User manual for access to CS OTE

Changes in certificates

Certificates from the supported CAs to CS OTE

As of October 1st 2017, the access to the web portal of CS OTE as well as the electronic signing in CS OTE will be possible using qualified certificates only. As of July 1st 2017, it will be possible to register only qualified certificates for accessing the web portal of CS OTE and using electronic signatures. CS OTE users will be enabled to use their current certificates (commercial certificates and OTECA certificates) in the web portal of CS OTE by September 30th 2017.

This change is based on the Regulation (EU) No. 910/2014 of the European Parliament and of the Council (eIDAS) and on the Act No. 297/2016 Coll. on trust services for electronic transactions. The qualified certificates in CS OTE are used in compliance with the statement of the Ministry of Interior - available under the following link.

The certificates OTECA and OTECA-TEST issued by company CGI IT Czech Republic s.r.o. will not be supported in CS OTE from 1. 10. 2017. Issuing of OTECA certificates, including renewal of certificates, will not be further ensured as of May 1st 2017.

As of July 1st 2017, until further notice, it will be possible **to register qualified system certificates only for an electronic signature in an automatic communication** (creation of an electronic mark), **until qualified certificates for electronic seals will be available** as a replacement of the current system certificates. As of October 1st 2017, it will not be possible to use commercial certificates for creation of an electronic mark (automated signature).

For **sending encrypted messages to CS OTE** through a secured e-mail the original OTECA certificate will be replaced with a **commercial certificate** by the Market Operator. The new commercial certificate of OTE will be placed on the OTE’s website for download and the users will be informed by the Market Operator in the near future. As of October 1st 2017, every market participant has to have a commercial certificate to be able to receive encrypted messages from CS OTE through encrypted e-mail.

As of October 1st 2017, the market participants will have to use **a commercial certificate to log in to OTE-COM application**. For electronic signing of data the same rules must be followed as in case of a web portal, i.e. as of October 1st 2017 all data must be signed with a qualified certificate only.

The planned change does not affect users who have been already using the qualified certificate for communication with the web portal of CS OTE. A list of certification authorities (CAs) issuing qualified certificates for electronic signature is posted bellow.

The list of certificates can be extended at the request of a market participant for verification of the certification authority by the market operator - please contact services@ote-cr.cz

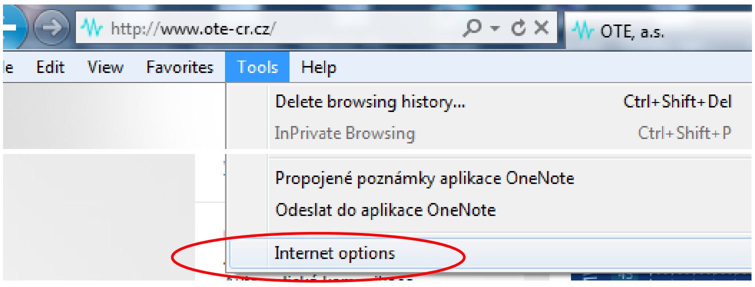
Authority Link	**State**	**Commercial CA**	**Qualified CA**	**Note**
První certifikační autorita, a.s. http://www.ica.cz/	CZ	**YES** všechny komerční certifikáty	**YES** I.CA Qualified 2 CA/RSA 02/2016 I.CA - Qualified Certification Authority, 09/2009 I.CA - Qualified root certificate	
Česká pošta, s.p. (PostSignum) http://www.postsignum.cz/	CZ	**YES** všechny komerční certifikáty	**YES** PostSignum Qualified CA PostSignum Qualified CA 2 PostSignum Qualified CA 3	
eIdentity a.s. http://www.eidentity.cz/app	CZ	**YES** všechny komerční certifikáty	**YES** ACAeID2.1 - Qualified Issuing Certificate (kvalifikovaný systémový certifikát vydávající CA)	
NetLock Ltd http://www.netlock.hu/	HU	**YES** NetLock (Class B Legal) NETLOCK Trust Advanced CA	**YES** NetLock (Class QA) NetLock (Class Q Legal) NetLock (Class Q) NetLock (Class Q Legal Spec.)	
GLOBALTRUST http://www.globaltrust.eu/	AU	**YES** GLOBALTRUST ADVANCED 1 GLOBALTRUST CLIENT 1 A-CERT CLIENT (jen stávající) A-CERT ADVANCED (jen stávající)	**YES** GLOBALTRUST QUALIFIED 1 GLOBALTRUST 2015 QUALIFIED 1	Previously ARGE DATEN
QuoVadis https://www.quovadisglobal.com/	CH/BE	**YES** QuoVadis Swiss Advanced CA G2	**YES** QuoVadis Belgium Issuing CA G1 QuoVadis Belgium Issuing CA G2	
GeoTrust https://www.geotrust.com/	US	**YES** GeoTrust SSL CA - G3	**NO**	
GoDaddy.com https://uk.godaddy.com/	US	**YES** GD Root Certificate Authority - G2	**NO**	

