

Private Key Management

Version: 1.1

Global Payments Europe, s.r.o.

Created **19.2.2016**

Last update **13.6.2016**



SERVICE. DRIVEN. COMMERCE

globalpaymentsinc.com

Author	Dimitrij Holovka
Manager	
Approved	
Version	1.1
Confidentiality	Confidential

Document history:

Version	Date	Author	Comments
1.0	19.2.2016	D. Holovka	Initial document version
1.1	29.3.2016	D. Holovka	Corrections

Table of contents

1.	Formula clause	3
2.	Introduction	4
2.1	General GP webpay security principle	4
2.1.1	How to obtain the private key	4
2.1.2	PKI functions	4
2.2	Using PKI in GP webpay	5
2.2.1	Ways of use	5
2.2.2	Message integrity verification	5
2.2.3	Message sender identity verification	5
3.	Private key and its management	7
3.1	Private key in general	7
3.2	How to obtain the private key	7
3.2.1	History	7
3.2.2	The present	8
3.3	The private key management	9
3.3.1	Format update	10
3.3.2	Password change	14
3.3.3	For developers	17



1. Formula clause

This document including any possible annexes and links is intended solely for the needs of an e-shop service provider (hereinafter referred to as "Customer").

Information included in this document (hereinafter referred to as "Information") are subject to intellectual property and copyright protection of the Global Payments Europe, s.r.o. (hereinafter referred to as "GPE") and are of a commercially confidential nature in accordance with the provisions of the section 504 of the Act No. 89/2012 Coll., Civil Code. The Customer is aware of the legal obligations in relation to the handling of Information.

Information or any part thereof may not be provided or in any way made available to third parties without the prior written consent of the GPE. At the same time, Information may not be used by the Customer for purposes other than for the purpose for which it serves. To avoid any doubts, without the prior written consent of the GPE, Information or any part thereof may be provided or in any way made available neither to companies providing payment processing services on the Internet.

The GPE to the extent permitted by applicable law retains all rights to this document and Information contained therein. Any reproduction, use, exposure, or other publication, or dissemination of Information or its part by methods known and as yet undiscovered without the prior written consent of the GPE is strictly prohibited. The GPE is not in any way responsible for any errors or omissions in Information. GPE reserves the right, without giving any reason, to amend or repeal any Information.

2. Introduction

This document describes principle of creating payments in the GP webpay payment gateway environment and authorisation of subsequent operations with payments.

2.1 General GP webpay security principle

In order to secure itself, the GP webpay system uses the so-called PKI (Public Key Infrastructure) model. This model uses asymmetric cryptography, using two different keys.

1. Private key – this part is secret and is owned only by the authorised person (i.e. key owner)
2. Public key – the public part that can be distributed any channel (even the unsecured) – e-mail, public repository of keys ...

A main characteristic of the private key is that no two keys in the world are identical – i.e. each and every key is original.

2.1.1 How to obtain the private key

- Public certification authority – a trusted commercial authority providing management of keys (i.e. issuance, revocation, renewal...). Its public key is located directly in web browsers, or in various run-times (run-time environment for other software – e.g. Java, .NET...). Keys issued by this authority are widely accepted as credible and are used for communication with banks and public institutions – e.g. Thawte (<https://www.thawte.com/>), První certifikační autorita a.s. (<http://www.ica.cz/>).
- Various general solutions – private keys are not generally accepted, nevertheless they are built on trust between a client and specific key provider – e.g. Komerční banka has its own certification authority and provides its clients with keys to enable their communication with internet banking.
- GP webpay enables its clients to obtain a private key via the web portal. This key can be used only in the GP webpay environment.

2.1.2 PKI functions

- access authentication (user's identity verification)
- messages integrity verification (message has not been altered in any way)
- undeniableness – using electronic signature
- privacy – messages encryption, symmetric and asymmetric encryption

GP webpay uses only two of the above mentioned functions – integrity verification and undeniableness.

2.2 Using PKI in GP webpay

2.2.1 Ways of use

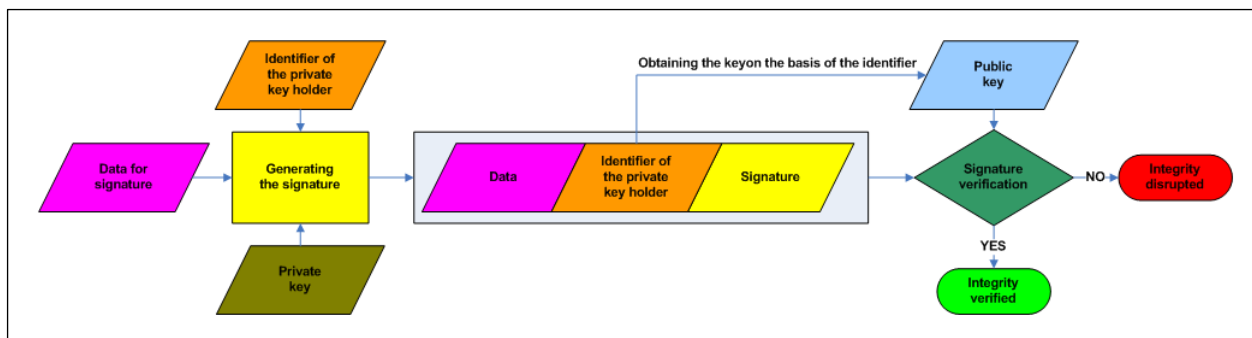
The private key is used for generating a signature of all the messages enabling manipulation with payments. A verified signature guarantees integrity of transmitted data and correct identity (undeniability of identity) of a message sender – there is no possibility to create a signature using the public part of key.

