

Old implementation

The following is the old, manual, way of installing SSL certs.

Tomcat 7 automatic installation

Using the TS commandline tools, you specify the domain and your email

```
tsinstallssl.sh server.acme.com sslresponsible@acme.com
```

After a couple of minutes you will be required to enter the domain an email again, and accept the terms of service

Tomcat 7 manual installation

Install and configure letsencrypt

Download an build certbot (letsencrypt client)

```
sudo yum -y install python27-devel git (deprecated)
```

```
sudo yum -y install python36 python36-pip
sudo yum -y install git-all
sudo git clone https://github.com/letsencrypt/letsencrypt /opt/letsencrypt
/opt/letsencrypt/letsencrypt-auto --debug --agree-tos
```

Create a config file

```
sudo touch /etc/letsencrypt/config.ini
sudo chmod 777 /etc/letsencrypt/config.ini
sudo echo "rsa-key-size = 4096" >> /etc/letsencrypt/config.ini
sudo echo "email = kpe@tempusserva.dk" >> /etc/letsencrypt/config.ini
```

Generate PKCS12 certificate

Generate a certificate

```
sudo mkdir /usr/share/tomcat7/webapps/ROOT
/opt/letsencrypt/letsencrypt-auto certonly --debug --webroot -w /usr/share/tomcat7/webapps/ROOT -d
letsencrypt.tempusserva.dk --config /etc/letsencrypt/config.ini --agree-tos
```

Convert to pkcs12 format

```
sudo -s
```

```
cd /etc/letsencrypt/live/letsencrypt.tempusserva.dk
openssl pkcs12 -export -out bundle.pfx -inkey privkey.pem -in cert.pem -certfile chain.pem -password
pass:TempusServaSecret
chmod 755 bundle.pfx
chmod 755 /etc/letsencrypt/live
```

```
Press: ctrl + d
```

Install certificate in Tomcat

Edit Tomcat configuration

```
sudo nano /usr/share/tomcat7/conf/server.xml
```

```
<Connector
  protocol="org.apache.coyote.http11.Http11NioProtocol"
  port="8443" maxThreads="200"
  scheme="https" secure="true" SSLEnabled="true"
  keystoreFile="/etc/letsencrypt/live/letsencrypt.tempusserva.dk/bundle.pfx"
  keystorePass="TempusServaSecret"

  ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WI
  TH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA"
  clientAuth="false" sslProtocol="TLS" keystoreType="PKCS12"/>
```

Reboot the server

```
service tomcat7 restart
```

Revision #5

Created 25 March 2025 09:44:26 by Admin

Updated 3 April 2025 12:22:50 by Theis Villumsen