THE USAGE OF ELECTRONIC CERTIFICATE

ON THE REGIONAL BOOKING PLATFORM,

TRADING PLATFORM,

AND FGSZ'S INFORMATION PLATFORM

1 October 2018

Version 2.4

Prepared by: FGSZ Ltd
Sales and Customer Support

FGSZ Ltd is committed to improve information security and maintaining a high level of its security standards. The Regional Booking Platform (RBP), Trading Platform (TP) and FGSZ's Information Platform (IP) supports the title-based access of System Users to the services implemented with WEB technology, on an up-to-date, convenient technical basis.

An appropriately issued and used electronic certificate is an indispensable precondition of becoming an active user of the abovementioned IT applications.

1. The notion of electronic certificate

The electronic certificate is an "electronic document", issued by a trusted service provider (TSP) organisation in order to prove the authenticity of a document sent by the owner of the electronic certificate via non-secured networks, and identify the sender credibly during data communications initiated by them.

2. General

The electronic certificate is an electronic code pair (key pair), comprising of a secret (private or signatory) and a public key. The secret key is possessed by the owner of the electronic certificate, no one else can have access to it (non-transferable), while the public key is accessible for anyone.

The electronic signature created with the secret and public key pair belonging to the electronic certificate can be used to encrypt documents, messages and network data communication. This type of encrypting process is called public key encrypting technology, while the different procedures, organisations and equipment collectively are called Public Key Infrastructure (PKI).

If a document or data connection is encoded with the signatory (secret) key, it can be decoded only with the public key belonging to the secret key, whilst we can be sure of the identity of the sender.

3. Requirements regarding the electronic certificate

There are several types of electronic certificates. The one necessary to access the Regional Booking Platform, Trading Platform and FGSZ's Information Platform should meet the below criteria:

- Issued by an external trusted service provider company authenticated for the issuance of electronic certificates
- The trusted service provider issues the electronic certificate after the examination of the natural or legal person's identity. The issued electronic certificate must be suitable for identifying the user, being it a natural or legal person.
- Registration of the electronic certificate within the platforms.
- The electronic certificate must comply with the below technical criteria in order to authenticate the user:
    - **Version**: v3
    - **Signature algorithm:** sha256RSA
    - **Signature hash algorithm:** sha256 (SHA1 not supported)
    - **Public key:** RSA, minimum 2048 Bits (e.g. ECC (384 Bits) is not supported)
    - **Issuer:** trusted (third-party) certificate issuer with a publicly accessible CRL list. Internally issued electronic certificates are not supported.
    - **Valid:** at least 1 year expiration period (or more)
    - **Key Usage:** Digital Signature (80)
    - **Enhanced Key Usage:** Client Authentication
    - **Serial number:** Certificate must have a unique serial number at the CA
    - **Subject E field and/or Subject Alternative Name (RFC822 Name)**: has to include your valid email address which the certificate was issued for. Certificates including host name values (DNS HOSTNAME) are not supported.
    - The entire certificate chain must be present (root and intermediate certificates)

Important notice:

The real e-mail address in the "E" attribute within the "owner" field of the electronic certificate, or in the alternative name filed is mandatory.

In order to maintain system security these applications do not support the use of multiple electronic certificates having the same e-mail address. The application operator is entitled to refuse new electronic certificates if the email address in the "E" field has already been registered in the system.

