

User Manual of Information System



Client station configuration

This document and its content are confidential. It is forbidden to reproduce the document or its parts, to show it to third parties or to use it for any other purposes than it was provided for without prior written agreement by OTE, a.s.

Date	Description of revision
30.12.2009	Final version
12.1.2011	Removal of outdated information
5.2.2011	Update new configuration for WIN7, Vista and MS Office
20.6.2011	Configuration for FireFox browser
1.11.2012	Update list of supported workstation configurations (IE v9. FireFox v12)
18.6.2013	Update WS configuration and sign package
12.8.2014	Update list of supported workstation configurations (IE v11. WIN7, WIN8.1)
02.02.2014	Update PKIComponent for FireFox
16.03.2015	Update CGI PKI Component pro IE
23.03.2015	SSL/TLS configuration change
20.12.2016	SafeNet SW and eTokens update
5.1.2017	Add configuration for new web browsers (Google Chrome, Microsoft Edge)
8.3.2018	Removal of outdated information about OTECA, OTECATEST certificates
15.3.2018	Instalation and advanced settings for OTE PKi Client used for access to CS OTE
22.5.2018	Installing new component OTE PKI + setting up for several web-browsers
20.9.2018	Update of Acces over OTE-COM application
27.11.2018	Update of Mozilla Firefox settings for using PKI component
26.2.2019	Another possibility of gaining certification authority file oteca.pem
6.5.2019	Insertion of paragraph about local storage from document Registration
26.6.2023	Update of compatible configuration and update of OTE-COM download

Contents

1	Workstation configuration	3
2	Browsers Google Chrome, Mozilla Firefox and Microsoft Edge	4
2.1	<i>Installation of Component OTE PKI Client for access to CS OTE.....</i>	<i>4</i>
2.2	<i>Post-install configuration.....</i>	<i>6</i>
2.2.1	Importing OTECA authority into Mozilla Firefox browser	6
2.2.2	Dissabling IPV6 DNS in Mozilla Firefox browser	9
2.2.3	Configuring web browser Microsoft Edge.....	9
2.2.4	Configuration of CS OTE portal	10
2.2.5	Deleting already initialized Local Storage for SW certificates	11
2.2.6	Pairing web application and the component	11
2.2.7	<i>Switchover from OTE PKI component to local certificate storage</i>	<i>13</i>
3	Settings of local certificates storage	15
3.1.1	Management of local certificates storage	15
3.1.2	Insert certificate to local certificates storage	16
3.1.3	Remove certificate from local certificates storage	17
3.1.4	Removing expired certificates from local storage.....	18
3.1.5	Choose primary certificate	19
3.1.6	Change password for local certificates storage access	19
3.1.7	Forgotten password for local certificates storage access.....	20
4	Re-registering the Certificate after validity expires	22
5	Instruction for the first access to the production environment of OTE-COM application	23
5.1	<i>Application OTE-COM Launcher Manager.....</i>	<i>23</i>
5.2	<i>Access to AMQP server from market participant's server (Automatic communication)</i>	<i>24</i>

1 Workstation configuration

Compatible web browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge (without compatible mode)

Compatible operating systems:

- Windows 10
- Windows 11

We recommend to use security updates from <http://windowsupdate.microsoft.com>.

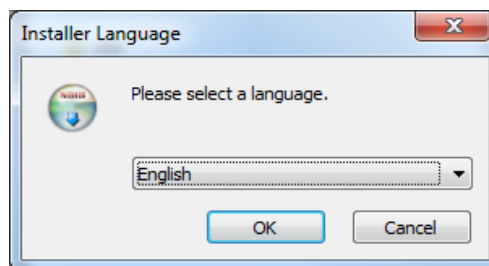
2 Browsers Google Chrome, Mozilla Firefox and Microsoft Edge

2.1 Installation of Component OTE PKi Client for access to CS OTE

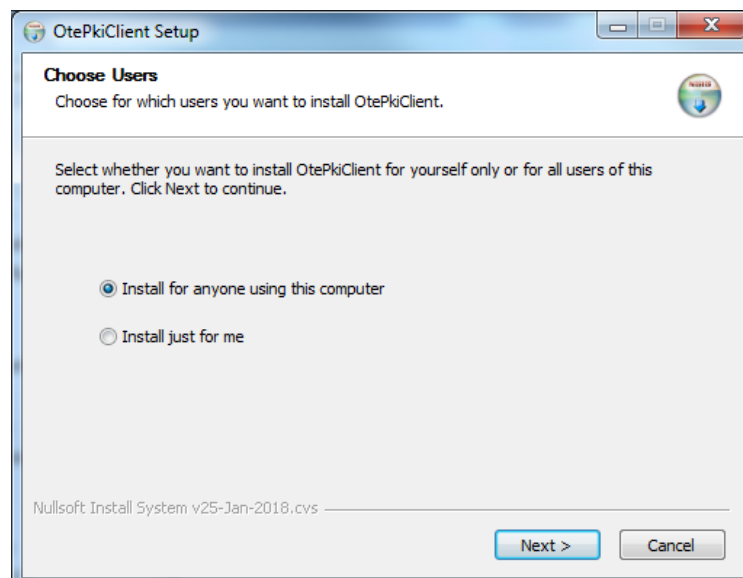
Link for downloading installation file is located on web page: http://www.ote-cr.cz/registration-and-agreements/access-to-cs-ote/konfigurace-pc?set_language=en in the table **A – Access to CS OTE through a web browser** (links for installation packages for IE and for other supported browsers 32-bit, 64-bit OS).

To start installation open the downloaded file:

- 1) You will be asked to choose the language of installation

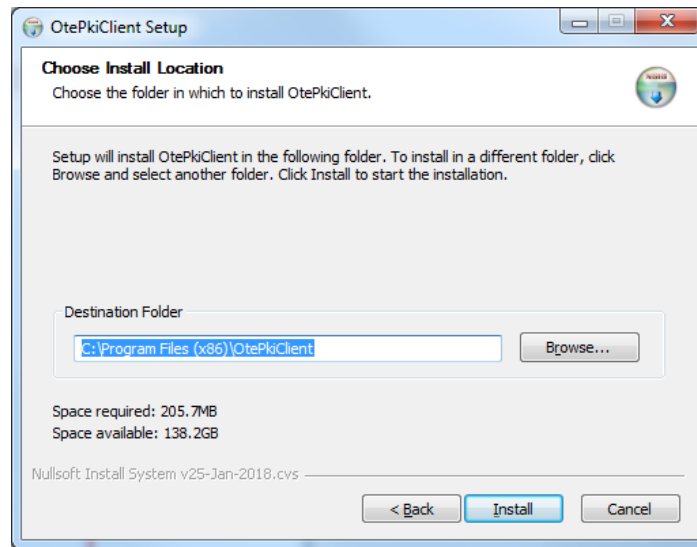


- 2) In next step, according to used browser, decide if to install OtePkiClient just for you or for anyone using this PC



