

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.

2016 OTE, a.s.

Date of revision:
20.12.2016

Document name:
Client station configuration

Document version:
EAF2315

Date	Describe 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12.1.2011	Removal of outdated information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)

2016 OTE, a.s.

Date of revision:
20.12.2016

Document name:
Client station configuration

Document version:
EAF2315

Contents

1	Workstation configuration	3
2	USB token iKey 2032, eToken 5000 (old iKey 4000) and eToken 5100 installation	4
2.1	<i>SafeNet Token Utilities v10.x installation guide.....</i>	4
2.2	<i>Internet Explorer browser settings</i>	8
2.2.1	Root authority OTECA installation	8
2.2.2	Set up of Trusted sites	13
2.2.3	Check ActiveX component settings	15
2.2.4	Compatibility view setting in Internet Explorer (IE)	17
2.2.5	Secure communication setting configuration.....	19
2.2.6	CGI PKI package installation for Internet Explore	19
2.2.7	Manual installation of CGI PKI sign package for Internet Explorer.....	22
2.3	<i>FireFox browser setting</i>	22
2.3.1	Import of the root certificate authority	22
2.4	<i>Google Chrome/Microsoft Edge browser setting</i>	26
2.4.1	Import of the root certificate authority	26

1 Workstation configuration

Supported configuration for workstations for running CS OTE is following:

Windows 7 (32bit) + MS IE11.0/FireFox(32bit)+ SAC 10.x + 3pieces SafeNet USB tokens (iKey 2032, eToken 5000 (earlier iKey 4000), eToken 5100) + Outlook 2016 /x86

Windows 7 (64bit) + MS IE11.0(32bit)/FireFox(32bit) + SAC 10.x + 3pieces SafeNet USB tokens (iKey 2032, eToken 5000 (earlier iKey 4000), eToken 5100) + Outlook 2016/ x64

Windows 10 (32bit) + MS IE11.0/Edge/FireFox/Chrome-last version + SAC 10. x + 3pieces SafeNet USB tokens (iKey 2032, eToken 5000 (earlier iKey 4000), eToken 5100) + Outlook 2016/ x86

Windows 10 (64bit) + MS IE11.0/Edge/FireFox/Chrome-last version + SAC 10. x + 3pieces SafeNet USB tokens (iKey 2032, eToken 5000 (earlier iKey 4000), eToken 5100) + Outlook 2016/ x64

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

2 USB token iKey 2032, eToken 5000 (old iKey 4000) and eToken 5100 installation

2.1 SafeNet Token Utilities v10.x installation guide

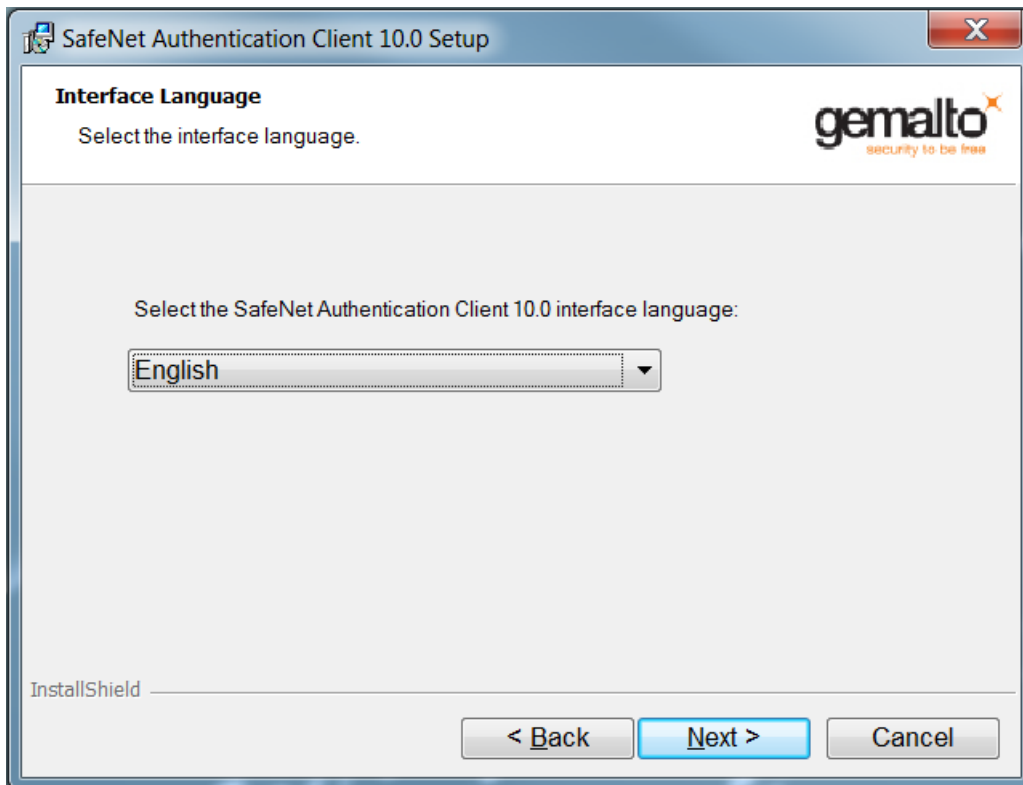
Installation package for SafeNet Token Utilities v10.x is available when user fills in certificate order form from link below:

<http://www.ote-cr.cz/registrace-a-smlouvy/files-registrace-a-smlouvy/objednavka-bezpecnostni-prvky-cs-ote.pdf>

Run SafeNet installation **before iKey token inserted into workstation USB!** Run file SafeNetAuthenticationClient-x32-x64-10.0.exe (works for both, 32bit and 64bit OS) and follow instructions below:



SafeNet installation wizard.

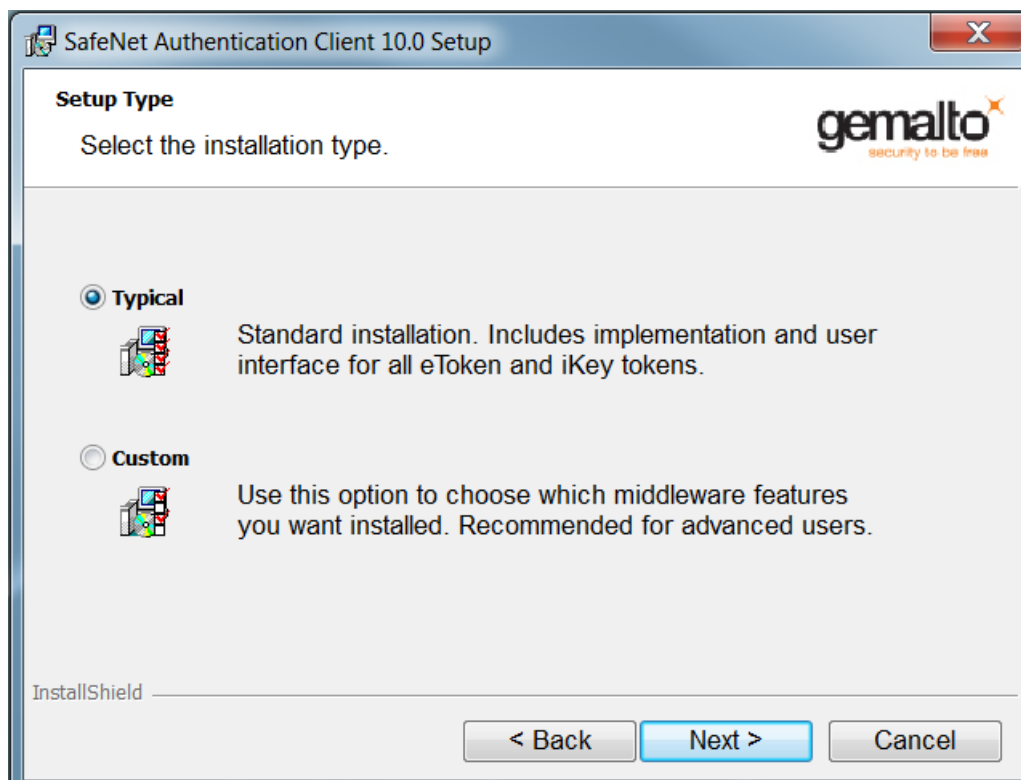


Choose the language from dropdown list, if necessary.

