User Manual
of Information System

Client station configuration

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12.1.2011	Removal of outdated information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8.3.2018	Removal of outdated information obout OTECA, OTECATEST certificates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

Contents

1 Workstation configuration

Supported configuration for workstation operating with CS OTE is following:

Windows 7 (32bit) + MS IE11.0/FireFox(32bit)+ Outlook 2016 /x86

Windows 7 (64bit) + MS IE11.0(32bit)/FireFox(32bit) + Outlook 2016/ x64

Windows 10 (32bit) + MS IE11.0/Edge/FireFox/Chrome-last version + Outlook 2016/ x86

Windows 10 (64bit) + MS IE11.0/Edge/FireFox/Chrome- last version + Outlook 2016/ x64

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

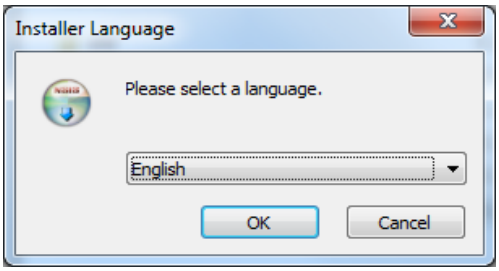
2 Browsers Google Chrome, Mozilla Firefox and Microsoft Edge

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

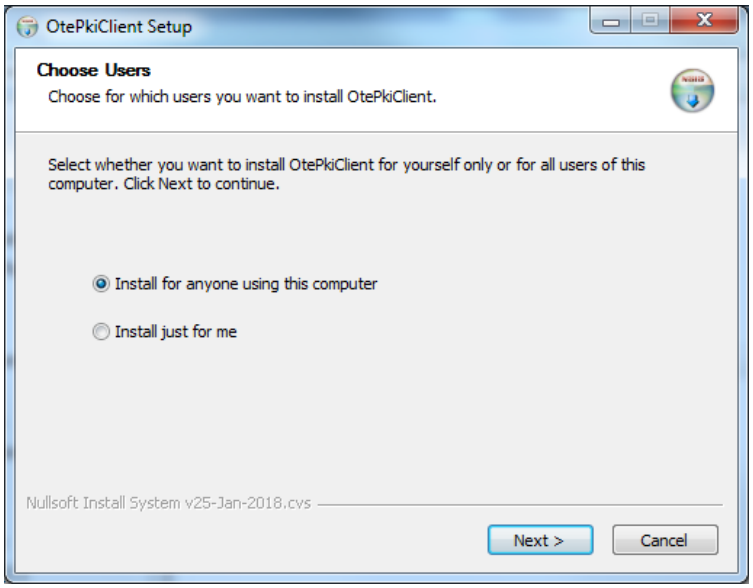
Link for downloading installation file is located on web page: http://www.ote-cr.cz/registration-and-agreements/access-to-cs-ote/konfigurace-pc?set_language=en in the table **A – Access to CS OTE through a web browser** (links for installation packages for IE and for other supported browsers 32-bit,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

To start installation open the downloaded file:

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

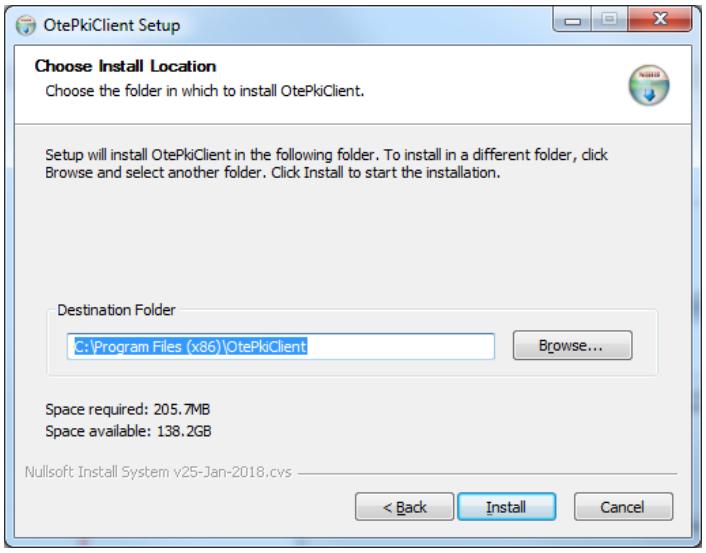


2) In next step, according to used browser, decide if to install OtePkiClient just for you or for anyone using this PC



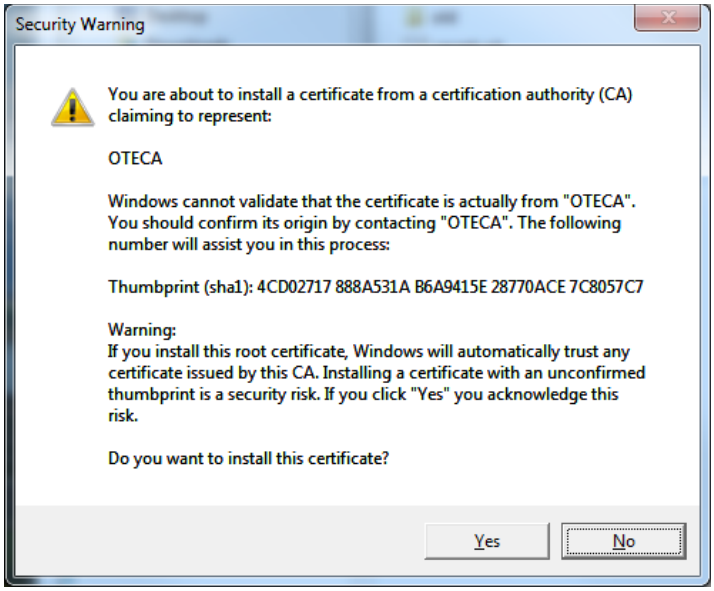
- Choosing “Install for anyone …” will locate installation into Program Files
- Choosing “Install just for me” will locate installation into User’s Folder

3) Now, it is possible to modify the location manually



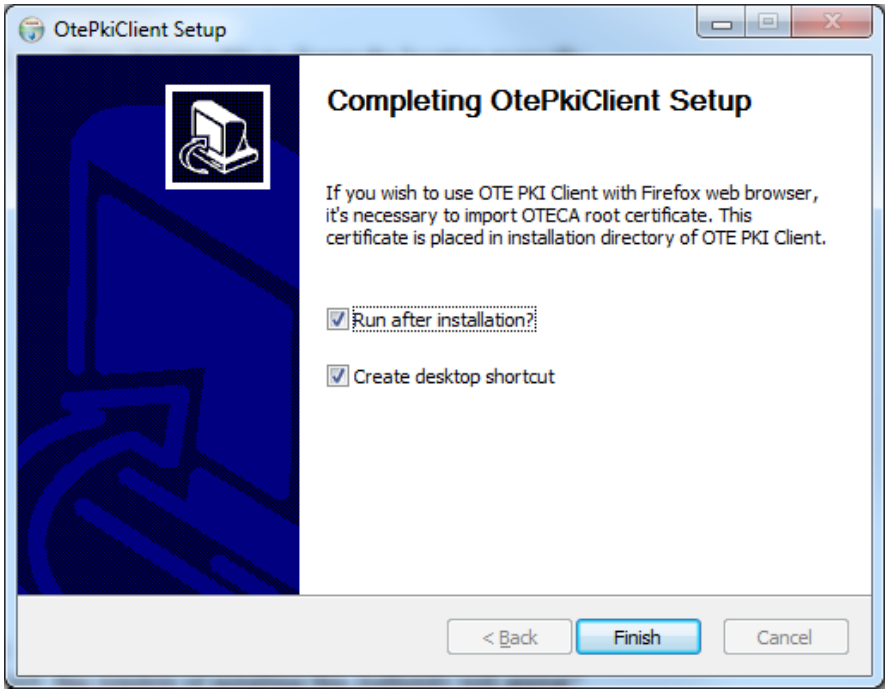
4) Is there OTECA Authority installed in Trusted Root Athorities on this PC ?