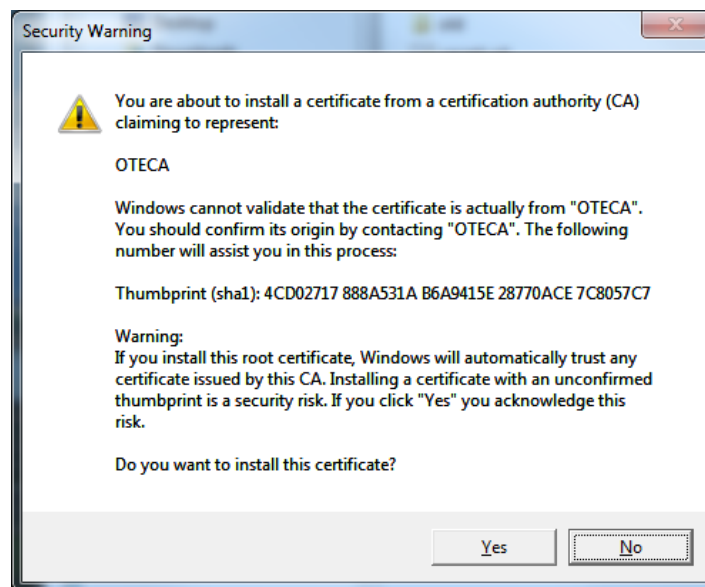
- Choosing “Install for anyone ...” will locate installation into Program Files

- Choosing “Install just for me” will locate installation into User’s Folder
- 3) Now, it is possible to modify the location manually



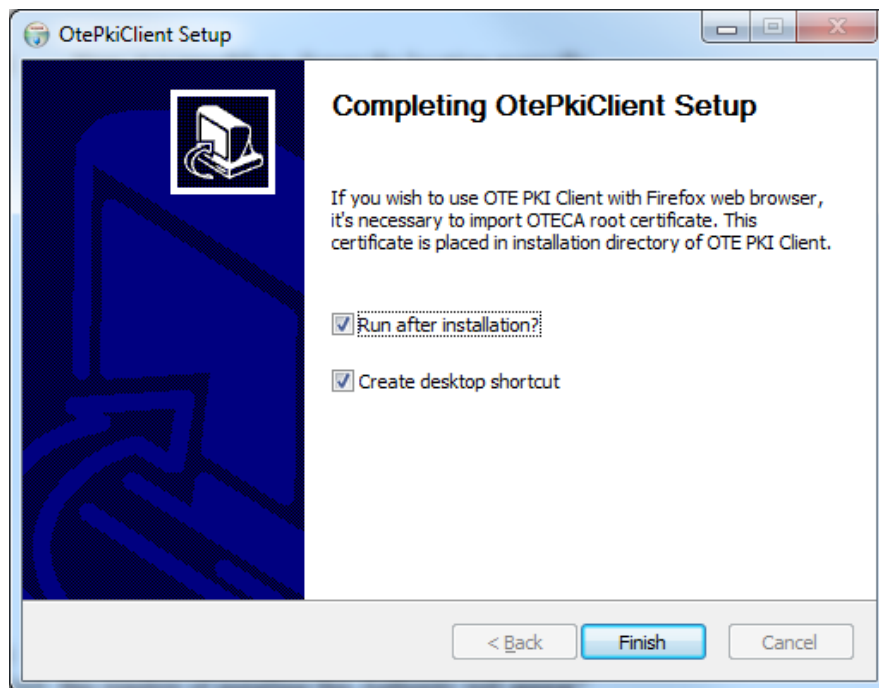
- 4) Is there OTECA Authority installed in Trusted Root Authorities on this PC ?

If this authority is in the system not installed yet, following window with information about installing this Authority will appear:



Pressing YES the installation will continue. Installed Authority is valid for all supported web browsers except Mozilla Firefox. Process of installing for this browser is described in the chapter 2.3.

5) Now we choose if to run OtePkiClient after Installation and if to create the Shortcut on Desktop.



2.2 Post-install configuration

If using another web-browser then Mozilla Firefox, please see the chapter 2.5.

2.2.1 Importing OTECA authority into Mozilla Firefox browser

In the case of using OtePikiClient with this web-browser it is necessary to install OTECA authority into the browser manually:

- a) Download the file oteca.pem from the link <https://www.ote-cr.cz/cs/registrace-a-smlouvy/pristup-do-cs-ote/files-konfigurace-pc/otecca.pem> and install it into the browser.

or

- b) Copy the text shown below into file called OTECA.pem and use this file for installing into web browser :

