


Renewing the TLS/SSL certificates

Languages:	Deutsch English
	UCS 4

Communication between the different systems in a UCS domain is largely encrypted via TLS (formerly SSL). A root certificate and host certificate for each computer are required for the TLS encryption. The root certificate is only valid for a specified period of time, as are the host certificates created with the root certificate. Once this period of time elapses, services which encrypt their communication with TLS (e.g. LDAP, UMC) no longer function. It is thus essential to verify the validity of the certificates and create new host certificates if necessary.

The following commands need to be performed on the UCS master.

`univention-certificate` can be used to check how long a certificate will remain valid:

```
univention-certificate dump -name ucs01.intra.example.org
[...]  
Validity Not Before: Jun 19 10:40:13 2016 GMT  
Not After : Jun 18 10:40:14 2018 GMT  
[...]
```

When doing so, the FQDN of the computer name (computer name + domain) must be entered. A list of all available certificates can be generated with:

`univention-certificate list` The certificates in a UCS domain usually have the same expiration period (default is 5 years from issuance onwards). If the root certificates expires, the certificate chain is considered invalid. Therefore it is necessary to renew all certificates, if the root certificate is about to expire. To create new certificates, proceed as follows:

Backup the old certificates:

```
cp -a /etc/univention/ssl /etc/univention/ssl$(date --iso)
```

Renewal of the certificates

```
Renew the root certificate entering the contents of the /etc/univention/ssl/password file as the  
password: cd /etc/univention/ssl/ucsCA  
openssl x509 -in CAcert.pem -out NewCAcert.pem -days "$(ucr get ssl/default/days)" /  
-passin file:/etc/univention/ssl/password /  
-signkey private/CAkey.pem  
mv NewCAcert.pem CAcert.pem
```

Renewing the TLS/SSL certificates

Attention: On very old UCS systems (before version 2.0) the folder "/etc/univention/ssl/ucsCA" was named "/etc/univention/ssl/udsCA"

Renewing all computer certificates:

```
eval "$(ucr shell)"
cd /etc/univention/ssl
for i in *".$domainname"; do univention-certificate renew -name "$i.$domainname" -days "$(ucr get ssl/default/days)"; done
```

Copy the new certificates

Copy the new certificates to the other systems (each UCS/UCC system except UCS Backups - here using ucs03 as an example computer) eval "\$(ucr shell)"

```
cd /etc/univention/ssl/
scp ucsCA/CAcert.pem root@ucs03:/etc/univention/ssl/ucsCA/
scp -r ucs03.$domainname root@ucs03:/etc/univention/ssl/
scp -r ucs03.$domainname/* root@ucs03:/etc/univention/ssl/ucs03.$domainname/
```

The last step is not necessarily required on a UCS Backup computer because those systems copy the certificates automatically via cron.

The following command should be used to make the newly created certificate available to all users via the UCS master 's central administration website `cp CAcert.pem /var/www/ucs-root-ca`. After the certificates have been renewed, the new information is not yet displayed in the Univention Management Console (UMC) and the corresponding monitoring check. It would only be updated during the next, regular check, as the cronjob set up for this purpose is only run once every day. To be able to verify the validity of the certificates immediately, the corresponding Univention Configuration Registry variables need to be evaluated. This can be done by running the following script `/usr/sbin/univention-certificate-check-validity`. All the services which use the SSL/TLS encryption need to be restarted. Alternatively, the system can be rebooted if it is not known exactly which services employ SSL/TLS.

SAML SSO

Since UCS 4.1 every UCS Master and UCS Backup is also a SAML Identity provider and every UCS system in the domain running the Univention Management Console (UMC) is a SAML Service provider. The SAML implementation for UCS uses also TLS encryption and a certificate for the DNS alias `ucs-ss0.$domainname` - this needs to be replaced, too.

On every SAML Identity provider (UCS Master and all UCS Backups), execute the following:

```
eval "$(ucr shell domainname)"
cp "/etc/univention/ssl/ucs-ss0.{$domainname}/cert.pem"
```

Renewing the TLS/SSL certificates

```
"/etc/simplesamlphp/ucs-sso.${domainname}-idp-certificate.crt"  
cp "/etc/univention/ssl/ucs-sso.${domainname}/private.key"  
"/etc/simplesamlphp/ucs-sso.${domainname}-idp-certificate.key"  
service univention-saml restart
```

On every SAML Service provider (every UCS system that is part of the domain), the new certificate needs to be evaluated:

```
eval "$(ucr shell ucs/server/sso/fqdn)"  
rm /usr/share/univention-management-console/saml/idp/*.xml  
ucr set  
umc/saml/idp-server="https://${ucsserverssofqdn}/simplesamlphp/saml2/idp/metadata.php" ||  
echo 'Failed!'  
/etc/init.d/univention-management-console-web-server restart  
univention-run-join-scripts --force --run-scripts 92univention-management-console-web-server.inst
```

Cyrus

Cyrus has been the default IMAP server until UCS 4.0-2. On systems where the cyrus mail server is running, the cert.pem and private.key must also be copied to /var/lib/cyrus/

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

Afterwards the permissions (owner) of the new files must be adjusted:

```
chown cyrus:mail /var/lib/cyrus/cert.pem  
chown cyrus:mail /var/lib/cyrus/private.key
```

AD Connection

If the AD connection is used, the certificates should be renewed as well.

```
cp /etc/univention/ssl/<FQDN of ad system>/{cert.pem,private.key}  
/var/www/univention-ad-connector/  
chgrp www-data /var/www/univention-ad-connector/{cert.pem,private.key}
```

After this step, the new certificates can be downloaded from the UMC module of the AD Connection. Please follow the AD Connection documentation on how to update the certificates on the Windows system.

Renewing the TLS/SSL certificates

RADIUS

If the RADIUS App (freeradius) is used, the cert.pem and private.key must also be copied to /etc/freeradius/ssl/

```
cp /etc/univention/ssl/"$(hostname -f)"/cert.pem /etc/freeradius/ssl/  
cp /etc/univention/ssl/"$(hostname -f)"/private.key /etc/freeradius/ssl/
```

Afterwards the permissions (owner) of the new files must be adjusted:

```
chown root:freerad /etc/freeradius/ssl/cert.pem  
chown root:freerad /etc/freeradius/ssl/private.key
```

```
$(ucr get ssl/default/days)
```

Unique solution ID: #1183

Author: Moritz Mühlenhoff

Last update: 2017-06-08 14:43