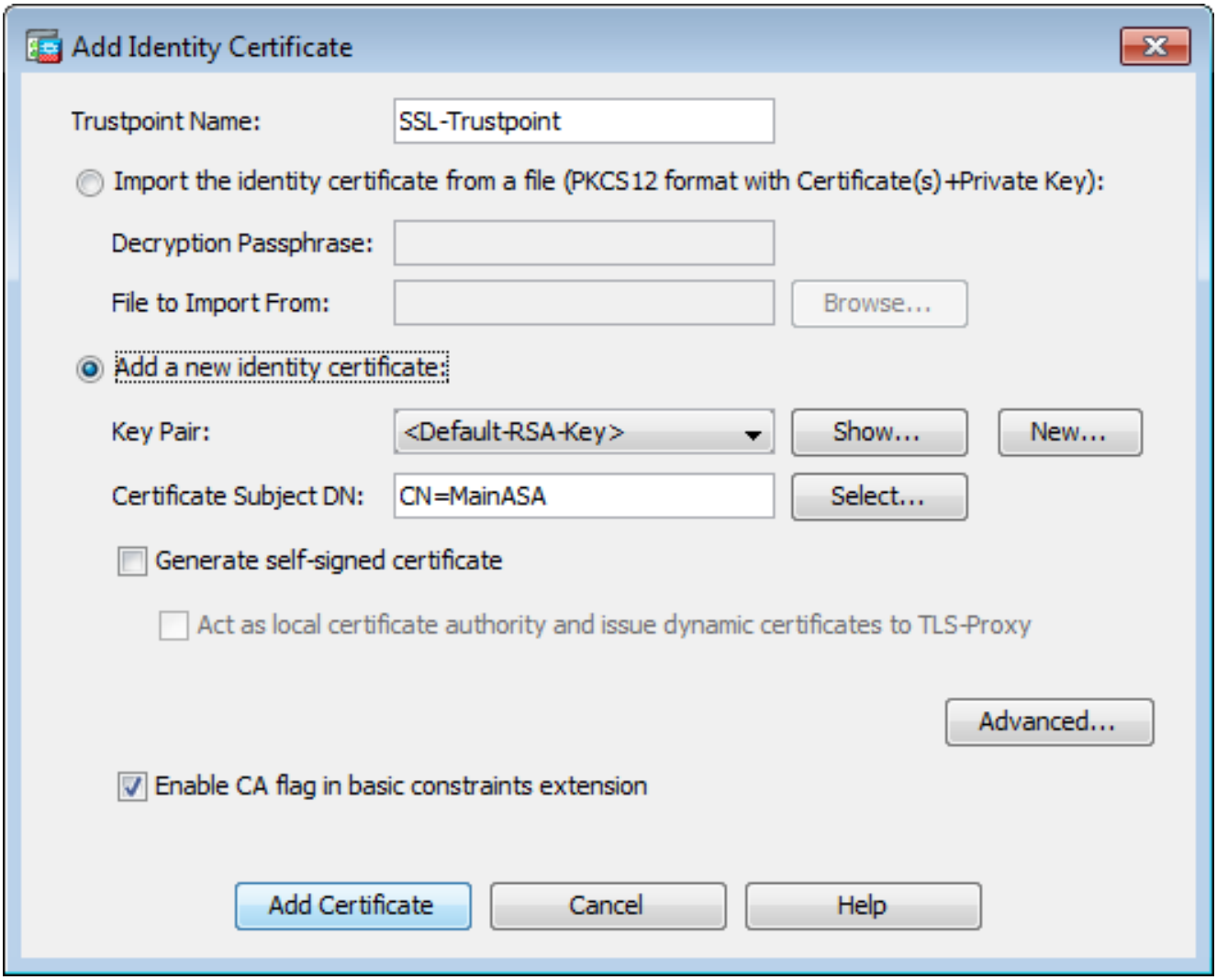
> **Hinweise:**
> 1. Überprüfen Sie mit der CA die benötigte Zifferngröße. Das CA/Browser Forum hat das Mandat, dass alle Zertifikate, die von den jeweiligen CAs generiert werden, eine Mindestgröße von 2048 Bit aufweisen.
> 2. ASA unterstützt derzeit keine 4096-Bit-Schlüssel (Cisco Bug ID CSCut53512) für die SSL-Serverauthentifizierung. IKEv2 unterstützt jedoch die Verwendung von 4096-Bit-Serverzertifikaten nur auf den Plattformen ASA 5580, 5585 und 5500-X.
> 3. Verwenden Sie den DNS-Namen der ASA im FQDN-Feld des CSR, um nicht vertrauenswürdige Zertifikatswarnungen zu verhindern und die strikte Zertifikatsüberprüfung zu durchlaufen.

Es gibt drei Methoden zum Generieren von CSR.

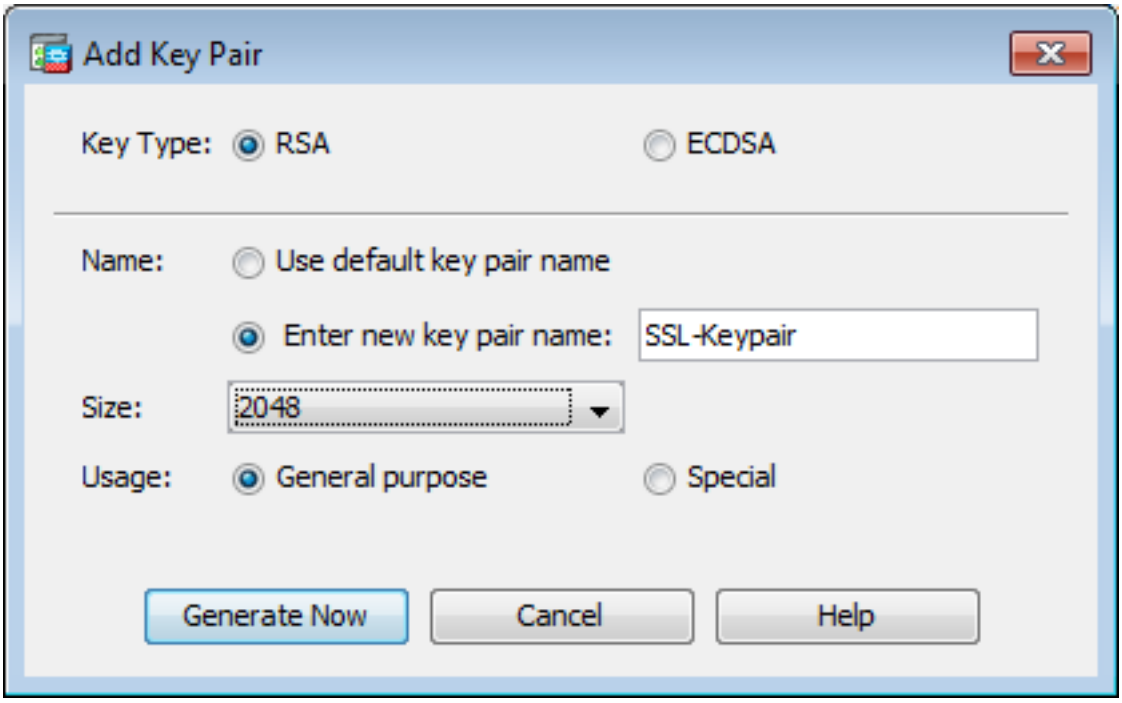
- Konfiguration mit ASDM
- Konfiguration mit der ASA CLI
- Verwenden von OpenSSL zum Generieren des CSR

1. Konfiguration mit dem ASDM

1. Navigieren zu **Configuration > Remote Access VPN > Certificate Management**, und wählen Sie **Identity Certificates**.
2. Klicken Sie auf **Add**.



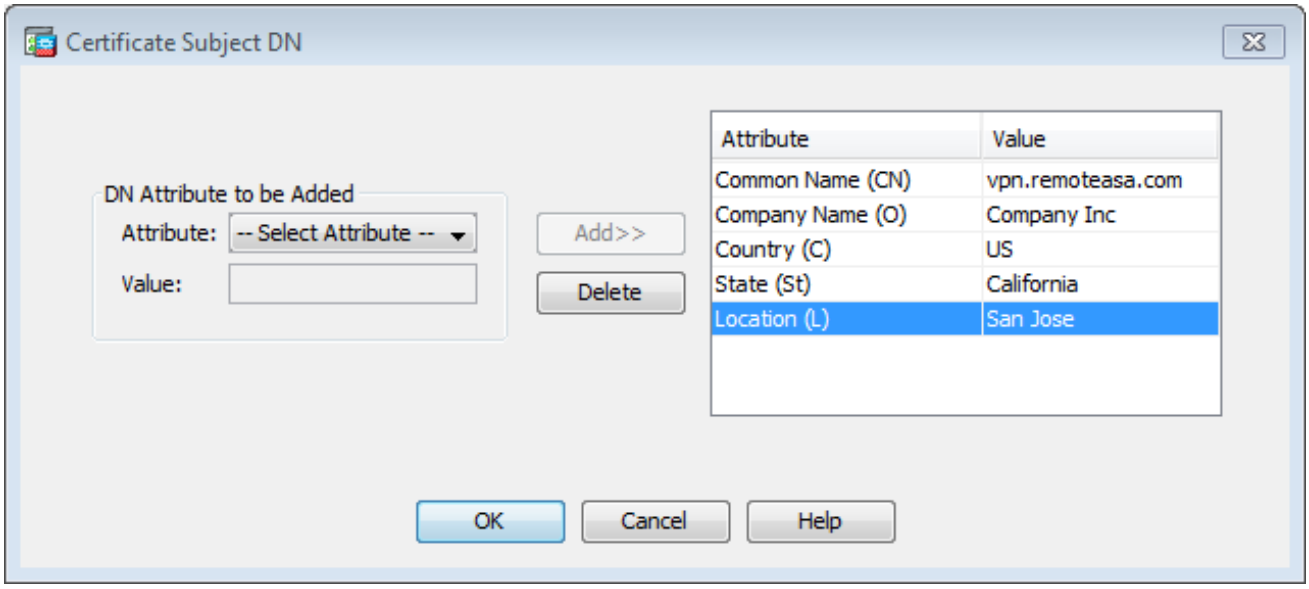
3. Definieren Sie im Eingabefeld Trustpoint Name einen Trustpoint-Namen.
4. Klicken Sie auf**Add a new identity certificate**ein.
5. Klicken Sie für das Schlüsselpaar auf**New**.



6. Wählen Sie den Schlüsseltyp aus: RSA oder ECDSA. (Die Unterschiede sind in Anhang A aufgeführt.)
7. Klicken Sie auf**Enter new key pair name**ein. Geben Sie den Namen des Schlüsselpaars für Erkennungszwecke an.
8. Wählen Sie**Key Size**. Auswählen**General Purpose for Usage** bei Verwendung von RSA.
9. Klicken Sie auf **Generate Now**. Das Schlüsselpaar wird erstellt.
10. Um die ZertifikatSubject DN zu definieren, klicken Sie auf**Select**und konfigurieren Sie die in dieser Tabelle aufgeführten Attribute:

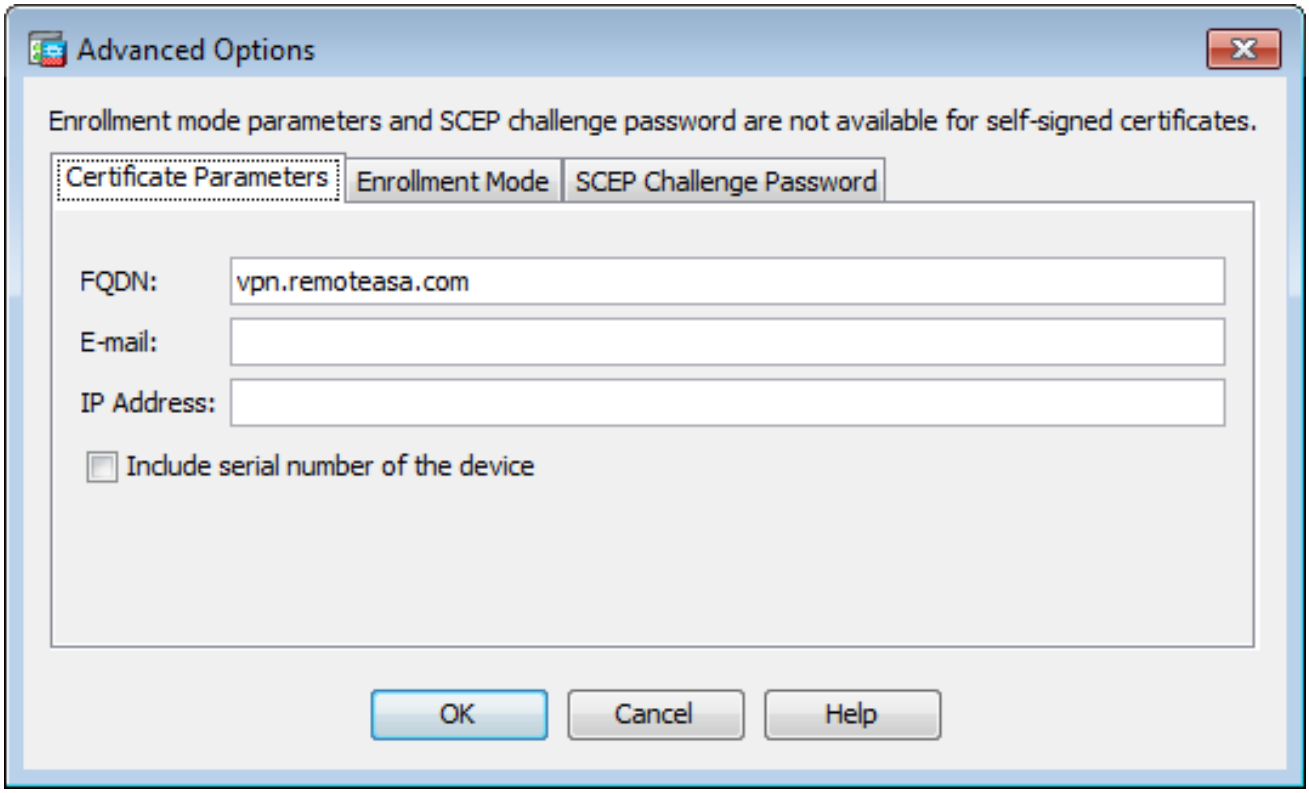
Attribute	Description
CN	FQDN (Full Qualified Domain Name) that will be used for connections to your firewall. For example, webvpn.cisco.com
OU	Department Name
O	Company Name (Avoid using Special Characters)
C	Country Code (2 Letter Code without Punctuation)
St	State (Must be spelled out completely. For example, North Carolina)
L	City
EA	Email Address

Um diese Werte zu konfigurieren, wählen Sie einen Wert aus der Dropdown-Liste **Attribute**, geben Sie den Wert ein, und klicken Sie auf
Hinzufügen.



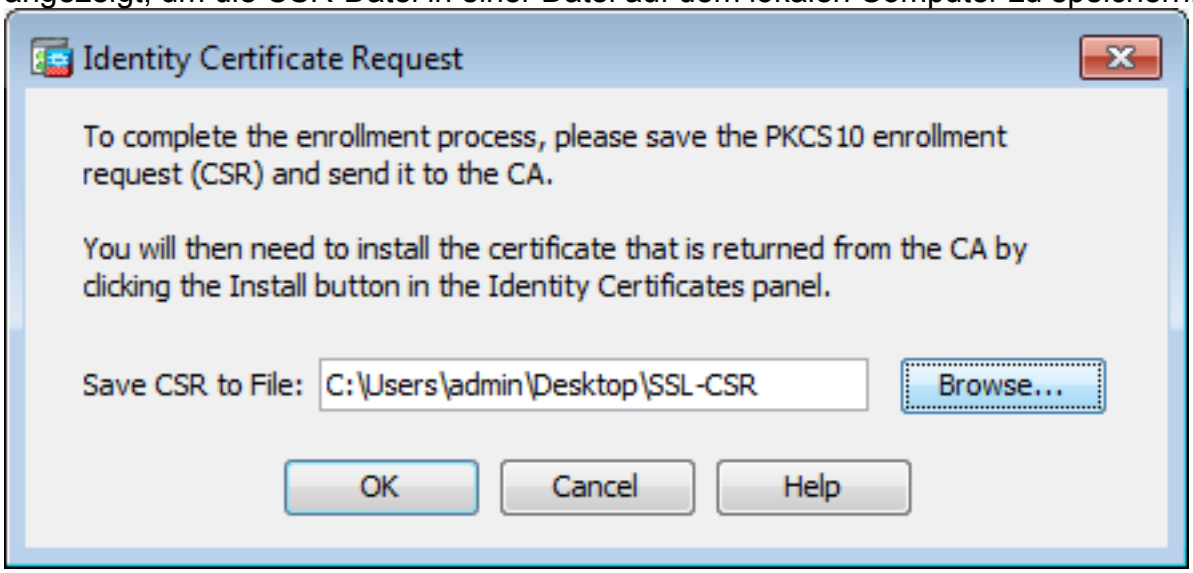
Anmerkung: Bei einigen Drittanbietern müssen vor Ausstellung eines Identitätszertifikats bestimmte Attribute enthalten sein. Wenn Sie sich nicht sicher sind, welche Attribute erforderlich sind, wenden Sie sich an den Hersteller, um weitere Informationen zu erhalten.

