COMPROTware:Testtool - Introduction to TLS-secured connections

Introduction and examples for TLS-secured connections

Real Thoughts GmbH, Welfenstraße 35, 76137 Karlsruhe, Germany,
e-mail info@realthoughts.de, https://www.realthoughts.com/; August 2026

Document version: `<$Version: 29$>`

First, simple test with *CPTT*

Test

- Get the IPv4 address for www.google.de
  - Linux: `$ ping -4 www.google.de`
  - MS Windows: `$ ping.exe -4 www.google.de`
- Start ***CPTT***. Change to protocol family "Raw data", to protocol "Raw date net"
- Set the IPv4 address to www.google.de (September, 2021: 142.251.36.195).
- Set Transport layer to TCP/IP, set Port no. 443
- Enable "Use TLS-secured connection".
- Select "TLS 1.3" as "Max. supported TLS version".
- Select "PEM" as "Certificate/key file format".
- Disable "Verify peer certificate".
- All other fields in section "TLS-secured connection" should be empty.
- Press Accept.
- Prepare a HTTP request:
  - In Main View, press right mouse button, select "Send Message ...".
  - Change to "LL Frame transparent".
  - Set Hexstring to `""GET /index.html HTTP/1.1" 0x0a 0x0a"` (the innermost quote characters are part of the Hexstring).
- Establish a connection: Action, Simulate Master.
- In window "Send Message": Press "Send".

```
    13:33:32.214
      Raw data net protocol profile:
        Max.Frame length = 250
        Delay after connection closed = 1sec
        Log communication errors = YES
        Delay after client connection estab. failed = 30sec
        TLS-secured connection enabled
          Max TLS version: TLS 1.3
          Certificate file format: PEM
          Local host leaf certificate - certificate file: <not specified>
          Local host leaf certificate - private key file: <not specified>
          Verify remote host leaf certificate: no
          Remote host leaf cert. - certificate chain file: <not specified>
          Remote host - Common name (CN): <not specified>
      Trying to connect to Slave at TCP:142.251.36.195:443 ...
    13:33:32.306
      Connection established to remote 142.251.36.195:443 via local 192.168.115.1:56991
        TLS-secured connection: TLSv1.3, TLS1-3-CHACHA20-POLY1305-SHA256
        Remote host leaf certificate:
          Serial no: 6A:2B:C4:96:86:8B:D1:AE:36:1E:E6:DB:4F:79:A9:84
          Subject: CN=google.com
          Issuer: C=US, O=Google Trust Services LLC, CN=GTS CA 1C3
          Valid: 2026-08-05 21:47:07 ... 2026-10-28 21:47:06
          Signed using: RSA with SHA-256; Public key: RSA key size: 2048 bits
          Key usage: Digital Signature,Key Encipherment
          Ext. key usage: TLS Web Server Authentication
M>> 13:33:36.725
M>>   0x47 0x45 0x54 0x20  0x2f 0x69 0x6e 0x64  0x65 0x78 0x2e 0x68  0x74 0x6d 0x6c 0x20    | GET /index.html
M>>   0x48 0x54 0x54 0x50  0x2f 0x31 0x2e 0x31  0x0a 0x0a                                   | HTTP/1.1
```

Explanation

- A TLSv1.3 connection is established.

- Used Cipher: TLS1-3-CHACHA20-POLY1305-SHA256
- For the ***CPTT*** side (this is the Master resp. client side) neither certificate nor a private key is specified.
- Google sends its certificate.
- If "Verify peer certificate" is enabled, connection establishment will fail because we do not have the Certificate chain file to verify Google's certificate.
- For TLS-secured connections to a web server, the client (***CPTT*** side) never needs a certificate or a key. If you specify in ***CPTT*** a local host certificate and a local host key, these information is ignored by the web server.

