THE USE OF ELECTRONIC CERTIFICATE

ON THE REGIONAL BOOKING PLATFORM

1 July 2016

Version 2.2

Prepared by: FGSZ Ltd
Information and Communication Technology
Process Control

FGSZ Ltd is committed to improving information security and maintaining a high level of its standard. The Regional Booking Platform (RBP) 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 condition of your becoming one of the active users of our informatical system.

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 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 person’s identity. The issued electronic certificate must be suitable for identifying a user.
- Public key of the electronic certificate must be registered on the RBP Portal. Furthermore, it must be sent together with the electronic certificate in Base64-coded format (without the secret key) via email to the rbp@fgsz.hu address.
- The electronic certificate must comply with the below technical criteria in order to authenticate the user:

Extension	Content	OID	Criticality	Field indication	Source
Key Usage	Digital signature, and/or Key Agreement	-	critical	mandatory	RFC 5280
Extended Key usage	Client Authentication	1.3.6.1.5.5.7.3.2	non-critical	recommended	

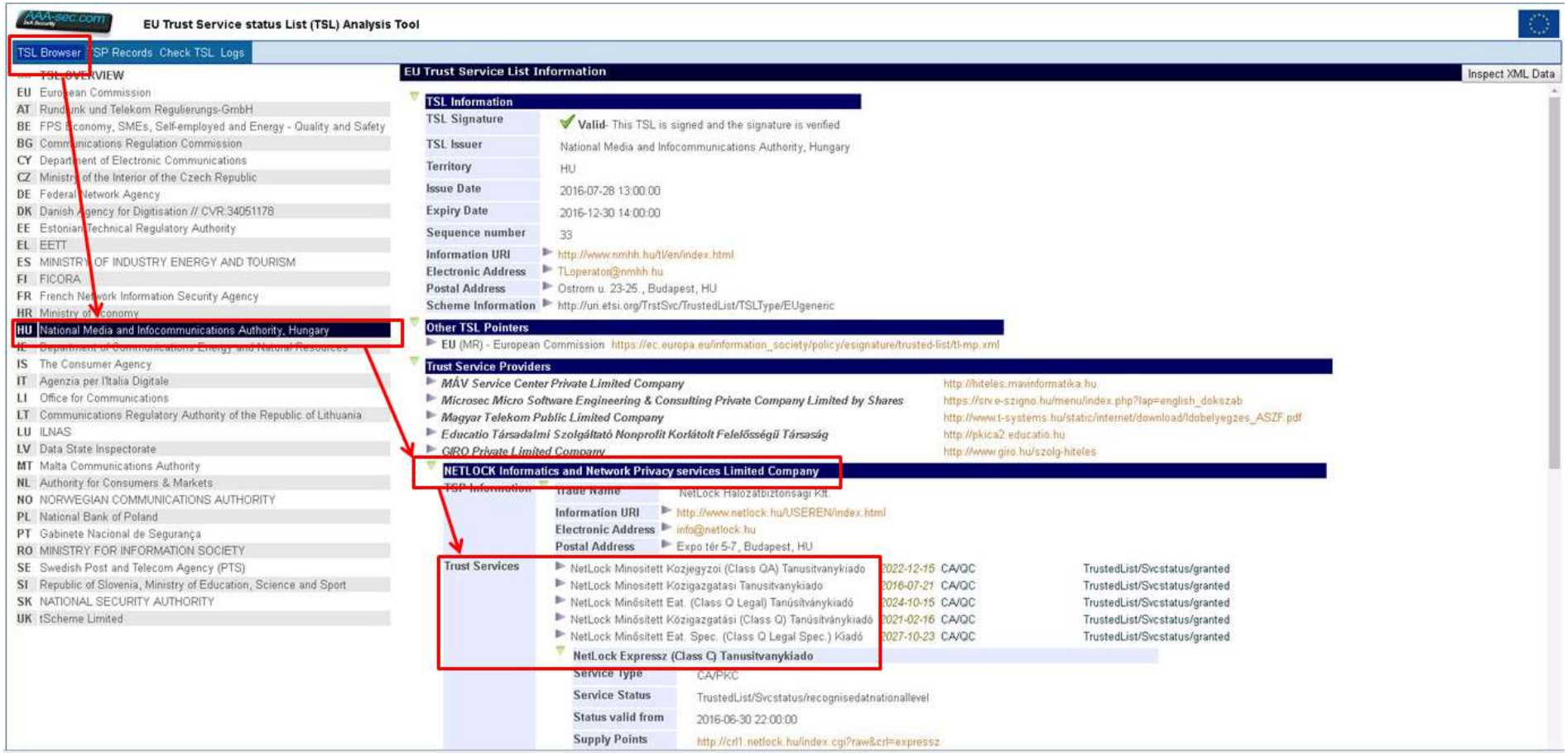
Important notice:

If you want to use other business applications of FGSZ e.g. eIP, EP, too, 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 electronic certificates having the same e-mail address. The application operator is entitled to refuse new electronic certificates if the address in the “E” field has already been registered in the system.

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: https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-certification-service-providers.

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 above mentioned national lists are not accepted from 1 July 2016 onwards.

