Zertifikatsverwaltung mit SCEP

Kurzanleitung

Stand: 2023-07-21

07-26 12:14

1. Zertifikatsverwaltung mit SCEP

Zertifikatbasierte Anmeldung mit

SCEP ist ein Protokoll, das die sichere und skalierbare Ausstellung von Zertifikaten an Netzwerkgeräte über existierende Zertifizierungsstellen vereinfacht.

Mit SCEP holen sich die Geräte ihre Zertifikate selbst. Hierfür muss eine berechtigte Person ein Einmal-Kennwort erstellen, das dem Gerät zur Verfügung gestellt wird. Das Endgerät kann mit diesem zeitlich begrenzt gültigen Kennwort ein Zertifikat vom SCEP-Service anfordern.

Damit die Zertifizierungsstelle (Certificate Authority, CA) mit dem Einmal-Kennwort nicht beliebige Zertifikate ausstellen kann, erstellen Sie eine Vorlage, in der Sie beispielsweise die Zertifikatklassen beschränken können.

Mit SCEP können Sie die Zertifikatsverwaltung beispielsweise für folgende Anforderungen unterstützen:

- 802.1X-Authentifizierung für LAN und WLAN
- VPN-Anbindung über Cisco AnyConnect
- Anbindung über Citrix NetScaler Gateway

Eine Kombination mehrerer Anforderungen ist jedoch nicht möglich.

Die eLux-Implementierung basiert auf dem **OpenSCEP**-Projekt. Die folgende Beschreibung setzt die Verwendung von Windows NDES voraus.

2. Windows als SCEP-Server

Hinweis
Ab Windows Server 2012 ist NDES (Network Device Enrollment Service) in die Zertifizierungsstelle (CA) eingebaut.
Die beschriebene Vorgehensweise ist als Beispiel zu verstehen und kann je nach Version und Umgebung abweichen.

NDES installieren

1. Installieren Sie die Serverrolle **AD CS** mit Feature **Network Device Enrolment Service**.
2. Richten Sie ein Dienstkonto für NDES ein, das später auf der CA entsprechend berechtigt wird.
3. Tragen Sie die Informationen für das Zertifikat der Registrierungsstelle (Registration Authority, RA) ein, damit ein Signatur-Zertifikat für diesen Enrollment-Prozess ausgestellt wird.
4. Legen Sie die Schlüssellänge fest.

In der IIS-Konsole werden die neuen virtuellen Verzeichnisse unterhalb der Default Web Site angezeigt.

Templates konfigurieren

Der SCEP-Server verwendet Templates zur Einreichung an die CA.

1. Hinterlegen Sie den LDAP-Namen des Templates in der Registry:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP

Default:	`IPSecIntermediateOffline`
EncryptionTemplate	<*templatename*>
GeneralPurposeTemplate	<*templatename*>
SignatureTemplate	<*templatename*>

2. Fügen Sie der CA das neue Template hinzu.
3. Konfigurieren Sie die Verwendung eines Einmal-Kennwortes in der Registry (Gültigkeitsdauer, maximale Anzahl).

Mit dem Einmalkennwort kann ein Client, der SCEP/NDES unterstützt, sich direkt an den SCEP-Server wenden und ein Zertifikat anfordern. Der Client verbindet sich zum Windows SCEP-Server mit der URL http://<CA_FQDN>/certsrv/mscep/mscep.dll

Einmal-Kennwort konfigurieren

entweder

- Kennwort deaktivieren (Variante A):
  [`HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP\EnforcePassword`] auf 0 setzen

oder

- festes Kennwort definieren (Variante B):
  [`HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP\UseSinglePassword`]

Berechtigungen für NDES-Dienstkonto setzen

- Setzen Sie die Berechtigung auf `full control`.

SCEP Application pool settings anpassen

- Setzen Sie die Option **Load User Profile** von `false` auf `true`.

Anfordern der Einmalkennworte

1. Melden Sie sich auf der SCEP-Administator-Webseite mit Ihrem NDES-Dienstkonto an:
   `http://<CA_FQDN>/certsrv/mscep_admin/`
2. Kopieren Sie das Challenge-Kennwort in die Konfigurationsdatei `scep.ini`.

3. SCEP für eLux konfigurieren

Damit die eLux-Clients die Zertifkatsverteilung durch SCEP nutzen können, bereiten Sie die Clients durch folgende Schritte vor.

