

更新SCEP在用于在ISE的BYOD 2012的RA证书的Windows服务器AD

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[问题](#)

[解决方案](#)

1. [识别旧有专用密钥](#)
2. [删除旧有专用密钥](#)
3. [删除旧有MSCEP-RA certificates](#)
4. [生成SCEP的新的证书](#)
 - 4.1. [生成Exchange登记证书](#)
 - 4.2. [生成CEP加密证明](#)
5. [验证](#)
6. [重新启动 IIS](#)
7. [创建新的SCEP RA配置文件](#)
8. [修改认证模板](#)

[参考](#)

简介

本文描述如何更新使用简单认证登记协议(SCEP)的两证书：Exchange登记代理程序和CEP加密证明在Microsoft Active Directory 2012。

先决条件

要求

Cisco 建议您了解以下主题：

- Microsoft Active Directory配置基础知识
- 基础知识公共密钥Infrastructure (PKI)
- 基础知识身份服务引擎(ISE)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎版本2.0
- Microsoft Active Directory 2012 R2

问题

思科ISE支持个人设备已注册的用途SCEP协议(onboarding的BYOD)。当曾经外部SCEP CA时，此CA由在ISE的一SCEP RA配置文件定义。当SCEP RA配置文件创建时，两证书自动地被添加到信任证书存储：

- CA根证明，
- 由CA签字的RA (注册审批机构)证书。

RA对接收和验证从注册设备的请求和转发发行客户端证书的它负责对CA。

当RA证书超时时，在CA侧(在本例中的Windows服务器2012没有自动地被更新)。应该由激活Directory/CA administartor手工完成那。

这是示例如何达到那在Windows服务器2012 R2。

最初的SCEP证书可视在ISE：

Edit SCEP RA Profile

* Name

Description

* URL

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	<u>7A 00 00 00 0A 9F 5D C3 13 CD 7A 08 FC 00 00 00 00 0A</u>
Validity From	<u>Tue, 14 Jun 2016 11:46:03 CEST</u>
Validity To	<u>Thu, 14 Jun 2018 11:46:03 CEST</u>

