

Renouvelez le certificat de RA SCEP sur l'AD 2012 de Windows Server utilisé pour BYOD sur ISE

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Problème](#)

[Solution](#)

1. [Identifiez les vieilles clés privées](#)
2. [Vieilles clés privées d'effacement](#)
3. [Vieux MSCEP-RA certificats de l'effacement](#)
4. [Générez les nouveaux Certificats pour SCEP](#)
 - 4.1. [Générez le certificat d'inscription d'échange](#)
 - 4.2. [Générez le certificat de cryptage de CÈPE](#)
5. [Vérifiez](#)
6. [Reprise IIS](#)
7. [Créez le nouveau profil de RA SCEP](#)
8. [Modifiez le modèle de certificat](#)

[Références](#)

Introduction

Ce document décrit comment renouveler deux Certificats qui sont utilisés pour l'inscription de certificat simple Protocol (SCEP) : Permutez le certificat d'agent d'inscription et de cryptage de CÈPE sur la Microsoft Active Directory 2012.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de configuration de Microsoft Active Directory
- Connaissance de base de clé publique Infrastructure (PKI)
- Connaissance de base du Cisco Identity Services Engine (ISE)

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Version 2.0 de Logiciel Cisco Identity Services Engine
- Microsoft Active Directory 2012 R2

Problème

Cisco ISE emploie le protocole SCEP pour prendre en charge l'enregistrement personnel de périphérique (BYOD onboarding). En utilisant un SCEP externe CA, ce CA est défini par un profil de RA SCEP sur ISE. Quand un profil de RA SCEP est créé, deux Certificats sont automatiquement ajoutés à la mémoire de Certificats de confiance :

- Certificat racine CA,
- Certificat de RA (autorité d'enregistrement) qui est signé par le CA.

Le RA est responsable de recevoir et de valider la demande du périphérique de enregistrement, et de l'expédier au CA qui délivre le certificat client.

Quand le certificat de RA expire, il n'est pas renouvelé automatiquement du côté CA (Windows Server 2012 dans cet exemple). Cela devrait être manuellement fait par l'administrateur actif Directory/CA.

Voici l'exemple comment réaliser cela sur les Windows Server 2012 R2.

SCEP initial délivre un certificat visible sur 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 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>

La supposition est que le CERTIFICAT MSCEP-RA est expiré et doit être renouvelé.

Solution

Attention : Toutes les modifications sur des Windows Server devraient être consultées son administrateur d'abord.

1. Identifiez les vieilles clés privées

Trouvez les clés de private associées avec les Certificats de RA sur le Répertoire actif utilisant l'outil de **certutil**. Ensuite cela localisent le **conteneur principal**.

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

Veillez noter que si le nom de votre certificat de l'initiale MSCEP-RA est différent puis il devrait être ajusté dans cette demande. Cependant, par défaut il devrait contenir le nom de l'ordinateur.

```
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. Vieilles clés privées d'effacement

Supprimez se référer des clés manuellement du répertoire ci-dessous :

```
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
<u>e326010c0b128829c971d6eab6c8e035_a5332417-3e8f-4194-bee5-9f97af7c6fd2</u>	14/06/2016 11:56	System file
ed07e6fe25b60535d30408fd239982ee_a5332417-3e8f-4194-bee5-9f97af7c6fd2	11/03/2016 15:17	System file
<u>f162c291346fb17bfc312ffe37d29258_a5332417-3e8f-4194-bee5-9f97af7c6fd2</u>	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. Vieux MSCEP-RA certificats de l'effacement

Après avoir supprimé les clés privées, enlevez les certificats MSCEP-RA de la console MMC.

MMC > fichier > ajout/suppression SNAP-dans... > ajoutez « Certificates » > compte > ordinateur local d'ordinateur

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>
<u>WIN2012-MSCEP-RA</u>	<u>LEMON CA</u>	<u>14/06/2018</u>	<u>Certificate Request ...</u>	<u><None></u>
<u>WIN2012-MSCEP-RA</u>	<u>LEMON CA</u>	<u>14/06/2018</u>	<u>Certificate Request ...</u>	<u><None></u>

