# UCSMでのサードパーティ証明書の作成と使用

内容				
<u>はじめに</u>				
<u>前提条件</u>				
<u>要件</u>				
<u>使用するコンポーネント</u>				
<u>設定手順</u>				
<u>トラストポイントの設定</u>				
<u>手順 1</u>				
<u>手順2</u>				
<u>手順3</u>				
<u>キーリングとCSRの作成</u>				
<u>手順1</u>				
<u>手順2</u>				
<u>手順3</u>				
<u>手順 4</u>				
<u>キーリングの適用</u>				
<u>手順1</u>				
<u>関連情報</u>				

## はじめに

このドキュメントでは、セキュアな通信のためにUnified Computing System(UCS)でサードパー ティ証明書を作成して使用する手順について説明します。

## 前提条件

要件

次の項目に関する知識があることが推奨されます。

- CA認証局へのアクセス
- UCSM 3.1

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

## 設定手順

## トラストポイントの設定

手順1

- CA認証局から証明書チェーンをダウンロードして、トラストポイントを作成します。証明 書サーバ内の<u>http://localhost/certsrv/Default.asp</u>を参照してください。
- encodingがBase 64に設定されていることを確認します。

Microsoft Active Directory Certificate Services - Enterprise CA-1	• Recording	00:06:21	Ш	
Download a CA Certificate, Certificate Chain, or CRL				
To trust certificates issued from this certification authority, install this CA certificate.				
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.				
CA certificate: Current [Enterprise CA-1(1)]				
Encoding method:				۲
⊙ DER ⊛Base 64				P
Install CA certificate Download CA certificate Download CA certificate Download latest base CRL Download latest delta CRL				-\$*

CA認証局からの証明書チェーンのダウンロード

#### 手順 2

・ダウンロードされた証明書チェーンはPB7形式です。



- OpenSSLツールで.pb7ファイルをPEM形式に変換します。
- たとえば、Linuxでは、変換を実行するためにターミナルで次のコマンドを実行できます
   : openssl pkcs7 -print\_certs -in <cert\_name>.p7b -out <cert\_name>.pem。

#### 手順 3

- UCSMでトラストポイントを作成します。
- Admin > Key Management > Trustpointの順に移動します。
- トラストポイントを作成するときに、このセクションのステップ2で作成した.PEMファイルの完全な内容を証明書の詳細スペースに貼り付けます。



キーリングとCSRの作成

### 手順 1

- ・ UCSM > Admin > Key Management > Keyringの順に移動します。
- サードパーティ証明書に必要なモジュールを選択します。

# Key Ring

Name :	3rd-party	
Modulus :	○ Mod2048 ○ Mod2560 ○ Mod3072 ○ Mod3584	Mod4096

### 手順 2

- ・ create certificate requestをクリックし、要求された詳細情報を入力します。
- 要求フィールドの内容をコピーします。



手順 3

### 証明書を生成するには、手順2でコピーした要求を次のスペースに貼り付けます。

Microsoft Active Directory Certificate Services - Enterprise CA-1

#### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 the Saved Request box.

		_	
<	>	~ ~	
ate: User - ING		_	
ites:			
<	>		
	Submit >	_	
	ate: User - ING Ites:	ate: User - ING V Ites:	ate: User - ING V Ites:

手順 4

 送信されると、新しい証明書が生成されます。ファイルを開き、このセクションのステップ 1で作成したキーリングの証明書フィールドに、新しく生成した証明書のすべての内容をコ ピーします。

Trusted Point :	Trust-test	Ψ.	
Certificate :	BEGIN CER MIIGLJCCBRagAw 9w0BAQsFADBIN CZImiZPyLGQBGI ZAEZFgJJTJEYME AxMPRW50ZXJw	TIFICATE IBAgIKS4anFAABAA IRgwFgYK RYIaW50cmFuZXQx 8YGA1UE cmIzZSBDQS0xMB4	)jDANBgkqhkiG QBgoJkiaJk/Is DTE4MDUwOD

 「キーリングとCSRの作成」のステップ3で作成したドロップダウンからトラストポイント を選択します。

キーリングの適用

手順 1

0

次に示すように、コミュニケーションサービスで作成したキーリングを選択します。

cisco	UCS Manager	
ж	All	All / Communication Management / Communication Services
- -	<ul> <li>Locally Authenticated Users</li> <li>Remotely Authenticated Users</li> <li>Roles</li> </ul>	Communication Services     Events     FSM       Redirect HTTP to HTTPS     : • Enabled   Disabled
Ŧ	▼ Key Management KeyRing default	Admin State : Enabled Disabled
Q	KeyRing Test_Keyring KeyRing ucsm_5108	HTTPS Admin State : Enabled Disabled
	TP root TP Trust-test	Port : 443 Operational Port : 443
	<ul> <li>Communication Management</li> <li>Call Home</li> </ul>	Cipher Suite Mode : High Strength Medium Strength Low Strength Custom
	Communication Services DNS Management Management Interfaces	Allowed SSL Protocols :

キーリングを変更すると、UCSMへのHTTPS接続がWebブラウザでセキュアとして表示されます



注:これを行うには、ローカルデスクトップもUCSMと同じCA認証局からの証明書を使 用する必要があります。



## 関連情報

• <u>テクニカル サポートとドキュメント - Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。