# Použití certifikátů v automatické komunikaci

OTE používá pro automatickou komunikaci tyto certifikáty a jejich kořenové autority:

|  |  |  |  |
| --- | --- | --- | --- |
| 1) |  | SERIALNUMBER = S251223  CN = CS OTE auth  O = OTE, a.s.  2.5.4.97 = NTRCZ-26463318  C = CZ | Pro zabezpečení webových služeb (BinarySecurityToken pro WS-Security)y+ autentizace TLS směrem OTE->účastník |
| 2) |  | SERIALNUMBER = S251223  CN = CSOTE  OU = PKI  O = OTE, a.s.  2.5.4.97 = NTRCZ-26463318  C = CZ | Určeno pro elektronickou pečeť dat zasílaných z CS OTE účastníkovi a podpis S/MIME zpráv. |
| 3) |  | SERIALNUMBER = S251223  CN = CSOTE Secure MIME  O = OTE, a.s.  2.5.4.97 = NTRCZ-26463318  C = CZ | Šifrování emailů směrem od účastníka do OTE |
| 4) |  | CN = \*.ote-cr.cz | SSL certifikát komunikačního serveru OTE (Thawte RSA CA G1) |

Kořenové autority:

1. Komerční PostSignum Public CA 4 zprostředkující autorita
2. Kvalifikovaná PostSignum Qualified CA 3 zprostředkující autorita
3. PostSignum Root QCA 4
4. PostSignum Root QCA 2
5. Thawte RSA CA 2018 zprostředkující autorita
6. DigiCert Global Root G2 kořenová autorita

Jejich použití je následující:

# Server-server komunikace

### Volání služby směrem účastník-> OTE

TLS: účastník volá OTE, pro autentizaci použije buď komerční certifikát podporované autority, nebo certifikát použít nemusí. CS OTE vrátí veřejnou část SSL certifikátu Thawte (4, s kořenovou a zprostředkující autoritou 9,10), který bude použit pro šifrování komunikace

SOAP: účastník použije pro podpis WS-Security kvalifikovaný certifikát, popřípadě použije kvalifikovaný certifikát i pro podpis xml zprávy. Ze strany OTE je následně vrácena odpověď (return code) digitálně podepsaná komerčním certifikátem CSOTE auth (1)

### Volání služby směrem OTE-> účastník

TLS: OTE volá účastníka, pro autentizaci použije komerční certifikát CSOTE auth (1), účastník vrátí jeho serverový komerční certifikát, kterým bude následně šifrována komunikace.

Serverový komerční certifikát účastníka musí splňovat následující parametry:

* Serverový komerční certifikát s extended key usage „Server Authentication“ (OID 1.3.6.1.5.5.7.3.1)
* V CN certifikátu musí být uvedena url serveru (je možné použít wildcard certifikát)
* Certifikát musí být platný a musí být vydán certifikační autoritou akceptovanou OTE. Seznam akceptovaných certifikačních autorit je zveřejněn na odkaze: <https://www.ote-cr.cz/cs/registrace-a-smlouvy/pristup-do-cs-ote/certifikaty>.

SOAP: OTE použije pro zabezpečení ws-security komerční certifikát CSOTE auth (1), pro elektronickou pečeť xml certifikát CSOTE (2)

### Potřebné nastavení:

Účastník musí do seznamu důvěryhodných certifikátů (truststore) pro ověřování TLS klientského certifikátu přidat řetězec **komerčních** autorit PostSignum (5, 7). V případě, že účastník používá další ověřovací mechanismy, musí je adaptovat na certifikát CSOTE auth (1), např. mapování DN na směrovací pravidla, mapování certifikátu (nebo jen CN) na systémového uživatele.

Do truststoru pro ws-security musí být přidány certifikáty řetězce **komerčních** autority PostSignum (5, 7). V případě, že účastník používá další ověřovací mechanismy, musí je adaptovat na komerční certifikát CSOTE auth (1).