-----BEGIN CERTIFICATE-----

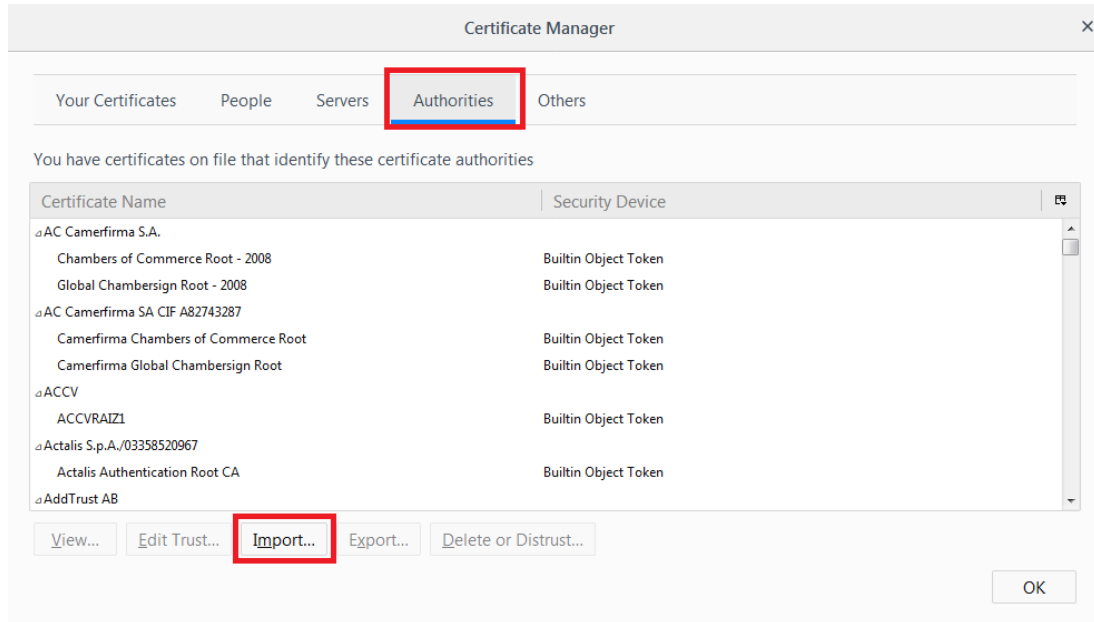
MIIFpDCCA4ygAwIBAgIKAg9tFwPoO3XI5TANBqkqhkiG9w0BAQsFADA/MQswCQYD
VQQGEwJDWjESMBAGA1UECgwJT1RFLCBhLnMuMQwwCgYDVQQGLDANQs0kxDjAMBgNV
BAMMBU9URUNBMB4XDTE4MDMwNTE3NDgwM1oXDTI4MDMwNTE3NDgwM1owPzELMAkG
A1UEBhMCQ1oxEjAQBgNVBAoMCU9URSwgYS5zLjEMMAoGA1UECwwDUETJM04wDAYD
VQQDDAVPVEVDQTCcAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgocGgIBANrqtuv
5zS9byhArdH2sTE+dAGSYT85RT71+ElkoCwpYbOsGsR3/7LzbQT0R7dn8iSDPR5a
hh0B8mdcWLYXOV0croBFs0WpGUiOSiwpKLFr+aXmtVNBfX5qF+GZWRj+G+NfhYgr
zARTN2Ws0MnQGZbXY0GuIWOwYItj9EA15qTE3IN/ereSzwkSwx3Fd2AigxL7V6Yw
pxU+rWe39MFH8prTPw6TI0xvPconZwObaIoHG54P4wRqEeuKnzaW4vZeinGvIXpn
5MamU2tQrMUGCMOEeycASPMEubSK8z6IyJ35ZQ31aeUk3lwrzp0CJZVFSztThn8T
9e1ZiPHxD3LbW5bGT7hSVqe7qe1qwdomYItQrRLJZ17YMBEA8vfgZHwjcja07QfX
ljYdUirnujTDgHqcu6RXVkhPvVbdFNcRe1o34+8TzmDXQOVOTSzjEoDgCb++Rvcp
+pxbbQUFM4ja3BH3Y9hV2GWSptET/FhY028gG2KkFpXAz7HzpnLjm27dvSH4RU3S
AYKm+cd/btgDI2fGzaKtVt50+trB2Wjl+GipsRkw2VmOdBDO++T28NcrOu7HNVBf
xNzpvHchoVOonWLBghxzqVDux+BWEriOIJYSebBbQdn0Vic5xB0+kcGMHmfJ6Dz
7sOh1ZgH3h3rYg7G88JxGVGbxFGZHMTYyamhAgMBAAGjgaEwgZ4wDwYDVR0TAAQH/
BAUwAwEB/zALBGNVHQ8EBAMCAQYwHQYDVR0OBBYEFQpk3trCPeD1gO1UhNgqi73M
7xMVMB8GA1UdIwQYMBAAFOpk3trCPeD1gO1UhNgqi73M7xMVMB4GA1UdEQQXMBWB
E290ZWNhLmN6QGxvZ21jYS5jb20wHgYDVR0SBBcwFYETb3RlY2EuY3pAbG9naWNh
LmNvbTANBqkqhkiG9w0BAQsFAAOCAGeAXL8eTcjeG0Yb341YzErb+KGM6S2gWAqk
eBbrVtVJ6uq41UYVuQ2radrN26ZMSedTyeCzmuq2bK3wLchBcQkeC/FY4gvDUVE5
nz3I0n4Ze6Q14r6ZgcklDWEymO+OvHKaaLuheOkRTYx2+EVoTIWI/44zqZ15moQB
DKSdTENQNRSTxp1pRElTpCYxd28Ssv0S0fQpeX1vOP1fQZ363AUVr8FnKnMb3CHY
5ua45Chal3MzoiEIFz3AIo6o5AwMqs+vTTTzAM7Y5qEfurEOPWw08Pgv6IoxKIFv
5P7BEbwlOha8kJpncAnoLmhucZoPH774a4XHdVdT1678CWd0f+JCDGOFfVtaXkKV
aUBHuw5vojEiPXZ7VGysiApZ0EM1FJ5IuZY03kjJ60q4Rj3I+436cdOk7P1S1BiQ
R0KrZmUpLChCwW42LVaIzh0//WlagXJ/2I12bKI1qzTkixSYkOV3t+OewfLmBBM/
nmLoDdKfrmkWaEkURL81911YhDgh2fwOn5cLwedq0XNzVGqnJW/knSjesfllt1Lv
79uUfXv6Yx3fXmG4Q6Pva++G4MXoccjEwndr83XrG7rTZlnF1qUrQGYjZduLiT8M
q7wCPGLXADYuDhV4ewN/SL1vfSR2oohcpbJ1f+a4eSXDbeq0jcN8YbT7+geY0tKc
iXTuTVuPZSI=

-----END CERTIFICATE-----

Actual installation in Mozilla Firefox browser:

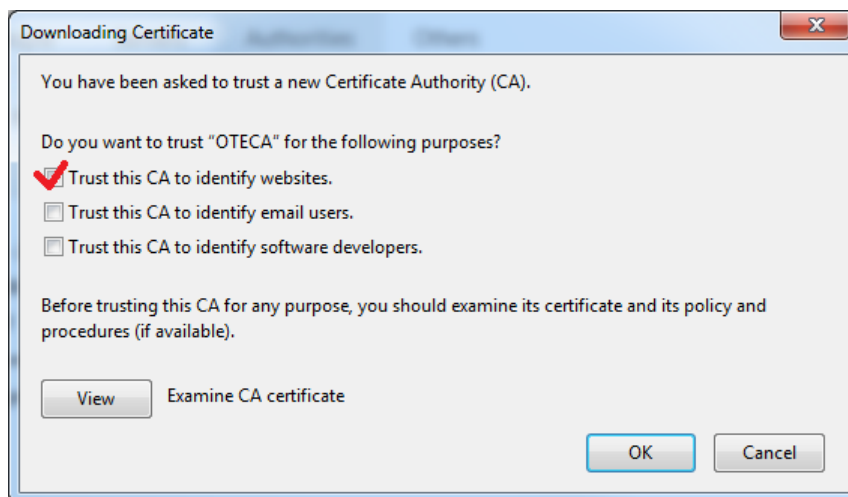
Menu -> Options -> Privacy & Security -> Certificates – View certificates...

Choosing the tab *Authorities* and pressing **Import**



In displayed window “Open file” select the file OTECA.pem.

Next step is to choose what type of identification is this Authority valid for:

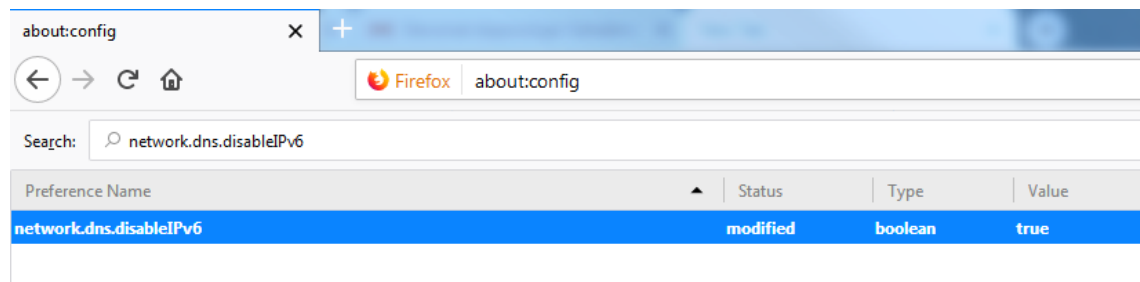


- Marking the first checkbox – **Trust this CA to identify websites**, and pressing OK will finish the import.

2.2.2 Disabling IPV6 DNS in Mozilla Firefox browser

In some specific configuration e.g. company network using WPAD, PKI component could not work more. Even after the above stated import of authority it is not possible to detect PKI component. Then, you need to change the browser's system settings by disabling searches of IPv6 in DNS.