1. Verification of certificate of supported CAs

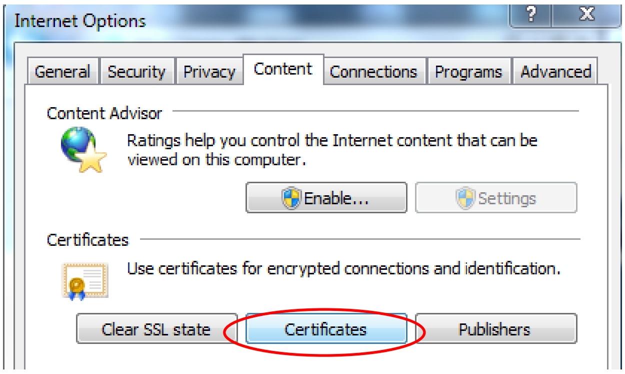
- ✓ **For access to CS OTE through web portal and electronic signing** it will be required using **qualified certificates** from qualified authorities only.

- ✓ **To log in application OTECOM and to encrypt the e-mail messages** it will be possible to use **commercial certificates** from commercial authorities only.

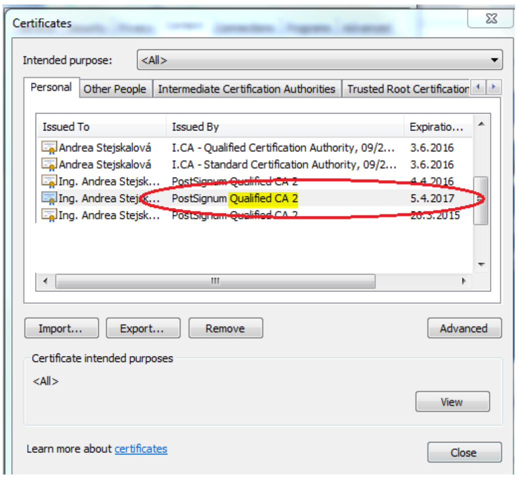
Step 1 – In Internet Explorer, section Tools, click on Internet options.


http://www.ote-cr.cz/
OTE, a.s.
e
Edit
View
Favorites
Tools
Help
Delete browsing history... Ctrl+Shift+Del
InPrivate Browsing Ctrl+Shift+P
Propojené poznámky aplikace OneNote
Odeslat do aplikace OneNote
Internet options

Step 2 – In the tab Content, click on Certificates



Step 3 – In the list of certificates checking of your certificate

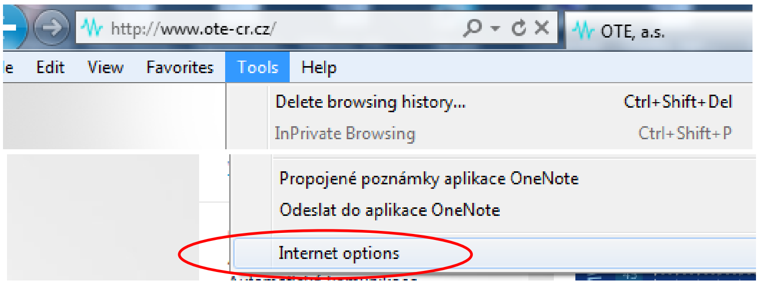

Certificates
Intended purpose: <All>
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification

Issued To	Issued By	Expiratio...
Andrea Stejskalová	I.CA - Qualified Certification Authority, 09/2...	3.6.2016
Andrea Stejskalová	I.CA - Standard Certification Authority, 09/2...	3.6.2016
Ing. Andrea Stejsk...	PostSignum Qualified CA 2	4.4.2016
Ing. Andrea Stejsk...	PostSignum Qualified CA 2	5.4.2017
Ing. Andrea Stejsk...	PostSignum Qualified CA 2	20.3.2015

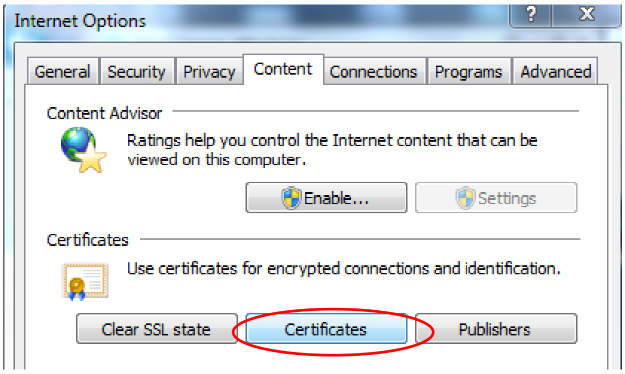
Import...
Export...
Remove
Advanced
Certificate intended purposes
<All>
View
Learn more about certificates
Close

2. To generate a public key of the certificate

Step 1 – In Internet Explorer, section Tools, click on Internet options



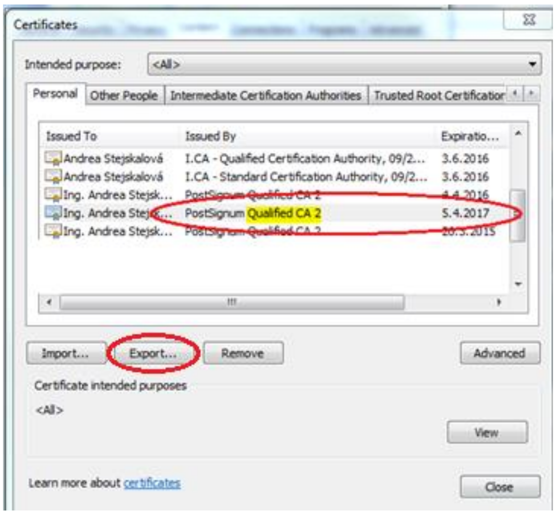
Step 2 – In the tab Content, click on Certificates



Ratings help you control the Internet content that can be viewed on this computer.

Use certificates for encrypted connections and identification.

Step 3 – In the list of certificates choose the appropriate certificate and click on Export to generate a public key



Intended purpose: <All>

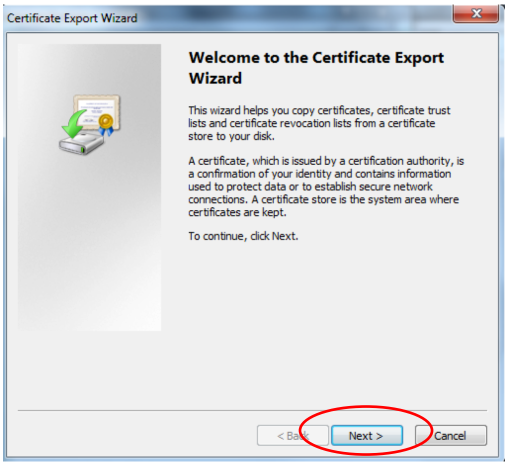
Issued To	Issued By	Expiratio...
Andrea Stejskalová	I.CA - Qualified Certification Authority, 09/2...	3.6.2016
Andrea Stejskalová	I.CA - Standard Certification Authority, 09/2...	3.6.2016
Ing. Andrea Stejsk...	PostSignum Qualified CA 2	4.4.2016
Ing. Andrea Stejsk...	PostSignum Qualified CA 2	5.4.2017
Ing. Andrea Stejsk...	PostSignum Qualified CA 2	20.5.2015

