

SSL-Infrastruktur unter UCS

Thema:	Dokumentation der eingebauten SSL-Infrastruktur unter UCS
Datum:	3. April 2011
Seitenzahl:	10
Versionsnummer:	8436
Autoren:	Univention GmbH feedback@univention.de

Inhaltsverzeichnis

1	Einführung	3
2	Einrichten der Root-CA	4
3	Zertifikatsverwaltung mit univention-certificate	4
3.1	Anlegen von Zertifikaten	5
3.2	Signieren von Zertifikaten	5
3.3	Erneuern des UCS-Root-Zertifikats	6
3.4	Erneuern von Zertifikaten	7
3.5	Zurückrufen von Zertifikaten	7
3.6	Ausgeben von Zertifikat-Informationen	7
3.7	Überprüfen des Zertifikat-Status	8
3.8	Auflisten vorhandener Zertifikate	8
4	Zertifizieren der UCS-CA durch eine übergeordnete CA	8
5	Signieren fremder Requests durch die UCS-CA	9

1 Einführung

Unter UCS werden sensitive Informationen, die über das Netzwerk übertragen werden, verschlüsselt, zum Beispiel durch die Verwendung von SSH oder SSL.

SSL kommt beispielsweise bei der Replikation des LDAP-Verzeichnisses und bei der Verbindung zwischen Web-Browser und dem Web-Server, wenn Univention Directory Manager aufgerufen wird, zum Einsatz.

Die Rechner, die verschlüsselt miteinander kommunizieren möchten, müssen sich ausweisen können, damit der gegenüberliegende Rechner die Authentizität des verwendeten Schlüssels überprüfen kann. Als Ausweis besitzt jeder Rechner ein so genanntes Zertifikat, das von einer Zertifizierungsstelle (Certification Authority, CA) herausgegeben und signiert wird.

UCS bringt seine eigene CA mit, von der jeder UCS-Rechner beim Domänenbeitritt automatisch ein Zertifikat für sich selbst und das öffentliche Zertifikat der CA bezieht. Diese CA tritt als Root-CA auf, signiert ihr eigenes Zertifikat also selbst und kann Zertifikate für andere Zertifizierungsstellen signieren. Wie die Root-CA in eine nachrangige Zertifizierungsstelle (Sub-CA) umgewandelt wird und der CA einer anderen oder vorhandenen Organisation untergeordnet werden kann, wird in Kapitel 4 erklärt.

Die UCS-CA befindet sich immer auf dem Domänencontroller Master. Auf einem Domänencontroller Backup befindet sich eine Kopie dieser CA, die über einen Cronjob standardmäßig alle 20 Minuten mit der CA auf dem Domänencontroller Master synchronisiert wird.

Achtung:

Die CA wird nur vom Domänencontroller Master zum Domänencontroller Backup synchronisiert und nicht umgekehrt. Es sollte also ausschließlich die CA auf dem Domänencontroller Master verwendet werden.



Übernimmt ein Domänencontroller Backup die Rolle des Domänencontroller Master durch Ausführung des Skriptes `univention-backup2master`, so kann die CA auf dem ehemaligen Domänencontroller Backup sofort verwendet werden.

Das UCS-Root-Zertifikat hat, ebenso wie die damit erstellten Rechnerzertifikate der Clients, einen bestimmten Gültigkeitszeitraum. Ist dieser Zeitraum abgelaufen, funktionieren Dienste, die ihre Kommunikation mit SSL verschlüsseln (z.B. LDAP) nicht mehr. Es ist deshalb notwendig, die Gültigkeit der Zertifikate zu überprüfen und rechtzeitig ein neues UCS-Root-Zertifikat sowie neue Rechnerzertifikate zu erstellen.



Durch die Univention Configuration Registry-Variable **`ssl/validity/warning`** wird festgelegt, wie viele Tage vor Ablauf des Gültigkeitszeitraums des SSL-Zertifikats bei Anmeldung am Univention Directory Manager-Web-Frontend eines Master- bzw. Backup-Servers ein Warnhinweis angezeigt wird. Zusätzlich wird das Ablaufdatum des SSL-Zertifikats im Bereich **Über** im Univention Directory Manager-Web-Frontend angezeigt. Da das SSL-Zertifikat eines Domänencontroller Master bei der Installation direkt nach dem UCS-Root-Zertifikat erzeugt wird, weist dieses Ablaufdatum bei einem Domänencontroller Master auch auf das Gültigkeitsende des UCS-Root-Zertifikats hin.

