



# Ministerstwo Finansów

## INSTRUCTIONS FOR USE OF THE CLIENT APPLICATION FOR SENDING JPK FILES

### Summary

The document contains the instructions of installation and operation of the JPK application enabling the creation, validation, encrypting, signing and sending Standard Audit Files to the system of the Ministry of Finance.

Warsaw, January 2017

## Table of Contents

Programme installation.....	2
Start up.....	2
Logging in.....	5
First start up of the application.....	5
User profile creation.....	5
Main Menu.....	7
Options Menu.....	8
Defining the Working catalogue.....	8
Defining the location of the cryptographic card driver reader file.....	9
Send the document menu.....	12
Selection of documents to send.....	12
Encryption key.....	14
Documents processing.....	15
Appending a qualified signature.....	16
Summary of the sending process and document sending.....	19
Status of documents sending Menu.....	21
History Menu.....	22
Tools Menu.....	24
Save the backup copy.....	24
Recover data from the backup copy.....	24
Management of certificates and symmetric keys.....	25
Conversion of CSV file to XML Menu.....	27
Explanations concerning generating of the CSV file.....	29

## Programme installation

1. Click the installation file twice,
2. Click the **Next** button,
3. Choose location where the installer should install the application. Default location is: C:\JPK\Klient JPK 2.0 and click **Next**,
4. Click **Install**,
5. Wait until the installer completes installation of files, which will be communicated by the change of window,
6. Click the **Finish** button,
7. The installation will be completed and the use of Klient JPK 2.0 application may be started.

## Start up

After launching of the application a start screen will appear containing three action buttons:

- **Check availability of updates** – checks whether available software updates exist,
- **Update** – updates the application to the latest available version,
- **Continue** – goes to the screen of logging to the application,

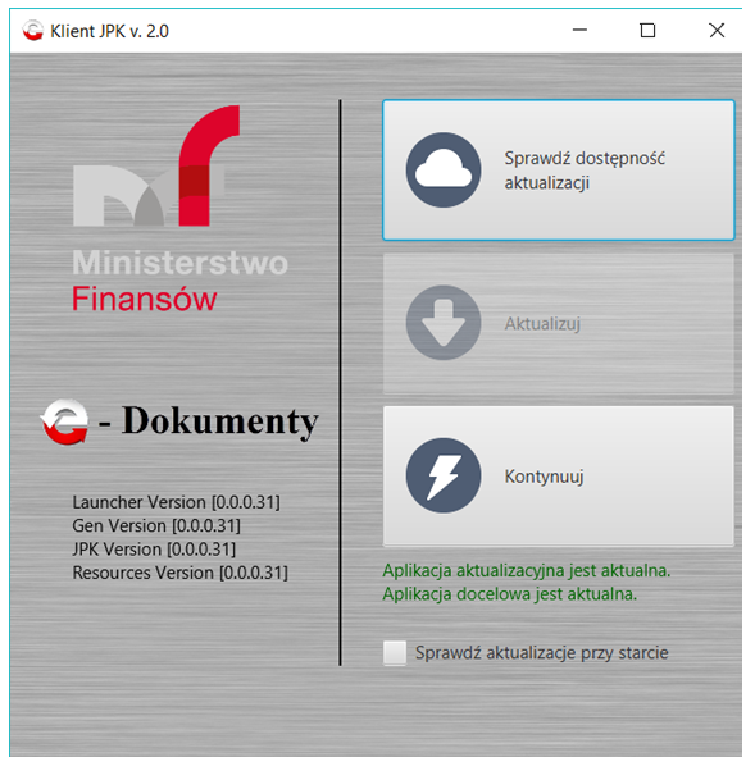


Only the **Check availability of updates** button is active.

After clicking the application will verify whether an update is available. In case the update is available, the remaining buttons will activate.

- The **Update** button – the application will update to the latest available version.
- The **Continue** button – the application will go to the [Log in](#) button.

**Note!** The **Continue** button will be active and it will enable transfer to the next screen of the application only if the available update is not critical for operation of the application. The relevant communication will be displayed on the screen after verification of update availability.



**Note!** In case if the following message is displayed under the buttons:

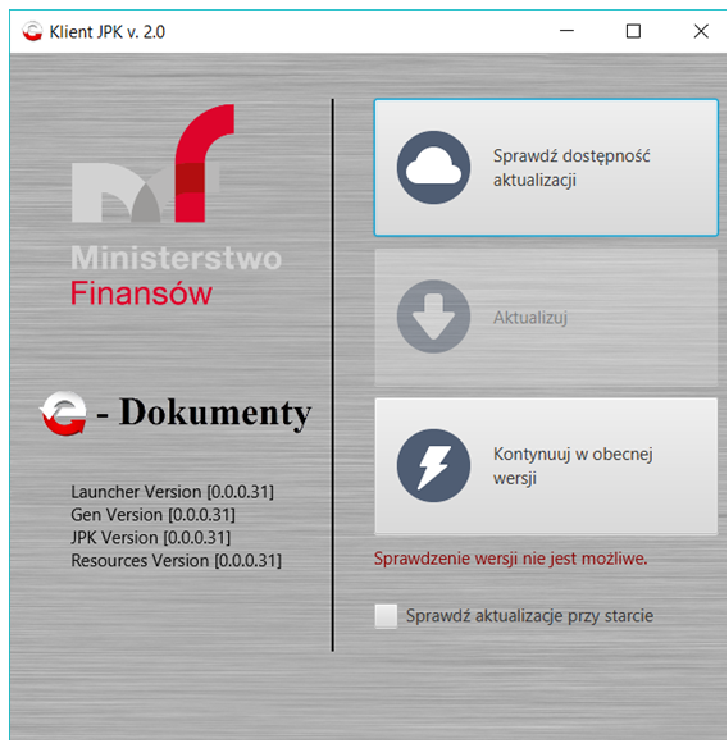
The update application is not valid.  
The application is not valid.  
The application is critical.

After clicking the **Update and close the application** button, the application will be closed. Following re-start of the application, the following message will be displayed:

The update application is valid.  
The application is not valid.  
The application is critical.

The **Update** button should be chosen, which will cause finishing of the application updating process. After completion of the update the **Continue** button will be activated. Upon clicking the **Continue** button transfer to the [Log in](#) screen will occur.

**Note!** In case if checking of updates is not possible, the following message will be displayed: **Checking of version is not possible** and the button: **Continue in the current version** will be displayed. Upon its clicking the transfer to the [Log in](#) screen will occur.



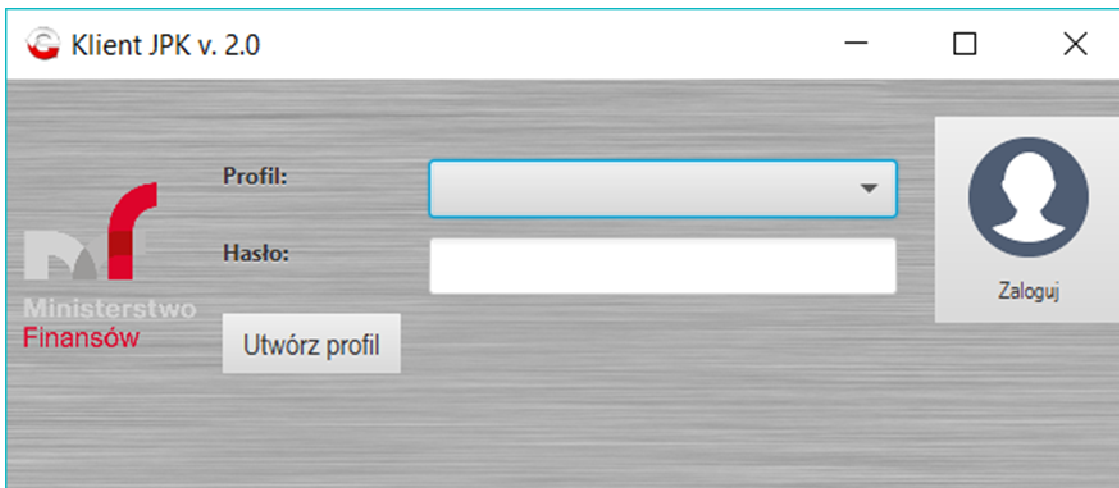
#### Additional options

- Check updates at the start - as a result of selection of this field, automatic checking whether the application update is available will take place after each start of the application.

**Note!** After each start of the application this field can be marked and checked. After completion of the work, the application remembers the last setting.

## Logging in

The application enables creating of user profiles. The access to the user profile is protected by password.



After entering the login and the password, and clicking the **Log in** button, the application goes to [Main Menu](#).

**Note!** The application does not give a possibility of change of recovery of user password. In case of password loss, a [new user profile](#) should be created.

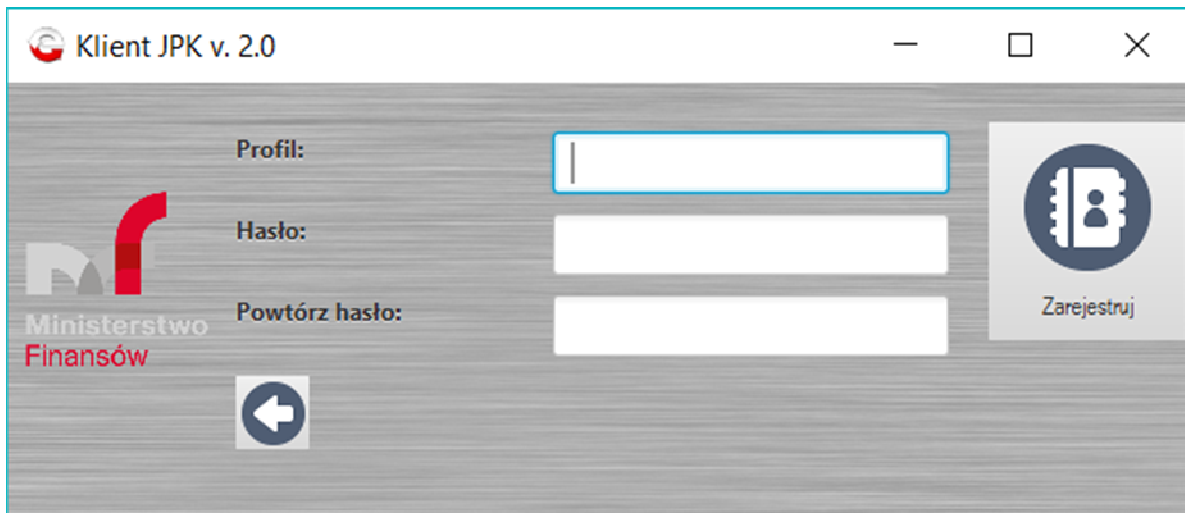
### First start-up of the application

1. Click the **Create profile** button.
2. The [user profile creation screen](#) will appear.

### User profile creation

This screen contains the form for creation of new application user.

