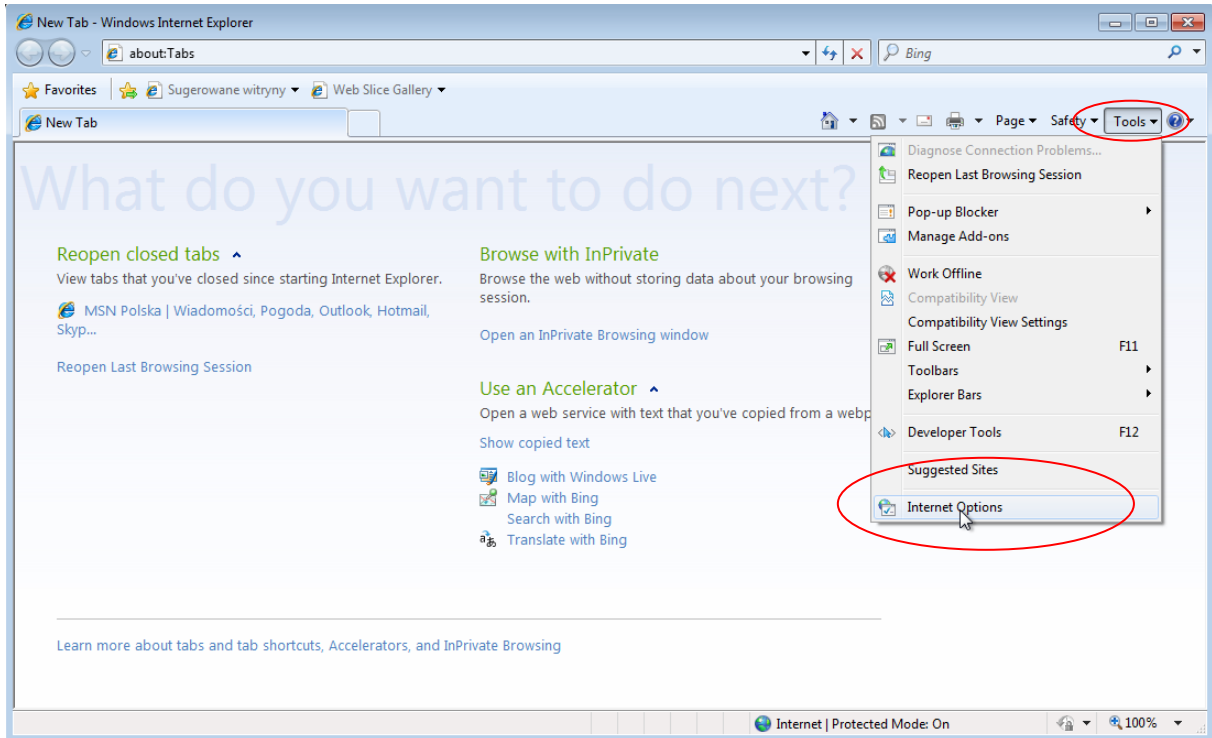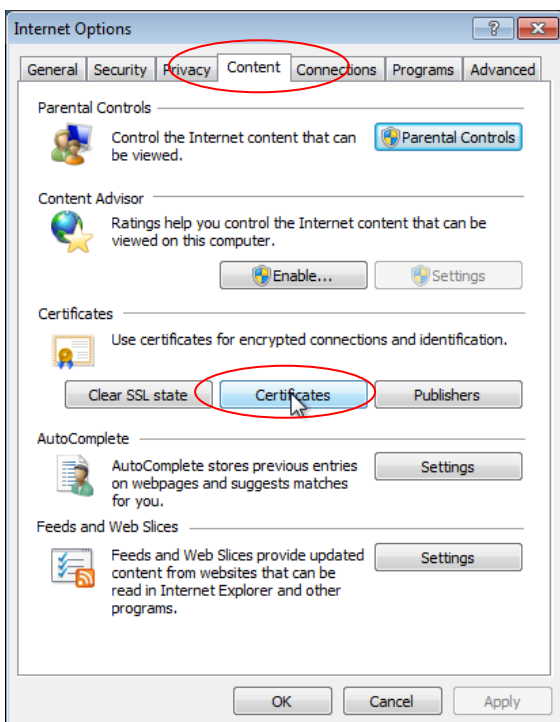# Export of certificate from local repository to the file

