Setting up MS Internet Explorer on Windows Vista

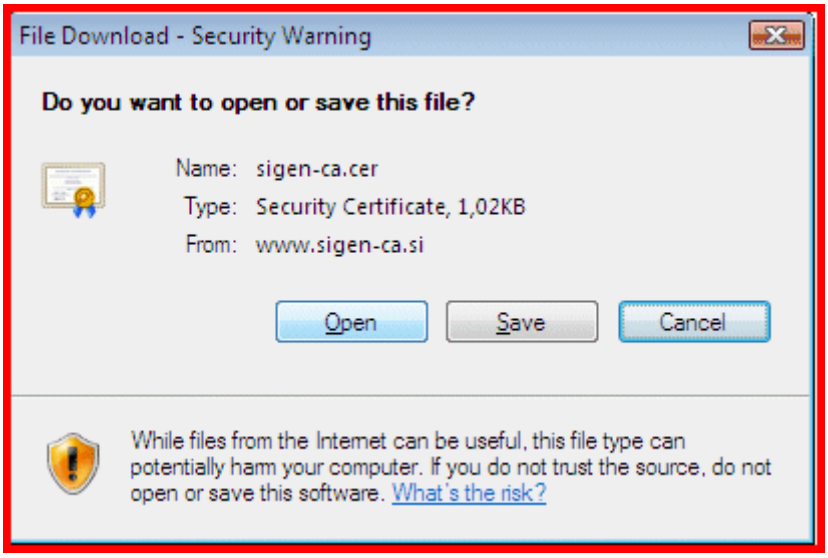
1. Installing root certificates from SIGEN-CA and SIGOV-CA, the certification authorities at the Ministry of Public Administration

The SIGEN-CA and SIGOV-CA root certificates must be installed to prevent warnings about suspicious certification authorities (CAs) when accessing public administration applications. The two certificates are not pre-installed in the browser.

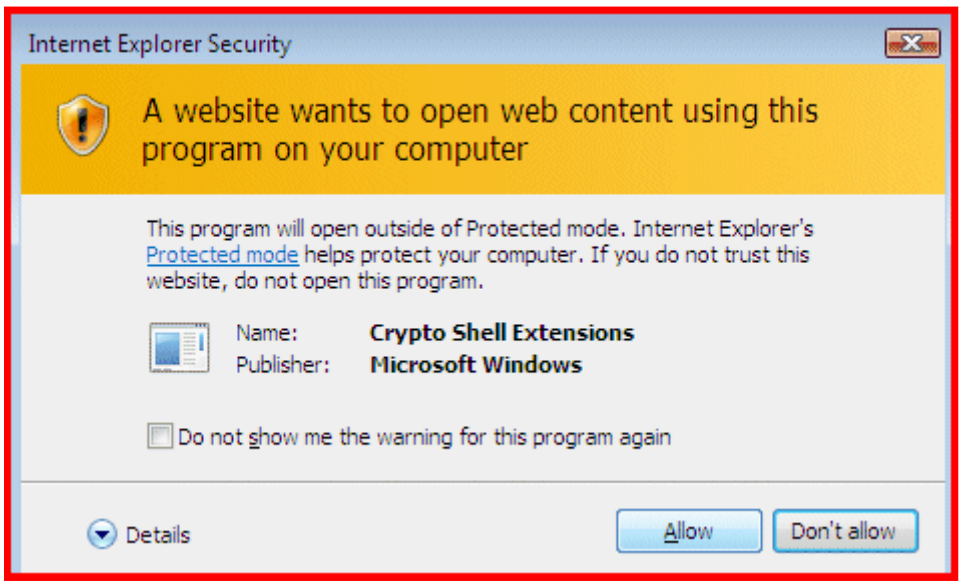
a) Installing the SIGEN-CA root certificate

Install the SIGEN-CA root certificate in the 'Trusted Root Certification Authorities' by clicking on the following link: http://www.sigen-ca.si/sigen-ca.crt.