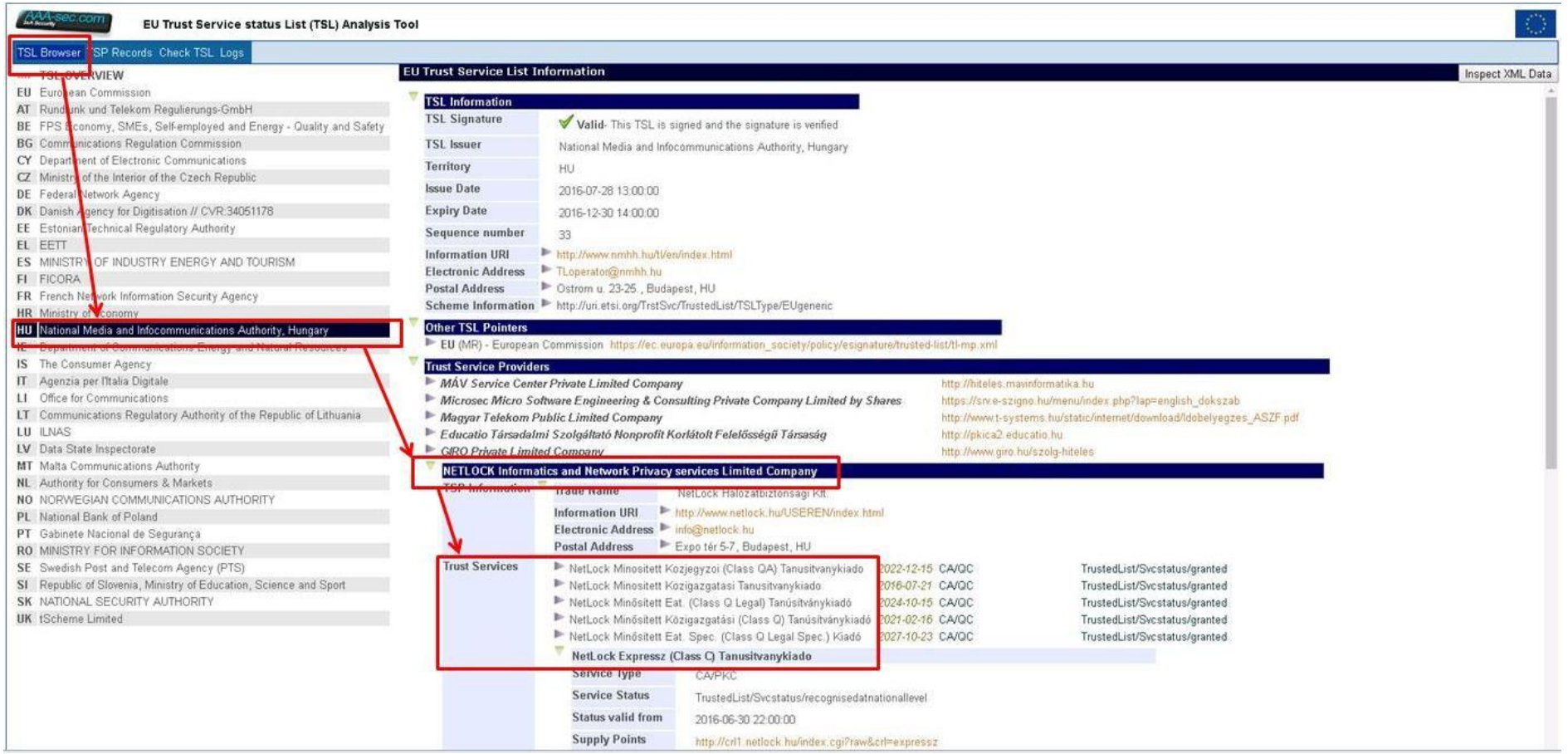
In case of natural persons using a corporate certificate on behalf of a legal person, the natural person users' responsibility of using a corporate certificate shall be exclusively governed by the relevant laws and internal corporate regulations applicable between the natural person and the legal person. In respect of such legal relationship, FGSZ Ltd

excludes in any case all liability and responsibility whatsoever in connection with the use of corporate certificates. Corporate certificates may be used for automated data exchange (server-server connection). Such technical user profiles related to corporate certificates are approved by the head of the organization responsible for the RBP customer support.

4 Obtaining an electronic certificate

The electronic certificate can be obtained from a certified organisation authenticated to issue electronic certificates (Trusted Service Provider – TSP), which is contained in one of the national trusted service provider lists of the EU Trusted Lists of Certification Service Providers, maintained by the responsible authority of the given Member State according to Regulation 910/2014/EU. The EU Trusted Lists of Certification Service Providers, containing the address of the national lists can be found under the following link: eIDAS Dashboard (europa.eu)

The following external tool may be of help in determining whether a certificate provider is a trusted service provider: **EU Trust Service status List (TSL) Analysis Tool** (see an example below for the check of an electronic certificate)



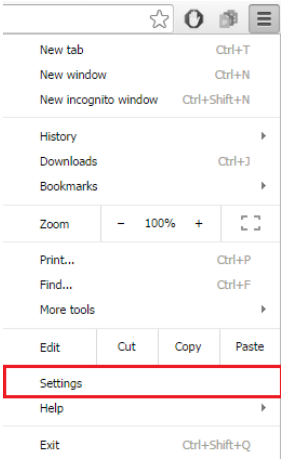
In case of newly registering users, service providers outside of one of the abovementioned national lists are not accepted from 1 July 2016 onwards.

The secret key of the electronic certificate must not be transferred or handed over.

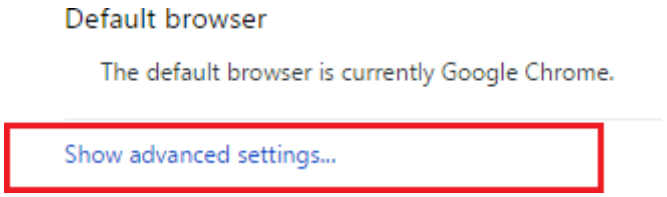
5. Installing the electronic certificate to the user's computer

The electronic certificate should be installed on your computer as follows:

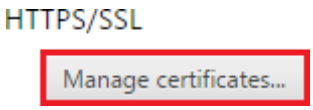
a. Using Google Chrome
   - Customize and control menu (1. step)
   - Settings submenu (2. step)
   - Show advanced settings (3. step)
   - Manage certificates (4. step)
   - Personal tab (default) (5. step)
   - Import button (6. step)
   - Next button (7. step)
   - Next button (8. step)
   - Type password (9. step)
   - Next button (10. step)
   - Certificate Store: the selected radio button by default is appropriate: "Automatically select the certificate storage…") (11. step)
   - Next button (12. step)
   - Finish button (13. step)



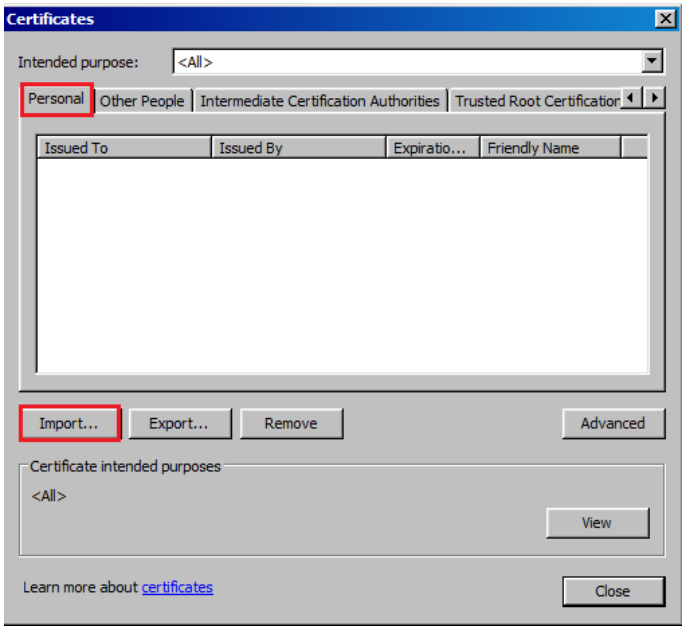
