ISE の BYOD に使用する Windows サーバ AD 2012 の SCEP RA 証明書を更新する

目次

はじめに
前提条件
要件
使用するコンポーネント
問題
解決策
1. 古いプライベートキーを識別して下さい
2. 古いプライベートキーを削除して下さい
3. 古い MSCEP-RA ceritificates を削除して下さい
4. SCEP のための新しい証明書を生成して下さい
4.1. Exchange 登録証明書を生成して下さい
4.2. CEP 暗号化証明を生成して下さい
5. 確認
6. IIS の再起動
7. 新しい SCEP RA プロファイルを作成して下さい
8. 証明書のテンプレートを修正して下さい
参考資料

概要

この文書に Simple Certificate Enrollment Protocol（SCEP）のために使用する 2 つの証明書を更新する方法を記述されています: Microsoft Active Directory 2012 の Exchange 登録エージェントおよび CEP 暗号化証明。

前提条件

要件

次の項目に関する知識が推奨されます。

- Microsoft Active Directory 設定の基本的な知識
- 公開キー Infrastracture（PKI）の基本的な知識
- Identity Services Engine（ISE）の基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Identity Services Engine バージョン 2.0

- Microsoft Active Directory 2012 R2

問題

Cisco ISE は個人的なデバイス登録（onboarding BYOD）をサポートするのに SCEP プロトコルを使用します。 外部 SCEP CA を使用するとき、この CA は ISE の SCEP RA プロファイルによって定義されます。 SCEP RA プロファイルが作成されるとき、2 つの証明書は信頼できる証明書記憶装置に自動的に追加されます:

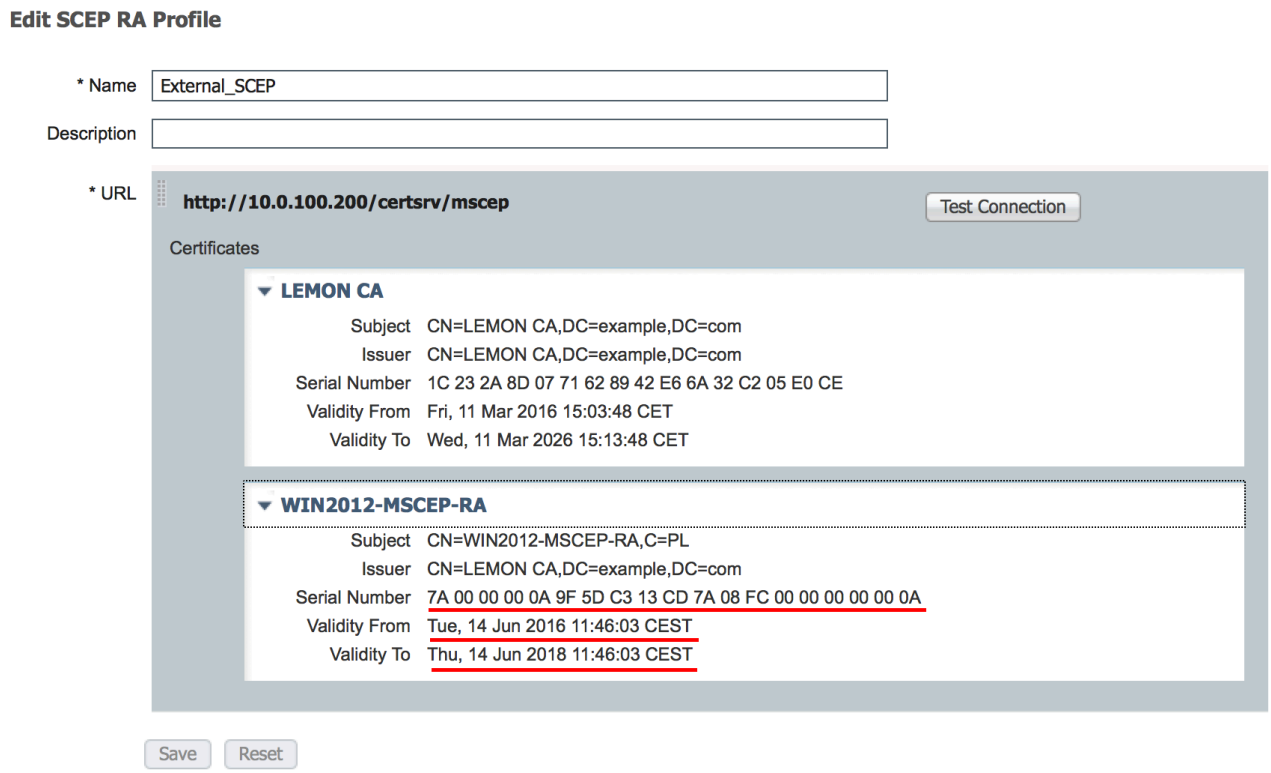
- CA ルート証明、
- CA によって署名する RA （登録局）証明書。

RA は受け取り、要求を登録デバイスからの検証したり、クライアント 認証を発行する CA へ転送する役割があります。

RA 証明書は切れるとき、CA 側面（この例の Windows サーバ 2012）で自動的に更新されません。 それはアクティブな Directory/CA administartor によって手動でする必要があります。

例は Windows サーバ 2012 R2 でそれを実現させる方法をここにあります。

ISE で目に見える最初の SCEP 証明書:



仮定は MSCEP-RA 証明書が期限切れで、更新されなければならないことです。

解決策

注意： Windows サーバのどの変更でも管理者と最初に参照する必要があります。

1. 古いプライベートキーを識別して下さい

privite キーを **certutil** ツールを使用してアクティブ ディレクトリの RA 証明書と関連付けられて見つけて下さい。 後それは**キー コンテナー**を取付けます。

```
certutil -store MY %COMPUTERNAME%-MSCEP-RA
```