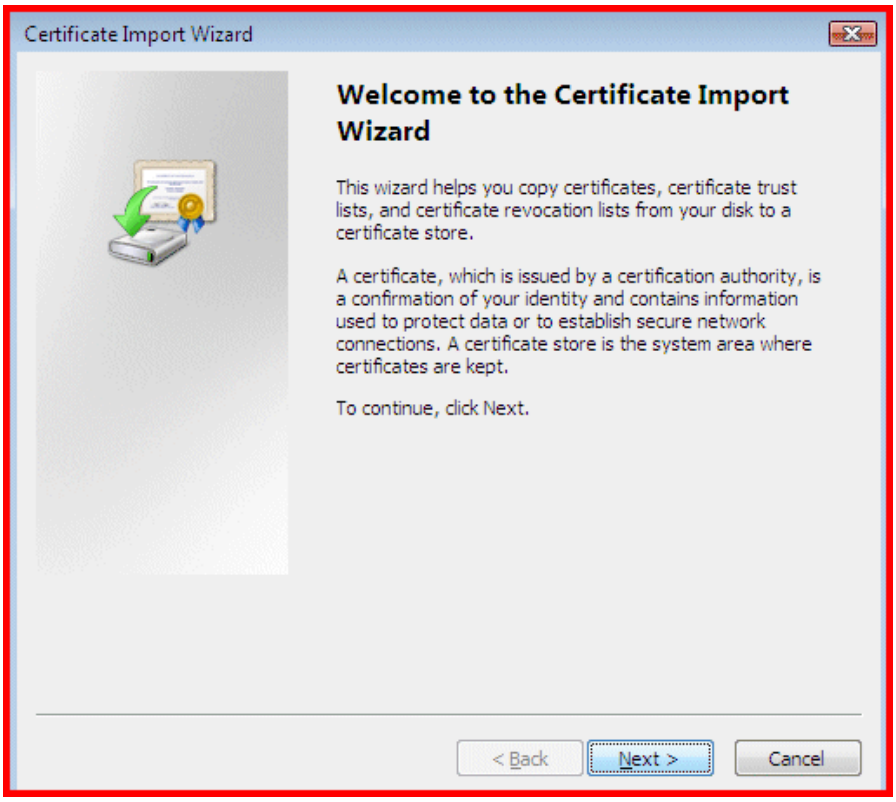
After the browser prompts you whether to Open or Save the file, click **'Open'**.



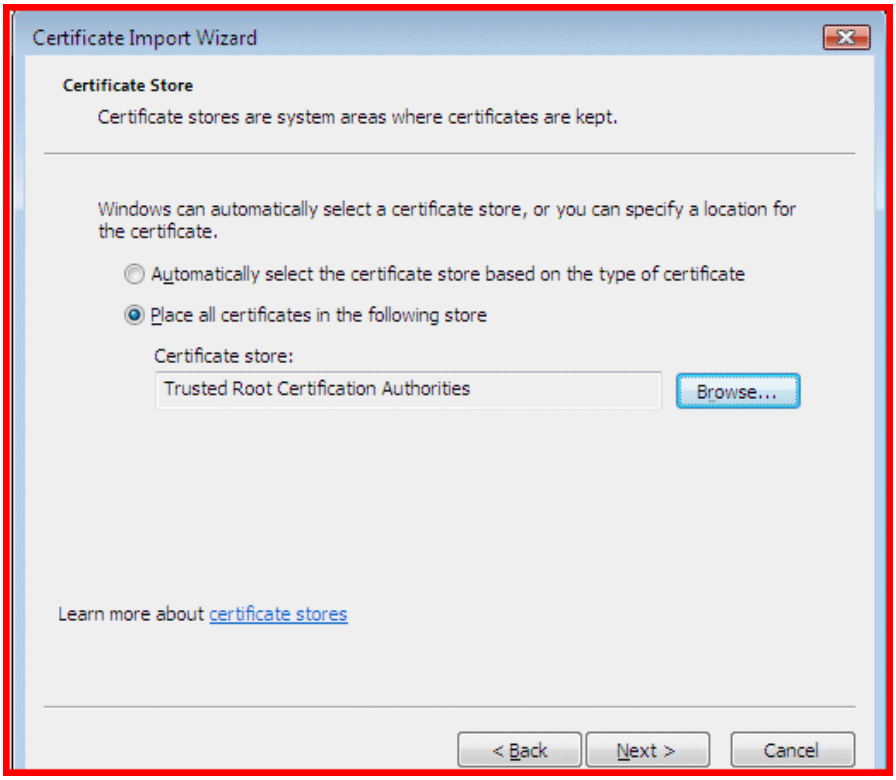
A security message appears. Click **'Allow'**.



