NARODOWY
BANK POLSKI

CHIRON GUI

Security Department
Warsaw, 2022

Contents

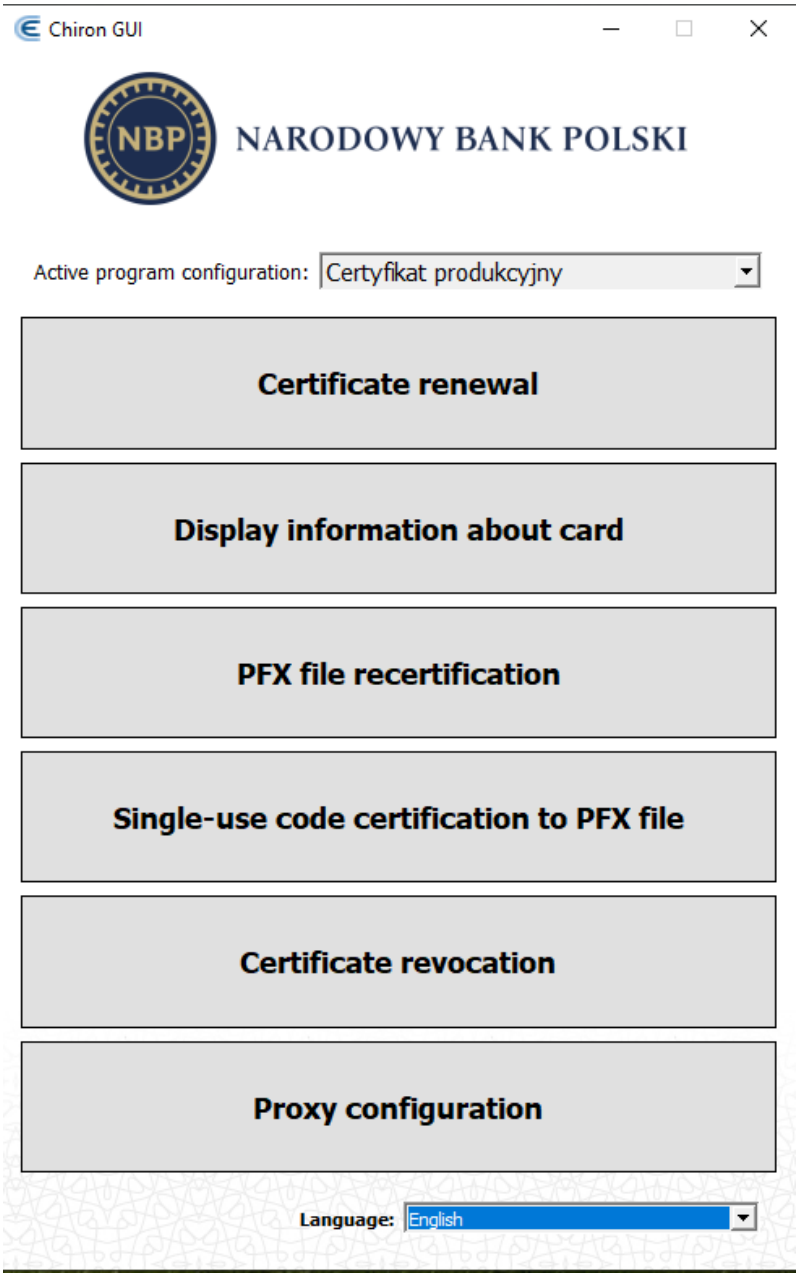
1. Introduction 3
2. Chiron GUI application 4
2.1. PROXY configuration. 5
2.2. Certificate renewal (smart card). 6
2.3. Display information about card. 8
2.4. PFX file recertification 8
2.5. Single-use code certification to PFX file. 10
2.6. Revoke user certificate. 11