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



Pressing YES the instalation will continue. Installed Authority is valid for all supported web browsers except Mozilla Firefox. Process of installing for this browser is decribed in the chapterr 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.

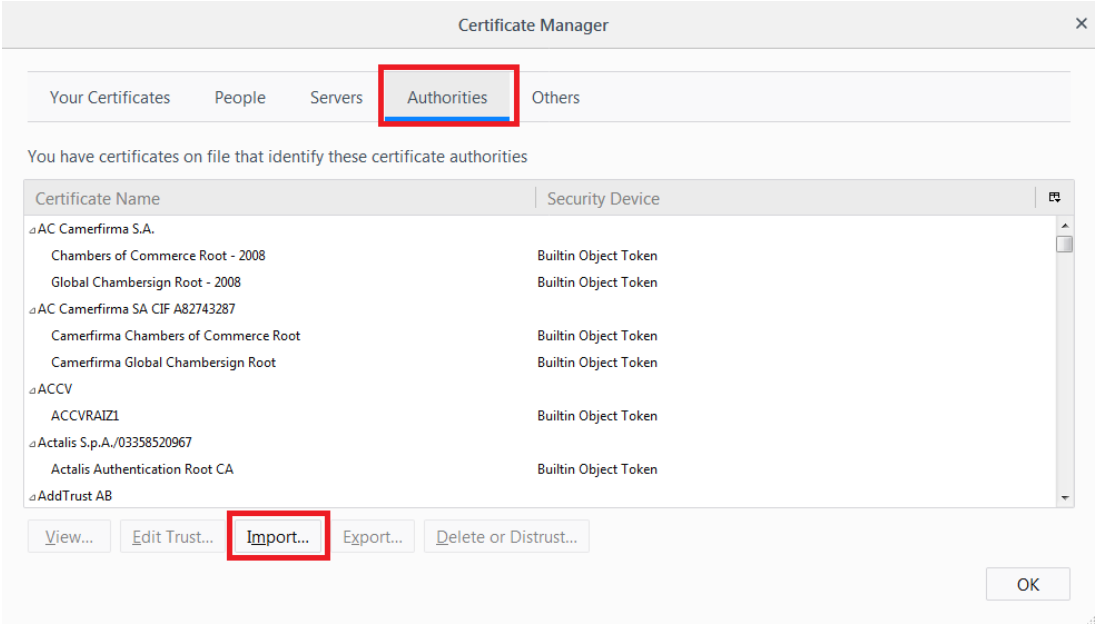
Save the text shown below into the file OTECA.pem:

```
-----BEGIN CERTIFICATE-----
MIIFpDCCA4ygAwIBAgIKAq9tFwPoO3XI5TANBgkqhkiG9w0BAQsFADA/MQswCQYD
VQQGEwJDWjESMBAGA1UECgwJT1RFLCBhLnMuMQwwCgYDVQQLDANQS0kxDjAMBgNV
BAMMBU9URUNBMB4XDTE4MDMwNTE3NDgwM1oXDTI4MDMwNTE3NDgwM1owPzELMAkG
A1UEBhMCQ1oxEjAQBgNVBAoMCU9URSwgYS5zLjEMMAoGA1UECwwDUEtJMQ4wDAYD
VQQDDAVPVEVDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBANrqtnuv
5zS9byhArdH2sTE+dAGSYT85RT71+ElkoCwpYbOsGsR3/7LzbQT0R7dn8iSDPR5a
hh0B8mdcWLYXOV0croBFs0WpGUiOSiwpKLFr+aXMtVNBfX5qF+GZWRj+G+NfhYgr
zARTN2Ws0MnQGZbXY0GuIWOwYItj9EA15qTE3IN/ereSzwkSwx3Fd2AigxL7V6Yw
pxU+rWe39MFH8prTPw6TI0xvPconZwObaIoHG54P4wRqEeuKnzaW4vZeinGvIXpn
5MamU2tQrMUGCMOEeycASPMEubSK8z6IyJ35ZQ31aeUk3lwrzp0CJZVFsZtThn8T
9e1ZiPHxD3LbW5bGT7hSVqe7qe1qwdomYItQrRLJZ17YMBEA8vfgZHwjcjaO7QfX
ljYdUirnujTDgHqcu6RXVkhPvVbdFNcRe1o34+8TzmDXQOVOTSzjEOdGcB++Rvcp
+pxbbQUFM4ja3BH3Y9hV2GWSPtET/FhY028gG2KkFpXAz7HzpnLjm27dvSH4RU3S
AYKm+cd/btgDI2fGzaKtVt50+trB2Wjl+GipsRkw2VmOdBDO++T28NcrOu7HNVBF
xNzpvHchoVOonWLbghxzqVDux+BWEriOIJYSebBbQdn0Vic5xB0+kcGMHMfnJ6Dz
7sOhlZgH3h3rYg7G88JxGVGbxFGZHMTYyamhAgMBAAGjgaEwgZ4wDwYDVR0TAQH/
BAUwAwEB/zALBgNVHQ8EBAMCAQYwHQYDVR0OBBYEFOpk3trCPeD1gOlUhNgqi73M
7xMVMB8GA1UdIwQYMBaAFOpk3trCPeD1gOlUhNgqi73M7xMVMB4GA1UdEQQXMBWB
E290ZWNhLmN6QGxvZ2ljYS5jb20wHgYDVR0SBBcwFYETb3RlY2EuY3pAbG9naWNh
LmNvbTANBgkqhkiG9w0BAQsFAAOCAgEAXL8eTcjeG0Yb341YzErb+KGm6S2gWAqk
eBbrVtVJ6uq4lUYVuQ2radrN26ZMSedTyeCzmuq2bK3wLchBcQkeC/FY4gvDUVE5
nz3I0n4Ze6Ql4r6ZgcklDWEymO+OvHKaaLuheOkRTYx2+EVoTIWI/44zqZl5moQB
DKSdTENQNRSTxp1pRElTpCYxd28Ssv0S0fQpeX1vOP1fQZ363AUVr8FnKnMb3CHY
5ua45Chal3MzoiEIFz3AIo6o5AwMqs+vTTTzAM7Y5qEfurEOPWw08Pgv6IoxKIFv
5P7BEbwlOha8kJpncAnoLmhucZoPH774a4XHdVdT1678CWd0f+JCDGOFFVtaXkKV
aUBHuw5vojEiPXZ7VGysiApZ0EM1FJ5IuZYo3kjJ60q4Rj3I+436cdOk7PlSlBiQ
R0KrZmUPlChCwW42LVaIzh0//WlagXJ/2Il2bKI1qzTkixSYkOV3t+OewfLmBBM/
nmLoDdKfrmkWaEkURL8l911YhDgh2fwOn5cLwedq0XNzVGqnJW/knSjesfllt1Lv
79uUfXv6Yx3fXmG4Q6PVa++G4MXoccjEwndr83XrG7rTZlnF1qUrQGYjZduLiT8M
q7wCPGLXADYuDhV4ewN/SLlvfSR2oohcpbJ1f+a4eSXDbeq0jcN8YbT7+geY0tKc
iXTuTVuPZSI=
-----END CERTIFICATE-----
```