Auf UCS-Systemen überprüft ein Cronjob täglich die Gültigkeit des lokalen Rechnerzertifikats

und des Root-Zertifikats und schreibt das Ablaufdatum in die Univention Configuration Registry-Variable `ssl/validity/days`. Der dort angegebene Wert spiegelt die Anzahl der Tage seit dem 1.1.1970 wieder. Ist die Gültigkeitsdauer des Root-Zertifikats kleiner als die des Rechner-Zertifikats, wird zusätzlich die Univention Configuration Registry-Variable `ssl/validity/ca` auf `true` gesetzt.

Um den Cronjob zu deaktivieren, muss die Univention Configuration Registry-Variable `ssl/validity/check` auf `no` gesetzt werden. Dabei ist zu beachten, dass bei deaktiviertem Cronjob Warnungen z.B. im Univention Directory Manager gar nicht oder mit falschem Datum angezeigt werden.

Soll das Ablaufdatum sofort aktualisiert werden (z.B. direkt nach der Installation), kann der folgende Befehl ausgeführt werden:

```
/usr/sbin/univention-certificate-check-validity
```

Anschließend kann der aktuelle Gültigkeitsstatus im Univention Directory Manager eingesehen werden.

2 Einrichten der Root-CA

Die Root-CA wird bei der Installation eines Domänencontroller Master automatisch eingerichtet. Dafür werden die Parameter `ssl_country`, `ssl_state`, `ssl_locality`, `ssl_organization`, `ssl_organizationalunit` und `ssl_email` im Installationsprofil benötigt. Bei der interaktiven Installation eines Domänencontroller Master erscheinen entsprechende Eingabefenster.

Die Werte aus dem Installationsprofil werden während der Installation in Univention Configuration Registry-Variablen übernommen. Bei den Variablennamen wird dabei der Unterstrich "_" aus den Profilvariablen durch einen Schrägstrich "/" ersetzt. Aus `ssl_email` wird z.B. `ssl/email`.

Der Common Name der UCS-Root-CA wird automatisch auf **Univention Corporate Server Root CA** gesetzt und in der Univention Configuration Registry-Variable `ssl/common` gespeichert.

Achtung:

Wenn diesen Variablen nach der Installation andere Werte zugewiesen und anschließend neue Zertifikate erzeugt werden, so ist nicht sichergestellt, dass diese Zertifikate mit dem Root-Zertifikat überprüft werden können.



3 Zertifikatsverwaltung mit univention-certificate

Zur Verwaltung der Zertifikate steht unter UCS der Befehl `univention-certificate` zur Verfügung, damit können neue Zertifikate beispielsweise angelegt oder zurückgezogen werden.

3.1 Anlegen von Zertifikaten

Standardmäßig werden für alle Rechner einer UCS-Domäne mit Ausnahme der Thin Clients und der Windows-Rechner automatisch Zertifikate erzeugt. Beim Domänencontroller Master geschieht dies bei der Installation, bei allen anderen Rechnern beim Domänenbeitritt. Für UCS-Server- und Clientsysteme ist es im Normalfall also nicht notwendig, Zertifikate mit `univention-certificate` zu erzeugen.

Mit dem Befehl

```
univention-certificate new -name <gewünschter Name des \
Zertifikats> -days <Gültigkeitsdauer in Tagen>
```

kann ein neues Zertifikat erzeugt werden. Als Name wird üblicherweise der FQDN des zu zertifizierenden Rechners eingesetzt. Wenn keine Gültigkeitsdauer angegeben wird, so wird der Vorgabewert von 730 Tagen verwendet. Der Vorgabewert kann durch Setzen der Univention Configuration Registry-Variable `ssl/default/days` geändert werden.

