SSL: Current custo diagnostic versions: How to secure the Connection between custo diagnostic client and custo diagnostic server

Basic information

By default the installation of the custo diagnostic server in Windows already creates a key pair with a self-signed certificate. This already permits an encrypted HTTPs connection with the IP port defined in the installation program. You may test it with your browser:

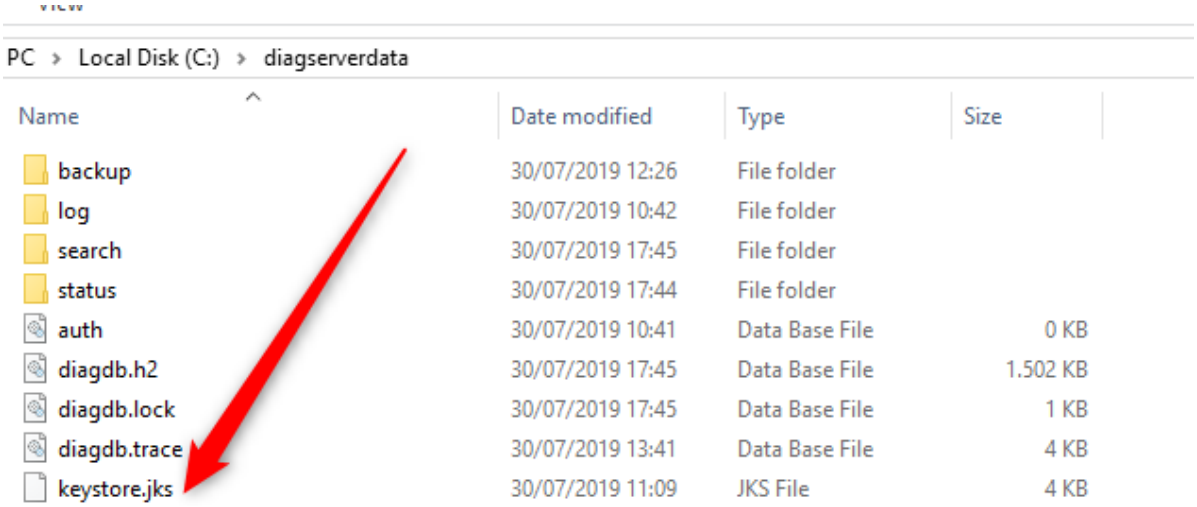
However neither the common name stored in the certificate probably matches with the client name nor the trust to this certificate is given. The custo diagnostic client expects both. Beyond that the certificate validity must be within the time range specified in the certificate and this is by default only a one year period.

On the other hand: There is already a key pair installed - so no new one needs to be created, which is good from the IT security point of view as you should avoid creating a key pair on another system: Even a certification authority (CA should never get in touch with the private key. The only task of the CA should be the proper signature of the public key of your system. Therefor ethe CA should be trusted by all customer clients and the certificate should have a reasonable validity monitored administratively.

Signature

The procedure consists of the creation of a certificate signing request (CSR), the signature of it by the CA and the import of the signed public key - the certificate. The CSR creation as well as the import of the certificate can be done either by command line program keytool (part of the the Java Runtime Engine installed with the custo diagnostic server) or via a graphic tool like the Keystore Explorer (see https://keystore-explorer.org/index.html).

With both tools you access the diagserver keystore stored in the diagserverdata directory:



Before you modify the keystore always create 2 backups of the original keystore file - one in the same directory and one outsiste of the keystore directory.

To modify it the custo diagnostic service (Apache Tomcat service) must be stopped. The keystore is installed in parallel to the Windows certificate store and the diagserver uses only that one for the web server SSL service.