Types of messages:

- Creating new payments by means of standard HTTP interface
- Payments management in the Portal – money capture/refund of a card holder
- Payments management by means of web-services – used at direct connection of the GP webpay system with merchant's payment system

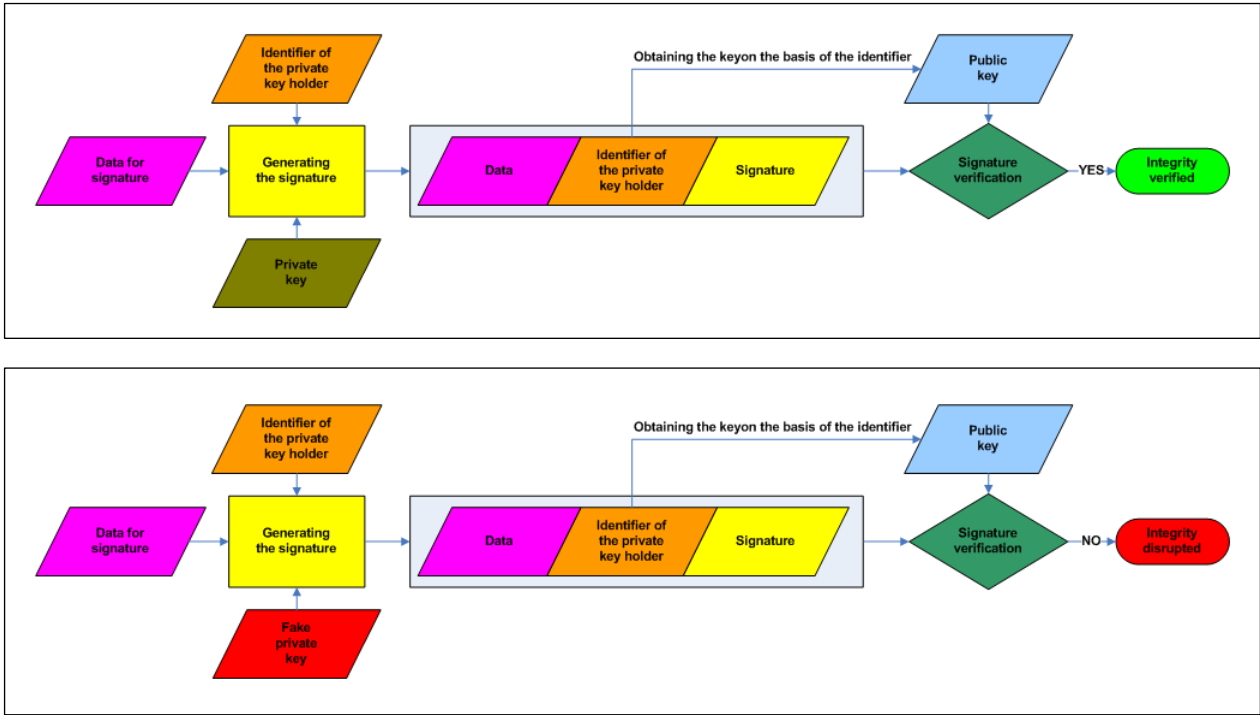
2.2.2 Message integrity verification

Every message modifying data (whether it is creating payments or operations with payments) contains not only data, but also a signature box. Signature is created on the side of the private key owner on the basis of input data and the private key with the use of a general algorithm for signature calculation. After the data are sent to the server, it carries out verification a similar way, but using relevant public key (public key is searched out on the basis of identifier of the message sender; the identifier is sent in a message). If the calculation differs, there must have occurred data disruption in the course of their transmission.



2.2.3 Message sender identity verification

A part of transmitted data is also an identifier of the message sender. On the basis of this identifier, the relevant public key is selected on the server side. If it was possible to verify the signature and provided that there are no two identical private keys, it can be stated that the data had really been sent by the private key holder.



3. Private key and its management

3.1 Private key in general

Private key is the basis of security of the GP webpay system. This key is solely owned by the key holder and it is necessary to observe maximally all the security requirements for confidentiality:

- Keep it in a secure place
- Always have it protected by password
- If the key is compromised, it is necessary to obtain a new key and to inform all the subjects using its public part for identity verification that the key has been compromised

Private key is stored in a data file. This file is called a repository, or keystore. Keystore can contain more private and public keys. To be able to differentiate among the keys in the keystore, there are names assigned to them – the so-called aliases. The keystore is protected by the central password and besides that, every private key is protected by its own password.

There are several formats of keystores. For our purposes, the following ones are sufficient (the below described conversion application supports precisely these formats):

JKS – keystore in the format supported by JAVA programming language

PFX – keystore in the format supported by Microsoft corporation (PKCS12)

PEM – keystore in the format supported by PHP programming language

The formats for distribution of the public key relate to these types as well:

PEM – keystore in the text format

DER – keystore in the binary format

3.2 How to obtain the private key

As mentioned above, private key can be obtained in a few different ways. For commercial purposes, or for communication with public administration, it is necessary to obtain a key from a trusted certification authority.

For the purposes of operating the GP webpay system, it is sufficient to obtain it by means available in the GP webpay.

If you have already bought any private key (there are several commercial certification authorities issuing/selling private keys), it can be used as well.

3.2.1 History

From the very beginning of functioning of the GP webpay, there has been a possibility to get the private key by means of individually delivered application “Key and certificate generation”. This application has been downloadable from the user environment GP webpay GUI and also as a part of distribution package of the documentation.

The following files are the result of generation:

<name>.ks – keystore file in the Java format – contains both the private and the public key

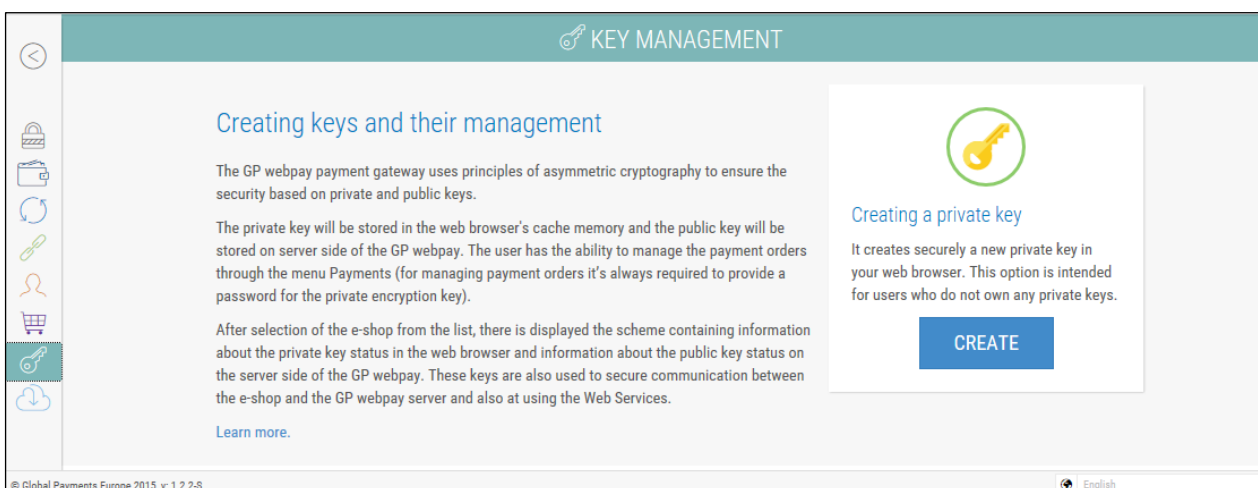
<name>.pfx – keystore file in the PKCS#12 format – contains both the private and the public key

<name>.pem – keystore file in the PEM format – contains both the private and the public key – e.g. for PHP apps

<name>.cer – file containing the public key

3.2.2 The present

The GP webpay Portal, the new graphic interface for management of orders, has incorporated management of both private and public keys of individual e-shops. Its part is also the possibility to generate the private key by means of the web browser.