Actual installation in Mozilla Firefox browser:

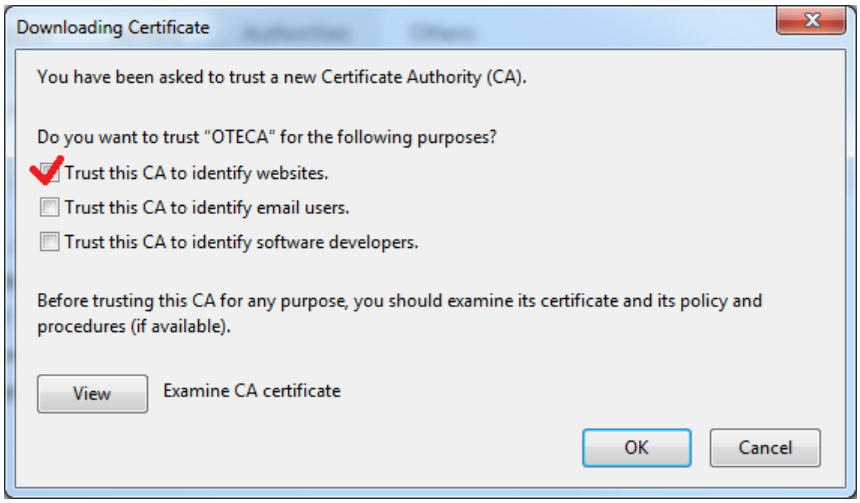
Menu -> Options -> Privacy & Security -> Certificates – View certificates…

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:

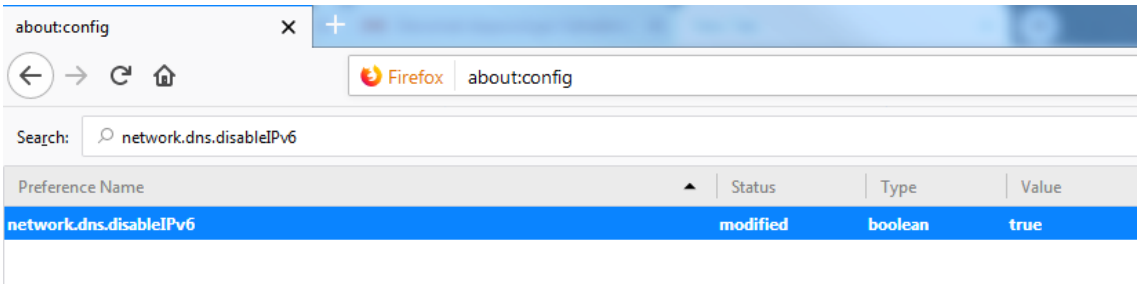


- Marking the first checkbox – ***Trust this CA to identify websites***, and pressing OK will finish the import.

2.2.2 Dissabling 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:

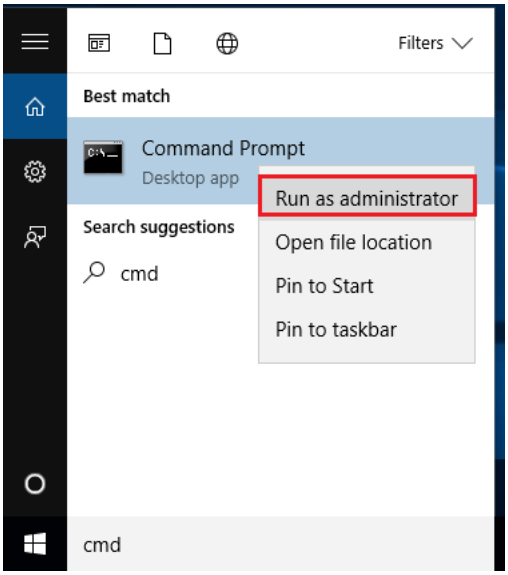


1) In address bar of the browser, type ***about: config*** and press ***Enter***.
2) Accept an entry warning only for experienced users
3) Find "***network.dns.disableIPv6***" and double-click this item to change the value from ***false*** to ***true***.
4) The bookmark can be closed, the settings are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

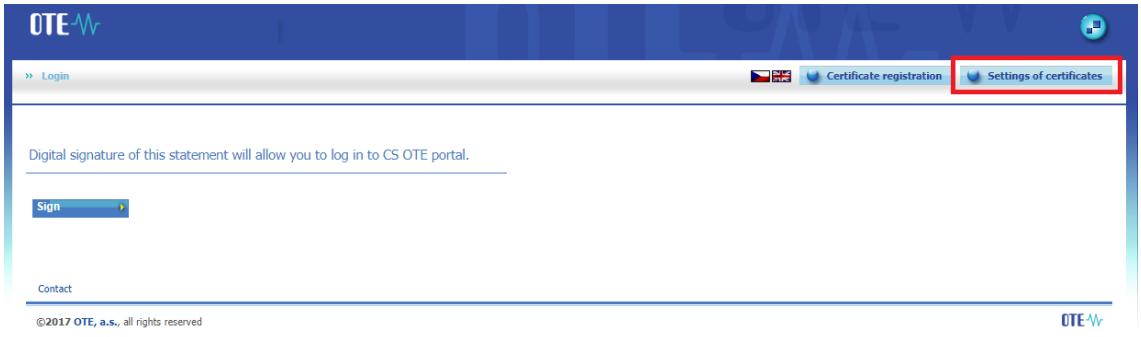
Communication CS OTE portal with OTE PKi Client is done through Local Storage.
If it is forbidden to save *Browsing history*, it is necessary to perform the steps below every time launching the browser.

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

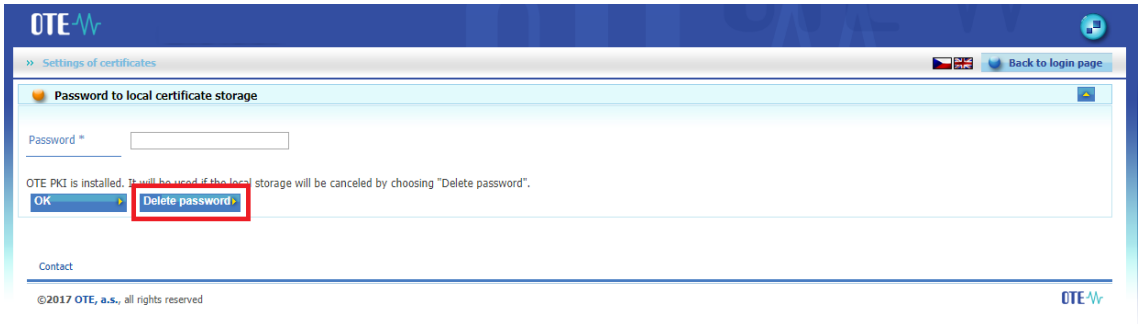
All the settings stated below must be performed for every web-browser and/or every user profile in operating system.