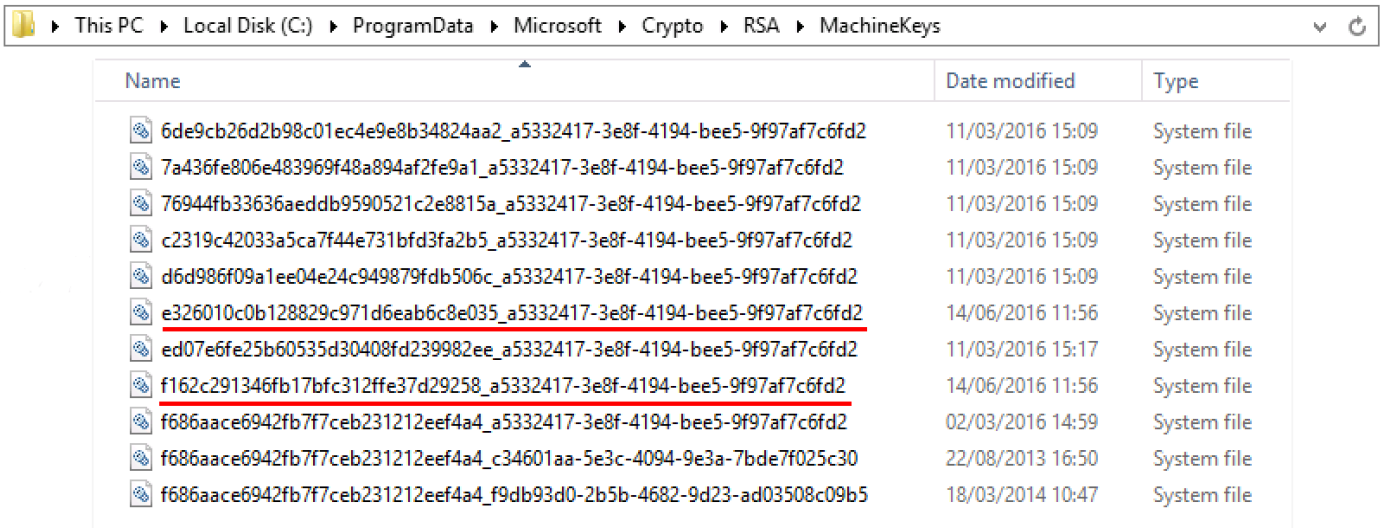
最初の MSCEP-RA 証明書の名前が異なっていたらそしてこの要求で調節する必要があることに注目して下さい。 ただし、デフォルトでそれはコンピュータ名が含まれているはずです。

```
C:\Users\Administrator>certutil -store MY %COMPUTERNAME%-MSCEP-RA
MY "Personal"
================ Certificate 0 ================
Serial Number: 7a00000000940c8eb5d5aa4e373000000000009
Issuer: CN=LEMON CA, DC=example, DC=com
 NotBefore: 14/06/2016 11:46
 NotAfter: 14/06/2018 11:46
Subject: CN=WIN2012-MSCEP-RA, C=PL
Certificate Template Name (Certificate Type): EnrollmentAgentOffline
Non-root Certificate
Template: EnrollmentAgentOffline, Exchange Enrollment Agent (Offline request)
Cert Hash(sha1): f3 3a b8 a7 ae ba 8e b5 c4 eb ec 07 ec 89 eb 58 1c 5a 15 ca
  Key Container = f162c291346fb17bfc312ffe37d29258_a5332417-3e8f-4194-bee5-9f97a
f7c6fd2
  Simple container name: le-84278304-3925-4b49-a5b8-5a197ec84920
  Provider = Microsoft Strong Cryptographic Provider
Private key is NOT exportable
Signature test passed

================ Certificate 3 ================
Serial Number: 7a00000000a9f5dc313cd7a08fc000000000000a
Issuer: CN=LEMON CA, DC=example, DC=com
 NotBefore: 14/06/2016 11:46
 NotAfter: 14/06/2018 11:46
Subject: CN=WIN2012-MSCEP-RA, C=PL
Certificate Template Name (Certificate Type): CEPEncryption
Non-root Certificate
Template: CEPEncryption, CEP Encryption
Cert Hash(sha1): 0e e1 f9 11 33 93 c0 34 2b bd bd 70 f7 e1 b9 93 b6 0a 5c b2
  Key Container = e326010c0b128829c971d6eab6c8e035_a5332417-3e8f-4194-bee5-9f97a
f7c6fd2
  Simple container name: le-0955b42b-6442-40a8-97aa-9b4c0a99c367
  Provider = Microsoft Strong Cryptographic Provider
Private key is NOT exportable
Encryption test passed
CertUtil: -store command completed successfully.
```

2. 削除古いプライベートキー

キーを下記のようにフォルダから手動で参照することを削除して下さい:

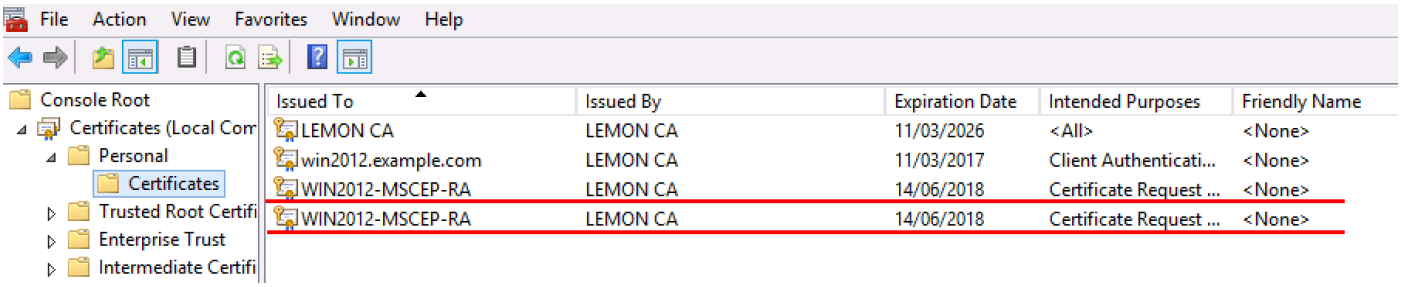
```
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
```



3. 古い MSCEP-RA ceritificates を削除して下さい

プライベートキーを削除した後、MMC コンソールから MSCEP-RA ceritificates を取除いて下さい。

MMC > ファイル > Add は/取除きますスナップインを… > Add 「Ceritificates」> コンピューターアカウント > ローカル コンピュータ