1-2. step



3. step

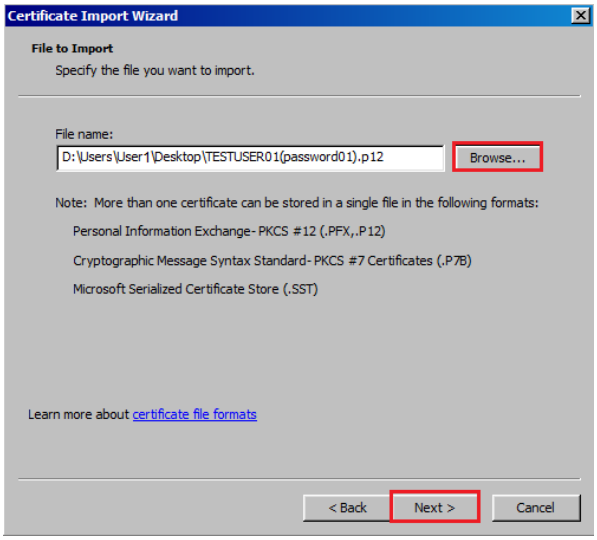


4. step

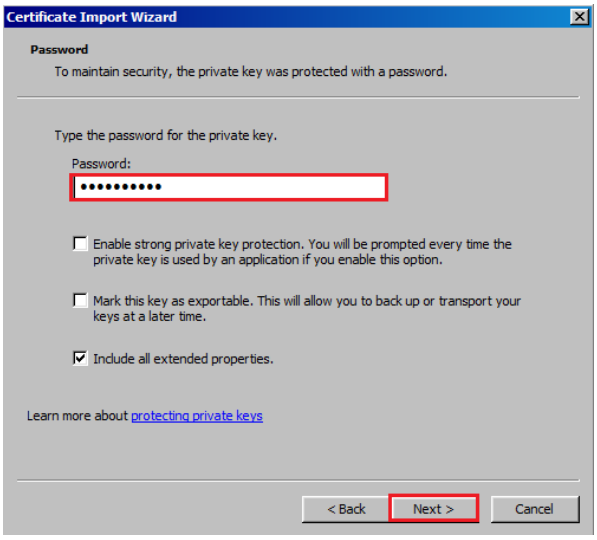


5.-6. step

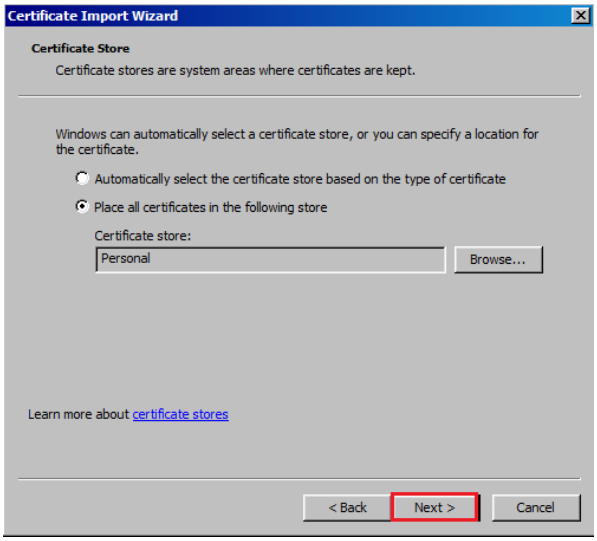
7. step



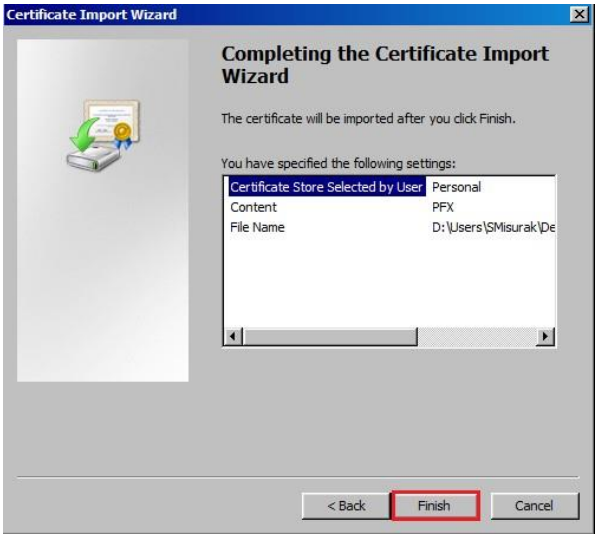
8. step



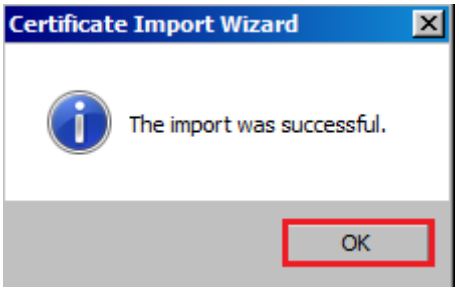
9.-10. step



11. step



12. step



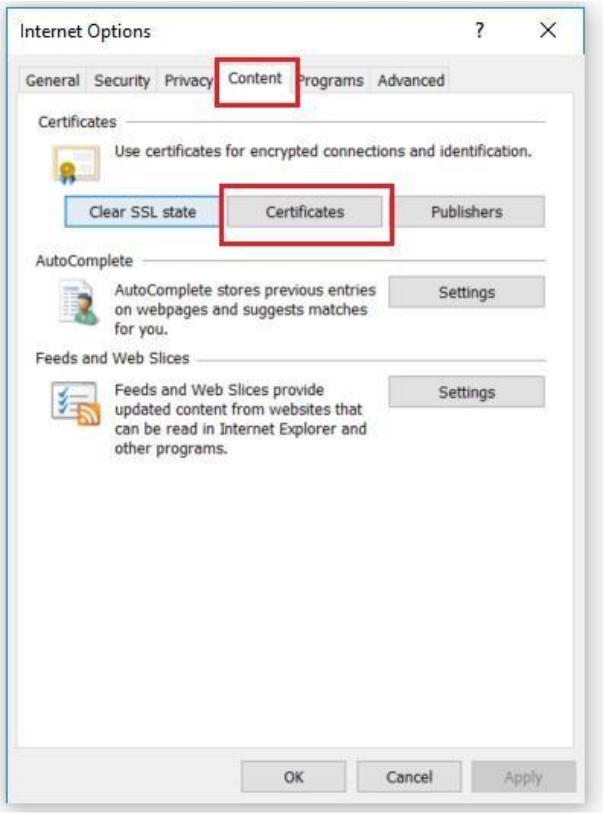
13. step

6. Extracting the public part (*.cer file) to the electronic certificate from the browser

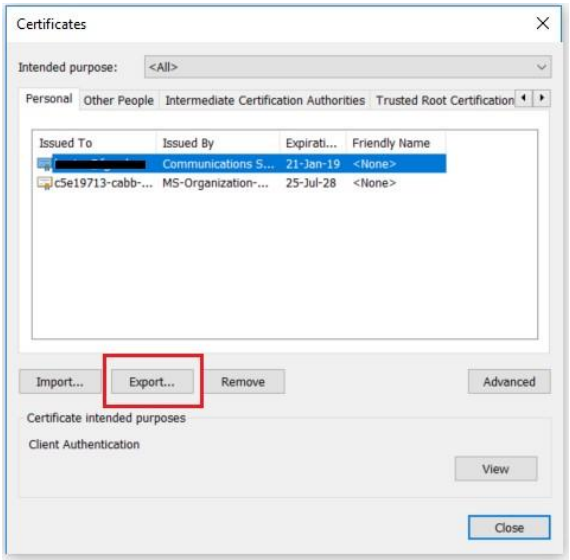
You can extract the public part (*.cer) file of your electronic certificate following the below steps:

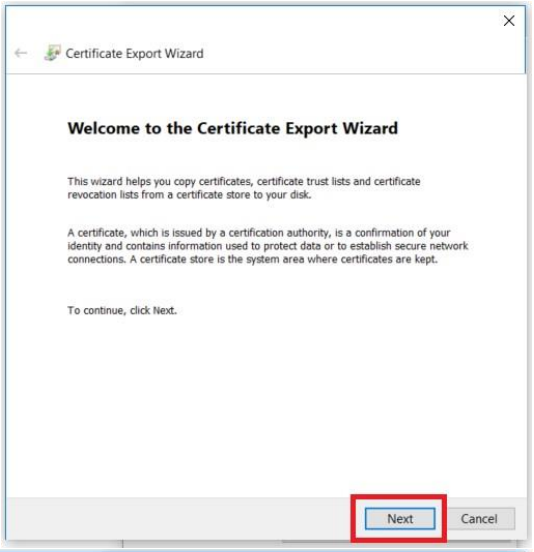
- Follow the path from “Tools” ➔ Internet options ➔ Content ➔ Certificates (Step 1)
- Select the required certificate, then click on “Export” (Step 2)
- The Certificate Export Wizard starts up. Click on “Next” (Step 3)
- Select “No, do not export the private key” (Step 4)
- Select „Base64 encoded X.509(.CER)” (Step 5)
- Save the *.cer file to your computer (Step 6)

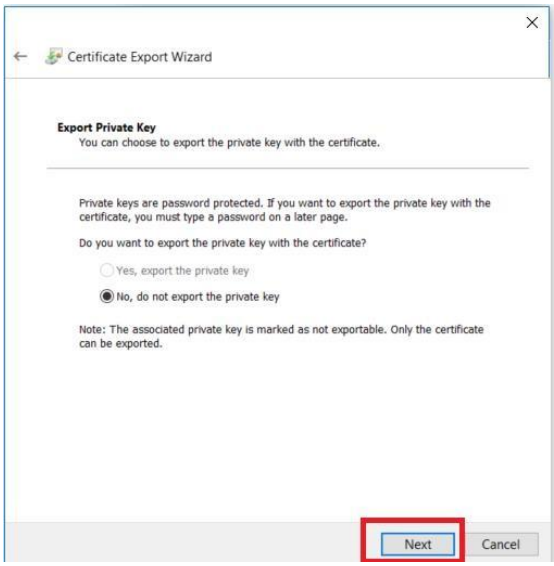
Step 1

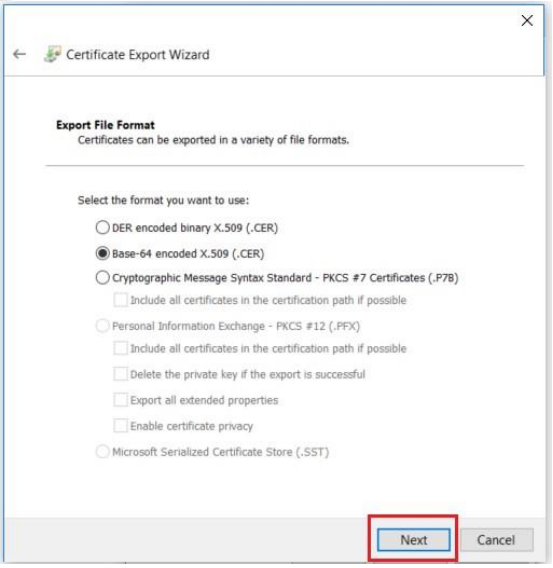


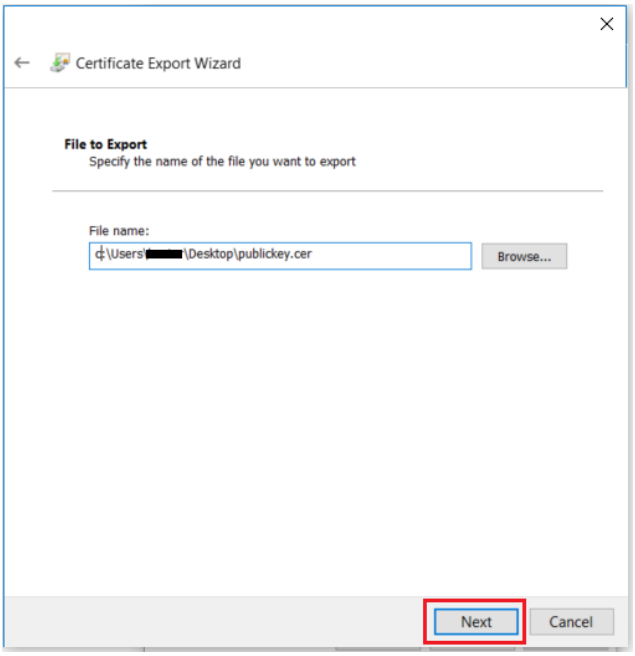
Steps 2-6


Certificates
Intended purpose:
<All>
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification
Issued To
Issued By
Expirati...
Friendly Name
Communications S...
21-Jan-19
<None>
c5e19713-cabb-...
MS-Organization-...
25-Jul-28
<None>
Import...
Export...
Remove
Advanced
Certificate intended purposes
Client Authentication
View
Close