To work with the keytool program start CMD in administative context (run as admin):

Create a key for the signing request:

```
In the data directoy of the custo diagnostic server:

"c:\Program Files\custo diagnostic server\jre"\bin\keytool -certreq -alias main -file test.customed.de.csr -
keystore keystore.jks -ext san=dns:test.customed.de -dname CN=test.customed.de
```

The program then asks for a password. The password is: custo1234

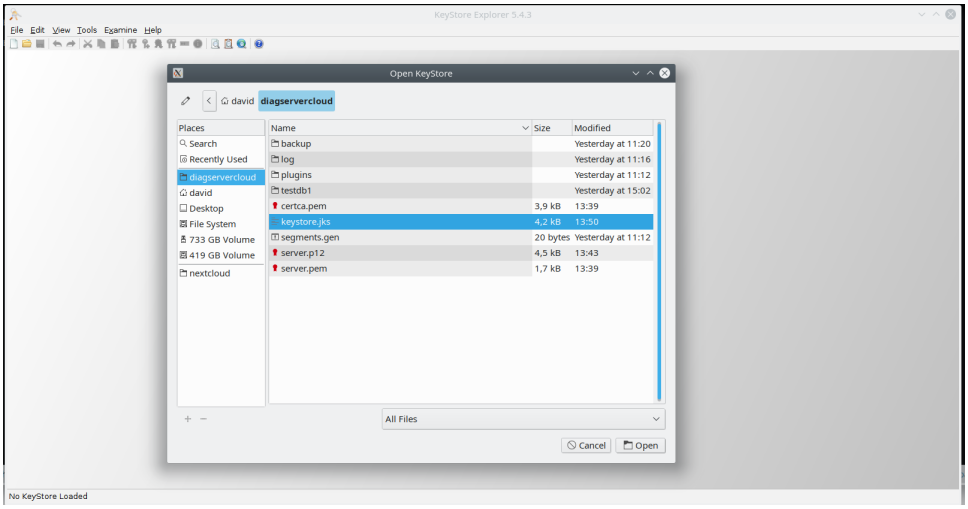
In this example a request for the server is test.customed.de created. For your server replace it by the full name of the server running custo diagnostic.

The result in this example is the file test.customed.de.csr. This is the file you need to transfer to the CA to get a signed certificate created.

The answer from a CA is normally a pkcs file or several PEM files.

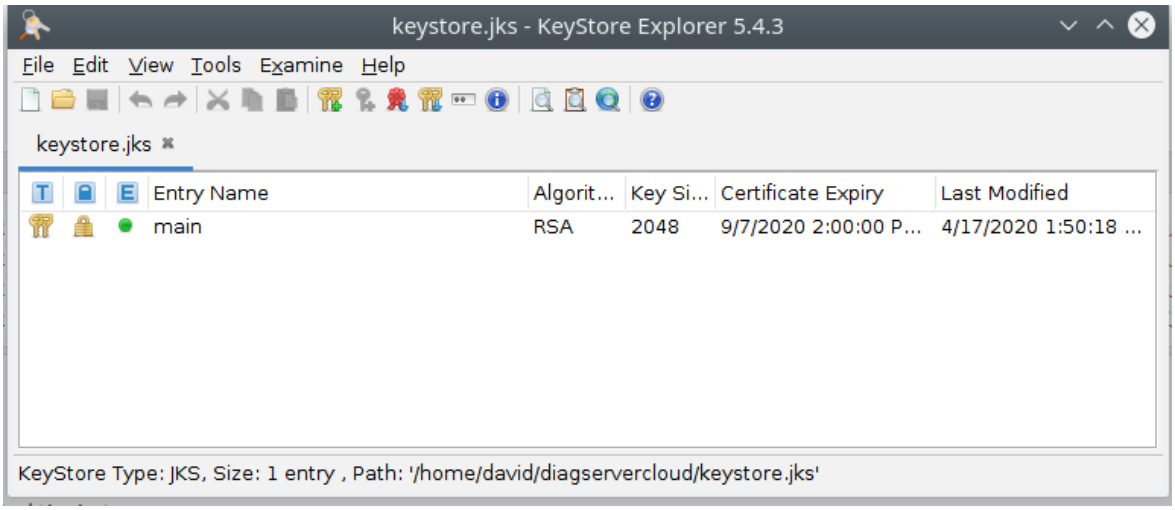
With the keystore explorer:

Open the keystore in the diagserverdata directory called keystore.jks:

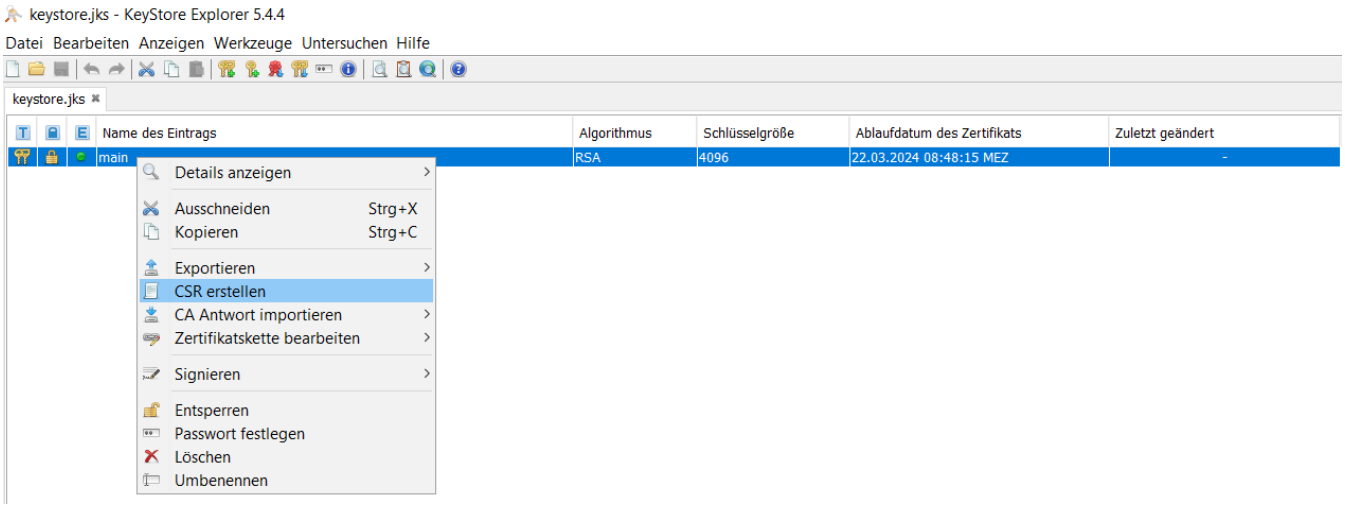


The keystore password is here as well "custo1234".

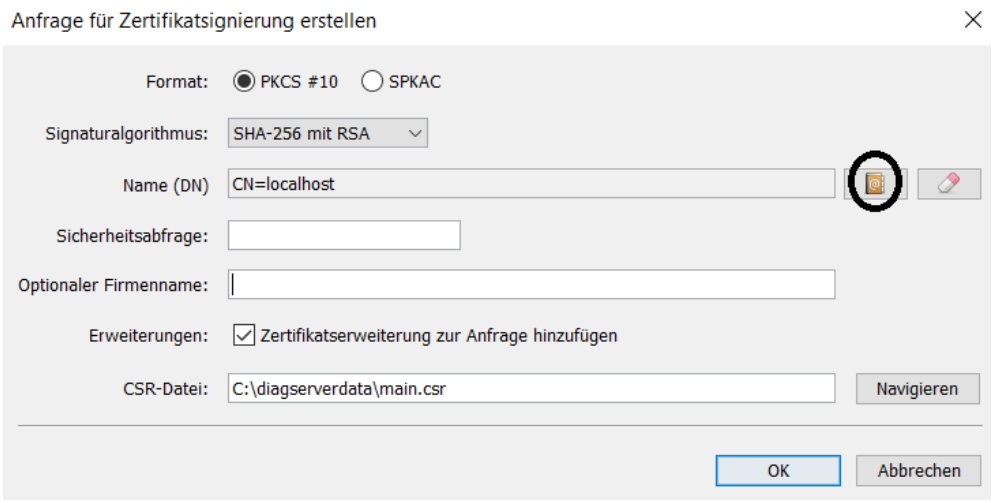
There should be only one entry called "main":