4. SCEP のための新しい証明書を生成して下さい

4.1. Exchange 登録証明書を生成して下さい

4.1.1. 下記の内容でファイル **cisco_ndes_sign.inf** を作成して下さい。 この情報は certreq.exetool によって使用された以降 証明書署名要求（CSR）を生成するために行います:

```
[NewRequest]
Subject = "CN=NEW-MSCEP-RA,OU=Cisco,O=Systems,L=Krakow,S=Malopolskie,C=PL"
Exportable = TRUE
KeyLength = 2048
KeySpec = 2
KeyUsage = 0x80
MachineKeySet = TRUE
ProviderName = "Microsoft Enhanced Cryptographic Provider v1.0
ProviderType = 1

[EnhancedKeyUsageExtension]
OID = 1.3.6.1.4.1.311.20.2.1

[RequestAttributes]
CertificateTemplate = EnrollmentAgentOffline
```

ヒント： このファイル テンプレートをコピーする場合、それを必要条件によって調節し、すべての文字がきちんとコピーされるかどうか確認することを確かめて下さい（を含む引用符）。

4.1.2. .INF ファイルに基づいてこのコマンドで CSR を作成して下さい:

```
certreq -f -new cisco_ndes_sign.inf cisco_ndes_sign.req
```

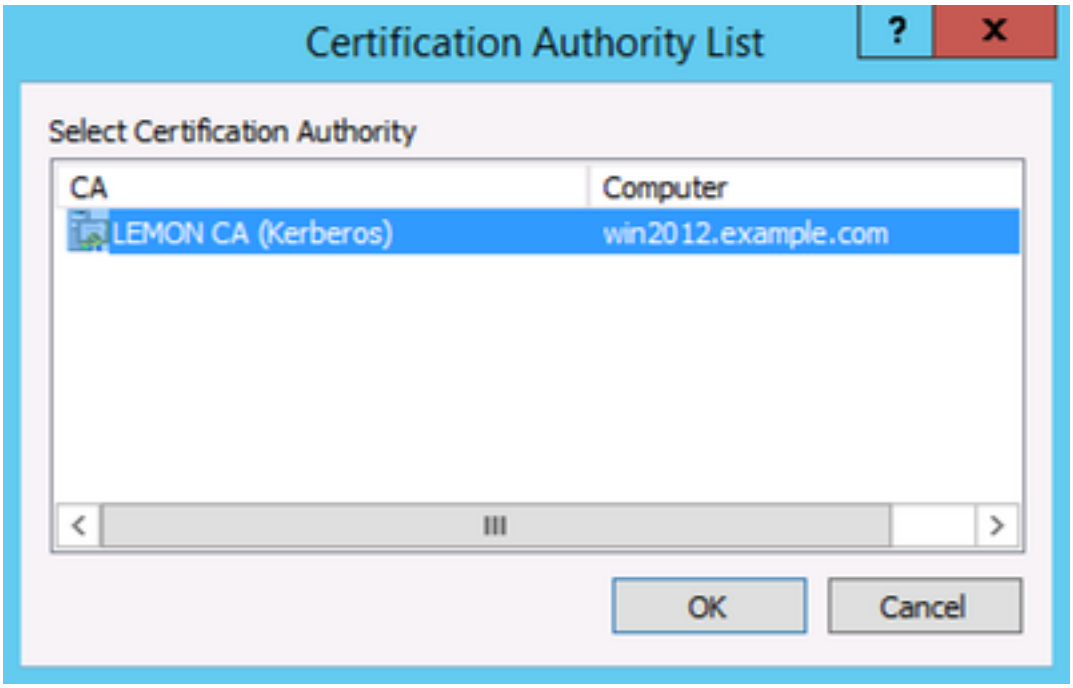
警告ダイアログ **ユーザー コンテキスト テンプレートがマシン コンテキストと**ポップアップすれば、『OK』 をクリック すれば**競合すれば**。 この警告は無視することができます。

```
C:\Users\Administrator\Desktop>certreq -f -new cisco_ndes_sign.inf cisco_ndes_si
gn.req
Active Directory Enrollment Policy
  {55845063-8765-4C03-84BB-E141A1DFD840}
  ldap:
User context template conflicts with machine context.

CertReq: Request Created

C:\Users\Administrator\Desktop>_
```