CPTT to *CPTT* TLS-secured connection

Test

- Start ***CPTT*** Change to protocol family "IEC 60870-5" and protocol "IEC 60870-5-104".
- Set Controlled Station IP address to 127.0.0.1 (is localhost), port no. to 19998 (is standard port no. for TLS-secured IEC 60870-5-104).
- Enable "Use TLS-secured connection".
- Select "TLS 1.3" as "Max. supported TLS version".
- Select "PEM" as "Certificate/key file format".
- Set "Leaf certificate certificate file" to `C:\Program Files (x86)\Real Thoughts GmbH\COMPROTware\Testtool\↩ doc\<release_no>\Demo_Certificate\ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-cert.pem`
- Set "Leaf certificate private key file" to `C:\Program Files (x86)\Real Thoughts GmbH\COMPROTware\Testtool\↩ doc\<release_no>\Demo_Certificate\ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-privkey.pem`
- Disable "Verify peer certificate".
- Clear "Certificate chain file" and "Common name (CN)".
- Press Accept.
- Save the current configuration: File, Save Configuration as user default.
- Start a second ***CPTT*** instance (it will overlap with the original instance, move the new window to another position).
- One ***CPTT*** instance: Action, Simulate Controlled Station.
- The other ***CPTT*** instance: Action, Simulate Controlling Station.
- A TLS-secured connection should be established, IEC 60870-5-104 Frames should be transmitted.
- Controlling Station log should look alike:

```
    13:52:01.811
      IEC 60870-5-104 protocol profile:
        Link Layer:
          Max.Frame length net = 250, gross = 252
          Timeout: t0 = 30sec, t1 = 15sec, t2 = 10sec, t3 = 20sec
          Parameter: k = 12, w = 8
          Auto STARTDT/STOPDT = YES
          Delay after connection closed = 1sec
          Log communication errors = YES
        Delay after client connection estab. failed = 30sec
        TLS-secured connection enabled
          Max TLS version: TLS 1.3
          Certificate file format: PEM
          Local host leaf certificate - certificate file: "ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-cert.pem"
            Serial no: 53:B0:E6:B7:6E:63:CB:4A:7F:F7:92:58:29:1B:26:22:55:26:B5:5D
            Subject: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Partner_A, emailAddress=info@realthoughts.de
            Issuer: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Real Thoughts GmbH (COMPROTware demo), emailAdd
            Valid: 2023-01-17 11:37:53 ... 2028-01-17 11:37:53
            Signed using: RSA with SHA-512; Public key: RSA key size: 2048 bits
          Local host leaf certificate - private key file: "ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-privkey.pem"
          Verify remote host leaf certificate: no
          Remote host leaf cert. - certificate chain file: "ReaTho-Demo-For_CPTT_1-Partner_B-cert_chain-cert.pem"
          Remote host - Common name (CN): <not specified>
      Trying to connect to Controlled Station at TCP:127.0.0.1:19998 ...
    13:52:01.918
      Connection established to remote 127.0.0.1:19998 via local 127.0.0.1:57221
        TLS-secured connection: TLSv1.3, TLS1-3-CHACHA20-POLY1305-SHA256
        Remote host leaf certificate:
          Serial no: 53:B0:E6:B7:6E:63:CB:4A:7F:F7:92:58:29:1B:26:22:55:26:B5:5D
          Subject: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Partner_A, emailAddress=info@realthoughts.de
          Issuer: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Real Thoughts GmbH (COMPROTware demo), emailAddre
          Valid: 2023-01-17 11:37:53 ... 2028-01-17 11:37:53
          Signed using: RSA with SHA-512; Public key: RSA key size: 2048 bits
C>> 13:52:02.010
C>>     U: STARTDT act
<<D 13:52:02.237
<<D     U: STARTDT con
```

- Controlled station log should look alike:

```
    13:52:01.188
      IEC 60870-5-104 protocol profile:
        Application Layer:
          Invoke qualified Message List to respond = no
        Link Layer:
          Max.Frame length net = 250, gross = 252
          Timeout: t0 = 30sec, t1 = 15sec, t2 = 10sec, t3 = 20sec
```

```
        Parameter: k = 12, w = 8
        Auto STARTDT/STOPDT = YES
        Delay after connection closed = 1sec
        Log communication errors = YES
      TLS-secured connection enabled
        Max TLS version: TLS 1.3
        Certificate file format: PEM
        Local host leaf certificate - certificate file: "ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-cert.pem"
          Serial no: 53:B0:E6:B7:6E:63:CB:4A:7F:F7:92:58:29:1B:26:22:55:26:B5:5D
          Subject: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Partner_A, emailAddress=info@realthoughts.de
          Issuer: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Real Thoughts GmbH (COMPROTware demo), emailAdd
          Valid: 2023-01-17 11:37:53 ... 2028-01-17 11:37:53
          Signed using: RSA with SHA-512; Public key: RSA key size: 2048 bits
        Local host leaf certificate - private key file: "ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-privkey.pem"
        Verify remote host leaf certificate: no
        Remote host leaf cert. - certificate chain file: "ReaTho-Demo-For_CPTT_1-Partner_B-cert_chain-cert.pem"
        Remote host - Common name (CN): <not specified>
    Waiting for connection from Controlling Station to TCP:0.0.0.0:19998 ...
  13:52:01.892
    Connection accepted from remote 127.0.0.1:57221 to 127.0.0.1:19998
      TLS-secured connection: TLSv1.3, TLS1-3-CHACHA20-POLY1305-SHA256
C>> 13:52:02.043
C>>     U: STARTDT act
<<D 13:52:02.046
<<D     U: STARTDT con
```