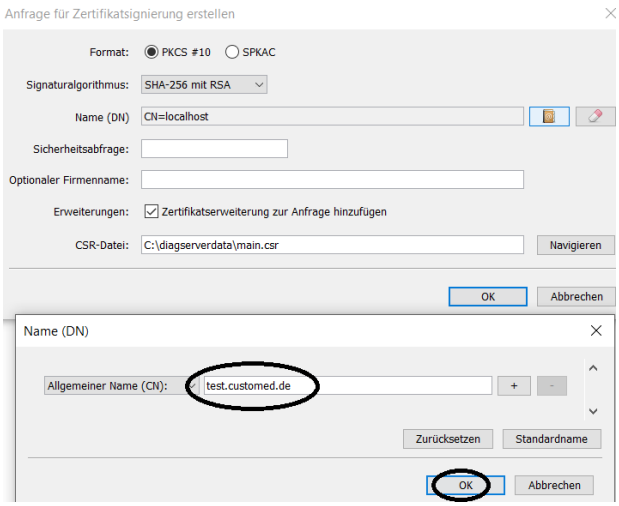
Right click on "main" and create a CSR request;



After entering the key store password that menu opens:



Modify there the domain name details - replace "test.customed,de" with the full name of your custo diagnostic server - as specified in the custocfg.ini:



By then clicking twice "OK" you get the CSR at the location you have specified above. Send that to the CA for the signature.

Import a PKCS#7 file

With the keytool program:

In our example use:

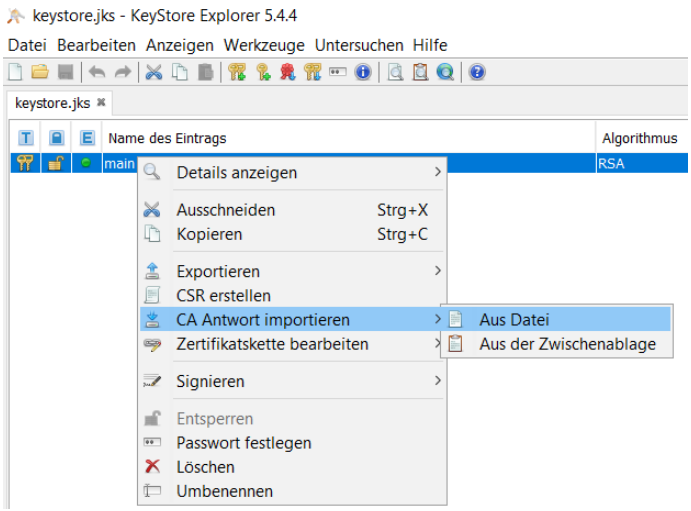
```
C:\diagserverdata>"c:\Program Files\custo diagnostic server\jre"\bin\keytool -importcert -alias main -file test.customed.de.pkcs -keystore keystore.jks -trustcacerts
```

The password of the keystore should still be custo1234.

With the keystore explorer:

Before you consider using the keystore explorer program for operations with write operations to the keystore file be aware that the file format written by the keystore explorer might not be readable for the used Apache Tomcat version. So always create a backup of the original keystore file before to be able to get one step back.