11. Wenn Sie die entsprechenden Werte hinzugefügt haben, klicken Sie auf**OK**. Das Dialogfeld Identitätszertifikat hinzufügen wird mit dem Zertifikat angezeigt.**Subject DN** field populated.
12. Klicken Sie auf **Erweitert**.



13. Im**FQDN**Geben Sie den FQDN ein, der für den Zugriff auf das Gerät aus dem Internet verwendet wird. Klicken Sie auf **OK**.
14. Lassen Sie das Kontrollkästchen CA in der Option Erweiterung mit grundlegenden Einschränkungen aktivieren aktiviert. Zertifikate ohne CA-Flag können jetzt nicht standardmäßig als CA-Zertifikate auf der ASA installiert werden. Die Erweiterung mit grundlegenden Einschränkungen gibt an, ob es sich bei dem Zertifikatum eine Zertifizierungsstelle handelt, und gibt die maximale Tiefe der gültigen Zertifizierungspfade an, die dieses Zertifikat enthalten. Deaktivieren Sie die Option, um diese Anforderung zu umgehen.
15. Klicken Sie auf **OK**, und klicken Sie dann auf**Add Certificate.** Es wird eine Eingabeaufforderung

angezeigt, um die CSR-Datei in einer Datei auf dem lokalen Computer zu speichern.



16. Klicken Sie auf **Browse**, wählen Sie einen Speicherort für die CSR-Datei und speichern Sie die Datei mit der Erweiterung .txt. **Anmerkung:** Wenn die Datei mit der Erweiterung .txt gespeichert wird, kann die PKCS#10-Anforderung geöffnet und mit einem Texteditor (z. B. Notepad) angezeigt werden.

2. Konfiguration mit der ASA CLI

Im ASDM wird der Vertrauenspunkt automatisch erstellt, wenn ein CSR generiert wird oder das Zertifizierungsstellenzertifikat installiert ist. In der CLI muss der Vertrauenspunkt manuell erstellt werden.

```
! Generates 2048 bit RSA key pair with label SSL-Keypair.

MainASA(config)# crypto key generate rsa label SSL-Keypair modulus 2048

INFO: The name for the keys will be: SSL-Keypair
Keypair generation process begin. Please wait...

 ! Define trustpoint with attributes to be used on the SSL certificate

MainASA(config)# crypto ca trustpoint SSL-Trustpoint
MainASA(config-ca-trustpoint)# enrollment terminal
MainASA(config-ca-trustpoint)# fqdn vpn.remoteasa.com
MainASA(config-ca-trustpoint)# subject-name CN=vpn.remoteasa.com,O=Company Inc,C=US,
St=California,L=San Jose
MainASA(config-ca-trustpoint)# keypair SSL-Keypair
MainASA(config-ca-trustpoint)# exit

 ! Initiates certificate signing request. This is the request to be submitted via Web or
Email to the third party vendor. MainASA(config)# crypto ca enroll SSL-Trustpoint

WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]: yes
% Start certificate enrollment ..
% The subject name in the certificate will be: subject-name CN=vpn.remoteasa.com,
O=Company Inc,C=US,St=California,L=San Jose % The fully-qualified domain name in the certificate
```

```
will be: vpn.remoteasa.com % Include the device serial number in the subject name? [yes/no]: no

Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----
MIIDDjCCAfYCAQAwgYkxETAPBgNVBAcTCFNhbiBKb3NlMRMwEQYDVQQIEwpDYWxp
Zm9ybmlhMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLQ29tcGFueSBJbmMxGjAYBgNV
BAMTEXZwbi5yZW1vdGVhc2EuY29tMSAwHgYJKoZIhvcNAQkCFhF2cG4ucmVtb3Rl
YXNhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK62Nhb9ktlK
uR3Q4TmksyuRMqJNrb9kXpvA6H200PuBfQvSF4rVnSwKOmu3c8nweEvYcdVWV6Bz
BhjXeovTVi17FlNTceaUTGikeIdXC+mw1iE7eRsynS/d4mzMWJmrvrsDNzpAW/EM
SzTca+BvqF7X2r3LU8Vsv6Oi8ylhco9Fz7bWvRWVtO3NDDbyolC9b/VgXMuBitcc
rzfUbVnm7VZDOf4jr9EXgUwXxcQidWEABlFrXrtYpFgBo9aqJmRp2YABQ1ieP4cY
3rBtgRjLcF+S9TvHG5m4v7v755meV4YqsZIXvytIOzVBihemVxaGA1oDwfkoYSFi
4CzXbFvdG6kCAwEAAaA/MD0GCSqGSIb3DQEJDjEwMC4wDgYDVR0PAQH/BAQDAgWg
MBwGA1UdEQQVMBOCEXZwbi5yZW1vdGVhc2EuY29tMA0GCSqGSIb3DQEBBQUAA4IB
AQBZuQzUXGEB0ix1yuPK0ZkRz8bPnwIqLTfxZhagmuyEhrN7N4+aQnCHj85oJane
4ztZDiCCoWTerBS4RSkKEHEspu9oohjCYuNnp5qa91SPrZNEjTWw0eRn+qKbId2J
jE6Qy4vdPCexavMLYVQxCny+gVkzPN/sFRk3EcTTVq6DxxaebpJijmiqa7gCph52
YkHXnFne1LQd41BgoLlCr9+hx74XsTHGBmI1s/9T5oAX26Ym+B2l/i/DP5BktIUA
8GvIY1/ypj9KO49fP5ap8al0qvLtYYcCcfwrCt+OojOrZ1YyJb3dFuMNRedAX37t
DuHNl2EYNpYkjVk1wI53/5w3
-----END CERTIFICATE REQUEST----- Redisplay enrollment request? [yes/no]: no

 ! Displays the PKCS#10 enrollment request to the terminal. Copy this from the terminal
to a text file to submit to the third party CA.
```

3. Verwenden von OpenSSL zum Generieren des CSR

OpenSSL nutzt die**openSSL config**um die Attribute anzuzeigen, die für die CSR-Generierung verwendet werden. Dieser Prozess führt zur Generierung eines CSR und eines privaten Schlüssels.

> **Vorsicht:** Stellen Sie sicher, dass der **private Schlüssel**, der generiert wird, nicht für andere Benutzer freigegeben wird, da dies die Integrität des Zertifikats beeinträchtigt.

1. Stellen Sie sicher, dass OpenSSL auf dem System installiert ist, auf dem dieser Prozess ausgeführt wird. Für Mac OSX- und GNU/Linux-Benutzer ist dies standardmäßig installiert.
2. Wechseln Sie zu einem funktionierenden Verzeichnis. Unter Windows: Standardmäßig sind die Dienstprogramme in **c:\Openssl\bin**. Öffnen Sie an diesem Ort eine Eingabeaufforderung.Unter Mac OSX/Linux: Öffnen Sie das Terminal-Fenster im Verzeichnis, das zum Erstellen der CSR-Anfrage erforderlich ist.
3. Erstellen Sie eine OpenSSL-Konfigurationsdatei mithilfe eines Texteditors mit den angegebenen Attributen. Speichern Sie anschließend die Datei als **openssl.cnf** an dem Speicherort, der im vorherigen Schritt erwähnt wurde (Wenn Sie Version 0.9.8h und höher verwenden, ist die Datei**openssl.cfg**)

```
 [req]
default_bits = 2048
default_keyfile = privatekey.key
distinguished_name = req_distinguished_name
req_extensions = req_ext

[req_distinguished_name]
commonName = Common Name (eg, YOUR name)
commonName_default = vpn.remoteasa.com

countryName = Country Name (2 letter code)
countryName_default = US
```

```
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = California

localityName = Locality Name (eg, city)
localityName_default = San Jose

0.organizationName = Organization Name (eg, company)
0.organizationName_default = Company Inc

[req_ext]
subjectAltName = @alt_names
[alt_names]
DNS.1 = *.remoteasa.com
```

4. Erstellen Sie mit dem folgenden Befehl den CSR und den privaten Schlüssel: **openssl req -new -nodes -out CSR.csr -config openssl.cnf**

```
 # Sample CSR Generation:

 openssl req -new -nodes -out CSR.csr -config openssl.cnf
Generating a 2048 bit RSA private key
.....................................................................................+++
.....................................+++ writing new private key to 'privatekey.key' ---
-- You are about to be asked to enter information that will be incorporated into your
certificate request. What you are about to enter is what is called a Distinguished Name or
a DN. There are quite a few fields but you can leave some blank For some fields there will
be a default value, If you enter '.', the field will be left blank. ----- Common Name (eg,
YOUR name) [vpn.remoteasa.com]: Country Name (2 letter code) [US]: State or Province Name
(full name) [California]: Locality Name (eg, city) [San Jose]: Organization Name (eg,
company) [Company Inc]:
```

   Senden Sie die gespeicherte CSR-Anfrage an den CA-Anbieter eines Drittanbieters. Nach Ausstellung des Zertifikats stellt die Zertifizierungsstelle das Identitätszertifikat und das Zertifizierungsstellenzertifikat bereit, das auf der ASA installiert werden soll.

Generierung von SSL-Zertifikaten auf der CA

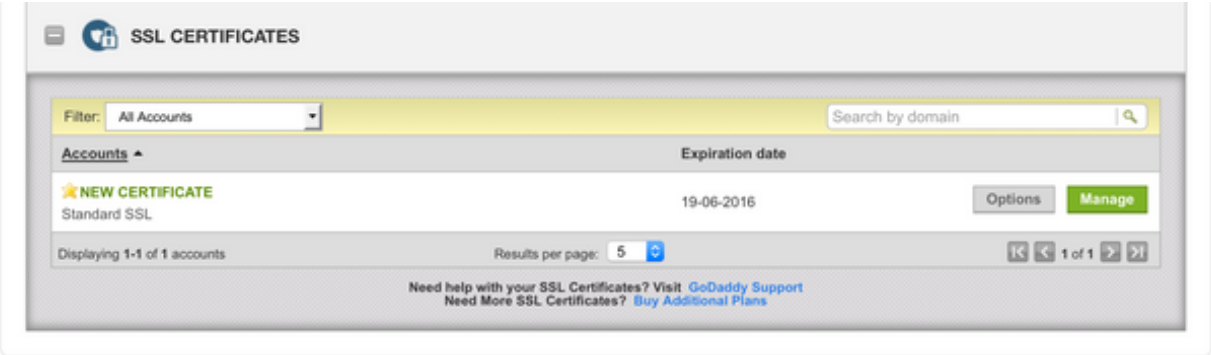
Im nächsten Schritt wird die CSR-Nummer von der CA signiert. Die Zertifizierungsstelle stellt entweder ein neu generiertes PEM-kodiertes Identitätszertifikat oder ein PKCS12-Zertifikat zusammen mit dem Zertifizierungsstellen-Zertifikatpaket bereit.

Wenn der CSR außerhalb der ASA (entweder über OpenSSL oder über die CA selbst) generiert wird, ist das PEM-kodierte Identitätszertifikat mit dem privaten Schlüssel und dem CA-Zertifikat als separate Dateien verfügbar. Anhang B enthält die Schritte zum Bündeln dieser Elemente in einer einzigen PKCS12-Datei (.p12- oder .pfx-Format).

In diesem Dokument wird die GoDaddy CA als Beispiel für die Ausstellung von Identitätszertifikaten an die ASA verwendet. Dieser Prozess kann bei anderen CA-Anbietern abweichen.Lesen Sie die CA-Dokumentation sorgfältig durch, bevor Sie fortfahren.

Beispiel für die Generierung von SSL-Zertifikaten auf GoDaddy CA

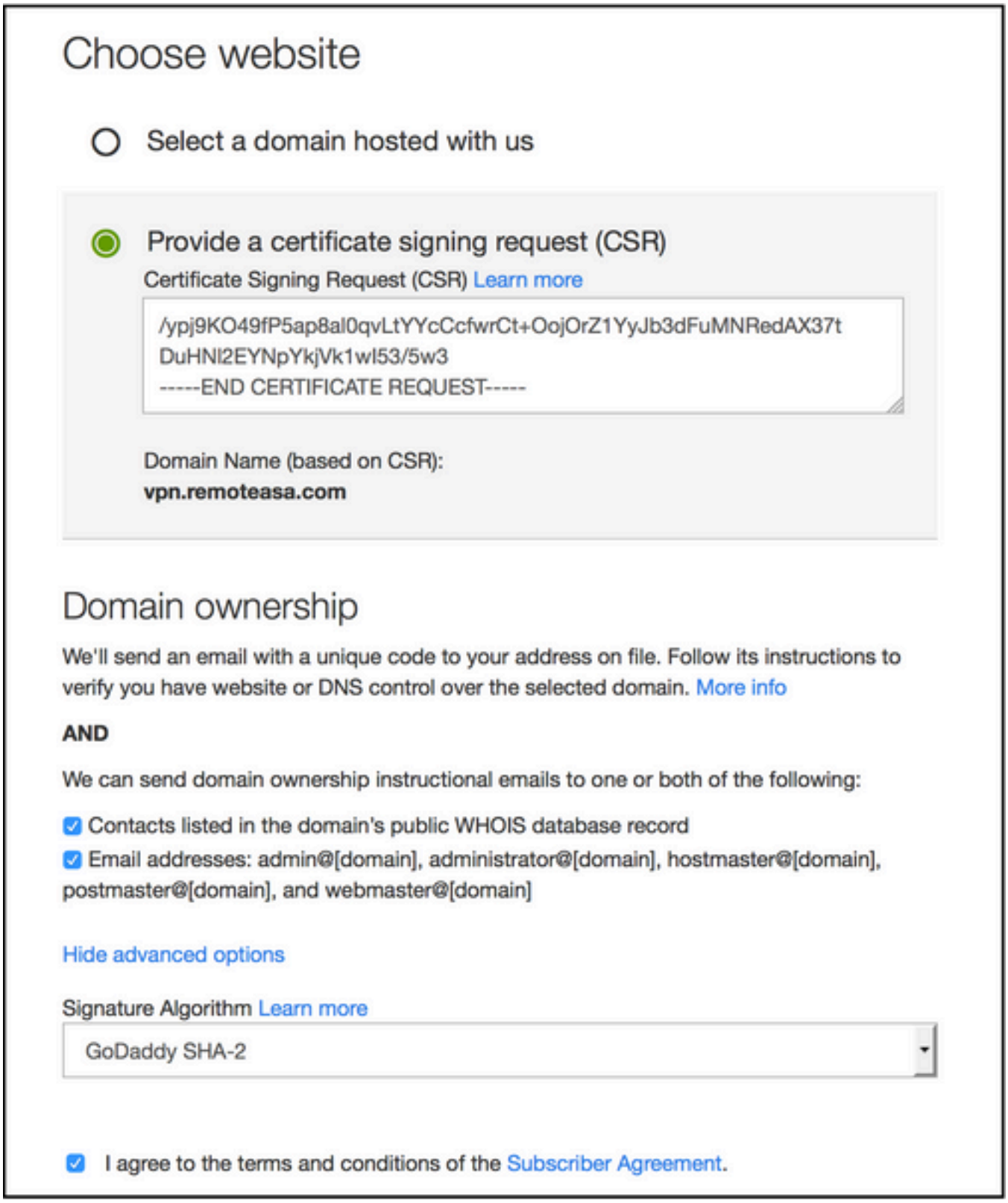
Navigieren Sie nach dem Kauf und der ersten Einrichtungsphase des SSL-Zertifikats zum GoDaddy-Konto, und zeigen Sie die SSL-Zertifikate an. Es muss ein neues Zertifikat geben. Klicken Sie auf **Manage** um fortzufahren.