4. Générez les nouveaux Certificats pour SCEP

4.1. Générez le certificat d'inscription d'échange

4.1.1. Créez un fichier `cisco_ndes_sign.inf` avec le contenu ci-dessous. Ces informations sont utilisées plus tard par le `certreq.exe` afin de générer la demande de signature de certificat (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
```

Conseil : Si vous copiez ce modèle de fichier, veuillez à l'ajuster selon vos conditions requises et à vérifier si tous les caractères sont correctement copiés (guillemets y compris).

4.1.2. Créez le CSR basé sur le fichier .INF avec cette commande :

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

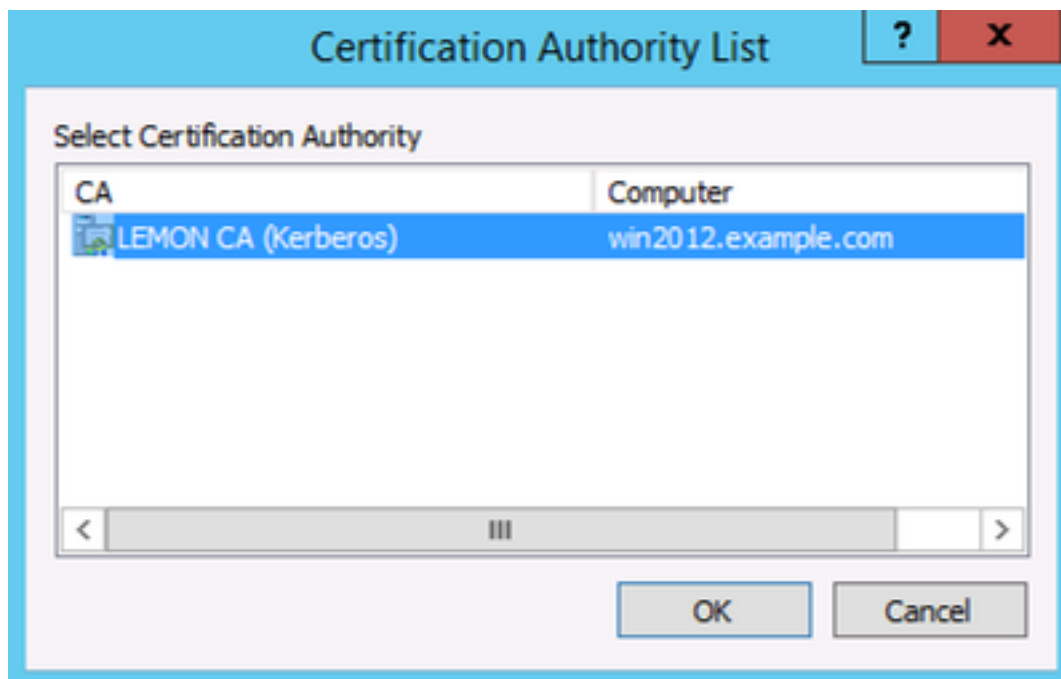
Si l'utilisateur d'avertissement de dialogue que **modèle de contexte est en conflit avec le contexte d'ordinateur** s'affiche, cliquez sur OK. Cet avertissement peut être ignoré.

```
C:\Users\Administrator\Desktop>certreq -f -new cisco_ndes_sign.inf cisco_ndes_sign.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. Soumettez le CSR avec cette commande :

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

Pendant cette procédure une fenêtre s'affiche et le CA approprié doit être choisi.



```
C:\Users\Administrator\Desktop>certreq -submit cisco_ndes_sign.req cisco_ndes_sign.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 Recevez le certificat délivré à l'étape précédente. En raison de cette commande, le nouveau certificat est importé et déplacé à la mémoire personnelle d'ordinateur local :

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

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

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

4.2. Générez le certificat de cryptage de CÈPE

4.2.1. Créez un nouveau fichier `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
```

Suivez les mêmes étapes comme décrit dans 4.1.

4.2.2. Générez un CSR basé sur le nouveau fichier `.INF` :

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

4.2.3. Soumettez la demande :

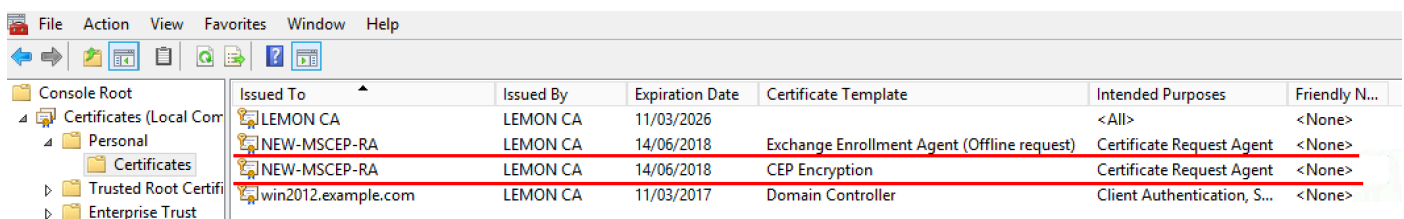
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

4.2.4 : Recevez le nouveau certificat en l'entrant dans la mémoire personnelle d'ordinateur local :

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

5. Vérifiez

Après s'être terminé l'étape 4, deux nouveaux Certificats MSCEP-RA apparaîtront dans la mémoire personnelle d'ordinateur local :



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>

Également vous pouvez vérifier les Certificats avec l'outil `certutil.exe` (assurez-vous que vous utilisez le nouveau nom correct de certificat). Des Certificats MSCEP-RA avec de nouveaux noms de terrain communal et nouveaux numéros de série devraient être affichés :

```
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. Reprise IIS

Redémarrez le serveur de l'Internet Information Services (IIS) afin d'appliquer les modifications :