The procedure is only recommended for experienced users because you need to change the settings in the Firefox system editor:

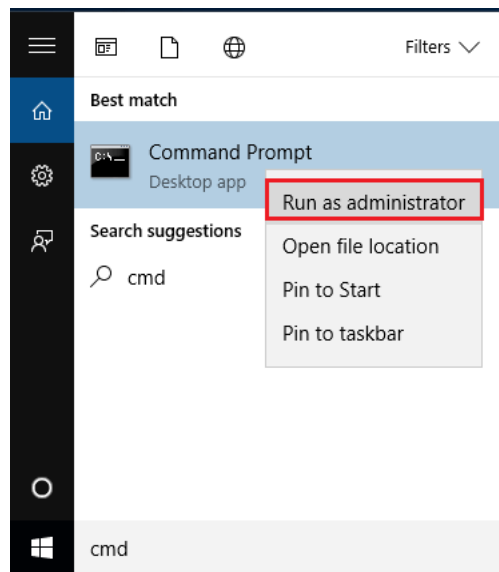


- 1) In address bar of the browser, type *about: config* and press *Enter*.
- 2) Accept an entry warning only for experienced users
- 3) Find "*network.dns.disableIPv6*" and double-click this item to change the value from *false* to *true*.
- 4) The bookmark can be closed, the settings are saved.

2.2.3 Configuring web browser Microsoft Edge

In the case of problems with detection of installed OTE PKi Klient in the browser Microsoft Edge (*forbidden communication web applications and local programs*), run the Command line as administrator:

- Windows MENU – *Search programs and file* type in CMD
- Consequently pressing right button of the mouse on cmd.exe and choosing *Run as administrator* will open window with command line. Type in following text:



- Choose Run as administrator, type admin Login and Password
- into new CMD window type this structure:

```
CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"
```

- pressing enter will execute modifications and the browser is now ready to use

2.2.4 Configuration of CS OTE portal

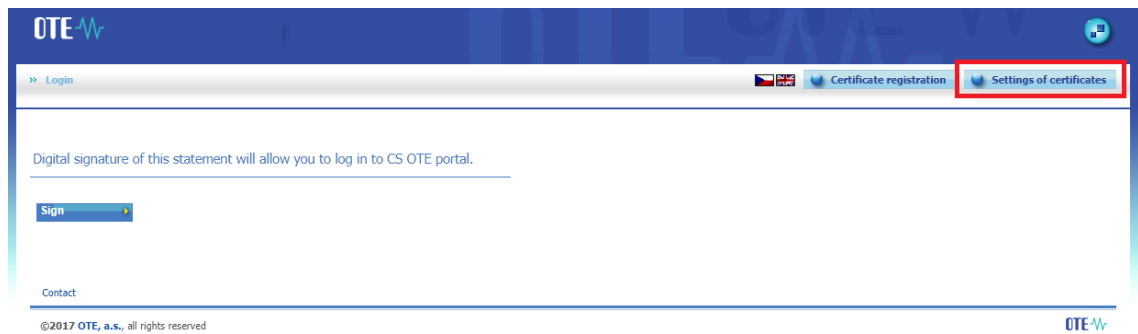
Communication CS OTE portal with OTE PKi Client is done through Local Storage. If it is forbidden to save *Browsing history*, it is necessary to perform the steps below every time launching the browser.

If the case the Local Storage was initialized for usage with certificates PKCS#12 (software cer.) , it is necessary to deconfigure it first.

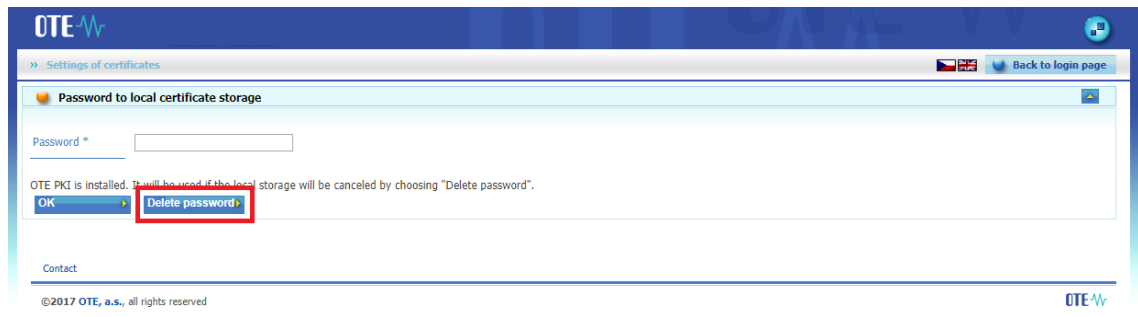
All the settings stated below must be performed for every web-browser and/or every user profile in operating system.

2.2.5 Deleting already initialized Local Storage for SW certificates

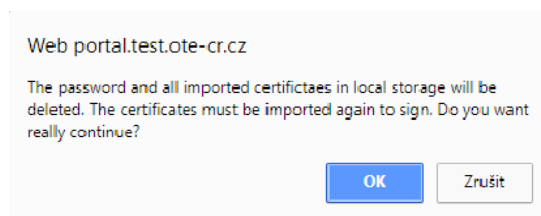
- login page to CS OTE - press the button *Settings of certificates*



- page Settings of certificates – press the button *Delete password*

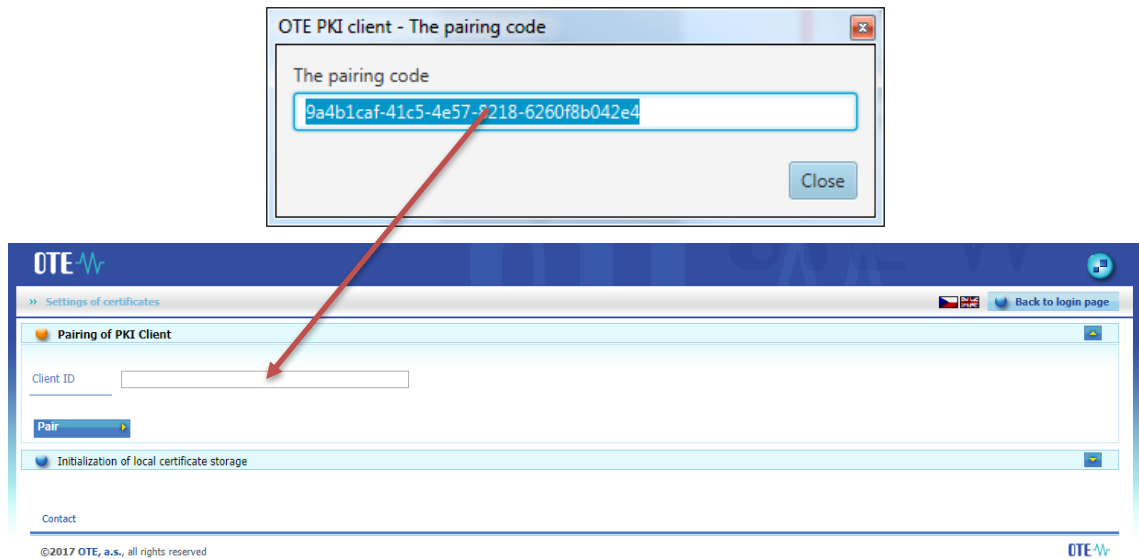


- in continuity to finish installation confirm the dialog box informing about deleting the Local Storage



2.2.6 Pairing web application and the component

After entering *Settings of certificates*, if the Local Storage is not used, automatically appears **Pairing dialog** (OTE PKI Client). In the web browser is shown section **Pairing PKi Client**, where the pairing code should be copied to.



