IEEE 802.1X-Authentifizierung mit SCEP

Kurzanleitung

Stand: 2020-06-19

06-23 03:29

1. IEEE 802.1X-Authentifizierung mit Unterstützung von SCEP

Zertifikatbasierte Anmeldung mit 802.1X

IEEE 802.1X ist ein Standard zur Authentifizierung und Autorisierung in IEEE-802-Rechnernetzen. Die Authentifizierung eines Client-Gerätes (Supplicant) erfolgt am Netzwerkzugang eines LAN oder WLAN durch einen Authenticator. Der Authenticator kann ein IEEE 802.1X-fähiger Router oder WLAN-Access-Point sein. Der Authenticator überprüft die Authentifizierungsinformationen mit Hilfe eines Authentifizierungsservers (RADIUS).

Als RADIUS-Server können Sie beispielsweise den Microsoft Netzwerkrichtlinienserver (Network Policy Server, NPS) oder die freie Software freeRADIUS einsetzen.

Der Supplicant wird in Form einer Softwareimplementierung umgesetzt. Wir unterstützen die freie Software-Implementierung **wpa_supplicant**.

Der Standard empfiehlt das Extensible Authentication Protocol (EAP) oder das PPP-EAP-TLS Authentication Protocol zur Authentifizierung.

Zertifikatsverwaltung mit SCEP

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.

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-Clients konfigurieren

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

1. Stellen Sie sicher, dass das eLux-Paket **Network Access Control** und das hierin enthaltene Feature-Paket **SCEP** auf den Clients installiert ist. Dies kann eine Anpassung der Image-definitions-Datei am Webserver mit Hilfe von ELIAS erfordern.
2. Konfigurieren Sie den SCEP-Agenten über die Datei `scep.ini` und übertragen Sie die Konfigurationsdatei anschließend mit der Scout Enterprise-Funktion Dateien auf die Clients. Für weitere Informationen siehe SCEP ini-Datei konfigurieren.
3. 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.
4. Um den SCEP-Agenten zu aktivieren, fügen Sie der Datei `terminal.ini` auf den Clients folgenden Eintrag hinzu. Verwenden Sie die Funktion **Erweiterte Dateieinträge** der Scout Enterprise-Konsole:

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

   Beachten Sie die Groß-/Kleinschreibung.
   Für weitere Informationen siehe Erweiterte Dateieinträge im Scout Enterprise-Handbuch.

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.[1]

3.1. Zertifikate für SCEP

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

client.pem	Client Zertifikat	
client.key	Privater Schlüssel des Client-Zertifikats	Ausnahme siehe unten
serverca.pem	Server CA Zertifikat	
serverca.key	Server CA-Schlüssel	notwendig für den Request
serverca.sig	Server CA Signatur	notwendig für den Request

[1] ab eLux RP 5.7.1000

Thin Clients mit TPM 2.0

– ab eLux RP 6.7 –

Wenn ein TPM 2.0-Modul im Thin Client verbaut ist, wird der private Schlüssel für das SCEP Client-Zertifikat standardmäßig nicht im Dateisystem, sondern im TPM 2.0-Modul gespeichert. Dies erfolgt automatisch und bedarf keiner gesonderten Konfiguration.

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.

Beim Update von eLux auf eine Version mit TPM 2.0-Unterstützung werden vorhandene private Schlüssel für SCEP Client-Zertifikate vom Dateisystem in das TPM 2.0-Modul verschoben.

Client-Zertifikate werden weiterhin 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.

Privaten SCEP-Schlüssel aus TPM 2.0-Modul löschen

- Verwenden Sie für die relevanten Geräte in der Scout Enterprise-Konsole das Kommando **Grundzustand** mit der Option **Scout Enterprise Server-Adresse am Client löschen**.

Privaten SCEP-Schlüssel außerhalb TPM 2.0-Modul speichern

- Um die private Schlüsseldatei des SCEP Client-Zertifikats im Dateisystem zu speichern, definieren Sie folgenden `terminal.ini`-Eintrag:[1]

Datei	`/setup/terminal.ini`	
Abschnitt	`Network`	
Eintrag	`DisableSCEP2TPM`	
Wert	`true`	Standardmäßig steht der Wert auf `false`.

  Für weitere Informationen siehe Erweiterte Dateieinträge im **Scout Enterprise**-Handbuch.

Die private Schlüsseldatei wird dann im Zertifikatspeicher unter `/setup/cacerts/scep` bzw. in dem in der `scep.ini` definierten Verzeichnis gespeichert.