Dále musí být akceptována pečeť CSOTE (2) při ověření elektronické pečetě xml zprávy

# Klient-server komunikace

TLS: účastník volá OTE, pro autentizaci použije buď komerční certifikát podporované autority, nebo certifikát použít nemusí. CS OTE vrátí SSL certifikát Thawte (4, s kořenovou a zprostředkující autoritou 9,10), který bude použit pro šifrování komunikace.

SOAP: účastník použije pro zabezpečení WS-Security kvalifikovaný certifikát, popřípadě použije kvalifikovaný certifikát i pro digitální podpis xml zprávy. Ze strany OTE je následně vrácena odpověď (return code) podepsaná komerčním certifikátem CSOTE auth (1). V případě, že je pomocí client-server komunikace vyzvedávána zpráva, která čeká na vyzvednutí touto komunikací, pak je xml zpráva v odpovědi zabezpečena certifikátem pro elektronickou pečeť CSOTE (2) a WS-Security odpovědní zprávy je zabezpečena komerčním certifikátem CSOTE auth (1).

### Potřebné změny:

Účastník musí do truststoru pro WS-Security přidat certifikáty řetězce **komerčních** autorit PostSignum (5, 7). V případě, že účastník používá další ověřovací mechanismy musí je adaptovat na certifikát CSOTE auth (1).

Dále musí být akceptována pečeť CSOTE (2) při ověření podpisu xml zprávy.

# E-mailová komunikace

### Směr účastník-> OTE

Účastník zasílaný e-mail podepíše svým kvalifikovaným certifikátem a zašifruje jej pomocí certifikátu CSOTE Secure MIME (3)

### Směr OTE-> účastník

OTE zasílaný e-mail zabezpečí elektronickou pečetí CSOTE (2) a zašifruje pomocí komerčního certifikátu uživatele

### Potřebné změny:

Účastník musí změnit ve svém poštovním klientu certifikát CSOTE Secure MIME (3). Účastník nainstaluje do Internetu Exploreru (windows truststore) certifikáty kořenové certifikační autority PostSignum (7) a do zprostředkujících autorit komerční PostSignum Public CA 4 zprostředkující autoritu (5) a kvalifikovanou PostSignum Qualified CA 2 (8) zprostředkující autoritu (6).

# Odkazy na certifikáty

1. CS OTE WS- [ZDE](https://www.ote-cr.cz/cs/registrace-a-smlouvy/pristup-do-cs-ote/csote_auth_2020-1.cer)
2. CS OTE – pečeť - [ZDE](https://www.ote-cr.cz/cs/registrace-a-smlouvy/pristup-do-cs-ote/csote_2020-4.cer)
3. CSOTE Secure MIME - [ZDE](http://www.ote-cr.cz/cs/registrace-a-smlouvy/pristup-do-cs-ote/csote_smime_2020.cer)
4. SSL certifikát komunikačního serveru OTE (Thawte RSA CA 2018) - [ZDE](https://www.ote-cr.cz/cs/registrace-a-smlouvy/pristup-do-cs-ote/certificate_ote-cr-cz.cer)

Kořenové autority

1. Komerční PostSignum Public CA 4 zprostředkující autorita – [ZDE](http://www.postsignum.cz/files/ca/postsignum_vca4_sub.cer)
2. Kvalifikovaná PostSignum Qualified CA 4 zprostředkující autorita – [ZDE](http://www.postsignum.cz/files/ca/postsignum_qca4_sub.cer)
3. PostSignum Root QCA 4 - [ZDE](http://www.postsignum.cz/files/ca/postsignum_qca4_root.cer)
4. PostSignum Root QCA 2 - [ZDE](http://www.postsignum.cz/files/ca/postsignum_qca2_root.cer)
5. Thawte RSA CA 2018 zprostředkující autorita – [ZDE](https://www.sslmarket.cz/download/ca-certificates/dc/Thawte%20RSA%20CA%202018.pem)
6. DigiCert Global Root G2 kořenová autorita – [ZDE](https://dl.cacerts.digicert.com/DigiCertGlobalRootG2.crt)