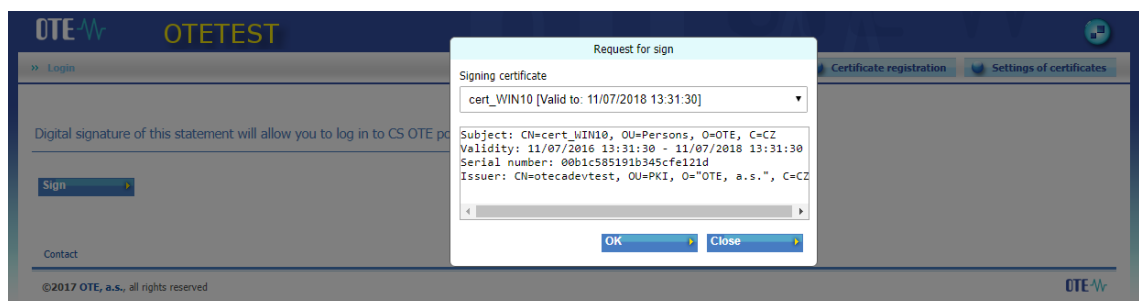
Inserting pairing code and pressing **Pair** will open web page with overview of all certificates in the Storage of operation system.

Activation process of OTE PKi Client is done.

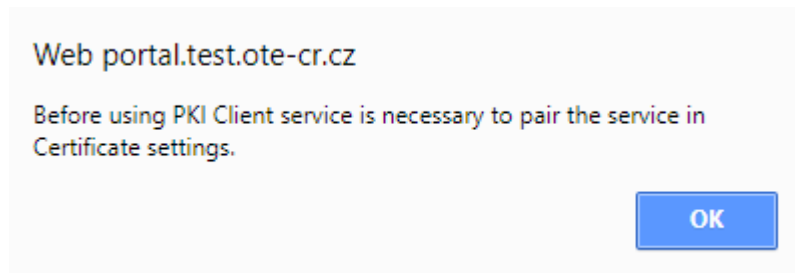
In the case of not viewing **Pairing dialog** automatically, it is possible to open it manually: in Taskbar do right click (of the mouse) on the icon OTE PKI Client and choose **Open pairing dialog**.



Pressing **Back to login page** and **Sign** enable to access CS OTE Portal.

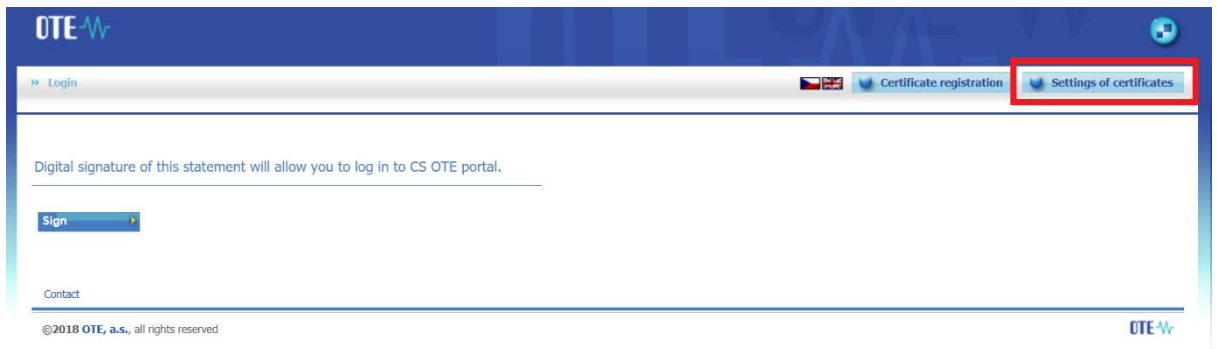


Local Storage is not used and OTE PKi Client is already installed. Before you pair web-browser with OTE PKi Client pressing **Sign** will evoke viewing window:

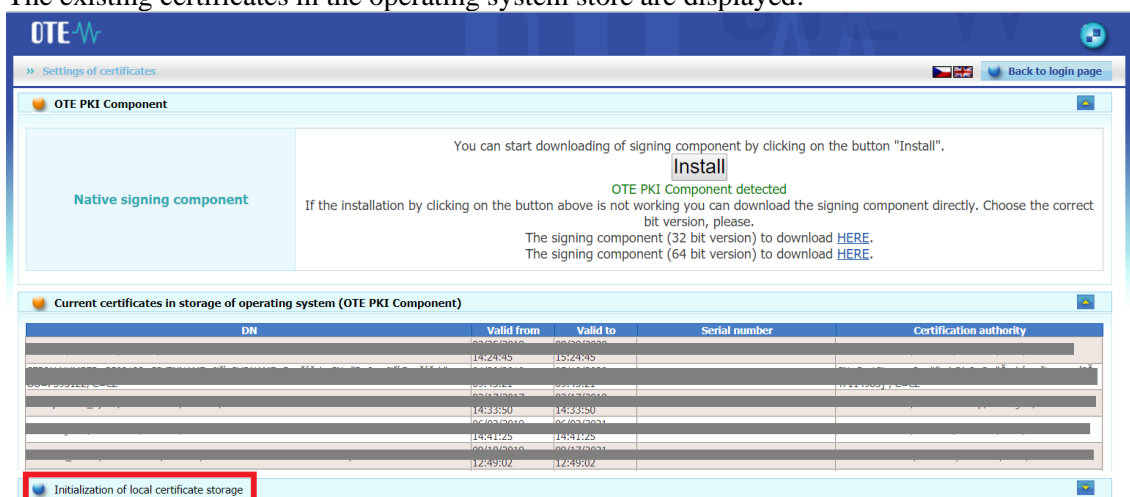


2.2.7 Switchover from OTE PKi component to local certificate storage

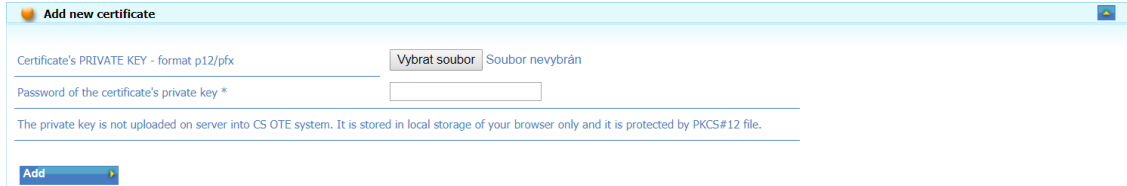
a) On the CS OTE portal login page, select the *Settings of certificates* button:



The existing certificates in the operating system store are displayed:



At the bottom is the **Initialization of local certificate storage** bar. Clicking this bar, entering and repeating the password will activate Local certificate storage. On the next page we are asked to add a certificate to the certificate storage.



Add new certificate

Certificate's PRIVATE KEY - format p12/pfx Soubor nevybrán

Password of the certificate's private key *

The private key is not uploaded on server into CS OTE system. It is stored in local storage of your browser only and it is protected by PKCS#12 file.

3 Settings of local certificates storage

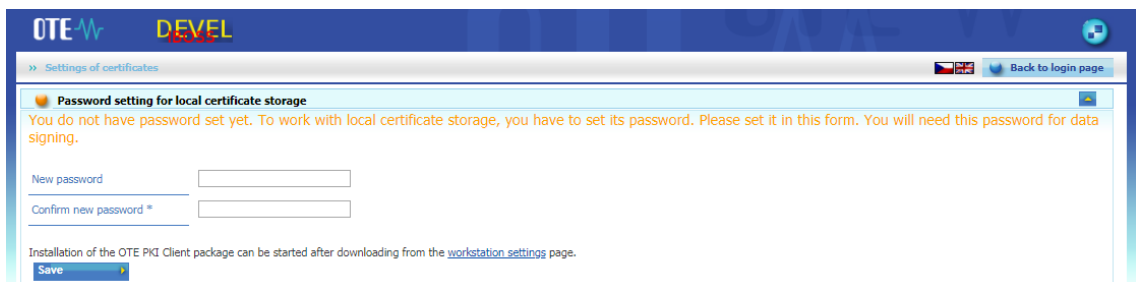
Local certificates storage preserves certificates for data signing. Storage is primarily for users who use modern web browser (Google Chrome, Microsoft Edge) for data signing.