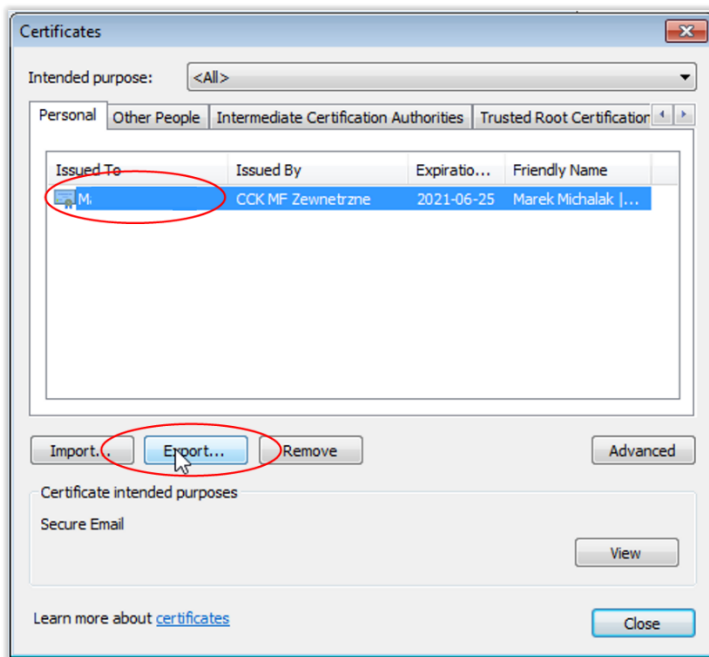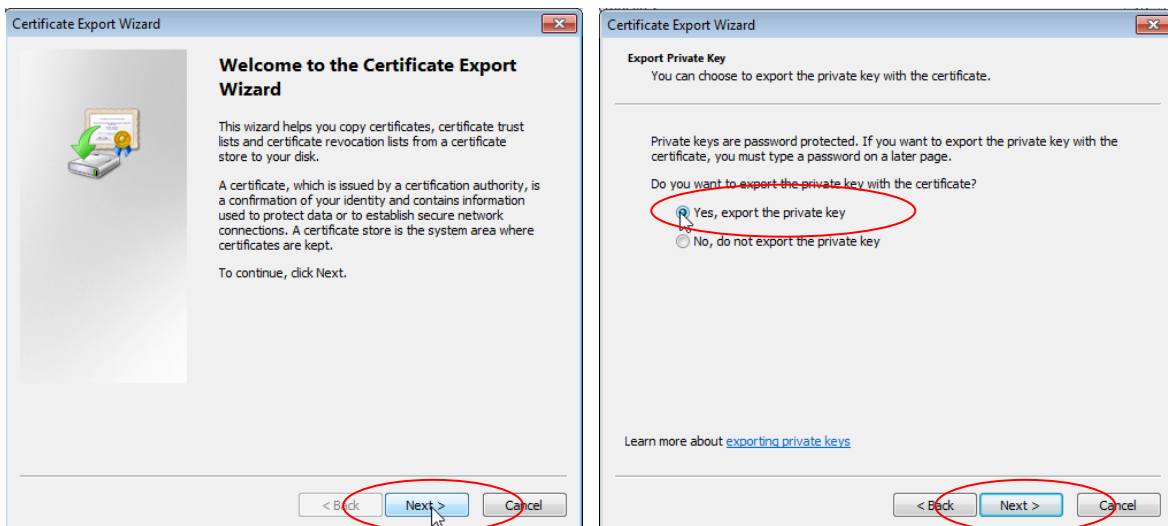1. Open "Internet Explorer" browser. Open menu „Tools" -> „Internet Options":

