

Erstellen eines signierten Zertifikats der Zertifizierungsstelle (Certificate Authority, CA) im CVP-Anrufserver für SIP Transport Layer Security (TLS)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie ein CA-signiertes Zertifikat für den Anrufserver des Customer Voice Portal (CVP) generiert wird und wie das CVP-Anrufserver-Zertifikat verifiziert wird. Ab CVP Version 11.6 wird die SIP-TLS-Kommunikation (Session Initiation Protocol) unterstützt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CVP
- SIP

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf CVP 11.6.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Schritt 1: Passwort für Keystore suchen

Navigieren Sie im CVP-Anrufserver zu `c:\Cisco\CVP\conf\security.properties`, um dieses Kennwort zu finden.

Diese Datei enthält das Passwort für den Keystore, das für den Betrieb des Keystore erforderlich ist.

Schritt 2: Erstellen Sie eine temporäre Variable, um die Eingabe des Schlüsselwortwerts jedes Mal zu vermeiden.

Navigieren Sie zu `c:\Cisco\CVP\conf\security`, und führen Sie den folgenden Befehl aus:

```
set kt=c:\Cisco\CVP\jre\bin\keytool.exe -storepass 592(!aT@Hbt{[c]b7n6{Mj6J[0P4C~X2?4!zv~5(@2*12Dm97) -storetype JCEKS -keystore.keystore
```

Hinweis: `Storepass` muss durch ein eigenes Keystore-Passwort ersetzt werden.

Schritt 3: Entfernen Sie die vorhandene Anrufserver-Zertifikat.

Navigieren Sie zu `c:\Cisco\CVP\conf\security`, um das vorhandene Zertifikat zu finden. Führen Sie diesen Befehl aus, um das Zertifikat zu löschen:

```
%kt% -delete -alias callserver_certificate
```

Nach dem Löschen des Zertifikats kann dieser Befehl verwendet werden, um alle Zertifikate im CVP-Server zu überprüfen:

```
%kt% -Liste
```

Führen Sie folgenden Befehl aus, um zu überprüfen, ob das Zertifikat des Anrufservers gelöscht wurde:

```
%kt% -list | findstr. Callserver
```

Schritt 4: Generieren Sie das Schlüsselpaar. Sie müssen ein 2048-Bit-Schlüsselpaar verwenden.

Navigieren Sie zu `c:\Cisco\CVP\conf\security`, und führen Sie den folgenden Befehl aus:

```
%kt% -genkeypair -alias callserver_certificate -v -keysize 2048 -keyalg RSA
```

Wenn Sie diesen Befehl ausführen, werden folgende Informationen angefordert:

Hinweis: Sie müssen den Hostnamen des Servers als Vor- und Nachnamen verwenden.

Wie lautet Ihr Vor- und Nachname?

[Unbekannt]: `col115cvpcall02`

Wie lautet der Name Ihrer Organisationseinheit?

[Unbekannt]: `TAC`

Wie lautet der Name Ihrer Organisation?

[Unbekannt]: `Cisco`

Wie lautet der Name Ihrer Stadt bzw. Ihres Ortes?

[Unbekannt]: `Sydney`

Wie heißt Ihr Bundesland?

[Unbekannt]: `NSW`

Wie lautet der Ländercode aus zwei Buchstaben für diese Einheit?

[Unbekannt]: `AU`

Ist CN=col115cvpcall02, OU=TAC, O=Cisco, L=Sydney, ST=NSW, C=AU korrekt?

[Nein]: Ja

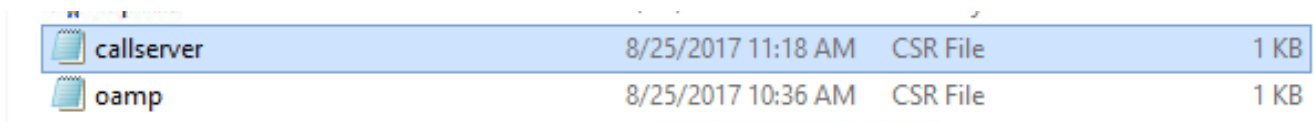
Schritt 5: Generieren Sie die neue Zertifikatssignierungsanfrage (Certificate Signing Request, CSR).

Navigieren Sie zu **c:\Cisco\CVP\conf\security**, und führen Sie den folgenden Befehl aus:

```
%kt% -certreq -alias callserver_certificate -file callserver.csr
```

Schritt 6: Unterzeichnen Sie die CSR-Anfrage durch eine interne Zertifizierungsstelle oder ein Drittanbieter-C.