Daraufhin wird eine Seite geöffnet, auf der Sie die CSR-Anfrage (CSR) anzeigen können, wie in diesem Bild gezeigt.

Auf Basis der eingegebenen CSR bestimmt die CA den Domänennamen, an den das Zertifikat ausgestellt werden soll.

Stellen Sie sicher, dass dieser mit dem FQDN der ASA übereinstimmt.

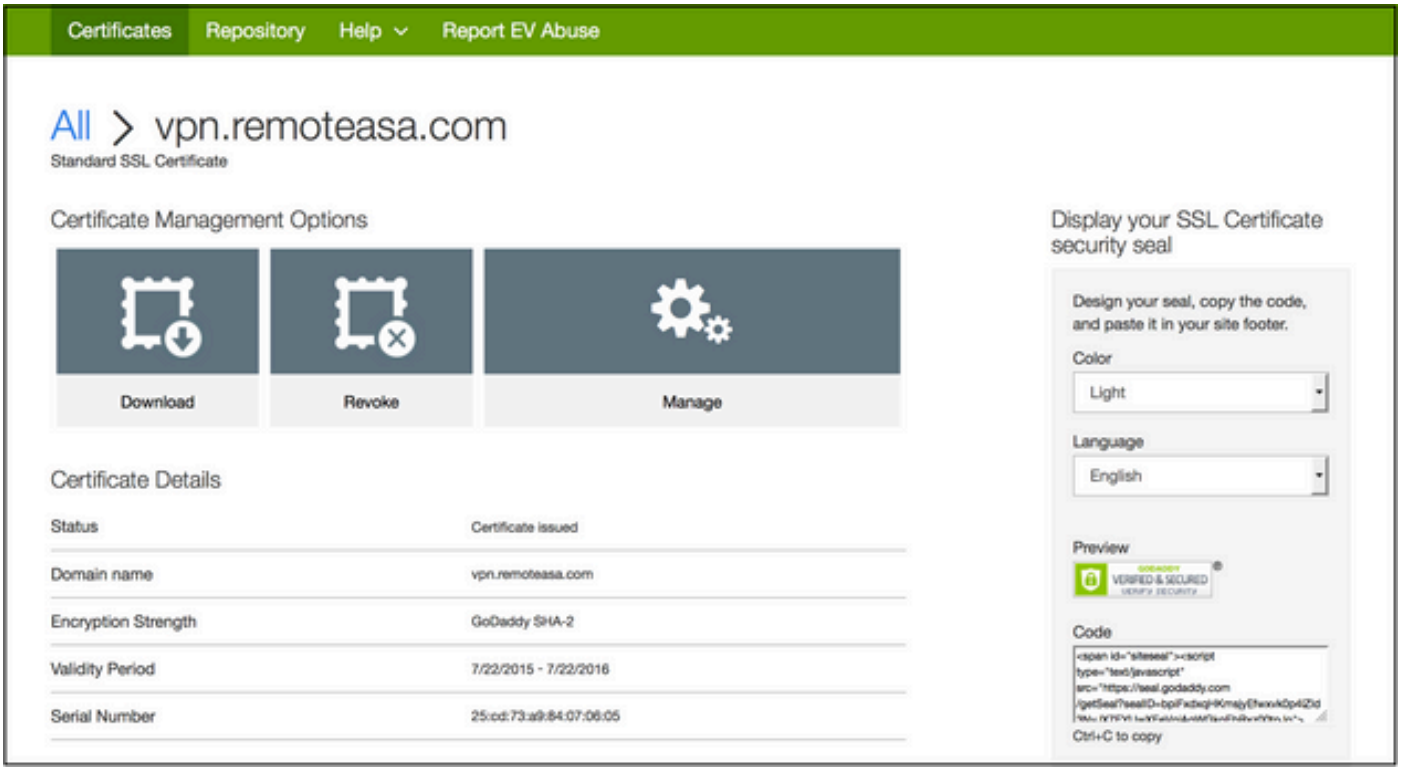


Hinweis: GoDaddy und die meisten anderen CAs verwenden SHA-2 oder SHA256 als Standard-Signaturalgorithmus für Zertifikate. ASA unterstützt den SHA-2-Signaturalgorithmus ab **Version 8.2(5)** [Versionen vor 8.3] und ab Version **8.4(1)** [nach Version 8.3] (Cisco Bug-ID CSCti30937). Wählen Sie den SHA-1-Signaturalgorithmus aus, wenn eine Version verwendet wird, die älter als 8.2(5) oder 8.4(1) ist.

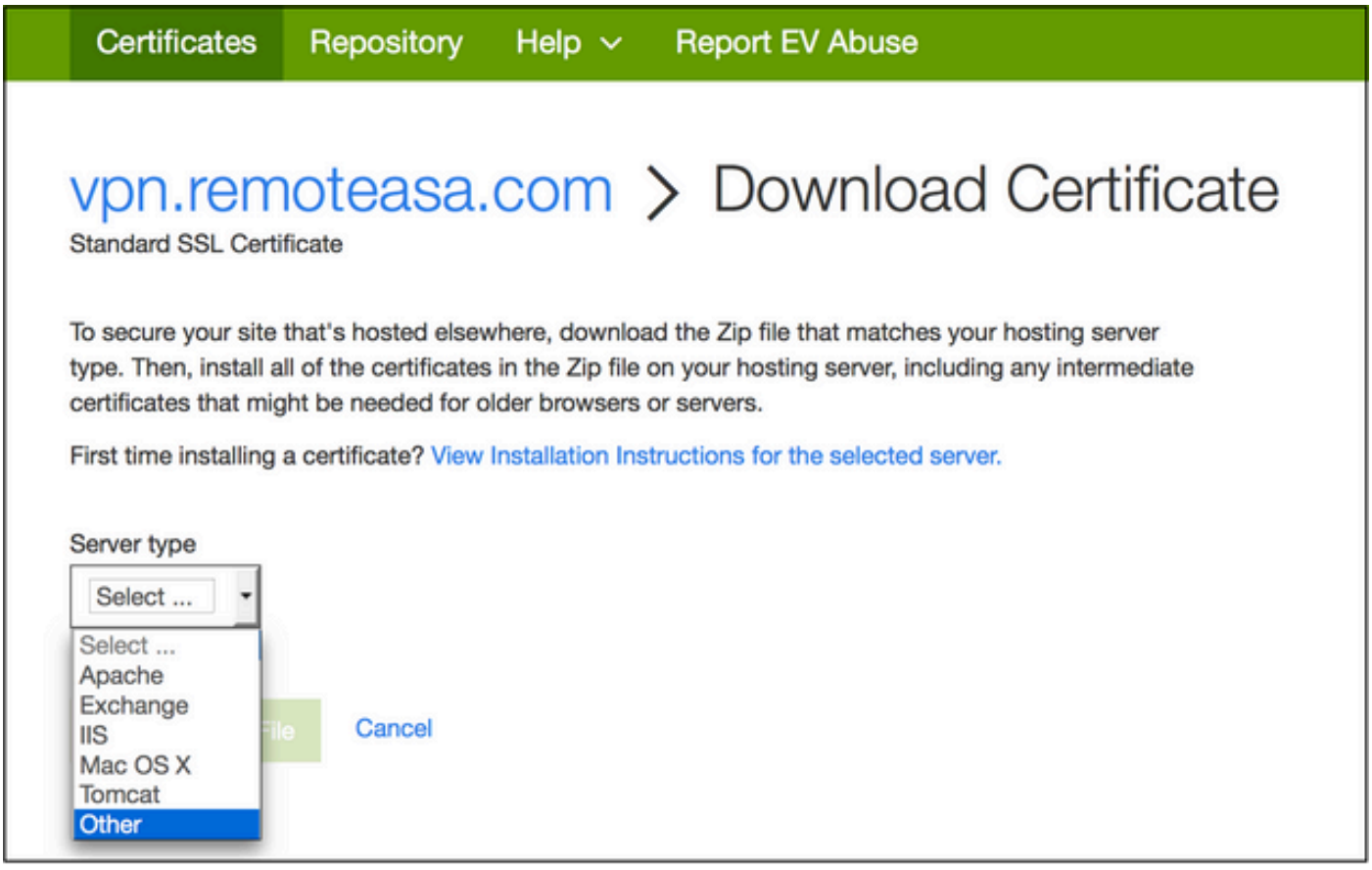
Nachdem die Anfrage gesendet wurde, verifiziert GoDaddy die Anfrage, bevor sie das Zertifikat ausstellt.

Nachdem die Zertifikatsanforderung validiert wurde, stellt GoDaddy das Zertifikat für das Konto aus.

Das Zertifikat kann dann zur Installation auf der ASA heruntergeladen werden. Klicken Sie auf **Download** um fortzufahren.



Auswählen**Other** als Servertyp und laden Sie das Zertifikats-Zip-Paket herunter.



Die ZIP-Datei enthält das Identitätszertifikat und GoDaddy CA-Zertifikatskettenpakete als zwei

separate CRT-Dateien. Setzen Sie die SSL-Zertifikatsinstallation fort, um diese Zertifikate auf der ASA zu installieren.

Installation von SSL-Zertifikaten auf der ASA

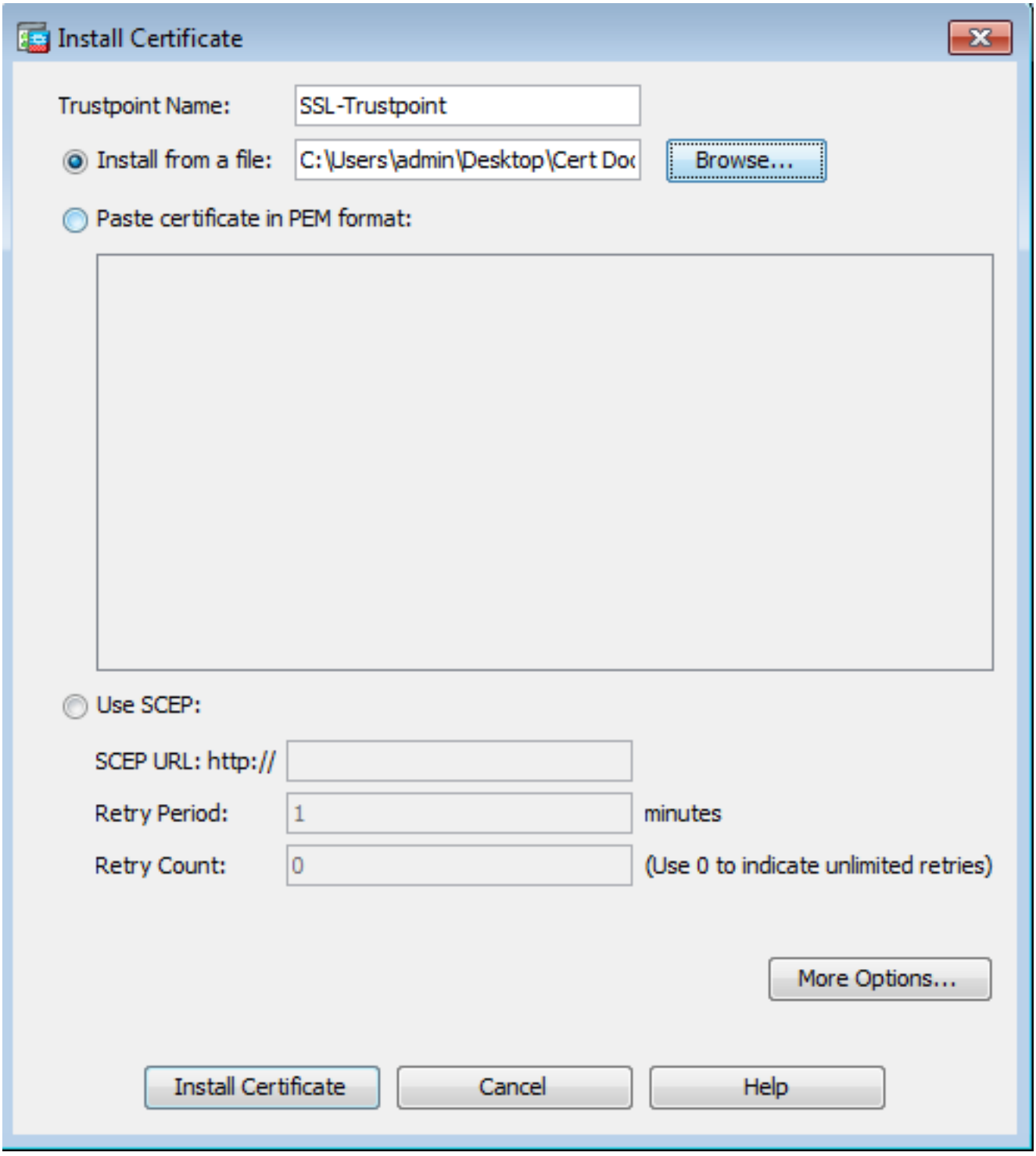
Das SSL-Zertifikat kann auf der ASA mit ASDM oder CLI auf zwei Arten installiert werden:

1. Importieren Sie das CA- und Identitätszertifikat separat in PEM-Formaten.
2. Importieren Sie auch die PKCS12-Datei (base64-verschlüsselt für CLI), in der Identitätszertifikat, Zertifizierungsstellenzertifikat und privater Schlüssel in der PKCS12-Datei gebündelt sind. **Hinweis**: Wenn die Zertifizierungsstelle eine Zertifizierungsstellenkette bereitstellt, installieren Sie nur das direkte Zwischen-Zertifizierungsstellenzertifikat in der Hierarchie des Vertrauenspunkts, der zum Generieren der CSR verwendet wird. Das Zertifikat der Stammzertifizierungsstelle und andere Zwischenzertifikate der Zertifizierungsstellen können in neuen Vertrauenspunkten installiert werden.