2. In „Internet Options" window go to „Content" – „Certificates" tab:
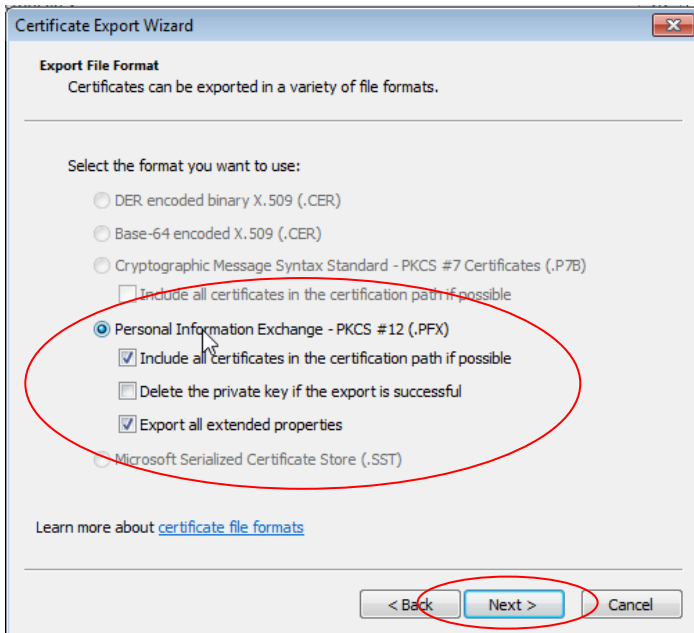
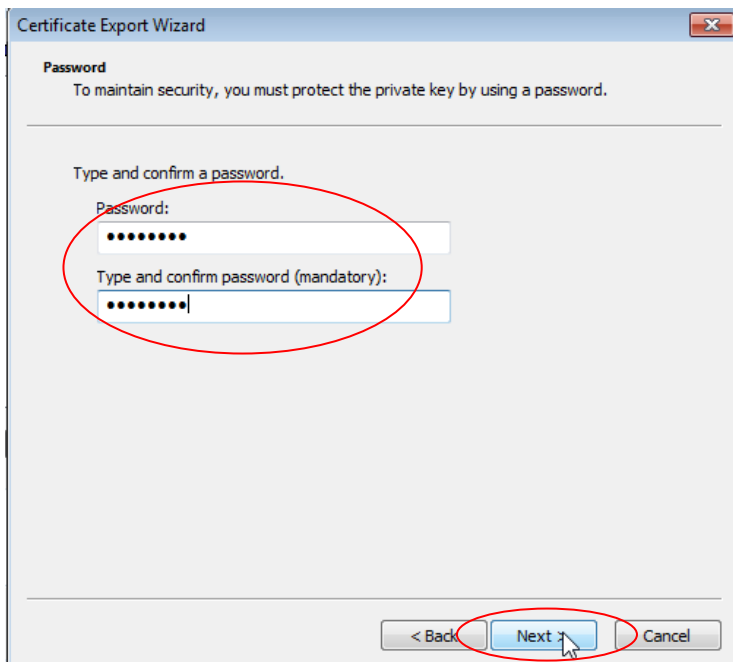3. In „Certificates" window mark your certificate and click „Export...":

4. In next window push „Next", In next mark option „Yes, export the private key" and push „Next":

5. In next window check/uncheck options exactly as shown on the screenshot below and push „Next":

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

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

< Back | Next > | Cancel

6. Create a password for securing the file, avoiding for using the certificate by other person, type it to fields shown below and push "Next":

Certificate Export Wizard

Password
To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password:
••••••••