The result of generation is the file "gpwebpay-pvk.key" in text format PEM.

This key can be inserted into the web browser (by import in the Portal).

At the same time it has to be preserved for future use – e.g. in another web browser.

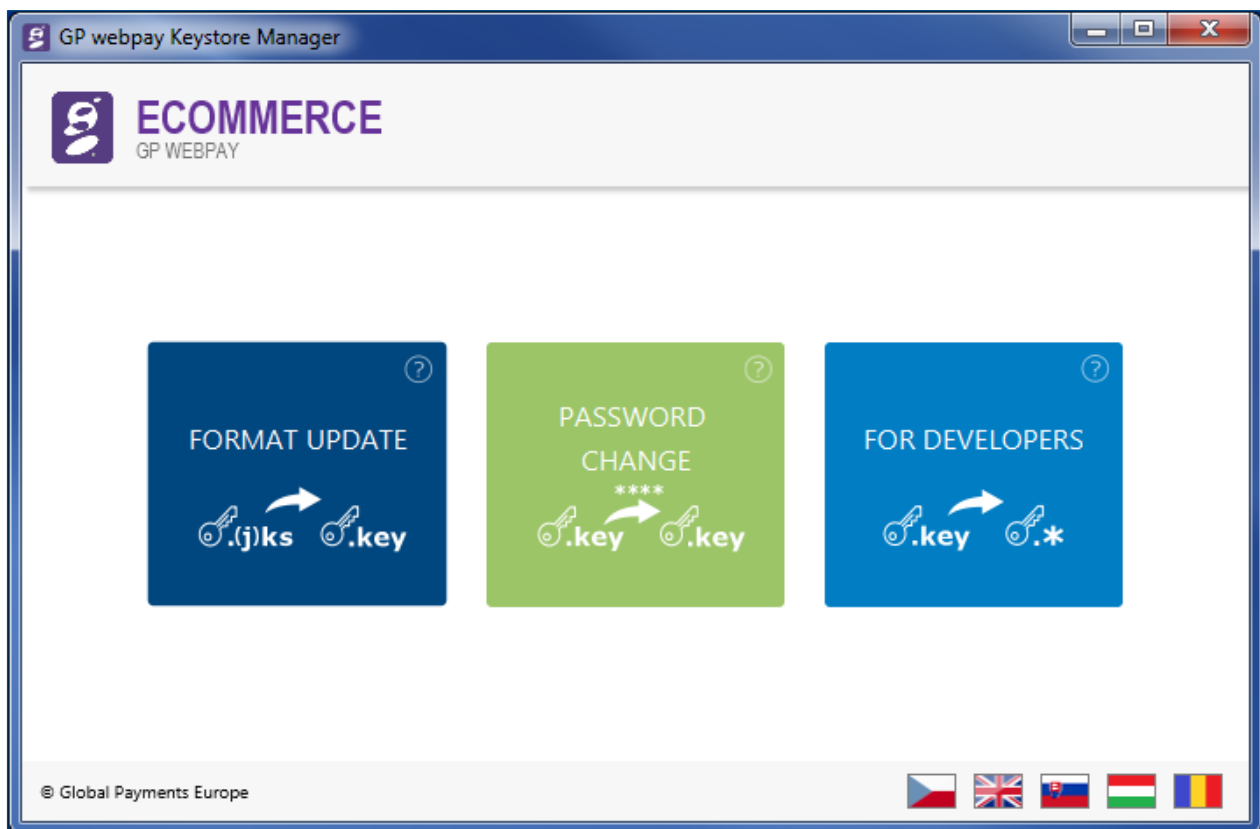
3.3 The private key management

To be able to operate with payments in the web application GP webpay Portal (hereinafter referred as the Portal), it is necessary to upload the private key to the web browser. This upload can be carried out after a successful login, directly in the environment of the Portal. The private key has to be stored in the text format PEM; this format is created also during key generation in the Portal (file "gpwebpay-pvk.key").

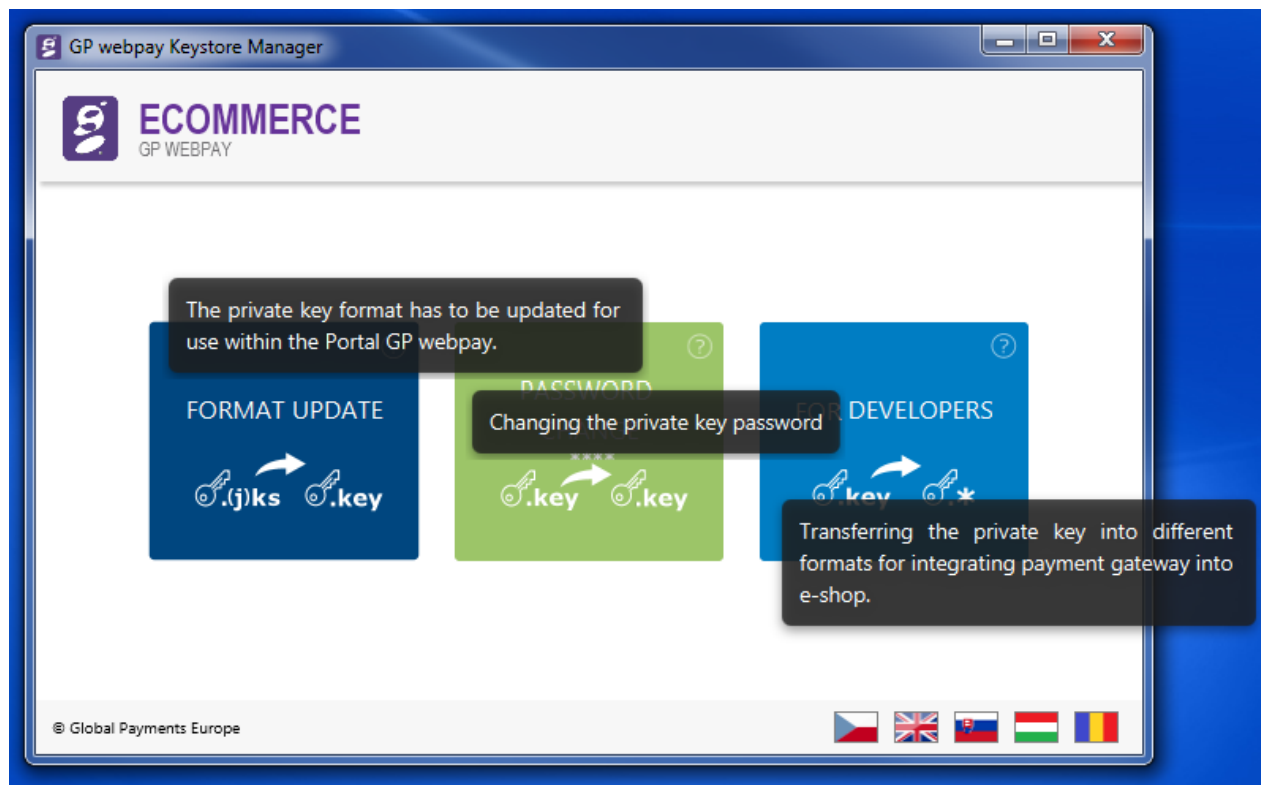
In case you have the private key from earlier, it is necessary to update the original format to the new one. The GP webpay Keystore Manager application can be used for this purpose. Application is available in the "Downloads" menu of the Portal and for its operation it requires to have the installed Java (downloadable from Oracle website <http://www.java.com>).