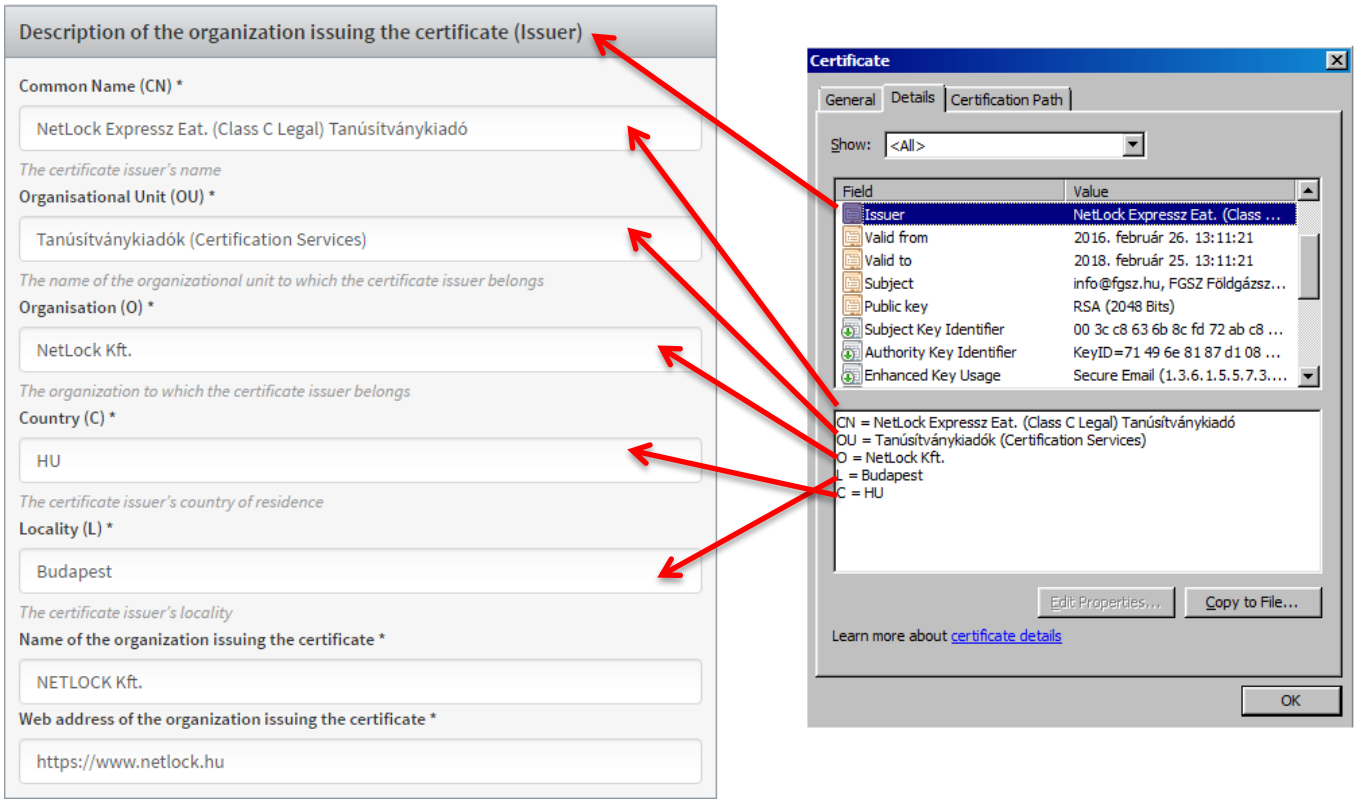
Already registered users having an electronic certificate issued by a service provider outside of the national lists will be accepted until 1 January 2017 by the RBP Operator. These users shall use a new certificate from this date onwards complying with the above mentioned rules.

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

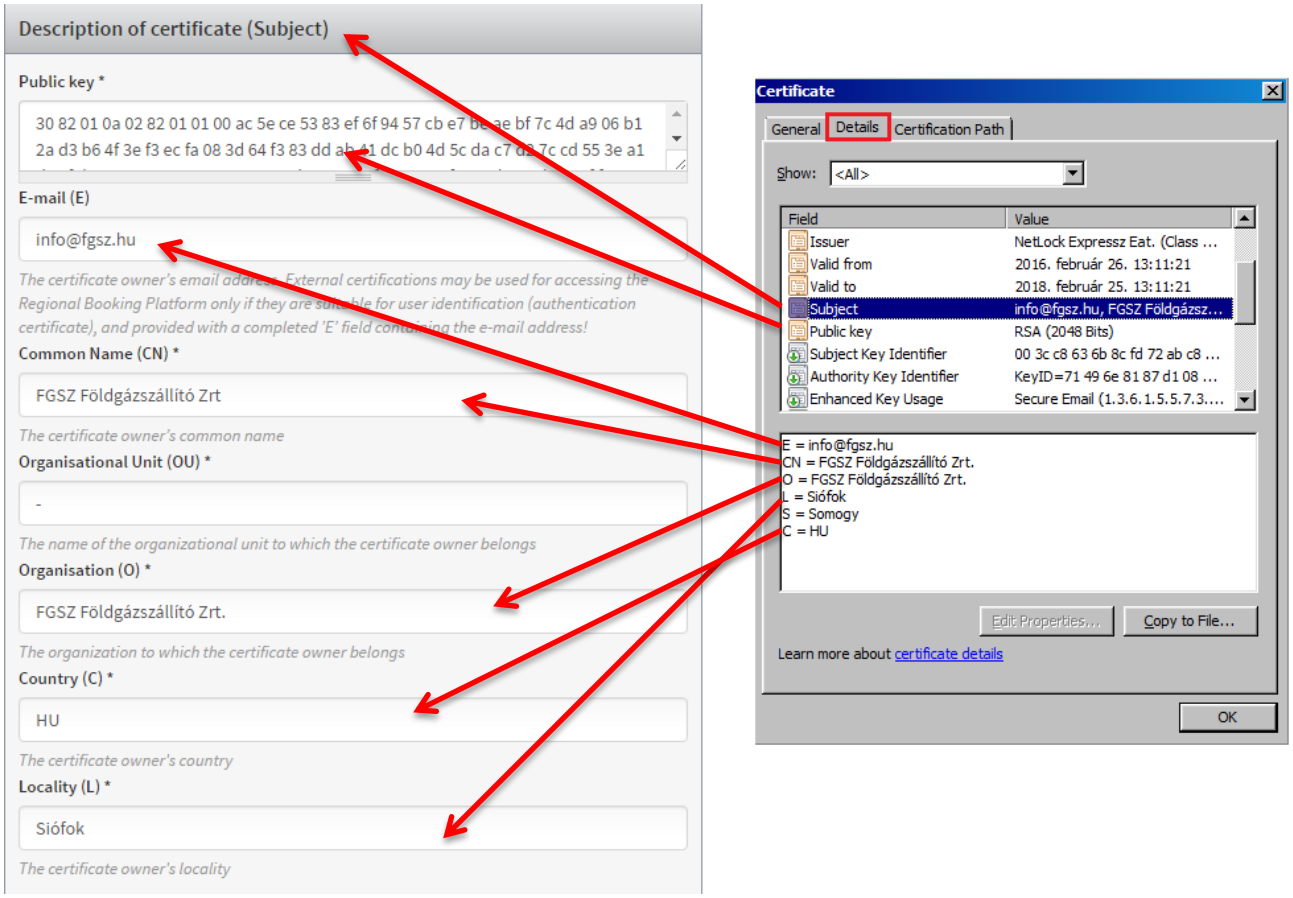
5. Submission of the electronic certificate's data during Network User registration

In order to be able to reach the RBP Application the electronic certificate of the prospective Network User must be registered during the Network User registration process. The required data can be obtained after the installation of the electronic certificate (according to point 6.) from the Internet browser of the Network User (according to point 11.). The required data can be divided into two categories: one regarding the issuer of the electronic certificate (issuer), and one regarding the prospective user of the electronic certificate (subject).

The data regarding the issuer of the certificate can be obtained in the Details tab of the certificate management window of the internet browser by clicking on the Issuer row (according to point 11.). In case the certificate does not contain information needed in one of the required fields it must be substituted with clearly recognisable fictive data. Exceptions to this rule are the „Common Name (CN)", „Name of the organization issuing the certificate" and „Web address of the organization issuing the certificate" fields, which must be filled out with legitimate data in order to have the certificate accepted. The example below demonstrates the fill out process.