1. Introduction

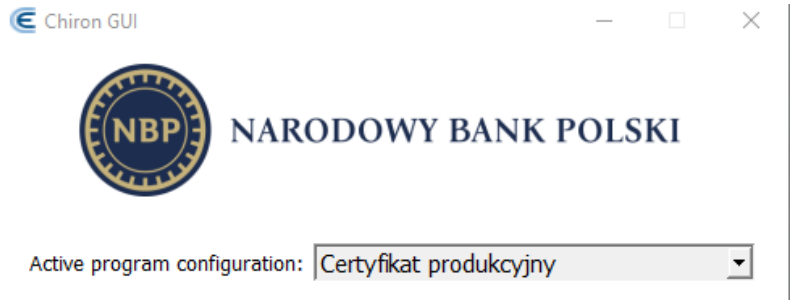
1. Since 21st of November 2022 a new remote certification system based on the Chiron GUI application has been in operation for all certificates in the DOCert system.
2. The Chiron GUI application requires to be installed on the user workstation.
3. Installation files of the Chiron GUI application are available at the www.docert.nbp.pl website under the "Remote certification" tab.
4. The Chiron GUI user manual is accessible at the www.docert.nbp.pl website under the "Instructions" tab.
5. A single Chiron GUI application services both production and test certificates (*there is no need to install separate applications for both types of certificates*).
6. The Chiron GUI application connects to the DOCert system servers of the following addresses:
    a. Test environment
        i. 193.109.212.15:443
        ii. 195.85.196.15:443
    b. Production environment
        i. 193.109.212.32:443
        ii. 195.85.196.32:443
7. The traffic between the Chiron GUI application and the abovementioned addresses is encrypted– the use of SSL/TLS decryptors or similar devices may result in a lack of the possibility to generate/renew the certificate *(we suggest exemptions should be added on SSL/TLS decryptors).*
8. The Chiron GUI application supports PROXY servers; configuration is possible from the application menu after it is started for the first time.
9. Application logs are stored in the log.log file placed in the catalogue in which the Chiron GUI application has been installed (in the case of the Windows system, the standard path is as follows: C:\Program Files(x86)\Chiron GUI\log.log).

2. Chiron GUI application

1) Starting the Chiron GUI application is possible from the operating system menu or via a special icon on the desktop.
2) Upon each start, the application tries to connect to servers (see point 1.1) to verify the configuration. If needed, the application will upload a new configuration.
3) Application window.

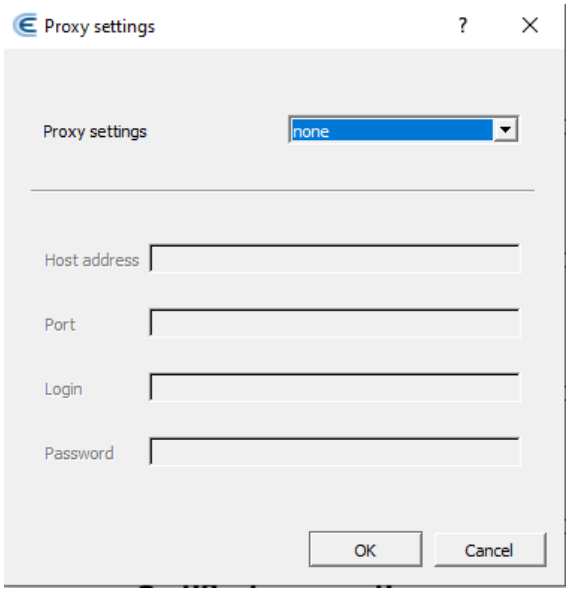


4) The active program configuration indicates if the certificates to be dealt with are certificates issued by the production authority **NBP CCK 2** (configuration "Certyfikat produkcyjny") or the test authority **NBP CCK TEST 2** (configuration "Certyfikat testowy").