Für jedes Zertifikat wird im Verzeichnis `/etc/univention/ssl/` ein Unterverzeichnis mit dem Namen des Zertifikats angelegt, das folgende Dateien enthält:

```
ls -la /etc/univention/ssl/<Unterverzeichnis>/
```

```
total 28
drwxr-x---  2 root  DC Backup Hosts  4096 Apr  1 22:05 .
drwxr-xr-x  9 root  DC Backup Hosts  4096 Apr  1 22:05 ..
-rw-r-x---  1 root  DC Backup Hosts  4422 Apr  1 22:05 cert.pem
-rw-r-x---  1 root  DC Backup Hosts  3297 Apr  1 22:05 openssl.cnf
-rw-r-x---  1 root  DC Backup Hosts   891 Apr  1 22:05 private.key
-rw-r-x---  1 root  DC Backup Hosts   838 Apr  1 22:05 req.pem
```

Die Datei `cert.pem` stellt das eigentliche Zertifikat dar. In `openssl.cnf` ist die Konfiguration von OpenSSL zum Zeitpunkt der Zertifikat-Erstellung festgehalten. Die Datei `private.key` enthält den privaten Schlüssel zu dem Zertifikat. In `req.pem` ist der ursprüngliche Client-Request, mit dem das Zertifikat erstellt wurde, dokumentiert.

Im Verzeichnis `/etc/univention/ssl/ucsCA/certs/` wird eine Kopie des Zertifikats mit Seriennummer als Dateiname gespeichert und ein Link auf die Kopie angelegt.

Außerdem wird das Zertifikat in der Datei `/etc/univention/ssl/ucsCA/index.txt` vermerkt und die Seriennummer in `/etc/univention/ssl/ucsCA/serial` wird erhöht.

3.2 Signieren von Zertifikaten

Die Zertifikate werden beim Anlegen automatisch von der CA signiert. Die Umwandlung der UCS-Root-CA in eine Sub-CA und die Signierung des Zertifikats durch eine übergeordnete CA wird in Kapitel 4 beschrieben.

In Kapitel 5 wird die Signierung von Requests, die auf anderen Rechnern erstellt wurden, näher erläutert.

3.3 Erneuern des UCS-Root-Zertifikats

Das UCS-Root-Zertifikat sowie die Rechner-Zertifikate können nur auf dem Domänencontroller Master neu generiert werden.

1. Zunächst sollte eine Sicherheitskopie von `/etc/univention/ssl` und seinen Unterverzeichnissen angelegt werden, z.B. mit

```
cp -a /etc/univention/ssl /etc/univention/ssl_$(date +"%d%m%Y")
```

2. Nach der Neuerzeugung des UCS-Root-Zertifikats müssen alle Rechnerzertifikate der Clients erneuert und auf die entsprechenden Rechner kopiert werden. Es ist daher sinnvoll, wie in Abschnitt 3.8 beschrieben, sich die Liste aller ausgestellten Zertifikate ausgeben zu lassen und ggf. auszudrucken.
3. Ein neues Root-Zertifikat mit einem Gültigkeitszeitraum von 1000 Tagen wird durch

```
cd /etc/univention/ssl/ucsCA
openssl x509 -in CAcert.pem -out NewCAcert.pem \
    -passin file:/etc/univention/ssl/password \
    -days 1000 -signkey private/CAkey.pem
```

erzeugt (hier wurde die relative lange Befehlszeile des openssl-Aufrufs der Lesbarkeit halber durch Backslash-Zeichen auf mehrere Zeilen umgebrochen). Dieses kann dann durch den Befehl

```
mv NewCAcert.pem CAcert.pem
```

an die Stelle des alten UCS-Root-Zertifikats verschoben werden.

4. Neue Rechnerzertifikate können wie folgt erstellt werden

```
eval $(univention-config-registry shell)
cd /etc/univention/ssl
for i in *.$domainname; do
    univention-certificate renew -name $i -days 1000;
done
```

5. Die neuen Rechnerzertifikate müssen dann auf die jeweiligen Rechnersysteme kopiert werden (hier am Beispielrechner ucs-slave):

```
eval $(univention-config-registry shell)
cd /etc/univention/ssl/
scp ucsCA/CAcert.pem root@ucs-slave:/etc/univention/ssl/ucsCA/
rsync -av ucs-slave.$domainname root@ucs-slave:/etc/univention/ssl/
```

Dieser Schritt ist auf Domänencontroller=Backup-Systemen nicht erforderlich, da dies wie oben beschrieben automatisch regelmäßig per cron erfolgt.