The data regarding the issuer of the certificate can be obtained in the Details tab of the certificate management window of the internet browser by clicking on the Issuer row (according to point 11.). In case the certificate does not contain information needed in one of the required fields it must be substituted with clearly recognisable fictive data. Exceptions to this rule are the „Public key", „E-mail (E)" and „Common Name (CN)" fields, which must be filled out with legitimate data in order to have the certificate accepted. The example below demonstrates the fill out process.



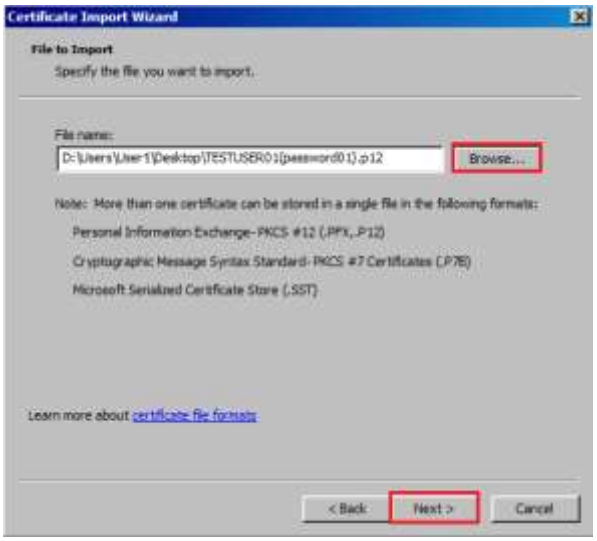
6. Installing the electronic certificate

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

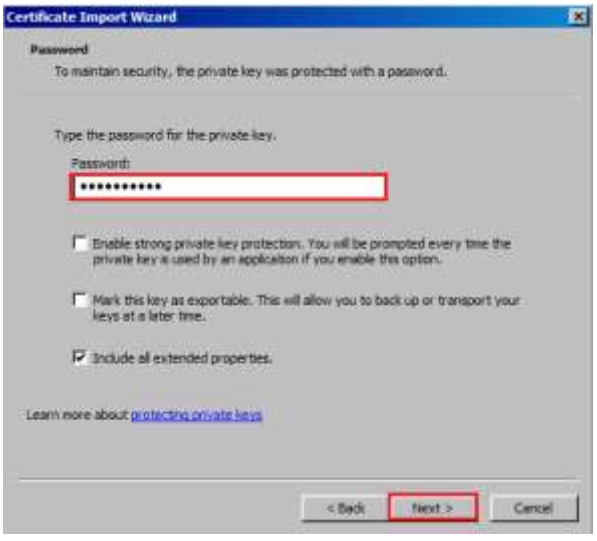
a. Using Internet Explorer:

- Find the storage of certificate with (most commonly a .p12 (PKCS #12) format file protected by a password) a file manager application (e.g. Windows Explorer, etc.),
- initiate installing by double clicking on the certificate storage's file
- Next button (1. step)
- Next button(2. step)
- Type password(3. step)
- Next button (4. step)
- Certificate Store: the selected radio button by default is appropriate: "Automatically select the certificate storage…") (5. step)
- Next button (6. step)
- Finish button (7. step)

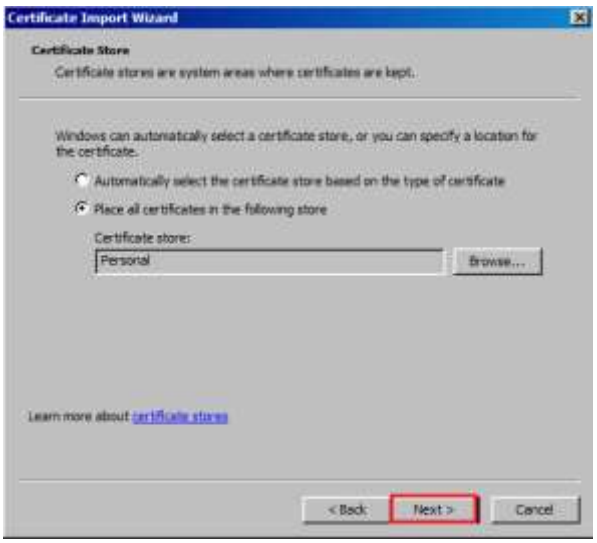
1. step



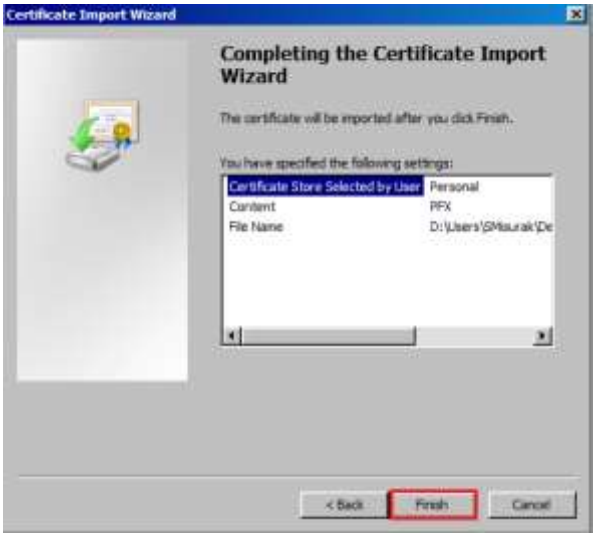
2. step



3.-4. step



5. step



6. step

7. step

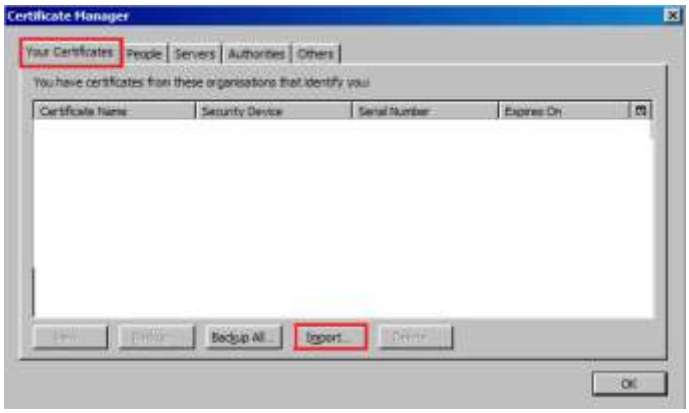
b. Using Firefox

- Options menu (1. step)
- Options submenu (2. step)
- Advanced icon (on top right) (3. step)
- Certificates tab (default) (4. step)
- View Certificates button (5. step)
- Your certificates tab (default) (6. step)