4.1.3. このコマンドで CSR を入れて下さい:

```
certreq -submit cisco_ndes_sign.req cisco_ndes_sign.cer
```

この手順の間にウィンドウはポップアップし、適切な CA は選択されなければなりません。




```
C:\Users\Administrator\Desktop>certreq -submit cisco_ndes_sign.req cisco_ndes_si
gn.cer
Active Directory Enrollment Policy
  {55845063-8765-4C03-84BB-E141A1DFD840}
  ldap:
RequestId: 11
RequestId: "11"
Certificate retrieved(Issued) Issued

C:\Users\Administrator\Desktop>_
```

4.1.4 前のステップで発行される証明書を受け入れて下さい。 このコマンドの結果として、新し

い証明書はローカル コンピュータ個人的な記憶装置にインポートされ、移動されます:

```
certreq -accept cisco_ndes_sign.cer
```

```
C:\Users\Administrator\Desktop>certreq -accept cisco_ndes_sign.cer

C:\Users\Administrator\Desktop>_
```

4.2. CEP 暗号化証明を生成して下さい

4.2.1. 新しいファイル cisco_ndes_xchg.inf を作成して下さい:

```
[NewRequest]
Subject = "CN=NEW-MSCEP-RA,OU=Cisco,O=Systems,L=Krakow,S=Malopolskie,C=PL"

Exportable = TRUE
KeyLength = 2048
KeySpec = 1
KeyUsage = 0x20
MachineKeySet = TRUE
ProviderName = “Microsoft RSA Schannel Cryptographic Provider”
ProviderType = 12

[EnhancedKeyUsageExtension]
OID = 1.3.6.1.4.1.311.20.2.1

[RequestAttributes]
CertificateTemplate = CEPEncryption
```

4.1 に記述されているように同じステップに従って下さい。

4.2.2. 新しい .INF ファイルに基づいて CSR を生成して下さい:

```
certreq -f -new cisco_ndes_xchg.inf cisco_ndes_xchg.req
```

4.2.3. 要求を入れて下さい:

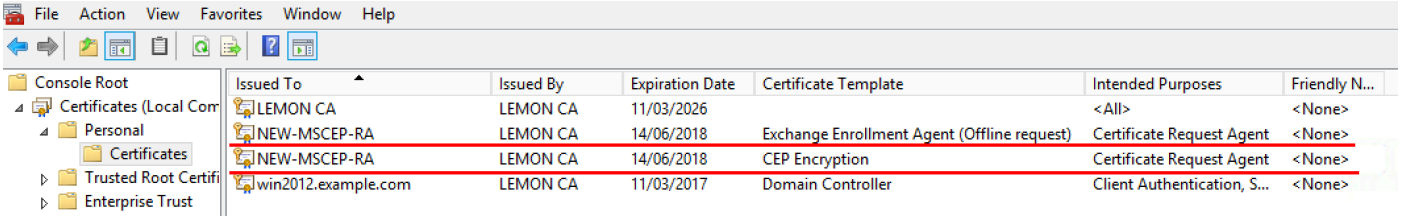
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

4.2.4: ローカル コンピュータ個人的な記憶装置にそれを移動することによって新しい証明書を受け入れて下さい:

```
certreq -accept cisco_ndes_xchg.cer
```

5. 確認

ステップ 4 を完了した後、2 つの新しい MSCEP-RA 証明書はローカル コンピュータ個人的な記憶装置に現われます:



また正しく新しい証明書名前を使用することを） certutil.exe ツールが付いている証明書を確認できます（確かめて下さい。 新しいよくある名前および新しいシリアル番号の MSCEP-RA 証明書は下記のように表示される必要があります:

```
certutil -store MY NEW-MSCEP-RA
```

```
C:\Users\Administrator\Desktop>certutil -store MY NEW-MSCEP-RA
MY "Personal"
================ Certificate 2 ================
Serial Number: 7a0000000cb250f5a9d6c11135000000000000c
Issuer: CN=LEMON CA, DC=example, DC=com
 NotBefore: 14/06/2016 13:40
 NotAfter: 14/06/2018 13:40
Subject: CN=NEW-MSCEP-RA, OU=Cisco, O=Systems, L=Krakow, S=Malopolskie, C=PL
Certificate Template Name (Certificate Type): CEPEncryption
Non-root Certificate
Template: CEPEncryption, CEP Encryption
Cert Hash(sha1): 31 4e 83 08 57 14 95 e9 0b b6 9a e0 4f c6 f2 cf 61 0b e8 99
  Key Container = 1ba225d16a794c70c6159e78b356342c_a5332417-3e8f-4194-bee5-9f97a
f7c6fd2
  Simple container name: CertReq-CEPEncryption-f42ec236-077a-40a9-b83a-47ad6cc8d
a0e
  Provider = Microsoft RSA SChannel Cryptographic Provider
Encryption test passed

================ Certificate 3 ================
Serial Number: 7a00000000b2813070a2b3616f000000000000b
Issuer: CN=LEMON CA, DC=example, DC=com
 NotBefore: 14/06/2016 13:35
 NotAfter: 14/06/2018 13:35
Subject: CN=NEW-MSCEP-RA, OU=Cisco, O=Systems, L=Krakow, S=Malopolskie, C=PL
Certificate Template Name (Certificate Type): EnrollmentAgentOffline
Non-root Certificate
Template: EnrollmentAgentOffline, Exchange Enrollment Agent (Offline request)
Cert Hash(sha1): 12 44 ba e6 4c 4e f8 78 7a a6 ae 60 9b b0 b2 ad e7 ba 62 9a
  Key Container = 320e64806bd159eca7b12283f3f67ee6_a5332417-3e8f-4194-bee5-9f97a
f7c6fd2
  Simple container name: CertReq-EnrollmentAgentOffline-0ec8b0c4-8828-4f09-927b-
c2f869589cab
  Provider = Microsoft Enhanced Cryptographic Provider v1.0
Signature test passed
CertUtil: -store command completed successfully.

C:\Users\Administrator\Desktop>_
```

6. IIS の再起動

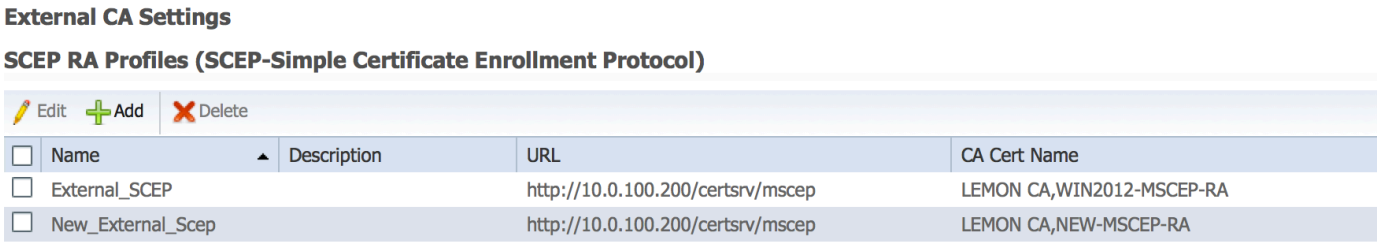
再起動 Internet Information Services （ IIS ）サーバ変更を加えるため:

```
iisreset.exe
```

```
C:\Users\Administrator\Desktop>iisreset.exe

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
```