1. All fields of the form should be filled in correctly.

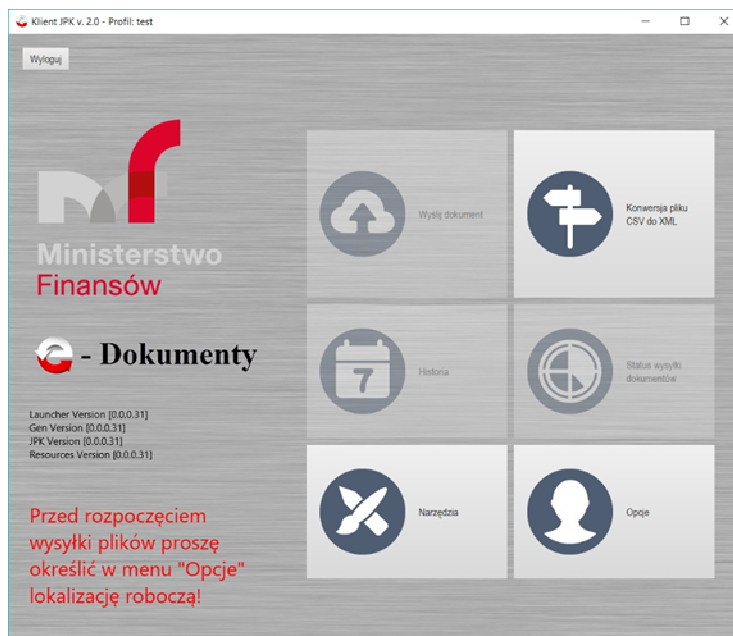


2. Click the **Register** button to create a user profile.
3. After registration of the profile, the application returns to the log in screen automatically.

**Note!** In the application requirements for the profile and the password are defined. The profile and the password must consist of at least three characters . Those fields must not contain Polish characters, However, they may contain non-letter characters, such as ; ' [ ] > ?).

## Main Menu

The Main Menu of the application contains six buttons whose clicking transfers to the relevant work



screen:

1. [Send the document](#)
2. [../AppData/Local/Temp/ Menu Wyślij dokument](#)Conversion of CSV file to XML
3. [../AppData/Local/Temp/ Menu Konwersja pliku](#)History
4. [../AppData/Local/Temp/ Menu Historia](#)Status of documents sending
5. [Tools](#)
6. [../AppData/Local/Temp/ Menu Narzędzia](#)Options

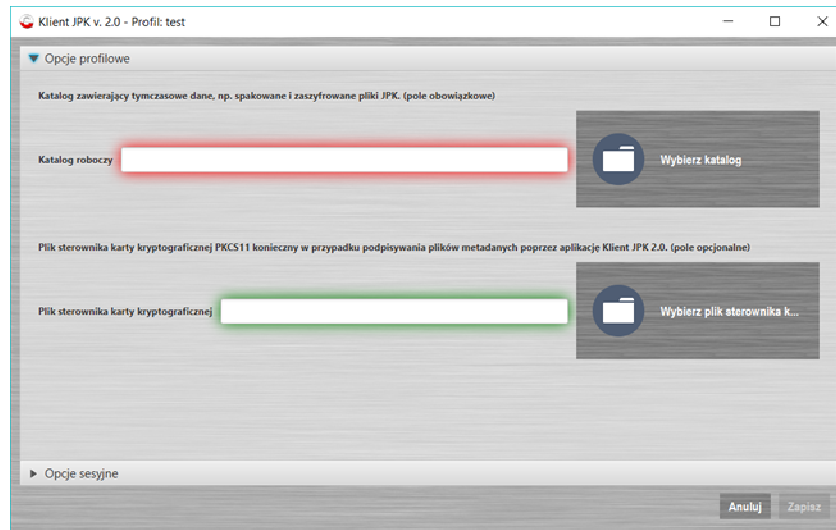
[../AppData/Local/Temp/ Menu Opcje](#)During the first launch of the application for a given user profile, **Send the document, History and Status of files sending** buttons are inactive. In order to enable sending of a document, setting of the application is required through defining of the working catalogue and indicating the file of the cryptographic card driver. On the main screen the following message is displayed:

**Before starting  
file sending, please  
define working location  
in the "Options" menu!**

In order to define the working location as well as indicate the file of the cryptographic card drivers, the **Options** button should be selected, which transfers to the [Options](#) Menu.



## Options Menu



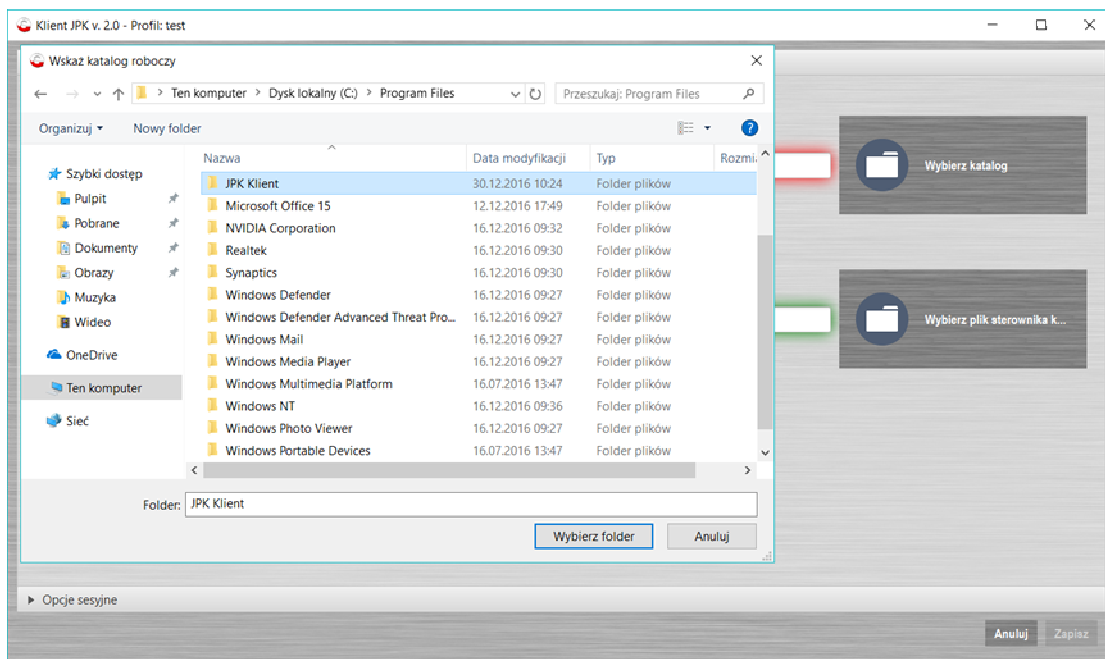
The Options Screen contains two fields:

1. [Working catalogue](#)
2. [Cryptographic card driver file](#)

### Defining the Working catalogue

In order to define the working catalogue, the following operations should be performed:

1. Click the button: **Select catalogue** which launches file explorer. By default the explorer indicates a catalogue in which the application is installed.
2. select a catalogue to act as the **Working catalogue**.
3. click **Select a folder**, which approves the selection made.
4. after clicking **Select a folder**, the application automatically returns to the [Options](#) menu.



In the example presented above the working catalogue with the following name was selected: **JPK Klient** in location **C:\Program Files\JPK Klient**.

### Defining the location of the cryptographic card driver reader file

On the option screen the following operations should be performed:

1. Click the **Select the cryptographic card driver reader file** button, which will launch a default file explorer. By default the explorer indicates a path: **C:\Program Files** (for the Windows system). Additionally the explorer will display only files with the extension relevant for cryptographic card drivers: **.dll** or **.so**.

**Note!** The name of the catalogue in which files of the installed card reader driver are located and the name of the file of this driver depend on the supplier of electronic signature card. At the same time, suppliers of the electronic signature card may require other drivers for the 32-bit and 64-bit Windows system.

Catalogues most commonly found for the Windows system:

C:\Program Files\nazwa programu do podpisu kwalifikowanego  
 C:\Program Files (x86)\ nazwa programu do podpisu kwalifikowanego  
 C:\Windows\System32

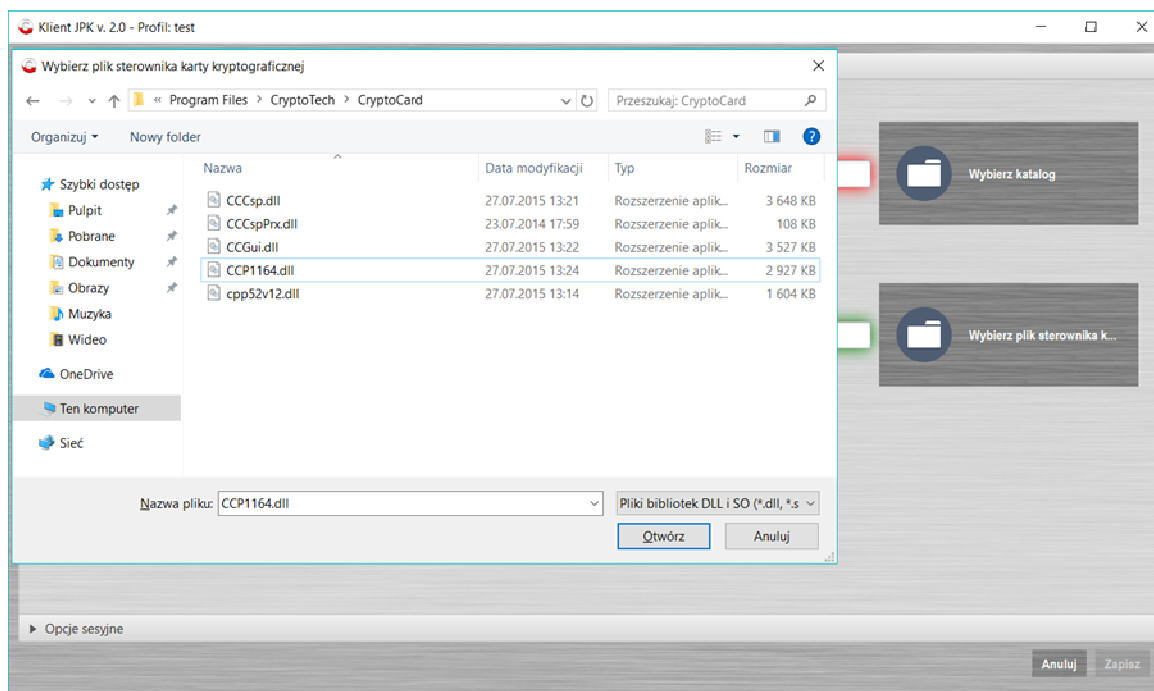
Examples of files of installed card reader driver for the Windows system:

CCPkiP11.dll  
 enigmap11.dll  
 cmP1164.dll  
 cmp11.dll  
 cryptoCertumPKCS11.dll  
 cryptoCertum3PKCS.dll

In case of indicating the incorrect cryptographic card driver file, the application will display the following message in an additional window: **Incorrect file of PKCS11 driver!**

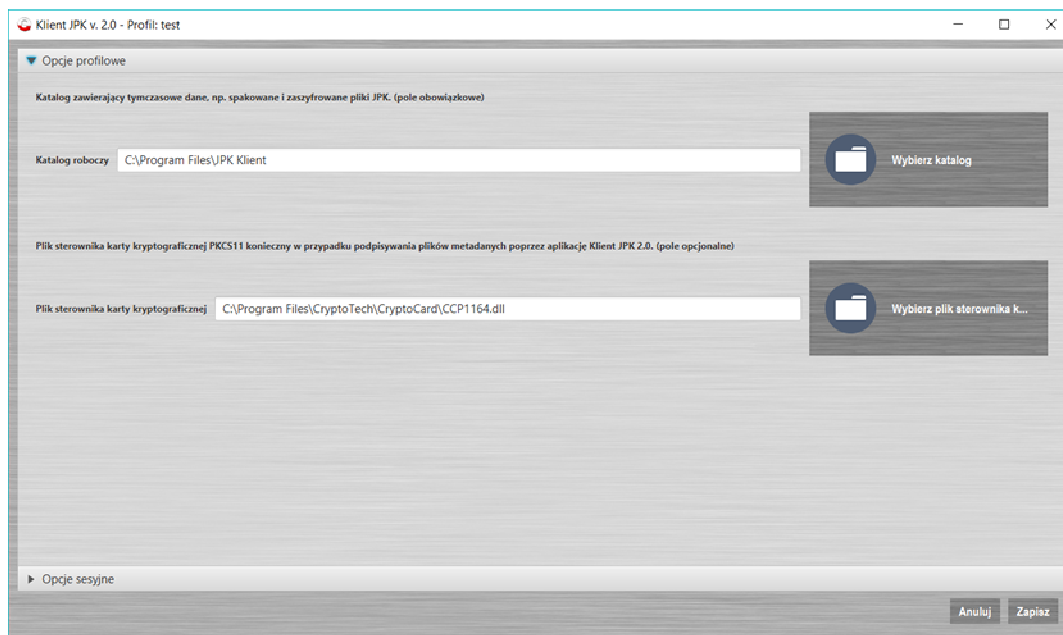
**In case of difficulties in defining the location or the name of the driver file contact with the qualified signature provider is required.**

2. Select the cryptographic card driver file
3. Clicking **Open** accepts the cryptographic card driver file selection.
4. Click **OK** on the confirmation screen.
5. After clicking **OK**, the application automatically returns to the [Options](#) menu.



#### Saving changes of the Options screen

The selected working location and location of the cryptographic card driver file should be saved in the memory of the application through clicking the **Save** button located in the bottom right hand corner of the [Options](#) menu. The application returns to the [Main Menu](#) automatically.



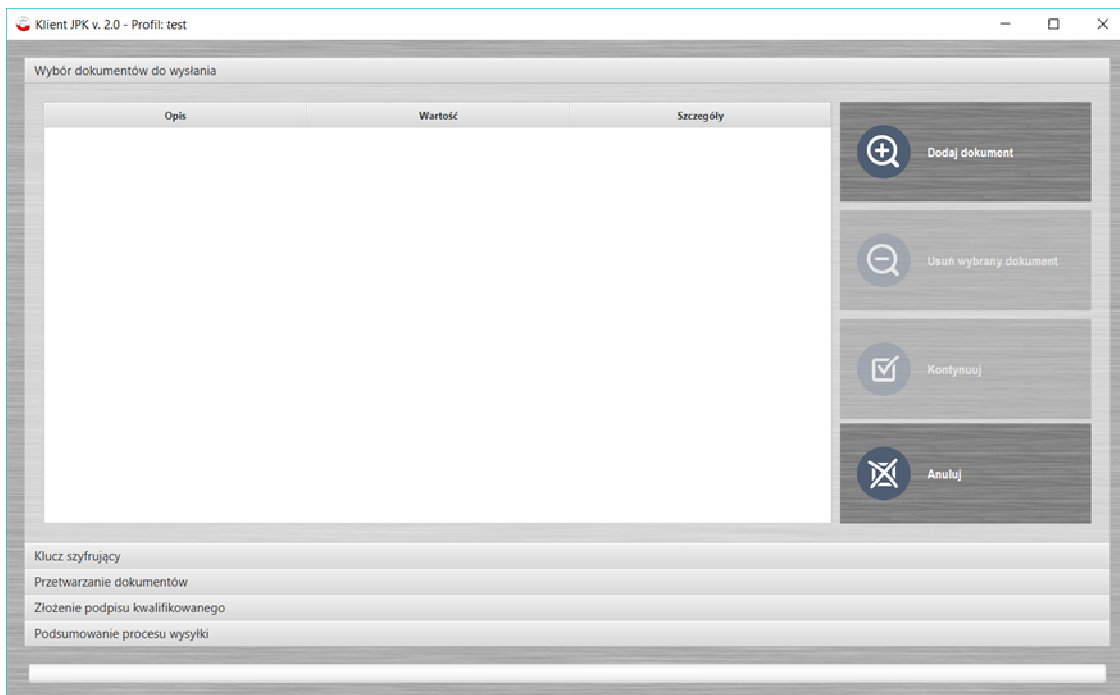
### Canceling changes of the Options screen

In order to cancel introduced changes, the **Cancel** button in the bottom right hand corner of the [Options](#) menu should be clicked. The application returns to the [Main Menu](#) automatically.

## Send the document menu

In order to start sending the JPK document to the Ministry of Finance, the **Send the document** button should be selected.

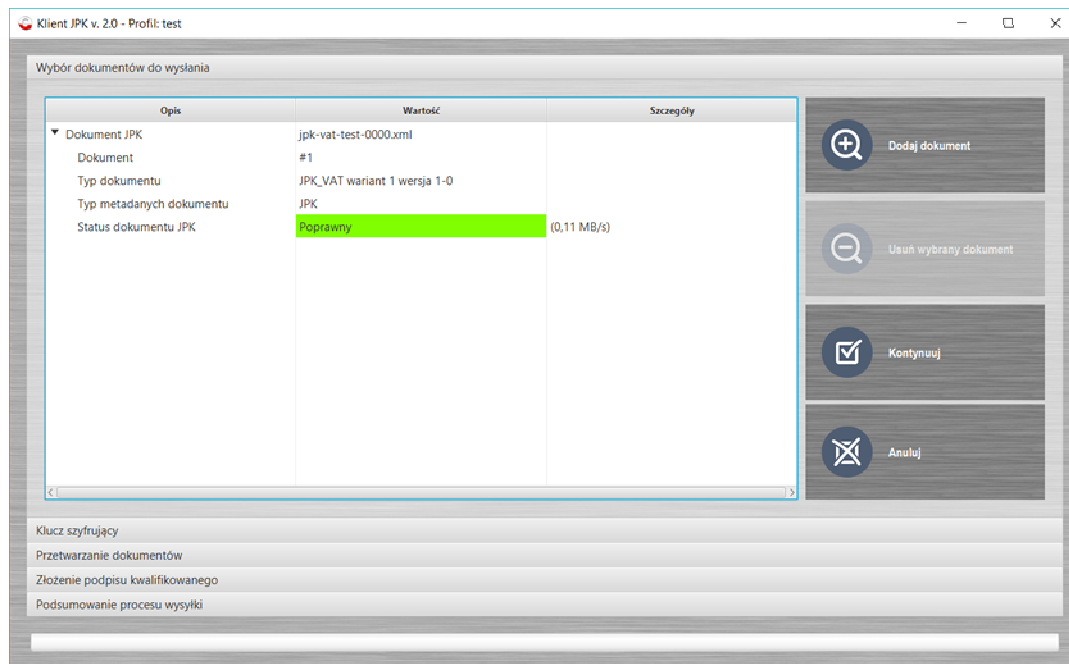
The process of sending starts from the [Selection of documents to send screen](#), enabling the selection of appropriate documents to be sent.



## Selection of documents to send

1. Click the **Add a document** button which will launch a default of file explorer in the **This computer** location (for the Windows 10 system).
2. Select the document location and the document to be send.
3. Clicking of **Open** accepts the document selection made.
4. After the selection of the document the application returns to the Selection of documents to send screen, on which it additionally displays details of the document or documents in three columns:
  - ⇒ Description - the column contains descriptions of the selected file in the drop-down menu
    - ▼ JPK document
      - Document
      - Document type
      - Type of document metadata
      - Status of JPK document
  - ⇒ Value - the column contains values of description of the selected document to be sent
    - Document name

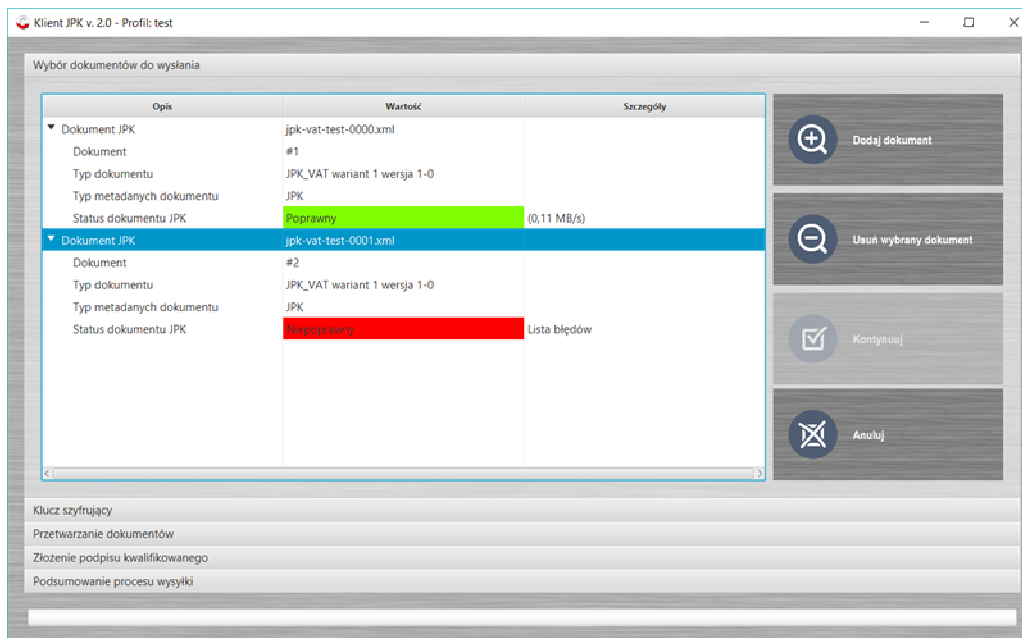
- Number of selected document assigned by the application in a given sending session
  - Name of recognised the JPK scheme
  - Type of document sending: JPK (for cyclical sending) or JPKAH (for sending on request)
  - **correct** on the green background or **incorrect** on the red background
- ⇒ Details - the column contains additional details for the selected file, e.g. the speed of file uploading to the application or the list of errors for an incorrect document.
5. Transfer to the next stage of the sending process takes place through selecting the button: **Continue** – the next [screen: Encryption key](#).