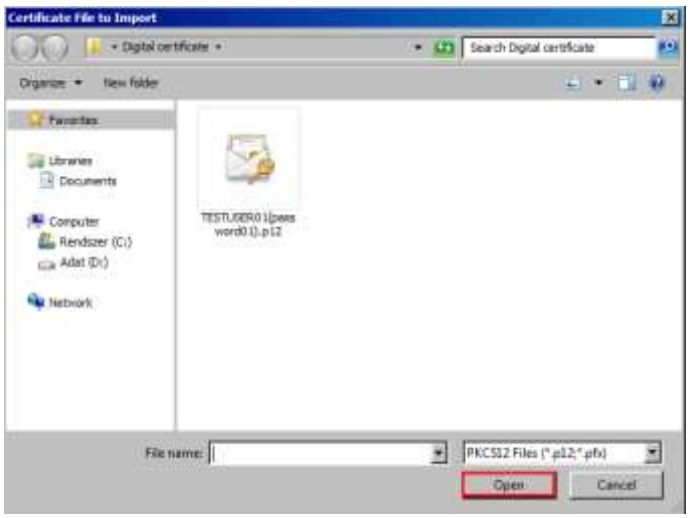
- Import button (7. step)
- Select the electronic certificate on the data storage device (8. step)
- Type password (9. step)
- OK button (10. step)

1.-2. step

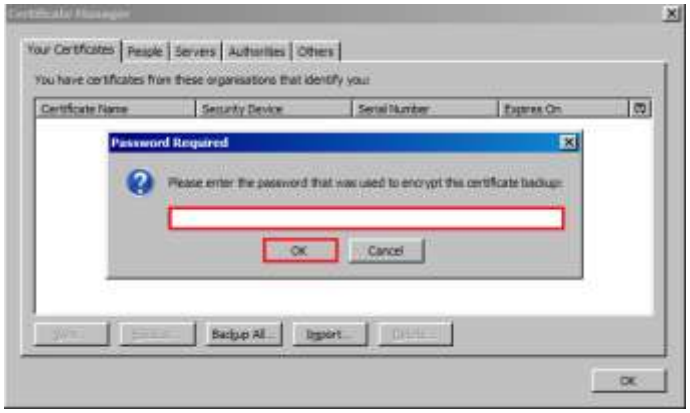
3.-4.-5. step



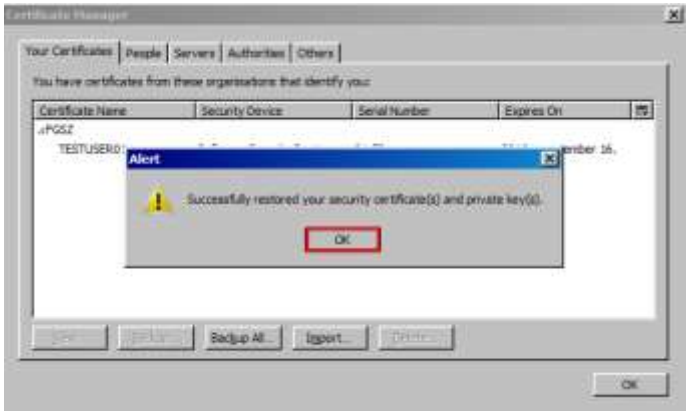
6.-7. step



8. step



9. step



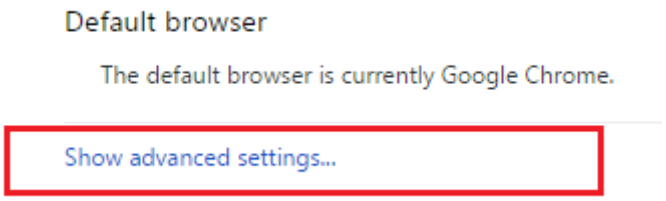
10. step

c. Using Google Chrome

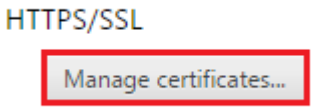
- Customize and control menu (1. step)
- Settings submenu (2. step)
- Show advanced settings (3. step)
- Manage certificates (4. step)
- Personal tab (default) (5. step)
- Import button (6. step)

- 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)