Open the pkcs answer file via the "import CA response" menu and install it:



Import PEM (in Windows CER or CRT) files

For PEM files, the response to the CSR must be in the form of a complete certificate chain. The PEM file for import under the alias "main" first contains the signed server certificate, followed by all associated intermediate certificates in the order of the chain. The root certificate can be added at the end if it was provided by the CA or is required by the setup.
On Windows, for example, the files are combined as follows:

```
C:\diagserverdata>type test.customed.de.pem intermediate.cert.pem intermediat2.cert.pem root.cert.pem > test.customed.de-fullchain.pem

C:\diagserverdata>"c:\Program Files\custo diagnostic server\jre"\bin\keytool -importcert -alias main -file test.customed.de-fullchain.pem -keystore keystore.jks -trustcacerts
```

Important: The "main" alias must not be deleted, because it contains the private key for which the CSR was generated. Back up the keystore before importing. After importing, use `keytool -list -keystore keystore.jks -v` to verify that "main" is displayed as a `PrivateKeyEntry` with the complete certificate chain.

Finally:

Restart the custo diagnostic service and check with a web browser (use the URL in the custocfg.ini and use https instead of http) if everything works as expected.

Prolongation of the certificate

Each certificate will expire one day. So please carefully monitor the expiration date of the SSL certificate: custo diagnostic will not complain even a second before expiration of the certificate - it will just stop working from the second after the expiration of the certificate on.

It is a good practice to prolong the certificate in time before expiration. To do so stop the custo diagnostic service and create a copy of the keystore file - better save than sorry! Then follow the signature steps above once more: Create a new CSR (signing request), send that to the CA and import that. Afterwards start the custo diagnostic service again.

Appendix: Import a PFX (in Windows called PKCS#12) file:

Some customers may be consulting resistent and want to install a full key pair. However in most cases the private key in it will be marked as not exportable and is secured by a password. In that case you need use the PFX as keystore for the Tomcat server.

For that stop the custo diagnostic service and create a backup of the server.xml and modify the server xml: Make that section a comment:

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
        maxThreads="250" SSLEnabled="true" scheme="https" secure="true" bindOnInit="false"
        clientAuth="false" sslProtocol="TLS" keystoreFile="C:/diagserverdata/keystore.jks" keystorePass="custo1234"
        keyAlias="main"
        truststoreFile="C:/diagserverdata/keystore.jks" truststorePassword="custo1234" />
```

... by adding <!-- before that section and → in the line below.

Then copy the key pair file to the diagserverdata directory and add a section like that:

```
<Connector
protocol="org.apache.coyote.http11.Http11NioProtocol"
port="443"
maxThreads="200"
scheme="https"
secure="true"
SSLEnabled="true"
keystoreFile="d:/diagserverdata/somefile.pfx"
keystorePass="password_from_your_pfx"
keystoreType="PKCS12"
clientAuth="false"
sslProtocol="TLS"/>
```

"d:/diagserverdata/somefile.pfx" is the absolute path and actual name for the PKCS#12 certificate
"password_from_your_pfx" is the actual password for the PKCS#12 file

Afterwards restart the custo diagnostic server.

Please note that those changes might be gone after a custo diagnostic server upgrade! So save your server.xml config always before an upgrade!

Appendix: Satellite system sync with HTTPs

If you set up a satellite system the Apache Tomcat server on the SAT system will not act as a server, but as a client.

In this case Apache Tomcat can use the server key store (keystore,jks) in the diagserverdata directory, but if it should not contain the CA certificates the use of the local client keystore cacerts (by default stored in (C:\Program Files\custo diagnostic server\jre\lib\security) might be an alternative . You can use the same tools as above to open that certificate store - the password is by default empty. Import the root certificate of the SSL certificate installed on the master server.

Now you need to configure Apache Tomcat to use its own keystore and not the one of the Windows operating system. For this open the "Configure custo diagnostic server" app on the SAT server and go to the Java tab. Remove the line "-Djavax.net.ssl.trustStoreType=WINDOWS-ROOT" and restart the custo diagnostic SAT server.

Please note that the config of the local certificate store might be lost after a custo diagnostic server upgrade - so better use a well configured Windows certificate store from the beginning.

Further information:

See also Tomcat HTTP / SSL Howto: https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html

https://www.namecheap.com/support/knowledgebase/article.aspx/9441/33/installing-an-ssl-certificate-on-tomcat/

https://www.sslshopper.com/ssl-converter.html