假定是MSCEP-RA证书超时并且必须被更新。

解决方案

Caution:在Windows服务器的所有更改应该首先与其管理员协商。

1. 识别旧有专用密钥

查找私有密钥关联与在活动目录的RA证书使用certutil工具。以后那找出关键容器。

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

请注意：，如果您的初始MSCEP-RA证书名称不同的然后在此请求应该调节它。默认情况下然而，它应该包含计算机名称。

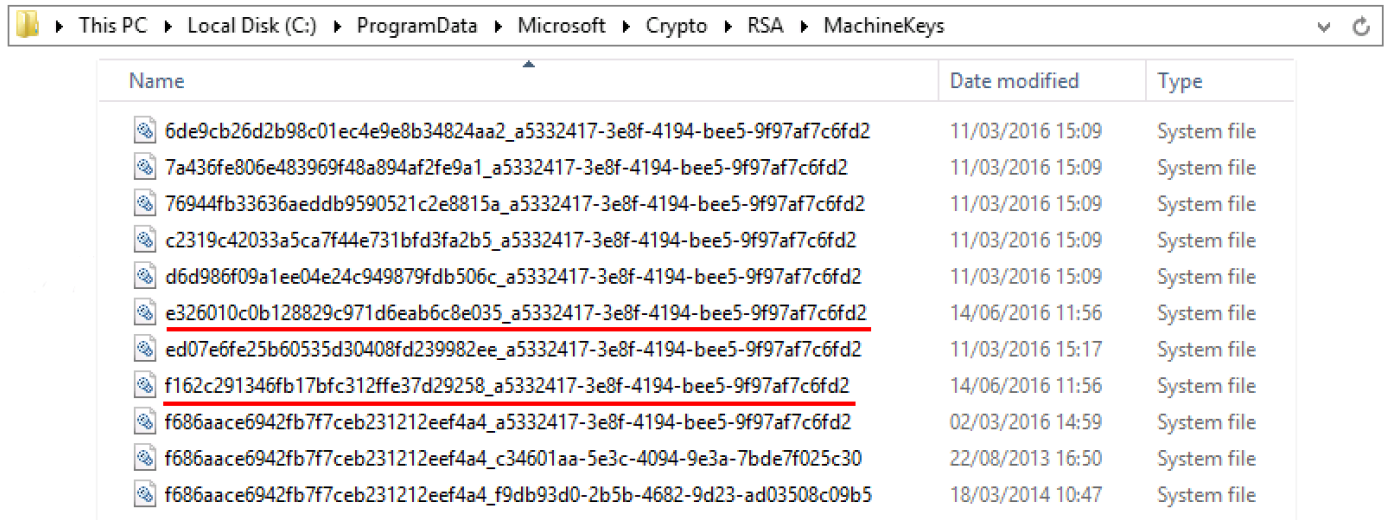
```
C:\Users\Administrator>certutil -store MY %COMPUTERNAME%-MSCEP-RA
MY "Personal"
===== Certificate 0 =====
Serial Number: 7a0000000940c8eb5d5aa4e373000000000009
Issuer: CN=LEMON CA, DC=example, DC=com
NotBefore: 14/06/2016 11:46
NotAfter: 14/06/2018 11:46
Subject: CN=WIN2012-MSCEP-RA, C=PL
Certificate 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-bee5-9f97af7c6fd2
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-bee5-9f97af7c6fd2
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. 删除旧有专用密钥

从下面文件夹删除手工参考密钥：

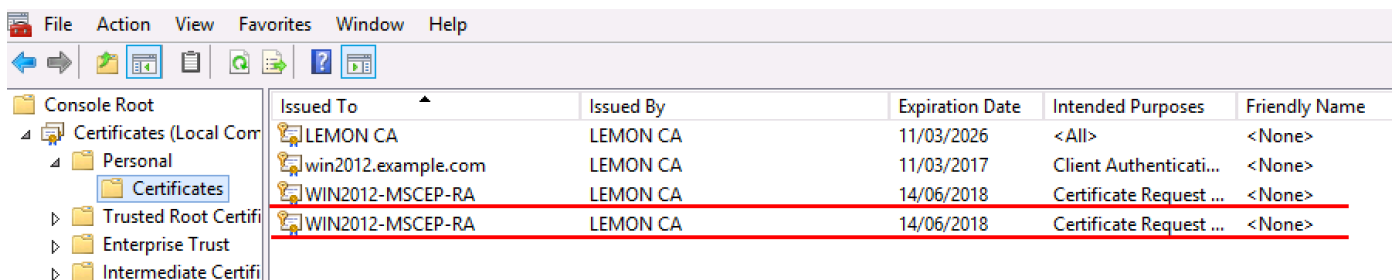
```
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
```



3. 删除旧有MSCEP-RA certificates

在删除专用密钥以后，请从MMC控制台取消MSCEP-RA certificates。

MMC > File>添加/删除管理单元...>Add "Certificates" >计算机帐户>本地计算机



4. 生成SCEP的新的证书

4.1. 生成Exchange登记证书

4.1.1. 创建一个文件cisco_ndes_sign.inf以下面内容。此信息使用的以后由certreq.exetool为了生成证书签名请求(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：如果复制此文件模板，请确保根据您的需求调节它和检查所有字符是否适当地复制(包括引号)。

4.1.2. 创建根据.INF文件的CSR用此命令：

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

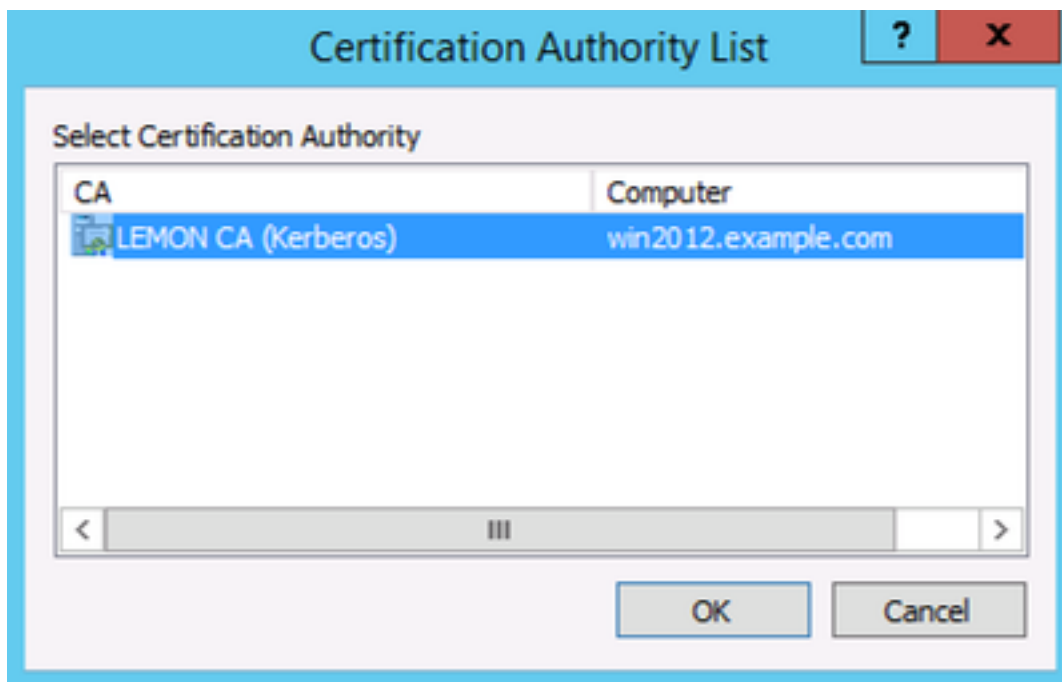
如果警告对话框用户模板与计算机上下文相冲突的上下文冒出，点击OK键。此警告可以忽略。