Hinweis
Das eLux-Paket **Network Access Control** und das hierin enthaltene Feature-Paket **SCEP** muss auf den Gerätenn installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

1. Konfigurieren Sie den SCEP-Agenten über die Datei `scep.ini` und übertragen Sie die Konfigurationsdatei anschließend mit der Scout-Funktion Dateien auf die Geräte . Für weitere Informationen siehe SCEP ini-Datei konfigurieren.
2. Stellen Sie sicher, dass die eLux-Clients die korrekte Zeit haben. Am besten konfigurieren Sie einen Zeitserver.

   Die lokale Zeit muss mit der Zeit der Zertifizierungsstelle übereinstimmen.
3. Um den SCEP-Agenten zu aktivieren, fügen Sie der Datei `terminal.ini` auf den Geräten folgenden Eintrag hinzu. Verwenden Sie die Funktion **Erweiterte Dateieinträge** der Scout Console:

Datei	`/setup/terminal.ini`
Abschnitt	`Network`
Eintrag	`SCEP`
Wert	`true`

   Beachten Sie die Groß-/Kleinschreibung.
   Für weitere Informationen siehe Erweiterte Dateieinträge im Scout-Handbuch.
4. Um SCEP für die 802.1X-Authentifizierung für LAN einzusetzen, aktivieren Sie in der Scout Console für die relevante OU in der **Netzwerk**-Geräte-Konfiguration für das LAN-Profil die Option **Erweitert > IEEE 802.1X-Authentifizierung > Aktivieren**. Für weitere Informationen siehe 802.1X für eLux konfigurieren in der 802.1X-Anleitung.

   Wenn Sie SCEP jedoch für eine andere Anforderung einsetzen möchten, stellen Sie sicher, dass die oben genannte Option für das Netzwerkprofil **LAN** nicht aktiviert ist.

Der Client generiert eine WPA-Konfigurationsdatei aus der Vorlage `/setup/scep/wpa.conf.scep`. Wenn Sie jedoch eine eigene WPA-Konfigurationsdatei nach `/setup/scep/wpa.conf` übertragen haben, hat diese Vorrang.

3.1. Zertifikate für SCEP

Folgende Zertifikate werden vom SCEP-Agenten standardmäßig in `/setup/cacerts/scep` abgelegt.

client.pem	Client-Zertifikat	
client.key	Privater Schlüssel des Client-Zertifikats	`2048` oder `4096`[1] RSA-Schlüssel kann im TPM 2.0-Modul gespeichert werden
serverca.pem	Server CA-Zertifikat	
serverca.key	Server CA-Schlüssel	notwendig für Verlängerung der Zertifikate
serverca.sig	Server CA Signatur	notwendig für Verlängerung der Zertifikate
serverra.pem	RADIUS Server-Zertifikat	

Clients mit TPM 2.0

Die entsprechenden Authentifizierungsverfahren über WPA-Supplicant für kabelgebundene Ethernet-Verbindungen und über IEEE 802.1x für WLAN-Komponenten berücksichtigen beide Speichermöglichkeiten für den privaten SCEP-Schlüssel – das Dateisystem und das TPM 2.0-Modul.

Client-Zertifikate werden immer im Dateisystem gespeichert.Das Rollout-Verfahren, mit dem die Clients die Client-Zertifikate initial erhalten, wird ausschließlich über kabelgebundene Ethernet-Verbindungen durchgeführt.Vorhandene Zertifikate können sowohl über kabelgebundene Ethernet-Verbindungen als auch über WLAN erneuert werden.

Standardmäßig wird auch der private Schlüssel des SCEP Client-Zertifikats im Dateisystem gespeichert, und zwar unter `/setup/cacerts/scep` bzw. in dem in der `scep.ini` definierten Verzeichnis.Bei einem Update von eLux auf eine Version mit TPM 2.0-Unterstützung bleiben vorhandene private Schlüssel für SCEP Client-Zertifikate im Dateisystem gespeichert.

Privater Schlüssel im TPM 2.0-Modul

- Um das TPM 2.0-Modul für den privaten Schlüssel zu nutzen, verwenden Sie folgenden Eintrag:

Datei	`scep.ini`	
Abschnitt	`Certificate`	
Eintrag	`UseTPM2`	
Wert	`true`	Standardmäßig steht der Wert auf `false`.

[1] ab eLux RP 6 2204

Dieser Parameter sorgt dafür, dass der private Schlüssel für jedes TPM 2.0-Gerät im TPM-Modul erzeugt wird.[1] Er wird nur dort gespeichert und kann weder angezeigt noch exportiert werden.Der Schlüssel verlässt niemals das TPM-Modul des Gerätes.

Bei einer Verlängerung des Zertifikats wird der private Schlüssel wiederverwendet.

