COMPROTware:Testtool - TLS-secured connections

Example for TLS-secured connections setup

Terms

There are many different terms used in documents about TLS-secured connections. Here we will use the terms introduced and used in the Internet RFC documents, see https://en.wikipedia.org/wiki/Request_for_Comments.

- Certificate: A certificate is used to prove the validity of a public key. A certificate includes information about the public key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). A certificate contains a public key. The public key is used to encrypt transmitted data.
- Root certificate: This certificate is the root for a chain of certificates.
- Root certificate's private key: This private key is used to generate derived certificates, that is intermediate and leaf certificates.
- Leaf certificate: This certificate is the last certificate in a certificate chain. It is the certificate used to authenticate a system or a device. In the RFCs a leaf certificate is also named end-entity certificate.
- Leaf certificate's private key: The private key of the leaf certificate is used to decrypt data received from the opposite partner.
- Certificate chain: Is a chain of certificates, starting with a root certificate, with some intermediate certificates and ending with a leaf certificate. The chain contains a least two certificates: The root and the leaf certificate. To verify a leaf ceritificate, the certificate chain used to generate the leaf certificate has to be known by the opposite partner.

See also:

- https://en.wikipedia.org/wiki/Public_key_certificate
- https://www.rfc-editor.org/rfc/rfc3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"
- https://www.rfc-editor.org/rfc/rfc5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
- https://en.wikipedia.org/wiki/Certificate_authority
- https://en.wikipedia.org/wiki/PKCS_12

Example files

Since CPTT T.2.22.5 the standard CPTT installation includes some example files for a TLS-secured conncetion setup with two separately running CPTT instances. These files can be used in the IEC 60870-5-104, DNP3 over LAN/WAN or MODBUS TCP/IP profiles as parameters for a typical TLS setup. The files can be found in the directory C:\Program Files (x86)\Real Thoughts GmbH\COMPROTware\Testtool\doc\2.22\Demo_Certificate.

The following files are used to setup the first CPTT instance, called "CPTT_1" or "Partner_A":

- ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-cert.pem
- ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-privkey.pem
- ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-password_TlsSecTcp.p12

The following file is used to setup the first CPTT instance, called "CPTT_1" for verification of the connection with "Partner_B":

- ReaTho-Demo-For_CPTT_1-Partner_B-cert_chain-cert.pem

An these files are used to setup the second CPTT instance, called "CPTT_2" or "Partner_B":

- ReaTho-Demo-For_CPTT_2-Partner_B-leaf_cert-cert.pem
- ReaTho-Demo-For_CPTT_2-Partner_B-leaf_cert-privkey.pem
- ReaTho-Demo-For_CPTT_2-Partner_B-leaf_cert-password_TlsSecTcp.p12

The following file is used to setup the second CPTT instance, called "CPTT_2" for verification of the connection with "Partner_A":

- ReaTho-Demo-For_CPTT_2-Partner_A-cert_chain-cert.pem

The files contain:

- ReaTho-Demo-For_CPTT_<cptt_idx>-Partner_<partner_idx>-leaf_cert-cert.pem: The leaf certificate for Partner_<partner_idx>, which should be used in CPTT_<cptt_idx> profile.
- ReaTho-Demo-For_CPTT_<cptt_idx>-Partner_<partner_idx>-leaf_cert-privkey.pem: The private key to the leaf certificate for Partner_<partner_idx>, which should be used in CPTT_<cptt_idx> profile.
- ReaTho-Demo-For_CPTT_<cptt_idx>-Partner_<partner_idx>-cert_chain-cert.pem: The certificate chain of the leaf certificate for Partner_<partner_idx>, which should be used in CPTT_<cptt_idx> profile.
- ReaTho-Demo-For_CPTT_<cptt_idx>-Partner_<partner_idx>-leaf_cert-password_TlsSecTcp.p12: A container with the leaf certificate and the private key to the leaf certificate for Partner_<partner_idx>, which should be used in CPTT_<cptt_idx> profile. The password for the container is "TlsSecTcp".

Example with PEM files

The file format PEM is described in RFC 1422. This file format is a container format for certificates, certificate chain, public key or private key. Files of this file format use the file extension .pem.

Here are the steps to setup "CPTT 1" for a TLS-secured TCP/IP connection:

- Start the first CPTT instance.
- Change to the IEC 60870-5-104 profile window.
- Insert the IP address and the TCP/IP port no of the second CPTT instance running IEC 60870-5-104.
- Enable "Use TLS-secured connection".
- Select "PEM" as certificate/key file format.
- In input field "Local host leaf certificate - certificate file" insert C:\Program Files (x86)\Real Thoughts GmbH\COMPROTware\Testtool\doc\2.22\Demo_Certificate\ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-cert.pem
- In input field "Local host leaf certificate - private key file" insert C:\Program Files (x86)\Real Thoughts GmbH\COMPROTware\Testtool\doc\2.22\Demo_Certificate\ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-privkey.pem
- Disable "Verify remote host leaf certificate".
- Press "Accept".