2.2.5 Deleting already initialized Local Storage for SW certificates

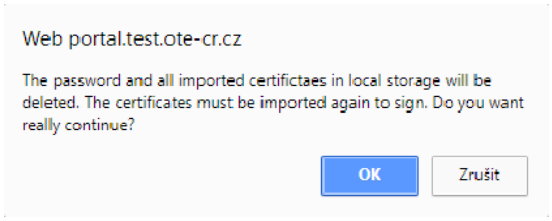
- login page to CS OTE - press the button ***Settings of certficates***



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

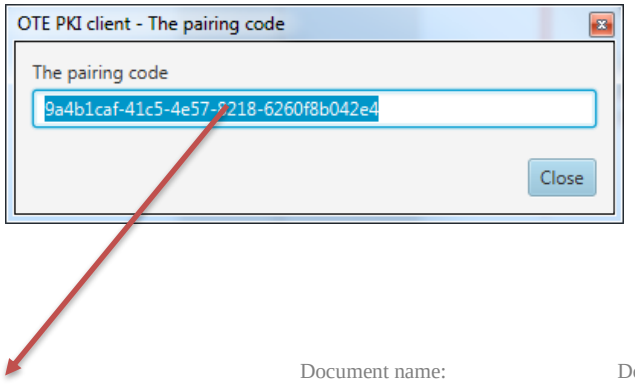


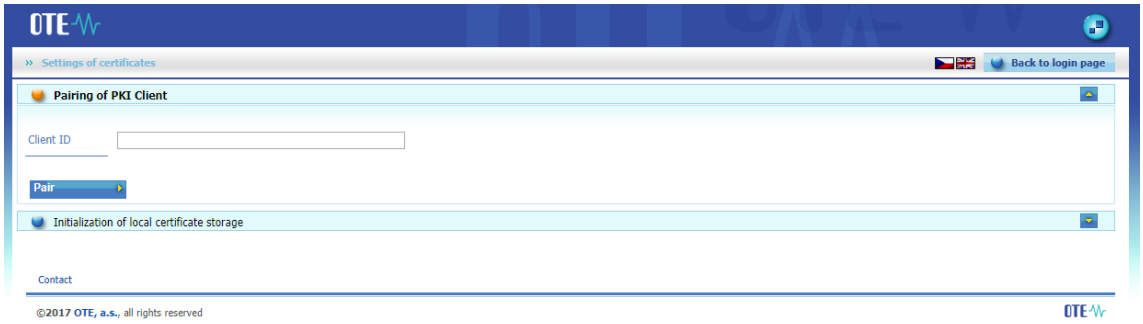
- in continuity to finish installation confirm the dialog box informing about deleting the Local Storage



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.



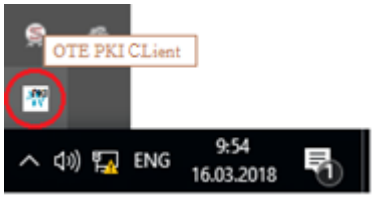


*Inserting pairing code and pressing **Pair** will open web page with overview of all certificates in the Storage of operation system.*

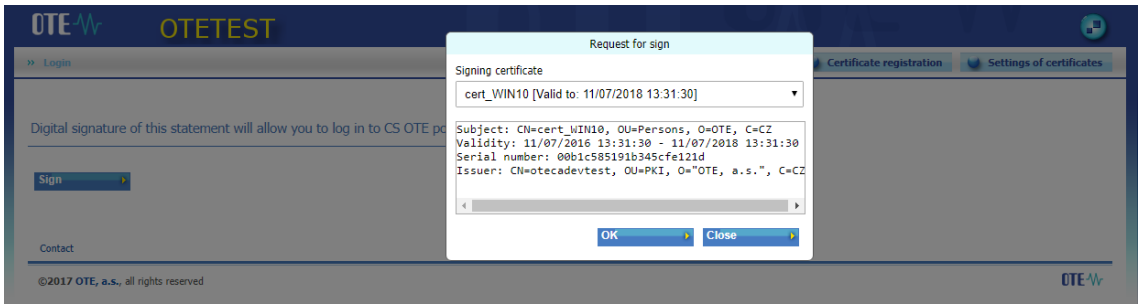
Activation process of OTE PKi Client is done.

---

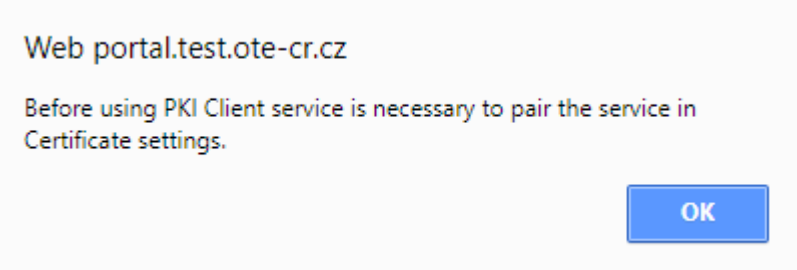
*In the case of not viewing **Pairing dialog** automatically, it is possible to open it manually: in Taskbar do right click (of the mouse) on the icon OTE PKI Client and choose **Open pairing dialog.***



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



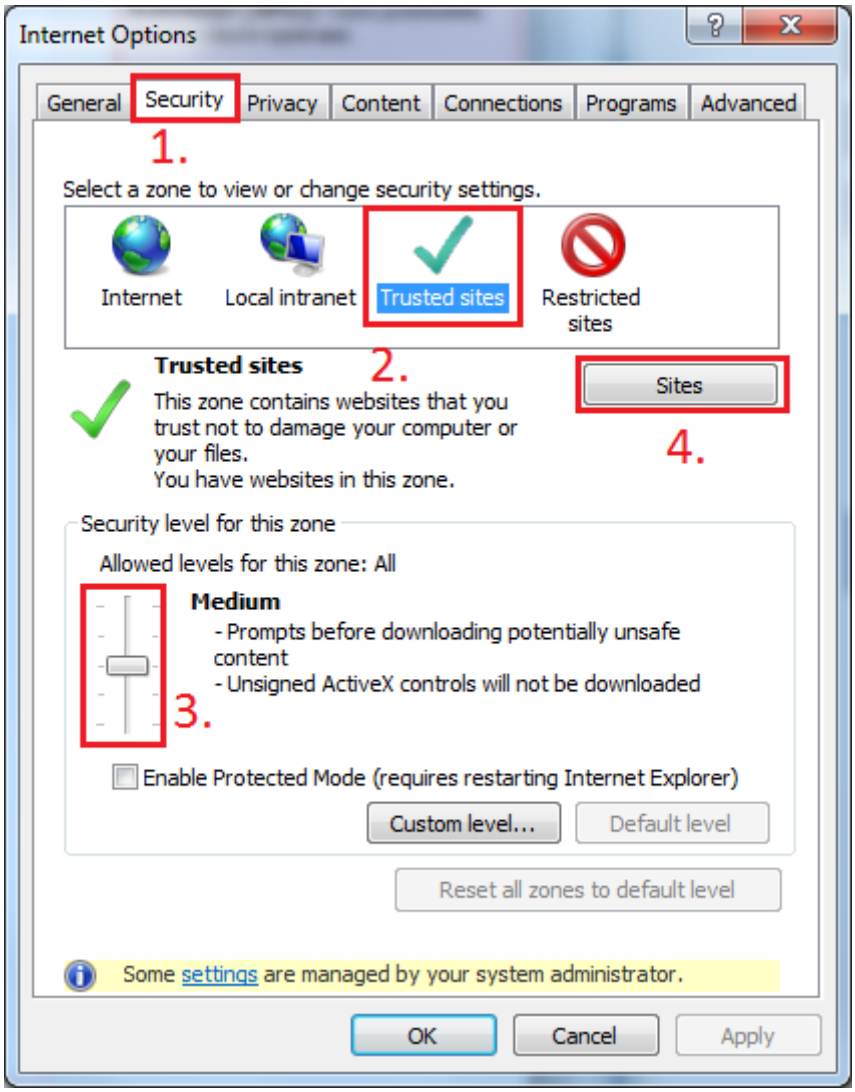
Local Storage is not used and OTE PKi Client is already installed. Before you pair web-browser with OTE PKi Client pressing **Sign** will evoke viewing window:

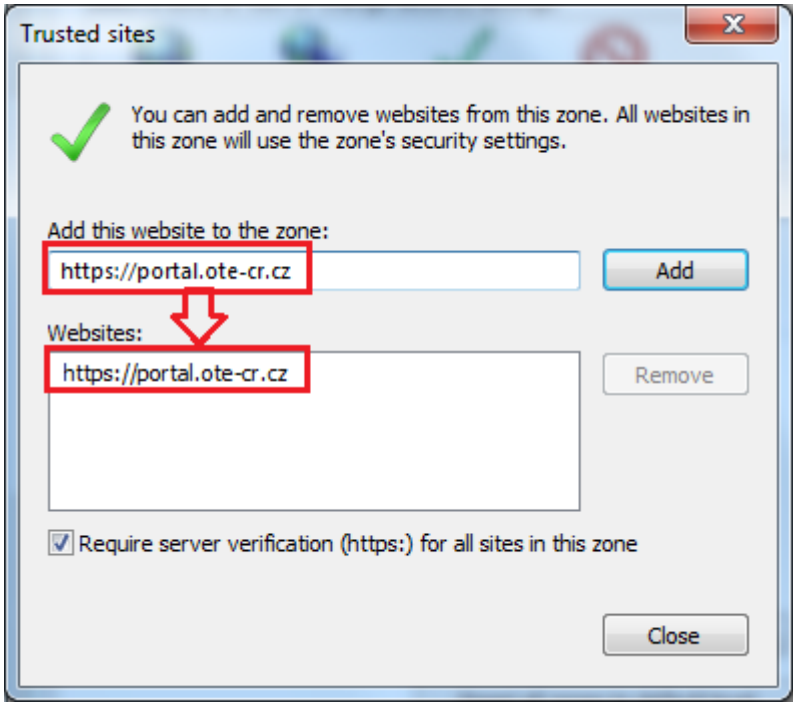

Web portal.test.ote-cr.cz
Before using PKI Client service is necessary to pair the service in Certificate settings.
OK

3 Internet Explorer browser settings

3.1.1 Set up of Trusted sites

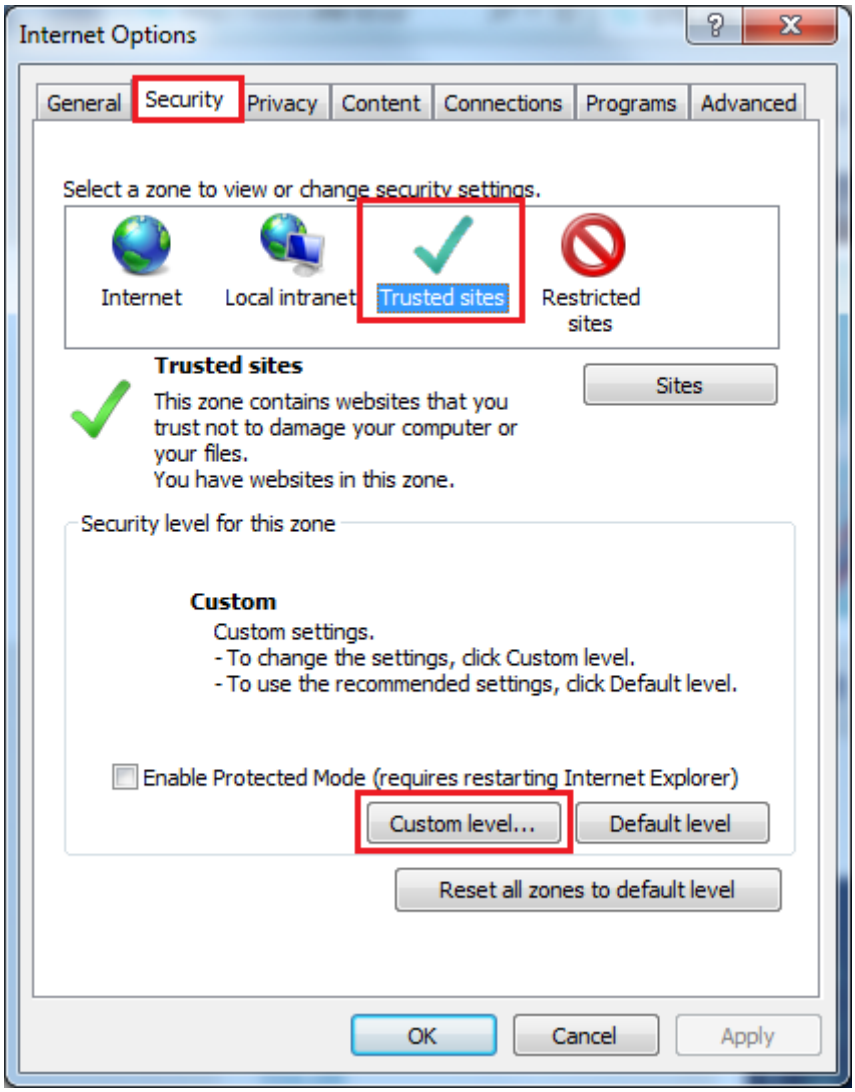
Internet browser settings should be standard but some functions may require adding the site **https://portal.ote-cr.cz/otemarket** into „Trusted sites“ (Tools/Options; see pictures below).