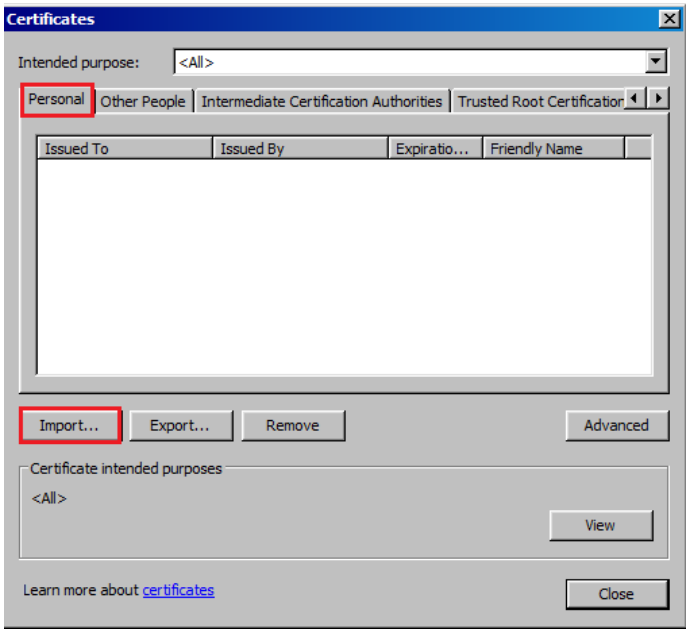
1-2. step



3. step

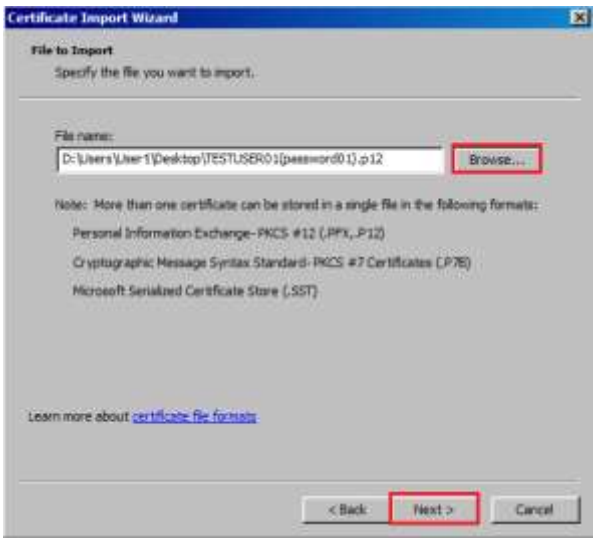


4. step

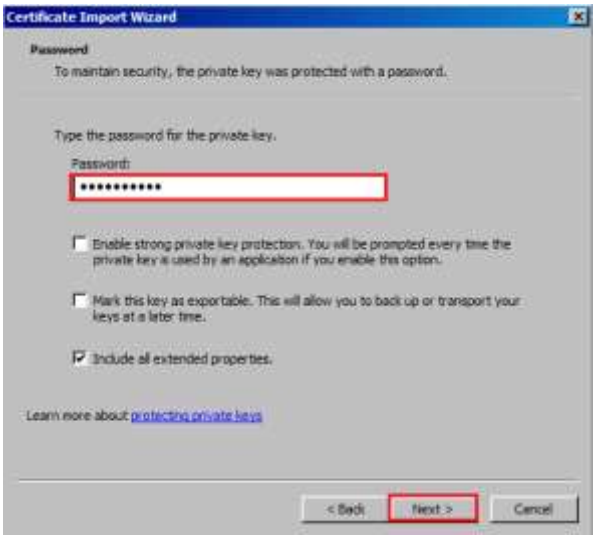


5.-6. step

7. step

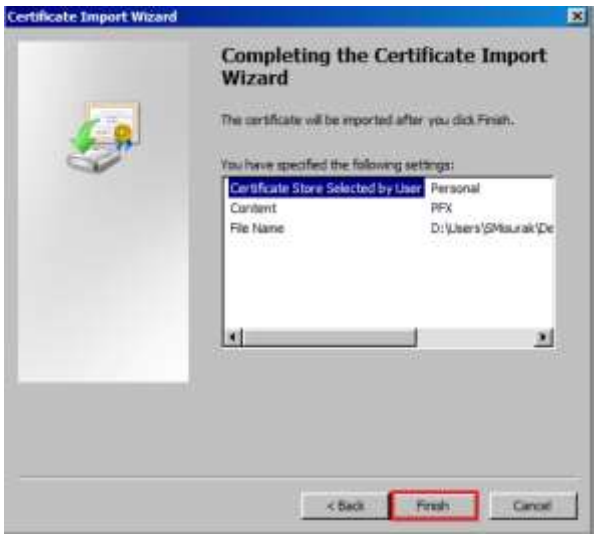


8. step



9.-10. step

11. step



12. step

13. step

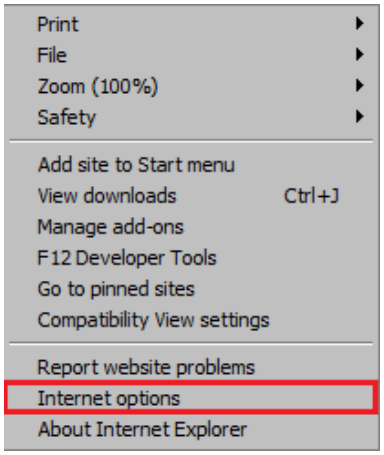
7. Sending the public key to the RBP Operator

You should send the public key of your electronic certificate for the operator via the registration process on the RBP Portal (https://rbp.eu). and send it to the rbp@fgsz.hu e-mail address.

Executing the following steps the public key can be reachable:

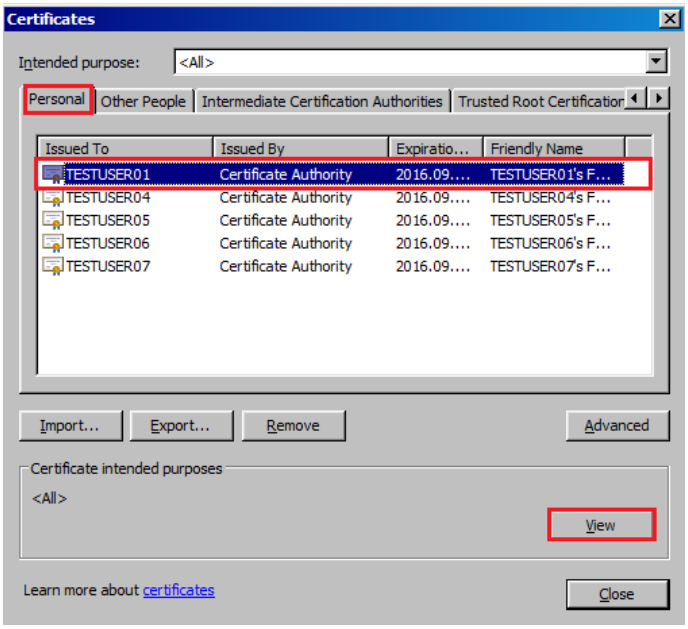
a. Using Internet Explorer

- Tools menu (1. step)
- Internet options submenu (2. step)
- Content tab(3. step)
- Certificates button (4. step)
- Personal tab (default) (5. step)
- Choose the required certificate, if there are more installed (6. step)
- View button (7. step)
- Details tab (8. step)
- Choose the Public key row in the listbox (9. step)
- Under the listbox the public key is shown and can be copied (10. step)

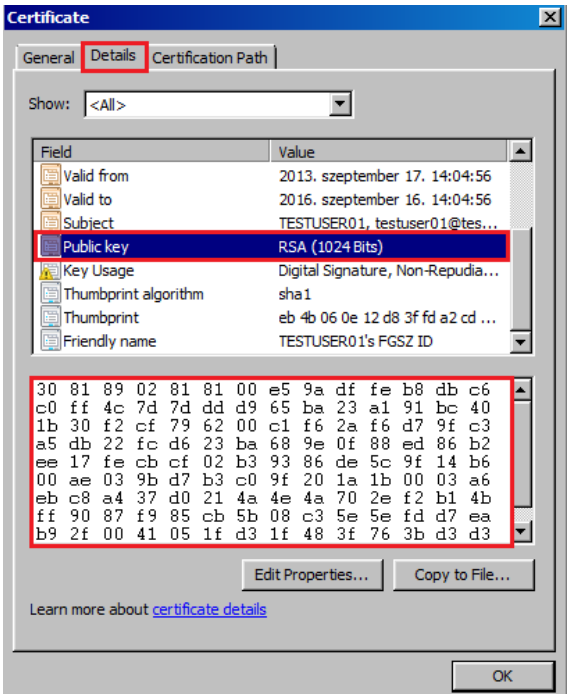


1-2. step

3.-4. step



5.-6.-7. step



8.-9.-10. step

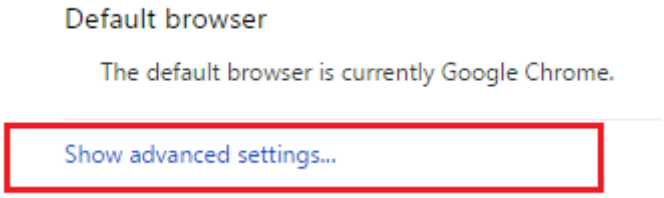
b. Using Firefox

The format of the public key displayed by Firefox is not supported by the RBP.