**Note!** The application will enable the transfer to the next stage of the document or documents sending process only after deleting of all documents validated as incorrect – [Removal of selected documents](#).

## Deleting of selected documents

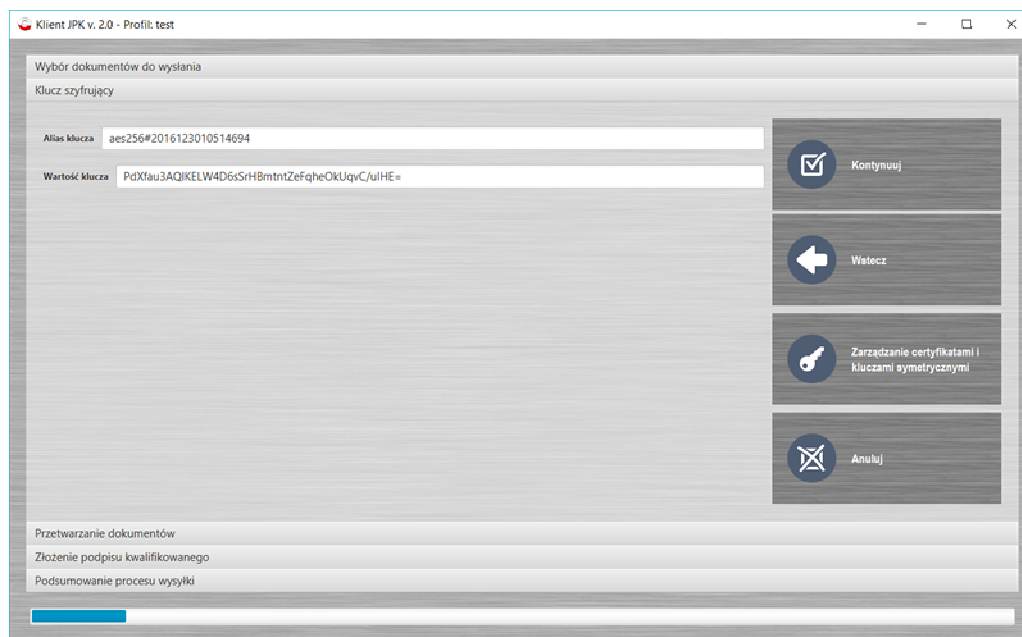
In order to delete the selected document from the list, the document should be checked (any row describing the document), and then the **Remove selected document** button should be clicked.



## Encryption key

The key serves for optional management of certificates and symmetric keys.

The application is programmed so that it sets the **Key alias** and the **Key value**. This enables moving to the next stage of the sending process through clicking the **Continue** button – [Documents processing screen](#).

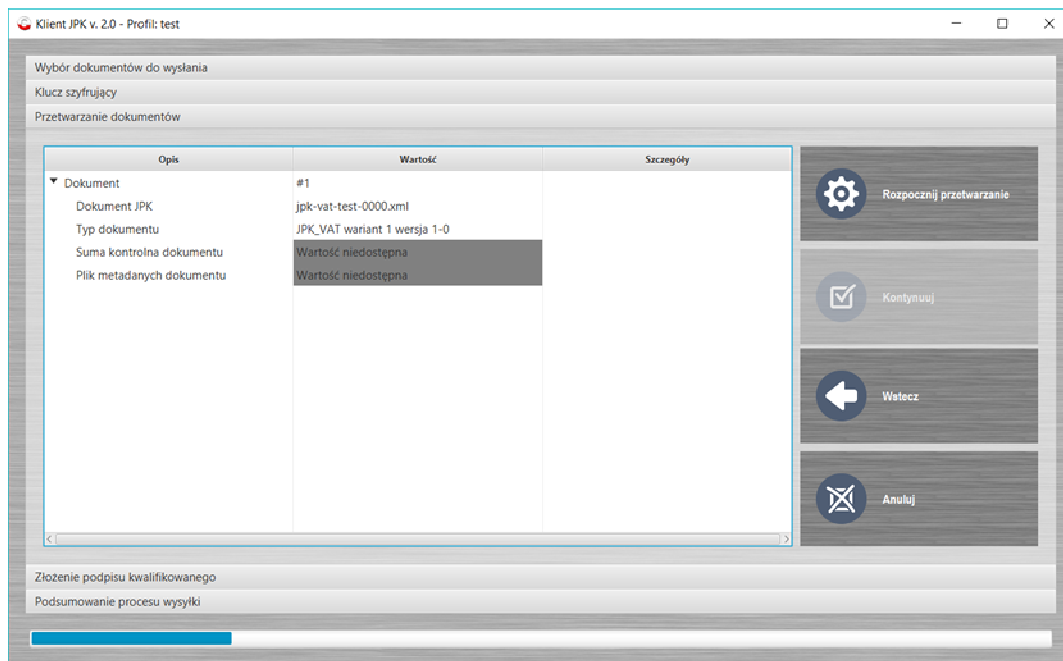


## Management of certificates and symmetric keys

In order to launch the optional process of management of symmetric keys the **Management of certificates and symmetric keys** button should be clicked. Clicking the button will cause transfer to the Management of symmetric keys [screen](#).

## Documents processing

The screen serves for processing of documents and presents the most important information on documents to be processed attached at the previous stages.



1. Click **Start processing** – the application will prepare the metadata file for the selected document and prepare the document for signing with the qualified signature.
2. The application displays the relevant message related to the metadata file of the document:
  - The text: **Data in the binary format** is displayed on the green background if the metadata file of the document is correct.
  - The text: **Data in the binary format** is displayed on the red background if the metadata file of the document was not verified or if the metadata file of the document is incorrect.
3. If the text **Data in the binary format** for all documents is displayed on the green background, the **Continue** button may be selected and the next stage of the sending process should be followed - moving to the [Qualified signature screen](#).

## Additional operations (optional)

Lines: **JPK document**, **Document control sum** and **Document metadata file** in the **Value** column has additional operations associated with file processing. The list of operations is displayed after clicking on the relevant row in the value column with the right mouse button.

For the **JPK document** row the following list of operations is available:

- Open - triggers additional programme opening a file for preview
- Show the path - displays a window with information concerning the path for file location



- Show folder with this file - launches File Explorer and opens the folder in which the indicated file is contained

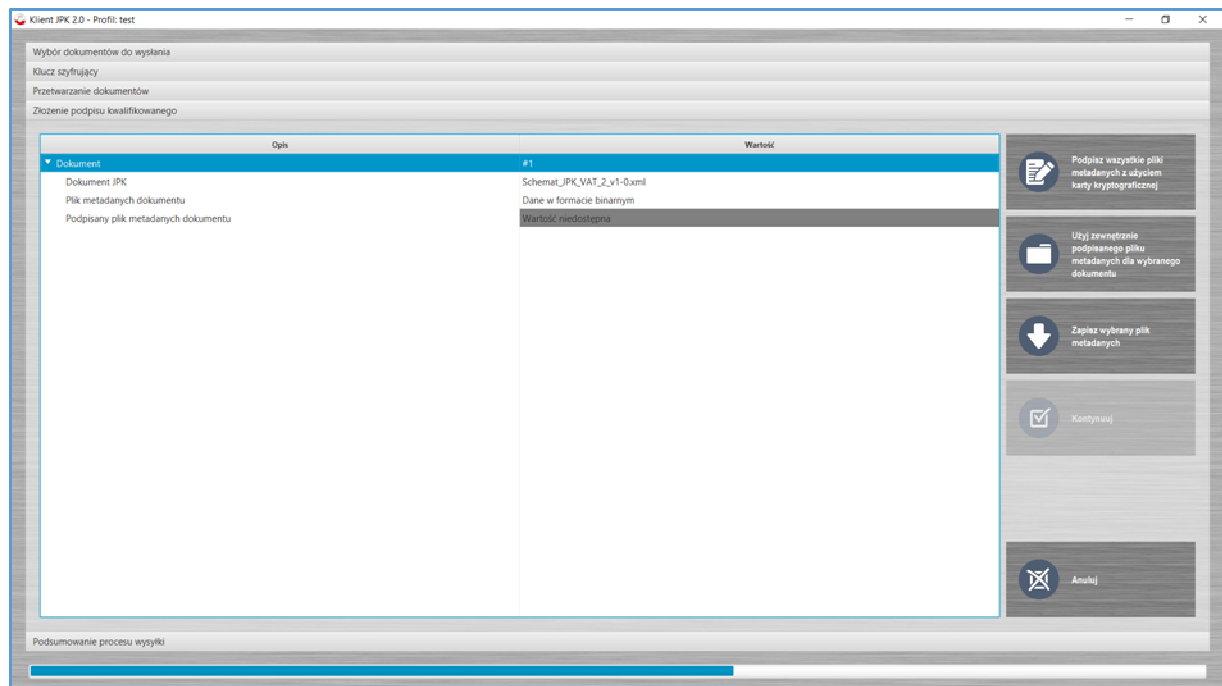
For rows: **Document control sum** and **Document metadata file** the following list of operations is available:

- Write to file – launches File Explorer and enables file saving in selected location
- Show binary data as text
- Show Base64 coded binary data
- Show binary data in hexadecimal format

Selection of any **Show** operation displays a window with binary data in the format relevant for the description of the operation.

