THE USE OF ELECTRONIC CERTIFICATE

ON THE INFORMATIC PLATFORM

01 July 2016

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 Informatic Platform (IP), established and operated in compliance with our legal obligation, supports the title-based access of Network 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 for becoming one of the active users of our informatic system.

1. Definition 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 information

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 by the means of the secret and public key pair belonging to the digital 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 are collectively 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 Informatic Platform should meet the below criteria:

- The electronic certificate shall be issued by an external trusted service provider company
- 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.
- Real e-mail address in the "E" attribute within the "Owner" field of the certificate or in the alternative name field (RFC822).

- 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 exchange	-	critical	mandatory	RFC 5280
Extended Key usage	Client Authentication	1.3.6.1.5.5.7.3.2	non-critical	recommended	

In order to maintain system security, the Informatic Platform does not support the use of certificates having the same e-mail address. The application operator is entitled to refuse new certificates if the e-mail address in the "E" attribute within the "Owner" field or in the alternative name field (RFC822) has already been registered in the system.

For further information see: https://fgsz.hu/en-gb For Our Partners / Informatic platform / Electronic certificate

4. Obtaining an electronic certificate

The electronic certificate can be obtained from a certified organisation that is authenticated to issue electronic certificates (Trusted Service Provider – TSP), and 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 the national lists can be found under the following link: https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-certification-service-providers.

Certificates issued by service providers that are not included in one of the above mentioned national lists are not accepted from 1 July 2016 onwards.

Previously registered Network Users shall obtain a certificate issued by a service provider that is included in one of the national lists, till 1 January 2017.

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

5. Installing the electronic certificate

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

a. If Internet Explorer is the default browser:

- find the key with a file manager application (e.g. Windows Explorer, etc.)
- initiate installing by double clicking on the key file
- press Next
- proceed to point c. below

b. If not Internet Explorer is the default browser

- Tools
- Internet options
- Content tab
- Certificates tab
- Personal tab (default)
- Import button
- Next button
- Browse – Select the digital certificate on the data storage device
- proceed to point c. below

c. Further steps of the installing process

- Next button
- Type password
- Next button
- Select personal storage (default)
- Next button
- Finish button

To log on to the Informatic Platform the Application form at the https://fgsz.hu/en-gb For Our Partners / Informatic platform / Electronic certificate website should be filled in:

signed duly and sent to ipsupport@fgsz.hu.

6. Uninstalling the electronic certificate

In order to prevent 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 advisable to uninstall the certificate from a computer you temporarily installed the electronic certificate on.

To uninstall the electronic certificate, the following steps need to be done using Internet Explorer:

- Tools
- Internet options
- Content tab
- Certificates button
- Personal tab (default)
- Remove
- Choose “Yes” in the pop up window

7. Using the electronic certificate

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

If more than one electronic certificate has been installed, a window - in which all the installed certificates are shown - will appear for choosing from the certificates the one you wish to use on the Informatic Platform.

8. 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 IPSupport@fgsz.hu, out of working hours to the colleagues on duty, and to one of the contact persons listed in the Informatic Platform User Agreement in order to prevent any misuse.

9. Dealing with frequent errors

The following four 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 Informatic Platform, the login is unsuccessful.
  To do: Check the status of the certificate according to point 10. If the certificate is not installed, it should be installed according to point 5, and then it is advisable to check if it was successful according to point 10. If the certificate is included in the list of installed certificates, its validity should be checked, see “electronic certificate expired” section.

- 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 Informatic 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 Informatic Platform, however it is not possible to enter the system with the chosen certificate.
  To do: Check the data in 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 authority, it has to be modified by the issuing company.

- the public key is not installed on the FGSZ servers

  Error: When entering the Informatic 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 8, 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 Informatic Platform, the login is unsuccessful.
  To do: Check the data in the certificate according to point 10, with special regard to the validity of the certificate. If it expired, the certificate can be renewed at the issuing authority or a new certificate can be applied for at another organisation.

10. Checking the electronic certificate

Checking the data of the installed digital keys provides an opportunity to eliminate several problems. If you wish to use the assistance of an FGSZ employee, the following data shall be necessary in order to overcome the problem.

Steps to follow during checking:

- Tools
- Internet options
- Content tab
- Certificates button
- Personal tab (default)
- Choose the required certificate, if there are more installed
- View button
- General tab (default)
- Validity and expiry date shown
- Details tab
- Issuing organisation, Start of validity, Expiry date, Owner, e-mail address (“E” field) shown