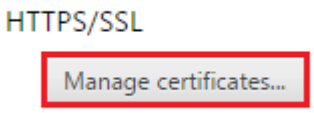
c. Using Google Chrome

- 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)
- Details tab (8. step)
- Choose the Public key row from the list box (9. step)
- Under the listbox the public key is shown and can be copied (10. step)

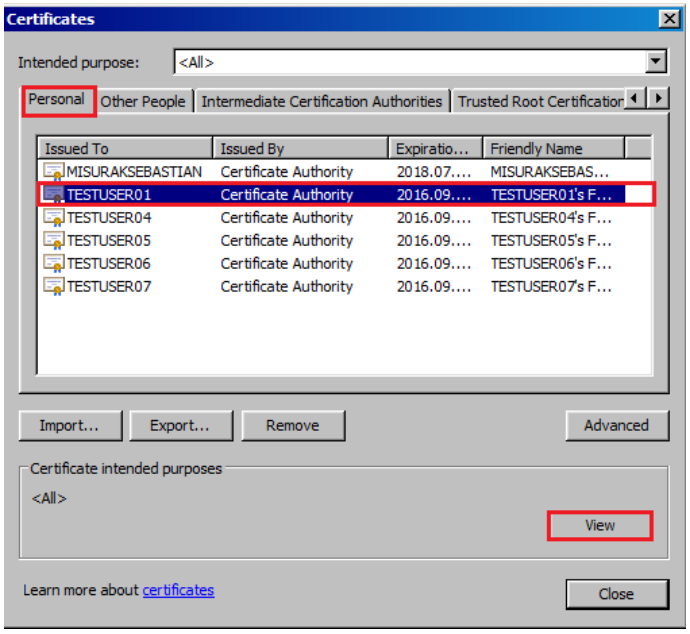
1.-2. step



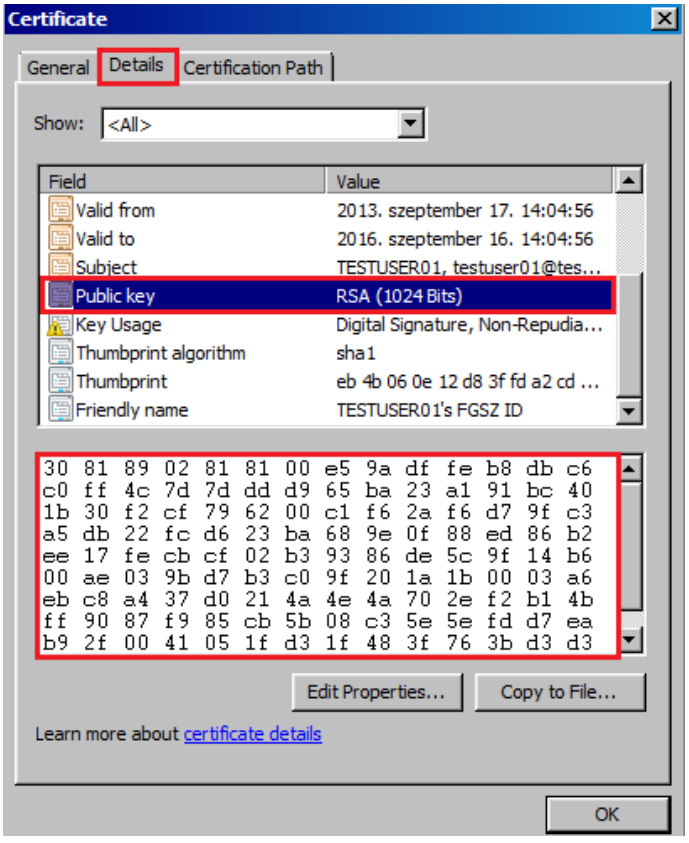
3. step



4. step



5.-6.-7. step

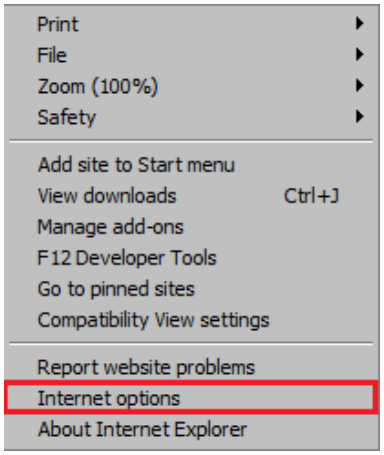


8.-9-10. step

8. Uninstalling the electronic certificate

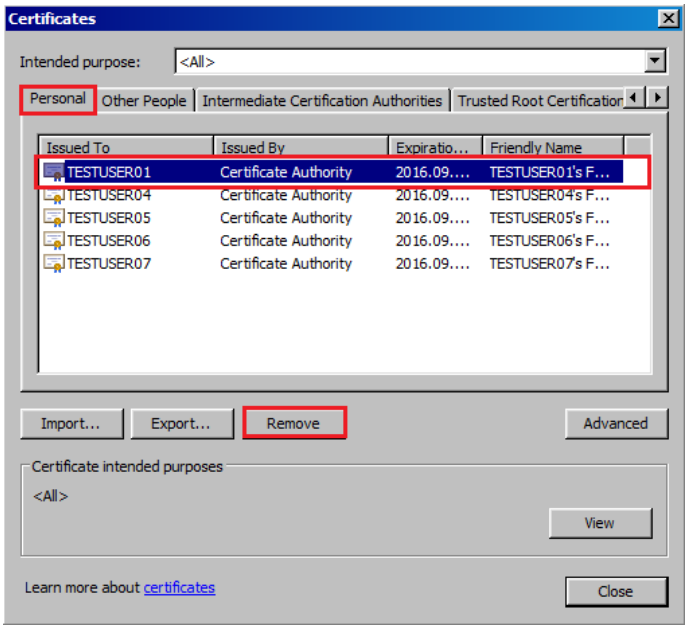
In order to avoid misuse of electronic certificates, the installed electronic certificate must be uninstalled if you do not wish to use it any more (in case of e.g. position change, computer change, etc.). It is also advised to uninstall the certificate from a computer you installed it on temporarily.

a. To uninstall the following steps need to be done using Internet Explorer:
   - Tools (1. step)
   - Internet options (2. step)
   - Content tab (3. step)
   - Certificates button (4. step)
   - Personal tab (default) (5. step)
   - Choose the required certificate, if there are more installed (6. step)
   - Remove (7. step)
   - Choose “Yes” in the pop up window (8. step)