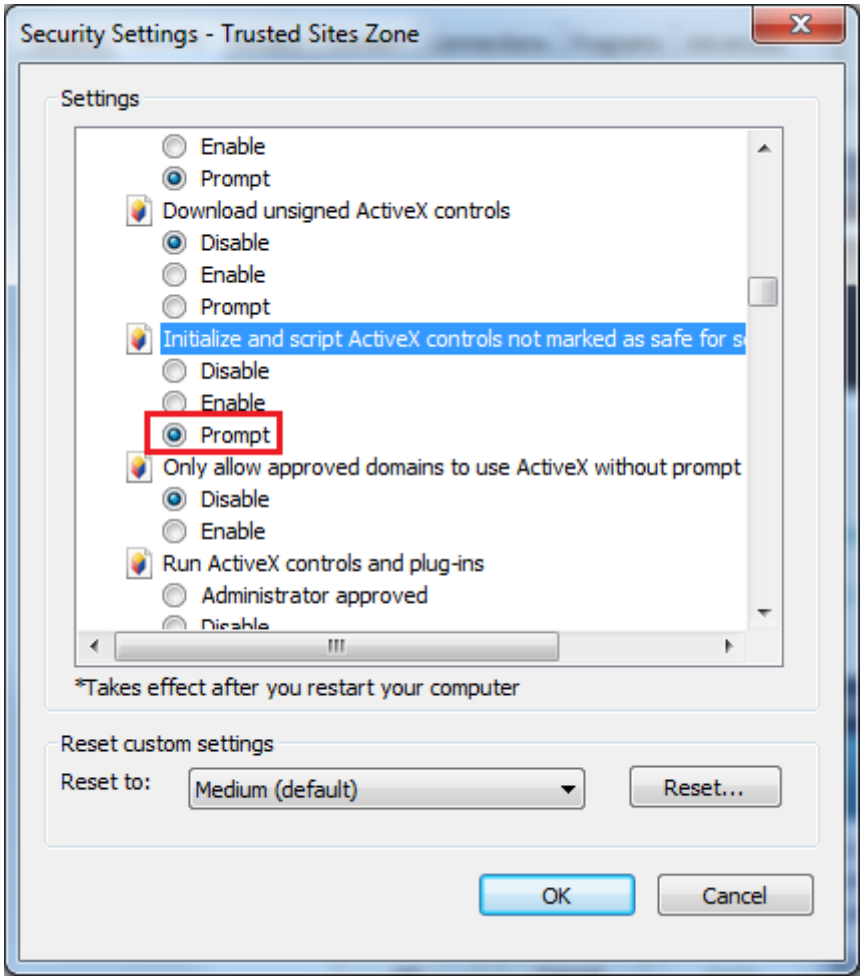



Trusted sites
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Add this website to the zone:
https://portal.ote-cr.cz
Add
Websites:
https://portal.ote-cr.cz
Remove
Require server verification (https:) for all sites in this zone
Close

3.1.2 Check ActiveX component settings

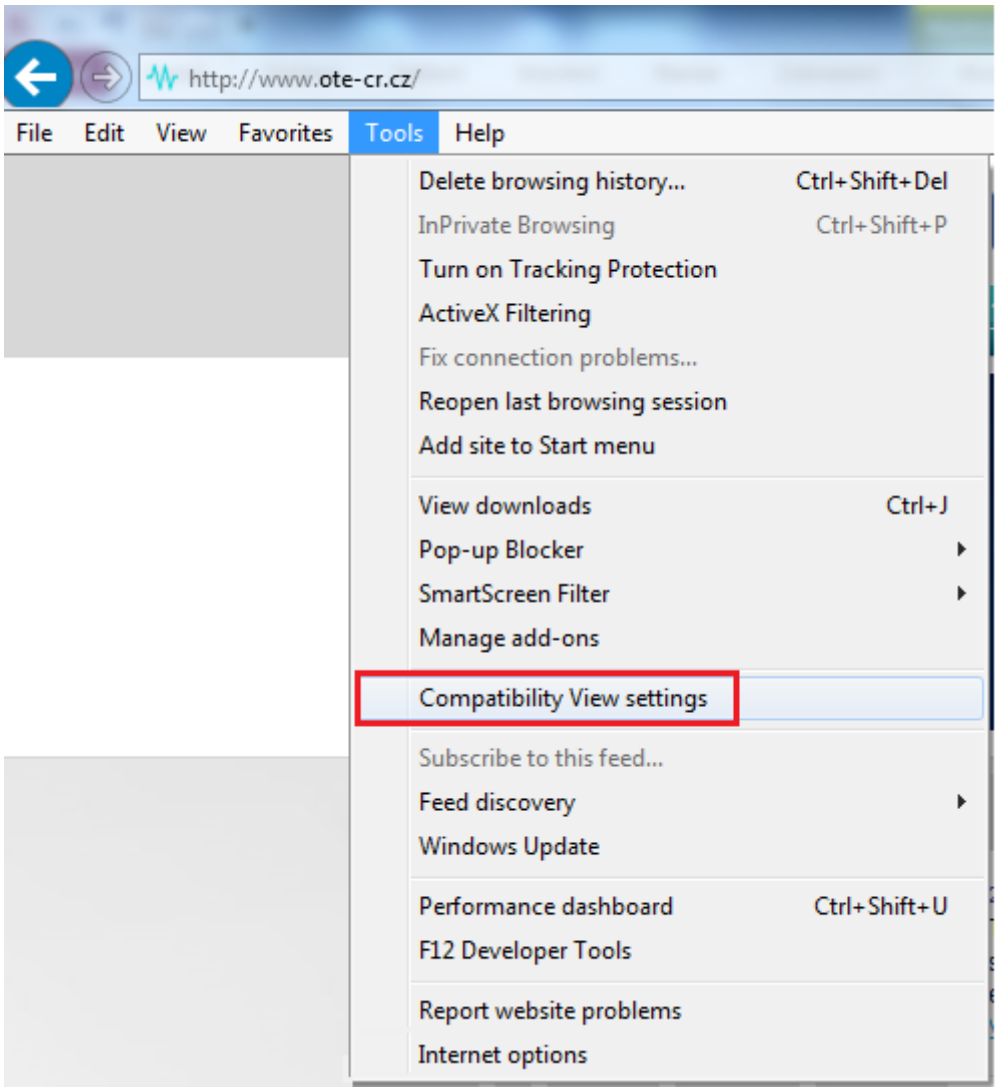
Download of ActiveX components on your workstation has to be set up for the properly CS OTE functionality. Please use the following instructions:



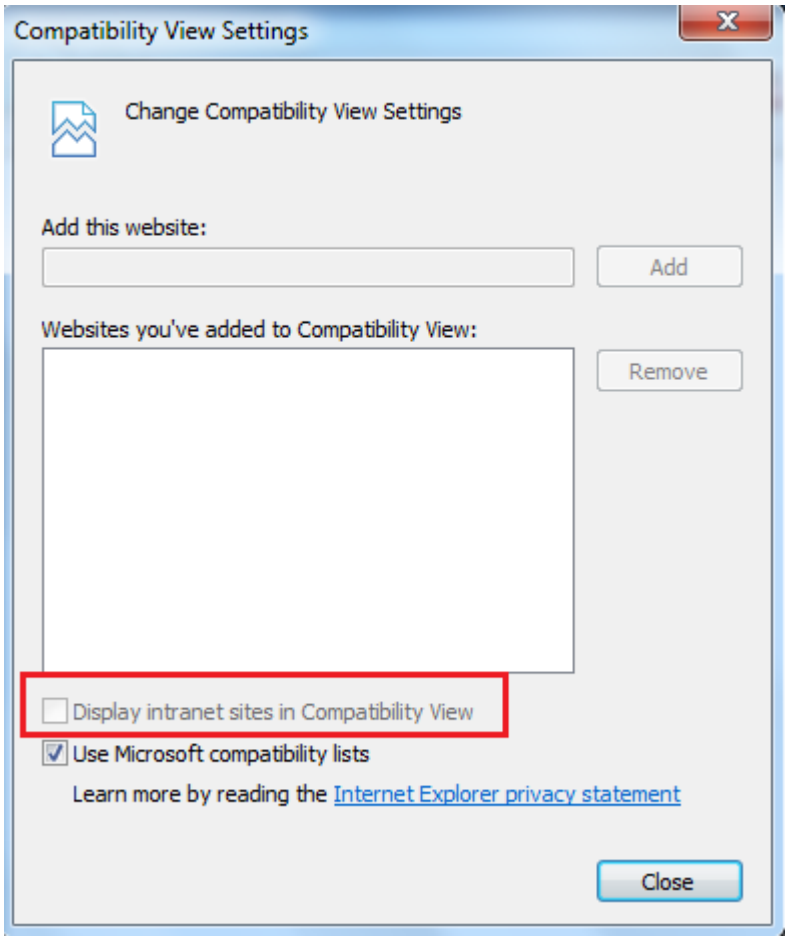

Security Settings - Trusted Sites Zone
Settings
Enable
Prompt
Download unsigned ActiveX controls
Disable
Enable
Prompt
Initialize and script ActiveX controls not marked as safe for s
Disable
Enable
Prompt
Only allow approved domains to use ActiveX without prompt
Disable
Enable
Run ActiveX controls and plug-ins
Administrator approved
*Takes effect after you restart your computer
Reset custom settings
Reset to:
Medium (default)
Reset...
OK
Cancel