GP webpay Keystore Manager application has these functionalities:

- Format update – format conversion of the initial file containing the private key
- Password change – changing the private key password in the new format
- For developers – automatic conversion of the private key in the new format into formats supported by various developer tools



Hover your mouse over a "tile" to display a brief description of functionality:

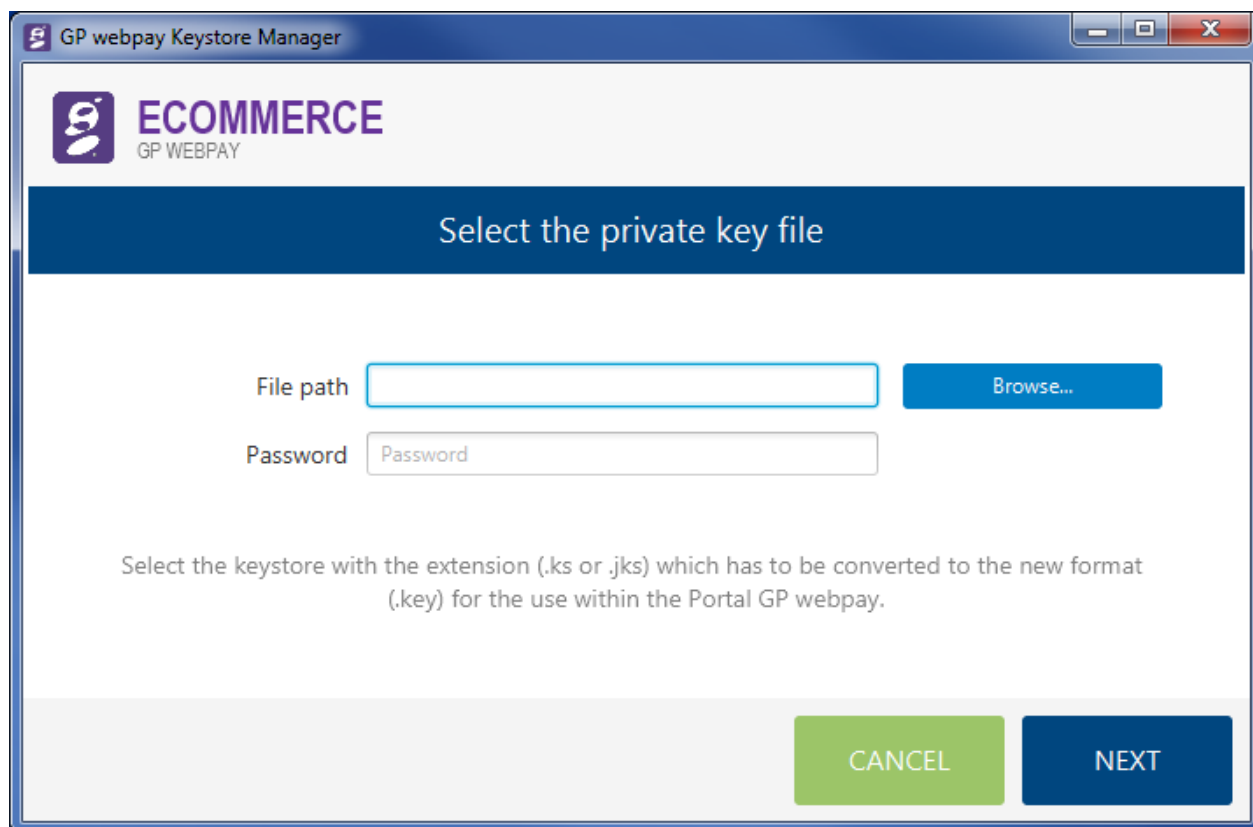


The application supports a few language versions. To switch among them, use the flag icons in the bottom part of the screen.