### Appending a qualified signature

The screen shows the stage of signing documents with a qualified key through the use of a cryptographic card or [the use of externally signed metadata file for selected document](#).



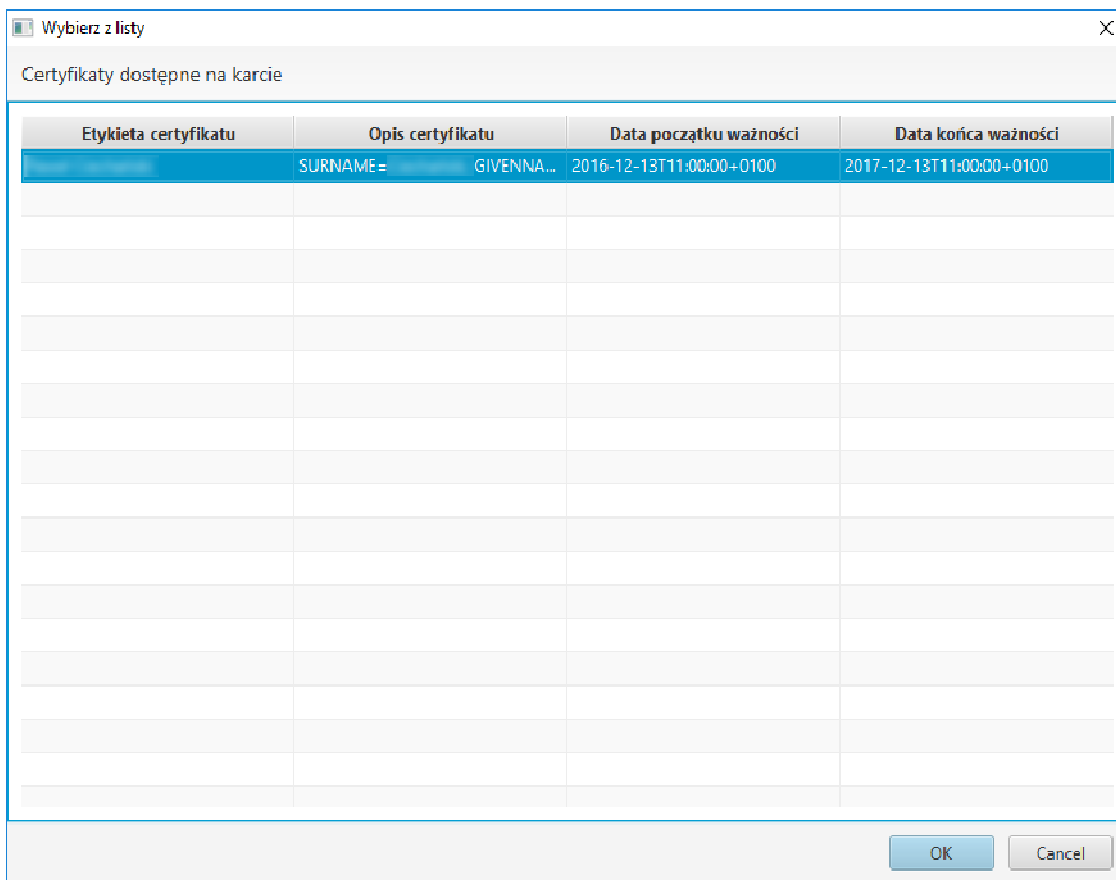
### Signing metadata files with a cryptographic card, using the Application

The Application enables signing of metadata files with the use of a cryptographic card, with no need to use the software dedicated for the qualified signature.

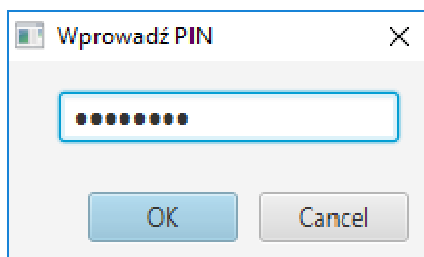
In order to use this functionality, the following operations should be performed:

1. Click **Sign all metadata files with the use of a cryptographic card**.

2. Select the certificate for file signing.



3. Accept the certificate selection by clicking the **OK** button.
4. Enter PIN code for file signing.



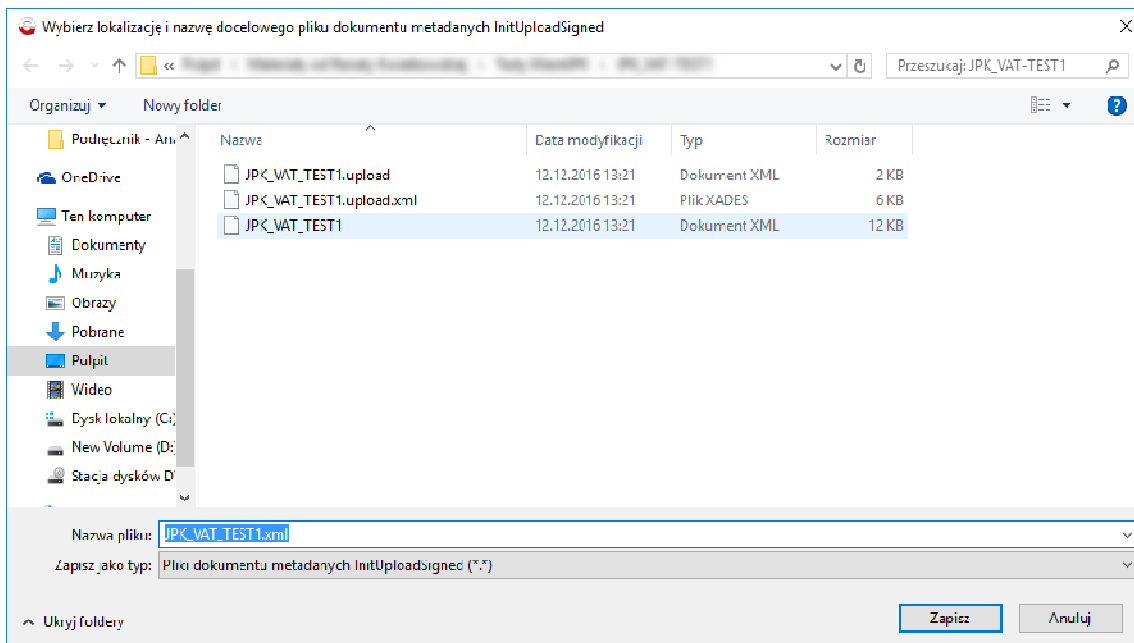
5. Accept the PIN code by clicking the **OK** button.
6. The process of signing the metadata file for the document using the application has been completed.

**Note!** Some qualified signatures may require entering the PIN code for each signed document separately.

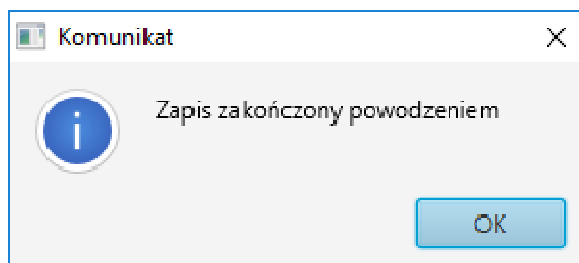
7. Click **Continue** in order to go to the next stage – [Summary of the sending process screen](#).

### Use of externally signed metadata file for the selected document

1. In order to unblock the metadata file record any field in the **Value** column should be clicked.
2. Click **Save selected metadata file**.

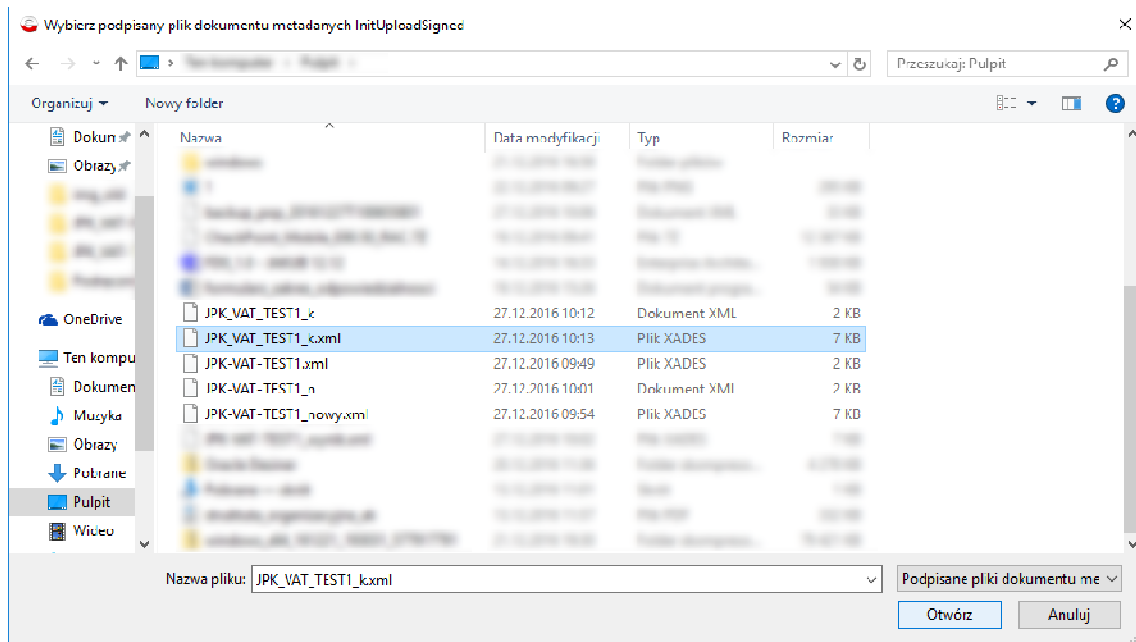


3. Click **Save** after selecting the location where the metadata file should be saved.
4. Click **OK** on file saving confirmation.