Der SCEP Agent erstellt via openssl eine Zertifikatanforderung (CSR) mit dem öffentlichen Schlüssel des TPM-Moduls.Wenn eine Verbindung zu einem 802.1X-gesichertem Port aufgebaut wird, wird geprüft ob ein gültiges Zertifikat vorliegt.Das Zertifikat muss mit dem privaten Schlüssel aus dem TPM-Chip signiert sein.Wenn das Zertifikat nicht vorhanden oder ungültig ist, wird die Verbindung abgelehnt.

Die Datei `client.key` bleibt im Dateisystem erhalten, enthält aber nur noch die Information zum öffentlichen Schlüssel.Durch den beibehaltenen Dateinamen ist gewährleistet, dass auch Geräte ohne TPM das gleiche Zertifikat nutzen können.

Um den Schlüssel aus dem TPM 2.0-Modul zu löschen, löschen Sie das TPM im BIOS/UEFI.Wir empfehlen, vorher Zertifikate zurückzuziehen, die noch Gültigkeit besitzen.

[1] ab eLux RP 6 2101

4.1. SCEP ini-Datei konfigurieren

Hinweis
Für die Konfigurationsdatei des SCEP-Agenten finden Sie eine Beispieldatei auf den Geräten:
`/setup/scep/scep.ini.sample`

1. Erstellen Sie die Textdatei `scep.ini` und fügen Sie die unten beschriebenen Abschnitte und Einträge ein.
2. Übertragen Sie die Datei `scep.ini` mit Hilfe der Scout- Funktion **Konfigurierte Dateiübertragung** auf die Geräte in das Verzeichnis `/setup/scep/`. Für weitere Informationen siehe Erweiterte Geräte-Konfiguration > Dateien im Scout-Handbuch.

Aus den Daten der `scep.ini` wird die Zertifikatanforderung erstellt. Optional können Sie die Zertifikatanforderung durch weitere Attribute erweitern. Für weitere Informationen siehe "Erweiterte SCEP-Zertifikatanforderung" auf Seite 15.

Abschnitte und Einträge für `scep.ini`

Abschnitt	Eintrag	Beschreibung	Beispiel
Admin	URI	Adresse des SCEP-Servers (URI)	`URI=http://ca.w2k12.sampletec-01.com/certsrv/mscep/`
	PROXY	Proxy-Server (optional)	`PROXY=proxy.sampletec-01.com:3800`

Abschnitt	Eintrag	Beschreibung	Beispiel
	ReNew	Anzahl der Tage, bevor das Zertifikat abläuft und das Gerät ein neues Zertifikat anfordert (Zeitspanne für Erneuerung) Ab diesem Tag versucht der Client, das Zertifikat zu erneuern. Der Wert muss kleiner sein als die Gültigkeitsdauer des Zertifikates. Standard: `30`	`ReNew=30` (Standard)
	ReNewCheckOnlyClient[1]	Alternative zu `ReNew`: Im Unterschied zu `ReNew` wird nur das Client-Zertifikat geprüft, aber nicht CA- und RA-Zertifikate	`ReNew=30` (Standard)
	ExpireCheck	Zeitintervall in Tagen, wie oft auf das ReNew-Datum geprüft wird	`ExpireCheck=1` (Standard)
	challengePassword	Einmal-Kennwort für den Request einmalig gültig für 60 Minuten Das Kennwort wird nach der erfolgreichen Übertragung der Zertifikate gelöscht.	(A): `challengePassword=12345` (B): `challengePassword=<über http://CA_FQDN/certsrv/mscep_admin/ angefordertes Kennwort>`

[1] ab eLux RP 6 2302.1000

Certificate	CNTYPE	Typ (`autoip|ip|dns|autodns|dnsfqdn|email`) `autoip` Die IP-Adresse des Gerätes wird als **CN** verwendet. `ip` Die von Ihnen als **CN** angegebene IP-Adresse der `scep.ini` (siehe nächste Option) wird verwendet. `dns` Der von Ihnen als **CN** angegebene Name wird verwendet (siehe nächste Option). `autodns` Der Hostname aus der `terminal.ini` wird als CN verwendet. `dnsfqdn` Der Hostname aus der `terminal.ini` mit angefügtem Domain-Namen wird als **CN** verwendet. `email` Die von Ihnen als **CN** angegebene Mail-Adresse wird verwendet (siehe nächste Option).	`CNTYPE=email`
	CN	Zertifikat/Name Wird für `CNTYPE=autoip|autodns|dnsfqdn` automatisch gesetzt	`CN=userxxx@sampletec-01.com`

