在Windows Server AD 2012上續訂SCEP RA證書，用於ISE上的BYOD

目錄

簡介
必要條件
需求
採用元件
問題
解決方案
1.識別舊私鑰
2.刪除舊私鑰
3.刪除舊的MSCEP-RA證書
4.為SCEP生成新證書
4.1.生成Exchange註冊證書
4.2.生成CEP加密證書
5.驗證
6.重新啟動IIS
7.建立新的SCEP RA配置檔案
8.修改證書模板
參考資料

簡介

本文說明如何續訂兩個用於簡單憑證註冊通訊協定(SCEP)的憑證：Microsoft Active Directory 2012上的Exchange註冊代理和CEP加密證書。

必要條件

需求

思科建議您瞭解以下主題：

- Microsoft Active Directory配置基礎知識
- 公開金鑰基礎架構(PKI)基礎知識
- 身份服務引擎(ISE)基礎知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎版本2.0
- Microsoft Active Directory 2012 R2

問題

Cisco ISE使用SCEP協定支援個人裝置註冊（BYOD自註冊）。 使用外部SCEP CA時，此CA由ISE上的SCEP RA配置檔案定義。建立SCEP RA配置檔案時，兩個證書會自動新增到受信任證書儲存中：

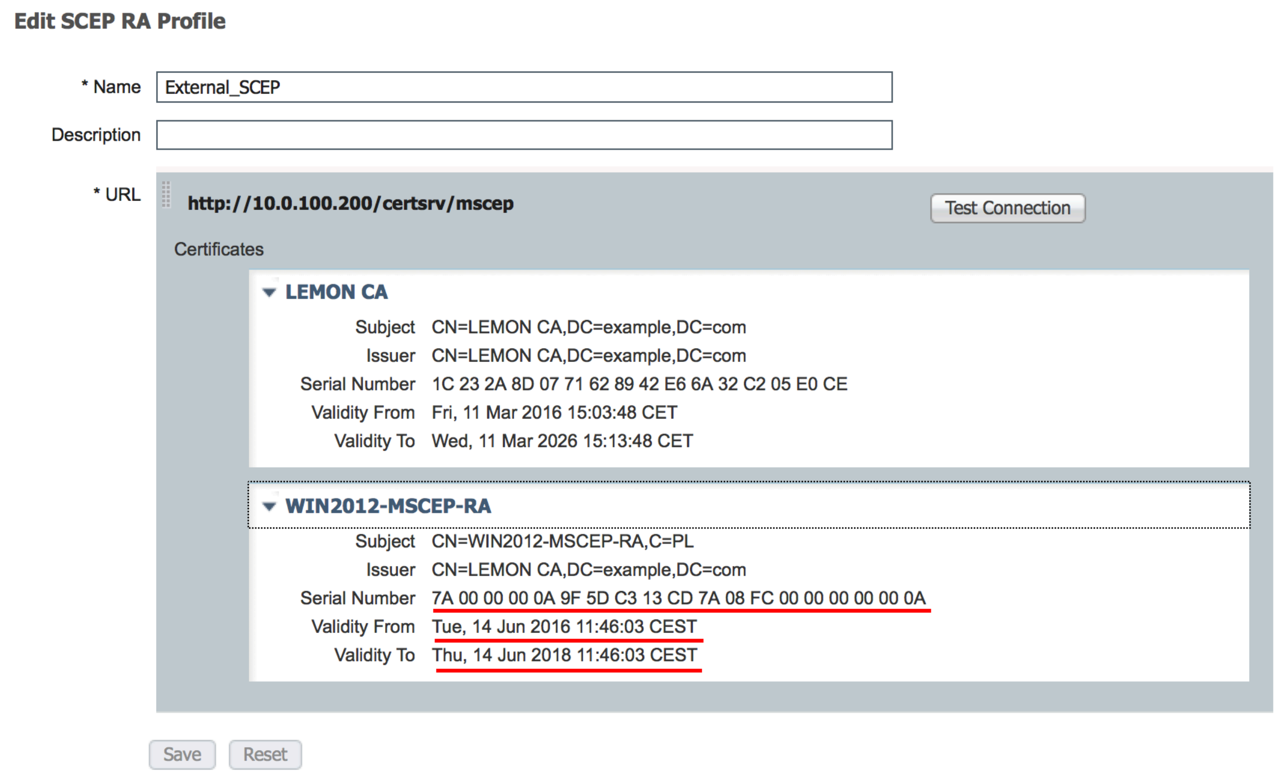
- CA根證書，
- RA（註冊機構）證書，由CA簽署。

RA負責接收和驗證來自註冊裝置的請求，並將其轉發到頒發客戶端證書的CA。

RA證書到期時，不會在CA端自動續訂（在本例中為Windows Server 2012）。 這應該由Active Directory/CA管理員手動完成。

以下示例說明如何在Windows Server 2012 R2上實現此功能。

初始SCEP證書在ISE上可見：



Edit SCEP RA Profile

* Name: External_SCEP

Description:

* URL: http://10.0.100.200/certsrv/mscep

Certificates

LEMON CA

Subject CN=LEMON CA,DC=example,DC=com
Issuer CN=LEMON CA,DC=example,DC=com
Serial Number 1C 23 2A 8D 07 71 62 89 42 E6 6A 32 C2 05 E0 CE
Validity From Fri, 11 Mar 2016 15:03:48 CET
Validity To Wed, 11 Mar 2026 15:13:48 CET

WIN2012-MSCEP-RA

Subject CN=WIN2012-MSCEP-RA,C=PL
Issuer CN=LEMON CA,DC=example,DC=com
Serial Number 7A 00 00 00 0A 9F 5D C3 13 CD 7A 08 FC 00 00 00 00 00 0A
Validity From Tue, 14 Jun 2016 11:46:03 CEST
Validity To Thu, 14 Jun 2018 11:46:03 CEST

假設MSCEP-RA證書已過期且必須續訂。

解決方案

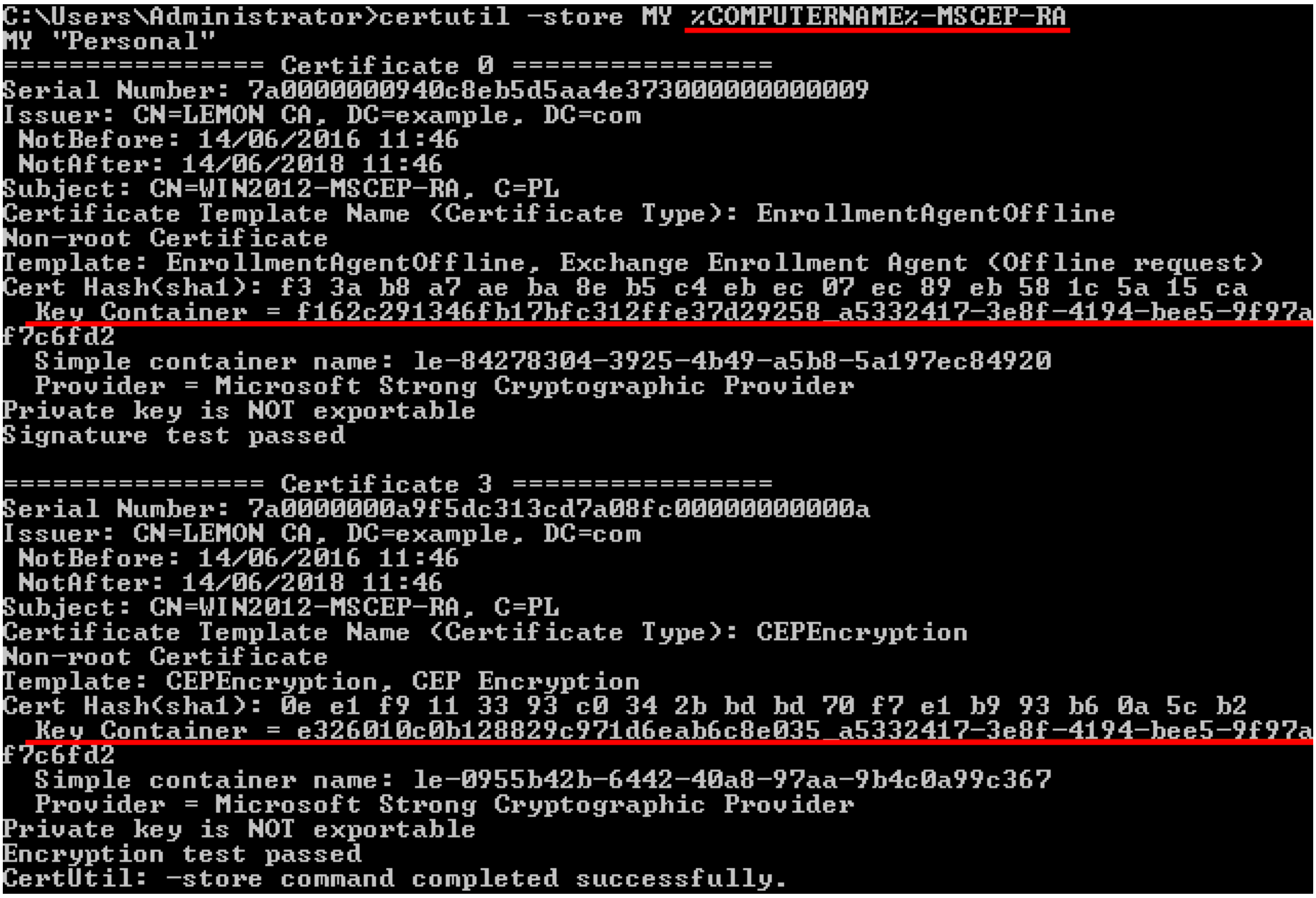
注意：對Windows Server所做的任何更改應首先諮詢其管理員。

1.識別舊私鑰

使用**certutil**工具在Active Directory上查詢與RA證書關聯的私鑰。找到金鑰容**器之後。**

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

請注意，如果您的初始MSCEP-RA證書的名稱不同，則應該在此請求中對其進行調整。但是，預設情況下，它應包含電腦名稱。

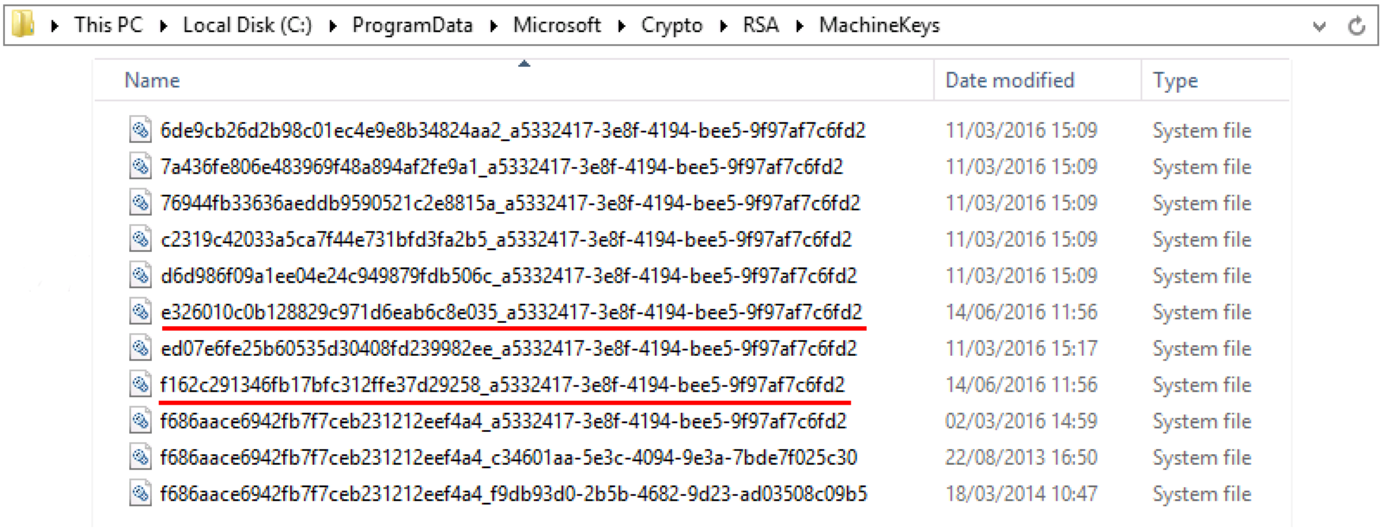


```
C:\Users\Administrator>certutil -store MY %COMPUTERNAME%-MSCEP-RA
MY "Personal"
================ Certificate 0 ================
Serial Number: 7a0000000940c8eb5d5aa4e373000000000009
Issuer: CN=LEMON CA, DC=example, DC=com
 NotBefore: 14/06/2016 11:46
 NotAfter: 14/06/2018 11:46