5. Sign the metadata file with the use of the qualified signature held.
6. Click **Use externally signed metadata file for the selected document**

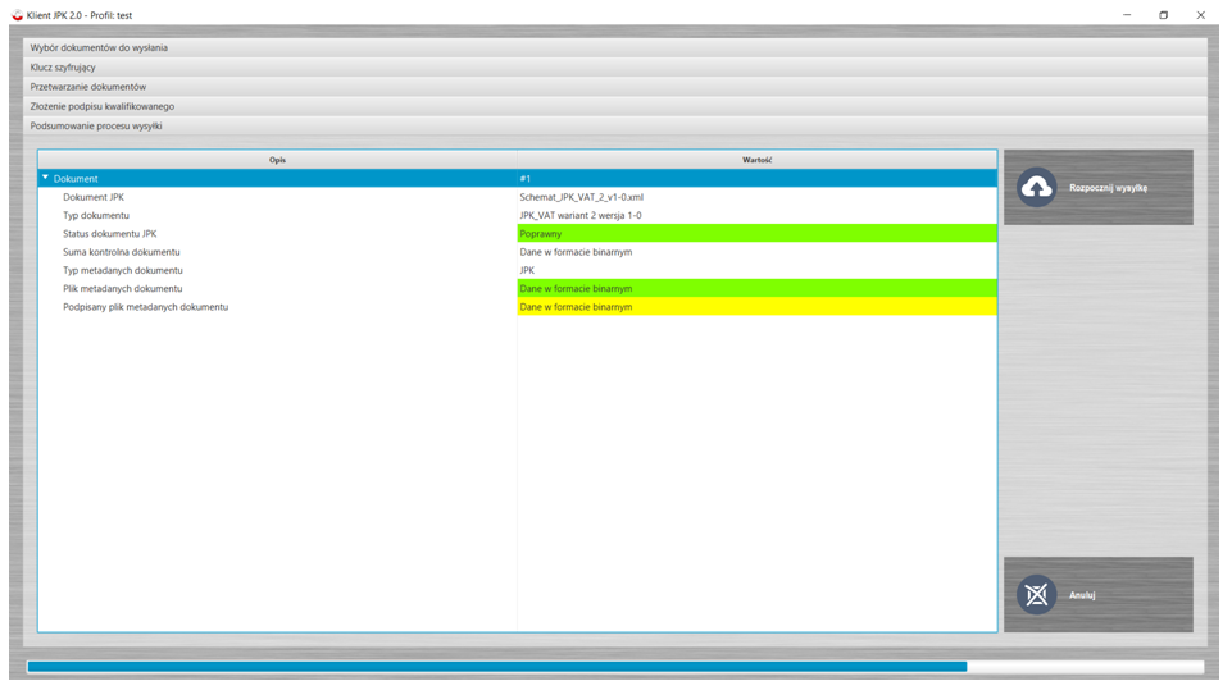
7. Select the signed metadata file for signing a file from location defined earlier and confirm by clicking the **Open** button.



8. Click **Continue** in order to go to the next stage – [Summary of the sending process screen](#).

### Summary of the sending process and document sending

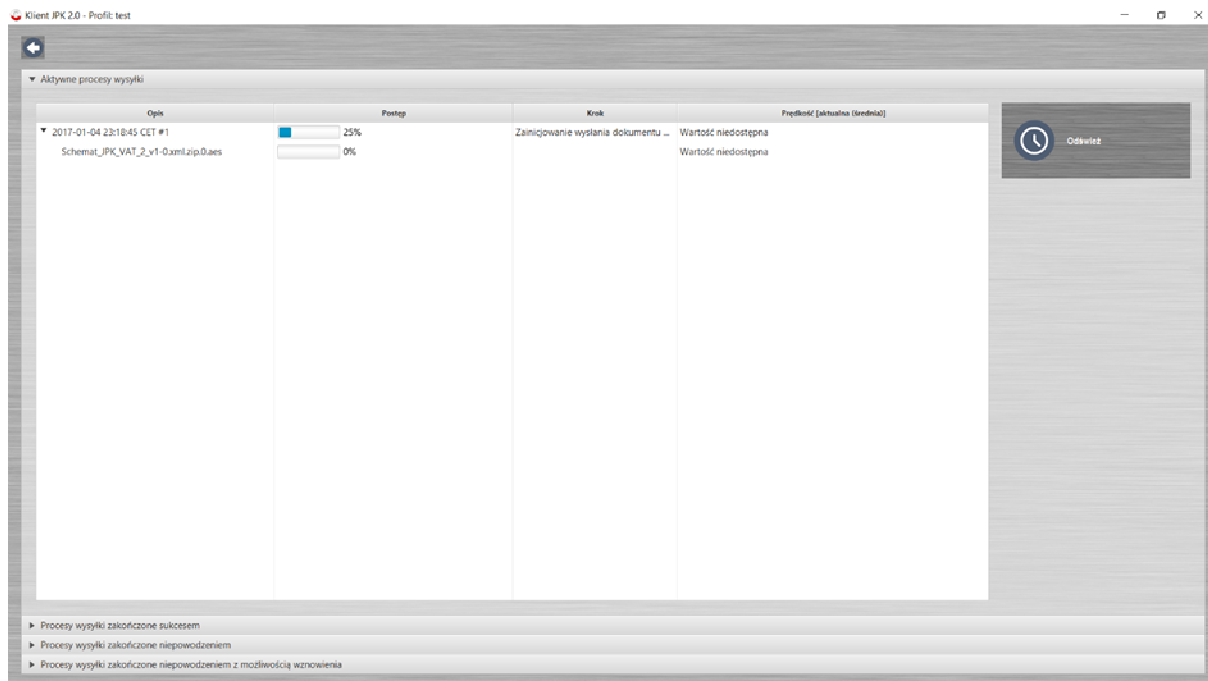
In order to send the document prepared the following operations should be performed:



1. Analyse information concerning the document. Information in the **Value** field for rows: **JPK document status**, **Document metadata file** and **Signed document metadata file** should be displayed in **green**. In case if information for the **Signed document metadata file** row is displayed in **yellow**, it means that the application was unable to validate a correctly signed

document metadata file, but sending is still possible. The final verification of the signed metadata file will be performed by the Ministry of Finance.

2. Click **Start sending**.
3. Analyse the message from the file sending process.
4. After clicking the **OK** button, the sending process will be completed. Automatic transfer to the Active sending processes screen will take place in the [Menu: Status of documents sending](#), in which information concerning the sending status in the active process will be displayed.



## Status of documents sending Menu

The Status of documents sending Menu presents information concerning the status of documents sending accomplished in the current sending session.

Information on the sending process is available on the relevant screen after clicking the appropriate bar at the bottom of the screen:

- ▶ Sending processes completed successfully
- ▶ Sending processes completed unsuccessfully
- ▶ Sending processes completed unsuccessfully, with a possibility of resumption

**Note!** In case of a sending process completed unsuccessfully, e.g. due to interruption of the internet connection or other technical problem preventing document sending, a possibility to resume the process exists. For that purpose it is necessary to:

1. Select the tab: **Sending processes completed unsuccessfully, with a possibility of resumption**, which will display the list of sending processes completed unsuccessfully, which can be resumed.
2. Select the process to be resumed.
3. Click the **Retry** button.

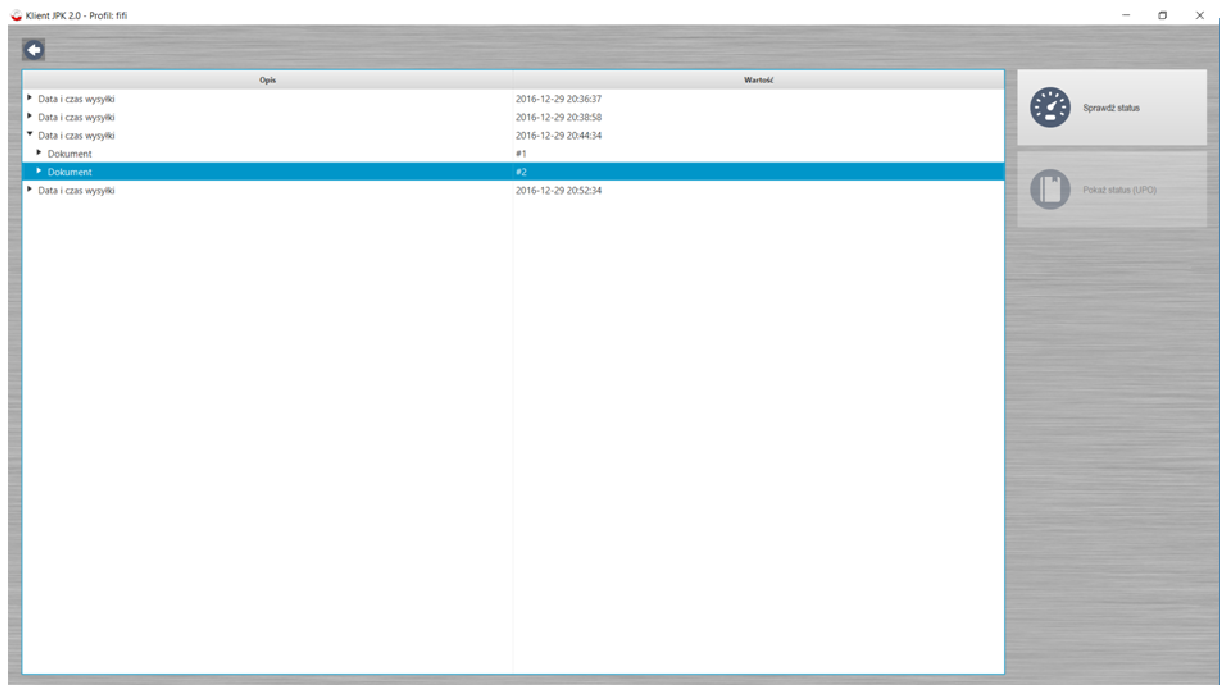
**Note!** The screen containing statuses of file sending stores the data only until logging out from the application.

Detailed information concerning the status of document processing by the Ministry of Finance may be checked through clicking the **History** button in the [Main Menu](#).

In order to return to the [Main Menu](#) the arrow in the top left hand corner of the screen should be clicked.