Navigieren Sie zu **c:\Cisco\CVP\conf\security**, um diese CSR-Datei zu finden:

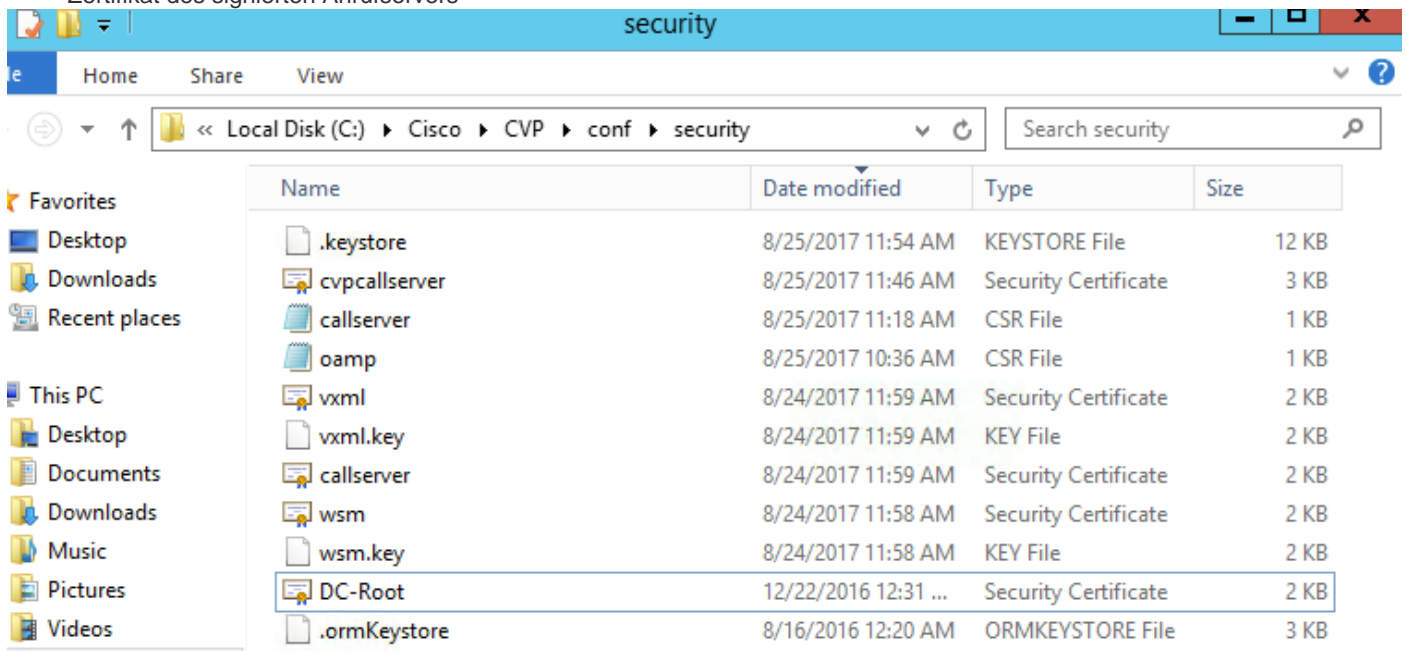


Name	Date modified	Type	Size
callserver	8/25/2017 11:18 AM	CSR File	1 KB
oamp	8/25/2017 10:36 AM	CSR File	1 KB

Schritt 7: Installieren Sie die Root CA.

Zwei Zertifikate werden in **c:\Cisco\CVP\conf\security** kopiert.

- Zertifikat der Stammzertifizierungsstelle
- Zertifikat des signierten Anrufservers



Führen Sie diesen Befehl aus:

```
%kt% -import -v -trustcacerts -alias root -file DC-Root.cer
```

In dieser Übung ist das Root CA-Zertifikat DC-Root.cer.

Schritt 8: Installieren Sie das von der CA signierte Anrufserver-Zertifikat.

Navigieren Sie zu **c:\Cisco\CVP\conf\security**

Führen Sie diesen Befehl aus:

```
%kt% -import -v -trustcacerts -alias callserver_certificate -file cvpcallserver.cer
```

In dieser Übung lautet das Anrufserverzertifikat cvpcallserver.cer.

Schritt 9: Überprüfen des neu installierten Zertifikats

Um das neu installierte Zertifikat zu überprüfen, navigieren Sie zu **C:\Cisco\CVP\conf\security>**
Führen Sie diesen Befehl aus:

```
%kt% -list -v -alias callserver_certificate Aliasname:callserver_certificate
```

Hinweis: Der Aliasname ist ein fester Systemwert. Sie müssen callserver_certificate verwenden.

Beispiel:

Erstellungsdatum: 25. August 2017

Eingabetyp: PrivateKeyEntry

Länge der Zertifikatskette: 2

Zertifikat [1]:

Eigentümer: CN=col115cvpcall02, OU=TAC, O=Cisco, L=Sydney, ST=NSW, C=AU

Emittent: CN=col115-COL115-CA, DC=col115, DC=org, DC=au

Seriennummer: 61000000e78c717ba3d3dc240000000000e

Gültig von: Freitag, 25. August 2017, 11:32:43 Uhr (AEST) bis: Stand: 25. August 2018, 11:42:43 Uhr

Zeugnisabdruck:

Nach Abschluss aller dieser Schritte wurde ein von der CA signiertes Zertifikat für den Anrufserver installiert. Dieses Zertifikat wird verwendet, wenn eine TLS-Verbindung für SIP hergestellt wird.

Überprüfen

Mit diesen beiden Befehlen können alle Zertifikate oder nur Serverzertifikate aufgelistet werden:

```
%kt% -Liste
```

```
%kt% -list | findstr. Callserver
```

Mit diesem Befehl können Zertifikatsdetails angezeigt werden:

```
Aliasname: callserver_certificate
```

```
%kt% -list -v -alias callserver_certificate
```

```
Aliasname:callserver_certificate
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

[Konfigurationsleitfaden für Cisco Unified Customer Voice Portal, Version 11.6\(1\)](#)

[Technischer Support und Dokumentation - Cisco Systems](#)