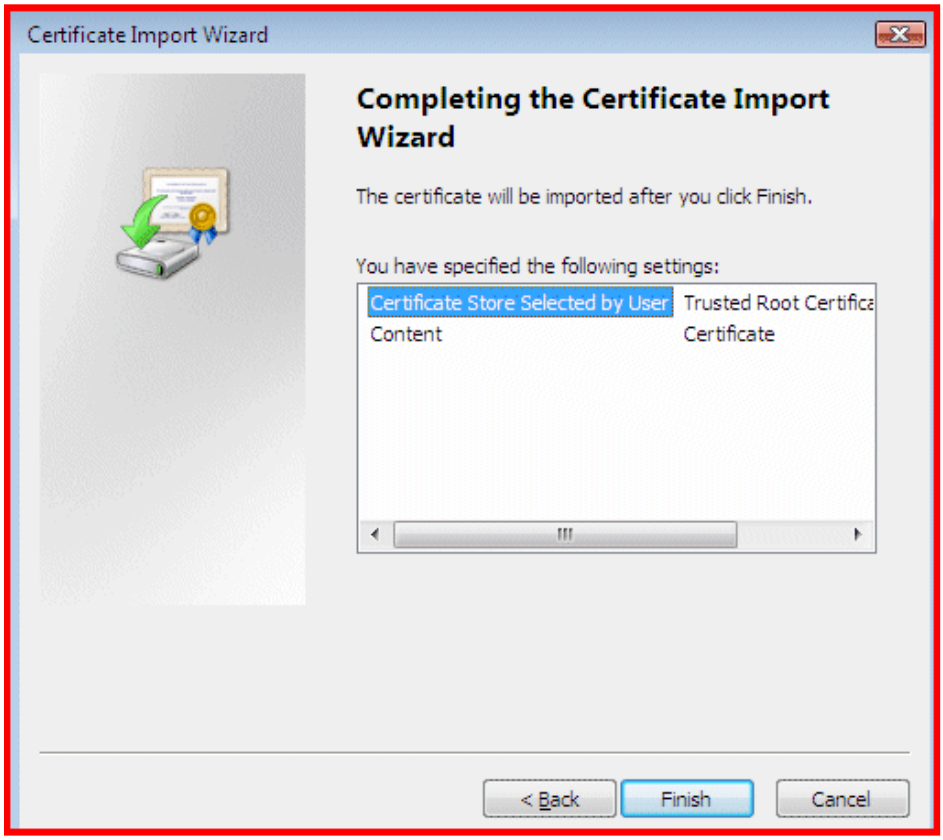
The Certificate Import Wizard is launched. Click **'Next'**.