Subject: CN=WIN2012-MSCEP-RA, 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: 7a0000000a9f5dc313cd7a08fc00000000000a
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.刪除舊私鑰

從下面的資料夾手動刪除引用鍵：

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



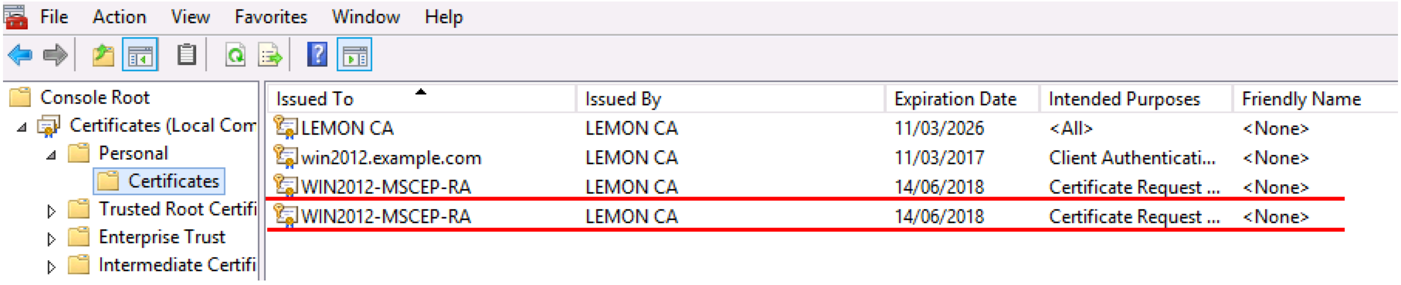
This PC ▸ Local Disk (C:) ▸ ProgramData ▸ Microsoft ▸ Crypto ▸ RSA ▸ MachineKeys

Name	Date modified	Type
6de9cb26d2b98c01ec4e9e8b34824aa2_a5332417-3e8f-4194-bee5-9f97af7c6fd2	11/03/2016 15:09	System file
7a436fe806e483969f48a894af2fe9a1_a5332417-3e8f-4194-bee5-9f97af7c6fd2	11/03/2016 15:09	System file
76944fb33636aeddb9590521c2e8815a_a5332417-3e8f-4194-bee5-9f97af7c6fd2	11/03/2016 15:09	System file
c2319c42033a5ca7f44e731bfd3fa2b5_a5332417-3e8f-4194-bee5-9f97af7c6fd2	11/03/2016 15:09	System file
d6d986f09a1ee04e24c949879fdb506c_a5332417-3e8f-4194-bee5-9f97af7c6fd2	11/03/2016 15:09	System file
e326010c0b128829c971d6eab6c8e035_a5332417-3e8f-4194-bee5-9f97af7c6fd2	14/06/2016 11:56	System file
ed07e6fe25b60535d30408fd239982ee_a5332417-3e8f-4194-bee5-9f97af7c6fd2	11/03/2016 15:17	System file
f162c291346fb17bfc312ffe37d29258_a5332417-3e8f-4194-bee5-9f97af7c6fd2	14/06/2016 11:56	System file