Certificate intended purposes

<All>

Learn more about certificates

Step 4 - Click Next



Certificate Export Wizard

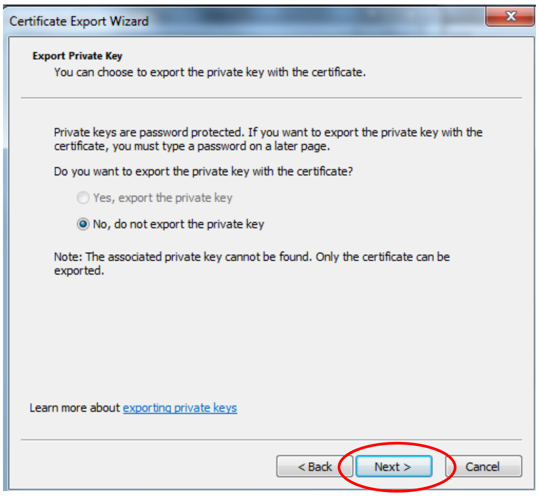
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Step 5 – Leave the settings and click Next



Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

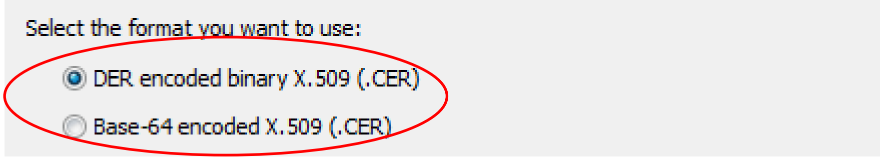
○ Yes, export the private key

● No, do not export the private key

Note: The associated private key cannot be found. Only the certificate can be exported.

Learn more about exporting private keys

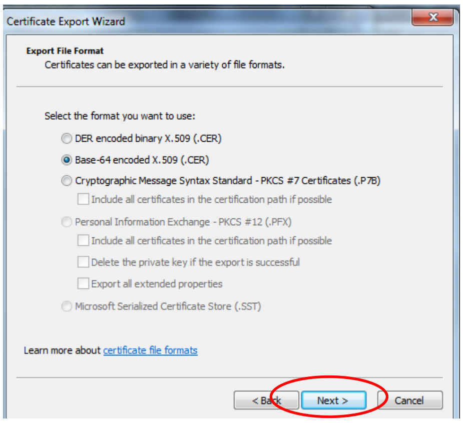
Step 6 – Choose the correct format **DER** or **Base-64** and click Next.
Only these formats may be uploaded to CS OTE



Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)



Certificate Export Wizard

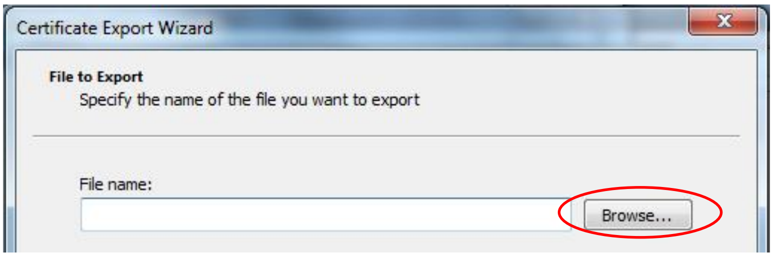
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ○ DER encoded binary X.509 (.CER)
- ● Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
- ○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Step 7 – Click Browse to choose the file directly