	OU
	ORGANIZATION
	LOCALITY
	STATE
		Zertifikat/Attribute (optional)	`OU=TestLab`
			`ORGANIZATION=SampleTec`
			`LOCALITY=Karlsruhe`
			`STATE=BW`

	OU1 OU2 OU3 OU4 OU5 OU6	Weitere Attribute für bis zu 6 OUs (optional) Die hier angegebenen OUs können können für eine Zertifikatanforderung verwendet werden.	OU1=Testlab OU2=KA_QA OU3=KA_DEV
	COUNTRY	Zertifikat/Land	`COUNTRY=DE`
	KEYLEN	Schlüssellänge (aus Zertifikatsvorlage) Erlaubte Werte: `2048` und `4096`[1] Eine falsche Schlüssellänge führt zur Ereignisanzeige **Falsches Challenge-Password** Wenn ein `4096`-Schlüssel nicht im TPM erzeugt werden kann(bei TPM 2.0 und **UseTPM2**), wird als Fallback ein 4k-RSA-Schlüssel im Dateisystem erzeugt.	`KEYLEN=2048`
	CertStore	Der Zertifikatspeicher kann frei gewählt werden. Mit diesem Parameter können Sie ein neues Verzeichnis angeben, das der SCEP-Agent am Gerät erstellt. Wenn Sie den Standard-Pfad `/setup/cacerts/scep` angeben, wird der private Schlüssel für das SCEP Client-Zertifikat für TPM 2.0-Geräte im TPM 2.0-Modul gespeichert.	`CertStore=/setup/cacerts/scep`

[1] ab eLux RP 6 2204

Zusätzliche Informationen

- Die Ablage kann für jede Zertifikatsdatei einzeln definiert werden.

  Die drei Parameter für die Dateiablage haben höhere Priorität als der Parameter **CertStore**.
  Die angegebenen Verzeichnisse müssen vorhanden sein.
  Client-Zertifikatsdateien können verkettet werden.

- Für den privaten Schlüssel (wenn im Dateisystem) können Zugriffsrechte gesetzt werden.
- Zertifikate können auf Gültigkeit gemäß Zertifikatssperrliste (CRL) überprüft werden[1]

Certificate	CA_Path	Pfad und Dateiname für Server CA-Zertifikat	`CA_Path=/setup/cacerts/scep/serverca.pem` (Standard)
	Client_Path	Pfad und Dateiname für das Client-Zertifikat	`Client_Path=/setup/cacerts/scep/client.pem` (Standard)
	ClientKey_Path	Pfad und Dateiname für die private Schlüsseldatei des Client-Zertifikats	`ClientKey_Path=/setup/cacerts/scep/client.key` (Standard)

Hinweis
Geben Sie für **Client_Path** und **ClientKey_Path** denselben Wert an, beispielsweise `/setup/cacerts/scep/client.pem`, wenn Sie die beiden Dateien aneinanderhängen möchten.

RA_Path	Pfad und Dateiname für RADIUS Server-Zertifikat	`/setup/cacerts/scep/serverra.pem` (Standard)

[1] ab eLux RP 6 2101

MODE	Bei zusätzlicher Nutzung eines RADIUS Server-Zertifikates: `RA` Erlaubte Werte: `CA` (Standard), `RA`	`CA`
ClientKey_Permission	Zugriffsrechte für die private Schlüsseldatei `0400` Nur mit Root-Rechten lesbar (Standard) `0444` Auch für Benutzer lesbar	`ClientKey_Permission=0400`
UseTPM2	Für Geräte mit TPM 2.0-Modul Ab eLux RP 6 2101: Der private Schlüssel wird im TPM 2.0-Modul erzeugt und verlässt dieses nicht. eLux RP 6.10 und 11: Die private Schlüsseldatei wird im TPM 2.0-Modul gespeichert. Erlaubte Werte: `false` (Standard), `true` Für weitere Informationen siehe "Zertifikate für SCEP" auf Seite 6.	`UseTPM2=true`
TPM2Fallback[1]	Wenn der private Schlüssel nicht im im TPM 2.0-Modul gespeichert werden kann (beispielsweise auf Geräten mit anderer TPM-Version), wird er im Dateisystem gespeichert. Erlaubte Werte: `true` (Standard), `false` `false`: Es gibt keinen Fallback. Auf Geräten ohne TPM 2.0 wird der Schlüssel gar nicht gespeichert.	`TPM2Fallback=true`