Here are the steps to setup "CPTT 2" for a TLS-secured TCP/IP connection:

- Start the second CPTT instance.
- Change to the IEC 60870-5-104 profile window.
- Insert the IP address and the TCP/IP port no of the first CPTT instance running IEC 60870-5-104.
- Enable "Use TLS-secured connection".
- Select "PEM" as certificate/key file format.
- In input field "Local host leaf certificate - certificate file" insert C:\Program Files (x86)\Real Thoughts GmbH\COMPROTware\Testtool\doc\2.22\Demo_Certificate\ReaTho-Demo-For_CPTT_2-Partner_B-leaf_cert-cert.pem
- In input field "Local host leaf certificate - private key file" insert C:\Program Files (x86)\Real Thoughts GmbH\COMPROTware\Testtool\doc\2.22\Demo_Certificate\ReaTho-Demo-For_CPTT_2-Partner_B-leaf_cert-privkey.pem
- Disable "Verify remote host leaf certificate".
- Press "Accept".

Now, both "CPTT 1" and "CPTT 2" are setup in a way that both CPTTs can be running as client or server. Start "CPTT 2" as Controlled Station, start "CPTT 1" as Controlling station and a TLS-secured connection should be established. With this setup and typical for TLS-secured connections, only the server's certificate is transmitted, the client's certificate is not transmitted.

To verify the received certificate, enhance the protocol profile for "CPTT 1" in the following way:

- Stop "CPTT 1".
- Enable "Verify remote host leaf certificate".
- In input field "Remote host leaf cert. - certificate chain file" insert C:\Program Files (x86)\Real Thoughts GmbH\COMPROTware\Testtool\doc\2.22\Demo_Certificate\ReaTho-Demo-For_CPTT_1-Partner_B-cert_chain-cert.pem
- In input field "Remote host - Common name" insert "Partner_B"
- Press "Accept".

And enhance the protocol profile for "CPTT 2" in the following way:

- Stop "CPTT 2".
- Enable "Verify remote host leaf certificate".
- In input field "Remote host leaf cert. - certificate chain file" insert C:\Program Files (x86)\Real Thoughts GmbH\COMPROTware\Testtool\doc\2.22\Demo_Certificate\ReaTho-Demo-For_CPTT_2-Partner_A-cert_chain-cert.pem
- In input field "Remote host - Common name" insert "Partner_A"
- Press "Accept".

Start "CPTT 2" as Controlled Station, start "CPTT 1" as Controlling station and a TLS-secured connection should be established. As "Verify remote host leaf certificate" is enabled in both CPTT instances, server and client certificates are transmitted and verified.

Example with PKCS#12 files

The certificate/private key file format PKCS#12 was introduced by RSA. It is now described in RFC 7292. This file format is a password-protected container format for certificates and private keys. Files of this file format use the file extension .p12.

Here are the steps to setup "CPTT 1" for a TLS-secured TCP/IP connection:

- Start the first CPTT instance.
- Change to the IEC 60870-5-104 profile window.
- Insert the IP address and the TCP/IP port no of the second CPTT instance running IEC 60870-5-104.
- Enable "Use TLS-secured connection".
- Select "PKCS#12" as certificate/key file format.
- In input field "Local host leaf certificate - certificate/private key file" insert C:\Program Files (x86)\Real Thoughts GmbH\COMPROTware\Testtool\doc\2.22\Demo_Certificate\ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-password_TlsSecTcp.p12
- In input field "Password for certificate/private key file" insert "TlsSecTcp".
- Press "Accept".

Here are the steps to setup "CPTT 2" for a TLS-secured TCP/IP connection:

- Start the first CPTT instance.
- Change to the IEC 60870-5-104 profile window.
- Insert the IP address and the TCP/IP port no of the second CPTT instance running IEC 60870-5-104.
- Enable "Use TLS-secured connection".
- Select "PKCS#12" as certificate/key file format.
- In input field "Local host leaf certificate - certificate/private key file" insert C:\Program Files (x86)\Real Thoughts GmbH\COMPROTware\Testtool\doc\2.22\Demo_Certificate\ReaTho-Demo-For_CPTT_2-Partner_B-leaf_cert-password_TlsSecTcp.p12
- In input field "Password for certificate/private key file" insert "TlsSecTcp".
- Press "Accept".

Now, both "CPTT 1" and "CPTT 2" are setup in a way that both CPTTs can be running as client or server. Start "CPTT 2" as Controlled Station, start "CPTT 1" as Controlling station and a TLS-secured connection should be established. With this setup and typical for TLS-secured connections, only the server’s certificate is transmitted, the client’s certificate is not transmitted.

Contact

Real Thoughts GmbH
Welfenstrasse 35 phone +49 721 627 6730
76137 Karlsruhe e-mail mailto:info@realthoughts.de
Germany website https://www.realthoughts.de/