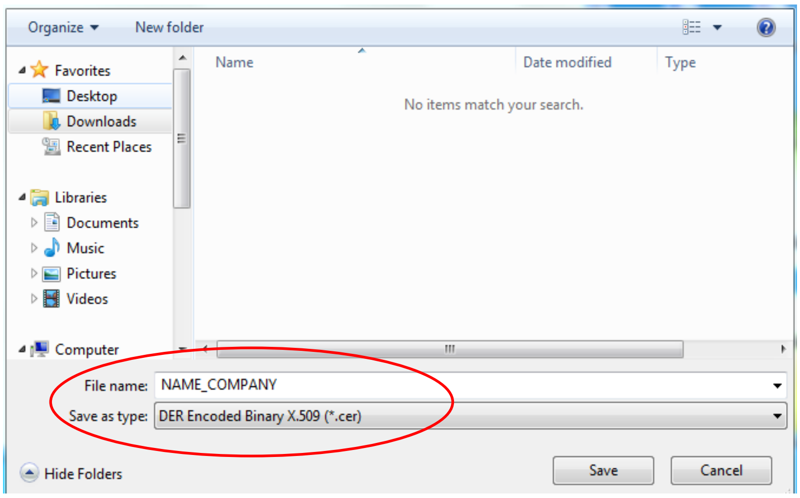


Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name:

Step 8 – Name the file, e.g. the name of a user and a company and click Save

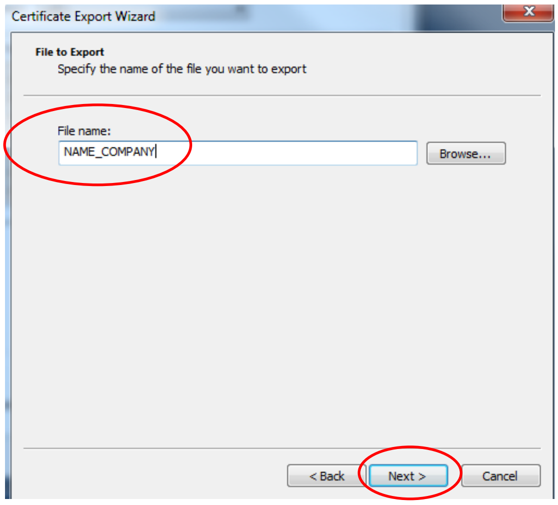


No items match your search.

File name: NAME_COMPANY

Save as type: DER Encoded Binary X.509 (*.cer)

Step 9 – Click Next

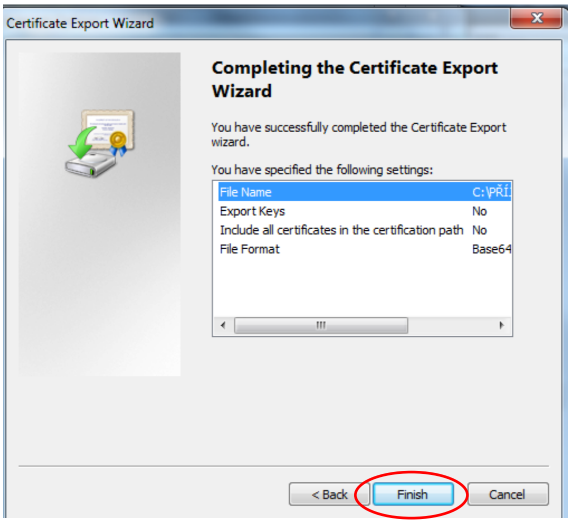

Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name: NAME_COMPANY

Step 10 – Click Finish


Certificate Export Wizard

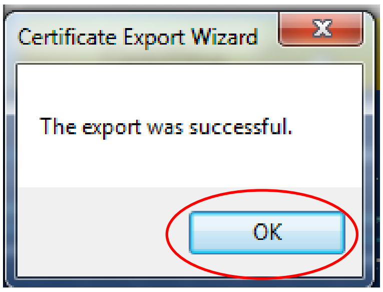
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\PŘÍ
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64

Step 11 – Successful export is confirmed by the following dialog:


Certificate Export Wizard

The export was successful.

