Konfigurationsanleitung
SCEP (Simple Certificate Enrollment Protocol)
Graphical User Interface (GUI)

08. Oktober 2012 ■ Version 1.0

www.neo-one.de

1.1 Konfiguration des Windows Server 2008

Unter Windows Server 2008 R2 Enterprise SP1 sollten Sie folgende Änderungen für SCEP machen, um die Dienste Active Directory, Web-Services und Zertifikatsserver zu nutzen:

- Installieren Sie Active Directory Service mit dcpromo.exe (Domäne **z.B. neo-one.de**).
- Installieren Sie die Rolle Active Directory Zertifikatdienste (Zertifizierungsstelle und Zertifizierungsstellen Webregistrierung).
    - Unternehmenszertifizierungsstelle.
    - Stammzertifizierungsstelle.
- Fügen Sie den Administrator der Gruppe IIS_IUSRS hinzu.
- Installieren Sie den Rollendienst Registrierungsdienst für Netzwerkgeräte.
    - Administrator / Kennwort
- Öffnen Sie regedit und verändern „UseSinglePassword" in nachfolgendem Pfad auf „1"
    - HKLM → Software → Microsoft → Cryptography → MSCEP → UseSinglePassword
- Starten Sie den WWW-Publishingdienst neu.
- Über folgende URL erhalten Sie das SCEP Kennwort.
    - http://127.0.0.1/certsrv/mscep_admin/

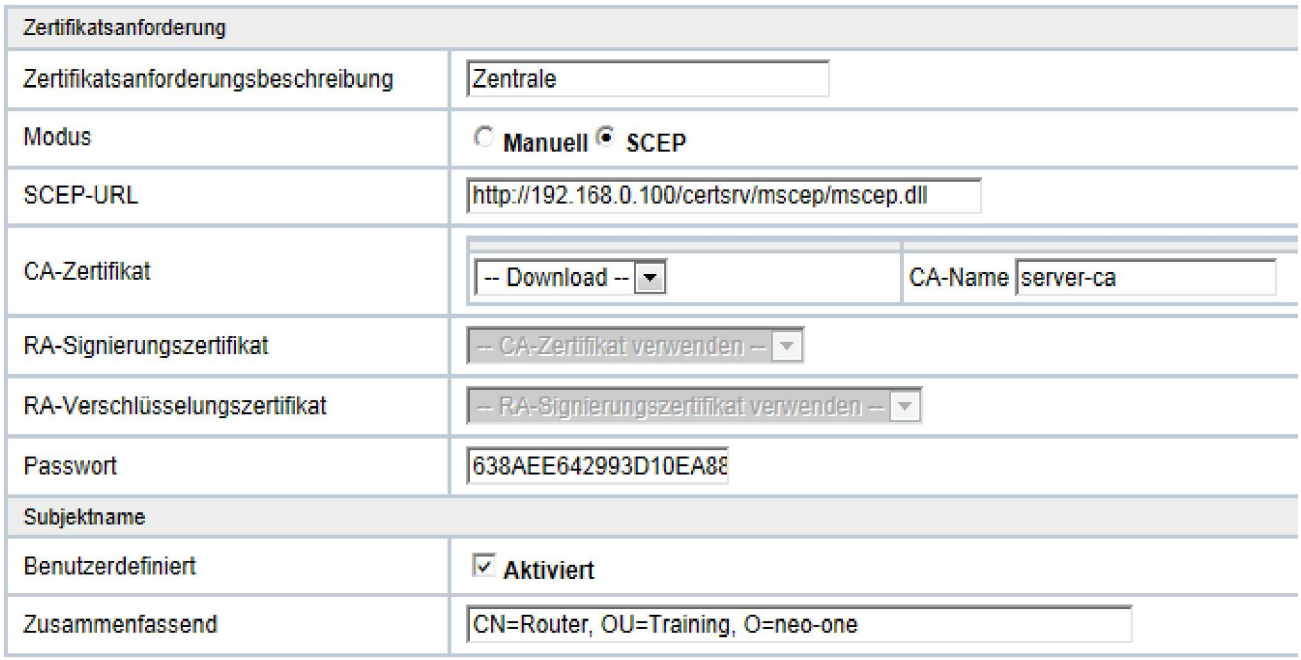
INFO

Sollten Sie einen neuen Benutzer angelegt und diesen der Gruppe IIS_IUSRS hinzugefügt haben, um ihn für den *Registrierungsdienst für Netzwerkgeräte* zu verwenden, müssen Sie sich an einem Rechner mit diesem Benutzer anmelden, um auf die URL **http://127.0.0.1/certsrv/mscep_admin/** zugreifen zu können.

