

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Problem](#)

[Solution](#)

[1. Identify old private keys](#)

[2. Delete old private keys](#)

[3. Delete old MSCEP-RA certificates](#)

[4. Generate new certificates for SCEP](#)

[4.1. Generate the Exchange Enrollment Certificate](#)

[4.2. Generate the CEP Encryption Certificate](#)

[5. Verify](#)

[6. Restart IIS](#)

[7. Create new SCEP RA profile](#)

[8. Modify certificate template](#)

[References](#)

Introduction

This document describes how to renew two certificates that are used for Simple Certificate Enrollment Protocol (SCEP): Exchange Enrollment Agent and CEP Encryption certificate on Microsoft Active Directory 2012.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Microsoft Active Directory configuration
- Basic knowledge of Public Key Infrastructure (PKI)
- Basic knowledge of Identity Services Engine (ISE)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine version 2.0
- Microsoft Active Directory 2012 R2

Problem

Cisco ISE uses SCEP protocol to support personal device registration (BYOD onboarding). When using an external SCEP CA, this CA is defined by a SCEP RA profile on ISE. When a SCEP RA Profile is created, two certificates are automatically added to the Trusted Certificates Store:

- CA root certificate,
- RA (Registration Authority) certificate which is signed by the CA.

RA is responsible for receiving and validating the request from the registering device, and forwarding it to the CA that issues the client certificate.

When the RA certificate expires, it is not renewed automatically on the CA side (Windows Server 2012 in this example). That should be manually done by the Active Directory/CA administrator.

Here is the example how to achieve that on Windows Server 2012 R2.

Initial SCEP certificates visible on 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>

Assumption is that MSCEP-RA CERTIFICATE is expired and has to be renewed.

Solution

Caution: Any changes on Windows Server should be consulted with its administrator first.

1. Identify old private keys

Find private keys associated with the RA certificates on the Active Directory using **certutil** tool. After that locate **Key Container**.

Please note that if the name of your initial MSCEP-RA certificate is different then it should be

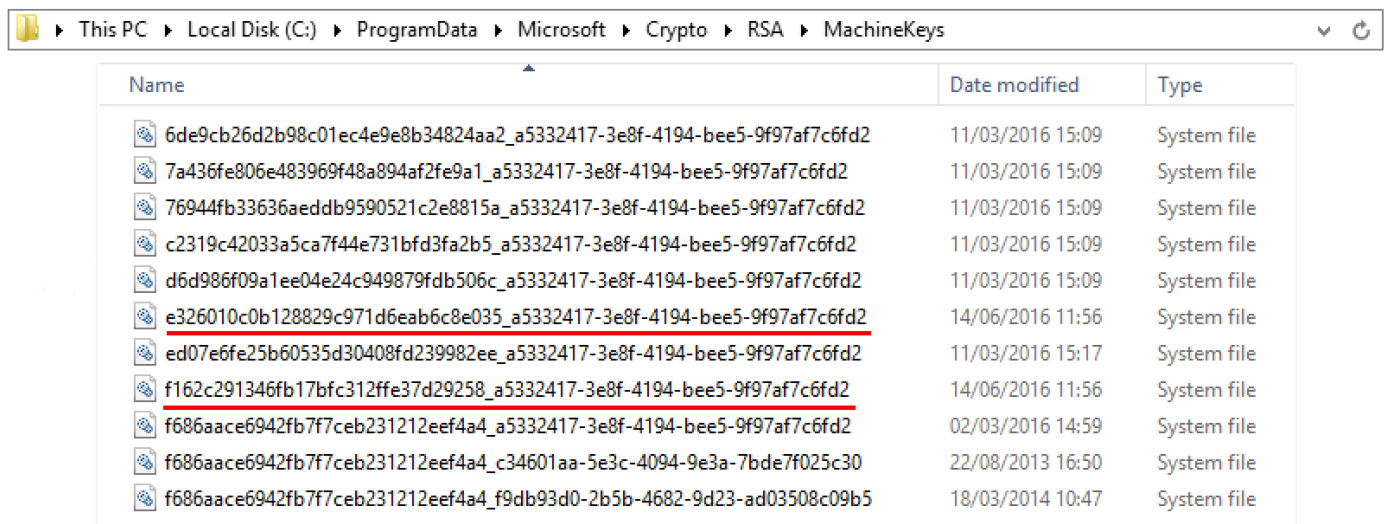
adjusted in this request. However, by default it should contain the computer name.

```
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. Delete old private keys

Delete referring keys manually from the folder below:



3. Delete old MSCEP-RA certificates

After deleting the private keys, remove MSCEP-RA certificates from the MMC console.

MMC > File > Add/Remove Snap-in... > Add "Certificates" > Computer account > Local computer

4. Generate new certificates for SCEP

4.1. Generate the Exchange Enrollment Certificate

4.1.1. Create a file **cisco_ndes_sign.inf** with the content below. This information is used later by the **certreq.exe** tool in order to generate the Certificate Signing Request (CSR):

Tip: If you copy this file template, make sure to adjust it as per your requirements and check if all characters are properly copied (including quotation marks).

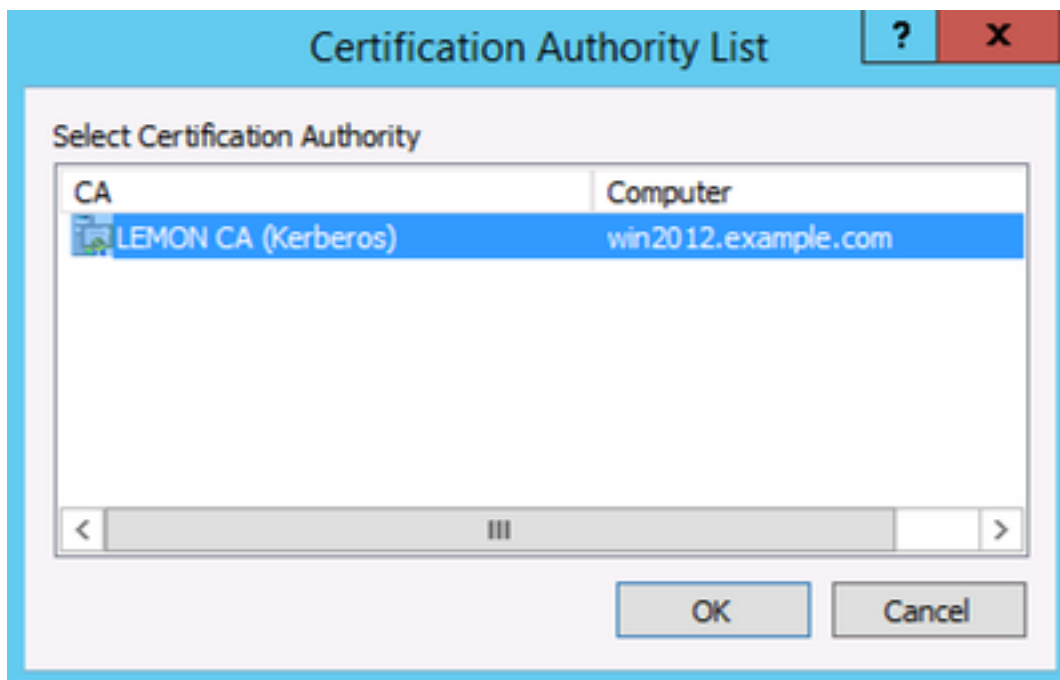
4.1.2. Create CSR based on the .INF file with this command:

If warning dialog **User context template conflicts with machine context** pops up, click OK. This warning can be ignored.