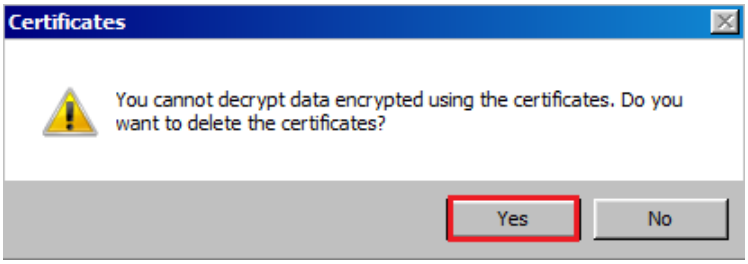


1.-2. step

3.-4. step



5.-6.-7. step

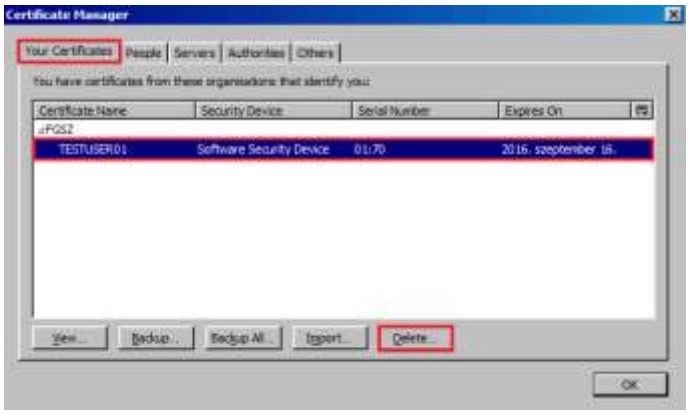


8. step

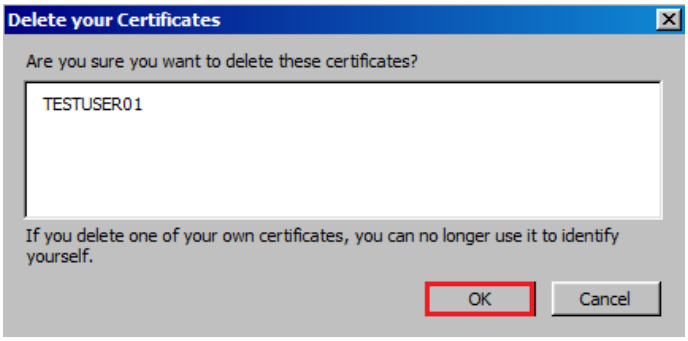
b. To uninstall the following steps need to be done using Firefox:
- Options menu (1. step)
- Options submenu (2. step)
- Advanced icon (3. step)
- Certificates tab (4. step)
- View Certificates button (5. step)
- Your Certificates tab (default) (6. step)
- Choose the required certificate (7. step)
-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

1.-2. step

3.-4.-5. step



6.-7.-8. step

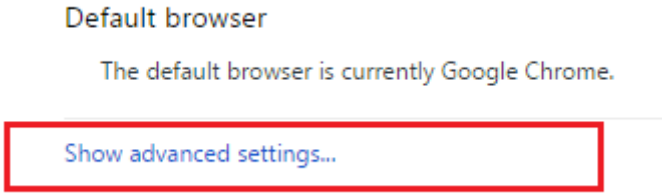


1. step

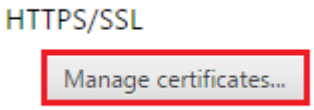
c. To uninstall the following steps need to be done using Google Chrome:

- 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)

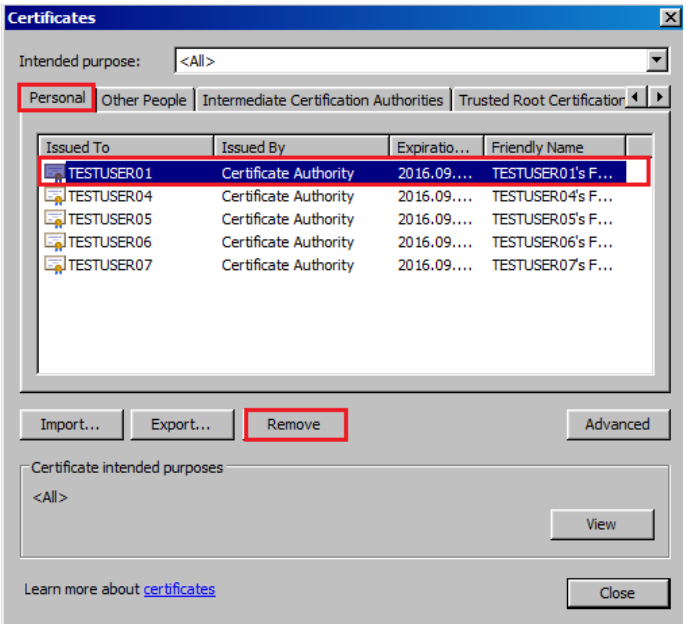
1.-2. step



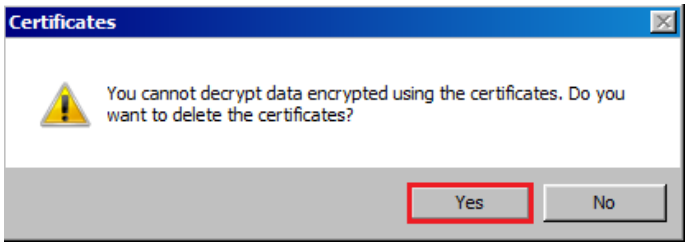
3. step



4. step



5.-6.-7. step



8. step

9. 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.

10. 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 rbp@fgsz.hu, 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.

11. 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 energy-based Informatic Platform (eIP), or the Balancing Platform (EP).

- 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.

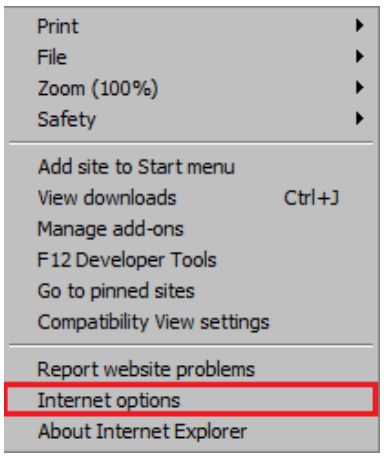
  To do: Check the data of the certificate according to point 10, with special regard to the e-mail address. If it does not correspond with the e-mail address provided in the application submitted to the issuing trusted service provider, it has to be modified by the issuing trusted service provider.