[1] ab eLux RP 6.9

3.2. SCEP ini-Datei konfigurieren

Hinweis
Für die Konfigurationsdatei des SCEP-Agenten finden Sie eine Beispieldatei auf den Clients: `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 Enterprise- Funktion **Konfigurierte Dateiübertragung** auf die Clients in das Verzeichnis `setup/scep/`. Für weitere Informationen siehe Erweiterte Geräte-Konfiguration > Dateien im Scout Enterprise-Handbuch.

Aus den Daten der `scep.ini` wird die Zertifikatanforderung erstellt. Optional können Sie die Zertifikatanforderung durch weitere Attribute erweitern.[1] Für weitere Informationen siehe "Erweiterte SCEP-Zertifikatanforderung" auf Seite 10.

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`
	ReNew	Anzahl der Tage, bevor das Zertifikat abläuft Ab diesem Tag versucht der Client, das Zertifikat zu erneuern.	`ReNew=30`
	ExpireCheck	Zeitintervall in Tagen, wie oft auf das ReNew-Datum geprüft wird	`ExpireCheck=1`

[1] ab eLux RP 6.8

Abschnitt	Eintrag	Beschreibung	Beispiel
	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>`

Hinweis

Nur für eLux RP 5: Wenn Sie das Kennwort in der Registry deaktiviert haben (Variante A), müssen Sie trotzdem einen Dummy-Wert angeben, der nicht ausgewertet wird.

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`[1] 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`

[1] ab eLux RP 6.7

	CN	Zertifikat/Name Wird für `CNTYPE=autoip|autodns|dnsfqn` automatisch gesetzt	`CN=userxxx@sampletec-01.com`

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

	OU1[1] OU2 OU3 OU4 OU5 OU6	Weitere Attribute für bis zu 6 OUs[2] (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) Die maximale Länge beträgt `2048`. Eine falsche Schlüssellänge führt zur Ereignisanzeige **Falsches Challenge-Password**	`KEYLEN=2048`
	CertStore[3]	Der Zertifikatspeicher kann ab eLux RP 6.8 frei gewählt werden.	`CertStore=/setup/cacerts/scep`

Hinweis

Wenn ein TPM 2.0-Modul im Thin Client verbaut ist, wird der private Schlüssel für das SCEP Client-Zertifikat nur dann im TPM 2.0-Modul gespeichert, wenn Sie den Standard-Pfad `/setup/cacerts/scep` angeben.

[1] ab eLux RP 6.8
[2] ab eLux RP 6.8
[3] ab eLux RP 6.8

3.3. Erweiterte SCEP-Zertifikatanforderung

– ab eLux RP 6.8 –

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 Makros und werden durch die Werte aus der `scep.ini` ersetzt.

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

4. 802.1X konfigurieren

Hinweis
802.1X können Sie für LAN oder WLAN konfigurieren. Die Vorgehensweise unterscheidet sich in der Ablage der Konfigurationsdatei und einigen Parametern. Für weitere Informationen siehe WPA-Supplicant konfigurieren.

1. Stellen Sie sicher, dass das eLux-Paket **WLAN drivers** und das hierin enthaltene Feature-Paket **WPA supplicant** auf den Clients installiert ist. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.
2. Übertragen Sie die benötigten Zertifikate mit der Scout Enterprise-Funktion Dateien auf die Clients nach `/setup/cacerts`.

   Hinweis
   Die Zertifikate Ihrer RADIUS-Umgebung benötigen als Common Name (CN) den FQDN.

3. Konfigurieren Sie die Datei `wpa.conf` und übertragen Sie die Datei anschließend mit der Scout Enterprise-Funktion Dateien auf die Clients. Für weitere Informationen siehe WPA-Supplicant konfigurieren.
4. Wenn Sie SCEP verwenden, können Sie die Datei `wpa.conf` alternativ über die Vorlage `wpa.conf.scep` generieren lassen. Für weitere Informationen siehe WPA-Konfiguration über Vorlage.
5. Aktivieren Sie in der Scout Enterprise-Konsole, für die relevante OU, in der Geräte-Konfiguration unter **Netzwerk > LAN > Erweitert > IEEE 802.1X-Authentifizierung** die Option **Aktivieren**.

Wenn die Konfiguration korrekt ist und die benötigten Zertifikate ausgerollt sind, können Sie Geräte am 802.1X-Port verwenden.