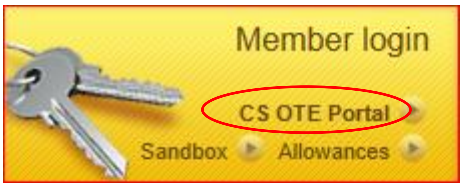
3. Registration of a public key in CS OTE

The public key of certificate has to be registered in CS OTE. After successful registration a user can log in CS OTE. The procedure for registration is as follows:

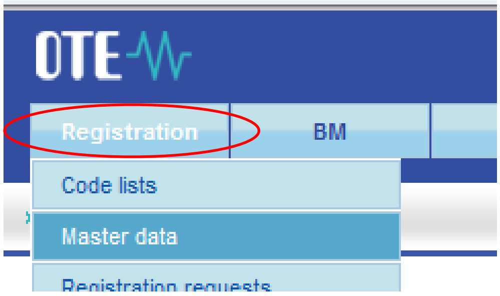
A) **A new user** or a **user with the expired certificate** cannot login in the CS OTE and their public key of a certificate has to be registered by an Authorized Person with administrator rights on behalf of their company. The Authorized Person is highlighted in the list of the users in CS OTE. The authorized person proceeds with the registration certificate by following the steps 1 to 6.

B) **The registered user with a still valid certificate in CS OTE (certificate renewal)** uploads the public key of a renewed certificate to CS OTE. A user may upload the public key only to their user account. The usern proceeds with the registration certificate by following the steps 1 to 6.

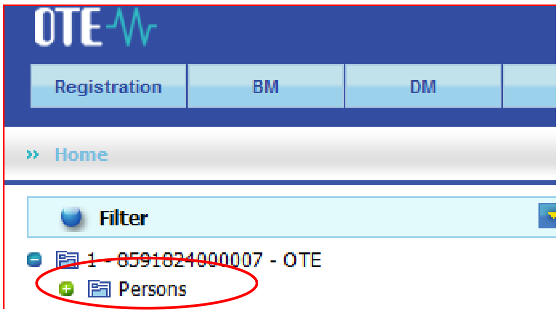
Step 1 – Login in CS OTE via a valid certificate



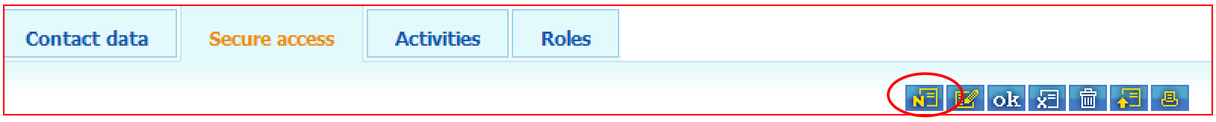
Step 2 – Choose tab Registration, click on Master data



Step 3 – Click on Persons and the name of user to which the certificate is registered