12. 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.

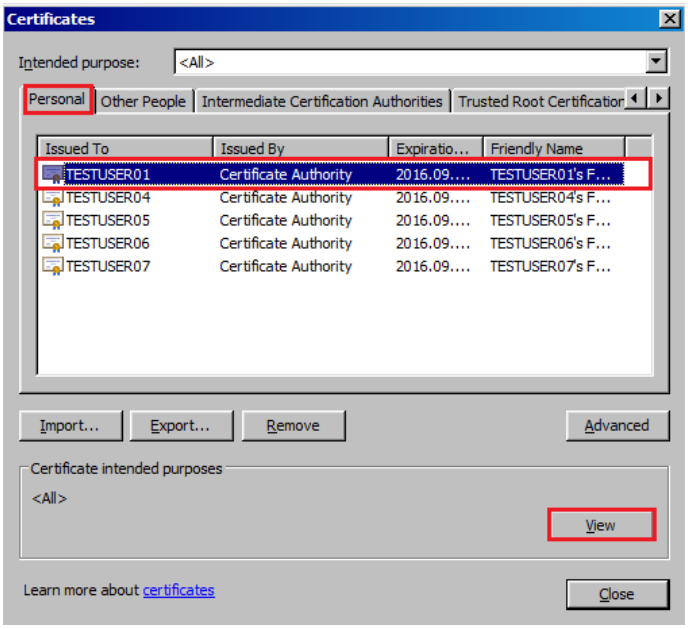
Steps to follow during checking:

a. Using Internet Explorer
   - Tools (1. step)
   - Internet options (2. step)
   - Content tab(3. step)
   - Certificates button (4. step)
   - Personal tab (default) (5. step)
   - Choose the required certificate, if there are more installed (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

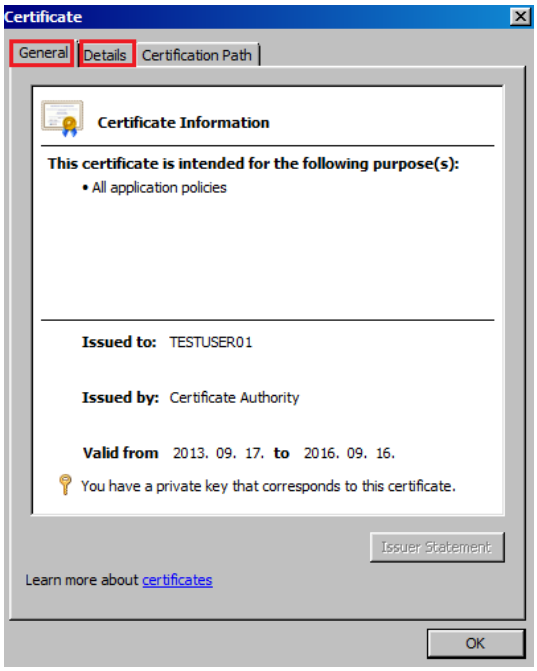


1-2. step

3.-4. step


Certificates
Intended purpose:
<All>
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certificatior
Issued To
Issued By
Expiratio...
Friendly Name
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

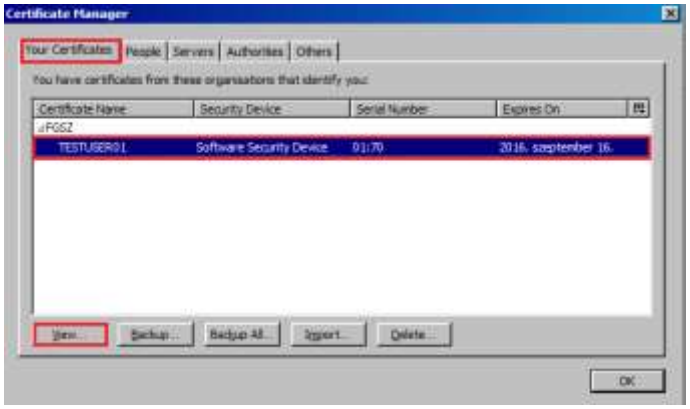

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All application policies
Issued to: TESTUSER01
Issued by: Certificate Authority
Valid from 2013. 09. 17. to 2016. 09. 16.
You have a private key that corresponds to this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

b. Using Firefox

- Options menu (1. step)
- Options submenu (2. step)
- Advanced icon (on top right) (3. step)
- Encryption tab (4. step)
- View Certificates button (5. step)
- Your Certificates tab (default) (6. step)
- Choose the required certificate (7. step)
- View… button (8. step)
- General tab: Owner, Issuing organisation, Start of validity, Expiry date
- Details tab: The owner's public key, etc. in the Certificate Fields treelist

1.-2. step

2.-3.-4. step

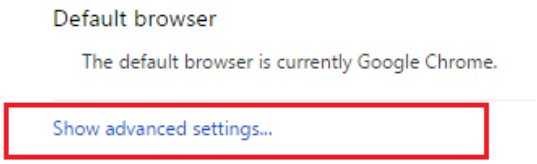


6.-7.-8. step

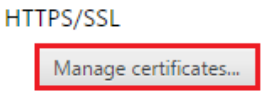
c. Using Google Chrome

- 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

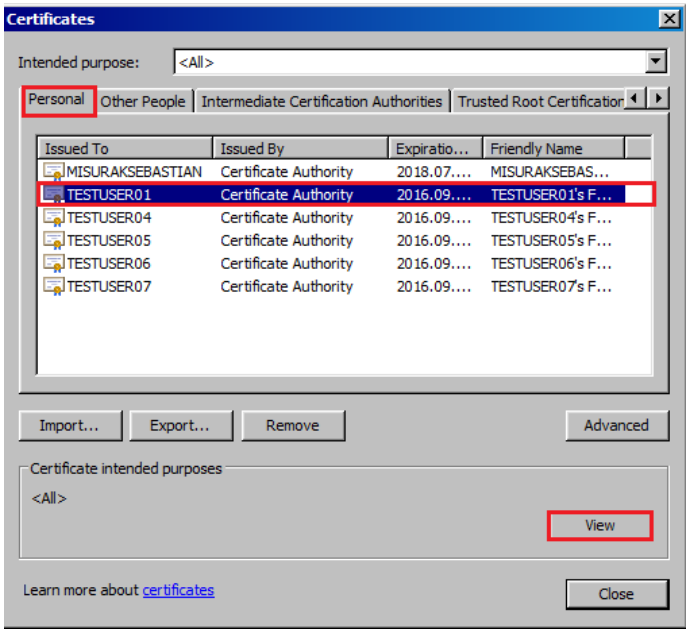
1-2. step



3. step



4. step



5.-6.-7. step