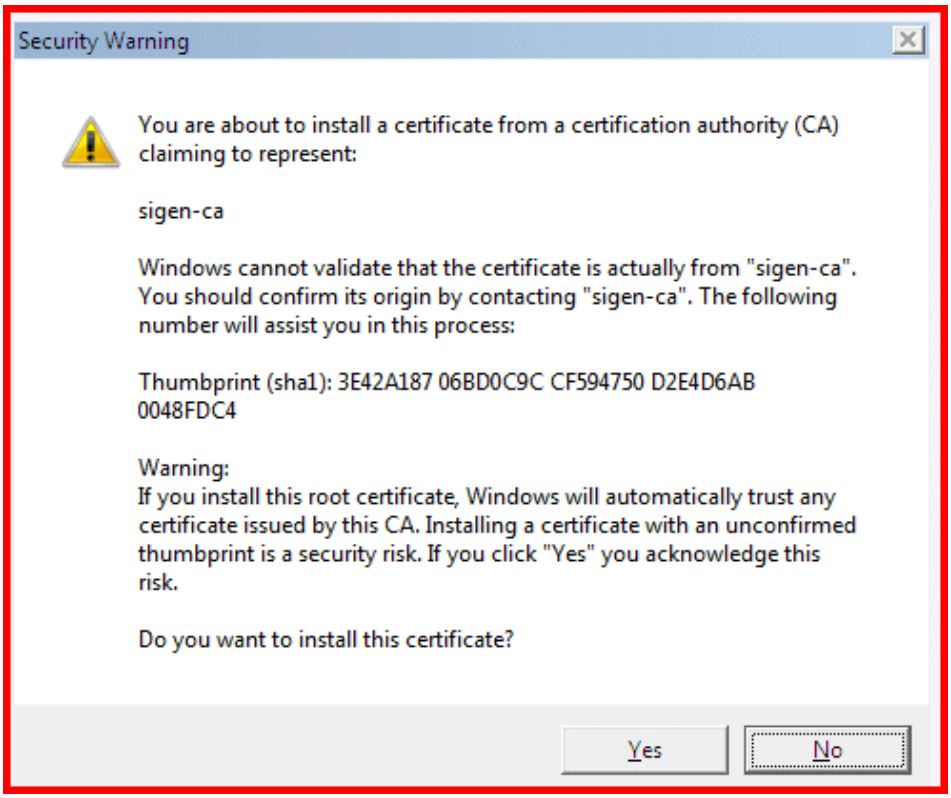
In the 'Certificate Store' window select **'Place all certificates in the following store**', then click **'Browse'** and select **'Trusted Root Certification Authorities'**. Click **'Next'**.



Complete the procedure by clicking **'Finish'**.



A security warning appears, containing information about the SIGEN-CA root certificate.



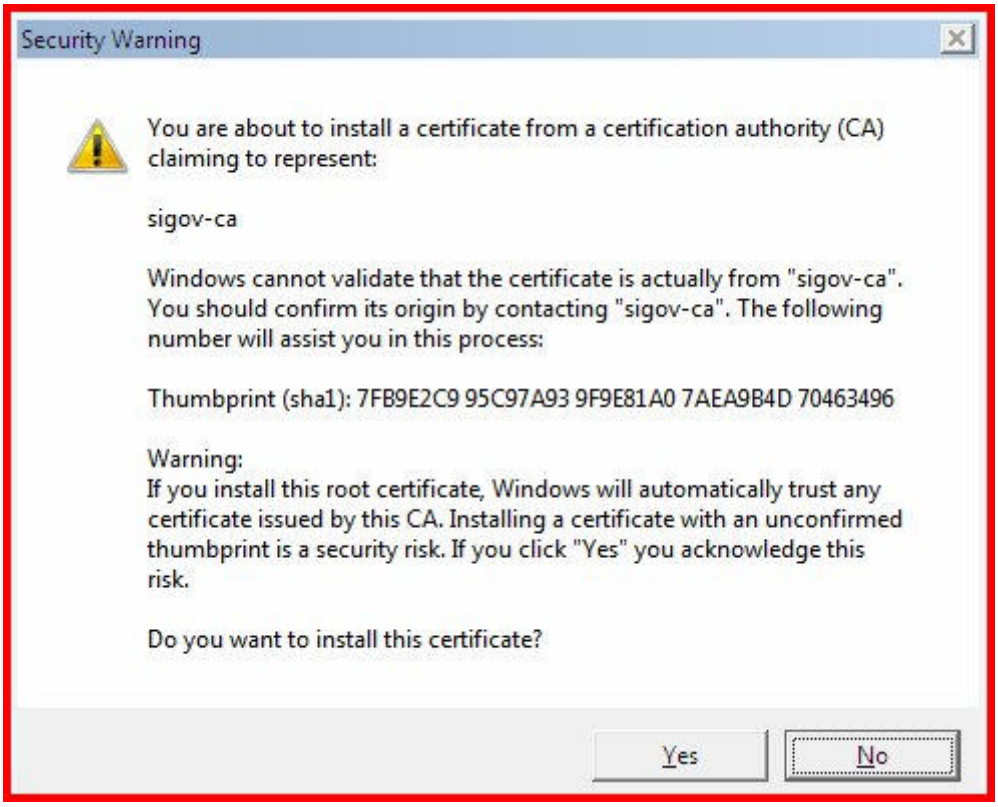
Make sure that the thumbprint (sha1) in the warning message matches the one on the picture above, i.e.:

3E42A187 06BD0C9C CF594750 D2E4D6AB 0048FDC4

After clicking **'Yes'** you will receive a confirmation the installation of the SIGEN-CA root certificate has been successful.

b) Installing the SIGOV-CA root certificate

Now install the SIGOV-CA root certificate, which issues server hostkey certificates to Government servers. The procedure is identical to installing the SIGEN-CA certificate. Begin by clicking on http://www.sigen-ca.si/sigov-ca.crt.
After the browser prompts you whether to Open or Save the file, click **'Open'**.
The Certificate Import Wizard is launched. Click **'Next'**.
In the 'Certificate Store' window select **'Place all certificates in the following store'**, then click **'Browse'** and select **'Trusted Root Certification Authorities'**. Click **'Next'**.
Confirm your selection by clicking **'Finish'**.
A security warning appears, containing information about the SIGOV-CA root certificate.

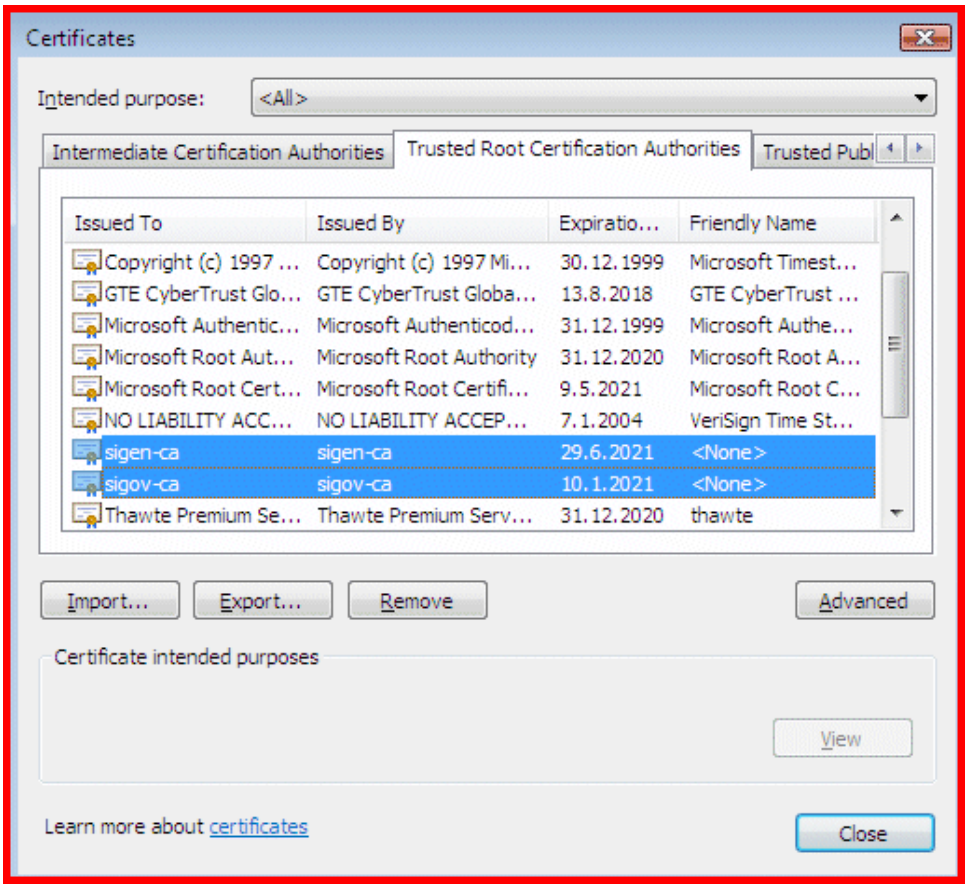