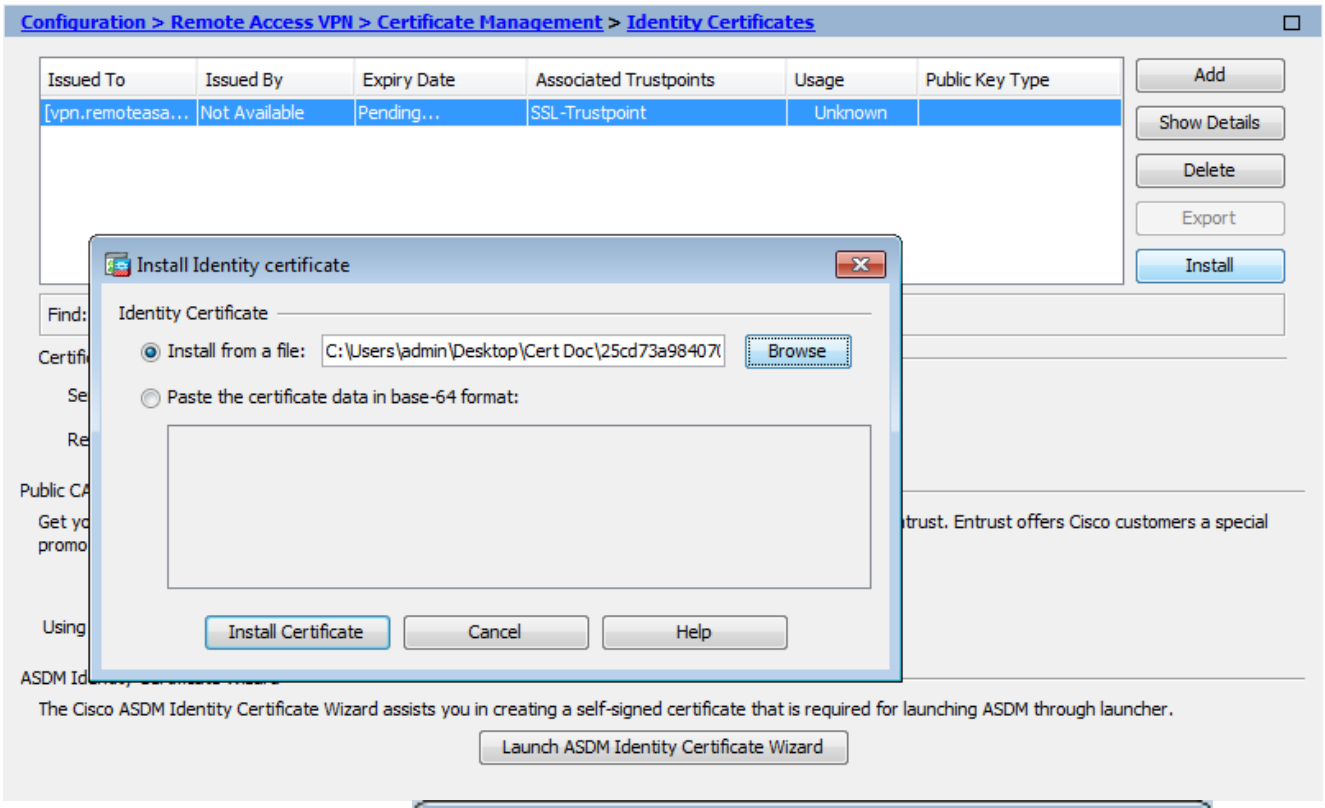
1.1 Installation des Identitätszertifikats im PEM-Format mit ASDM

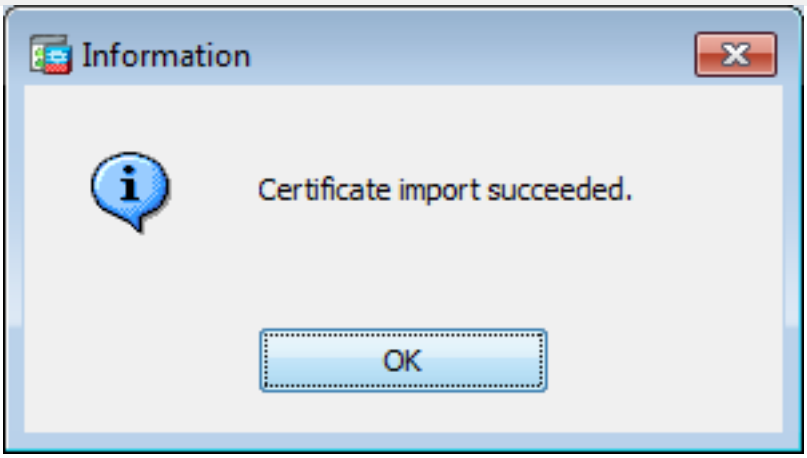
Bei den angegebenen Installationsschritten wird davon ausgegangen, dass die CA ein PEM-verschlüsseltes Identitätszertifikat (.pem, .cer, .crt) und Zertifizierungsstellenzertifikat-Bündel bereitstellt.

1. Navigieren zu **Configuration > Remote Access VPN > Certificate Management**, und wählen Sie Zertifizierungsstellenzertifikate aus.
2. Das PEM-kodierte Zertifikat wird in einem Texteditor gespeichert, und das Base64 CA-Zertifikat, das vom Fremdhersteller bereitgestellt wurde, wird in das Textfeld kopiert und eingefügt.

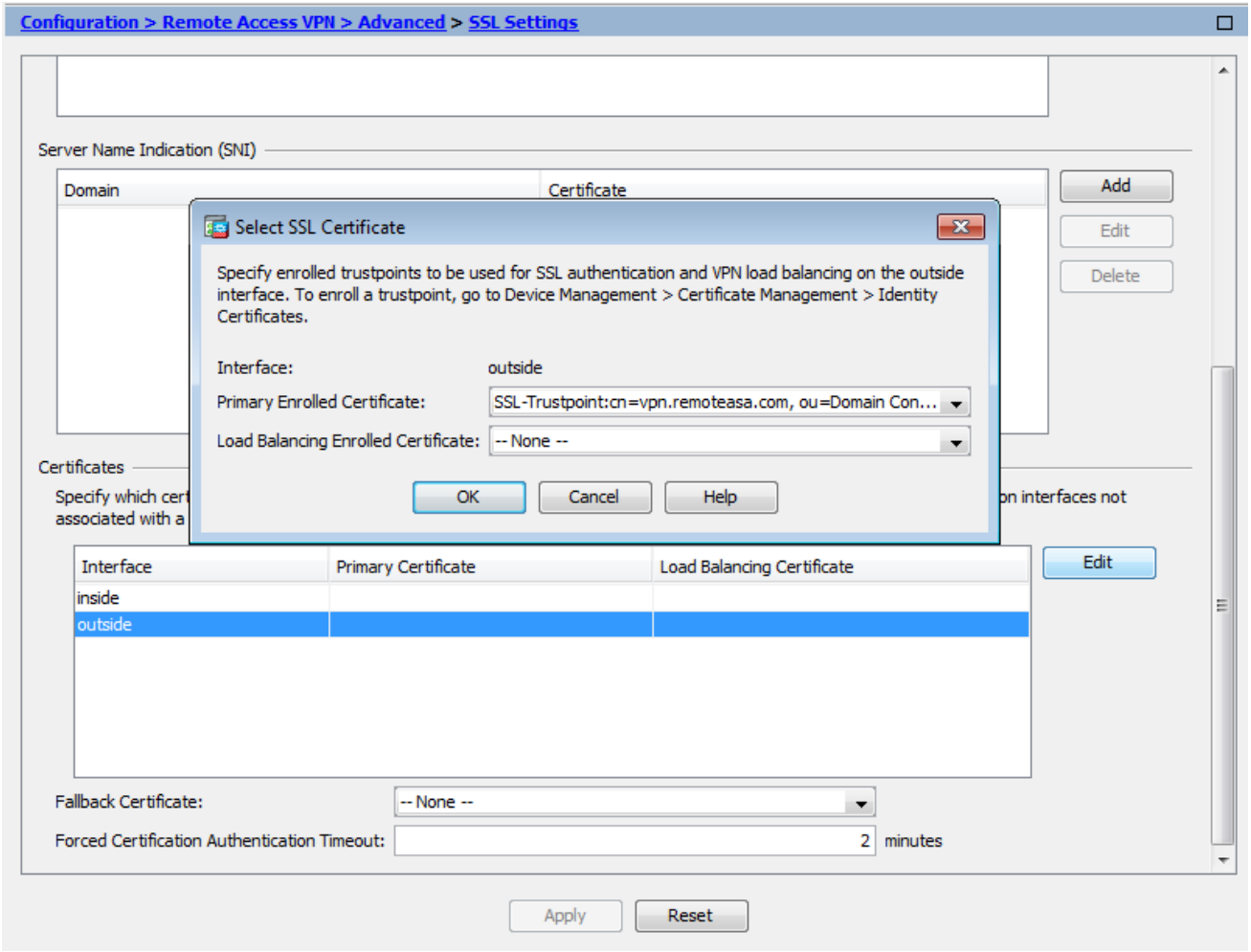


3. Klicken Sie auf **Zertifikat installieren**.
4. Navigieren zu**Configuration > Remote Access VPN > Certificate Management**, und wählen Sie Identitätszertifikate aus.
5. Wählen Sie das zuvor erstellte Identitätszertifikat aus. Klicken Sie auf **Install**.
6. Klicken Sie auf die Option**Install from a file** , und wählen Sie das PEM-kodierte Identitätszertifikat aus. Alternativ können Sie das PEM-kodierte Zertifikat in einem Texteditor öffnen und das Base64-Identitätszertifikat des Fremdherstellers kopieren und in das Textfeld einfügen.





7. Klicken Sie auf **Add Certificate**.
8. Navigieren zu**Configuration > Remote Access VPN > Advanced > SSL Settings**.
9. Wählen Sie unter Certificates (Zertifikate) die Schnittstelle aus, die zum Beenden von WebVPN-Sitzungen verwendet wird. In diesem Beispiel wird die externe Schnittstelle verwendet.
10. Klicken Sie auf **Edit**.
11. Wählen Sie in der Dropdownliste Zertifikat das neu installierte Zertifikat aus.



12. Klicken Sie auf OK.
13. Klicken Sie auf **Apply**. Das neue Zertifikat wird nun für alle WebVPN-Sitzungen verwendet, die auf der angegebenen Schnittstelle enden.

1.2. Installation eines PEM-Zertifikats über die CLI

```
MainASA(config)# crypto ca authenticate SSL-Trustpoint

Enter the base 64 encoded CA certificate. End with the word"quit"on a line by itself

-----BEGIN CERTIFICATE----- MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEh
MB8GA1UEChMYVGhlIEdvIERhZGR5IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBE
YWRkeSBDbGFzcyAyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTA0MDYyOTE3
MDYyMFoXDTM0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRo
ZSBHbyBEYWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3Mg
MiBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTCCASAwDQYJKoZIhvcNAQEBBQADggEN
ADCCAQgCggEBAN6d1+pXGEmhW+vXX0iG6r7d/+TvZxz0ZWizV3GgXne77ZtJ6XCA
PVYYYwhv2vLM0D9/AlQiVBDYsoHUwHU9S3/Hd8M+eKsaA7Ugay9qK7HFiH7Eux6w
wdhFJ2+qN1j3hybX2C32qRe3H3I2TqYXP2WYktsqbl2i/ojgC95/5Y0V4evLOtXi
EqITLdiOr18SPaAIBQi2XKVlOARFmR6jYGB0xUGlcmIbYsUfb18aQr4CUWWoriMY
avx4A6lNf4DD+qta/KFApMoZFv6yyO9ecw3ud72a9nmYvLEHZ6IVDd2gWMZEewo+
YihfukEHU1jPEX44dMX4/7VpkI+EdOqXG68CAQOjgcAwgb0wHQYDVR0OBBYEFNLE
sNKR1EwRcbNhyz2h/t2oatTjMIGNBgNVHSMEgYUwgYKAFNLEsNKR1EwRcbNhyz2h
/t2oatTjoWekZTBjMQswCQYDVQQGEwJVUzEhMB8GA1UEChMYVGhlIEdvIERhZGR5
IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBEYWRkeSBDbGFzcyAyIENlcnRpZmlj
YXRpb24gQXV0aG9yaXR5ggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQAD
ggEBADJL87LKPpH8EsahB4yOd6AzBhRckB4Y9wimPQoZ+YeAEW5p5JYXMP80kWNy
OO7MHAGjHZQopDH2esRU1/blMVgDoszOYtuURXO1v0XJJLXVggKtI3lpjbi2Tc7P
TMozI+gciKqdi0FuFskg5YmezTvacPd+mSYgFFQlq25zheabIZ0KbIIOqPjCDPoQ
```

```
HmyW74cNxA9hi63ugyuV+I6ShHI56yDqg+2DzZduCLzrTia2cyvk0/ZM/iZx4mER
dEr/VxqHD3VILs9RaRegAhJhldXRQLIQTO7ErBBDpqWeCtWVYpoNz4iCxTIM5Cuf ReYNnyicsbkqWletNw+vHX/bvZ8= --
---END CERTIFICATE----- quit INFO: Certificate has the following attributes: Fingerprint:
96c25031 bc0dc35c fba72373 1e1b4140 Do you accept this certificate? [yes/no]: yes Trustpoint
'SSL-Trustpoint' is a subordinate CA and holds a non self-signed certificate. Trustpoint CA
certificate accepted. % Certificate successfully imported
```

!!! - Installing Next-level SubCA in the PKI hierarchy.
!!! - Create a separate trustpoint to install the next subCA certificate (if present)
in the hierarchy leading up to the Root CA (including the Root CA certificate)

```
MainASA(config)#crypto ca trustpoint SSL-Trustpoint-1
MainASA(config-ca-trustpoint)#enrollment terminal
MainASA(config-ca-trustpoint)#exit
MainASA(config)#
MainASA(config)# crypto ca authenticate SSL-Trustpoint-1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself


-----BEGIN CERTIFICATE-----
MIIEfTCCA2WgAwIBAgIDG+cVMA0GCSqGSIb3DQEBCwUAMGMxCzAJBgNVBAYTAlVT
MSEwHwYDVQQKExhUaGUgR28gRGFkZHkgR3JvdXAsIEluYy4xMTAvBgNVBAsTKEdv
IERhZGR5IENsYXNzIDIgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTQwMTAx
MDcwMDAwWhcNMzEwNTMwMDcwMDAwWjCBgzELMAkGA1UEBhMCVVMxEDAOBgNVBAgT
B0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxGjAYBgNVBAoTEUdvRGFkZHku
Y29tLCBJbmMuMTEwLwYDVQQDEyhHbyBEYWRkeSBSb290IENlcnRpZmljYXRlIEF1
dGhvcml0eSAtIEcyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv3Fi
CPH6WTT3G8kYo/eASVjpIoMTpsUgQwE7hPHmhUmfJ+r2hBtOoLTbcJjHMgGxBT4H
Tu70+k8vWTAi56sZVmvigAf88xZ1gDlRe+X5NbZ0TqmNghPktj+pA4P6or6KFWp/
3gvDthkUBcrqw6gElDtGfDIN8wBmIsiNaW02jBEYt9OyHGC0OPoCjM7T3UYH3go+
6118yHz7sCtTpJJiaVElBWEaRIGMLKlDliPfrDqBmg4pxRyp6V0etp6eMAo5zvGI
gPtLXcwy7IViQyU0AlYnAZG0O3AqP26x6JyIAX2f1PnbU21gnb8s51iruF9G/M7E
GwM8CetJMVxpRrPgRwIDAQABo4IBFzCCARMwDwYDVR0TAQH/BAUwAwEB/zAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFDqahQcQZyi27/a9BUFuIMGU2g/eMB8GA1Ud
IwQYMBaAFNLEsNKR1EwRcbNhyz2h/t2oatTjMDQGCCsGAQUFBwEBBCgwJjAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMDIGA1UdHwQrMCkwJ6Al
oCOGIWh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2Ryb290LmNybDBGBgNVHSAEPzA9
MDsGBFUdIAAwMzAxBggrBgEFBQcCARYlaHR0cHM6Ly9jZXJ0cy5nb2RhZGR5LmNv
bS9yZXBvc2l0b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEAWQtTvZKGEacke+1bMc8d
H2xwxbhuvk679r6XUOEwf7ooXGKUwuN+M/f7QnaF25UcjCJYdQkMiGVnOQoWCcWg
OJekxSOTP7QYpgEGRJHjp2kntFolfzq3Ms3dhP8qOCkzpN1nsoX+oYggHFCJyNwq
9kIDN0zmiN/VryTyscPfzLXs4Jlet0lUIDyUGAzHHFIYSaRt4bNYC8nY7NmuHDKO
KHAN4v6mF56ED71XcLNa6R+ghlO773z/aQvgSMO3kwvIClTErF0UZzdsyqUvMQg3
qm5vjLyb4lddJIGvl5echK1srDdMZvNhkREg5L4wn3qkKQmw4TRfZHcYQFHfjDCm
rw==
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint:     81528b89 e165204a 75ad85e8 c388cd68
Do you accept this certificate? [yes/no]: yes

Trustpoint 'SSL-Trustpoint-1' is a subordinate CA and holds a non self-signed certificate.

Trustpoint CA certificate accepted.

% Certificate successfully imported
BGL-G-17-ASA5500-8(config)#
```