```
iisreset.exe
```




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

7. Créez le nouveau profil de RA SCEP

Sur ISE créez un nouveau profil de RA SCEP (avec le même URL de serveur que le vieil), ainsi de nouveaux Certificats sont téléchargés et ajoutés à la mémoire de Certificats de confiance :

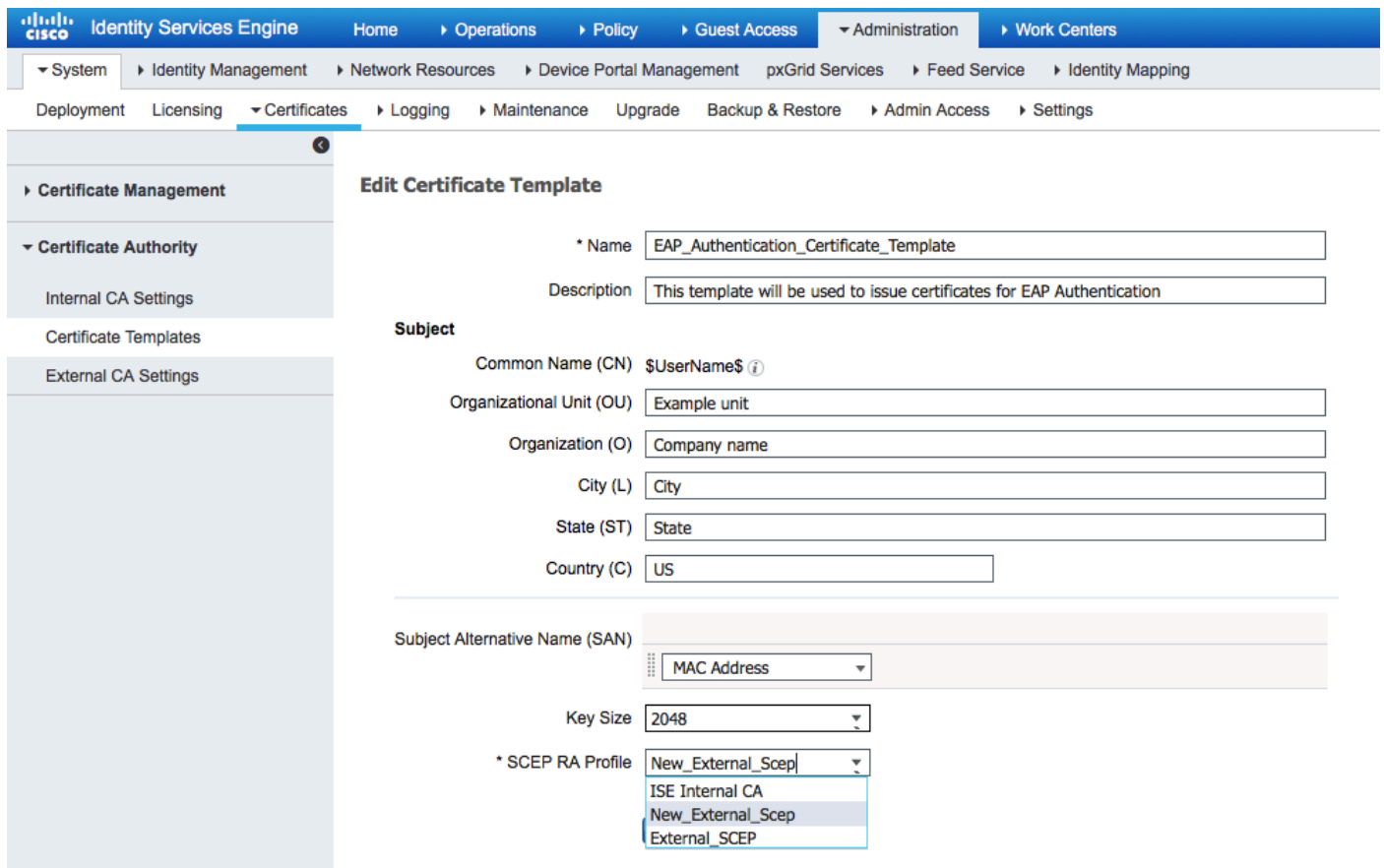
External CA Settings

SCEP RA Profiles (SCEP-Simple Certificate Enrollment Protocol)

 Edit	 Add	 Delete			
<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. Modifiez le modèle de certificat

Assurez-vous que le nouveau profil de RA SCEP est spécifié dans le modèle de certificat utilisé par BYOD (vous pouvez le vérifier dans la *gestion > le système > les Certificats > des modèles d'autorité de certification > de Certificats*) :



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

- 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 from a dropdown menu that also includes ISE Internal CA and External_SCEP)

Références

1. [Article de zone de Microsoft Technet](#)
2. [Guides de configuration de Cisco ISE](#)