4.1. WPA-Supplicant konfigurieren

Hinweis
Für die Konfigurationsdatei des WPA-Supplicant finden Sie Beispieldateien auf den Clients: `setup/scep/wpa.conf.*`

1. Erstellen Sie eine individuelle Konfigurationsdatei `wpa.conf`.

   Standardmäßig enthält die Datei folgende Angaben:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
ap_scan=0
network={
   key_mgmt=IEEE8021X
   eapol_flags=0
   eap=TLS
   identity="Common Name wie im Zertifikat angegeben"
   ca_cert="/setup/cacerts/scep/serverca.pem"
   client_cert="/setup/cacerts/scep/client.pem"
   private_key="/setup/cacerts/scep/client.key"
   }
```

   Hinweis
   Für `identity` können Sie alternativ den Hostnamen des Gerätes über eine Variable setzen:[1]
   `identity="__HOSTNAME__"`
   Korrekte Schreibweise: Zwei Unterstriche gefolgt von dem Wort `HOSTNAME` (in Großbuchstaben) gefolgt von zwei Unterstrichen.

   Fügen Sie weitere Einträge entsprechend Ihrer CA-Implementierung hinzu, beispielsweise wenn Sie auf eine externe Stammzertifizierungsstelle zugreifen:

```
ca_cert="/setup/cacerts/<root_extern>.pem"
ca_cert="/setup/cacerts/<intermediate_extern>.pem"
ca_cert="/setup/cacerts/<subordinate_intern>.pem"
ca_cert="/setup/cacerts/<radius>.ssl"
```

   Wenn das RADIUS-Zertifikat statt FQDN den NetBIOS-Namen enthält, verwenden Sie folgende Einträge:

```
ca_cert="/setup/cacerts/<intermediate>.pem"
ca_cert="/setup/cacerts/<root>.pem"
```

[1] ab eLux RP 6.9

Achtung

Die Groß-/Kleinschreibung der Zertifikat-Dateinamen muss mit der Schreibweise der übertragenen Zertifikat-Dateien übereinstimmen.

2. Übertragen Sie die Konfigurationsdatei `wpa.conf` mit Hilfe der Scout Enterprise- Funktion **Konfigurierte Dateiübertragung** auf die Clients in folgendes Verzeichnis:

LAN	`setup/scep/`
WLAN	`setup/wlan/`

Für weitere Informationen siehe Erweiterte Geräte-Konfiguration > Dateien im **Scout Enterprise**-Handbuch.

Für weitere Informationen zur 802.1X-Konfiguration für WLAN siehe WPA-Unterstützung im **Scout Enterprise**-Handbuch.

4.2. WPA-Konfiguration über Vorlage

– nur bei Verwendung von SCEP –

Hinweis

Die folgenden Informationen beziehen sich nur auf die Konfiguration von 802.1X für LAN.

Wenn Sie SCEP einsetzen, können Sie die auf den Clients bereitgestellte Vorlage `setup/scep/wpa.conf.scep` verwenden:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
ap_scan=0
network={
  key_mgmt=IEEE8021X
  eapol_flags=0
  eap=TLS
  identity="__IDENTITY__"
  ca_cert="/setup/cacerts/scep/serverca.pem"
  client_cert="/setup/cacerts/scep/client.pem"
  private_key="/setup/cacerts/scep/client.key"
  }
```

Hinweis

Die Variable __IDENTITY__ wird durch den CN des Client-Zertifikats ersetzt.

Der Client wertet diese Vorlage aus und erstellt die Datei `wpa.conf`, wenn folgende Bedingungen erfüllt sind:

- SCEP ist für den Client in der `terminal.ini` konfiguriert.
- Es ist keine individuelle `/setup/scep/wpa.conf` vorhanden.[1]

Wenn erforderlich passen Sie die Vorlage an und übertragen sie mit Hilfe der Scout Enterprise-Funktion **Konfigurierte Dateiübertragung** auf die Clients nach `setup/scep/wpa.conf.scep`. Beachten Sie, dass eine eventuell vorhandene individuelle `/setup/scep/wpa.conf`[2] Vorrang hat.[3]

Hinweis

Die aus der Vorlage generierte `wpa.conf` wird in einem temporären Verzeichnis erstellt und ist nur über die Diagnosedateien zu sehen.

[1] ab eLux RP 5.7.1000

[2] see WPA-Supplicant konfigurieren

[3] ab eLux RP 5.7.1000

5. Diagnose für SCEP und 802.1X

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 Diagnosedateien anfordern im Scout Enterprise-Handbuch.

`/var/log/messages`	Protokolldatei des Kernels[1]
`/tmp/systemd-journal.log`	Protokolldatei für Netzwerk-Aktivitäten[2]
`/setup/logs/scepagent.log`[3]	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 Diagnosedateien konfigurieren im Scout Enterprise-Handbuch.

[1] relevant bis eLux RP 6.3
[2] ab eLux RP 6.4
[3] temporäre Version unter `/var/log/scepagent.log`