# Use of certificates in Automatic Communication

OTE uses following certificates and their root authorities for Automatic Communication:

|  |  |  |  |
| --- | --- | --- | --- |
| 1) |  | SERIALNUMBER = ICA - 10465001  CN = CSOTE  2.5.4.97 = NTRCZ-26463318 | web services security (BinarySecurityToken for WS-Security) |
| 2) |  | SERIALNUMBER = S251223  CN = CSOTE  OU = PKI  O = OTE, a.s. [IČ 26463318]  2.5.4.97 = NTRCZ-26463318  C = CZ | electronic seal of data sent from CS OTE to participant and S / MIME message signature. |
| 3) |  | SERIALNUMBER = S251223  CN = CSOTE Secure MIME  O = OTE, a.s. [IČ 26463318]  C = CZ | Encryption of emails from participant to OTE and TLS authentication in direction OTE-> participant |
| 4) |  | CN = \*.ote-cr.cz | SSL authentication certificate of communication server OTE(Thawte TLS RSA CA G1) |

Root Authorities

1. Commercial I.CA Intermediate Authority
2. Qualified I.CA Intermediate Authority
3. Root Authority I.CA
4. Thawte TLS RSA CA G1 Intermediate Authority
5. DigiCert Global Root G2 Root Authority
6. PostSignum Root QCA 2 Root Authority
7. PostSignum Qualified CA 2 Intermediate Authority
8. PostSignum Public CA 3 Intermediate Authority

Their use will be as follows:

# Server-server communication

### Calling the service in the direction Participant-> OTE

TLS: Participant calls OTE, using either a commercial certificate of supported authority for authentication or does not use any certificate. CS OTE returns the SSL certificate Thawte (4, with root and intermediate authorities 8 and 9) to be used for communication encryption.

SOAP: Participant uses qualified certificate for the ws-security signature, eventually also to sign an XML message. Message returned (return code) from OTE will be signed by CS OTE (1) certificate.

### Calling the service in the direction OTE-> Participant

TLS: OTE calls the participant using the CS OTE Secure MIME certificate (3) for authentication, the participant returns his commercial server certificate that will be used for encryption of communication.

Participants commercial server certificate must meet the following:

* commercial server certificate must have extended key usage „Server Authentication“
* In CN of the certificate must be servers URL (it is possible to use wildcard certificate)
* Certificate must be valid and it must be issued by certification authority accepted by OTE. List of these certification authorities can be found on this page: <https://www.ote-cr.cz/en/registration-and-agreements/access-to-cs-ote/certificates>

SOAP: OTE uses the CS OTE certificate (1) for the signature ws-security, for xml signature OTE uses seal CS OTE (2)

### Necessary settings:

Participants have to check if they have string of I.CA commercial authority certificates (5, 7) in the truststore for TLS client certificate authentication. If participant uses additional validation mechanism, it has to be adapted to CS OTE Secure MIME (2) certificate, e.g. DN mapping to routing rules, certificate mapping (or just CN) to the system user.

I.CA qualified authority certificates (6, 7) must be added to the ws-security truststore. If participant uses additional validation mechanism, it has to be adapted to CS OTE certificate (1).

In addition, the CS OTE seal (2) must be accepted when verifying the xml signature

# Client-server communication

TLS: Participant calls OTE, using either a commercial certificate of authority supported for authentication, or does not need a certificate. CS OTE returns the SSL certificate Thawte (4, with root and intermediate authorities 8 and 9) to be used for communication encryption

SOAP: Participant uses qualified certificate for the ws-security signature, eventually also to sign an XML message. Message returned from OTE will be signed by CS OTE (1) certificate.

If the client-server communication is picking up a message (waiting to be picked up by this communication), then the xml message in response will be signed with the CS OTE seal (2) and the ws-security response message will be signed with CS OTE certificate (1)

### Necessary settings:

I.CA qualified authority certificates (5, 6) must be added to the ws-security truststore. If participant uses additional validation mechanism, it has to be adapted to CS OTE certificate (2).

In addition, the CS OTE seal (2) must be accepted when verifying the xml signature

# SMTP e-mail communication

### Direction participant->OTE

Participant signs the mail by his qualified certificate and encrypts it with the CS OTE secure MIME certificate (3)

### Direction OTE->participant

OTE signs e-mail by CS OTE (2) certificate and encrypts it with participant’s commercial certificate.

### Necessary settings

Participants have to change CS OTE secure MIME (3) in their e-mail clients. Participants have to install I.CA root Authority into the internet explorer (windows truststore) into the root authorities and PostSignum Public CA 3 Intermediate Authority (12) and PostSignum Qualified CA 2 Intermediate Authority (11) in to the Intermediate Authorities.

**Certificate references**

1. CS OTE WS- [HERE](https://www.ote-cr.cz/cs/registrace-a-smlouvy/pristup-do-cs-ote/csote_auth_2020-1.cer)
2. CS OTE - SEAL - [HERE](https://www.ote-cr.cz/cs/registrace-a-smlouvy/pristup-do-cs-ote/csote_2020-4.cer)
3. CSOTE Secure MIME - [HERE](http://www.ote-cr.cz/cs/registrace-a-smlouvy/pristup-do-cs-ote/csote_smime_2020.cer)
4. SSL certificate of communication server OTE (Thawte TLS RSA CA G1) - [HERE](https://www.ote-cr.cz/cs/registrace-a-smlouvy/pristup-do-cs-ote/certificate_ote-cr-cz.crt)

Root Authorities

1. Commercial I.CA Intermediate Authority - <https://www.ica.cz/HCA-commercial>
2. Qualified I.CA Intermediate Authority - <https://www.ica.cz/HCA-qualificate>
3. Root Authority I.CA - <https://www.ica.cz/HCA-root-en>
4. Thawte TLS RSA CA G1 Intermediate Authority - <https://www.digicert.com/digicert-root-certificates.htm>
5. DigiCert Global Root G2 Root Authority - <https://www.digicert.com/digicert-root-certificates.htm>
6. PostSignum Root QCA 2 - http://www.postsignum.cz/files/ca/postsignum\_qca2\_root.cer
7. PostSignum Qualified CA 2 - <http://www.postsignum.cz/files/ca/postsignum_qca2_sub.cer>
8. PostSignum Public CA 3 - http://www.postsignum.cz/files/ca/postsignum\_vca3\_sub.cer