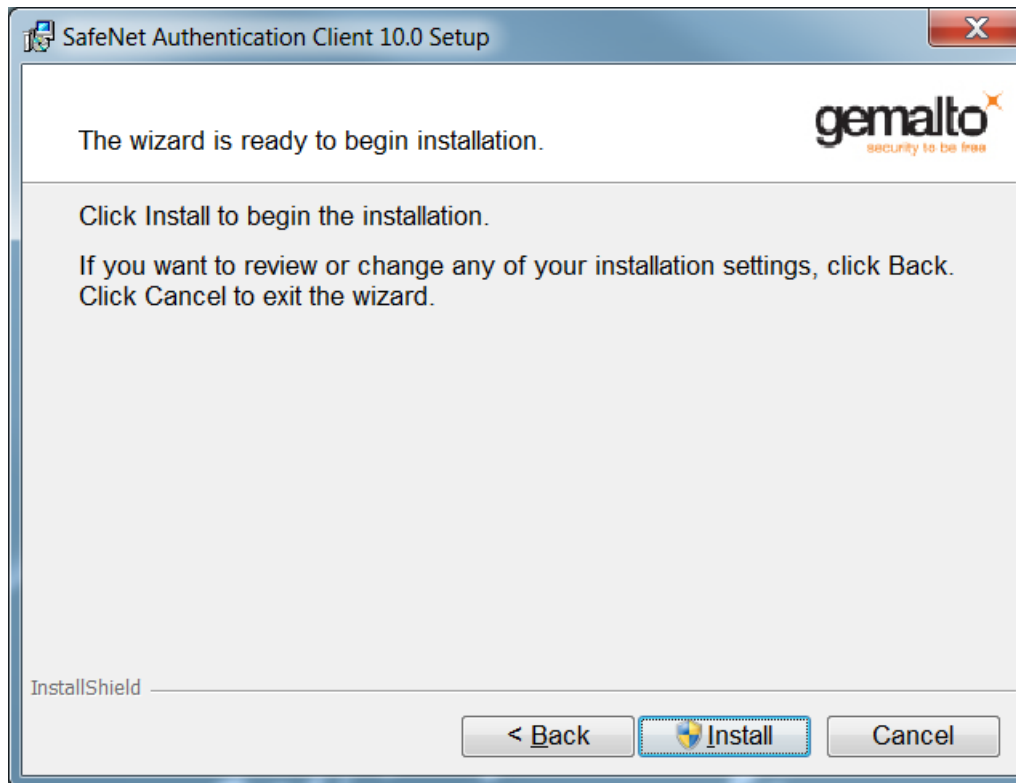




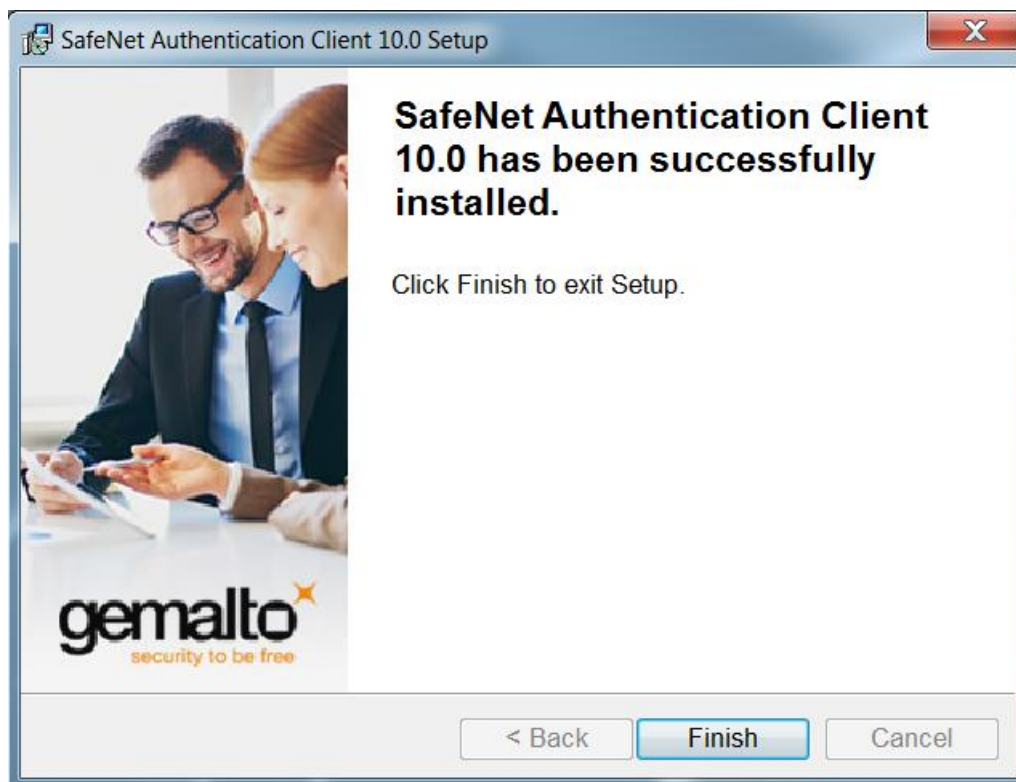
Change a different folder if necessary.



Choose Standard installation type.



Press install. The installation process may take several minutes.



After the (successful) installation following screen will display.

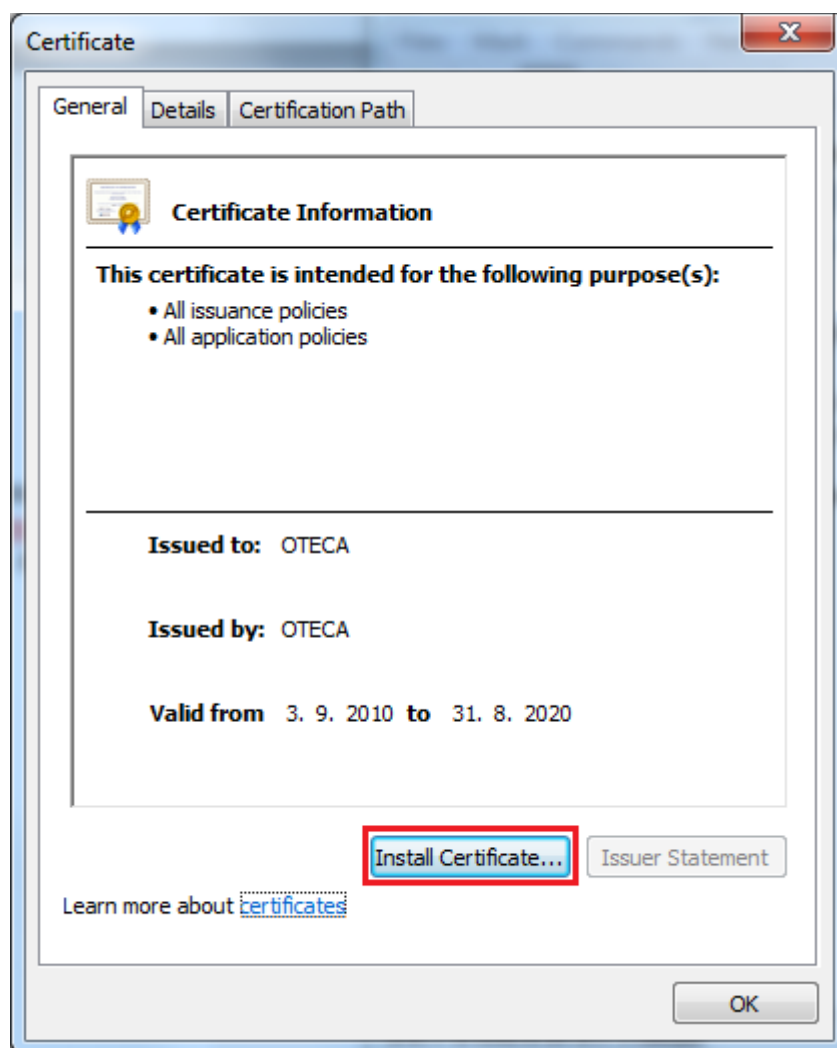
2.2 Internet Explorer browser settings

2.2.1 Root authority OTECA installation

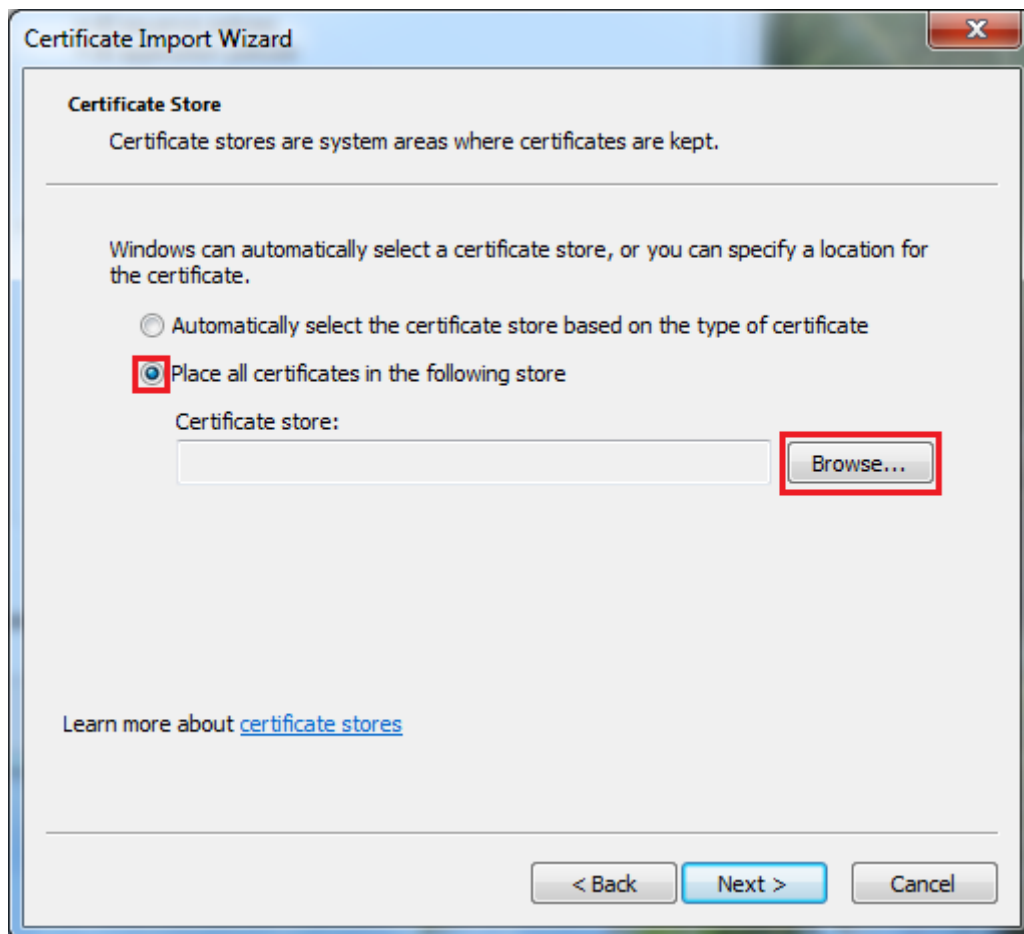
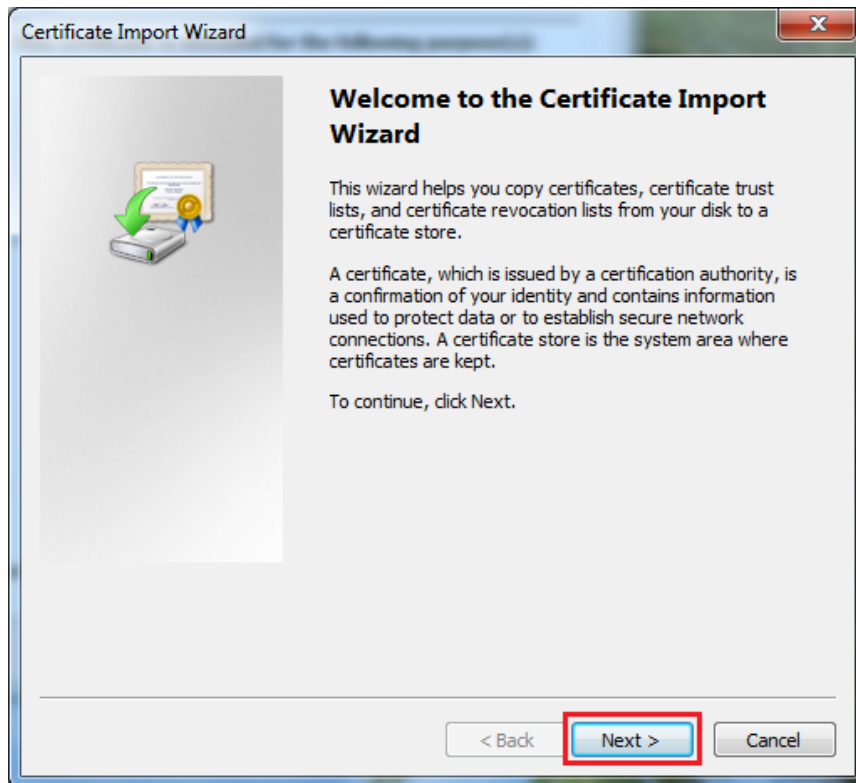
If you see warning showed below during accessing <https://portal.ote-cr.cz/otemarket> you need to install root certificate of OTECA certificate authority (and for access to sand environment you need to install OTECATEST certificate authority). These certificates are available on OTE public web site:

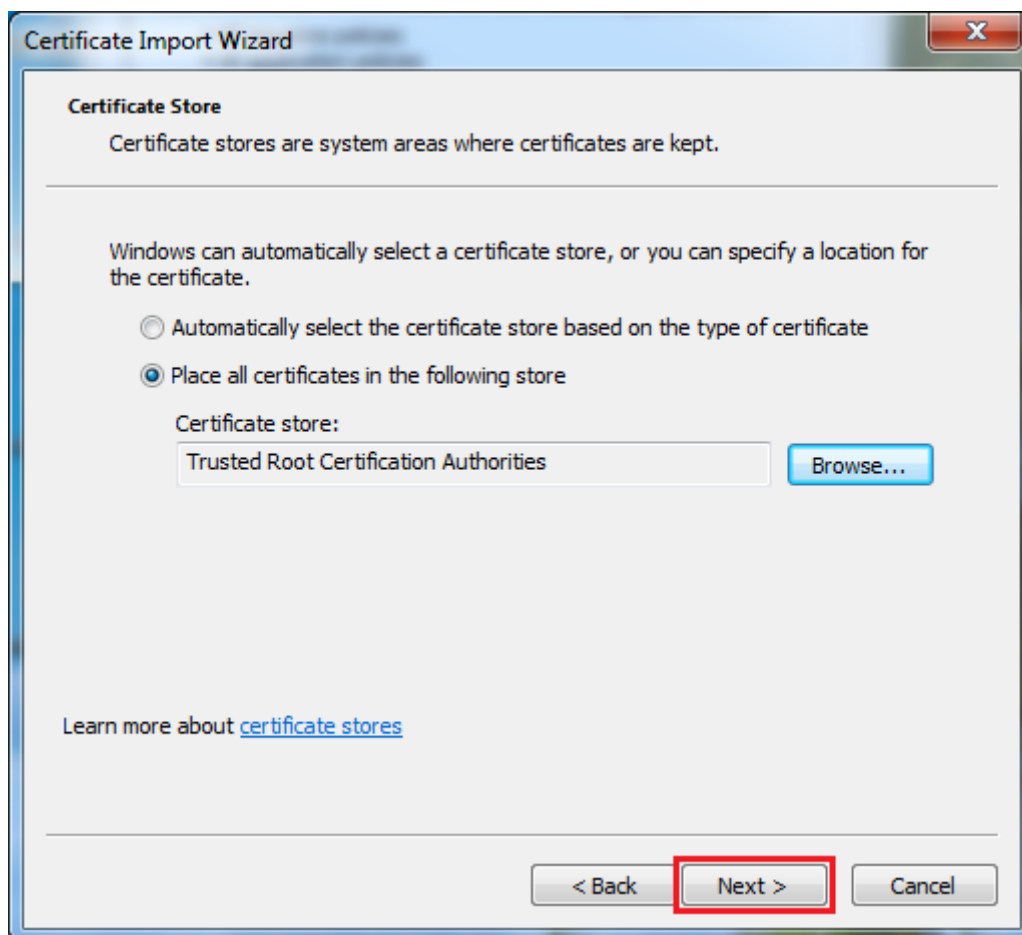
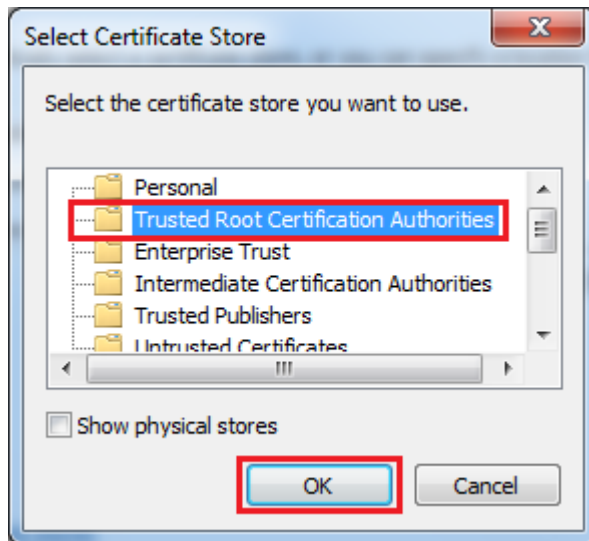
<http://www.ote-cr.cz/registration-and-agreements/access-to-cs-ote/konfigurace-pc>

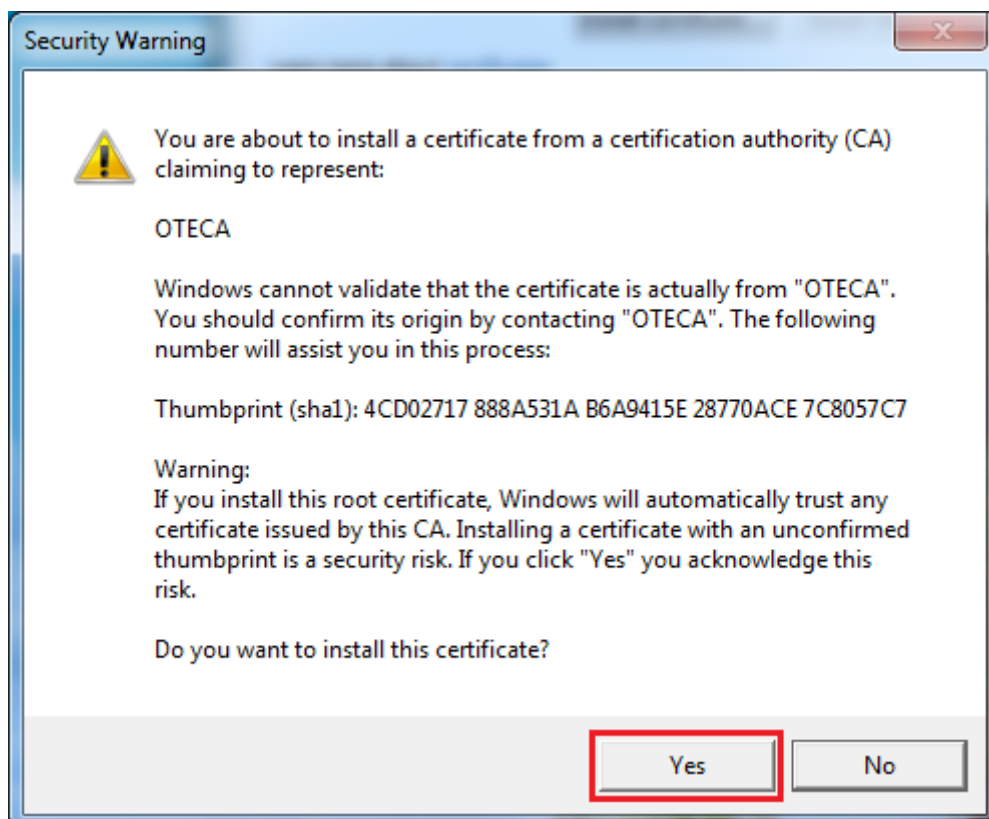
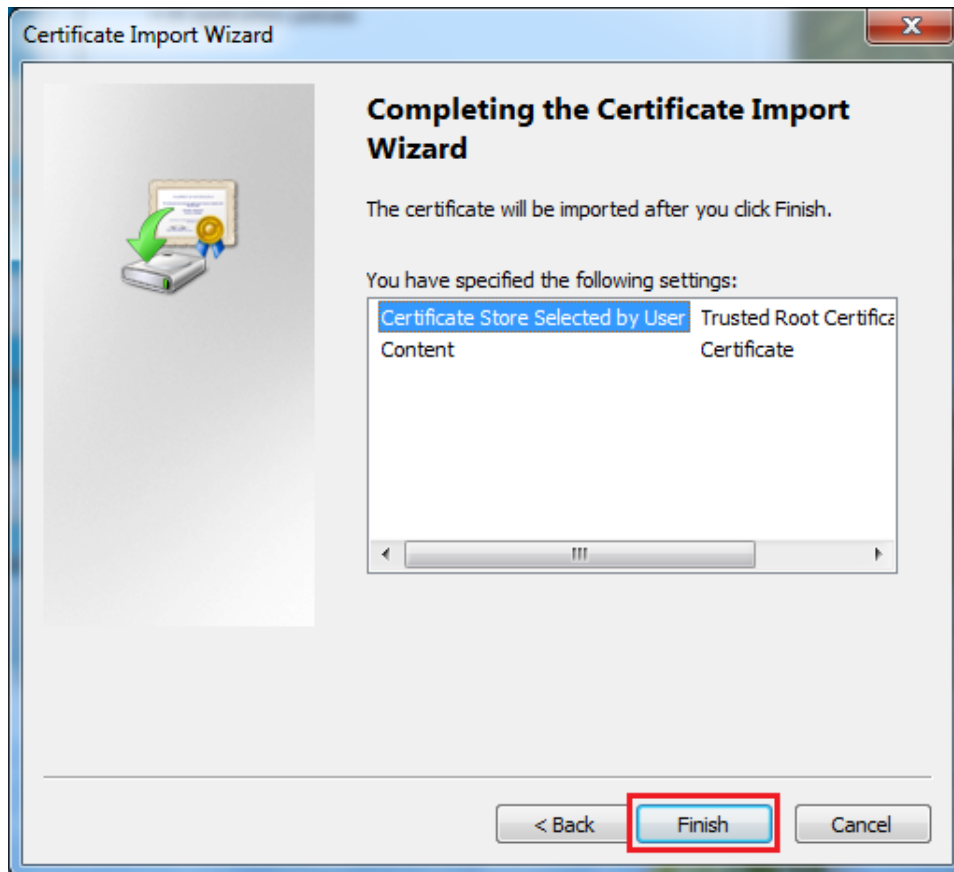
Double click on OTECA.cer file and follow the steps below:

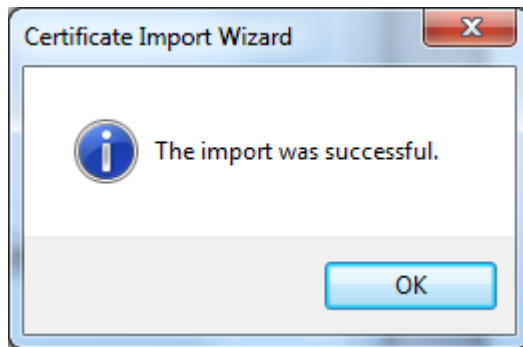


Press „Install certificates“ button to install it on your workstation.