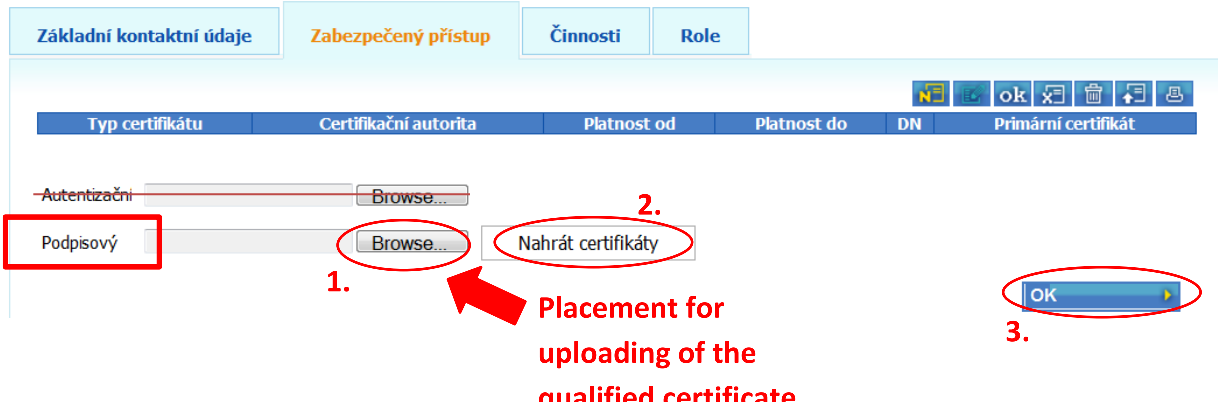


Step 4 – In tab Secure access, click on the field New



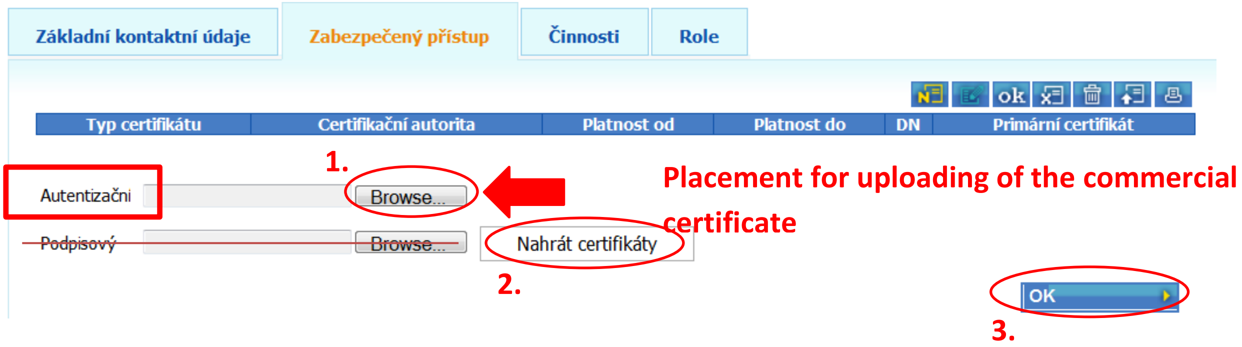
Step 5 – The upload of the public part of certificate shall be proceed by Browse button. The relevant public part of the certificate can be uploaded as follows:

- ✓ "**Qualified" type** (Signing till July 1, 2017) - **is used for access to CS OTE through web portal and for electronic signing.**



As of July 1, 2017 the section name will be changed from "Signing" to "Qualified" in CS OTE.

- ✓ **Commercial "type** (Authentication till July 1, 2017) - **is used to log in OTECOM, TLS authentication and to encrypt e-mail messages.**



1.

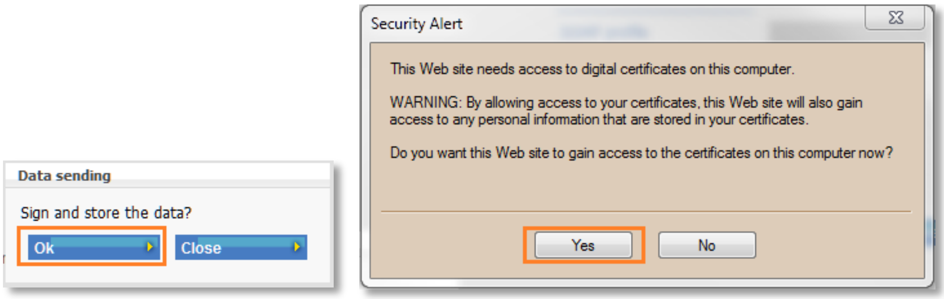
Placement for uploading of the commercial certificate

2.

3.

As of July 1, 2017 the section name will be changed from "Authentication" to "Commercial" in CS OTE.

Step 6– sign and store the renewal proces


Data sending

Sign and store the data?

Security Alert

This Web site needs access to digital certificates on this computer.

WARNING: By allowing access to your certificates, this Web site will also gain access to any personal information that are stored in your certificates.

Do you want this Web site to gain access to the certificates on this computer now?

After a successful registration a renewed certificate is displayed under a original certificates.