3.1.1 Management of local certificates storage

Press „Registration” item in menu, then „Certification management”, „Settings of local certifications storage”.

Registration	
Master data	
Certificate management	List of all certificates
Mobile access	Certificate activation
Administration	Settings of local certificates storage
OTE News	

If you are log in for the first time, enter your password which you want to use for local certificate storage access. Press „Save” button, then you will be redirected to local certificates storage.



OTE DEVEL

Settings of certificates

Back to login page

Password setting for local certificate storage

You do not have password set yet. To work with local certificate storage, you have to set its password. Please set it in this form. You will need this password for data signing.

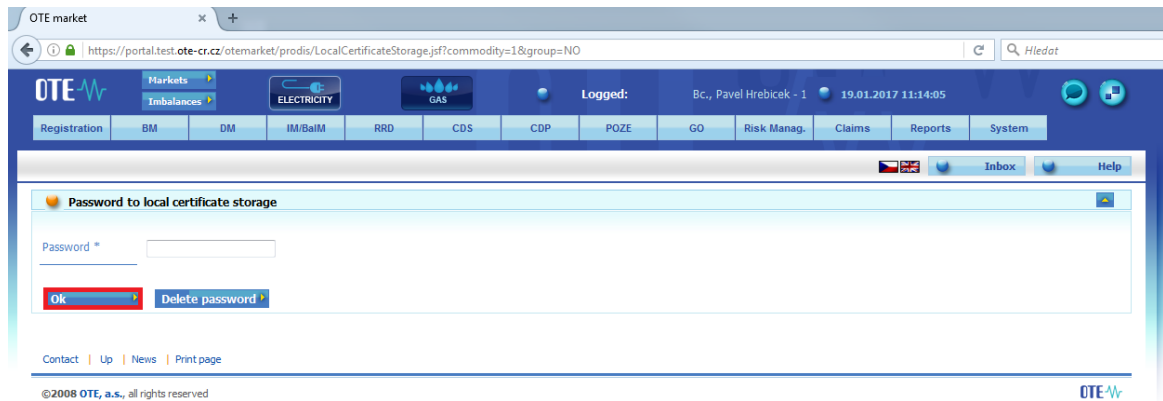
New password

Confirm new password *

Installation of the OTE PKI Client package can be started after downloading from the [workstation settings](#) page.

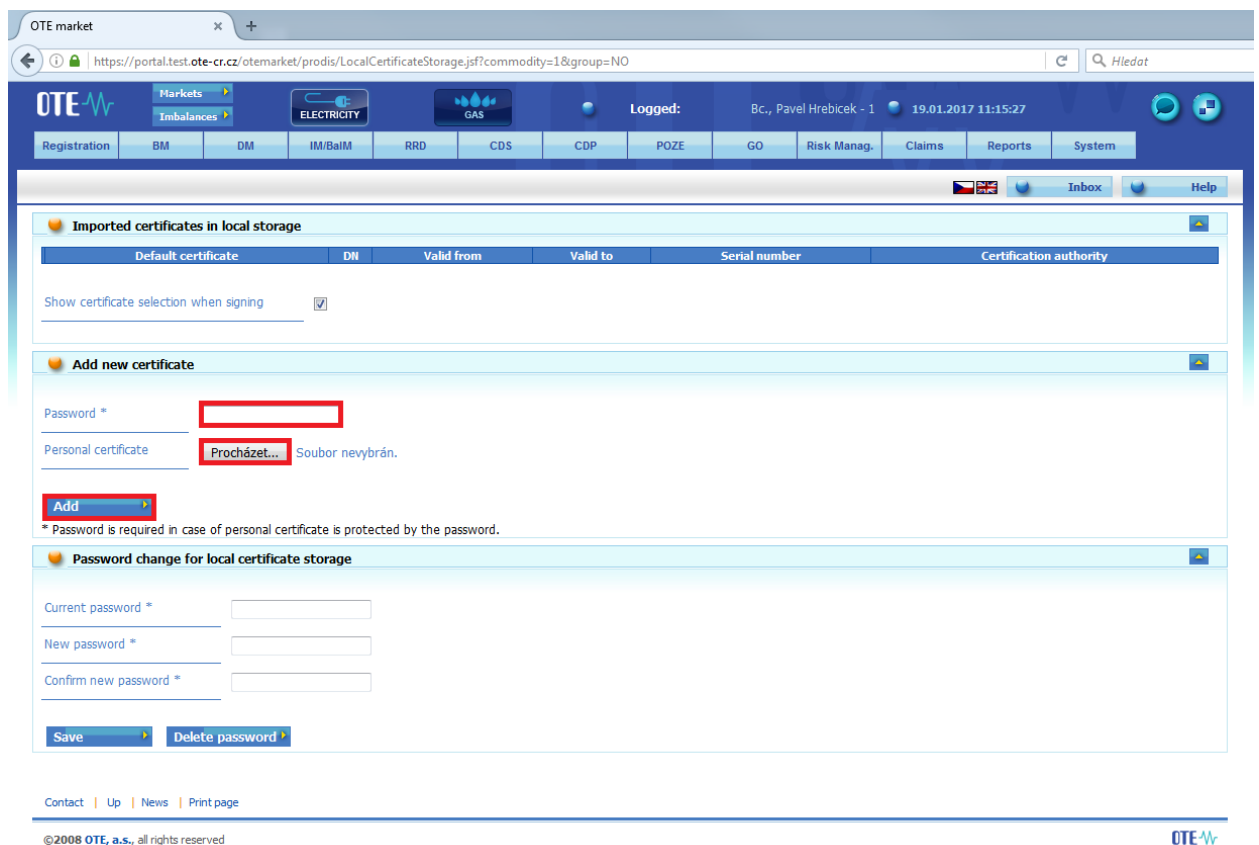
Save

If you already have your password to the local certificates storage, just enter the password. Press „Ok” button, then you will be redirected to local certificates storage.



3.1.2 Insert certificate to local certificates storage

Press „Procházet” button and choose certificate which you want to import to local certificates storage. Then enter password which is provided with a certificate and press „Add” button.



If an import was successful, you should see your certificate in „Imported certificates in local storage” section.

The screenshot shows the OTE market web application interface. The main content area is titled "Imported certificates in local storage". It contains a table with the following data:

	Default certificate	DN	Valid from	Valid to	Serial number	Certification authority
Remove	<input checked="" type="radio"/>	C=CZ, O=OTE, OU=Persons, CN=otecert_SW	11/22/2016 12:17:53	11/22/2018 12:17:53	174ef2c01d4019ebdf7d	C=CZ, O=OTE, a.s., OU=PKI, CN=otecadevtest

Below the table, there is a checkbox labeled "Show certificate selection when signing" which is checked. Below that is the "Add new certificate" section, which includes a password field, a "Personal certificate" field with a "Procházet..." button, and a message: "Certificate successfully loaded". A note below states: "* Password is required in case of personal certificate is protected by the password." Below this is the "Password change for local certificate storage" section, which has three password input fields: "Current password", "New password", and "Confirm new password". At the bottom of this section are "Save" and "Delete password" buttons.