f686aace6942fb7f7ceb231212eef4a4_a5332417-3e8f-4194-bee5-9f97af7c6fd2	02/03/2016 14:59	System file
f686aace6942fb7f7ceb231212eef4a4_c34601aa-5e3c-4094-9e3a-7bde7f025c30	22/08/2013 16:50	System file
f686aace6942fb7f7ceb231212eef4a4_f9db93d0-2b5b-4682-9d23-ad03508c09b5	18/03/2014 10:47	System file

3.刪除舊的MSCEP-RA證書

刪除私鑰後，從MMC控制檯刪除MSCEP-RA證書。

MMC >「檔案」>「新增/刪除管理單元......」>「新增「證書」>「電腦帳戶」>「本地電腦」



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
LEMON CA	LEMON CA	11/03/2026	<All>	<None>
win2012.example.com	LEMON CA	11/03/2017	Client Authenticati...	<None>
WIN2012-MSCEP-RA	LEMON CA	14/06/2018	Certificate Request ...	<None>
WIN2012-MSCEP-RA	LEMON CA	14/06/2018	Certificate Request ...	<None>

4.為SCEP生成新證書

4.1.生成Exchange註冊證書

4.1.1.使用下列內容建立檔案**cisco_ndes_sign.inf**。**certreq.exe**工具稍後會使用此資訊來產生憑證簽署請求(CSR):

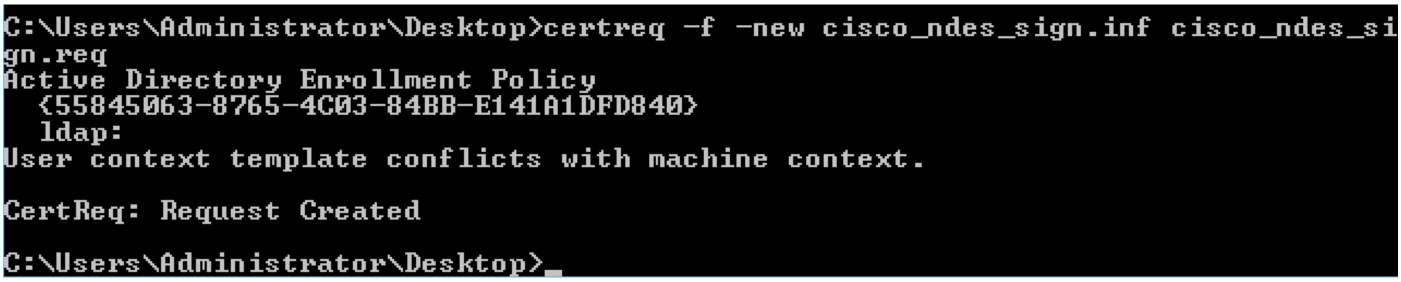
```
[NewRequest]
Subject = “CN=NEW-MSCEP-RA,OU=Cisco,O=Systems,L=Krakow,S=Malopolskie,C=PL”
Exportable = TRUE
KeyLength = 2048
KeySpec = 2
KeyUsage = 0x80
MachineKeySet = TRUE
ProviderName = “Microsoft Enhanced Cryptographic Provider v1.0
ProviderType = 1