2.1. PROXY configuration.

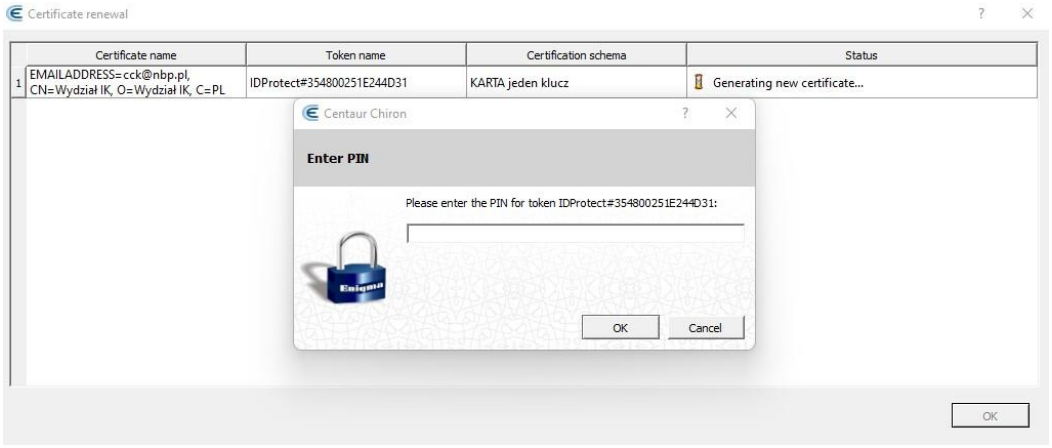
1) After the Chiron GUI application is started for the first time, the PROXY configuration (if required) can be set using the menu.
    a. none – no proxy;
    b. system – configuration uploaded from the operating system;
    c. config – entering data manually;
        i. Host address,
        ii. Port,
        iii. Login and password (if required).



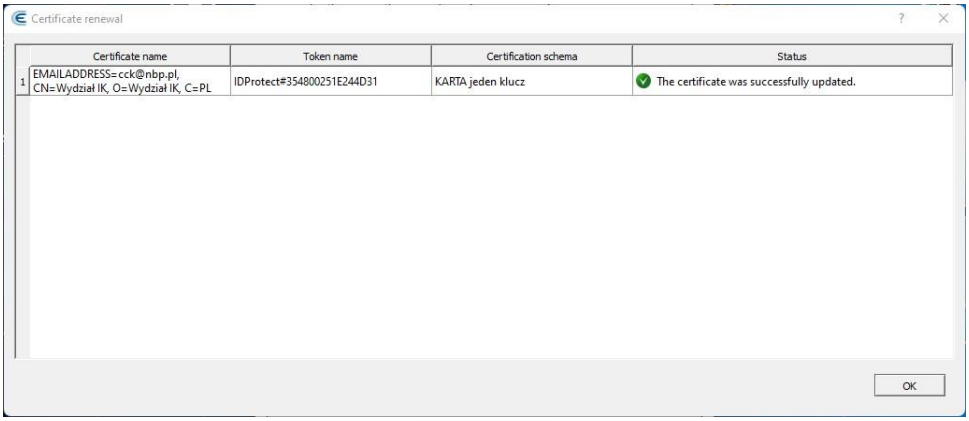
2.2. Certificate renewal (smart card).

1) Enter the smart card into the card reader;
2) Start the Chiron GUI application;
3) Select the required environment (Test certificate or Production certificate);
4) Select "Renew the certificates stored on the smart card";
5) If more than one card reader is installed on the computer, the application will ask you to select the card reader together with the card on which the certificate to be renewed is stored;

6) Enter PIN for the card;