1.2 Zertifikate im Router

Gehen Sie in folgendes Menü, um SCEP im Router zu konfigurieren:

GUI → Zertifikate → Zertifikatsliste → Anforderung



Folgende Punkte sind hier relevant:

Feld	**Bedeutung**
Zertifikatsanforderungs-beschreibung	Geben Sie dem Eintrag und den zu importierenden Zertifikaten einen Namen.
Modus	Bestimmen Sie, ob die Zertifikate manuell oder über das Protokoll SCEP importiert werden.
SCEP-URL	Geben Sie die URL an, über die die Zertifikate beim Windows Server 2008 angefordert werden.
CA-Zertifikat / Name	Geben Sie den Namen des CA Zertifikat an.
Passwort	Geben Sie das SCEP Kennwort der CA an.
Subjektname	Bestimmen Sie die Identitätsmerkmale für das Zertifikat.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Als Zertifikatsanforderungsbeschreibung verwenden Sie z.B. **Zentrale**.
- Wählen Sie bei Modus **SCEP** aus.
- Verwenden Sie als SCEP-URL z.B. **http://192.168.0.100/certsrv/mscep/mscep.dll**
- Bei CA-Zertifikat / Name verwenden Sie z.B. **Download** / **server-ca**
- Tragen Sie bei Passwort z.B. **638AEE642993D10EA882F9BEE22ABC15** ein.

- Konfigurieren Sie bei Subjektname folgende Werte
  - Der Haken bei Benutzerdefiniert ist z.B. **aktiviert**.
  - Bei Zusammenfassend nutzen Sie z.B. **CN=Router, OU=Training, O=neo-one**

1.3 Kontrolle

In der Zertifikatsübersicht sehen Sie nach dem Speichern die importierten Zertifikate

Beschreibung	Subjektname	Typ
Zentrale-ras	MAILTO=ca@neo-one.de, CN=SERVER-CA, OU=Training, O=neo-one, L=Krefeld, ST=NRW, C=DE	Peer
Zentrale-rae	MAILTO=ca@neo-one.de, CN=SERVER-CA, OU=Training, O=neo-one, L=Krefeld, ST=NRW, C=DE	Peer
Zentrale-ca	CN=CA, DC=neo-one, DC=de	Stamm-CA
Zentrale-user	CN=Router, OU=Training, O=neo-one	Eigenes

An der Shell können Sie den Import mit folgendem Befehl sichtbar machen:

- **debug ipsec&**

```
14:13:24 INFO/IPSEC: SPD: created private key index 8
14:13:25 INFO/IPSEC: SCEP 9: Success, received 3648 bytes
14:13:25 INFO/IPSEC: CertMgmt 9: Encountered PKCS#7 certificate with 3 certificates
inside.
14:13:25 INFO/IPSEC: SPD: added certificate 1 ("Zentrale-ras").
14:13:25 INFO/IPSEC: SPD: added certificate 2 ("Zentrale-rae").
14:13:25 INFO/IPSEC: SPD: added CA certificate 3 ("Zentrale-ca").
14:13:25 INFO/IPSEC: CertMgmt 9: Retrieved CA certificate 3, RA Signing certificate
1, RA Encryption certificate 2 for enrollment
14:13:25 INFO/IPSEC: CertMgmt 9: Auto saving in 5 seconds!
14:13:25 INFO/IPSEC: SPD: added certificate 1 ("Zentrale-ras").
14:13:25 INFO/IPSEC: SPD: added certificate 2 ("Zentrale-rae").
14:13:25 INFO/IPSEC: SPD: added CA certificate 3 ("Zentrale-ca").
14:13:26 INFO/IPSEC: SCEP 9: Success, received 1175 bytes
14:13:26 INFO/IPSEC: SPD: added certificate 4 ("Zentrale-user").
14:13:26 INFO/IPSEC: CertMgmt 9: Auto saving in 5 seconds!
14:13:26 INFO/IPSEC: SPD: added certificate 4 ("Zentrale-user").
14:13:31 INFO/IPSEC: CertMgmt 0: Auto saving...
```