Explanation

- In this example for both client and server side (Controlling Station and Controlled Station side) a certificate and a private key is specified. Untypically both have the same certificate and private key.
- Typically only the client will request and check the certificate.
- The ***CPTT*** instance which simulated the client will show the certificate returned by the server.
- In the profile of the ***CPTT*** instance which simulated the client you can clear the fields "Leaf certificate certificate file" and "Leaf certificate private key file". This will not change the behavior.

Advanced *CPTT* to *CPTT* TLS-secured connection

Test

- IN BOTH ***CPTT*** INSTANCES, DO THE FOLLOWING:
  - Use profile from previous test.
  - Enabled "Verify peer certificate".
  - Set "Certificate chain file" to `C:\Program Files (x86)\Real Thoughts GmbH\COMPROTware\Testtool\↩ doc\<release_no>\Demo_Certificate\ReaTho-Demo-For_CPTT_2-Partner_A-cert_chain-cert.pem`
  - Set "Common name (CN)" to "Partner_A".
  - Press Accept.
- One ***CPTT*** instance: Action, Simulate Controlled Station.
- The other ***CPTT*** instance: Action, Simulate Controlling Station.
- A TLS-secured connection should be established, IEC 60870-5-104 Frames should be transmitted.
- Controlling Station log should look alike:

```
  14:05:49.723
    IEC 60870-5-104 protocol profile:
      Link Layer:
        Max.Frame length net = 250, gross = 252
        Timeout: t0 = 30sec, t1 = 15sec, t2 = 10sec, t3 = 20sec
        Parameter: k = 12, w = 8
        Auto STARTDT/STOPDT = YES
        Delay after connection closed = 1sec
        Log communication errors = YES
      Delay after client connection estab. failed = 30sec
      TLS-secured connection enabled
        Max TLS version: TLS 1.3
        Certificate file format: PEM
        Local host leaf certificate - certificate file: "ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-cert.pem"
          Serial no: 53:B0:E6:B7:6E:63:CB:4A:7F:F7:92:58:29:1B:26:22:55:26:B5:5D
          Subject: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Partner_A, emailAddress=info@realthoughts.de
          Issuer: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Real Thoughts GmbH (COMPROTware demo), emailAdd
          Valid: 2023-01-17 11:37:53 ... 2028-01-17 11:37:53
          Signed using: RSA with SHA-512; Public key: RSA key size: 2048 bits
        Local host leaf certificate - private key file: "ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-privkey.pem"
        Verify remote host leaf certificate: YES
        Remote host leaf cert. - certificate chain file: "ReaTho-Demo-For_CPTT_2-Partner_A-cert_chain-cert.pem"
          Serial no: 58:3B:A1:26:A9:34:0F:F1:A0:4B:3A:34:DC:0C:F7:77:49:F4:F5:35
          Subject: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Real Thoughts GmbH (COMPROTware demo), emailAd
          Issuer: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Real Thoughts GmbH (COMPROTware demo), emailAdd
          Valid: 2023-01-17 11:37:52 ... 2028-01-17 11:37:52
          Signed using: RSA with SHA-512; Public key: RSA key size: 2048 bits
        Remote host - Common name (CN): "Partner_A"
    Trying to connect to Controlled Station at TCP:127.0.0.1:19998 ...
  14:05:49.835
    Connection established to remote 127.0.0.1:19998 via local 127.0.0.1:57368
```

```
        TLS-secured connection: TLSv1.3, TLS1-3-CHACHA20-POLY1305-SHA256
        Remote host leaf certificate:
          Serial no: 53:B0:E6:B7:6E:63:CB:4A:7F:F7:92:58:29:1B:26:22:55:26:B5:5D
          Subject: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Partner_A, emailAddress=info@realthoughts.de
          Issuer: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Real Thoughts GmbH (COMPROTware demo), emailAddre
          Valid: 2023-01-17 11:37:53 ... 2028-01-17 11:37:53
          Signed using: RSA with SHA-512; Public key: RSA key size: 2048 bits
C>> 14:05:49.957
C>>     U: STARTDT act
<<D 14:05:50.246
<<D     U: STARTDT con
```