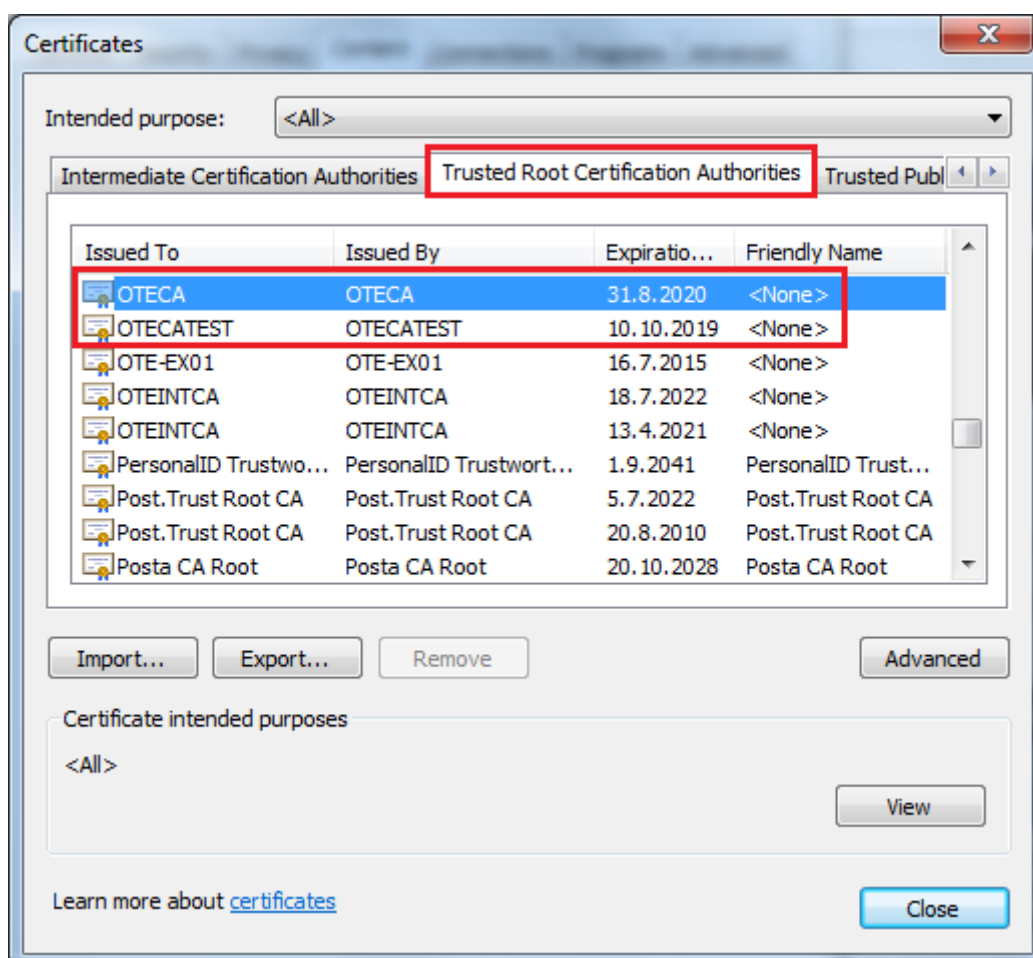






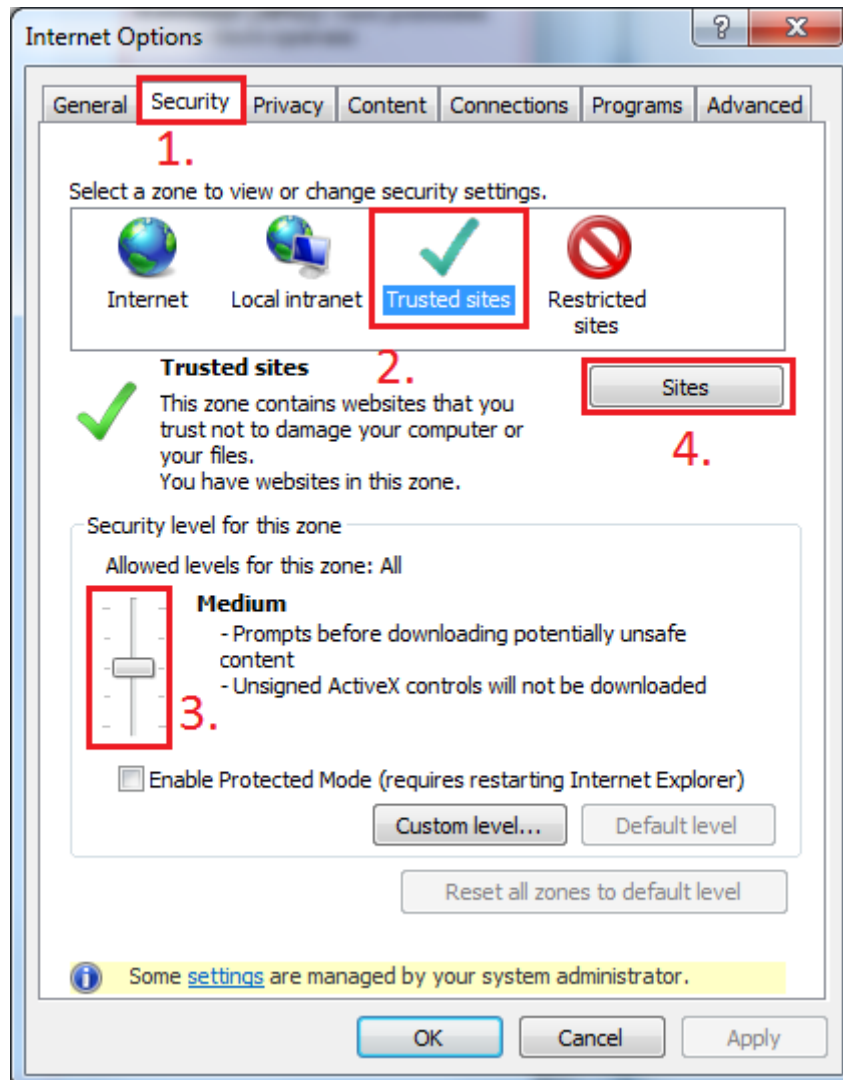


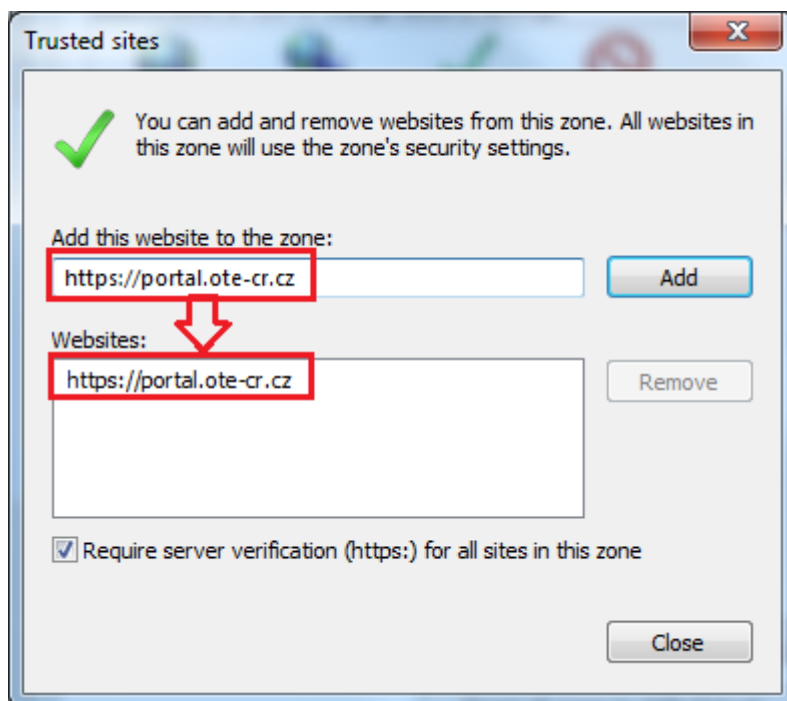
When the import is successful, root certificates is presented in the list of „Trusted Root Certification Authorities“.



2.2.2 Set up of Trusted sites

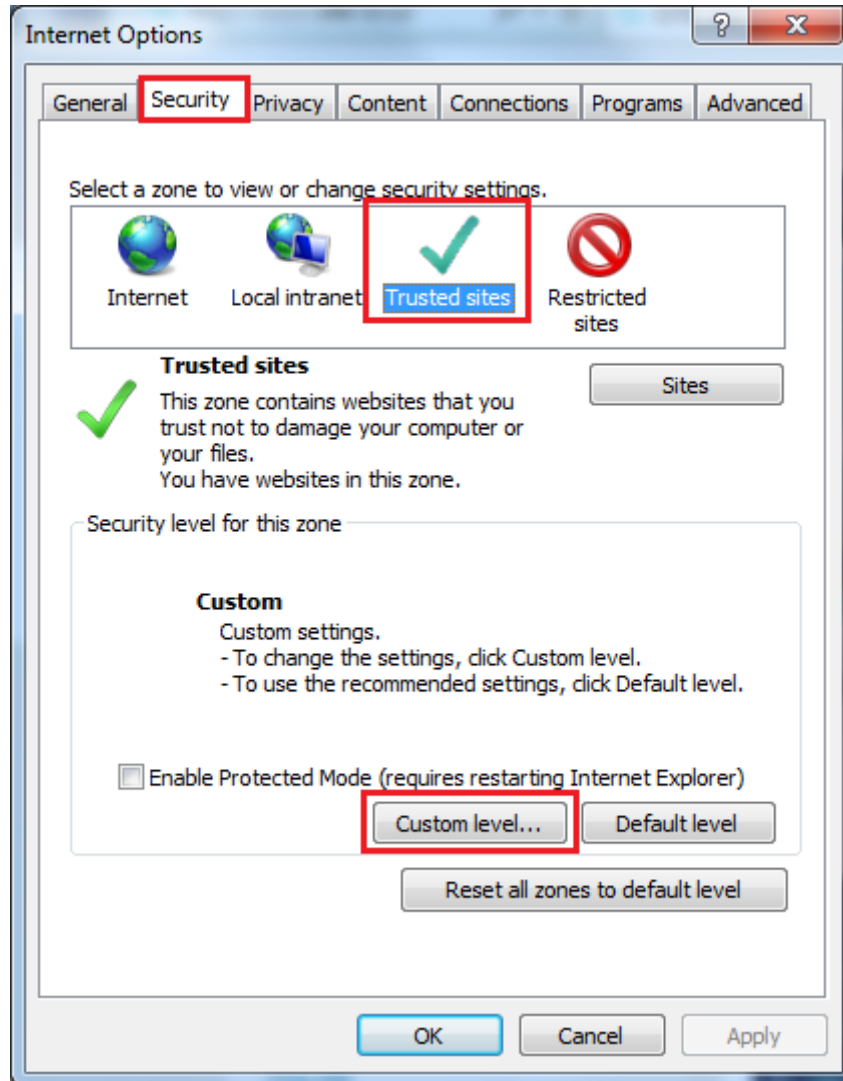
Internet browser settings should be standard but some functions may require adding the site <https://portal.ote-cr.cz/otemarket> into „Trusted sites“ (Tools/Options; see pictures below).