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.
Next
Cancel


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 is marked as not exportable. Only the certificate can be exported.
Next
Cancel

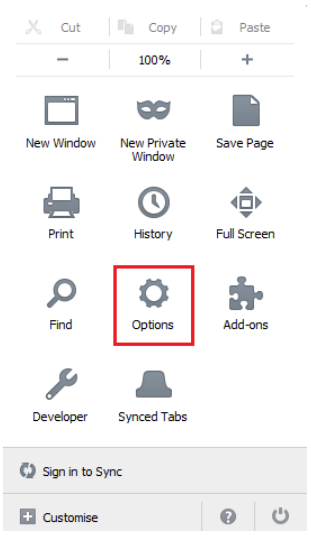

Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification 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
Enable certificate privacy
Microsoft Serialized Certificate Store (.SST)
Next
Cancel


Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
C:\Users\[redacted]\Desktop\publickey.cer
Browse...
Next
Cancel

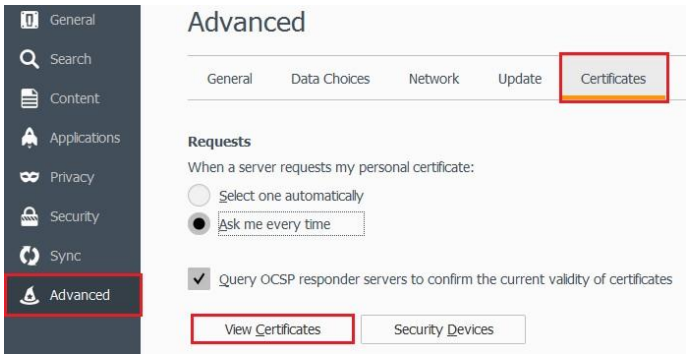
7. Uninstalling the electronic certificate

In order to avoid misuse of electronic certificates, the installed electronic certificate must be uninstalled if you do not wish to use it any more (in case of e.g. position change, computer change, etc.). It is also advised to uninstall the certificate from a computer you installed it on temporarily.

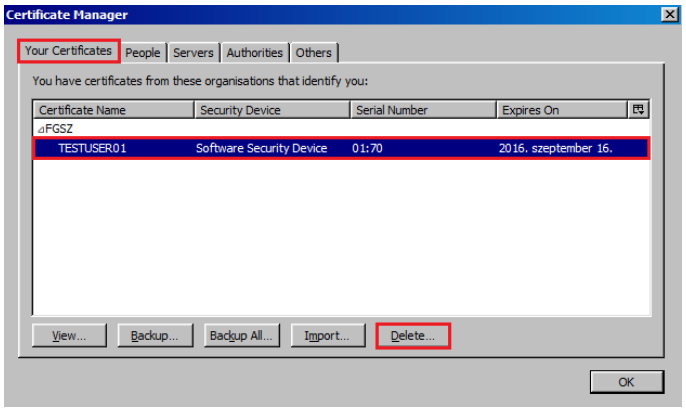
a. To uninstall the following steps need to be done using Firefox:
- Options menu (1. step)
- Options submenu (2. step)
- Advanced icon (3. step)
- Certificates tab (4. step)
- View Certificates button (5. step)
- Your Certificates tab (default) (6. step)
- Choose the required certificate (7. step)
- Delete… button (8. step)
- OK button (9. step)



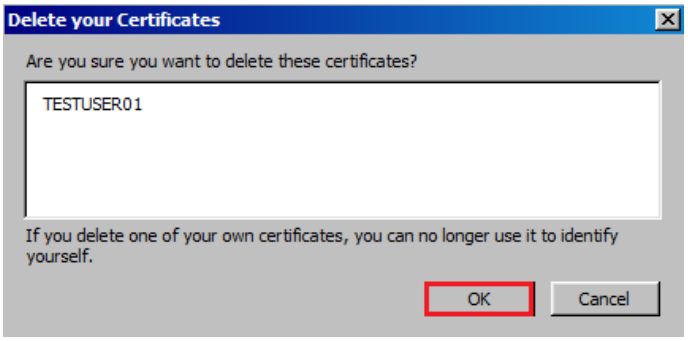
1.-2. step



3.-4.-5. step



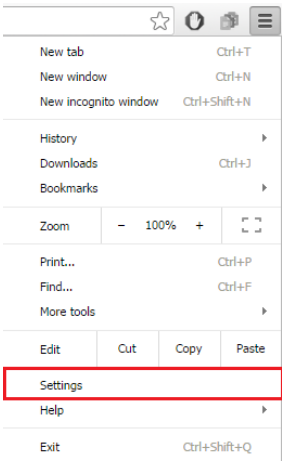
6.-7.-8. step



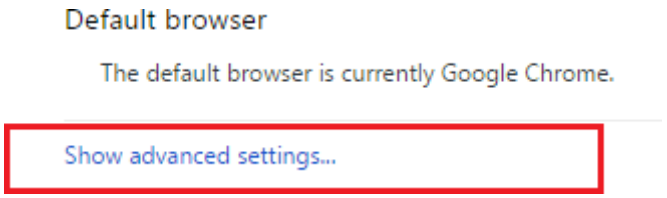
1. step

b. To uninstall the following steps need to be done using Google Chrome:

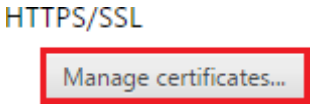
- Customize and control menu (1. step)
- Settings submenu (2. step)
- Show advanced settings (3. step)
- Manage certificates (4. step)
- Personal tab (default) (5. step)
- Select the certificate (6. step)
- Remove button (7. step)
- OK button (8. step)



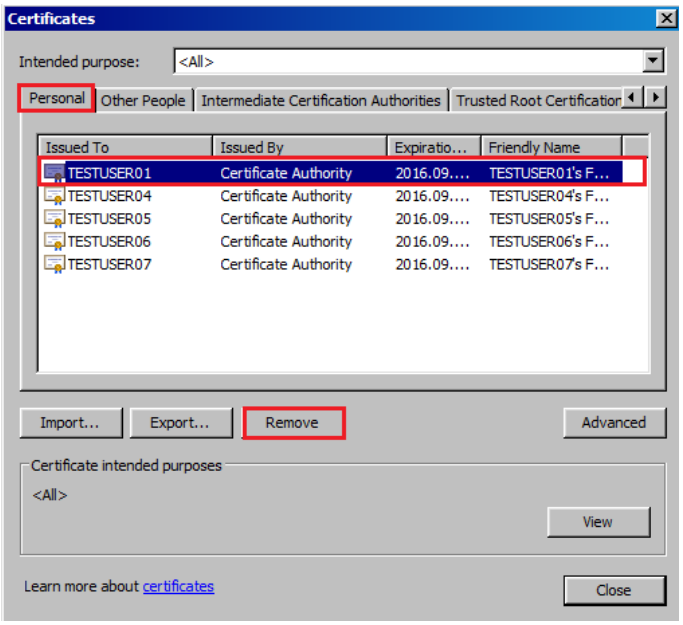
1.-2. step



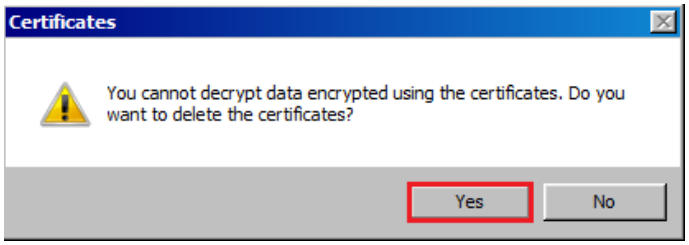
3. step



4. step



5.-6.-7. step



8. step

8. Using the electronic certificate

If one electronic certificate has been installed, the system enters the user immediately when logging on to the Regional Booking Platform,

If more than one electronic certificate was installed, a pop-up window - in which all the installed certificates are shown - will appear for choosing from the certificates the one you wish to use on the Regional Booking Platform.

9. Lost or stolen computer

In case you lose your computer or it gets stolen, you are kindly asked to report it immediately during working hours at support@rbp.eu, out of working hours to the colleagues on duty, and to one of the contact persons listed in the Regional Booking Platform User Agreement in order to prevent any misuse.

10. Dealing with frequent errors

The following types of errors occur generally:

- the electronic certificate (private key) is not installed properly on the user's computer

  Error: The window for choosing the certificate does not appear, or it appears but the list does not contain the required certificate when entering the Regional Booking Platform, the login is unsuccessful.

  To do: Check the status of the certificate according to point 11. If the electronic certificate is not installed, it should be installed according to point 5, and then it is advised to check if it was successful according to point 11. If the electronic certificate is included in the list of installed certificates, its validity should be checked, see "electronic certificate expired" section below.

- the public key is not installed on the FGSZ servers

  Error: When entering the Regional Booking Platform an error message indicates contact failure, login is unsuccessful.

  To do: Unsuccessful login should be reported to one of the contact persons listed in point 6, who will check the existence of the given public key on the FGSZ servers and will help with the further steps.

- the electronic certificate expired

  Error: The window for choosing the certificate does not appear, or it appears but the list does not contain the required certificate when entering the Regional Booking Platform, the login is unsuccessful.

  To do: Check the data in the certificate according to point 11, with special regard to the validity of the certificate. If it expired, the certificate can be renewed at the issuing trusted service provider or a new certificate can be applied for at another trusted service provider.