3.1.3 Compatibility view setting in Internet Explorer (IE)

Browser IEv11 should be configured the following recommendation. Go to browser menu Tools – Compatibility View settings



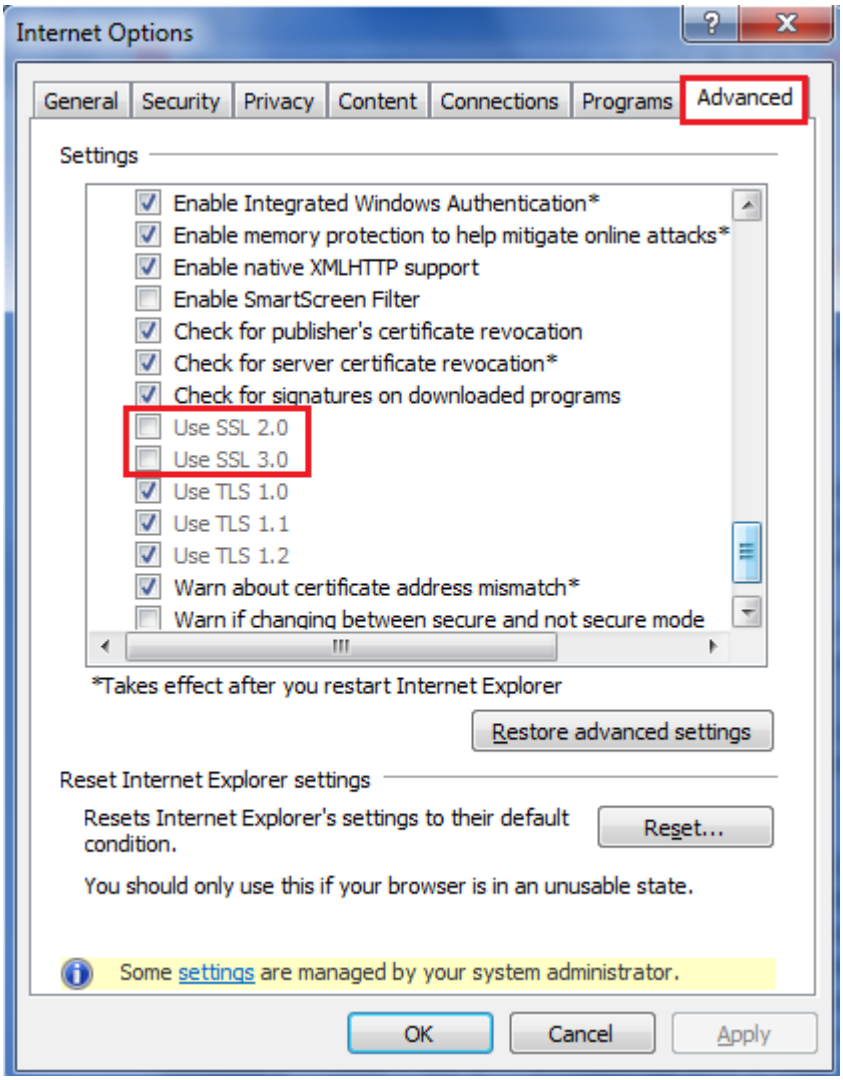
Remove implicit checkbox „Display intranet sites in Compatibility view“, as presented below.



Close the dialog.

3.1.4 Secure communication setting configuration

Check the secure setting configuration, menu Internet Option – Advanced. See screen copy below.

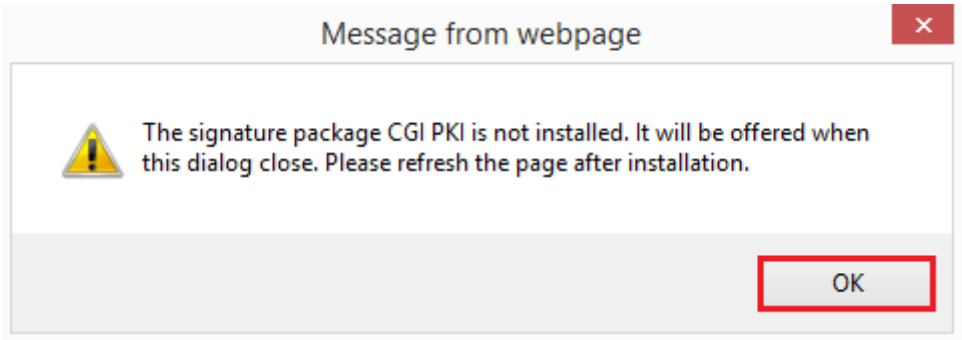


Let the TLS setting and remove checkboxes from SSL and confirm change by press OK button.

3.1.5 CGI PKI package installation for Internet Explore

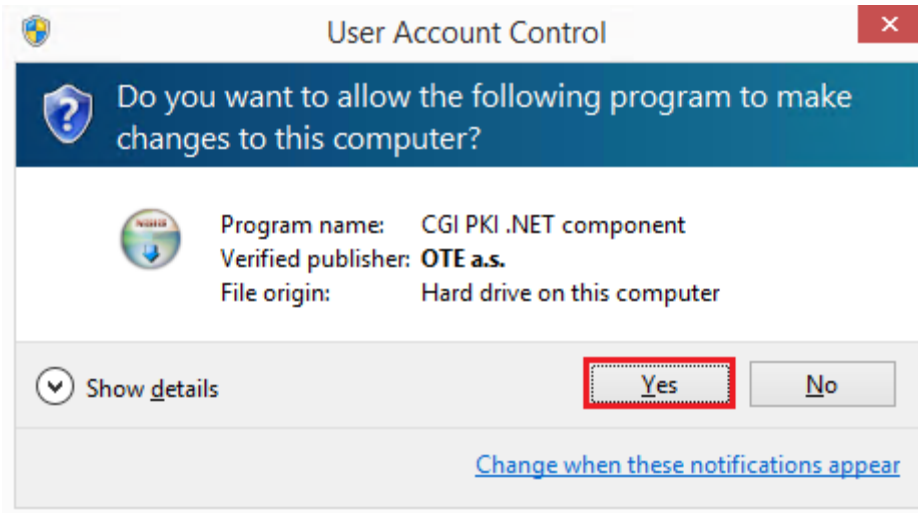
CGI PKI package has to be installed on a local workstation. How to install this is described in chapters below. User has to have admin rights to install these new components in system registry. **Admin rights are mandatory!**

When user logins into CS OTE portal (https://portal.ote-cr.cz/otemarket), new dialog for download CGI PKI package ActiveX appears.