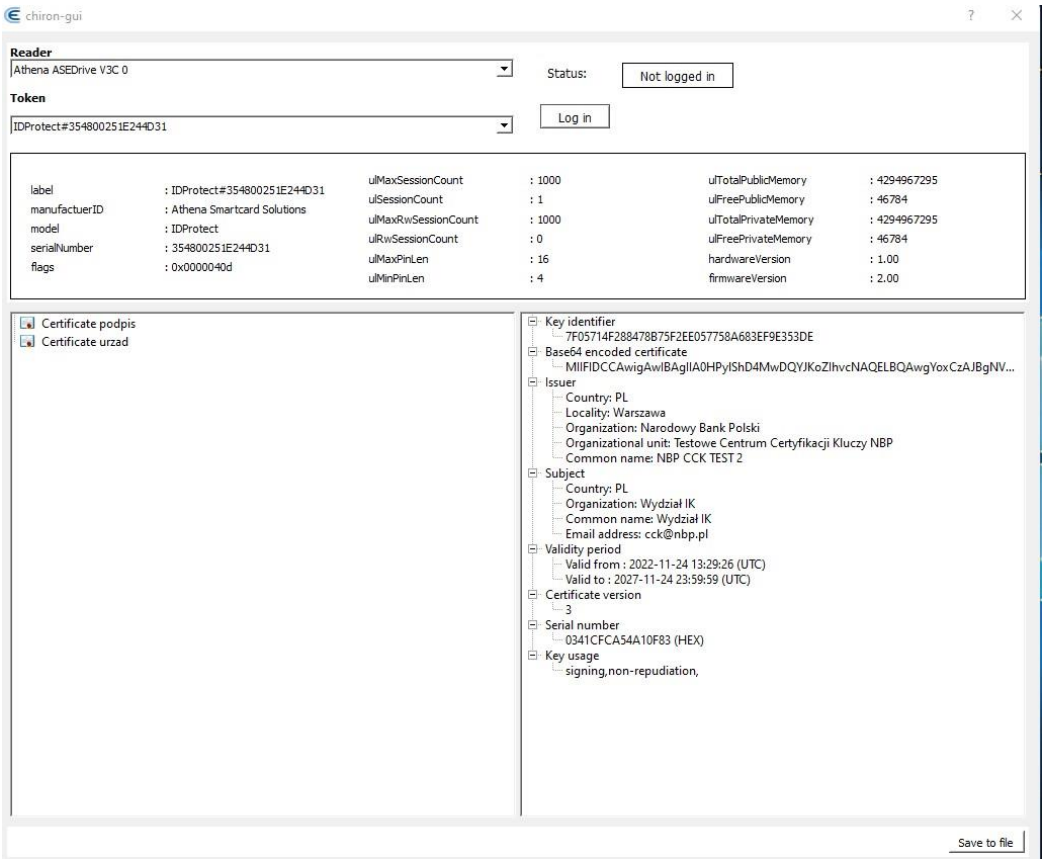


7) Wait for the message ending the certificate renewal process.



2.3. Display information about card.

1) The option enables the display of the information about the certificates and keys stored on the card;
2) When you select the option the following window will pop up:

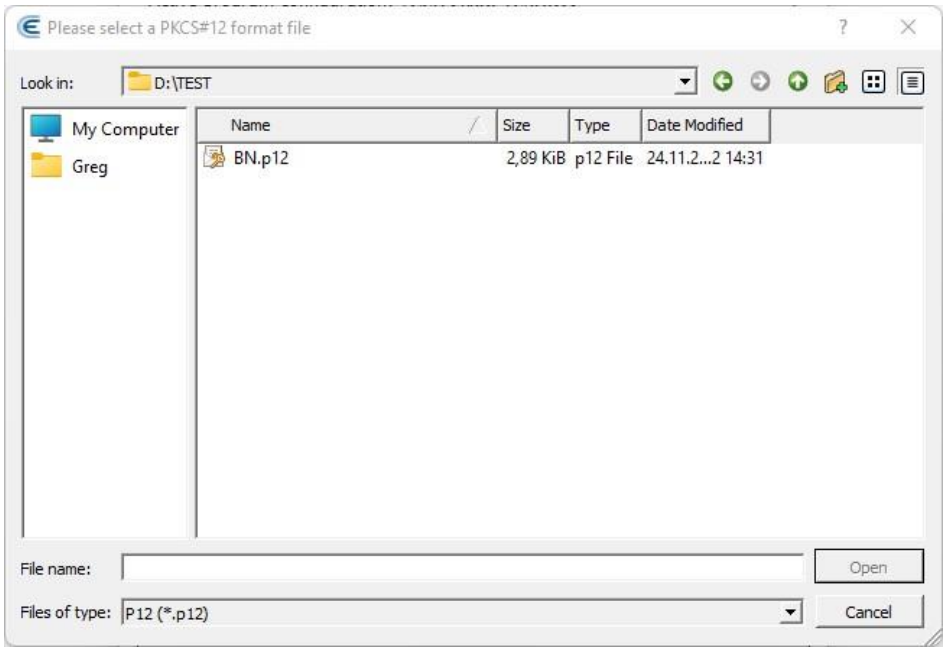


3) The following operations are possible using the window:
    a. Logging in to the card;
    b. Viewing certificates and keys;
    c. Generating a report from the card content (Save to file).