Make sure that the thumbprint (sha1) in the warning message matches the one picture above, i.e.:

7FB9E2C9 95C97A93 9F9E81A0 7AEA9B4D 70463496

After clicking **'Yes'** you will receive a confirmation the installation of the SIGOV-CA root certificate has been successful.

If you open the 'Trusted Root Certification Authorities' folder, you will see that it contains both certificates. To open the folder click **'Tools'** -> **'Internet Options'** -> **'Content'** -> **'Certificates'**.



With the certificates installed and a secure HTTPS connection established to any server that uses a digital certificate from the certification authorities at the Ministry of Public Administration, the URL bar should be white and without warnings.

If this does not happen, close and reopen the web browser, so that it identifies the two new certificates as trusted.

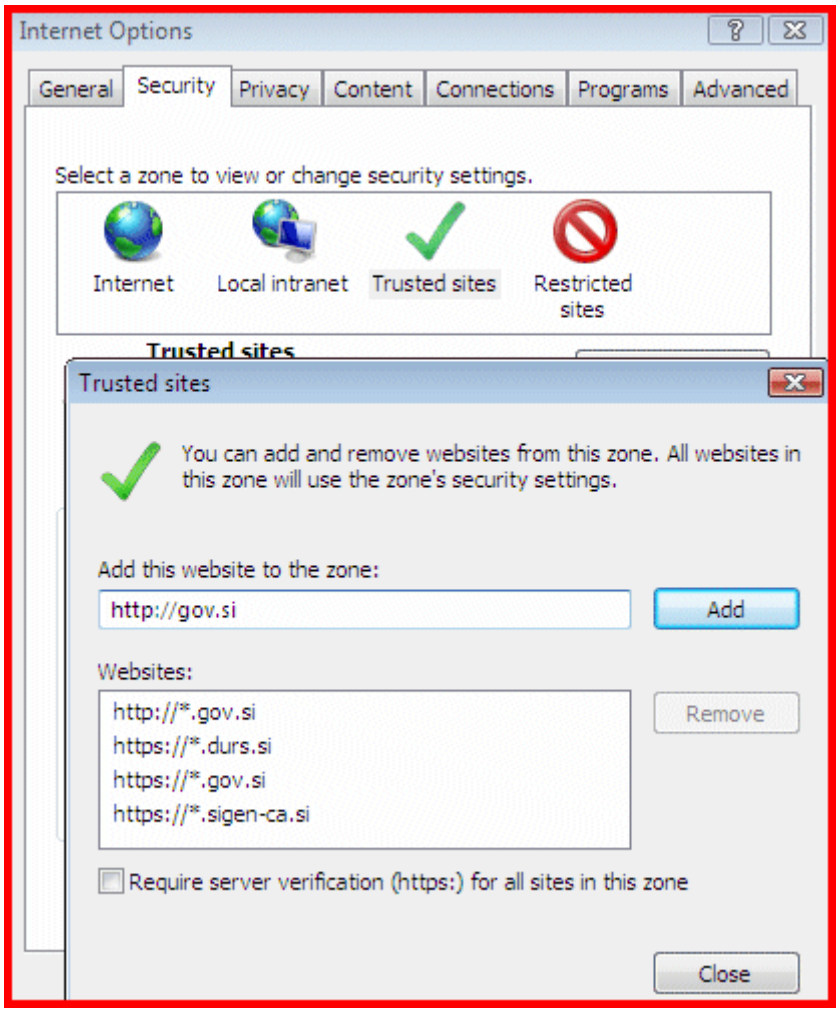
2. Making the e-Uprava web site a trusted site