[EnhancedKeyUsageExtension]
OID = 1.3.6.1.4.1.311.20.2.1

[RequestAttributes]
CertificateTemplate = EnrollmentAgentOffline
```

> **提示：**如果複製此檔案模板，請確保根據要求對其進行調整，並檢查是否所有字元都已正確複製（包括引號）。

4.1.2.使用以下命令根據.INF檔案建立CSR:

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

如果彈出警告對**話框「使用者上下文模板與電腦上下文**衝突」，請按一下「確定」。可以忽略此警告。

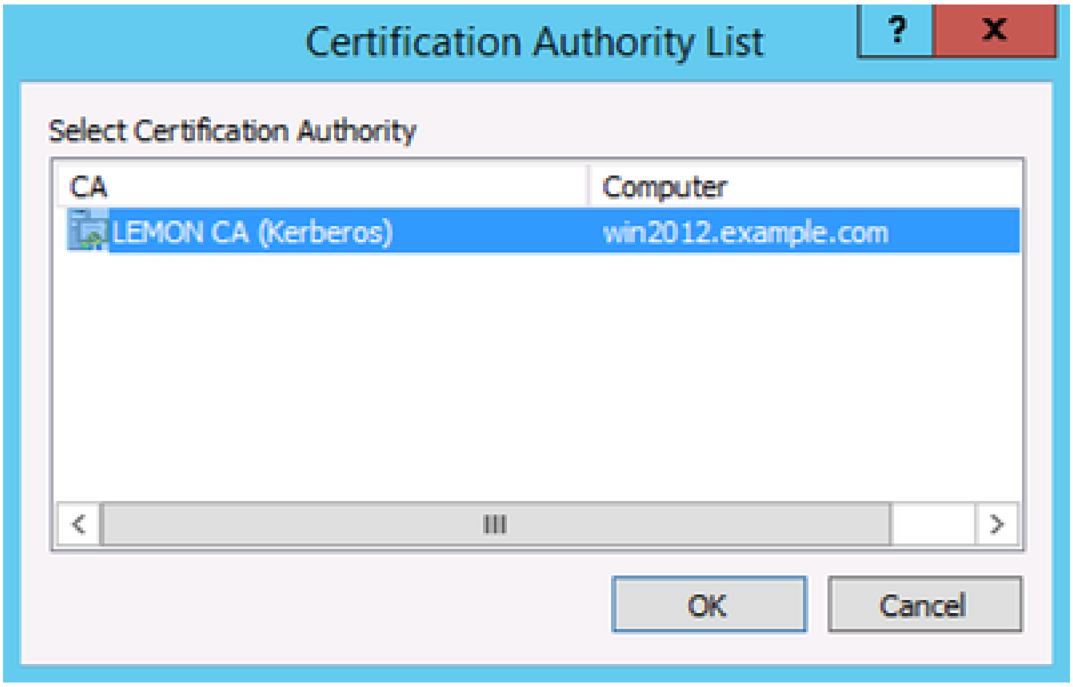


```
C:\Users\Administrator\Desktop>certreq -f -new cisco_ndes_sign.inf cisco_ndes_si
gn.req
Active Directory Enrollment Policy
  {55845063-8765-4C03-84BB-E141A1DFD840}
  ldap:
User context template conflicts with machine context.

CertReq: Request Created

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

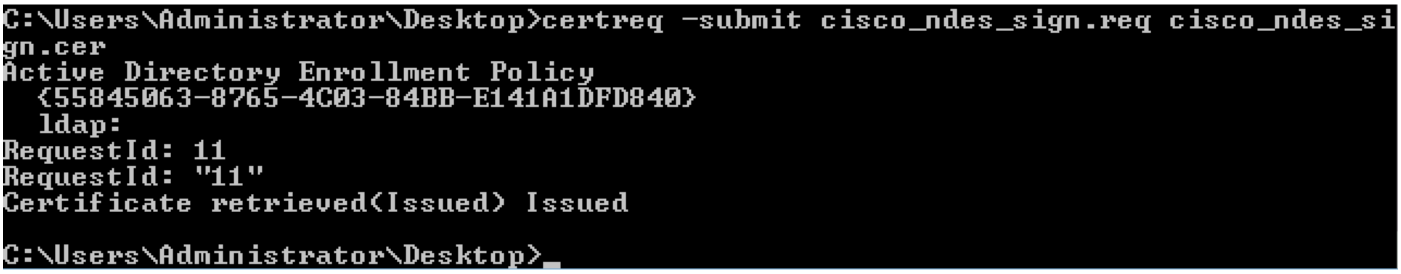
4.1.3.使用以下命令提交CSR:

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

在此過程中，會彈出一個視窗，您必須選擇適當的CA。



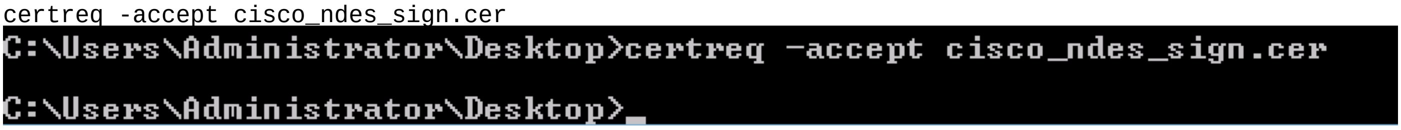
CA	Computer
LEMON CA (Kerberos)	win2012.example.com



```
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接受上一步頒發的證書。使用此命令後，新證書將匯入並移動到Local Computer Personal store:

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



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

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

4.2.生成CEP加密證書

4.2.1.建立新檔案**cisco_ndes_xchg.inf**:

```
[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
```

按照4.1中所述的相同步驟操作。

4.2.2.根據新的.INF檔案產生CSR:

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

4.2.3.提交請求：

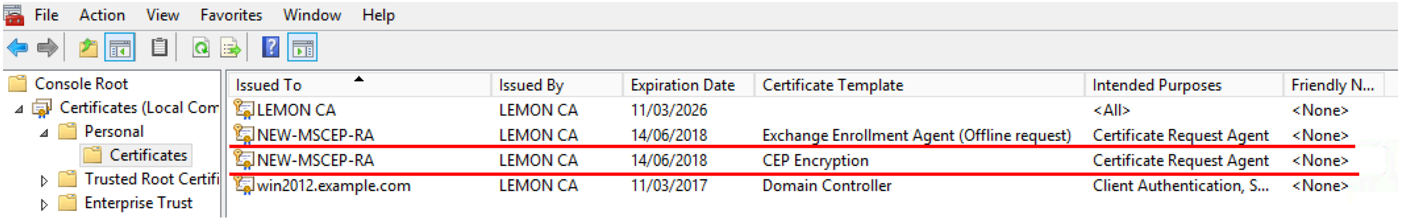
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