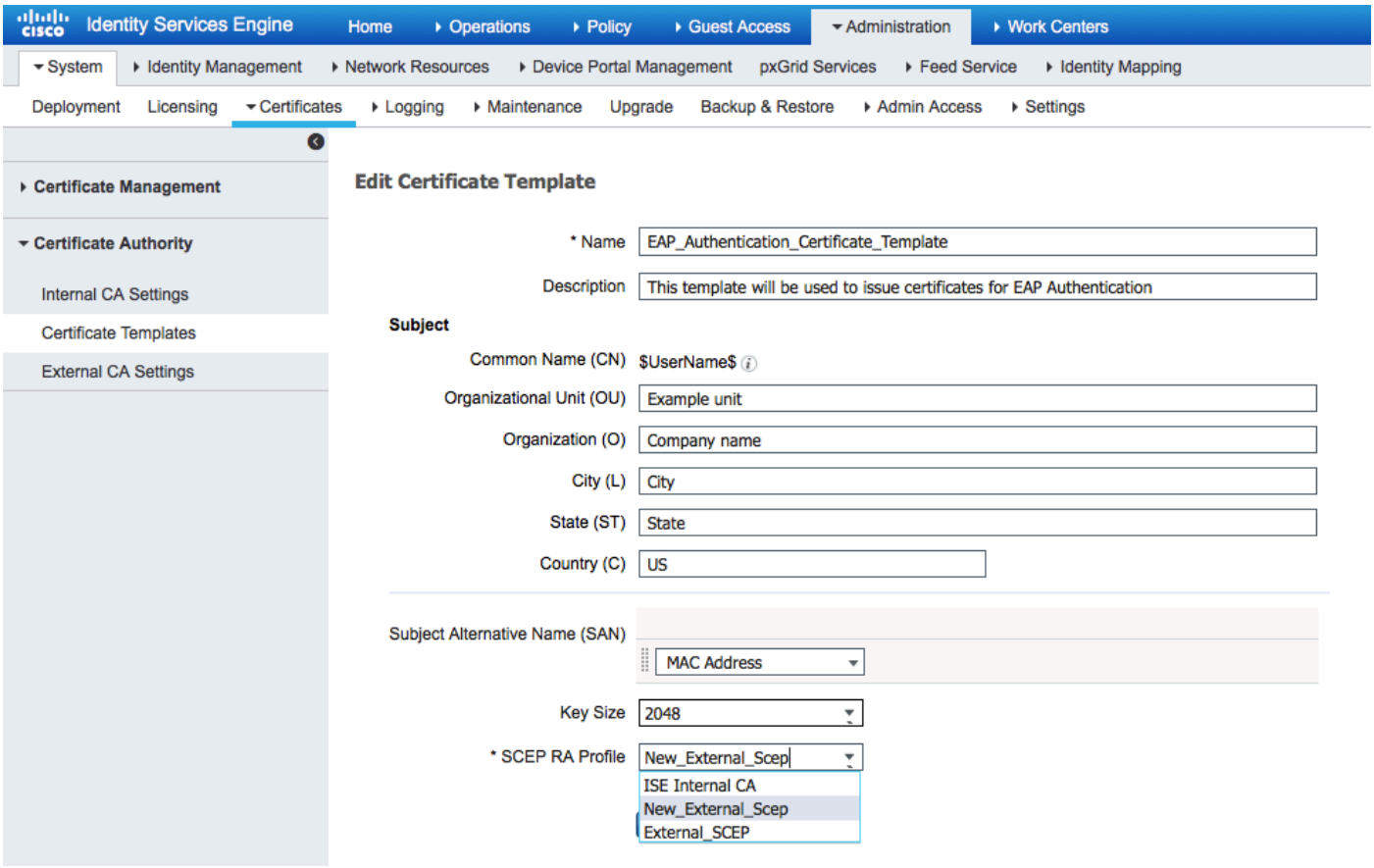
7. 新しい SCEP RA プロファイルを作成して下さい

ISE で新しい SCEP RA プロファイルを（古いものと同じサーバ URL と）作成して下さい、そうすれば新しい証明書は信頼できる証明書記憶装置にダウンロードされ、追加されます:



8. 証明書のテンプレートを修正して下さい

新しい SCEP RA プロファイルが BYOD（*Administration* > *システム* > *証明書* > *認証局* > *証明書テンプレート*でそれをチェックできます）によって使用される証明書のテンプレートで規定 されることを確かめて下さい:



参考資料

1. Microsoft Technet ゾーン技術情報
2. Cisco ISE コンフィギュレーション ガイド