- Controlled station log should look alike:

```
    14:05:48.956
      IEC 60870-5-104 protocol profile:
        Application Layer:
          Invoke qualified Message List to respond = no
        Link Layer:
          Max.Frame length net = 250, gross = 252
          Timeout: t0 = 30sec, t1 = 15sec, t2 = 10sec, t3 = 20sec
          Parameter: k = 12, w = 8
          Auto STARTDT/STOPDT = YES
          Delay after connection closed = 1sec
          Log communication errors = YES
        TLS-secured connection enabled
          Max TLS version: TLS 1.3
          Certificate file format: PEM
          Local host leaf certificate - certificate file: "ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-cert.pem"
            Serial no: 53:B0:E6:B7:6E:63:CB:4A:7F:F7:92:58:29:1B:26:22:55:26:B5:5D
            Subject: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Partner_A, emailAddress=info@realthoughts.de
            Issuer: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Real Thoughts GmbH (COMPROTware demo), emailAdd
            Valid: 2023-01-17 11:37:53 ... 2028-01-17 11:37:53
            Signed using: RSA with SHA-512; Public key: RSA key size: 2048 bits
          Local host leaf certificate - private key file: "ReaTho-Demo-For_CPTT_1-Partner_A-leaf_cert-privkey.pem"
          Verify remote host leaf certificate: YES
          Remote host leaf cert. - certificate chain file: "ReaTho-Demo-For_CPTT_2-Partner_A-cert_chain-cert.pem"
            Serial no: 58:3B:A1:26:A9:34:0F:F1:A0:4B:3A:34:DC:0C:F7:77:49:F4:F5:35
            Subject: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Real Thoughts GmbH (COMPROTware demo), emailAd
            Issuer: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Real Thoughts GmbH (COMPROTware demo), emailAdd
            Valid: 2023-01-17 11:37:52 ... 2028-01-17 11:37:52
            Signed using: RSA with SHA-512; Public key: RSA key size: 2048 bits
          Remote host - Common name (CN): "Partner_A"
      Waiting for connection from Controlling Station to TCP:0.0.0.0:19998 ...
    14:05:49.802
      Connection accepted from remote 127.0.0.1:57368 to 127.0.0.1:19998
        TLS-secured connection: TLSv1.3, TLS1-3-CHACHA20-POLY1305-SHA256
        Remote host leaf certificate:
          Serial no: 53:B0:E6:B7:6E:63:CB:4A:7F:F7:92:58:29:1B:26:22:55:26:B5:5D
          Subject: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Partner_A, emailAddress=info@realthoughts.de
          Issuer: C=DE, ST=BaWue, L=Karlsruhe, O=Real Thoughts GmbH, OU=RaD, CN=Real Thoughts GmbH (COMPROTware demo), emailAddre
          Valid: 2023-01-17 11:37:53 ... 2028-01-17 11:37:53
          Signed using: RSA with SHA-512; Public key: RSA key size: 2048 bits
C>> 14:05:49.957
C>>     U: STARTDT act
<<D 14:05:49.957
<<D     U: STARTDT con
```

Explanation

- The "Certificate chain file" specified in ***CPTT*** instance 1 contains the Certificate chain to verify the Leaf certificate from ***CPTT*** instance 2. And vice versa. A "Certificate chain file" contains a chain of certificate (at least two cerfiticates).
- The "Common name (CN)" needs to be the same value as the item in the certificate of the opposite ***CPTT***
- Now, with "Verify peer certificate" enabled, both ***CPTT*** instances will show the opposite certificate.

More explanation

- A pem file is a file in ASCII format which may contain a private key, a ceritificate or a certificate chain. You can examine this file. It starts with "——BEGIN CERTIFICATE——" or "——BEGIN RSA PRIVATE KEY——" or alike.
- In contrast a p7 file typically contains (in binary format) a certificate chain, a p12 file typically contains a certificate and a private key.
- We always have 2 or 3 files which belong together:
  - Leaf certificate certificate file: For ***CPTT*** instance 1, send to ***CPTT*** instance 2 to identify ***CPTT*** instance 1 and to encrypt sent data.
  - Leaf certificate private key file: For ***CPTT*** instance 1, used by ***CPTT*** instance 1 for decryption of received data.
  - Certificate chain file: For ***CPTT*** instance 2 to verify the certificate received from ***CPTT*** instance 1.

Contact

Real Thoughts GmbH

Welfenstrasse 35
76137 Karlsruhe
Germany

phone +49 721 627 6730
e-mail info@realthoughts.de
https://www.realthoughts.de/