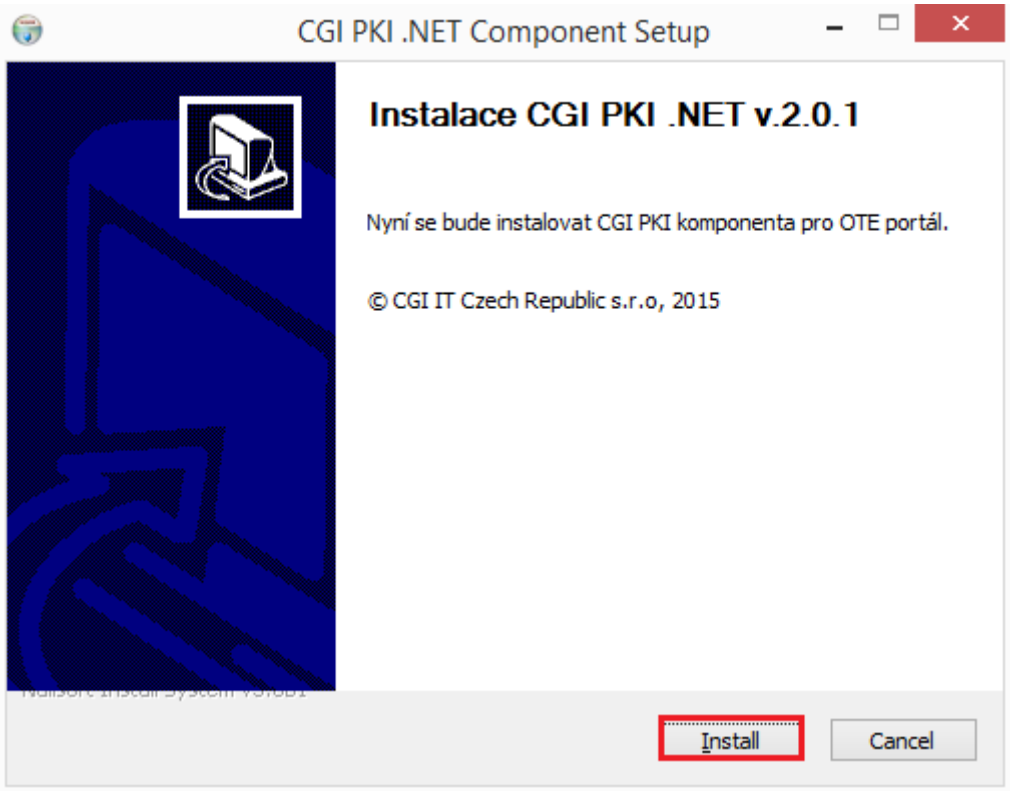


Press „OK“ button and then press „Run“ button

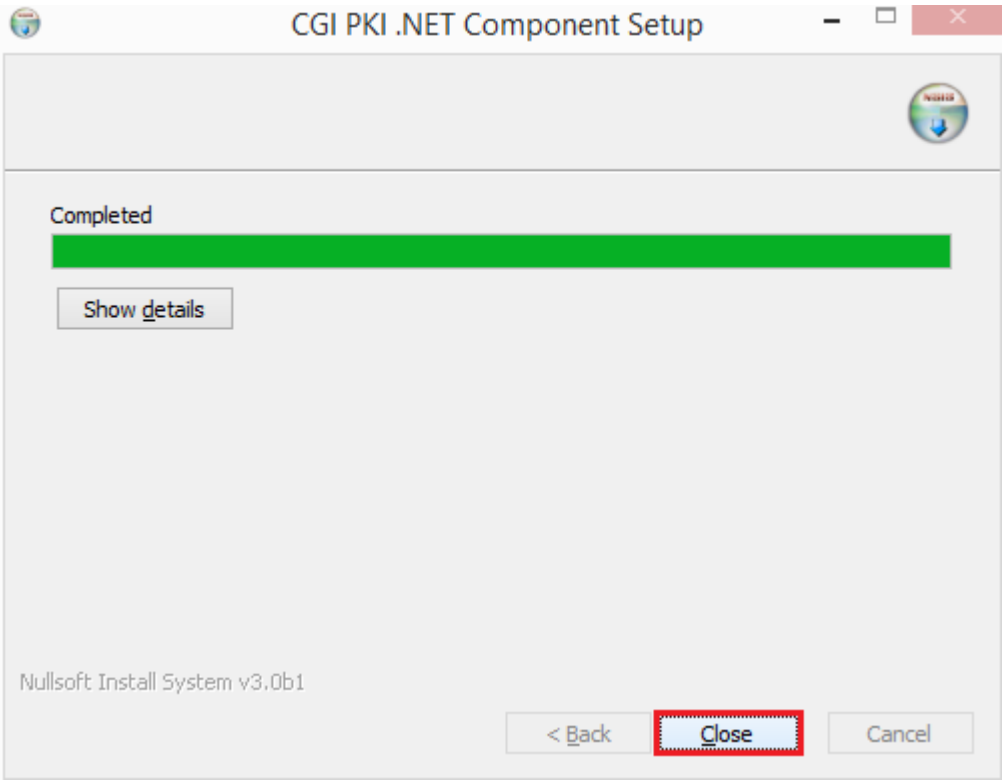
Press „Yes“ button



Press „Install“ button



Press „Close“ button



After these steps CGI PKI component is successfully installed.

3.1.6 Manual installation of CGI PKI sign package for Internet Explorer

In case of any technical problems with, CGI PKI sign package can be downloaded directly from site below and manually installed.

- Download installation package from link below https://www.ote-cr.cz/registrace-a-smlouvy/pristup-do-cs-ote/files-konfigurace-pc/OtePortalPki.exe
- Close all Internet Explorer windows
- Run the installation wizard
- Follow the installation wizard
- The sign process should work now.

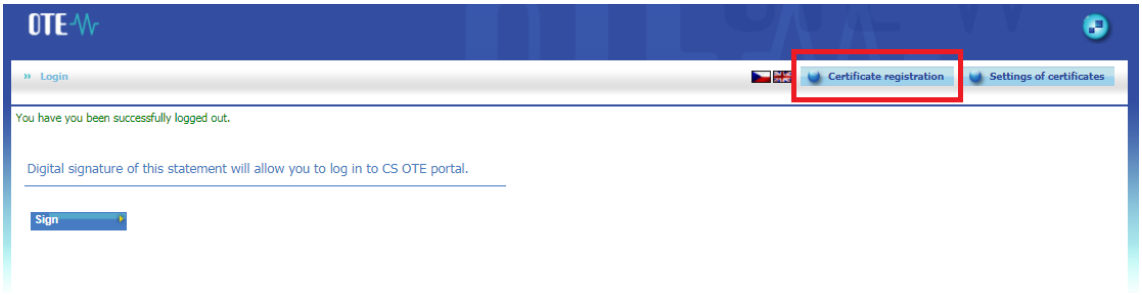
4 Re-registering the Certificate after validity expires

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 i tis 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.

  A) OTE-COM Launcher Manager (LM) for Electricity:

  - For 32 bit version: http://www.ote-cr.cz/LauncherManager-PROD-windows-i586.exe
  - For 64 bit version: http://www.ote-cr.cz/LauncherManager-PROD-windows-x64.exe

  B) OTE-COM Launcher Manager (LM) for Gas:

  - For 32 bit version: http://www.ote-cr.cz/OTE-COM-GAS-PROD-windows-i586.exe
  - For 64 bit version: http://www.ote-cr.cz/OTE-COM-GAS-PROD-windows-x64.exe

  - Manual for installation of OTE Launcher Manager you can download 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.