If you want to use other business applications of FGSZ e.g. the Informatic Platform (IP), or the Trading Platform (TP).

- the electronic certificate does not contain an e-mail address in the required field

  Error: The window for choosing the certificate appears when logging on to the Regional Booking Platform, however it is not possible to enter the system with the chosen certificate.

  To do: Check if the certificate was successfully installed according to point 10, with special regard to the e-mail address.

- the e-mail address is incorrect in the required field

  Error: The window for choosing the certificate appears when logging on to the Regional Booking Platform, however it is not possible to enter the system with the chosen certificate.

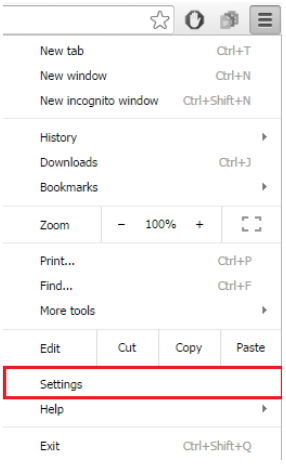
  To do: Check the data of the certificate according to point 10, with special regard to the e-mail address. If it does not correspond with the e-mail address provided in the application submitted to the issuing trusted service provider, it has to be modified by the issuing trusted service provider.

11. Verifying the electronic certificate

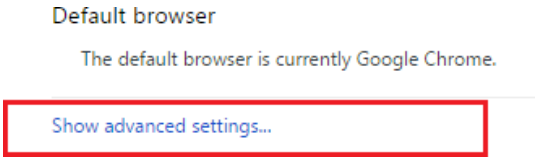
Verifying the data of the installed electronic certificates provides an opportunity to eliminate several problems. If you call in the aid of an RBP Operator, the following data shall be necessary in order to overcome the problem.

Steps to follow during checking:

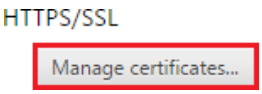
a. Using Google Chrome
   - Customize and control menu (1. step)
   - Settings submenu (2. step)
   - Show advanced settings (3. step)
   - Manage certificates (4. step)
   - Personal tab (default) (5. step)
   - Select the certificate (6. step)
   - View button (7. step)
   - General tab (default): Validity and expiry date shown
   - Details tab: Issuing organisation, Start of validity, Expiry date, Owner, e-mail address (“E” field) shown



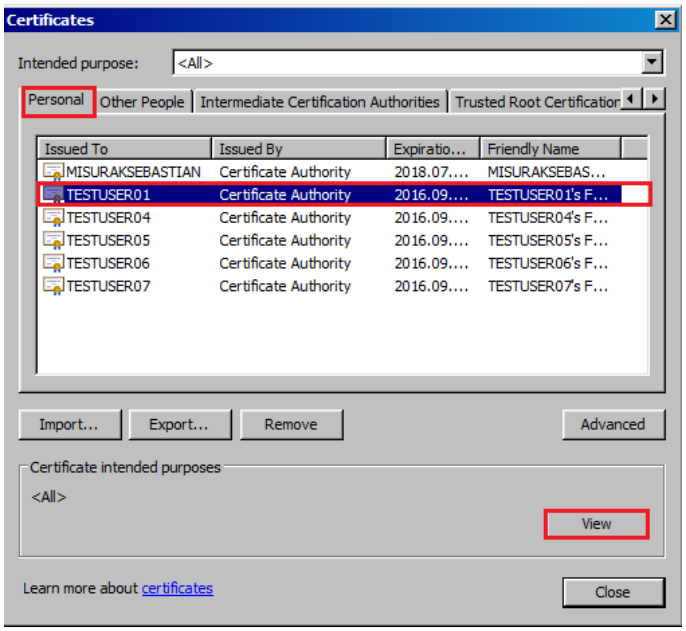
1-2. step



3. step



4. step


Certificates
Intended purpose:
<All>
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification
Issued To
Issued By
Expiratio...
Friendly Name
MISURAKSEBASTIAN
Certificate Authority
2018.07....
MISURAKSEBAS...
TESTUSER01
Certificate Authority
2016.09....
TESTUSER01's F...
TESTUSER04
Certificate Authority
2016.09....
TESTUSER04's F...
TESTUSER05
Certificate Authority
2016.09....
TESTUSER05's F...
TESTUSER06
Certificate Authority
2016.09....
TESTUSER06's F...
TESTUSER07
Certificate Authority
2016.09....
TESTUSER07's F...
Import...
Export...
Remove
Advanced
Certificate intended purposes
<All>
View
Learn more about certificates
Close

5.-6.-7. step


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All application policies
Issued to: TESTUSER01
Issued by: Certificate Authority
Valid from 2013. 09. 17. to 2016. 09. 16.
You have a private key that corresponds to this certificate.
Issuer Statement
Learn more about certificates
OK