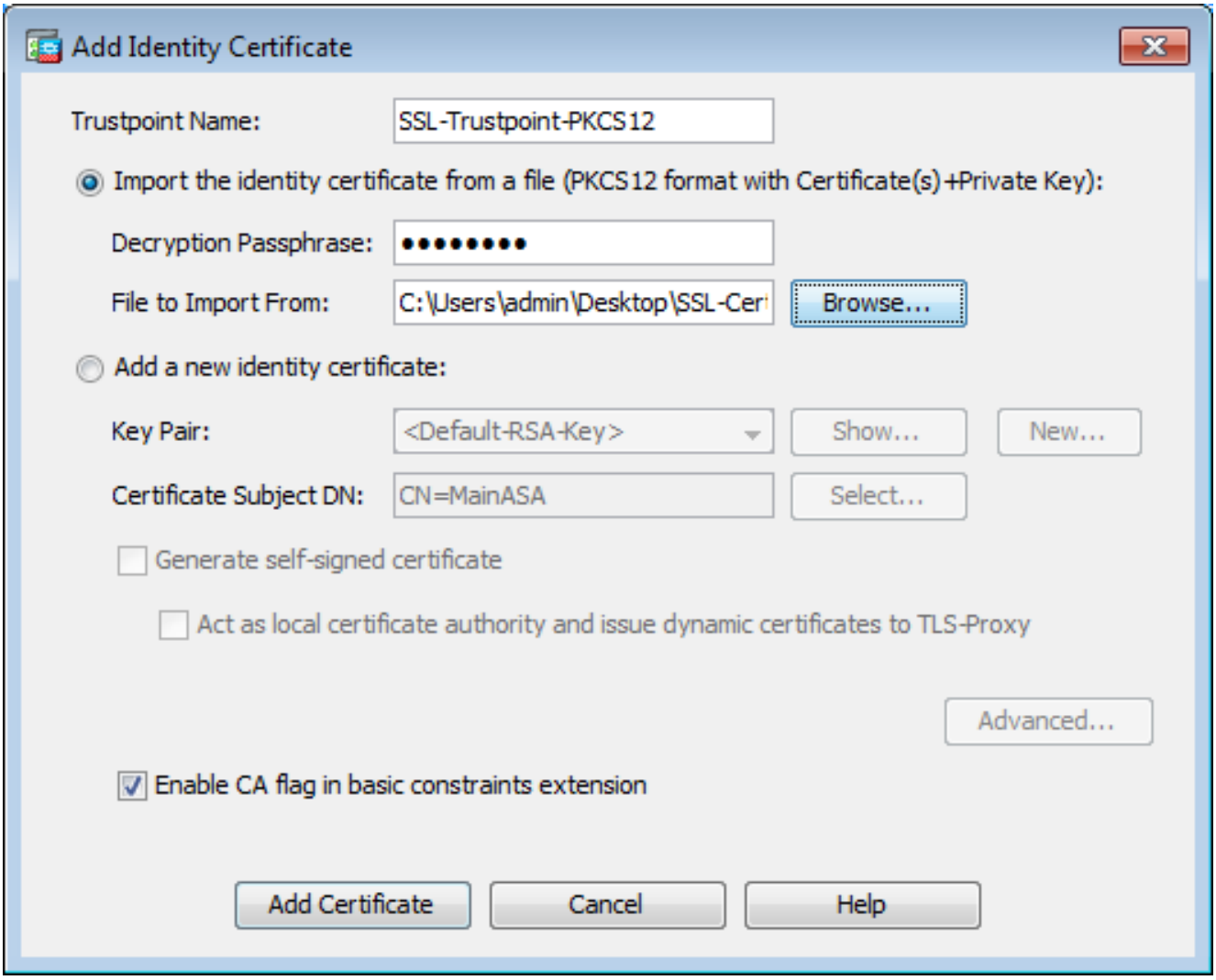
!!! - Similarly create additional trustpoints (of the name "SSL-Trustpoint-n",
where n is number thats incremented for every level in the PKI hierarchy) to
import the CA certificates leading up to the Root CA certificate.

```
!!! - Importing identity certificate (import it in the first trustpoint that was
created namely "SSL-Trustpoint") MainASA(config)# crypto ca import SSL-Trustpoint certificate
WARNING: The certificate enrollment is configured with an fqdn that differs from the system
fqdn. If this certificate will be used for VPN authentication this may cause connection
problems. Would you like to continue with this enrollment? [yes/no]: yes % The fully-qualified
domain name in the certificate will be: vpn.remoteasa.com Enter the base 64 encoded certificate.
End with the word "quit" on a line by itself ----BEGIN CERTIFICATE-----
MIIFRjCCBC6gAwIBAgIIJc1zqYQHBgUwDQYJKoZIhvcNAQELBQAwgbQxCzAJBgNV
BAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY290dHNkYWxlMRow
GAYDVQQKExFHb0RhZGR5LmNvbSwgSW5jLjEtMCsGA1UECxMkaHR0cDovL2NlcnRz
LmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvMTMwMQYDVQQDEypHbyBEYWRkeSBTZWN1
cmUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IC0gRzIwHhcNMTUwNzIyMTIwNDM4WhcN
MTYwNzIyMTIwNDM4WjA/MSEwHwYDVQQLExhEb21haW4gQ29udHJvbCBWYWxpZGF0
ZWQxGjAYBgNVBAMTEXZwbi5yZW1vdGVhc2EuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEArrY2Fv2S2Uq5HdDhOaSzK5Eyok2tv2Rem8DofbTQ+4F9
C9IXitWdLAo6a7dzyfB4S9hx1VZXoHMGGNd6i9NWLXsWU1Nx5pRMaKR4h1cL6bDW
ITt5GzKdL93ibMxYmau+uwM3OkBb8QxLNNxr4G+oXtfavctTxWy/o6LzKWFyj0XP
tta9FZW07c0MNvKiUL1v9WBcy4GK1xyvN9RtWebtVkM5/iOv0ReBTBfFxCJ1YQAG
UWteu1ikWAGj1qomZGnZgAFDWJ4/hxjesG2BGMtwX5L1O8cbmbi/u/vnmZ5Xhiqx <snip>
CCsGAQUFBwIBFitodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHkuY29tL3JlcG9z
aXRvcnkvMHYGCCsGAQUFBwEBBGowaDAkBggrBgEFBQcwAYYYaHR0cDovL29jc3Au
Z29kYWRkeS5jb20vMEAGCCsGAQUFBzAChjRodHRwOi8vY2VydGlmaWNhdGVzLmdv
ZGFkZHkuY29tL3JlcG9zaXRvcnkvZ2RpZzIuY3J0MB8GA1UdIwQYMBaAFEDCvSeO
zDSDMKIz1/tss/C0LIDOMEYGA1UdEQQ/MD2CEXZwbi5yZW1vdGVhc2EuY29tghV3
d3cudnBuLnJlbW90ZWFzYS5jb22CEXZwbi5yZW1vdGVhc2EuY29tMB0GA1UdDgQW
BBT7en7YS3PH+s4z+wTRlpHr2tSzejANBgkqhkiG9w0BAQsFAAOCAQEAO9H8TLNx
2Y0rYdI6gS8n4imaSYg9Ni/9Nb6mote3J2LELG9HY9m/zUCR5yVktra9azdrNUAN
1hjBJ7kKQScLC4sZLONdqG1uTP5rbWR0yikF5wSzgyMWd03kOR+vM8q6T57vRst5
69vzBUuJc5bSu1IjyfPP19z1l+B2eBwUFbVfXLnd9bTfiG9mSmC+4V63TXFxt1Oq
xkGNys3GgYuCUy6yRP2cAUV1lc2tYtaxoCL8yo72YUDDgZ3a4PyO1EvC1FOaUtgv
6QNEOYwmbJkyumdPUwko6wGOC0WLumzv5gHnhil68HYSZ/4XIlp3B9Y8yfG5pwbn 7puhazH+xgQRdg== -----END
CERTIFICATE----- quit INFO: Certificate successfully imported ! Apply the newly installed SSL
certificate to the interface accepting SSL connections MainASA(config)# ssl trust-point SSL-
Trustpoint outside
```

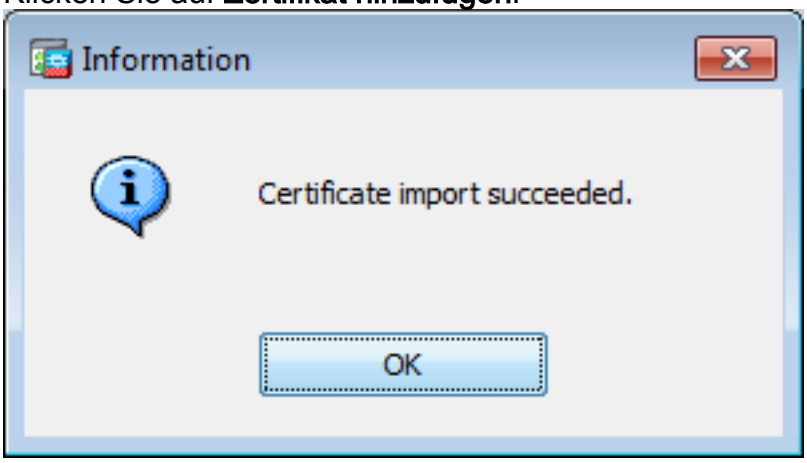
2.1 Installation eines PKCS12-Zertifikats mit ASDM

In Fällen, in denen der CSR nicht auf der ASA generiert wird, z. B. im Fall eines Platzhalterzertifikats oder wenn ein UC-Zertifikat generiert wird, kann ein Identitätszertifikat zusammen mit dem privaten Schlüssel als separate Dateien oder eine einzelne gebündelte PKCS12-Datei (p12- oder pfx-Format) empfangen werden. Führen Sie die folgenden Schritte aus, um diesen Zertifikatstyp zu installieren.

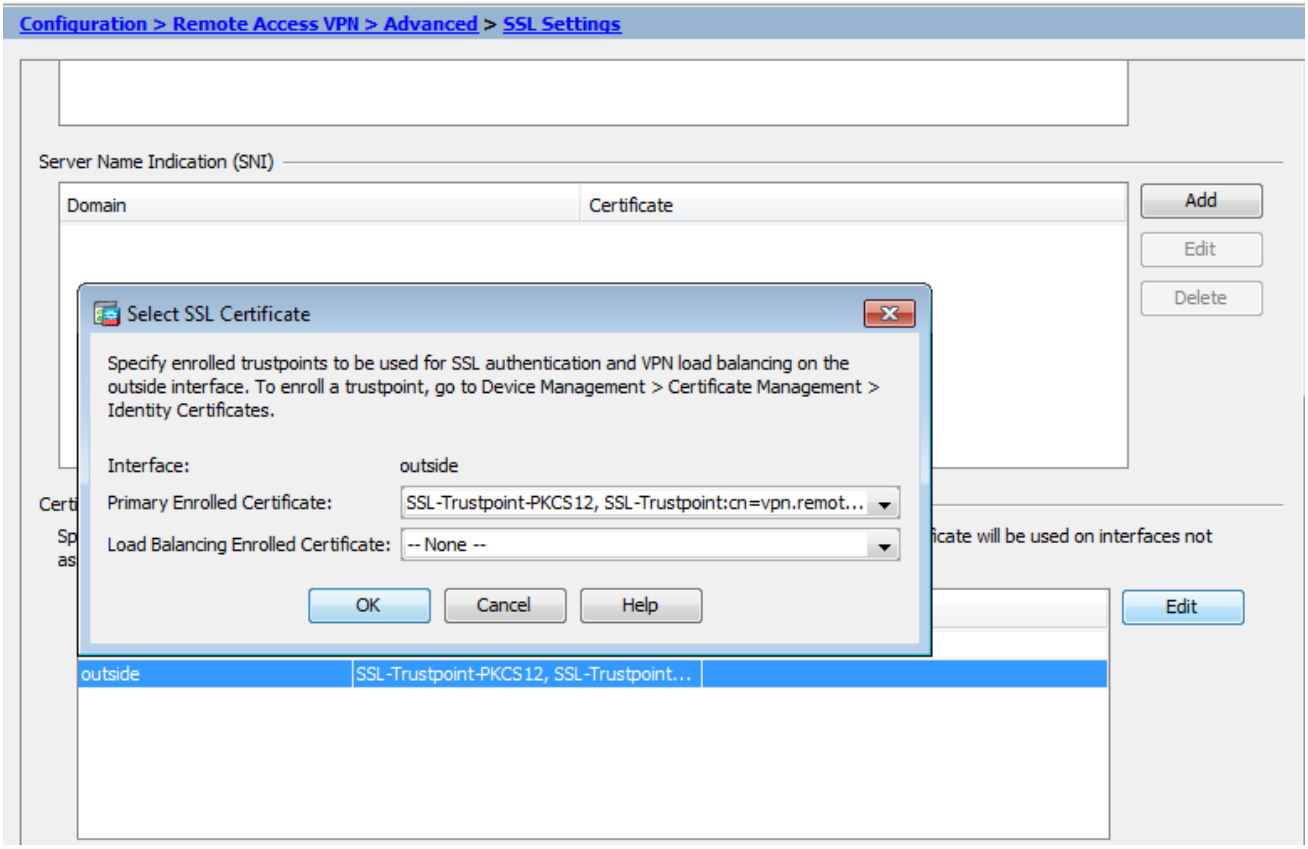
1. Das Identitätszertifikat, bündeln Sie das Zertifizierungsstellenzertifikat und den privaten Schlüssel in einer einzigen PKCS12-Datei. Anhang B enthält die erforderlichen Schritte für OpenSSL. Wenn die CA bereits gebündelt ist, fahren Sie mit dem nächsten Schritt fort.
2. Navigieren zu**Configuration > Remote Access VPN > Certificate Management,** und wählen **Identity Certificates.**
3. Klicken Sie auf **Add**.
4. Geben Sie einen Trustpoint-Namen an.
5. Klicken Sie auf **Import the identity certificate from a file**ein.
6. Geben Sie die Passphrase ein, die zum Erstellen der PKCS12-Datei verwendet wird. Durchsuchen und wählen Sie die PKCS12-Datei aus. Geben Sie die Passphrase des Zertifikats ein.



7. Klicken Sie auf **Zertifikat hinzufügen**.



8. Navigieren zu**Configuration > Remote Access VPN > Advanced**, und wählen Sie **SSL Settings.**
9. Wählen Sie unter Certificates (Zertifikate) die Schnittstelle aus, die zum Beenden von WebVPN-Sitzungen verwendet wird. In diesem Beispiel wird die externe Schnittstelle verwendet.
10. Klicken Sie auf **Edit**.
11. Wählen Sie in der Dropdownliste Zertifikat das neu installierte Zertifikat aus.



12. Klicken Sie auf **OK**.
13. Klicken Sie auf **Apply**. Das neue Zertifikat wird nun für alle WebVPN-Sitzungen verwendet, die auf der angegebenen Schnittstelle enden.