```
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. Submit the CSR with this command:

During this procedure a window pops up and proper CA has to be chosen.



```
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 Accept the certificate issued at the previous step. As a result of this command, the new certificate is imported and moved to the Local Computer Personal store:

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

4.2. Generate the CEP Encryption Certificate

4.2.1. Create a new file **cisco_ndes_xchg.inf**:

Follow the same steps as described in 4.1.

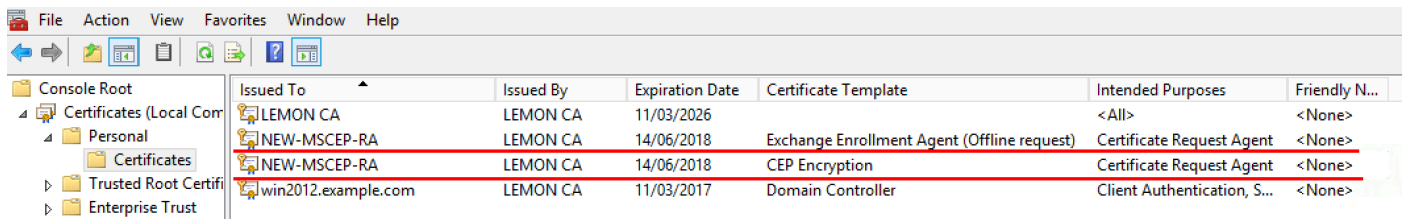
4.2.2. Generate a CSR based on the new .INF file:

4.2.3. Submit the request:

4.2.4: Accept the new certificate by moving it into the Local Computer Personal store:

5. Verify

After completing step 4, two new MSCEP-RA certificates will appear in the Local Computer Personal Store:



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>

Also you can verify the certificates with **certutil.exe** tool (make sure you use the correct new certificate name). MSCEP-RA certificates with new Common Names and new Serial Numbers should be displayed:

```
C:\Users\Administrator\Desktop>certutil -store MY NEW-MSCEP-RA
MY "Personal"
===== Certificate 2 =====
Serial Number: 7a0000000b250f5a9d6c111350000000000c
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 = 320e6480bd159eca7b12283f3f67ee6_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. Restart IIS

Restart Internet Information Services (IIS) server in order to apply the changes:

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

7. Create new SCEP RA profile

On ISE create a new SCEP RA profile (with the same server URL as the old one), so new certificates are downloaded and added to the Trusted Certificates Store:

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. Modify certificate template

Make sure the new SCEP RA profile is specified in the Certificate template used by BYOD (you can check it in *Administration > System > Certificates > Certificate Authority > Certificates Templates*):

Identity Services Engine Administration > Work Centers > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Identity Mapping > Certificates > Logging > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings

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
ISE Internal CA
New_External_Scep
External_SCEP

References

1. [Microsoft Technet zone article](#)
2. [Cisco ISE configuration guides](#)