```
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. 提交CSR用此命令：

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

在此步骤期间窗口冒出，并且适当的CA必须选择。



```
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接受证书发出在上一步。由于此命令，新证书导入并且被搬到本地计算机个人存储：

```
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加密证明

4.2.1. 创建一个新的文件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

遵从同样步骤正如4.1所描述。

4.2.2. 生成根据新的.INF文件的CSR :

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

4.2.3. 提交请求 :

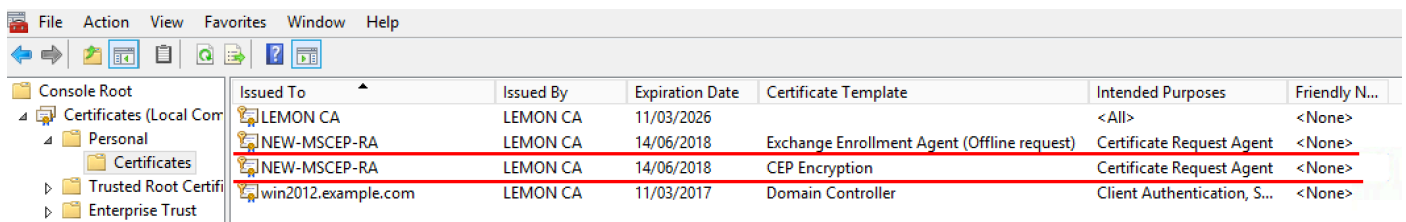
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

4.2.4 : 通过移动它接受新证书到本地计算机个人存储 :

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

5. 验证

在完成步骤以后4 , 两新的MSCEP-RA证书在本地计算机个人存储将出现 :



The screenshot shows the Windows Certificate Manager interface. The left pane shows the 'Certificates (Local Computer)' tree with 'Personal' > 'Certificates' selected. The right pane displays a table of certificates:

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>

并且您能验证证书用**certutil.exe**工具(请确保您使用正确新证书名称)。应该显示MSCEP-RA证书用新的公用名称和新的序列号 :

```
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. [重新启动 IIS](#)

重新启动互联网信息服务(IIS)服务器为了应用更改：

```
iisreset.exe
```

```

C:\Users\Administrator\Desktop>iisreset.exe
Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted

```

7. 创建新的SCEP RA配置文件

在ISE请创建一新的SCEP RA配置文件(与服务器URL和旧有一个一样)，如此新建的证书下载并且被添加到信任证书存储：

External CA Settings

SCEP RA Profiles (SCEP-Simple Certificate Enrollment Protocol)

<input type="checkbox"/>	Name	Description	URL	CA Cert Name
<input type="checkbox"/>	External_SCEP		http://10.0.100.200/certsrv/mscep	LEMON CA,WIN2012-MSCEP-RA
<input type="checkbox"/>	New_External_Scep		http://10.0.100.200/certsrv/mscep	LEMON CA,NEW-MSCEP-RA

8. 修改认证模板

确保新的SCEP RA配置文件指定在BYOD使用的认证模板(您在 *管理>System >证书能检查它>认证机关>认证模板*) :

The screenshot shows the 'Edit Certificate Template' configuration page in the Cisco Identity Services Engine (ISE) web interface. The page is titled 'Edit Certificate Template' and contains the following fields and options:

- 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 (selected), ISE Internal CA, New_External_Scep, External_SCEP

参考

1. [Microsoft Technet区域条款](#)
2. [思科ISE配置指南](#)