2.4. PFX file recertification

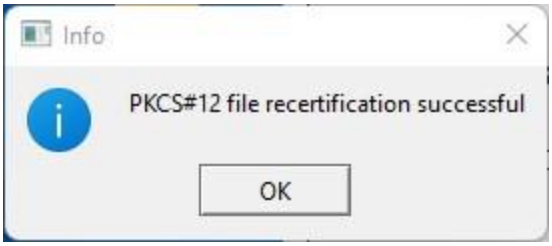
1) The option enables renewal of the certificate stored in the form of a file with extension .p12 or .pfx;

2) Select the file containing the certificate to be renewed;



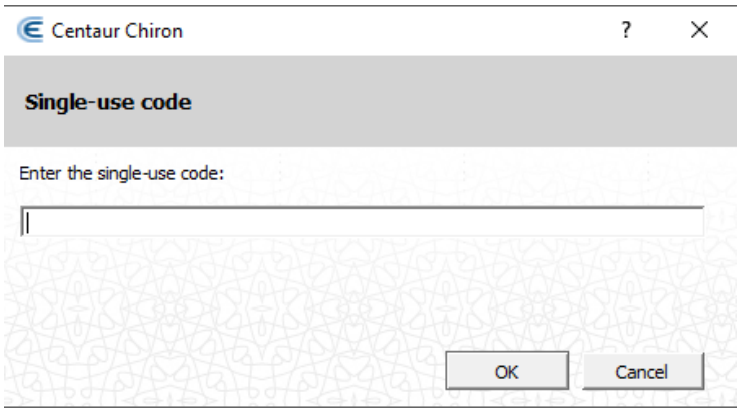
3) Enter the password to the file selected in point 2 above;

4) Indicate the path and the name of the file in which the new cryptographic keys and the certificate are to be stored. The password to the new file will be the same as the password entered in point 3 above.

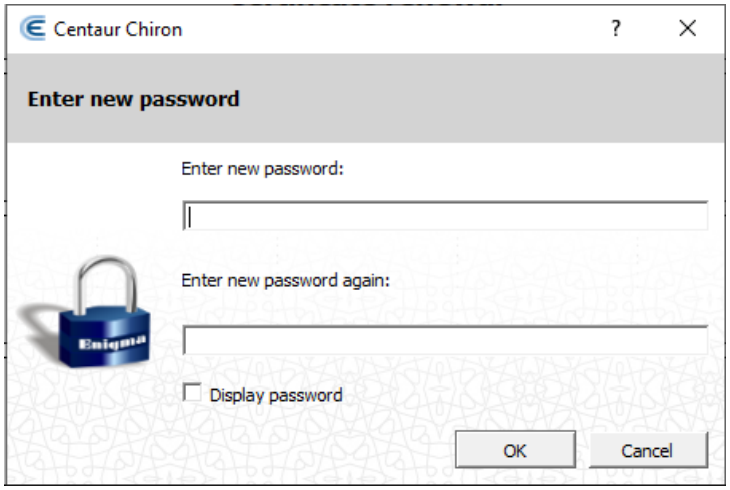


2.5. Single-use code certification to PFX file.

1) The option enables the generation of a new certificate using a single-use code. When you select the option, the following window will pop up:



2) Enter the received code (in a single string of characters; letter case is irrelevant);
3) Indicate the path and the name of the file in which new cryptographic keys and the certificate are to be stored;
4) Enter the password to protect the generated cryptographic keys and the certificate.



2.6. Revoke user's certificate.

1) The option enables revocation of all user certificates issued in the DOCert system;
2) **NOTE: This option is available only for selected IT systems and certain types of certificates;**
3) To revoke certificates, enter the data received in the User Registration Point;

4) Confirm by clicking OK.