6. Auf Rechnern, auf denen der Cyrus-Mailserver läuft, sind zusätzlich die Dateien `cert.pem` und `private.key` nach `/var/lib/cyrus/` zu kopieren:

```
cp /etc/univention/ssl/$(hostname -f)/cert.pem /var/lib/cyrus
cp /etc/univention/ssl/$(hostname -f)/private.key /var/lib/cyrus/
```

7. Alle Dienste, die SSL-Verschlüsselung benutzen, müssen neu gestartet werden. Alternativ kann auch ein Neustart des Systems durchgeführt werden.

3.4 Erneuern von Zertifikaten

Mit dem Befehl

```
univention-certificate renew -name <Name des Zertifikats> \  
-days <Gültigkeitsdauer in Tagen>
```

kann ein einzelnes Zertifikat erneuert werden. Die Gültigkeitsdauer wird ab dem aktuellen Datum gerechnet, nicht ab dem bisherigen Ablaufdatum des Zertifikats. Wenn keine Gültigkeitsdauer angegeben wird, so wird der Vorgabewert von 730 Tagen verwendet. Der Name des Zertifikats ist so anzugeben, wie er in der Liste der vorhandenen Zertifikate (siehe Kapitel 3.8) erscheint.

3.5 Zurückrufen von Zertifikaten

Mit dem Befehl

```
univention-certificate revoke -name <Name des Zertifikats>
```

wird ein Zertifikat zurückgerufen, d.h. es bleibt gespeichert, ist aber nicht mehr gültig. Wenn ein neues Zertifikat mit demselben Namen erzeugt wird, wird das Verzeichnis des alten Zertifikats in `/etc/univention/ssl` allerdings überschrieben. Nur die Datei `/etc/univention/ssl/ucsCA/certs/<NummerdesZertifikats>.pem` bleibt erhalten.

3.6 Ausgeben von Zertifikat-Informationen

Mit dem Befehl

```
univention-certificate dump -name <Name des Zertifikats>
```

werden die Informationen, die in einem Zertifikat (also in der Datei `/etc/univention/ssl/<Zertifikat-Unterverzeichnis>/cert.pem`) gespeichert sind, ausgegeben.

Achtung:

Die Ausgabe des oben angegebenen Befehls enthält unter anderem die folgenden Zeilen. Sie geben lediglich die Gültigkeitsdauer an und sagen nichts darüber aus, ob das Zertifikat tatsächlich gültig ist. Die Gültigkeit ist, wie in Kapitel 3.7 beschrieben, zu prüfen.

```
Validity  
Not Before: <Datum>  
Not After: <Datum>
```

3.7 Überprüfen des Zertifikat-Status

Mit dem Befehl

```
univention-certificate check -name <Name des Zertifikats>
```

wird geprüft, ob das angegebene Zertifikat gültig oder ungültig (also zurückgerufen oder abgelaufen) ist.

3.8 Auflisten vorhandener Zertifikate

Mit dem Befehl

```
univention-certificate list
```

wird eine Liste aller vorhandenen, gültigen Zertifikate ausgegeben.

4 Zertifizieren der UCS-CA durch eine übergeordnete CA

Die in UCS integrierte CA kann durch eine andere CA zertifiziert werden. Dadurch wird die UCS-CA, die standardmäßig eine Root-CA ist, in eine Sub-CA umgewandelt.

Dabei kann folgendermaßen vorgegangen werden:

1. Zunächst sollte eine Sicherheitskopie von `/etc/univention/ssl` und seinen Unterverzeichnissen angelegt werden.
2. Nach der Installation des Domänencontroller Master liegt die Signierungsanfrage (Request) unter `/etc/univention/ssl/ucsCA/CAreq.pem`. Diese Anfrage muss mit der übergeordneten CA unterschrieben werden. Durch die Signatur wird aus der Anfrage ein Zertifikat.
3. Falls das UCS-Zertifikat und das Zertifikat der übergeordneten CA nicht im PEM-Format vorliegen, so muss dies umgewandelt werden. Im folgenden Beispiel wird ein Zertifikat im DER-Format umgewandelt:

```
openssl x509 -inform der -outform pem -in MpublicCA.der \  
-out MPublicCA.pem
```