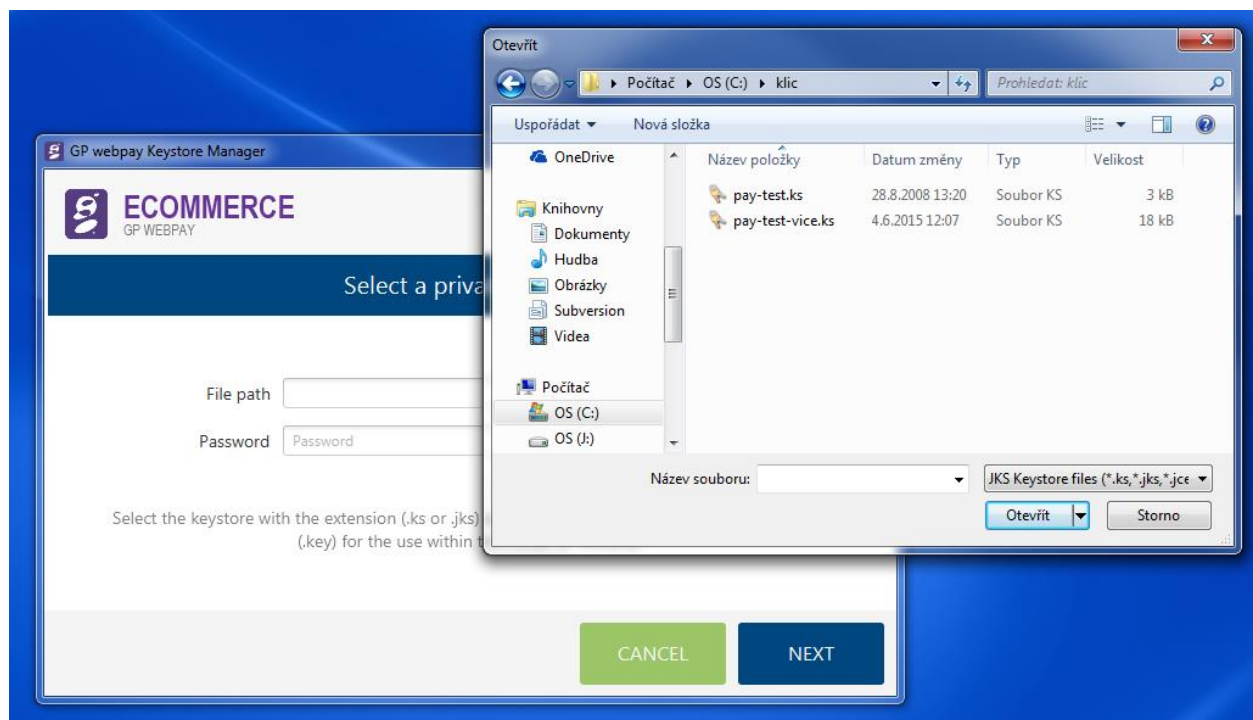
3.3.1 Format update

This “tile” serves for the format update of the initial private key, which was used in the old GUI for merchants. The original format is in the JAVA structure and has – in most cases – file name extension “.ks”, or “.jks”. The new format is in the PEM structure and the private key is stored in the file “gpwebpay-pvk.key”.

By clicking the “FORMAT UPDATE” tile, there is displayed a window to select the file containing the private key in the old format:



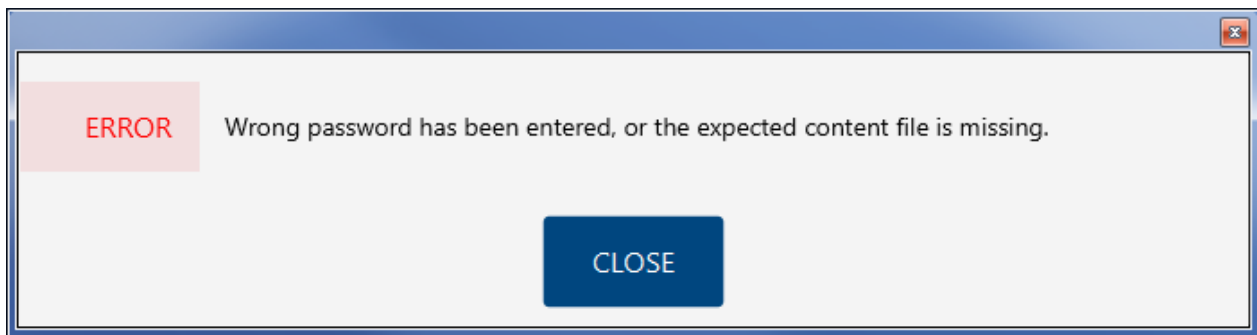
In the input box “File path”, it is necessary to find the file containing the original key by scrolling through the directory structure.



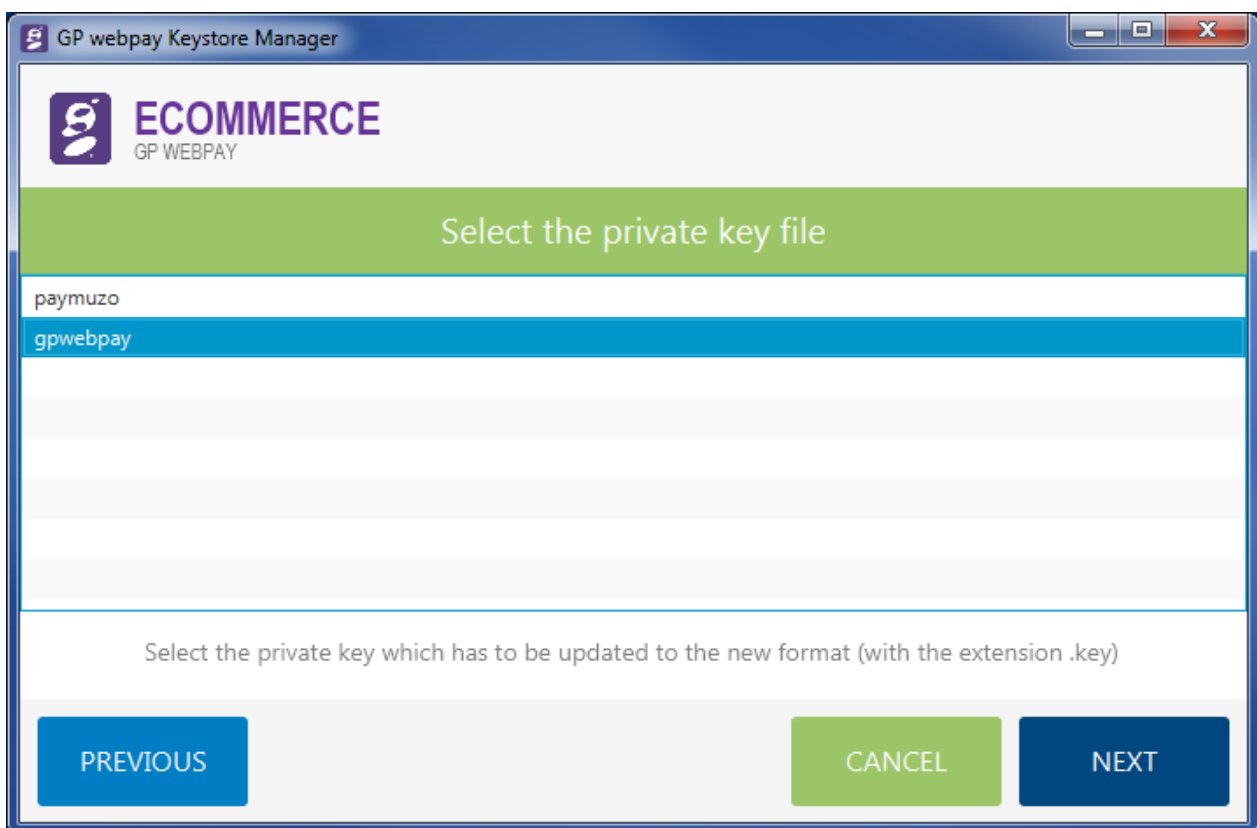
Confirm your selection of the private key file by clicking the “Open” button.