4.2.4 :通過將新證書移動到Local Computer Personal store來接受它：

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

5.驗證

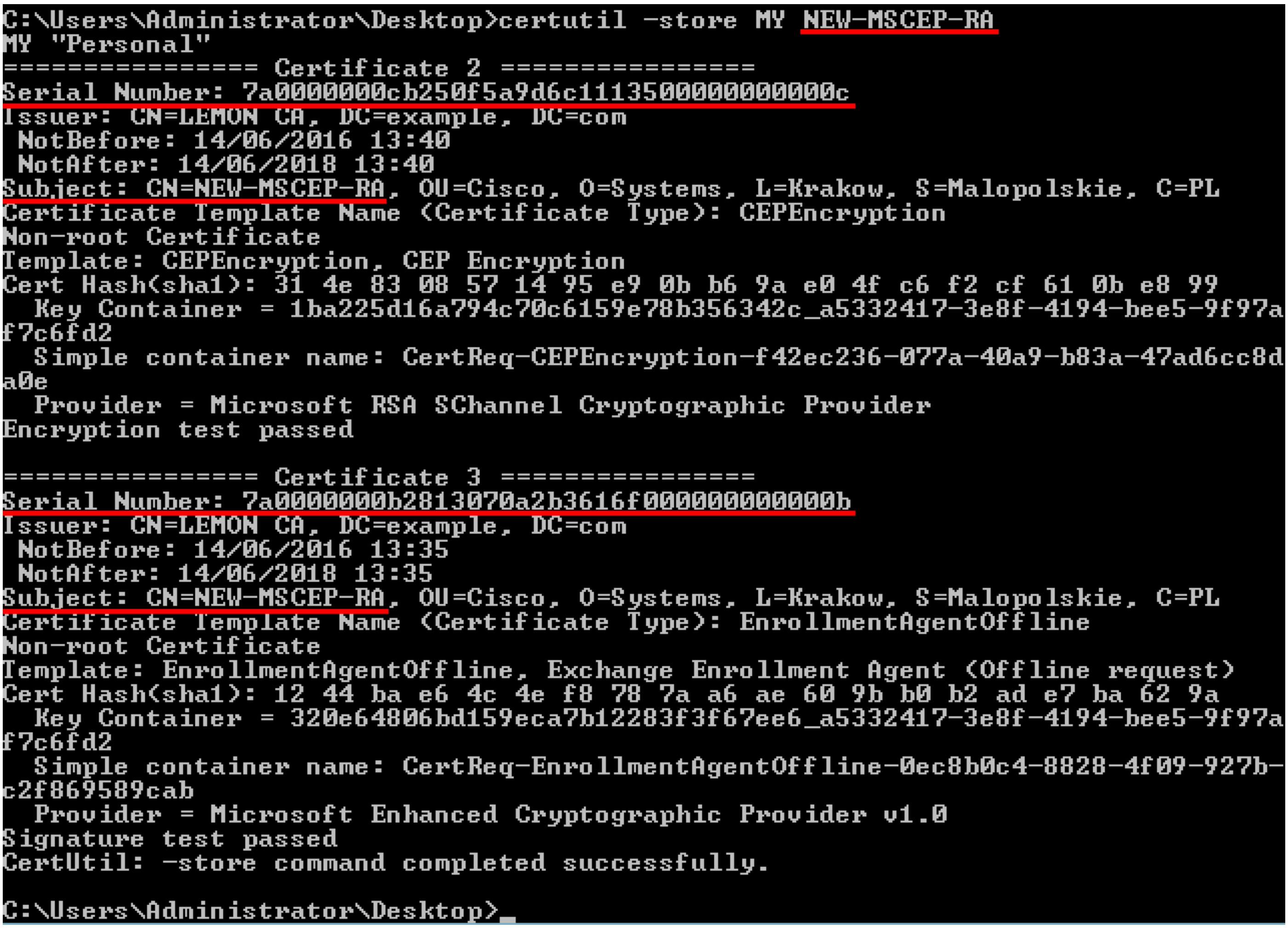
完成步驟4後，Local Computer Personal Store中將出現兩個新的MSCEP-RA證書：



Issued To	Issued By	Expiration Date	Certificate Template	Intended Purposes	Friendly N...
LEMON CA	LEMON CA	11/03/2026		<All>	<None>
NEW-MSCEP-RA	LEMON CA	14/06/2018	Exchange Enrollment Agent (Offline request)	Certificate Request Agent	<None>
NEW-MSCEP-RA	LEMON CA	14/06/2018	CEP Encryption	Certificate Request Agent	<None>
win2012.example.com	LEMON CA	11/03/2017	Domain Controller	Client Authentication, S...	<None>

您也可以使用**certutil.exe**工具驗證憑證（確保使用正確的新憑證名稱）。應顯示具有新通用名稱和新序列號的MSCEP-RA證書：

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

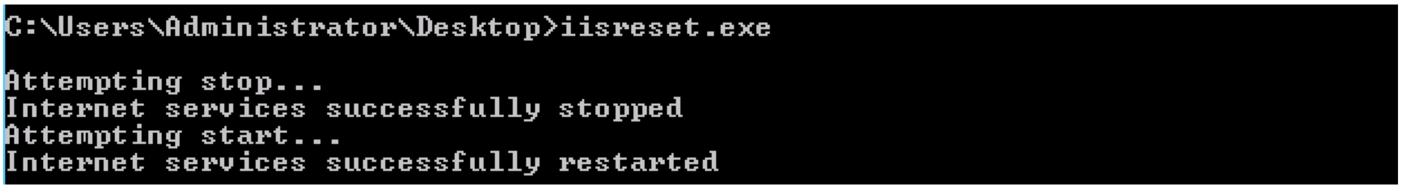