2.2 Installation eines PKCS12-Zertifikats mit CLI

```
  MainASA(config)# crypto ca trustpoint SSL-Trustpoint-PKCS12
MainASA(config-ca-trustpoint)# enrollment terminal
MainASA(config-ca-trustpoint)# exit

MainASA(config)# crypto ca import SSL-Trustpoint-PKCS12 pkcs12 cisco123

Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
-----BEGIN PKCS12-----
MIISNwIBAzCCEfEGCSqGSIb3DQEHAaCCEeIEghHeMIIR2jCCEdYGCSqGSIb3DQEH
BqCCEccwghHDAgEAMIIRvAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIWO3D
hDti/uECAQGAghGQ9ospee/qtIbVZh2T8/Z+5dxRPBcStDTqyKy7q3+9ram5AZdG
Ce9n5UCckqT4WcTjs7XZtCrUrt/LkNbmGDVhwGBmYWiOS7npgaUq0eoqiJRK+Yc7
LN0nbho6I5WfL56/JiceAMlXDLr/IqqLg2QAApGdN+F5vANsHse2GsAATewBDLt7
Jy+SKfoNvvIw9QvzCiUzMjYZBANmBdMCQ13H+YQTHitT3vn2/iCDlzRSuXcqypEV
q5e3heiOO75lE8TDLWmO3PMvwIZqi8yzWesjcTt1Kd4FoJBZpB70/v9LntoIUOY7
kIQM8fHb4ga8BYfbgRmG6mkMmO1STtbSvlvTa19WTmdQdTyCa+G5PkrryRsy3Ww1
lkGFMhImmrnNADF7HmzbyslVohQZ7h09iVQY9krJogoXHjmQYxG9brf0oEwxSJDa
mGDhhESh+s/WuFSV9Z9kiTXpJNZxpTASoWBQrrwmO5v8ZwbjbVNJ7sVdbwpUl6d+
NNFGR7LTqO8hpupeeJnY9eJc2yYqeAXWXQ5kLOZo6/gBEdGtEaZBgCFK9JZ3bl3A
xqxGifanWPnLYG611NKuNjTgbjhnEEYI2uZzU0qxnlKa8zyXw+lzrKuJscDbkAPZ
wKtw8K+p4OzXVHhuANo6MDvffNRY1KQDtyK1inoPH5ksVSE5awkVam4+HTcqEUfa
16LMana+4QRgSetJhU0LtSMaQfRJGkha4JLq2t+JrCAPz2osARlTsBOjQBNq6YNj
0uB+gGk2Gl8Q5Nln6K1fz0XBFZLWEDBLsaBRO5MAnE7wWtO0+4awGYqVdmIF1lkf
XIRKAiQEr1pZ6BVPuvsCNJxaaUHzufhYI2ZAckasKBZOT8/7YK3fnAaGoBCz4cHa
o2EEQhq2aYb6YTv0+wtLEWGHzsbGZEM/u54XmsXAI7g28LGJYdfWi509KyV+Ac1V
KzHqXZMM2BbUQCNcTF5JIMiW+r62k42FdahfaQb0vJsIe/IwkAKG7y6DIQFs0hwg
ZlPXiDbNr1k4e8L4gqupMKWg853PY+oY22rLDC7bul1CKtixIYBCvbn7dAYsI4GQ
```

l6xXhNu3+iye0HgbUQQCfTU/mBrA0ZO+bpKjWOCfqNBuYnZ6kUEdCI7GFLH9QqtM
K7YinFLoHwTWbi3MsmqVv+Z4ttVWy7XmikoO2nMynJMP6/CNV8OMxMKdC2qm+c1j
s4QlKcAmFsQmNp/7SIP1wnvOc6JbUmC1O520U/r8ftTzn8C7WL62W79cLK4HOr7J
sNsZnOz0JOZ/xdZT+cLTCtVevKJOQMK3vMsiOuy52FkuF3HnfrmBqDkbR7yZxELG
RCEL0EDdbp8VP0+IhNlyz1q7975SscdxFSL0TvjnHGFWd14ndoqN+bLhWbdPjQWV
l3W2NCI95tmHDLGgp3P0OlS+RjdCEGGMg+9cpgBfFC1JocuTDIEcUbJBY8QRUNiS
/ubyUagdzUKt1ecfb9hMLP65ZNQ93VIw/NJKbIm7b4P/1Zp/lFP5eq7LkQPAxE4/
bQ4mHcnwrs+JGFkN19B8hJmmGoowH3p4IEvwZy7CThB3E1ejw5R4enqmrgvHqpQe
B7odN1OFLAHdo1G5BsHExluNEsEb4OQ0pmKXidDB5B001bJsr748fZ6L/LGx8Al3
<snip>
ijDqxyfQXY4zSytljSMwMtYA9hG5I79Sg7pnME1E9xq1DOoRGg8vgxlwiciKtLxp
LL0ReDY31KRYv00vW0gf+tE7lST/3TKZvh0sQ/BE0V3kHnwldejMFH+dvyAA9Y1E
c8O+tdafBFX4B/HP46E6heP6ZSt0xAfRW1/JF4ljNvUNVO9VtVfR2FTyWpzZFY8A
GG5XPIA80WF6wKEPFHIcN8scY+Vot8kXxG96hwt2Cm5NQ2OnVzxUZQbpKsjs/2jC
3HVFe3UJFBsY9UxTLcPXYBSIG+VeqkI8hWZp6clTfNDLY2ELDylQzp1mBg2FujZa
YuE0avjCJzBzZUG2umtS5mHQnwPF+XkOujEyhGMauhGxHp4nghSzrUZrBeuL9lUF
2mbpsOcgZkzxMS/rjdNXjCmPFloRBvKkZSlxHFrE/5ZopAhn4i7YtHQNrz9U4RjQ
xo9cUuaJ+LNmvzE8Yg3epAMYZ16UNGQQkVQ6ME4BcjRONzW8BYgTq4+pmT1ZNq1P
X87CXCPtYRpHF57eSo+tHDINCgfqYXD6e/7r2ngfiCeUeNDZ4aVl2XxvZDaUlBPP
Tx5fMARqx/Z8BdDyBJDVBjdsxmQau9HLkhPvdfGlZIWdTe13CzKqXA5Ppmpjt4q9
GnCpC53m76x9Su4ZDw6aUdBcgCTMvfaqJC9gzObee2Wz+aRRwzSxu6tEWVZolPEM
v0AA7po3vPeklgOnLRAwEoTTn4SdgNLWeRoxqZgkw1FC1GrotxF1so7uA+z0aMeU
lw73reonsNdZvRAcVX3Y6UNFdyt70Ixvo1H4VLzWm0K/oP62C9/eqqMwZ8zoCMPt
ENna7T+7Os66SCbMmXCHwyhO0tygNKZFFw/AATFyjqPMWPAxGuPNOrnB6uYCn0Hk
1BU7tF143RNIZaQQEH3XnaPvUuAA4C0FCoE3h+/tVjtfNKDvFmb6ZLZHYQmUYpyS
uhdFEpoDrJH1VmI2Tik/iqYWaZ+oDqXPHQXnJhw25h9ombR4qnD+FCfwFCGtPFON
o3QffZ53C95n5jPHVMyUrOxDdpwnvzCQPdj6yQm564TwLAmiz7uDlpqJZJe5QxHD
nolv+4MdGSfVtBq+ykFoVCaamqeaq6sKgvAVujLXXEs4KEmIgcPqATVRG49ElndI
LO1DEQyKhVoDGebAuVRBjzwAm/qxWxxFv3hrbCjpHCwEYms4Wgt/vKKRFsuWJNZf
efHldwlltkd5dKwSvDocPT/7mSLtLJa94c6AfgxXy9zO+FTLDQwzxga7xC2krAN1
yHxR2KHN5YeRL+KDzu+u6dYoKAz+YAgwlW6KbeavALSuH4EYqcvg8hUEhp/ySiSc
RDhuygxEovIMGfES4FP5V52lPyDhM3Dqwhn0vuYUmYnX8EXURkay44iwwI5HhqYJ
lptWyYo8Bdr4WNwt5xqszGzYR6mmGeAIin7bDunsF1uBHWYF4dyKlz1tsdRNMYqQ
+W5q+QjVdrjldWv/bMFOaqEjxeNWBRqjzcff3BxMnwvVxtgqxFvRh+DZxiJoiBG+
yx7x8np2AQ1r0METSSxbnZzfnKZKVvBVMkIC6Jsmt2WEVTQvoFJ8em+nemOWgTi/
hHSBzjE7RhAucnHuifOCXOgvR1SDDqyCQbiduc1QjXN0svA8Fqbea9WEH5khOPv3
pbtsL4gsfl2pv8diBQkVQgiZDi8Wb++7PR6ttiY65kVwrdsoNl1/qq+xWOd3tB4/
zoH9LEMgTy9Sz7myWrB9EOOZ8BIjL1M8oMigEYrTDOc3KbyW1S9dd7QAxiuOBaX1
8J8q1OydvTBzmqcjeSsFH4/1NHn5VnfOZnNpui4uhpOXBG+K2zJUJXm6dq1AHBlE
KQFsFZpNNyave0Kk8JzQnLAPd7OUU/IksyOCGQozGBH+HSzVp1RDjrrbC342rkBj
wnI+j+/1JdWBmHdJMZCfoMZFLSI9ZBqFirdii1/NRu6jh76TQor5TnNjxIyNREJC
FE5FZnMFvhM900LaiUZff8WWCOfeRDMttLXb1nuxPFl+lRk+LNlPLVptWgcxzfsr
JXrGiwjxybBB9oCOrACq8fGAtEs8WRxJyDH3Jjmn9i/Gl6J1mMCUF//LxAH2WQx8
Ld/qS5OM2iFCffDQjxAj0K6DEN5pUebBv1Em5SOHXvyq5nxgUh4/y84CWaKjw0MQ
5tbbLMlnc7ALIJ9LxZ97YiXSTyeM6oBXBFx6RpklkDv05mlBghSpVQiMcQ2ORIkh
UVVNbSHOl9S3cb5wqxaWqAKBqb4h1uLGVbYWZf2mzLZ8U5U5ioiqoMBqNZbzTXpO
EqEFuatTllQvCRbcKS3xou4MAixcYUxKwEhbZA/6hd10XSBJwe7jKBV9M6wliKab
UfoJCGTAf3sY68lqrMPrbBt0eeWf1C02Sd9Mn+V/jvnil7mxYFFUpruRq3r1LeqP
J5camfTtHwyL8N3Q/Zwp+zQeWZiLA8a/iAVu/hYLR1bpF2WCK0lOtJqkvVmrLVLz
maZZjbJeOft5cP/lRxbKlS6Gd5dFTEKDE15c6gWUX8RKZP6Q7iaE5hnGmQjm8Ljl
kXwF+ivoxOQ8a+Gg1bVTROc7tqW9e9/ewisV1mwvEB6Ny7TDS1oPUDHM84pY6dqi
1+Oio07Ked4BySwNlYy9yaJtBTZSCstfP+ApLidN7pSBvvXf1aHmeNbkPOZJ+c+t
fGpUdL6V2UTXfCsOPHTC0ezA15sOHwCuPchrDIj/eGUwMS3NfS25XgcMuvnLqGVO
RzcRzlZIg8G0oLYwOCuzoY0D/m9010O1ahePyA9tmVB7HRRbytLdaW7gYeEikoCv
7qtBqJFF17ntWJ3EpQHZUcVClbHIKqjNqRbDCY7so4AlIW7kSEUGWMIUDhprE8Ks
NpnvPH2i9JrYrTeROyUI0tL/7SATd2P0a2lxz/zUWekeqd0bmVCsAgQNbB2XkrR3
XS0B52ol+63e8KDqS2zL2TZd3daDFidHlB8QB26tfbfOAcaObJH5/dWP8ddo8UYo
Y3JqTl0malxSJhaMHmQdZIQp49utW3TcjqGllYS4HEmcqtHud0ShaUysC6239jlQ
KlFWrwXTlBC5vnq5IcOMqx5zyNbfxXz28969cWoMCyU6+kRw0TyF6kF7EEv6XWca
XLEwABx+tKRUKHJ673SyDMu96KMV3yZN+RtKbCjqCPVTP/3ZeIp7nCMUcj5sW9HI
N34yeI/0RCLyeGsOEiBLkucikC32LI9ik5HvImVTELQ0Uz3ceFqU/PkasjJUve6S
/n/1ZVUHbUk71xKR2bWZgECl7fIel7wlrbjpF3Wbk+Er0kfYcsNRHxeTDpKPSt9s
u/UsyQJiyNARG4X3iYQlsTce/06Ycyri6GcLHAu58B02nj4CxolCplABZ2N79HtN
/7Kh5L0pS9MwsDCHuUI8KFrTsET7TB1tIU99FdB19L64sl/shYAHbccvVWU50Wht

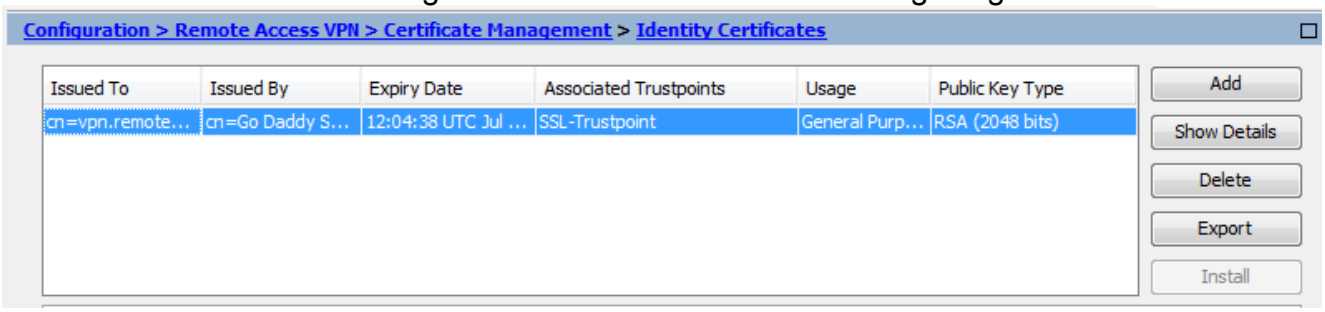
```
PdLoaErrX81Tof41IxbSZbI8grUC4KfG2sdPLJKu3HVTeQ8LfllbBLxfs8ZBS+Oc
v8rHlQ012kY6LsFGLehJ+/yJ/uvXORiv0ESp4EhFpFfkp+o+YcFeLUUPd+jzb62K
HfSCCbLpCKyEay80dyWkHfgylqxmb9ud0oMO50aFJyqR0NjNt6pcxBRY2A6AJR5S
IIC26YNwbh0GjF9qL2FiUqnNH/7GTqPnd2qmsB6FTIwSBT6d854qN7PRt+ZXgdtQ
OjcYt1r9qpWDZpNFK8EzizwKiAYTsiEh2pzPt6YUpksRb6CXTkIzoG+KLsv2m3b8
OHyZ9a8z81/gnxrZlls5SCTfOSU70pHWh8VAYKVHHK+MWgQr0m/2ocV32dkRBLMy
2R6P4WfHyI/+9de1x3PtIuOiv2knpxHv2fKM6sQw45F7XkmwHxjq1YRJ6vIwPTAh
MAkGBSsOAwIaBQAEFFTRETzpisHKZR+Kmen68VrTwpV7BBSQi0IesQ4n4E/bSVsd
qJSzcwh0hgICBAA=
-----END PKCS12-----
quit
INFO: Import PKCS12 operation completed successfully

!!! Link the SSL trustpoint to the appropriate interface MainASA(config)# ssl trust-point SSL-
Trustpoint-PKCS12 outside
```

Überprüfung

Führen Sie diese Schritte aus, um die erfolgreiche Installation des Drittanbieter-Zertifikats und die Verwendung für SSL VPN-Verbindungen zu überprüfen.

Anzeigen vorhandener Zertifikate über ASDM

1. Navigieren zu**Configuration > Remote Access VPN > Certificate Management,**und wählen **Identity Certificates.**
2. Das vom Fremdhersteller ausgestellte Identitätszertifikat wird angezeigt.