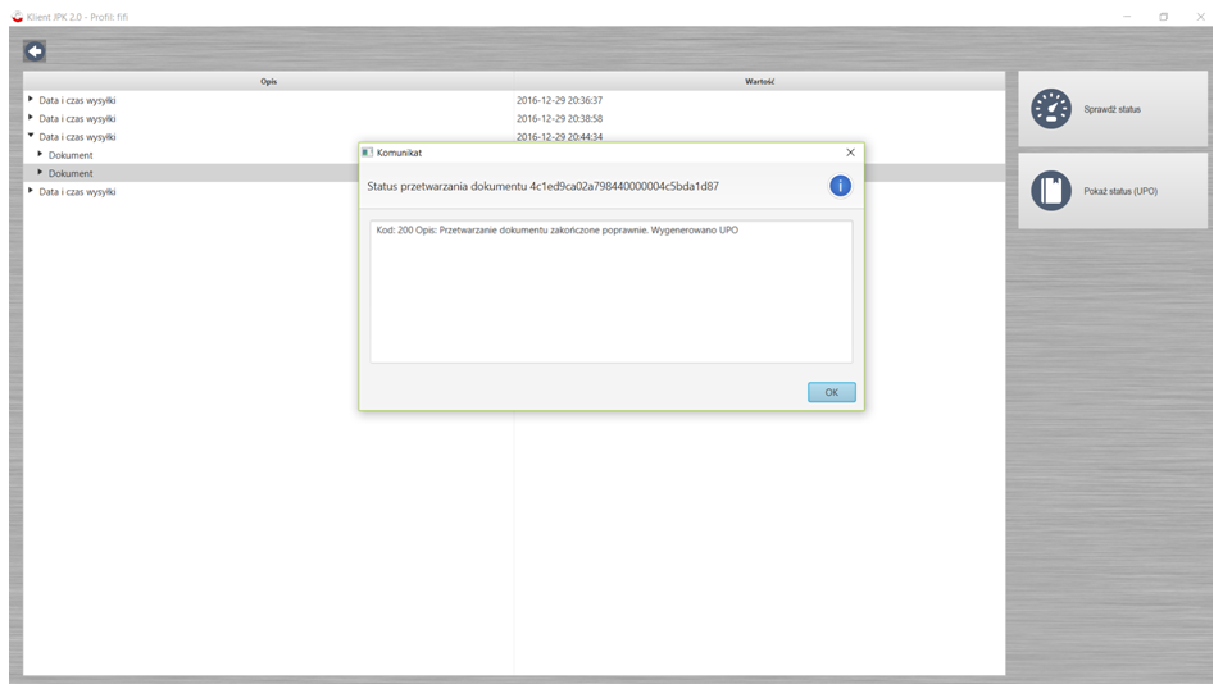
## History Menu

The history screen saves operations of JPK files sending for all sending sessions performed so far.



In order to view information on the status of documents sent in historic sessions, the following operations should be performed:

1. Select a sending session described in the **Value** column with the date and hour.
2. Click the arrow placed on the left hand side of the text: **Sending date and time** which will result in developing information concerning individual documents sent in a given session.
3. Check the selected document. This will trigger the **Check the status** button.
4. Click **Check the status**.
5. Analyse the displayed message on the status of file sending.

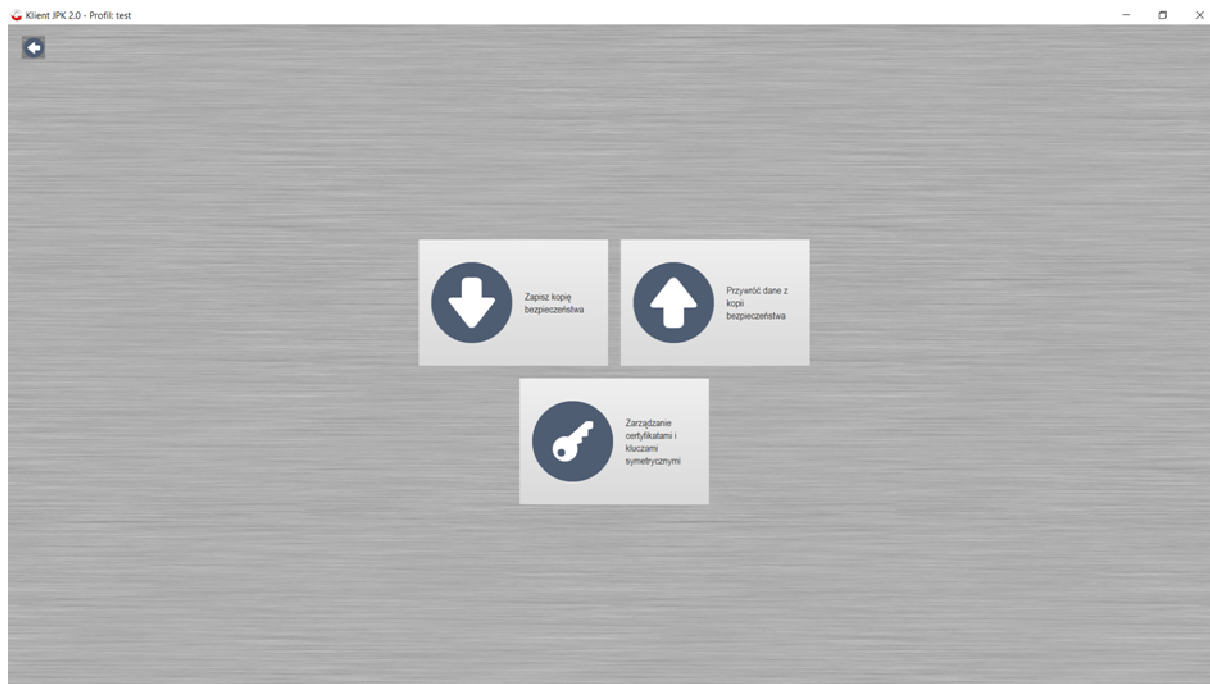


6. Click **OK** to close the message.
7. In case the UPO was generated, the **Show the status (UPO)** button will be triggered.
8. Clicking the **Show the status (UPO)** button will generate the UPO document in the .pdf format, which will open in the default programme operating .pdf files.
9. In order to return to the [Main Menu](#) the arrow in the top left hand corner of the screen should be clicked.



## Tools Menu

The screen contains three tools enabling preparation and management of files for the process of sending JPK files:



1. [Save the backup copy](#)
2. [Recover data from the backup copy](#)
3. [../AppData/Local/Temp/ Przywróć dane zManagement of certificates and symmetric keys](#)

### Save the backup copy

1. Click the **Save the backup copy** button.
2. Select the place and the folder for saving a backup copy.
3. Confirm the selection by clicking the **Select the folder** button.
4. Close the message informing of the saving status through clicking the **OK** button.
5. Saving of the backup copy is complete.

### Recover data from the backup copy

1. Click the **Recover data from the backup copy** button which will launch a default file explorer in the **This computer** location (the Application displays files with .xml only, where the backup copy is saved).
2. Select the file location and the data file containing data required for recovery.
3. Click the **Open** button accepting the selection of data to be recovered.
4. Enter the log-in password in order to confirm data recovery from the backup copy.
5. Close the message through clicking the **OK** button.

## Management of certificates and symmetric keys

The screen contains two management options:

1. Certificates management
2. Symmetric keys management

### Certificates management

1. Click the **Management of certificates and symmetric keys** button
2. Select the required action among three available actions:
  - a. Upload the current certificate – loads the current certificate through clicking the **Upload the current certificate** button
  - b. Upload the certificate from the file - loads the required certificate from the file:
    - i. Click **Upload certificate from the file**
    - ii. Select the required file containing the certificate
    - iii. Confirm the selection of the file with the certificate through clicking the **Open** button
  - c. Save the certificate in the database - saves the certificate to the base



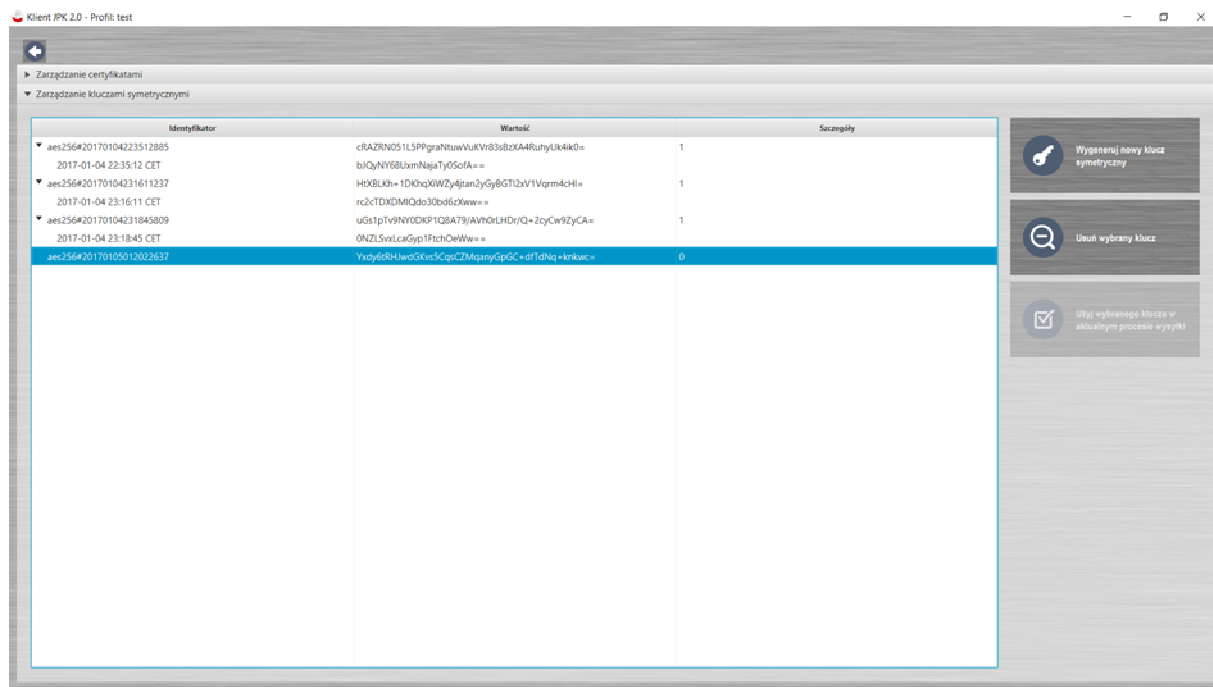
### Symmetric keys management

The screen contains current symmetric keys and includes three options:

1. [Generate a new symmetric key](#)
2. [Delete the selected symmetric key](#)
3. [../AppData/Local/Temp/ Usuć wybrany kluczUse the selected symmetric key](#)

[../AppData/Local/Temp/ Użyj wybranego klucza](#)Generate a new symmetric key

1. Click the **Generate a new symmetric key** button
2. The new generated key will automatically add to the table presenting available keys



*Delete the selected symmetric key*

1. Select and check the key from the table displaying available symmetric keys
2. Click the **Delete the selected key** button
3. The deleting process is complete