In the menu select **'Tools'** -> **'Internet Options'** -> **'Security'**

In the 'Trusted Sites' tab select **'Sites'**, and add the addresses of e-Uprava servers you wish to access. We recommend you to add the following URLs:

- https://gov.si (displayed as an additional domain https://*.gov.si)
- https://sigen-ca.si
- https://durs.si

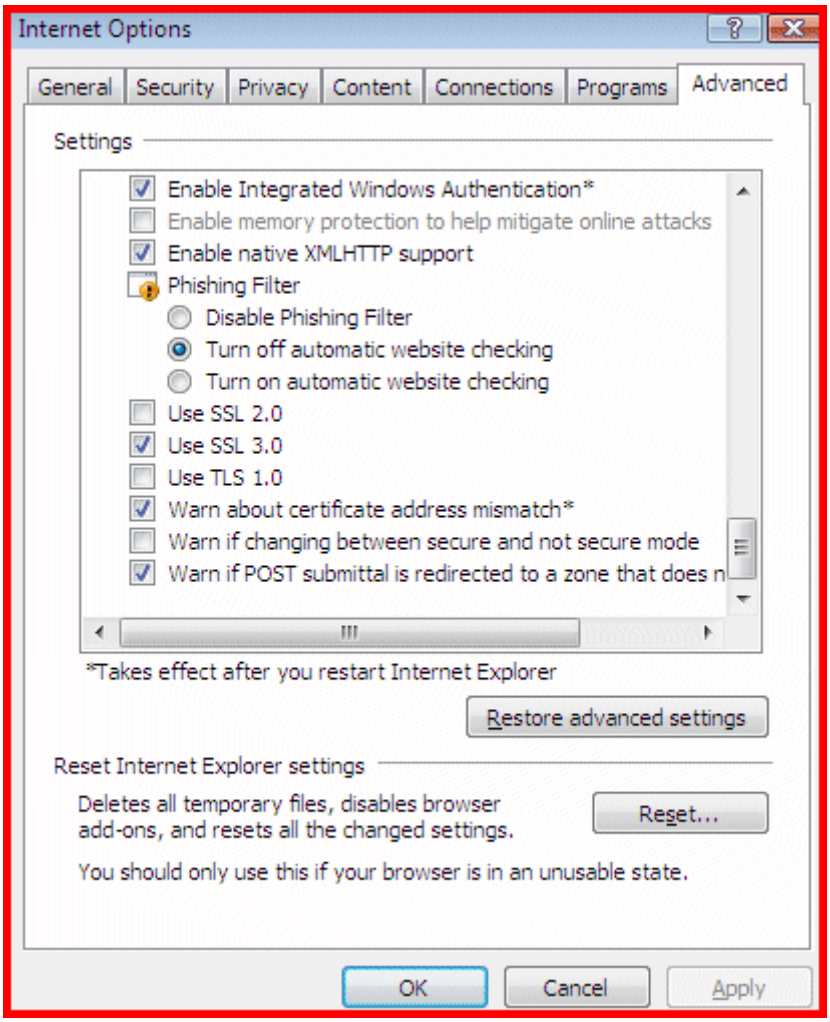
We also recommend you to add http://gov.si (displayed as http://*.gov.si), to avoid annoying browser warning messages when the connection is switched between http and https. To do this, first uncheck the box at the bottom ('Require server verification (https:) for all sites in this zone'). Once you have added the URL http://gov.si, check the box so as to prevent the possibility of unintentionally adding unverified servers among trusted ones.



3. Protocol settings

In the menu select **'Tools'** -> **'Internet Options'** -> **'Advanced'**

Uncheck the box next to 'Use TLS 1.0' and click **'OK'**.



This setting prevents the browser from using the above-mentioned protocol, which some e-Uprava servers do not support.