3.1.3 Remove certificate from local certificates storage

Press „Remove” button in „Imported certificates in local storage” section.

OTE market

Markets
Imbalances

ELECTRICITY GAS

Logged: Bc., Pavel Hrebíček - 1 19.01.2017 11:17:39

Registration BM DM IM/BalM RRD CDS CDP POZE GO Risk Manag. Claims Reports System

Inbox Help

Imported certificates in local storage

	Default certificate	DN	Valid from	Valid to	Serial number	Certification authority
Remove	<input checked="" type="radio"/>	C=CZ, O=OTE, OU=Persons, CN=otecert_SW	11/22/2016 12:17:53	11/22/2018 12:17:53	174ef2c01d4019ebdf7d	C=CZ, O=OTE, a.s., OU=PKI, CN=otecadevtest

Show certificate selection when signing

Add new certificate

Password *

Personal certificate otecert_SW.p12

Add

* Password is required in case of personal certificate is protected by the password.

Password change for local certificate storage

Current password *

New password *

Confirm new password *

Save **Delete password**

Contact | Up | News | Print page

©2008 OTE, a.s., all rights reserved

Press „OK” button

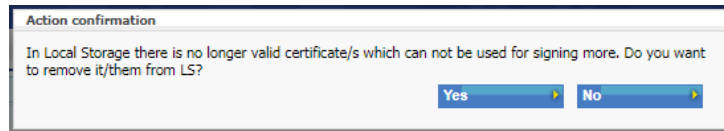
Do you really want to delete the certificate from local storage?



If deleting certificate was successful, you shouldn't see your certificate in „Imported certificates in local storage” section.

3.1.4 Removing expired certificates from local storage

Clicking on login page to CS OTE cause running detection of expired certificates. In the case your Local Storage contain some expired certificate the system will announce it by displaying the window:



Clicking “Yes” we might remove expired from local storage directly. Choosing “No” will not perform any action.

After that content of local storage is normally displayed.

3.1.5 Choose primary certificate

If you have more than one certificate in your local certificates storage, you should choose your primary certificate. This certificate will be used for data signing, when you uncheck „Show certificate selection when signing” option.

	Default certificate	DNI	Valid from	Valid to	Serial number	Certification authority
Remove	<input checked="" type="radio"/>	C=CZ, O=OTE, OU=Persons, CN=OTE	10/14/2016 11:08:36	10/14/2018 11:08:36	00bcc95159680f75196890	C=CZ, O=OTE, a.s., OU=PKI, CN=otecadevtest
Remove	<input type="radio"/>	C=CZ, O=OTE, OU=Persons, CN=otecer_SW	11/22/2016 12:17:53	11/22/2018 12:17:53	174ef2c01d4019ebdf7d	C=CZ, O=OTE, a.s., OU=PKI, CN=otecadevtest

Show certificate selection when signing

Add new certificate

Password *

Personal certificate [Procházet...](#) OTE.p12

[Add](#)

* Password is required in case of personal certificate is protected by the password.

Password change for local certificate storage

Current password *

New password *

Confirm new password *

[Save](#) [Delete password](#)

3.1.6 Change password for local certificates storage access

Enter your current password in „Password change for local certificate storage section. Then enter your new password and confirm this password. Press „Save” button. If change password was successful, you should see Password successfully changed.

The screenshot shows the 'Imported certificates in local storage' section of the OTE market application. It features a table with one certificate entry and a 'Password change for local certificate storage' form below it.

Remove	Default certificate	DN	Valid from	Valid to	Serial number	Certification authority
	<input checked="" type="radio"/>	C=CZ, O=OTE, OU=Persons, CN=OTE	10/14/2016 11:08:36	10/14/2018 11:08:36	00bcc95159680f75198890	C=CZ, O=OTE, a.s., OU=PKI, CN=otecadevtest

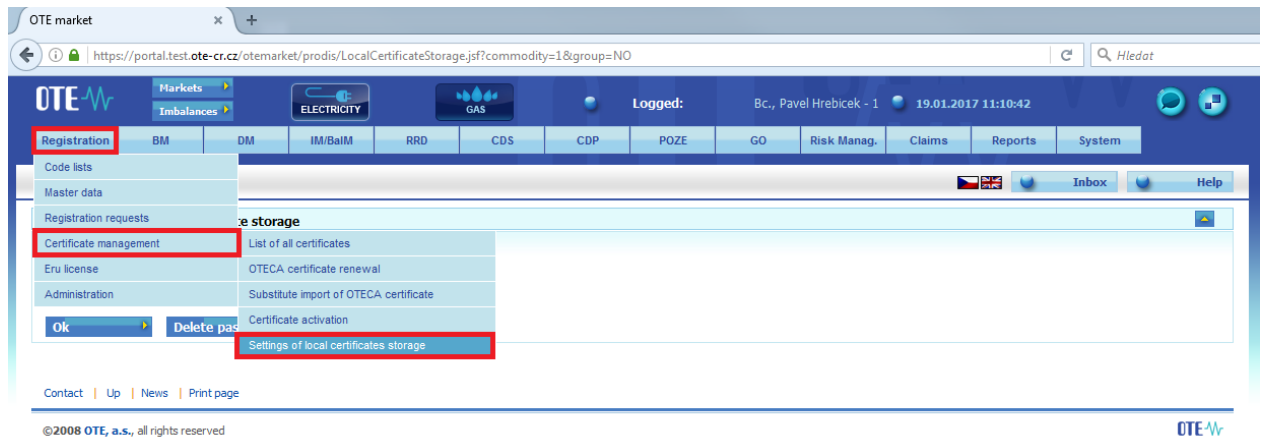
Below the table, there is a checkbox for 'Show certificate selection when signing' which is checked.

The 'Add new certificate' section includes a 'Password *' field, a 'Personal certificate' section with a 'Procházet...' button and the text 'Soubor nevybrán.', and an 'Add' button.

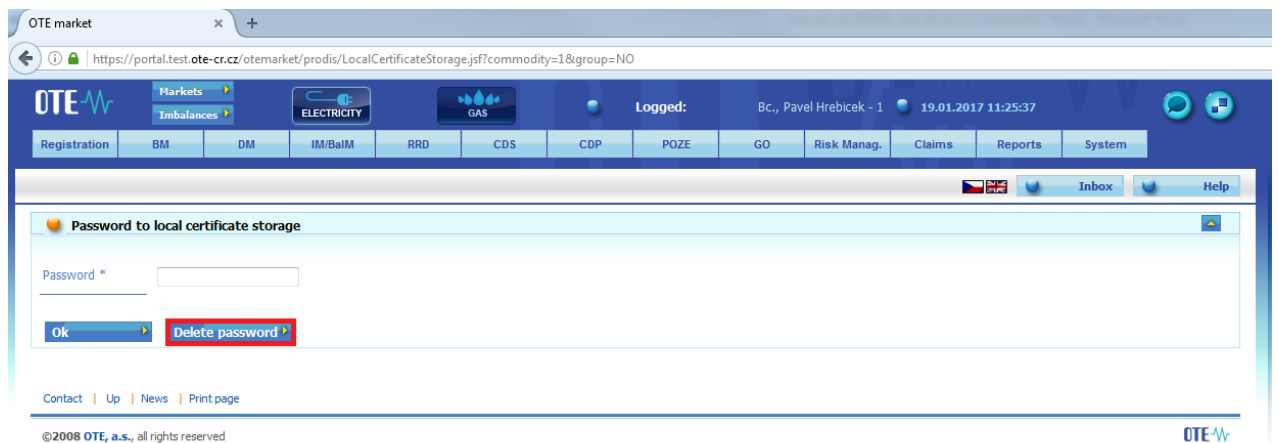
The 'Password change for local certificate storage' section contains three password fields: 'Current password *', 'New password *', and 'Confirm new password *'. Below these fields are 'Save' and 'Delete password' buttons.