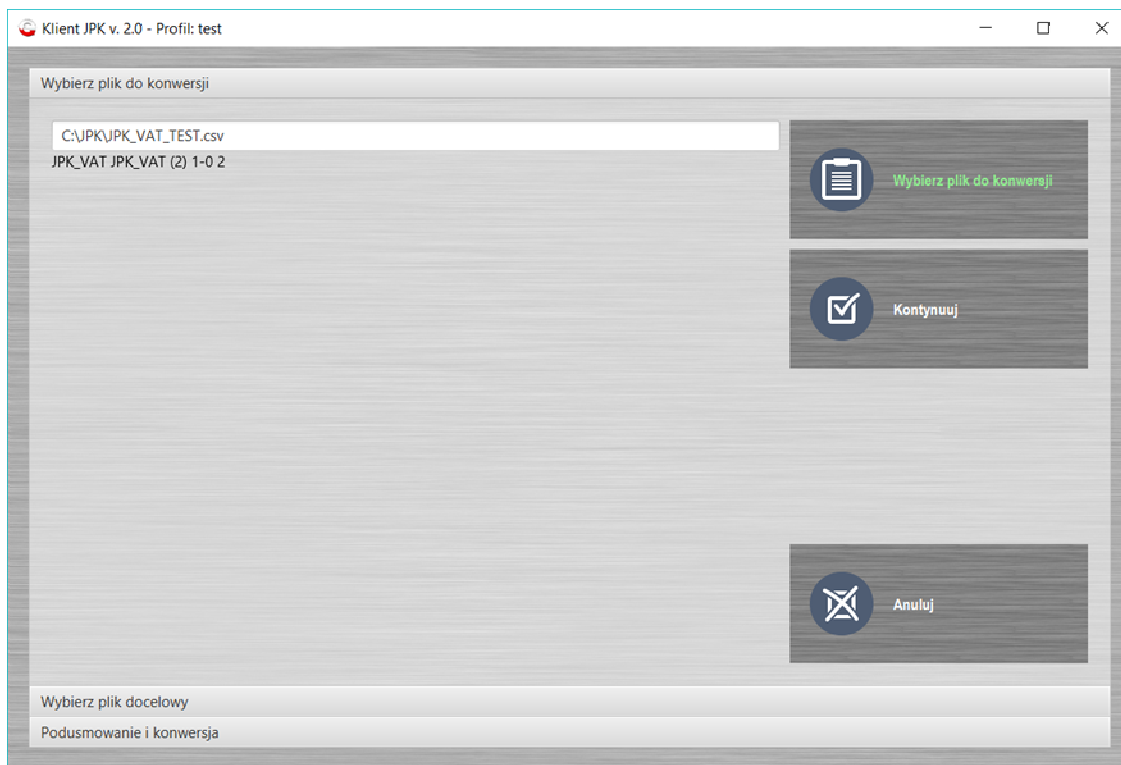
**Note!** In case of starting the sending process and moving during its execution to the symmetrical keys management process, it will not be possible to delete the key selected in a given sending process.

*Use the key selected in the current sending process*

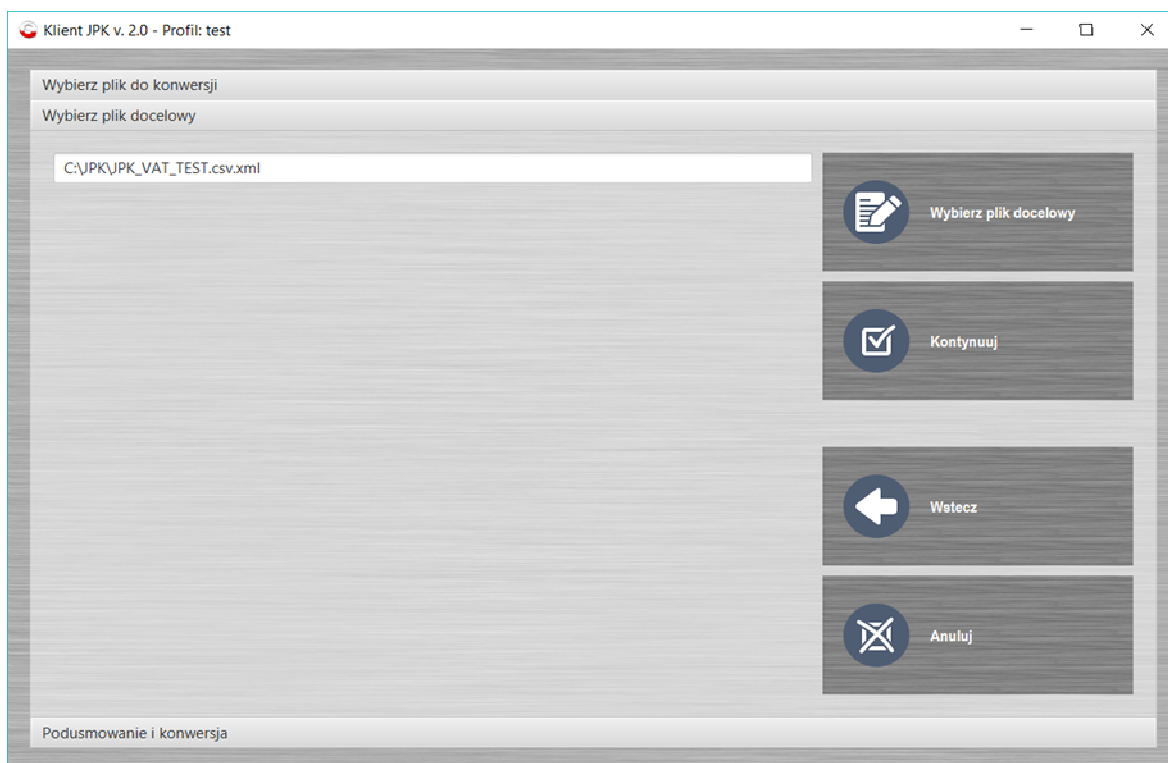
1. Select and check the key from the table displaying available symmetric keys through clicking the left mouse button.
2. Click the **Use the key selected in the current sending process** button.
3. The key selection process is complete.

## Conversion of CSV file to XML Menu

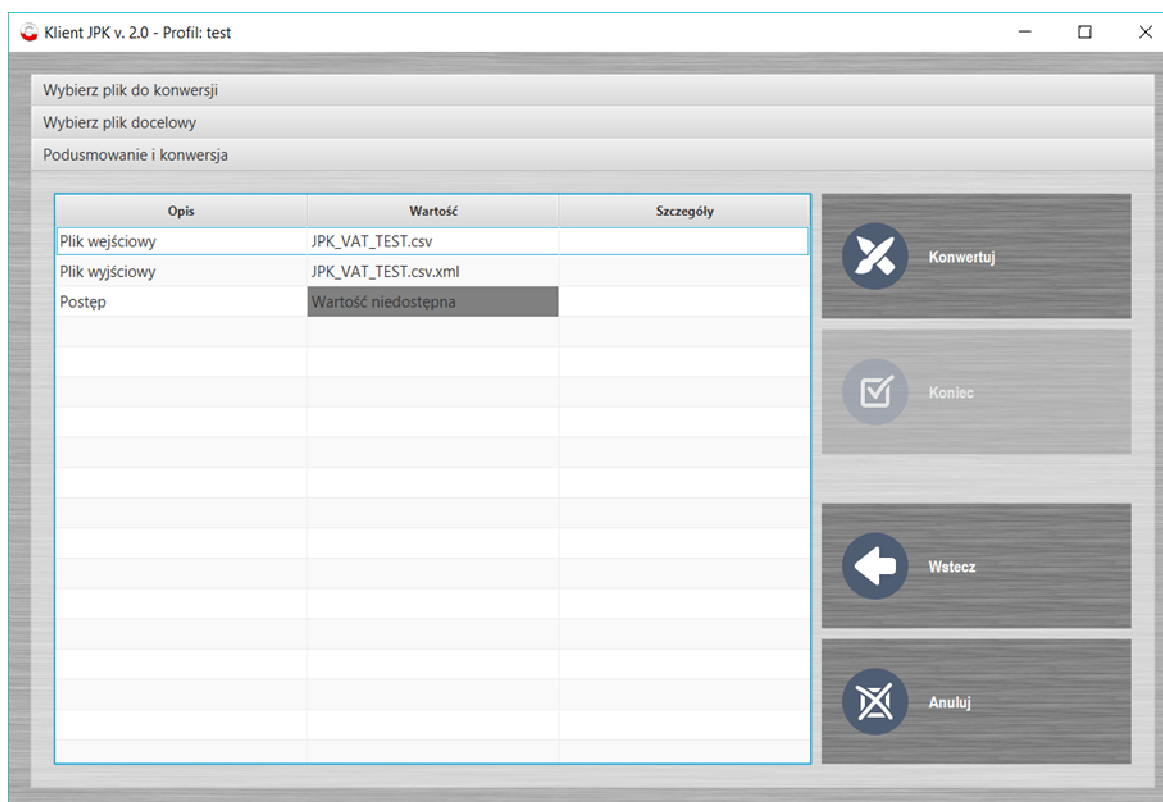
1. Click the **Conversion of CSV file to XML** button.
2. Click the **Select a file for conversion** button.
3. Select the required CSV file to be converted to the XML format.



4. Confirm the selection through clicking the **Open** button
5. Click the **Continue** button to go to the next stage of the process – Select the destination file



6. Click **Select the destination file** and select or enter the name and place where the file converted to XML should be saved.
7. Confirm the selection through clicking the **Open** button.
8. Click the **Continue** button to go to the next stage of the process – Summary and conversion



9. Click the **Convert** button.
10. The **Finish** button returns to the [Main Menu](#).

#### Explanations concerning generating of the CSV file

**Note!** Generating of the CSV file from local source data (XLS, ODS, database) does not guarantee its accuracy. Only the adequate formatting of generated data in the CSV file or the adequate formatting of source data and generating of the CSV file may guarantee the expected accuracy.

Examples of CSV files for variant 1 and 2 of JPK\_VAT, made available on the website of the Ministry of Finance <http://www.mf.gov.pl/kontrola-skarbowa/dzialalnosc/jednolity-plik-kontrolny> in the link “Client application for sending JPK files”, are illustrative files formatted correctly – the structure and format of the data is compliant with the requirements. Importing of an example in the client application will create a correct file in the XML format, compliant with a given JPK\_VAT scheme.

In the same location a document called “Specification of the CSV format of JPK documents” can be found, containing the description of the structure and format of data in the CSV file.