Anzeigen vorhandener Zertifikate über die CLI

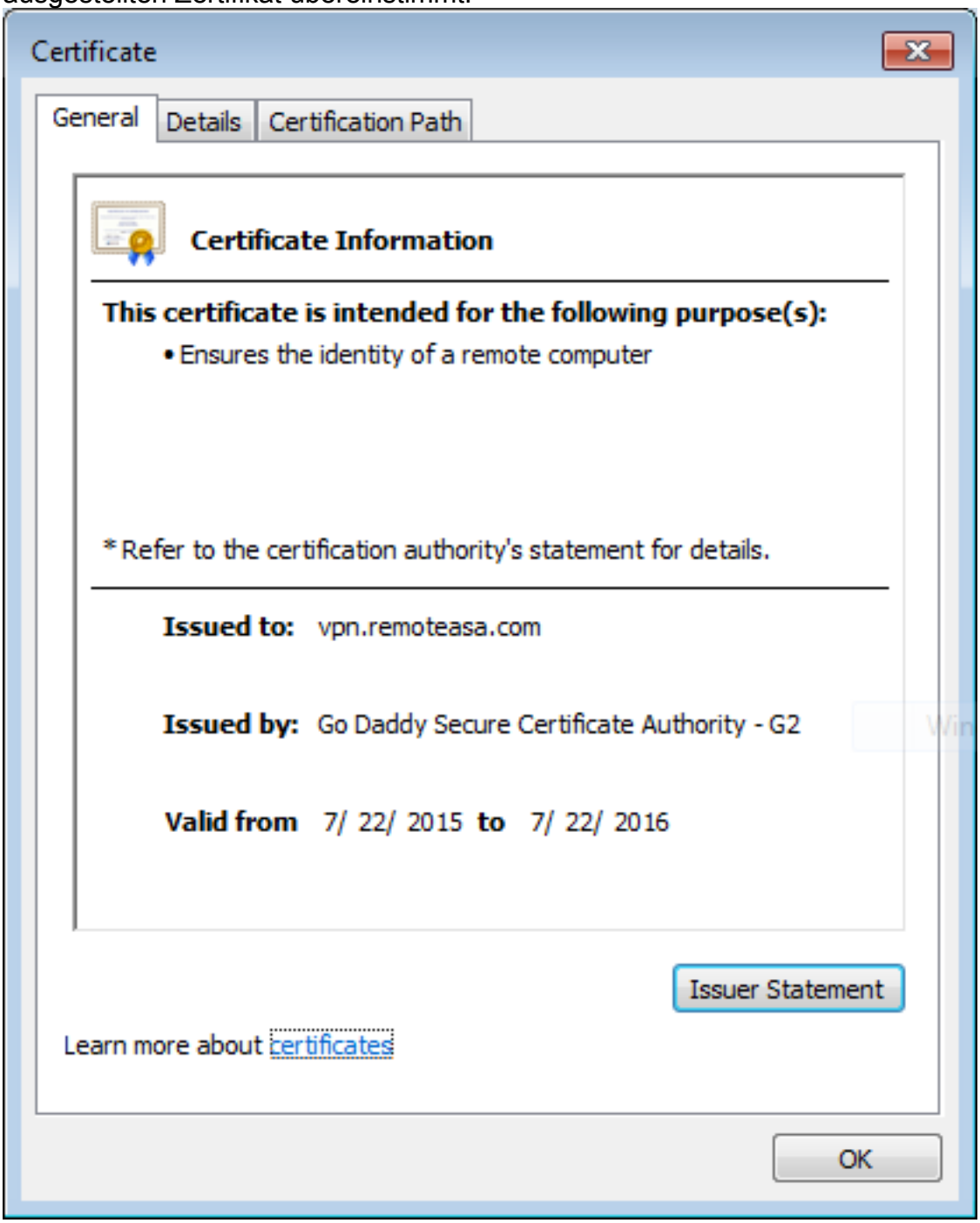
```
 MainASA(config)# show crypto ca certificate

Certificate
  Status: Available
  Certificate Serial Number: 25cd73a984070605
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject Name:
    cn=vpn.remoteasa.com
    ou=Domain Control Validated
  OCSP AIA:
```

```
    URL: http://ocsp.godaddy.com/
  CRL Distribution Points:
    [1]  http://crl.godaddy.com/gdig2s1-96.crl
  Validity Date:
    start date: 12:04:38 UTC Jul 22 2015
    end   date: 12:04:38 UTC Jul 22 2016
  Associated Trustpoints: SSL-Trustpoint

CA Certificate
  Status: Available
  Certificate Serial Number: 07
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=Go Daddy Root Certificate Authority - G2
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject Name:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
    c=US
  OCSP AIA:
    URL: http://ocsp.godaddy.com/
  CRL Distribution Points:
    [1]  http://crl.godaddy.com/gdroot-g2.crl
  Validity Date:
    start date: 07:00:00 UTC May 3 2011
    end   date: 07:00:00 UTC May 3 2031
  Associated Trustpoints: SSL-Trustpoint

CA Certificate
 Status: Available
 Certificate Serial Number: 1be715
 Certificate Usage: General Purpose
 Public Key Type: RSA (2048 bits)
 Signature Algorithm: SHA256 with RSA Encryption
 Issuer Name:
   ou=Go Daddy Class 2 Certification Authority
   o=The Go Daddy Group\, Inc.
   c=US
 Subject Name:
   cn=Go Daddy Root Certificate Authority - G2
   o=GoDaddy.com\, Inc.
   l=Scottsdale
   st=Arizona
   c=US
 OCSP AIA:
   URL: http://ocsp.godaddy.com/
 CRL Distribution Points:
   [1]  http://crl.godaddy.com/gdroot.crl
 Validity Date:
   start date: 07:00:00 UTC Jan 1 2014
   end   date: 07:00:00 UTC May 30 2031
 Associated Trustpoints: SSL-Trustpoint-1

...(and the rest of the Sub CA certificates till the Root CA)
```

Überprüfen des installierten Zertifikats für WebVPN mit einem Webbrowser

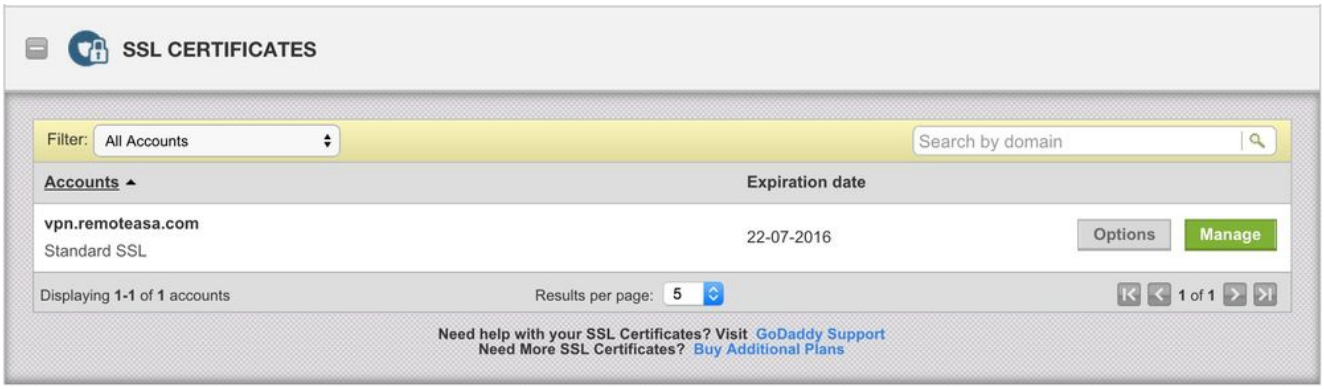
Überprüfen Sie, ob WebVPN das neue Zertifikat verwendet.

1. Stellen Sie über einen Webbrowser eine Verbindung zur WebVPN-Schnittstelle her. Verwenden Sie https:// zusammen mit dem FQDN, der zum Anfordern des Zertifikats verwendet wird (z. B. https://vpn.remoteasa.com).
2. Doppelklicken Sie auf das Sperrsymbol, das in der rechten unteren Ecke der WebVPN-Anmeldeseite angezeigt wird. Die Informationen zum installierten Zertifikat müssen angezeigt werden.
3. Überprüfen Sie den Inhalt, um sicherzustellen, dass er mit dem vom Fremdhersteller ausgestellten Zertifikat übereinstimmt.

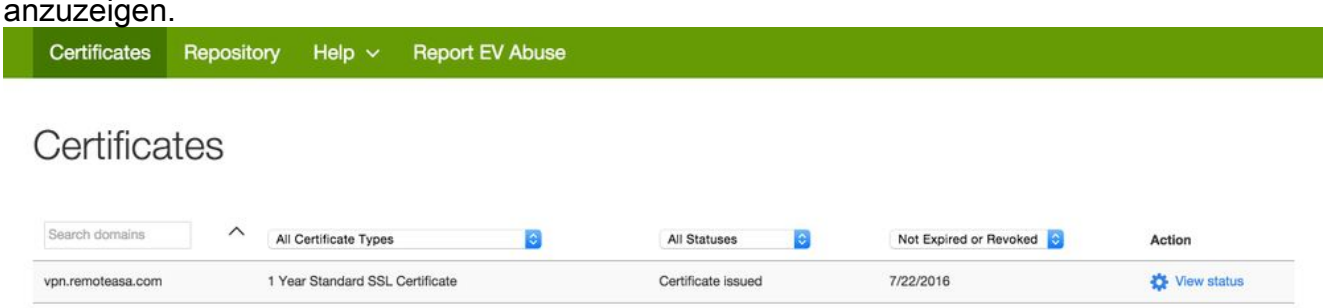


Verlängern Sie das SSL-Zertifikat auf der ASA

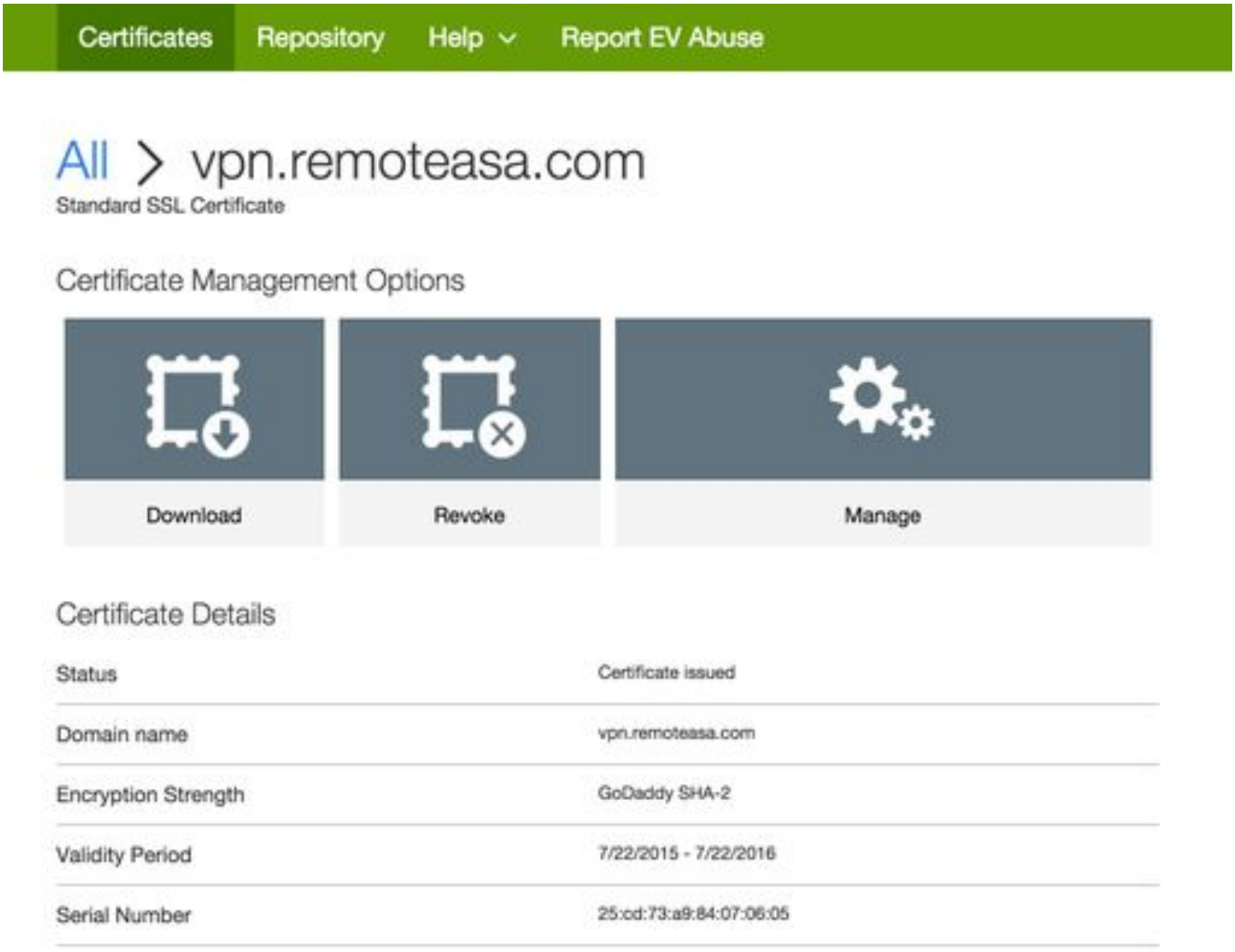
1. Regeneriert die CSR entweder auf der ASA, mit OpenSSL oder auf der CA mithilfe der gleichen Attribute wie das alte Zertifikat. Befolgen Sie die Schritte unter CSR Generation.
2. Senden Sie die CSR-Anfrage an die CA, und generieren Sie ein neues Identitätszertifikat im PEM-Format (.pem, .cer, .crt) zusammen mit dem Zertifizierungsstellenzertifikat. Im Falle eines PKCS12-Zertifikats gibt es auch einen neuen privaten Schlüssel. Bei GoDaddy CA kann das Zertifikat mit einem neuen CSR neu verschlüsselt werden.Wechseln Sie zum GoDaddyaccount, und klicken Sie unter SSL-Zertifikate **auf Verwalten**.



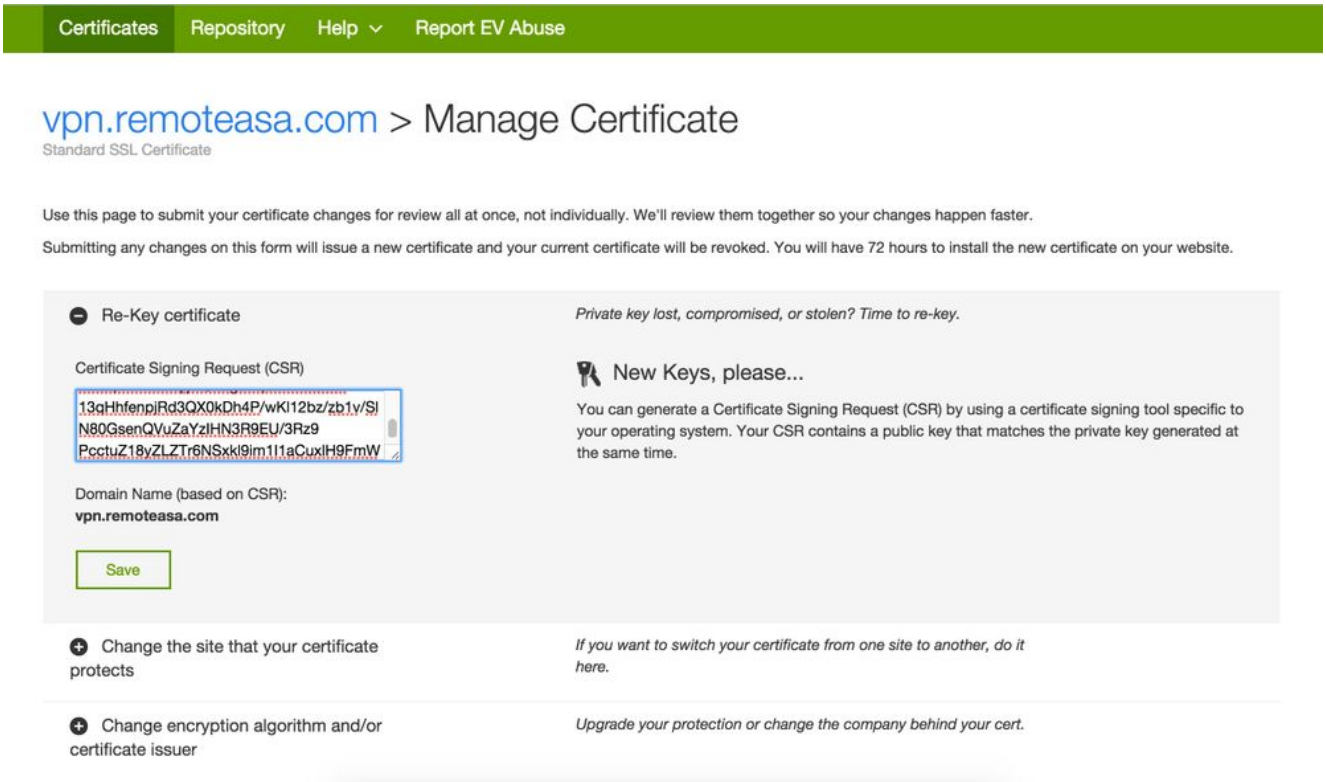
Klicken Sie auf **Status anzeigen**, um den gewünschten Domänennamen anzuzeigen.



Klicken Sie auf **Verwalten**, um Optionen für die erneute Schlüssel des Zertifikats anzugeben.



Erweitern Sie die Option **Re-Key Certificate**, und fügen Sie den neuen CSR hinzu.



Speichern und mit dem nächsten Schritt fortfahren. GoDaddy wird ein neues Zertifikat auf Basis der bereitgestellten CSR-Anfrage ausstellen.

3. Installieren Sie das neue Zertifikat auf einem neuen Trustpoint, wie im Abschnitt "Installation des SSL-Zertifikats" im ASA-Abschnitt gezeigt.