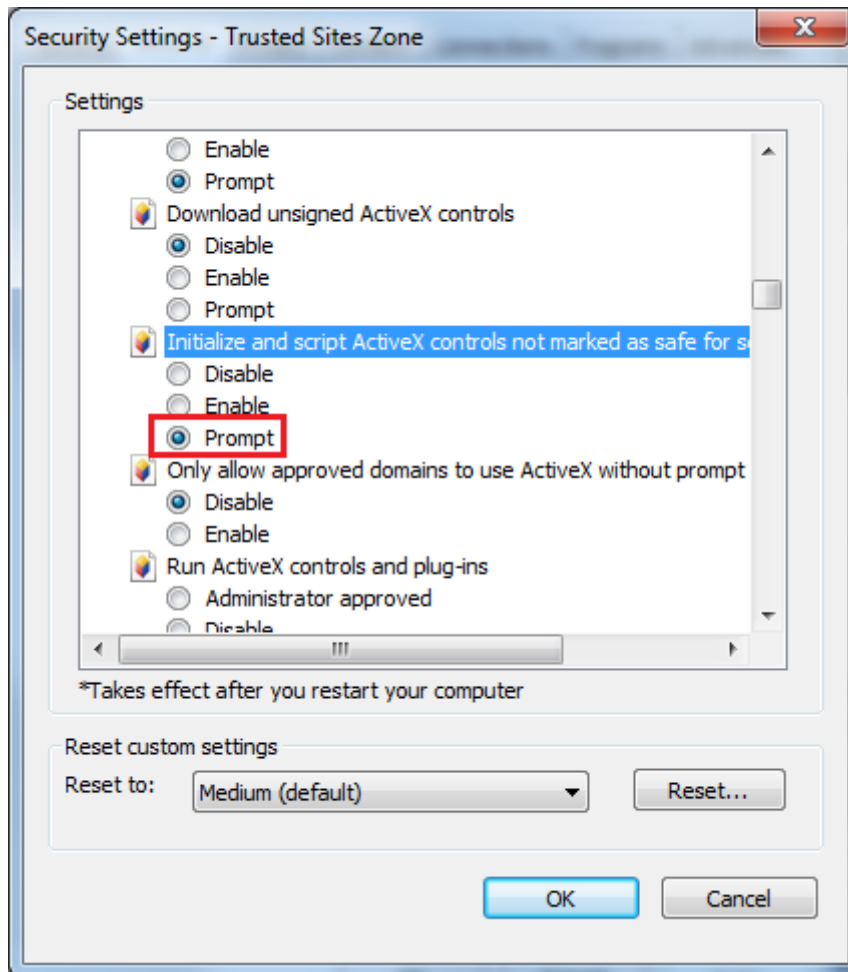




2.2.3 Check ActiveX component settings

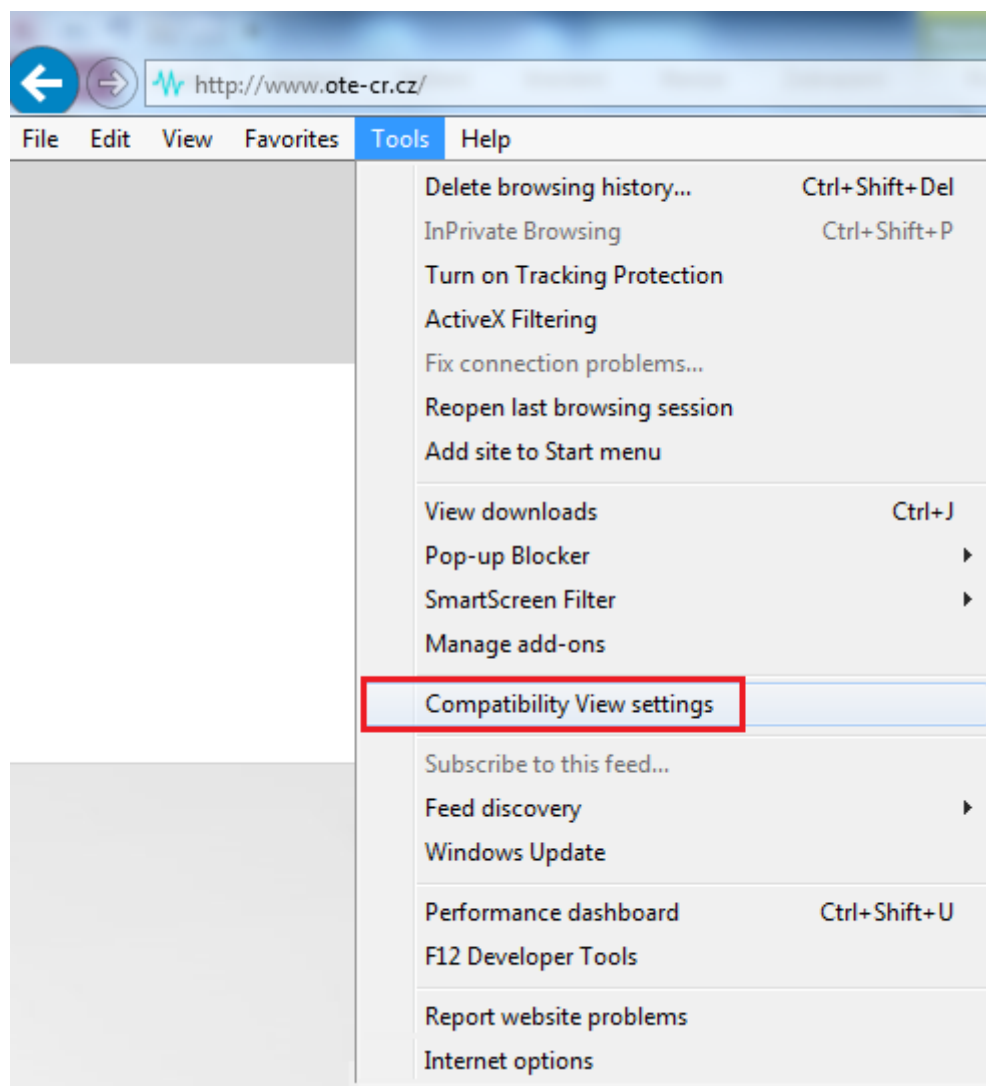
Download of ActiveX components on your workstation has to be set up for the properly CS OTE functionality. Please use the following instructions:



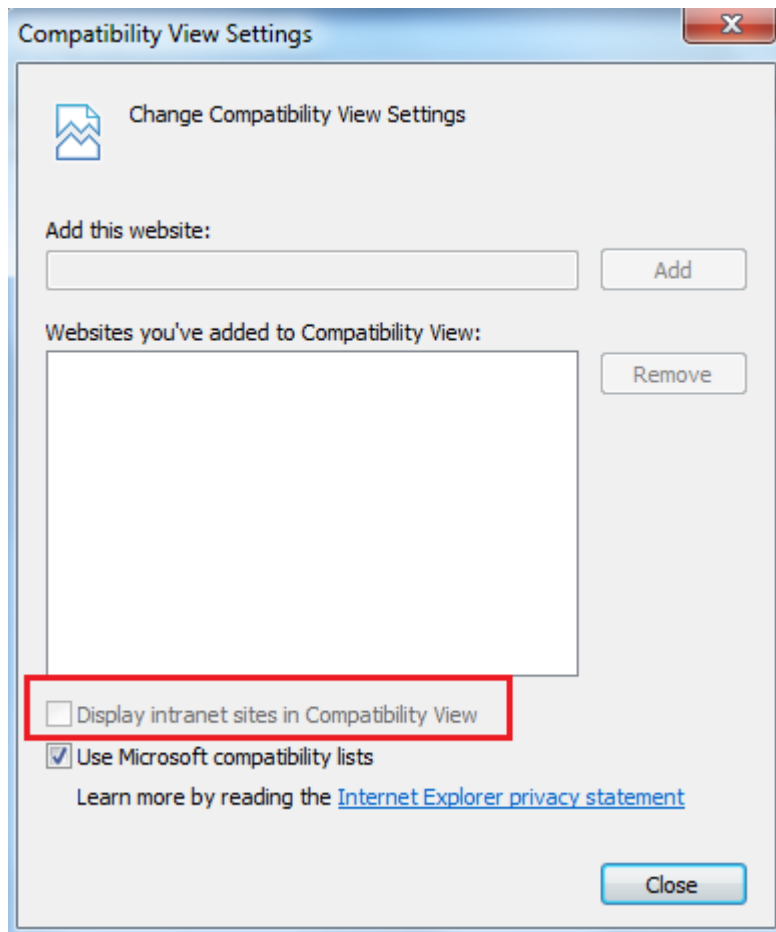


2.2.4 Compatibility view setting in Internet Explorer (IE)

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



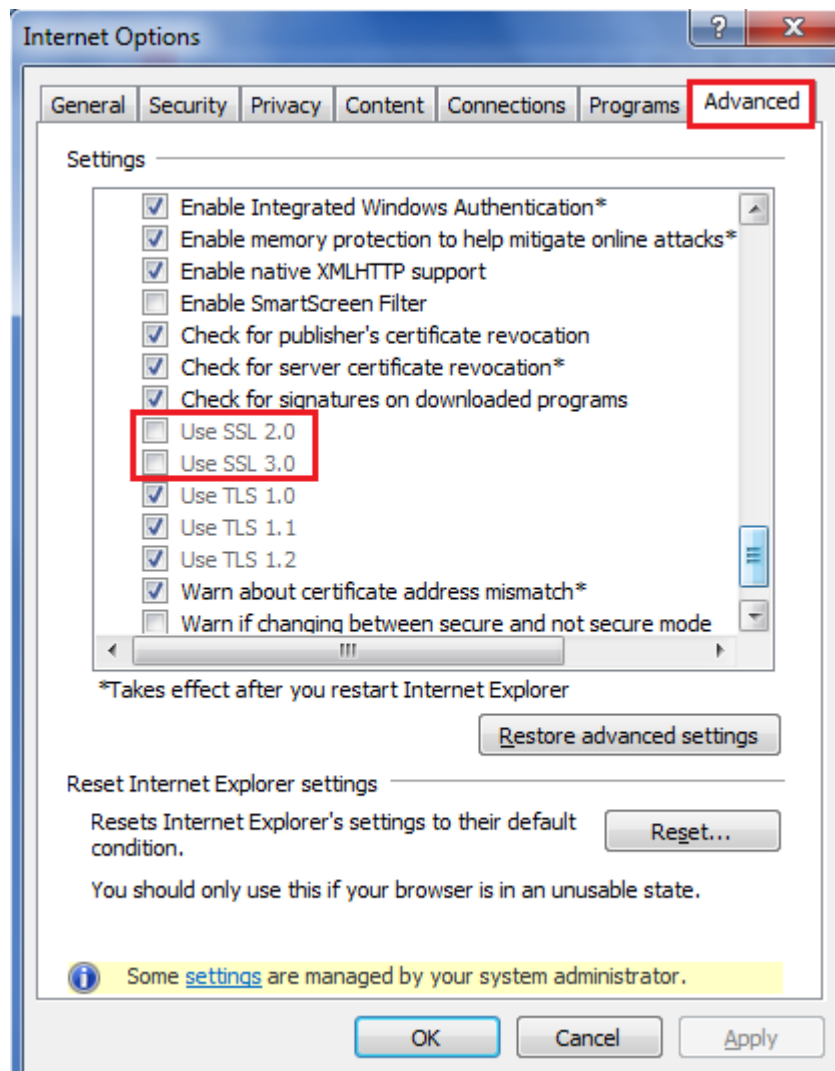
Remove implicit checkbox „Display intranet sites in Compatibility view“, as presented below.



Close the dialog.

2.2.5 Secure communication setting configuration

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

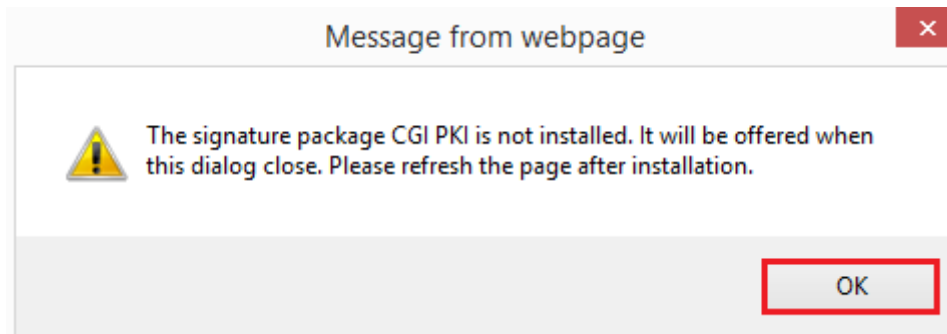


Let the TLS setting and remove checkboxes from SSL and confirm change by press OK button.

2.2.6 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!**

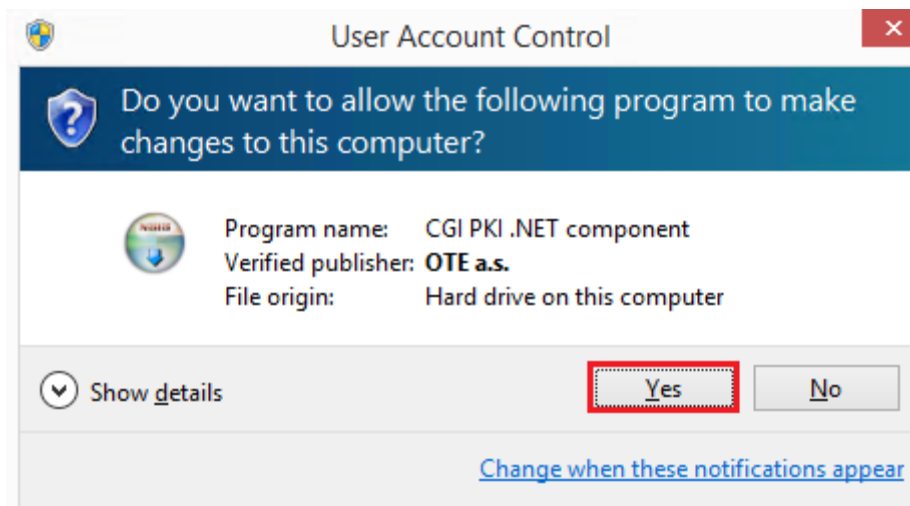
When user logs into CS OTE portal (<https://portal.ote-cr.cz/otemarket>), new dialog for download CGI PKI package ActiveX appears.