The selection window closes and the application waits for the password to the original keystore and for pressing the “Next” button. There follows an attempt to retrieve the file content.

If the wrong password is entered, or if the file does not contain the private key, the following message is displayed:



In case that the keystore file contains more private keys, the list of keys is displayed and it is necessary to select the right private key:



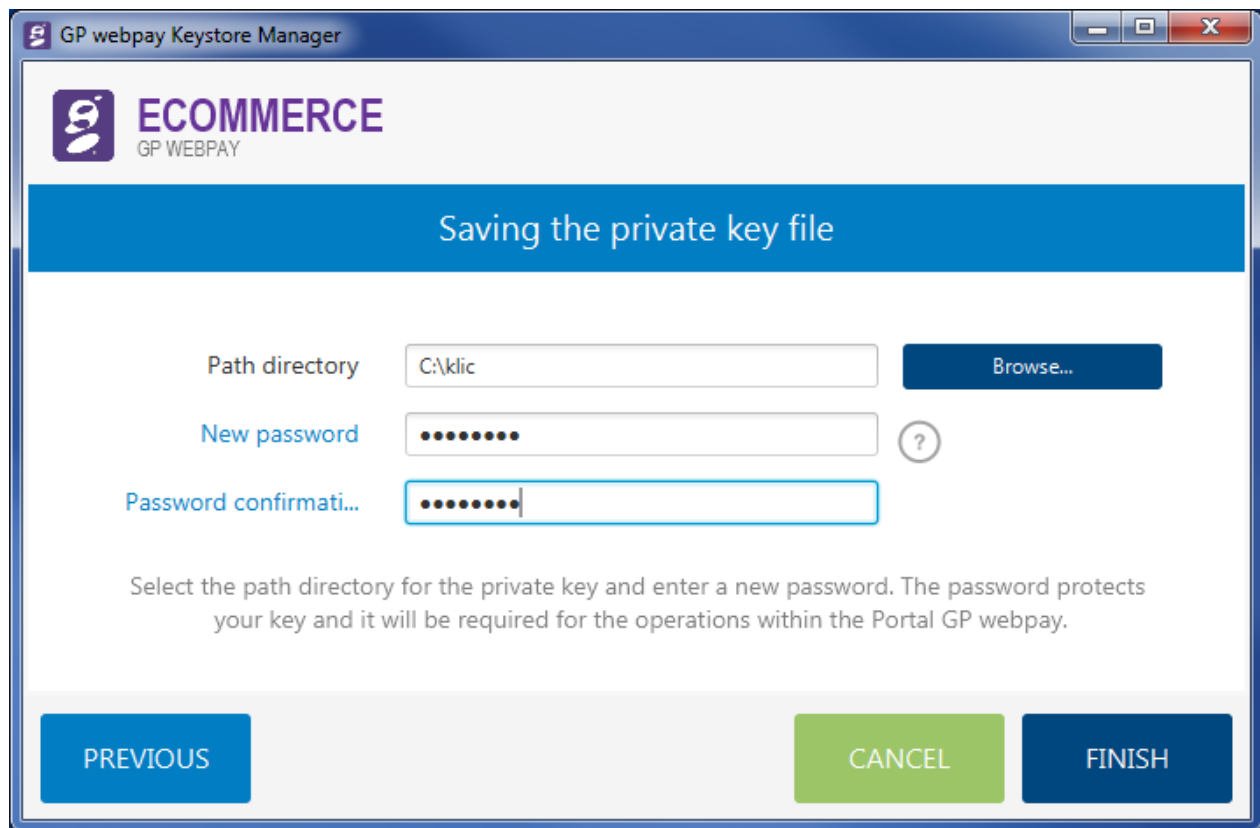
and continue by clicking the “Next” button“. If there is only one private key, this screen is skipped.

After the correctness of the input file is verified, or key selection is confirmed, you are prompted for selection of the destination directory to save the converted file and a request to enter a new password for the private key. The password has to be entered twice to avoid typing errors.

The password must be min. 8 characters and contain at least 3 types of the following requested types of characters:

- upper case letter
- lower case letter
- figure

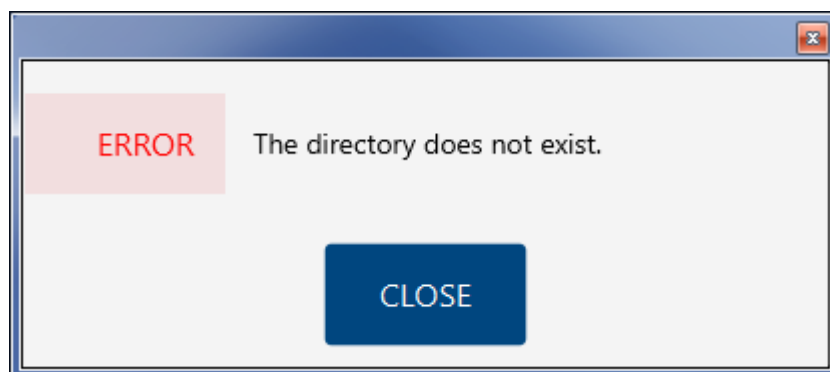
- special character



The screenshot shows a window titled "GP webpay Keystore Manager". Inside, there is a header with the "ECOMMERCE GP WEBPAY" logo. Below this is a blue banner that reads "Saving the private key file". The main area contains three input fields: "Path directory" with the text "C:\klic" and a "Browse..." button; "New password" with a masked password "....." and a help icon (?); and "Password confirmati..." with a masked password ".....". Below these fields is a text instruction: "Select the path directory for the private key and enter a new password. The password protects your key and it will be required for the operations within the Portal GP webpay." At the bottom, there are three buttons: "PREVIOUS" (blue), "CANCEL" (green), and "FINISH" (blue).