3.1.7 Forgotten password for local certificates storage access

Press „Registration” item in menu, then „Certification management”, „Settings of local certifications storage”.

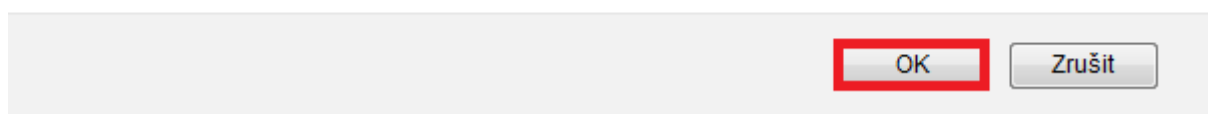


Press „Delete password” button. **All your certificates will be deleted from local certificates storage, if you are deleting your password!**



Press „OK” button.

When you delete the password also all stored certificates will be deleted. Do you really want to delete it?



Then you will be redirected to screen, where you enter your new password for local certificates storage access. Press „Save” button and then you will be redirected to local certificates storage.

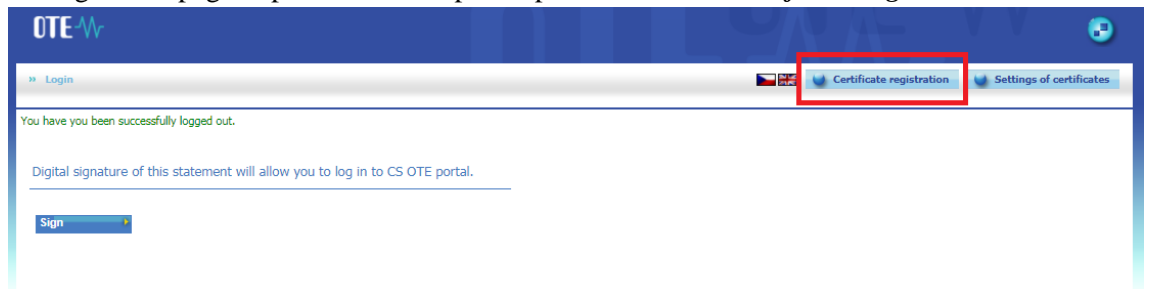
4 Re-registering the Certificate after validity expires

Accessing CS OTE portal after validity end-date of Certificate with company ID

- 1) New certificate with the same company ID, as expired one, upload into *Local Machine Store*, respectively into *) *Certificate Manager* of used web-browser.

*) web. browser: *MENU – Settings – Certificates – Manage certificates – Personal cert. – upload new certificate*

- 2) On login web-page to portal CS OTE please press the button *Certificate registration*:



- pressing **Sign** on the next page will continue in re-registration process
- dialog box „**Request for sign**“ is shown. All sign certificates registered in Local Machine Store are visible there. Choosing the new one and pressing **OK** will result in new web page with information about User and Certificate.
- If all viewed information is correct, we can finish re-registration process by pressing **Register**

Viewing notice on the next page - ***The certificate was successfully registered.*** informs about ending the process correctly.

Now it is possible to use this certificate as usual.

5 Instruction for the first access to the production environment of OTE-COM application

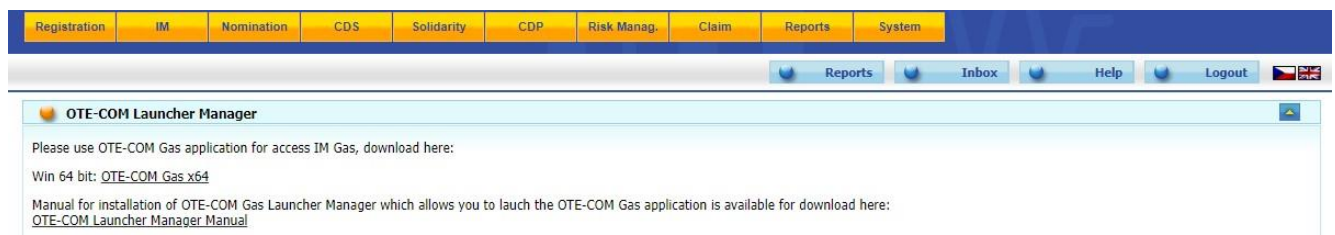
Access to the OTE-COM production environment is possible by following two ways:

1. Application OTE- COM (Fat client)
2. Direct access to AMQP server from market participant's server (Automatic communication)

5.1 Application OTE-COM Launcher Manager

First, it is necessary to download and install the production version of OTE-COM Launcher Manager (LM) for Electricity (A) or for Gas (B) which allows run of the production version of OTE-COM application.

- OTE-COM Gas x64 can be downloaded in IM section under the tab OTE-COM Launcher Manager



- OTE-COM Electricity x64 can be downloaded in IM section under the tab OTE-COM Launcher Manager



- Manual for installation of OTE Launcher Manager can be downloaded [here](#).
- Communication of the application goes through http/https protocol which in normal cases does not cause any trouble. However, complications may occur if market participants use the proxy server. In this case it is necessary in the OTE-COM Launcher Manager settings (clicking the button O) set the HTTP proxy and allow access to <http://www.ote-cr.cz> and <https://portal.ote-cr.cz>, respectively contact your IT department and ask them about settings.

- Please note that it may be needed to allow direct access to URL amqp.ote-cr.cz (IP 91.209.101.43), port 5671 in the infrastructure of the market participant.
- Each participant, who is accessing CS OTE Portal with the personal certificate, has the access to applications OTE-COM (through LM) with same certificate. In terms of personal certificates, there is no need to change anything on the market participants' side.
- Information about installation of the root certificates, that has to be installed to access the OTE- COM application, can be found in the manual of OTE Launcher Manager.

5.2 Access to AMQP server from market participant's server (Automatic communication)

- Communication for OTE-COM LM:
 - Electricity (A) goes through URL amqp.ote-cr.cz (91.209.101.43), port 5671, virtualhost = market.
 - GAS (B) goes through URL amqp.ote-cr.cz (91.209.101.43), port 5671, virtualhost = marketGAS
- Supported TLS interface: version 1.2.
- For this type of communication is necessary for market participants to implement appropriate interface according the [specification](#). Templates for OTE-COM messages are available [here](#). In this case it is not used functionality of the proxy.
- For this communication is used AMQP protocol, which does not support HTTP / SOCKS proxy configuration on the market participant side. In this case it is necessary to ask IT department.
- Each participant, who is accessing CS OTE Portal with the personal certificate, has the access to AMQP server (through Automatic communication) with same certificate. In terms of personal certificates, there is no need to change anything on the market participants' side.
- Information about installation of the root certificates, that has to be installed to access the OTE- COM application, can be found in the manual of OTE Launcher Manager.