Type and confirm password (mandatory):
••••••••

< Back | Next > | Cancel

7. In next window show the path and name of the file with certificate (button „Browse…") and push "Next":
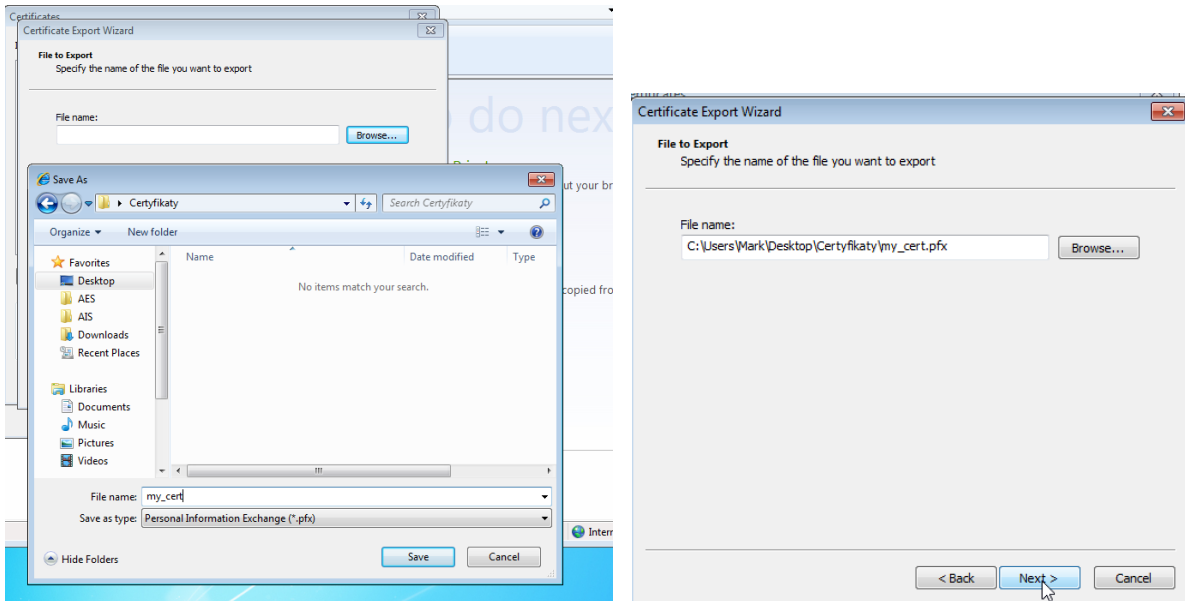

8. In the window with the summary information, click "Finish". During the export, you may be prompted to enter a password for the private key (password, that is assumed when you generate a certificate on PUESC). The process should finish saving the certificate to a file in the specified location.
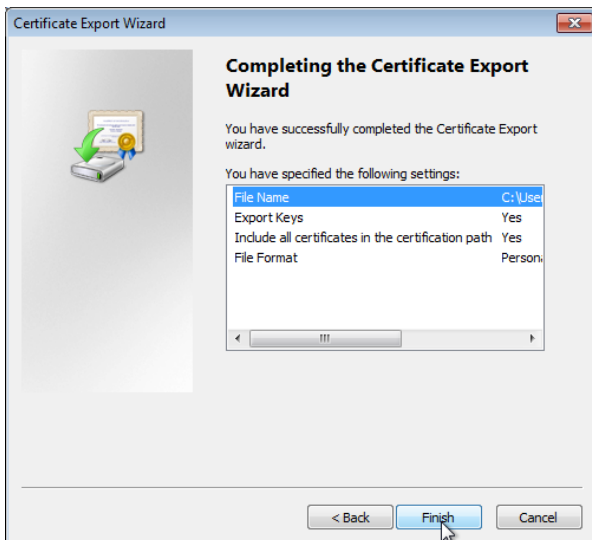
Registration of personal certificate in Wrota Celne