4. Das UCS-Zertifikat muss an zwei Stellen gespeichert werden (`/etc/univention/ssl/ucsCA/CAcert.pem` und eine Kopie in `/etc/univention/ssl/ucsCA/certs/00.pem`):

```
cd /etc/univention/ssl  
cp <Pfad>/CAcert.pem ucsCA/CAcert.pem  
cp ucsCA/CAcert.pem ucsCA/newcerts/00.pem  
source /usr/share/univention-ssl/make-certificates.sh  
move_cert ucsCA/newcerts/00.pem
```

Der letzte Befehl verschiebt das Zertifikat aus dem Verzeichnis `/etc/univention/ssl/ucsCA/newcerts/` in das Verzeichnis `/etc/univention/ssl/ucsCA/certs/` und legt dort einen Link auf das Zertifikat an.

5. Das Zertifikat kann nun auf dem Webserver abgelegt werden:

```
cd /etc/univention/ssl
openssl x509 -in ucsCA/CAcert.pem -out \
/var/www/ucs-root-ca.crt
```

6. Das CA-Zertifikat der übergeordneten CA muss ebenfalls auf dem Domänencontroller Master gespeichert werden:

```
mkdir -p /etc/univention/ssl/mca/
cp <Pfad>/MPublicCA.pem /etc/univention/ssl/mca/
```

7. Nun kann die Zertifikatskette erzeugt werden:

```
cd /etc/univention/ssl
cat mca/MPublicCA.pem >> ucsCA/CAcert.pem
```

8. Der Webserver muss nun so eingerichtet werden, dass dieser die Chain-Datei zusammen mit seinem Zertifikat an die Clients schickt. Dazu muss die folgende Zeile

```
SSLCertificateChainFile /etc/univention/ssl/CAChain.pem
```

in die Datei `/etc/univention/templates/files/etc/apache2/mods-available/ssl.conf` eingefügt werden. Die Einstellungen können mit dem Befehl

```
univention-config-registry commit \
/etc/apache2/mods-available/ssl.conf
```

übernommen werden, danach muss der Webserver neu gestartet werden:

```
/etc/init.d/apache2 restart
```

9. Das CA-Zertifikat der übergeordneten CA muss auf den Clients importiert werden, damit die Clients entsprechend andere Zertifikate überprüfen können, die von der UCS-CA unterschrieben wurden.

10. Folgende Browser-Einstellungen sind auf den Clients vorzunehmen:

- Im Browser Firefox sind keine speziellen Einstellungen erforderlich.
- Bei Microsoft Internet Explorer schalten Sie die TLS 1.0-Unterstützung ein über **Extras** → **Internetoptionen** → **Erweitert** → **Sicherheit**.
- Der Browser Konqueror unterstützt derzeit keine Zertifikatsketten.

5 Signieren fremder Requests durch die UCS-CA

Mit dem folgenden Befehl kann eine Signierungsanfrage (Request), der auf einem anderen Rechner erstellt wurde, mit der UCS-CA signiert werden:

```
openssl ca -batch -config /etc/univention/ssl/openssl.cnf \  
-in <Request> -out <Zertifikat> -passin pass`cat \  
/etc/univention/ssl/password`
```

Dabei ist **<Request>** durch den Dateinamen mit Pfad, unter dem die eingegangene Anfrage gespeichert ist (Bsp. [/etc/univention/ssl/fqdn/req.pem](#)), zu ersetzen. Die Anfrage sollte im PEM-Format vorliegen oder muss ggf. umgewandelt werden. Die Umwandlung könnte mit folgendem Befehl durchgeführt werden:

```
openssl x509 -inform der -outform pem -in request.der -out \  
req.pem
```

Dabei ist **<Zertifikat>** durch den Dateinamen mit Pfad, unter dem das fertige Zertifikat gespeichert werden soll (Bsp. [/etc/univention/ssl/fqdn/cert.pem](#)), zu ersetzen. Das Verzeichnis ist vorher anzulegen, falls es nicht existiert.

Standardmäßig wird unter UCS von allen Zertifikaten eine Kopie unter [/etc/univention/ssl/ucsCA/certs](#) gespeichert. Dafür ist der Befehl

```
move_cert /etc/univention/ssl/ucsCA/newcerts/*
```

auszuführen.