As all necessary information is entered, it is possible to finish the action by pressing the “Finish” button. It is also possible to return to the previous step by pressing the “Previous” button, or to jump back to the start screen by pressing the “Cancel” button.

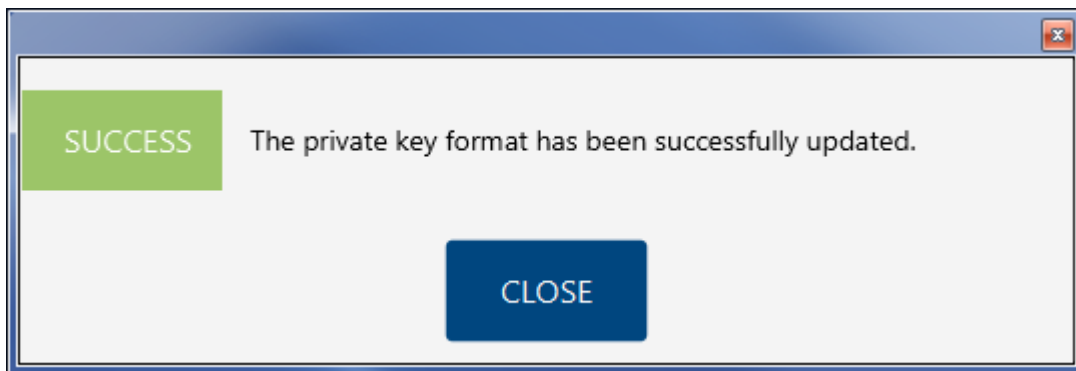
If a non-existing directory is entered, the following message is displayed, when you try to continue:



In case of inequality of passwords, the following message is displayed:



If everything has been entered correctly, the key is converted and the following message is displayed:



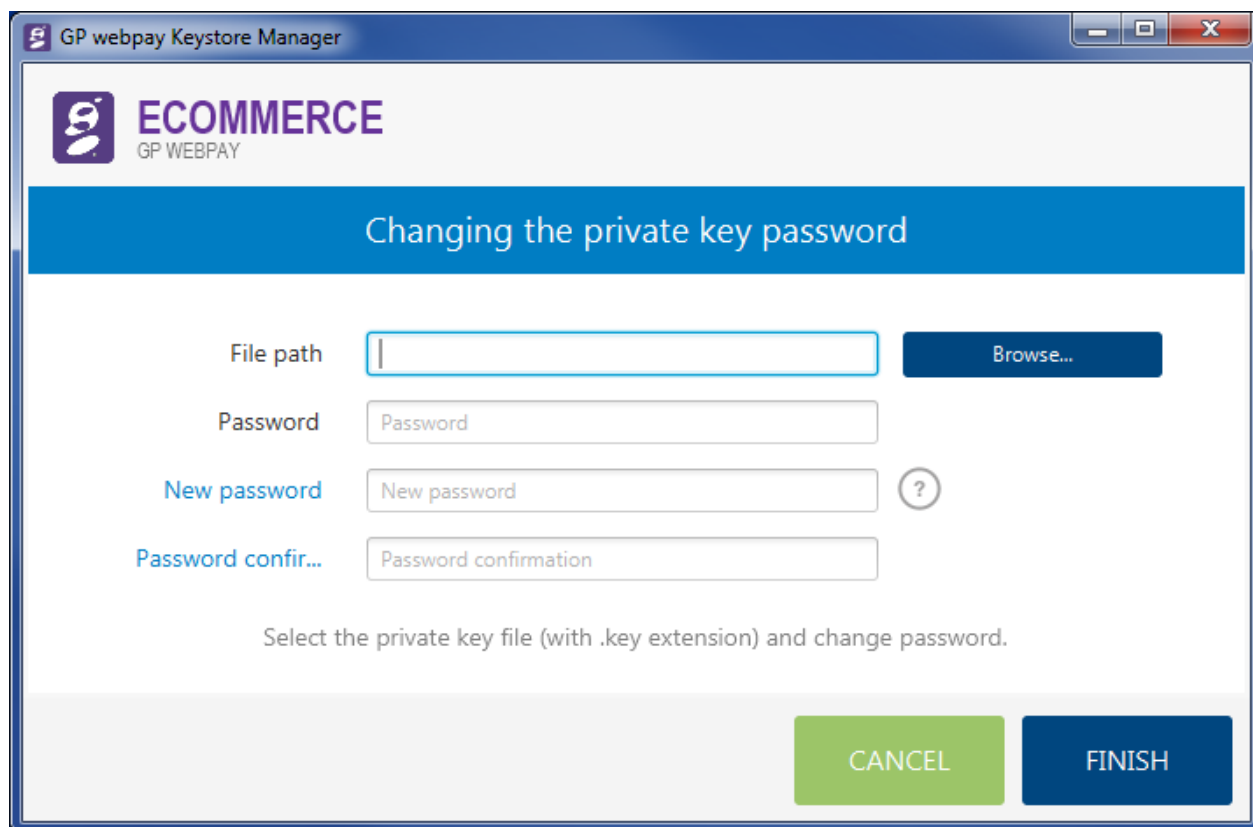
In the selected destination directory is created a file named "gpwebpay-pvk.key". The file contains the private key in the text format PEM.

By pressing the "Close" button, the application returns to the initial screen.