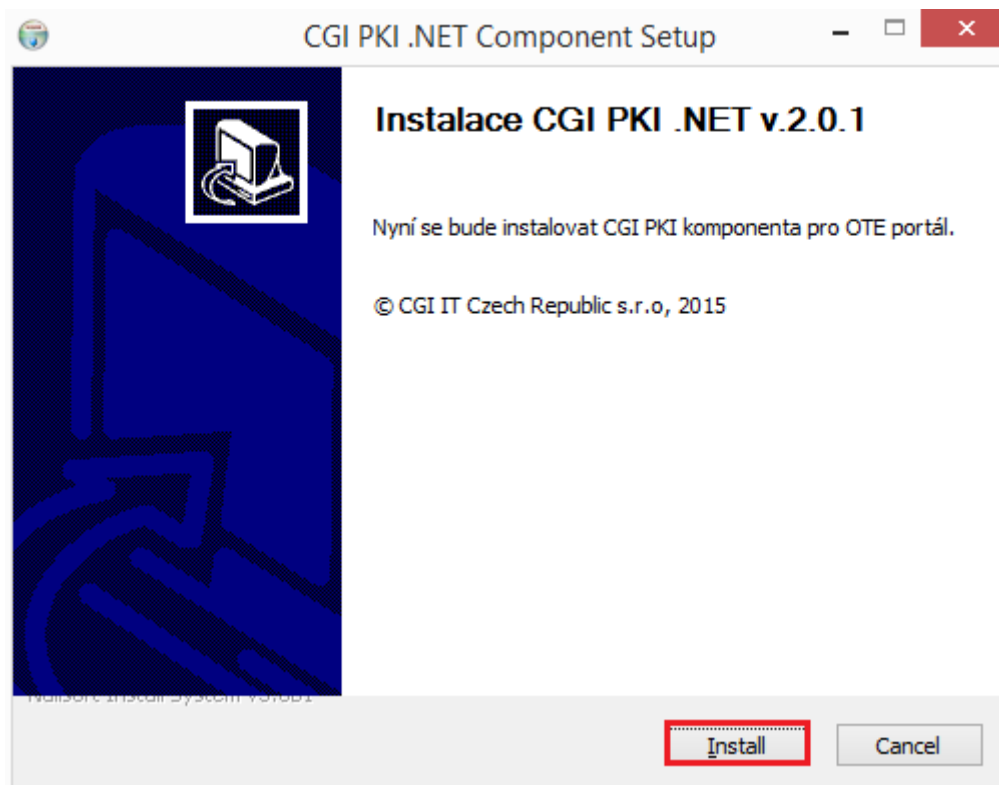
Press „OK“ button and then press „Run“ button



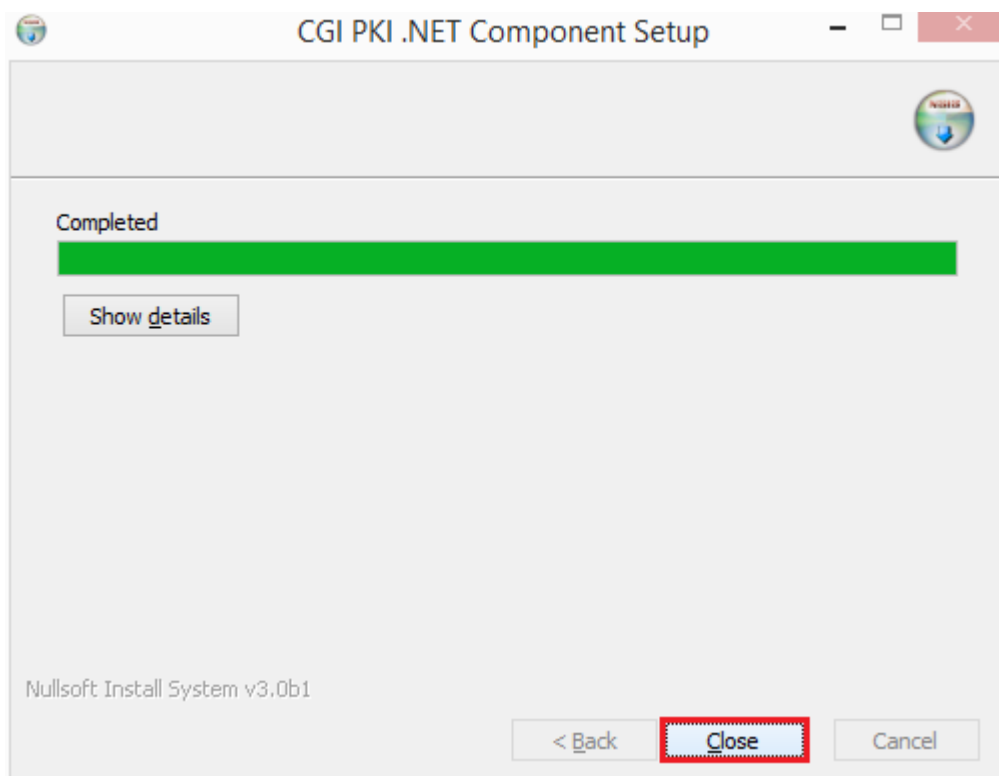
Press „Yes“ button



Press „Install“ button



Press „Close“ button



After these steps CGI PKI component is successfully installed.

2016 OTE, a.s.

Date of revision:
20.12.2016

Document name:
Client station configuration

Document version:
EAF2315

2.2.7 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/regitrace-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.

2.3 FireFox browser setting

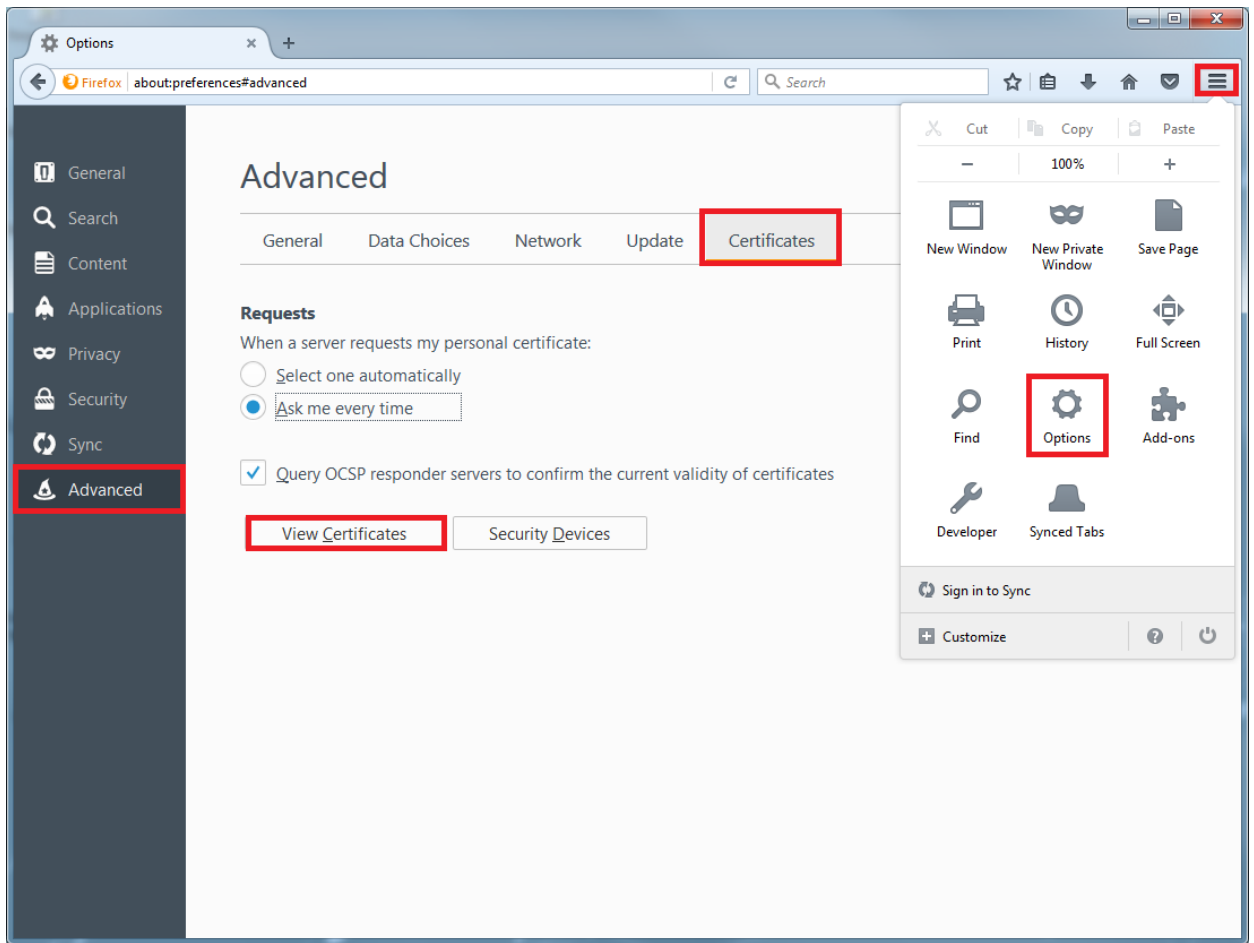
Please follow instructions below for setting access elements in Firefox.

2.3.1 Import of the root certificate authority

Only for access to sand environment you need to install OTECATEST certificate authority. These certificates are available on OTE public web site: http://www.ote-cr.cz/registration-and-agreements/access-to-cs-ote/konfigurace-pc?set_language=en

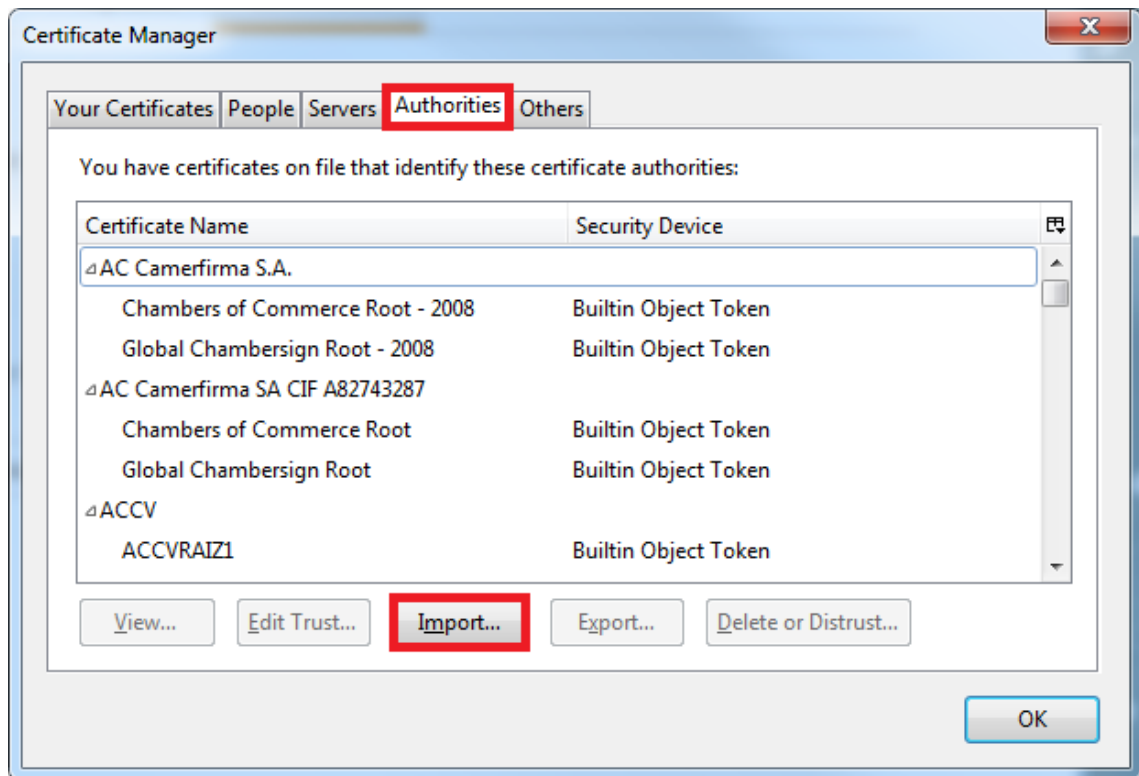
Press  icon in menu, select Options, section Advanced, sheet Certificates.