1. After logging-in in order to register a certificate, use the menu option "Configuration" – "User certificates" and click the "Add item":
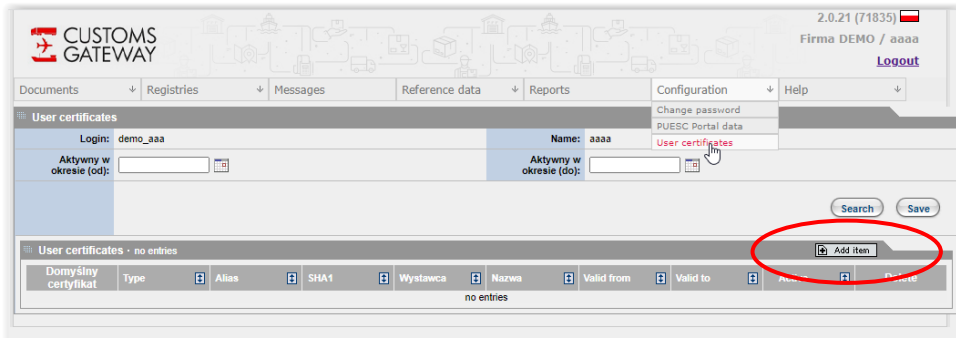
2. In the add certificate window, you indicate the location of the certificate file (click the "Wybierz plik" button), and then in the "Hasło do magazynu certyfikatów" you must provide the password that was used when writing the certificate to a file (' Export certificate... " step 6), and then click "read keystore file".
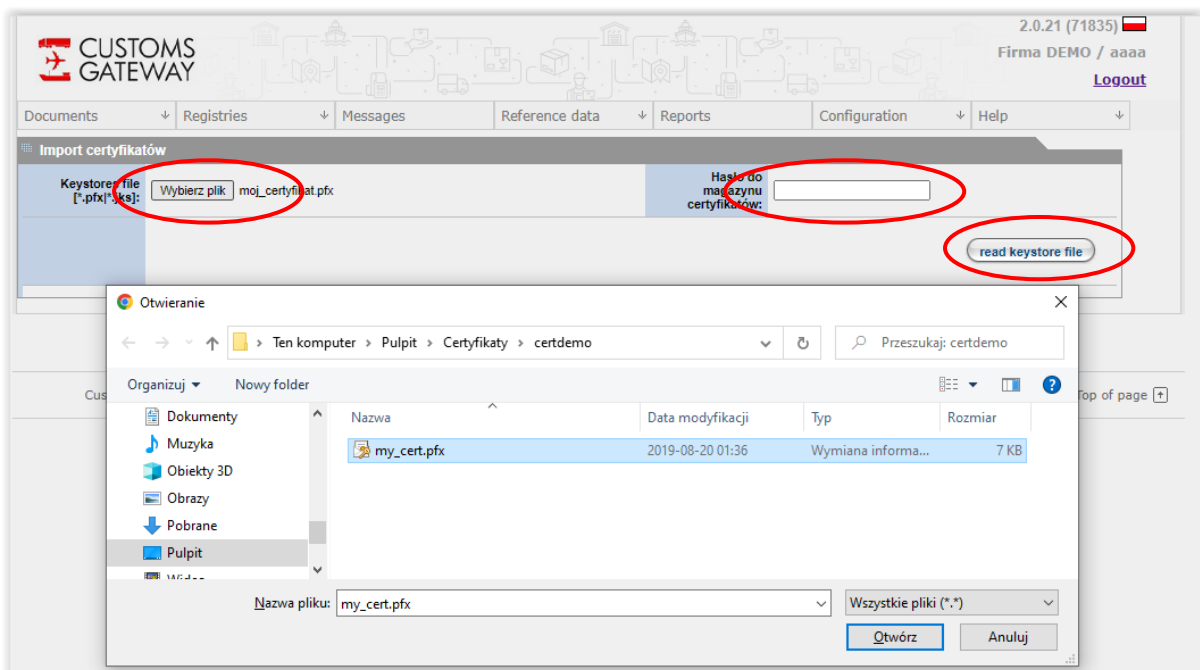
3. After the correct upload of the file the window appears, as shown below. You must then select the check-box in the "importuj" column , enter the password to a file with certificate again in the last column and click the "Importuj certyfikaty" button:

4. After reopening the certificate store (the "Configuration"-> "User certificates" option), a window with a list of currently registered certificates is displayed, on which the user may deactivate his certificate (uncheck the box in the column "Active"), delete it ("x" mark in the "Delete" column) or add a new certificate.