Häufig gestellte Fragen

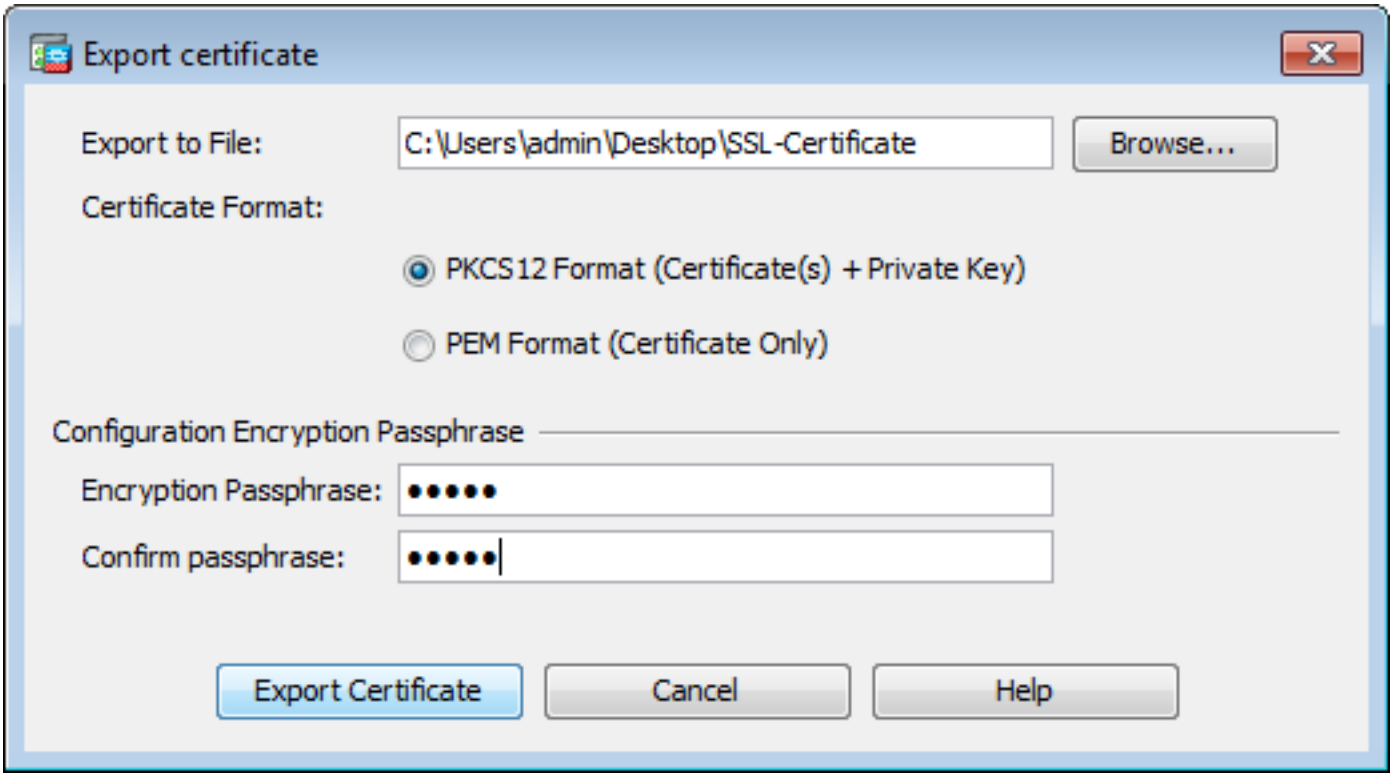
1. Wie können Identitätszertifikate am besten von einer ASA auf eine andere ASA übertragen werden?

Exportieren Sie das Zertifikat zusammen mit den Schlüsseln in eine PKCS12-Datei.

Verwenden Sie diesen Befehl, um das Zertifikat über die CLI von der ursprünglichen ASA zu exportieren:

```
ASA(config)#crypto ca export
```

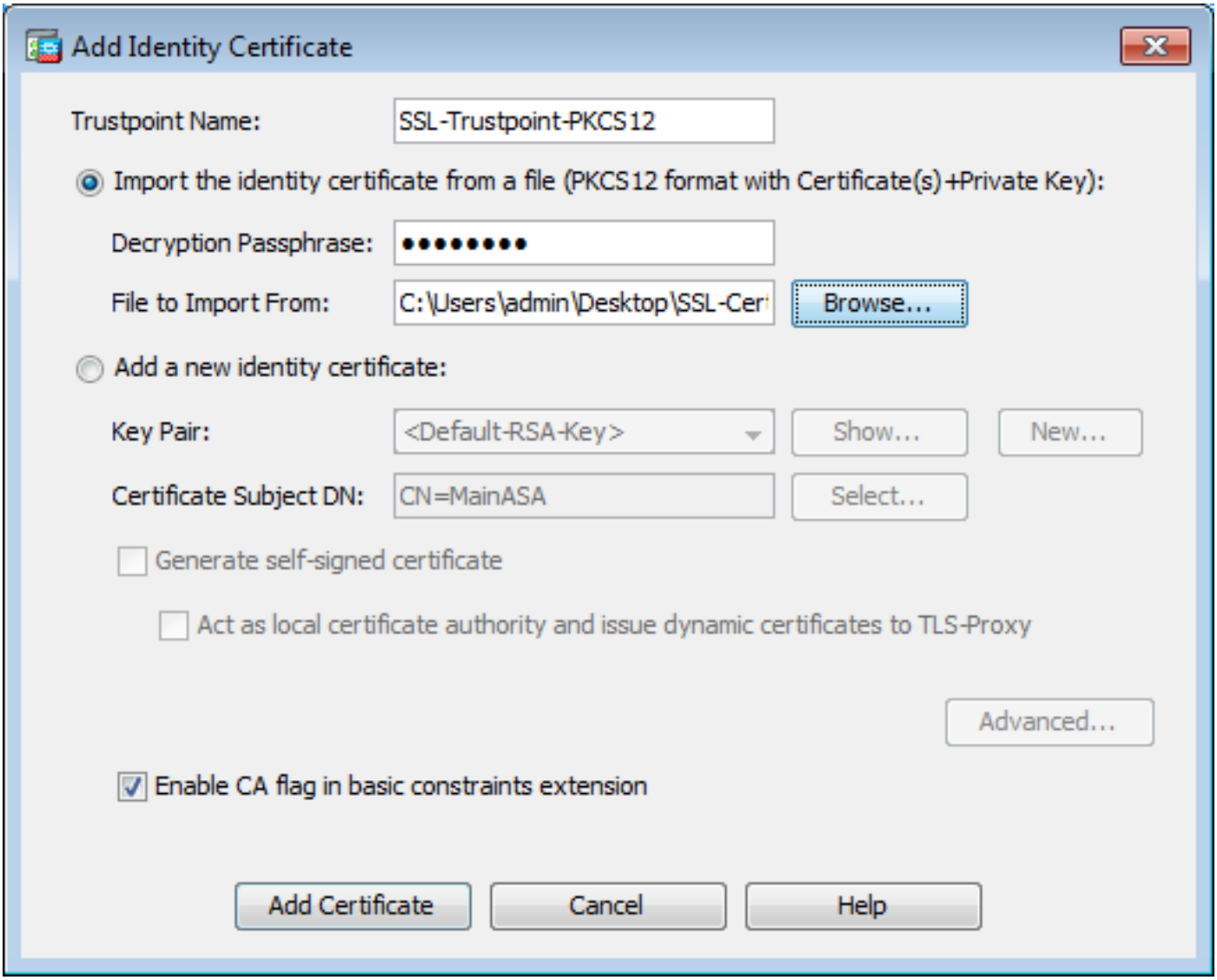
Entsprechende ASDM-Konfiguration:



Verwenden Sie diesen Befehl, um das Zertifikat über die CLI in die Ziel-ASA zu importieren:

```
ASA(config)#crypto ca import
```

Entsprechende ASDM-Konfiguration:



Dies kann auch über die Backup/Restore-Funktion im ASDM mit den folgenden Schritten erfolgen:

1. Melden Sie sich über ASDM bei der ASA an, und wählen Sie**Tools > Backup Configuration**.
2. Sichern Sie alle Konfigurationen oder nur die Identitätszertifikate.
3. Öffnen Sie auf der Ziel-ASA das ASDM, und wählen Sie**Tools > Restore Configuration.**

2. Wie werden SSL-Zertifikate für die Verwendung mit VPN Load Balancing-ASAs generiert?

Es gibt mehrere Methoden, um ASAs mit SSL-Zertifikaten für eine VPN-Lastenausgleichsumgebung einzurichten.

1. Verwenden Sie ein einzelnes Unified Communications/Multiple Domains Certificate (UCC), das den Lastenausgleich-FQDN als DN und jeden ASA FQDN als separaten Subject Alternative Name (SAN) aufweist. Es gibt mehrere bekannte CAs wie GoDaddy, Entrust, Comodo und andere, die solche Zertifikate unterstützen. Bei der Auswahl dieser Methode ist zu beachten, dass die ASA derzeit die Erstellung eines CSR mit mehreren SAN-Feldern nicht unterstützt. Dies wurde in der Erweiterung Cisco Bug ID CSCso70867 dokumentiert. In diesem Fall gibt es zwei Optionen zum Generieren der CSR Über die CLI oder ASDM. Wenn der CSR an die CA übermittelt wird, fügen Sie die verschiedenen SANs im CA-Portal selbst hinzu.Verwenden Sie OpenSSL, um den CSR zu generieren und mehrere SANs in die Datei

openssl.cnf einzubinden.Nachdem die CSR-Anfrage an die Zertifizierungsstelle gesendet wurde und das Zertifikat generiert wurde, importieren Sie dieses PEM-Zertifikat an die ASA, die die CSR-Anfrage generiert hat. Exportieren und importieren Sie anschließend dieses Zertifikat im PKCS12-Format auf die anderen ASAs der Mitgliedsstaaten.
2. Verwenden eines Wildcard-Zertifikats Im Vergleich zu einem UC-Zertifikat ist dies eine weniger sichere und flexible Methode. Falls die CA keine UC-Zertifikate unterstützt, wird entweder auf der CA oder mit OpenSSL eine CSR-Nummer generiert, wobei der FQDN auf dem Formular *.domain.com steht. Nachdem die CSR-Anfrage an die CA gesendet und das generierte Zertifikat gesendet wurde, importieren Sie das PKCS12-Zertifikat in alle ASAs im Cluster.
3. Verwenden Sie ein separates Zertifikat für jede der angeschlossenen ASAs und das für den Lastenausgleichs-FQDN. Dies ist die am wenigsten effektive Lösung. Die Zertifikate für die einzelnen ASAs können wie in diesem Dokument gezeigt erstellt werden. Das Zertifikat für den VPN Loadbalancing FQDN wird auf einer ASA erstellt und als PKCS12-Zertifikat exportiert und in die anderen ASAs importiert.

3. Müssen die Zertifikate von der primären ASA in ein ASA-Failover-Paar auf die sekundäre ASA kopiert werden?

Es ist nicht erforderlich, die Zertifikate manuell von der primären auf die sekundäre ASA zu kopieren, da die Zertifikate zwischen den ASAs synchronisiert werden sollten, solange Stateful Failover konfiguriert ist. Wenn bei der Ersteinrichtung des Failovers die Zertifikate nicht auf dem Standby-Gerät angezeigt werden, geben Sie den Befehl **write standby** aus, um eine Synchronisierung zu erzwingen.

4. Wenn ECDSA-Schlüssel verwendet werden, ist der Prozess zur Generierung von SSL-Zertifikaten anders?

Der einzige Unterschied in der Konfiguration ist der Schritt zur Generierung der Tastatur, bei dem anstelle eines RSA-Tastenfeldes ein ECDSA-Tastenfeld generiert wird. Die restlichen Schritte bleiben gleich. Der CLI-Befehl zum Generieren von ECDSA-Schlüsseln wird hier angezeigt:

```
 MainASA(config)# cry key generate ecdsa label SSL-Keypair elliptic-curve 256
INFO: The name for the keys will be: SSL-Keypair
Keypair generation process begin. Please wait...
```

Fehlerbehebung

Befehle für die Fehlerbehebung

Diese Debug-Befehle werden bei einem Fehler bei der Installation eines SSL-Zertifikats über die CLI gesammelt:

debug crypto ca 255

debug crypto ca messages 255

debug crypto ca transaktionen 255

Häufige Probleme

Nicht vertrauenswürdige Zertifikatswarnung bei Verwendung eines gültigen SSL-Zertifikats eines Drittanbieters auf der externen Schnittstelle auf ASA mit Version 9.4(1) und höher

Lösung: Dieses Problem tritt auf, wenn ein RSA-Tastenfeld mit dem Zertifikat verwendet wird. Auf ASA-Versionen ab 9.4(1) sind alle ECDSA- und RSA-Verschlüsselungen standardmäßig aktiviert, und die sicherste Verschlüsselung (in der Regel eine ECDSA-Verschlüsselung) wird für die Aushandlung verwendet. In diesem Fall legt die ASA anstelle des aktuell konfigurierten RSA-basierten Zertifikats ein selbstsigniertes Zertifikat vor. Es gibt eine Verbesserung, um das Verhalten zu ändern, wenn ein RSA-basiertes Zertifikat auf einer Schnittstelle installiert und von der Cisco Bug ID CSCuu02848 verfolgt wird.

Empfohlene Aktion: Deaktivieren Sie ECDSA-Chiffren mit den folgenden CLI-Befehlen:

```
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:
DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5"
```

Oder navigieren Sie mit dem ASDM zu**Configuration > Remote Access VPN > Advanced**, und wählen Sie**SSL Settings**. Wählen Sie im Abschnitt Verschlüsselung die Option tlsv1.2 **Cipher version aus** und bearbeiten Sie sie mit der benutzerdefinierten Zeichenfolge AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA DES:-CBC-SHA:RC4-SHA:RC4-MD5

Anhang

Anhang A: ECDSA oder RSA

Der ECDSA-Algorithmus ist Teil der Elliptic Curve Kryptography (ECC) und verwendet eine Gleichung einer elliptischen Kurve zur Generierung eines Public Key, während der RSA-Algorithmus das Produkt aus zwei Primzahlen plus einer kleineren Zahl zur Generierung des Public Key verwendet. Dies bedeutet, dass mit ECDSA die gleiche Sicherheitsstufe wie RSA erreicht werden kann, jedoch mit kleineren Schlüsseln. Dadurch wird die Rechungszeit reduziert und die Verbindungszeiten für Sites, die ECDSA-Zertifikate verwenden, erhöht.

Das Dokument zur Verschlüsselung der nächsten Generation und zur ASA enthält detailliertere Informationen.

Anhang B: Verwenden von OpenSSL zum Generieren eines PKCS12-Zertifikats aus einem Identitätszertifikat, einem CA-Zertifikat und einem privaten Schlüssel

1. Überprüfen Sie, ob OpenSSL auf dem System installiert ist, auf dem dieser Prozess ausgeführt wird. Für Mac OSX- und GNU/Linux-Benutzer wird dies standardmäßig installiert.
2. Wechseln Sie zu einem funktionierenden Verzeichnis. Unter Windows: Standardmäßig sind die Dienstprogramme in C:\Openssl\bin installiert. Öffnen Sie an diesem Ort eine Eingabeaufforderung.Unter Mac OSX/Linux: Öffnen Sie das Terminalfenster im Verzeichnis, das zum Erstellen des PKCS12-Zertifikats erforderlich ist.
3. Speichern Sie im Verzeichnis, das im vorherigen Schritt erwähnt wurde, die Dateien private key (privateKey.key), Identity Certificate (certificate.crt) und root CA Certificate Chain (CACert.crt). Kombinieren Sie den privaten Schlüssel, das Identitätszertifikat und die

Stammzertifizierungskette der Zertifizierungsstelle in einer PKCS12-Datei. Geben Sie eine Passphrase ein, um Ihr PKCS12-Zertifikat zu schützen.

```
strong> openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in
certificate.crt -certfile CACert.crt
```

4. Konvertieren Sie das generierte PKCS12-Zertifikat in ein Base64-verschlüsseltes Zertifikat:

```
openssl base64 -in certificate.pfx -out certificate.p12
```

Importieren Sie anschließend das Zertifikat, das im letzten Schritt zur Verwendung mit SSL generiert wurde.

Zugehörige Informationen

- ASA 9.x-Konfigurationshandbuch - Konfigurieren digitaler Zertifikate
- So erhalten Sie ein digitales Zertifikat von einer Microsoft Windows CA mithilfe von ASDM auf einer ASA
- Technischer Support und Dokumentation für Cisco Systeme