[1] ab eLux RP 6 2204

	CrlCheck[1]	Geben Sie optional bis zu fünf zusätzliche Zertifikate an (neben CA_Path, Client_Path und RA_Path), die der SCEP-Agent auf Gültigkeit gemäß Zertifikatssperrlisten (CRL) prüfen soll. Die Überprüfung findet bei jedem Verbindungsaufbau statt oder, falls die Verbindung länger bestehen bleibt, in dem Zeitintervall, den Sie unter `ExpireCheck` definiert haben.	`CrlCheck1=/setup/cacerts/myrootca.pem` `CrlCheck2=/setup/cacerts/myintermediate.pem`
	CrlCheckEnabled[2]	`true` (Standard): Prüfung aller Zertifikate auf Gültigkeit gemäß Zertifikatssperrlisten (CRL) `false`: Es findet keine Prüfung auf CRLs statt.	`CrlCheckEnabled=true`
	FirstCrlOnly[3]	`true`: Wenn mehrere CRLs eingetragen sind, wird nur die erste heruntergeladen und geprüft. Dies reduziert die Last auf der PKI-Infrastruktur. `false` (Standard): Alle vorhandenen CRLs werden heruntergeladen und geprüft.	`FirstCrlOnly=true`

[1] ab eLux RP 6 2101
[2] ab eLux RP 6 2110
[3] ab eLux RP 6 2204

5.1. Erweiterte SCEP-Zertifikatanforderung

Hinweis
Diese Funktion ist nur notwendig, wenn Sie den SCEP-Agenten mit weiteren Attributen, die nicht über die `scep.ini` gesetzt werden, konfigurieren möchten.

Die Zertifikatanforderung wird aus den Werten der Datei `scep.ini` erstellt und ist auf dem Gerät in Form der Datei `/setup/scep/clientreq.conf.in` vorhanden. Diese Datei wird bereits mit SCEP als Vorlage installiert und hat standardmäßig folgende Einträge:

```
[req]
prompt=no
distinguished_name=req_distinguished_name
string_mask=nombstr
attributes=req_attributes

[req_attributes]
challengePassword=__CHALLENGEPASSWORD__

[req_distinguished_name]
C=__COUNTRY__
ST=__STATE__
L=__LOCALITY__
O=__ORGANIZATION__
OU=__OU__
1.OU=__OU1__
2.OU=__OU2__
3.OU=__OU3__
4.OU=__OU4__
5.OU=__OU5__
6.OU=__OU6__
CN=__CN__

[__X509V3__]
subjectAltName=critical,__CNTYPE__:__ALTNAME__
```

Die mit Unterstrichen gekennzeichneten Felder sind Variablen und werden durch die entsprechenden Werte der `scep.ini` ersetzt.

Wenn die in der `scep.ini` bereitgestellten Attribute ausreichen, ist das Bearbeiten der Datei `clientreq.conf.in` nicht notwendig.

Zertifikatanforderung um weitere Attribute erweitern

1. Holen Sie die mit SCEP installierte Datei `/setup/scep/clientreq.conf.in` von einem Gerät, beispielsweise mit Hilfe der **Diagnose**-Funktion.

2. Bearbeiten Sie die Datei. Fügen Sie beliebige weitere openSSL-Abschnitte und -Attribute hinzu. Für weitere Informationen siehe https://www.openssl.org/docs/man1.0.2/man1/openssl-req.html
3. Übertragen Sie die Datei mit Hilfe der Funktion **Konfigurierte Dateiübertragung** auf die relevanten Clients nach `/setup/scep/clientreq.conf.in`.

Hinweis
Diese Datei - und nicht die `scep.ini` - ist die Quelle für die Zertifikatanforderung. Löschen Sie nur Felder, die Sie nicht benötigen!

---

6. Diagnose für SCEP

Client-Zertifikat in einer Shell angezeigen

- Verwenden Sie folgendes Kommando:
  `openssl x509 -in /setup/cacerts/scep/client.pem -noout -text`

Alle Informationen des Zertifikats werden angezeigt.

Protokolldateien anzeigen

1. Schalten Sie die erweitere Protokollierung ein.
2. Fordern Sie die Diagnosedateien an. Für weitere Informationen siehe Diagnose für SCEP im Scout-Handbuch.

`/tmp/systemd-journal.log`	Protokolldatei für Netzwerk-Aktivitäten
`/setup/logs/scepagent.log` [1]	Protokolldatei des SCEP-Agenten, enthält den letzten Zertifikat-Transfer Diese Datei ist nicht in der Vorlage `#System` enthalten, sondern muss über eine eigene Vorlage definiert werden. Für weitere Informationen siehe Geräte-Diagnose im Scout-Handbuch.

[1] temporäre Version unter `/var/log/scepagent.log`