# Sending a document using a certificate stored in the system

1.   In the document window, select the "Send" command, in the next window press "Approve":
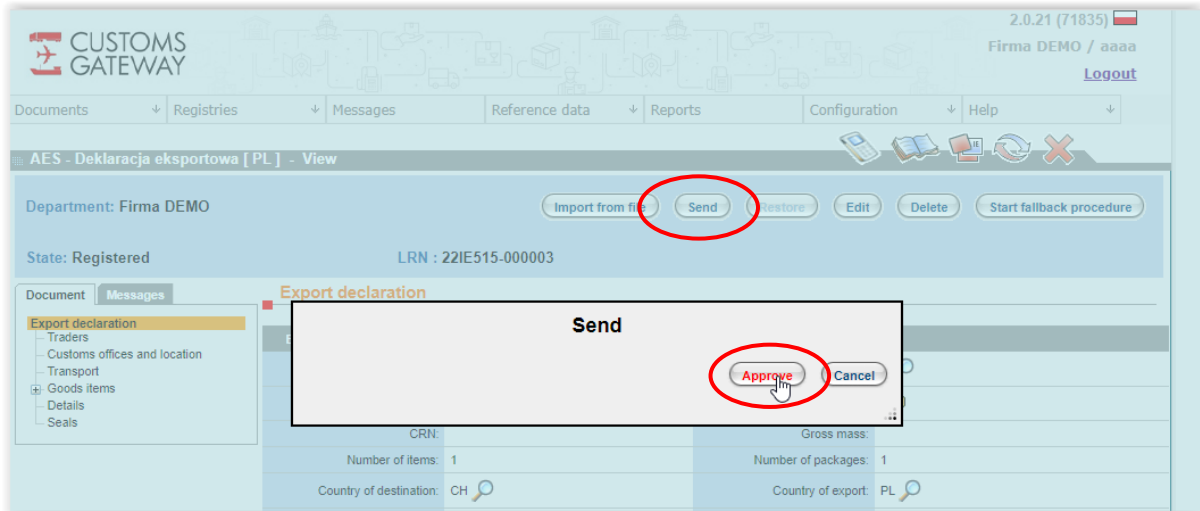
2.   In the message preview window, indicate the method of signature as "Certificate stored in the system (recommended)", and then press "Sign and send":
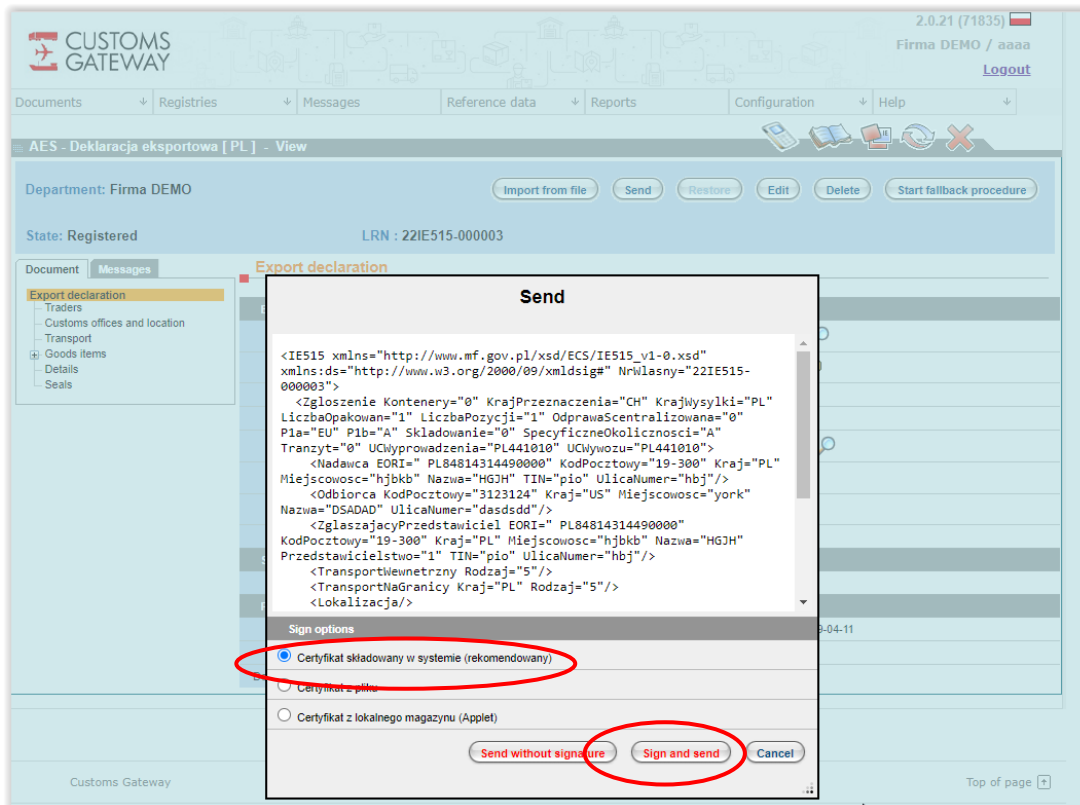
Select the certificate with which the message should be signed and click "Sign and send":
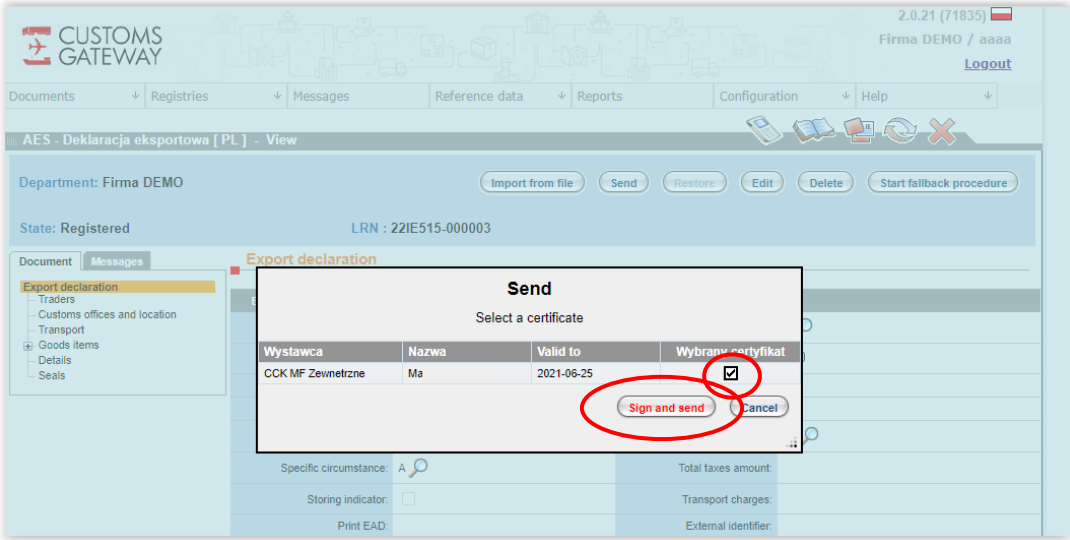
After the process is completed correctly, the document goes to the "Sent" status.