Press „View Certificates“ button.

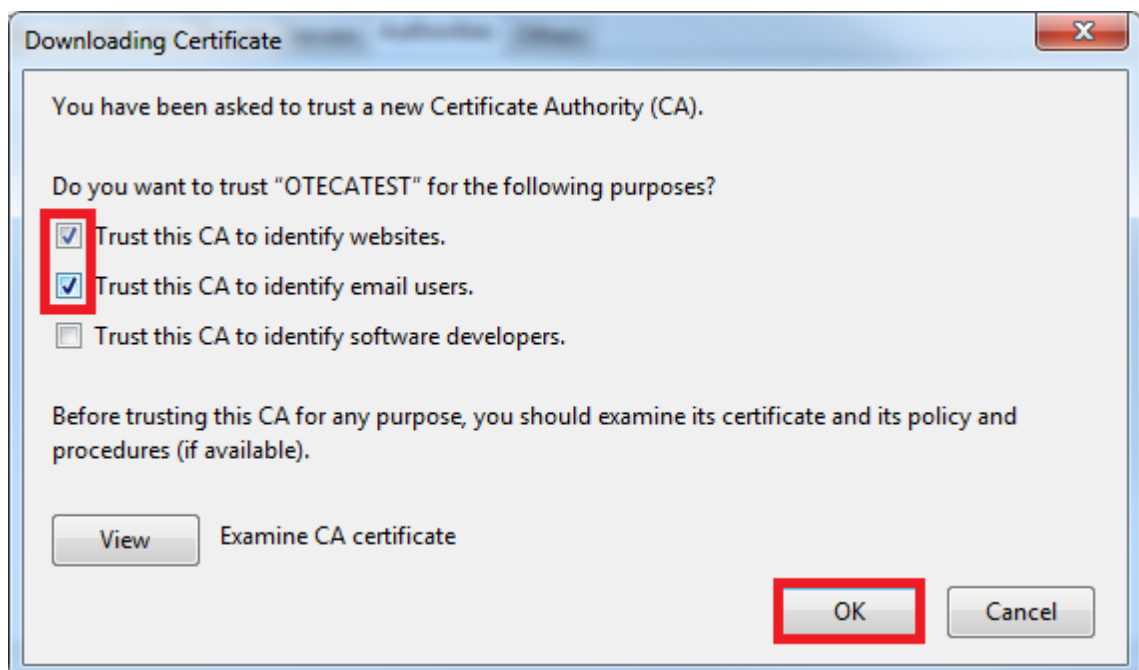


Select „Authorities“ sheet.

Press „Import“ button to find root authority certificate in one of format *.pem, *.cer or *.der.



Check Trust this CA to identify websites and Trust this CA to identify email users options. Press OK button.



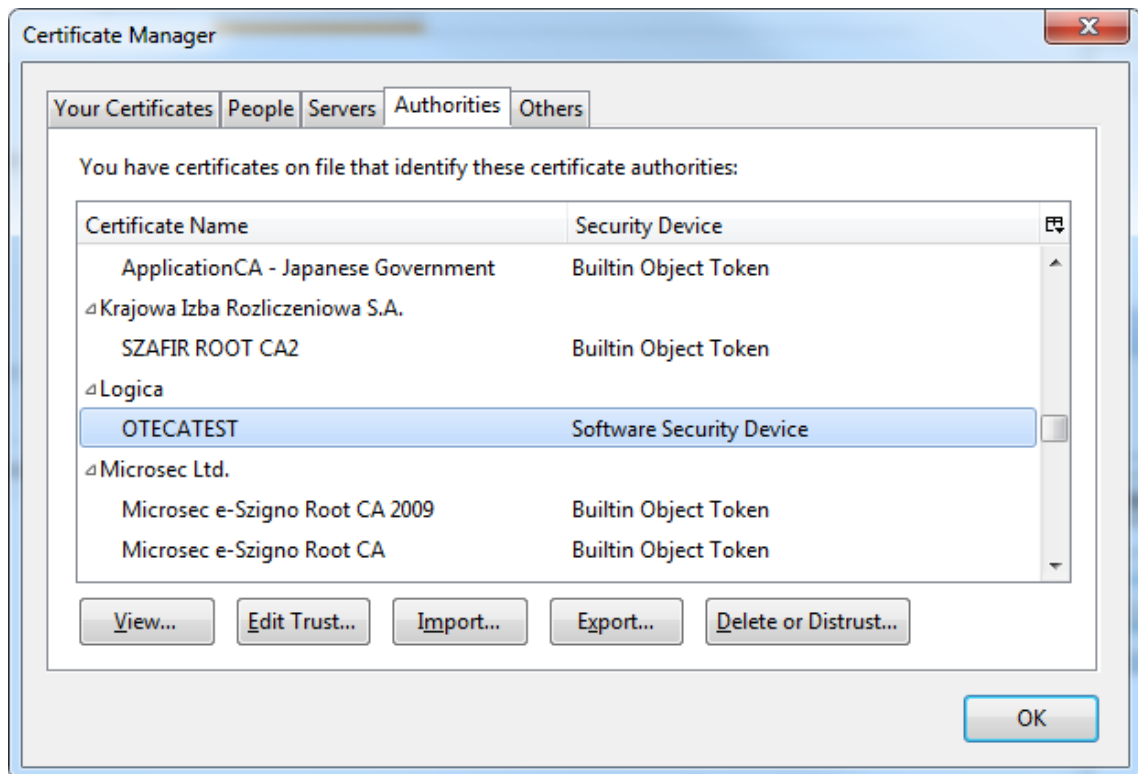
When the import is successfully completed (OTECATEST), the following link will display as on enclosed screen-copy.

2016 OTE, a.s.

Date of revision:
20.12.2016

Document name:
Client station configuration

Document version:
EAF2315



2.4 Google Chrome/Microsoft Edge browser setting

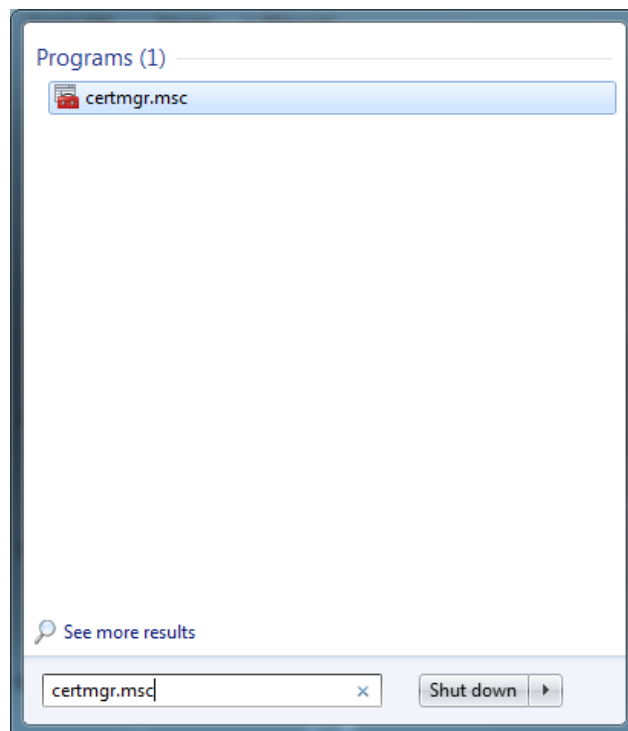
2.4.1 Import of the root certificate authority

Only for access to sand environment you need to install OTECATEST certificate authority. These certificates are available on OTE public web site: http://www.ote-cr.cz/registration-and-agreements/access-to-cs-ote/konfigurace-pc?set_language=en

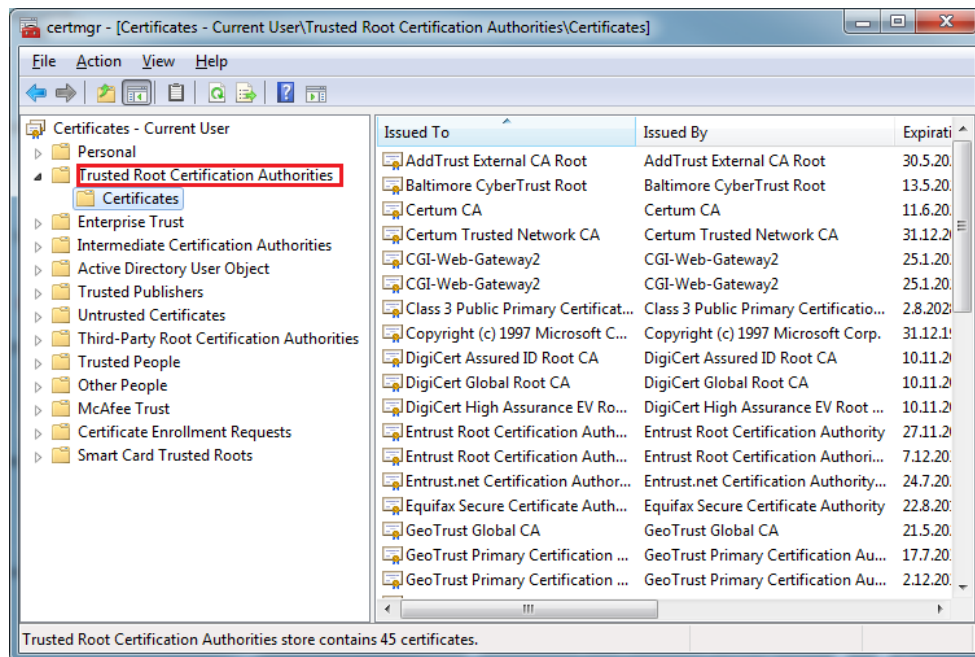
Press Start button.