```
C:\Users\Administrator\Desktop>certutil -store MY NEW-MSCEP-RA
MY "Personal"
================ Certificate 2 ================
Serial Number: 7a0000000cb250f5a9d6c1113500000000000c
Issuer: CN=LEMON CA, DC=example, DC=com
 NotBefore: 14/06/2016 13:40
 NotAfter: 14/06/2018 13:40
Subject: CN=NEW-MSCEP-RA, 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: 7a0000000b2813070a2b3616f000000000000b
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.重新啟動IIS

重新啟動Internet Information Services(IIS)伺服器以應用更改：

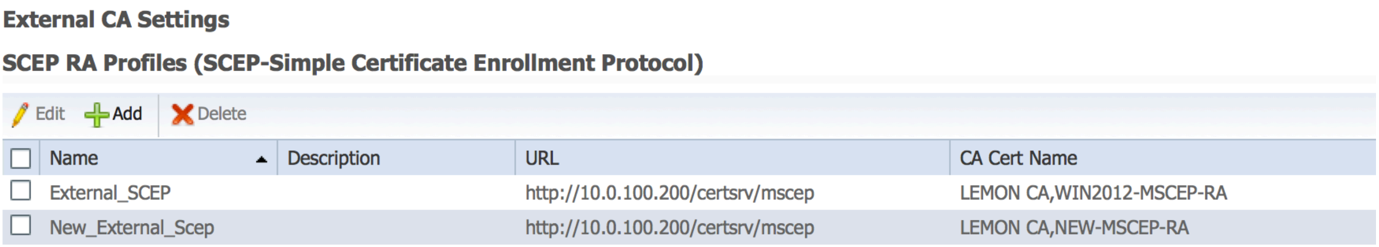
```
iisreset.exe
```



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

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

7.建立新的SCEP RA配置檔案

在ISE上建立一個新的SCEP RA配置檔案（與舊配置檔案具有相同的伺服器URL），這樣新證書將被下載並新增到受信任的證書儲存中：



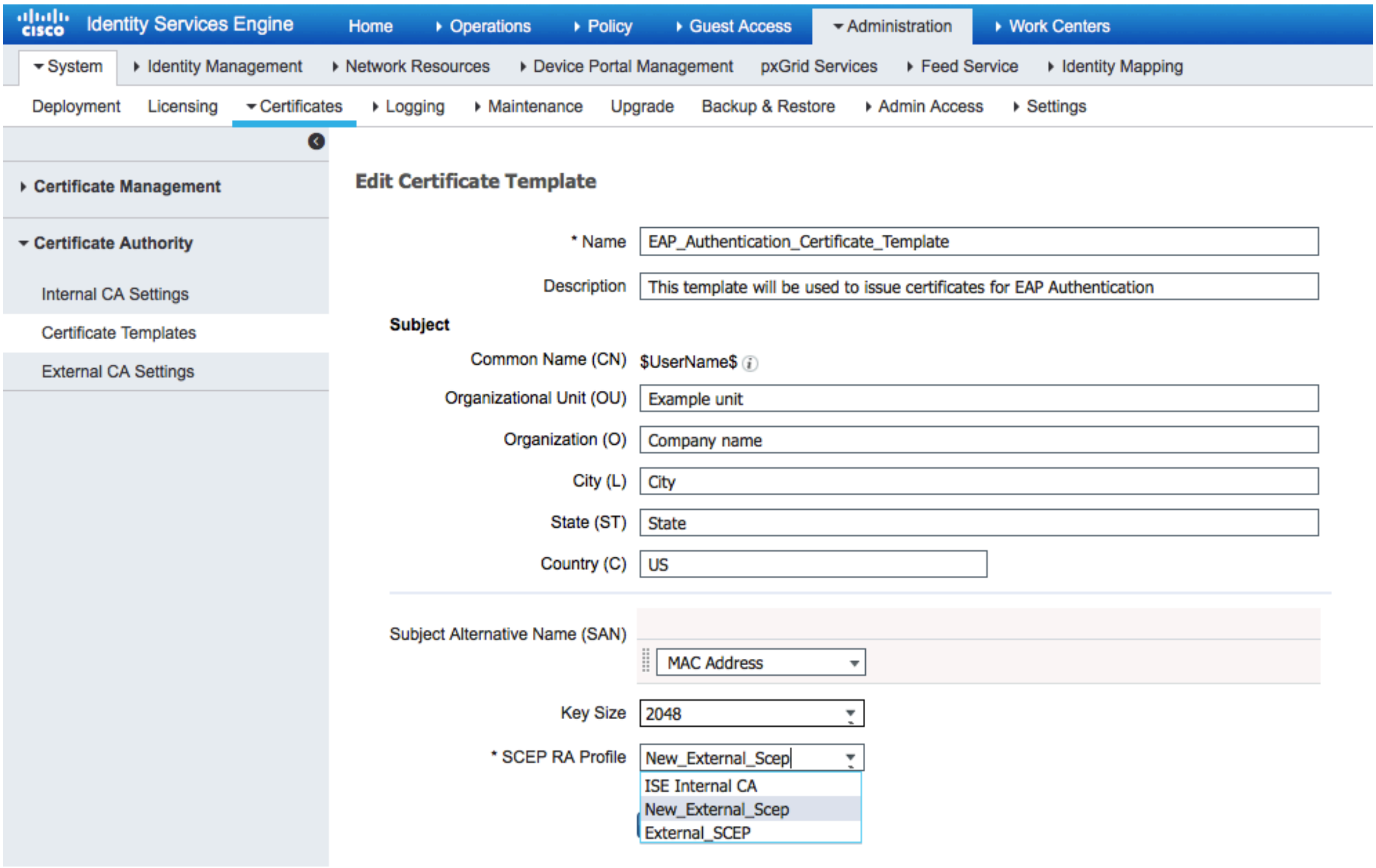
External CA Settings

SCEP RA Profiles (SCEP-Simple Certificate Enrollment Protocol)

☐	Name ▲	Description	URL	CA Cert Name
☐	External_SCEP		http://10.0.100.200/certsrv/mscep	LEMON CA,WIN2012-MSCEP-RA
☐	New_External_Scep		http://10.0.100.200/certsrv/mscep	LEMON CA,NEW-MSCEP-RA

8.修改證書模板

確保在BYOD使用的證書模板中指定新的SCEP RA配置檔案(您可以在*管理>系統>證書>證書頒發機構>證書模板*中選中它):



Edit Certificate Template

* Name: EAP_Authentication_Certificate_Template

Description: This template will be used to issue certificates for EAP Authentication

Subject

Common Name (CN): $UserName$

Organizational Unit (OU): Example unit

Organization (O): Company name

City (L): City

State (ST): State

Country (C): US

Subject Alternative Name (SAN): MAC Address

Key Size: 2048

* SCEP RA Profile: New_External_Scep

參考資料

1. [Microsoft Technet zone文章]()

2. [Cisco ISE配置指南]()