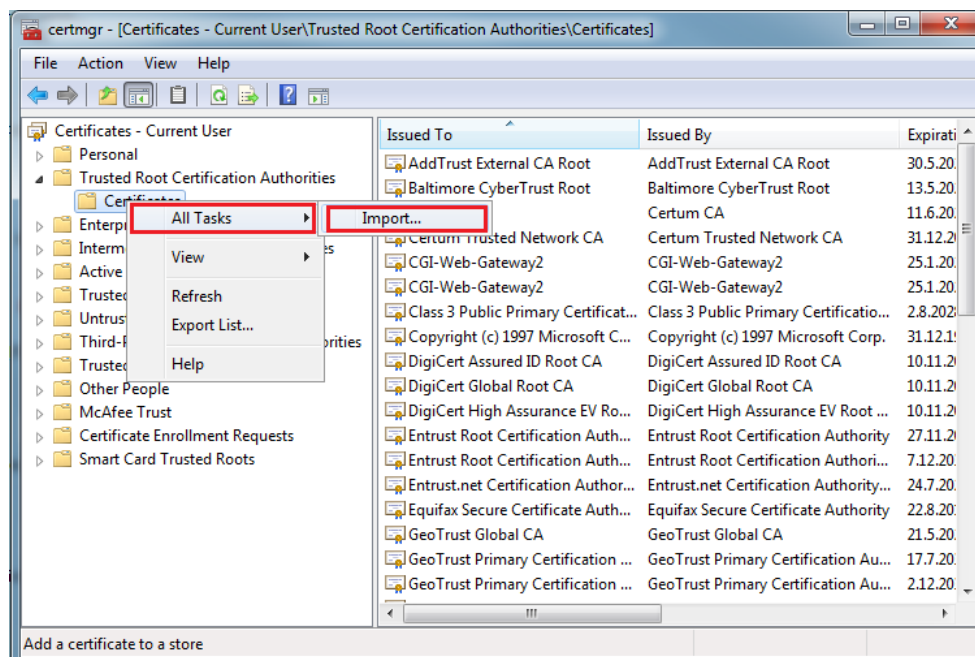
Enter certmgr.msc command into command line. Press on certmgr.msc program icon. Enter your account login and password. Then you should see certificates management window.



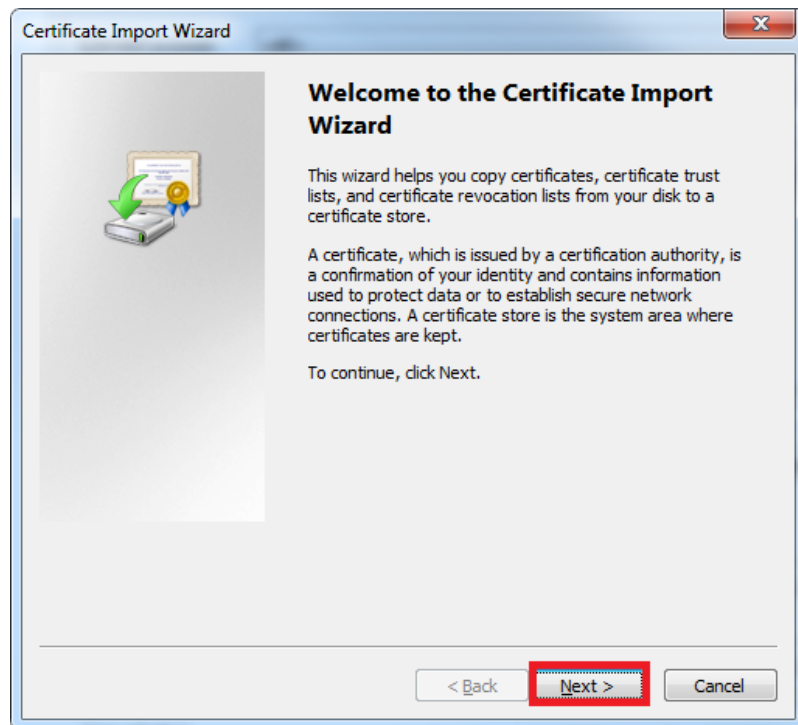
Select „Trusted Root Certification Authorities “ sheet, section „Certificates”.



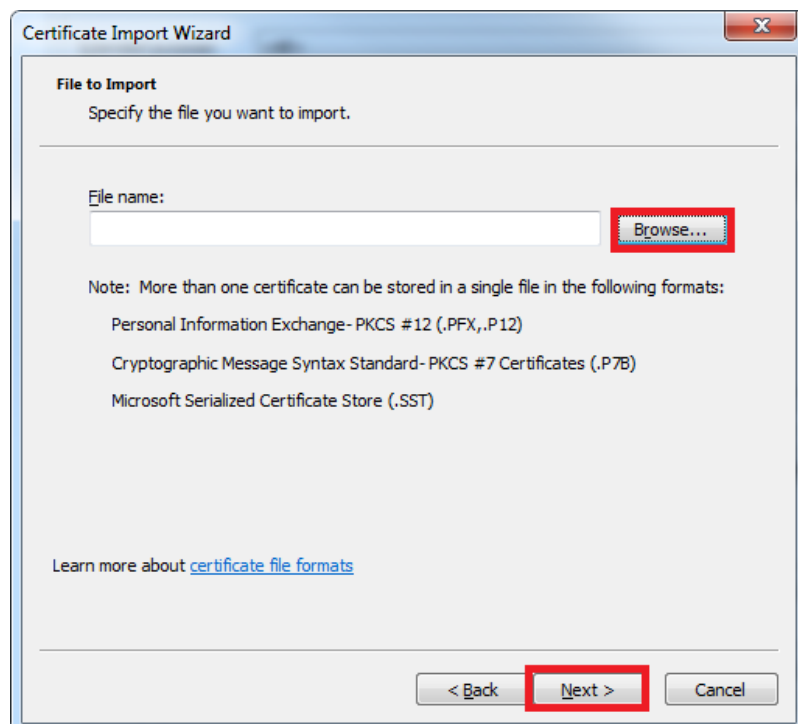
Press right mouse button on „Certificates” section, then press „All Tasks”, „Import”



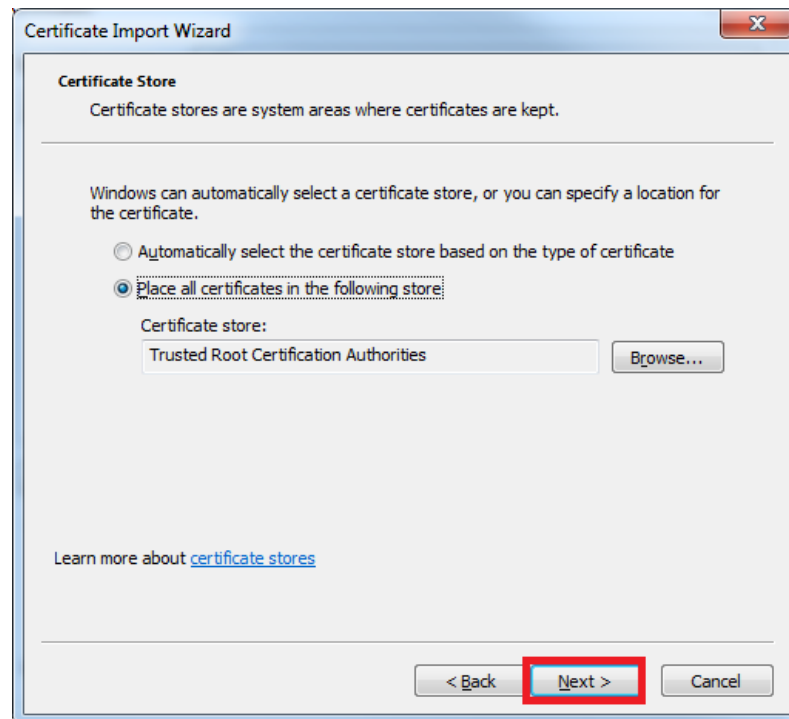
Press Next button.



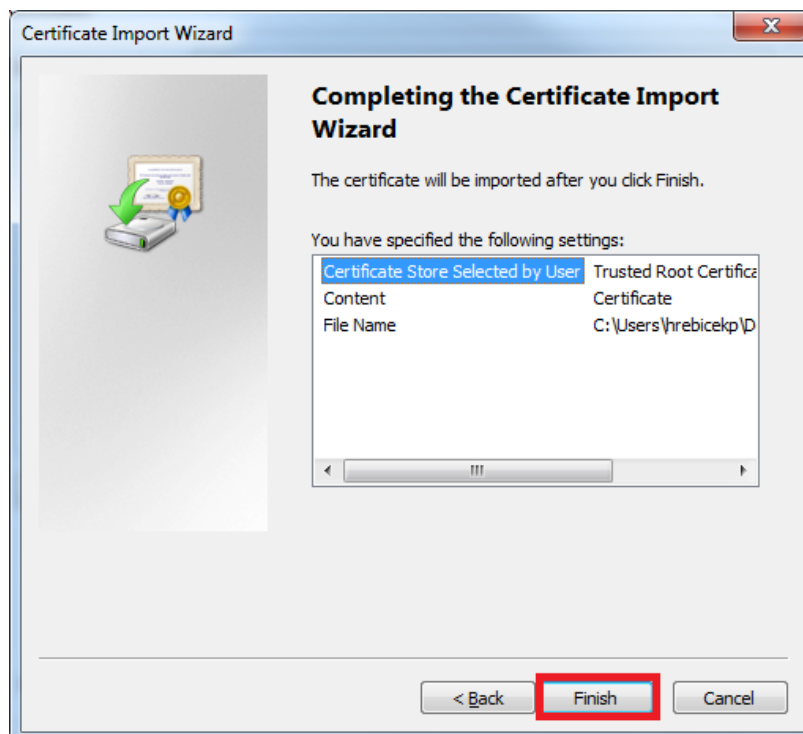
Press „Browse” button. Choose root certificate authority OTECATEST in your filesystem.



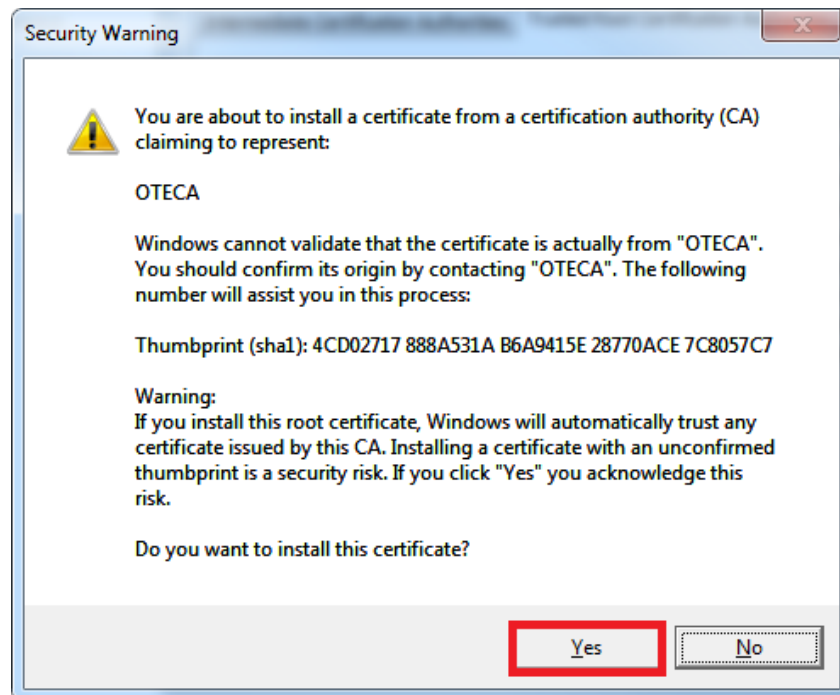
Leave setting in default state – check „Place all certificates in the following store” option.



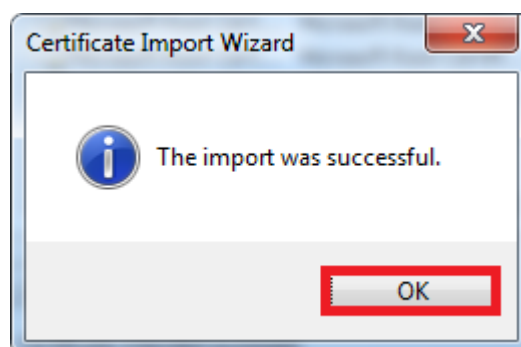
Press Finish button.



Press Yes button.



Press OK button.



If import was successful, you should see OTECATEST certificate in certificates list.