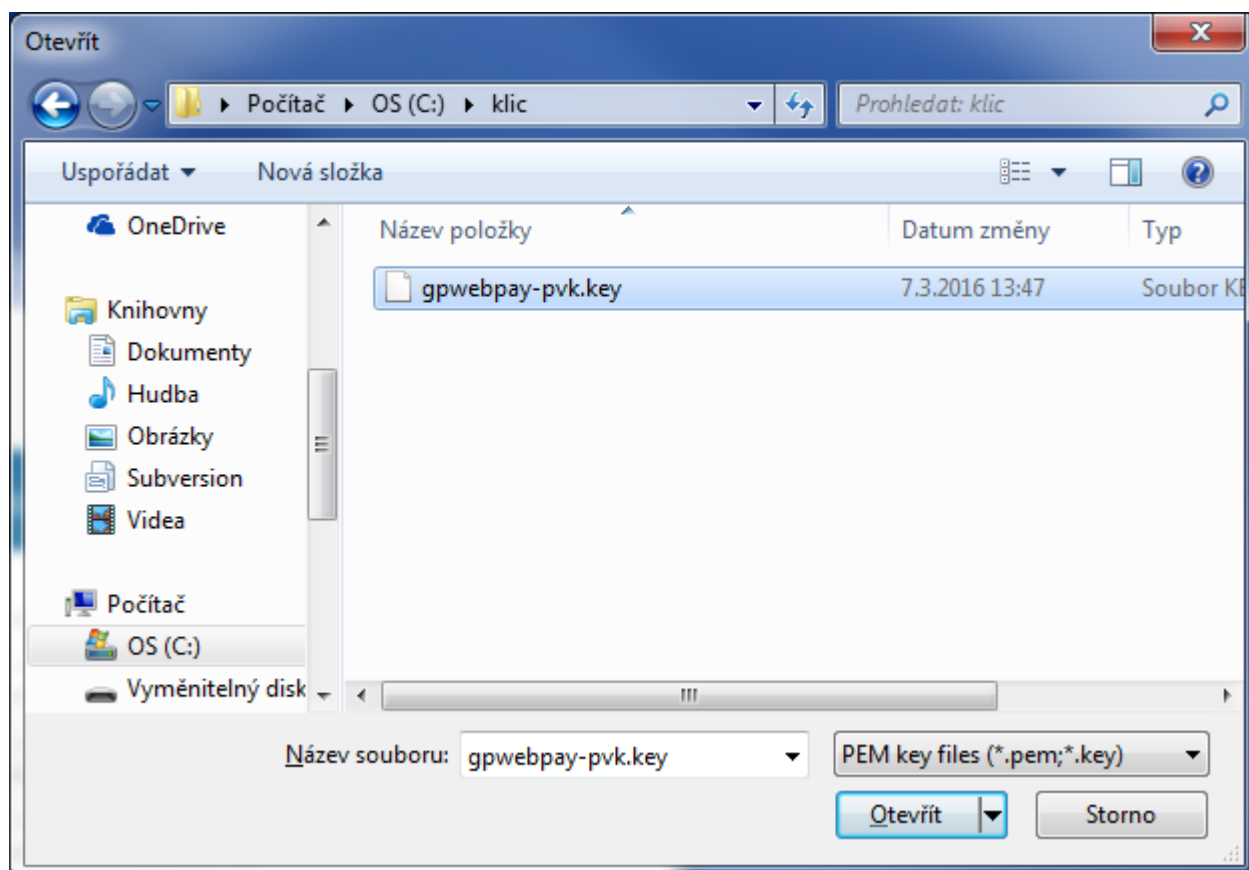
3.3.2 Password change

This option works with the new format of keystore and it is necessary to update the keystore file first – see the previous chapter – or to use the file in the new format obtained from the GP webpay Portal.

By pressing the "file", a new window is opened to enter the necessary data:



First, it is necessary to find the directory containing the private key file by means of the “Browse” button:

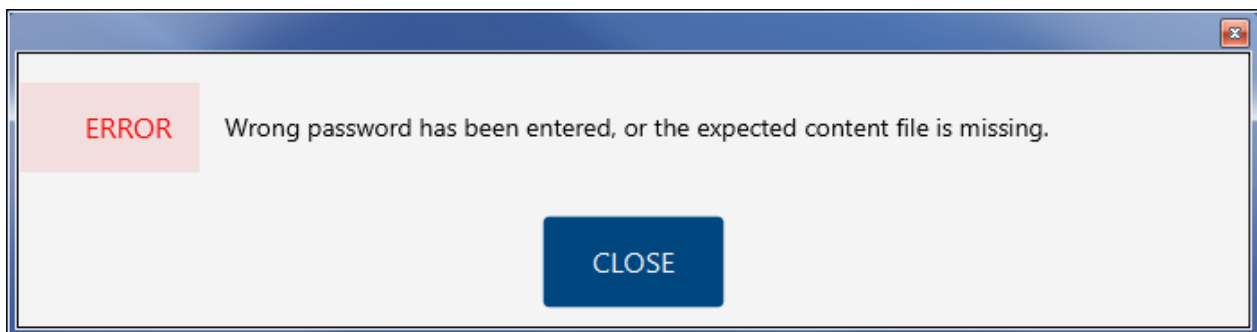


and to “Open” the relevant file. It is also necessary to enter the password to the original key and the new password as well (and of course to verify the new password by entering it twice).

The password must be min. 8 characters and contain at least 3 types of the following requested types of characters:

- upper case letter
- lower case letter
- figure
- special character

If the incorrect old password is entered or if the file format is incorrect, the following message is displayed:



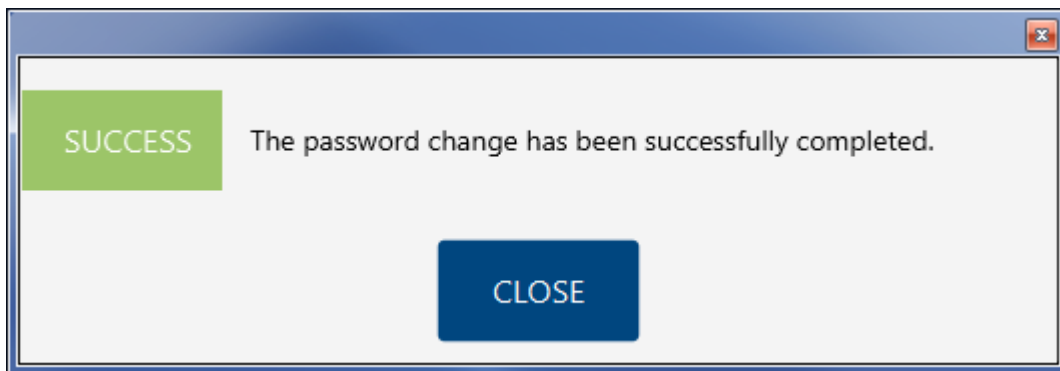
If the new password is not entered or it does not meet the necessary security requirements, the following message is displayed:



If the new password does not match the confirmation password, this situation is indicated by the following message:



If the values are entered correctly, there is displayed the following confirmation of a successful password change:



And there follows a return to the start screen.

3.3.3 For developers

The section “FOR DEVELOPERS” is primarily devoted for programmers implementing the payment gateway into a merchant’s e-shop.

Selection starts the process of converting the keystore format to the next most common keystore formats and simultaneously saves the public part of the key into the generally used formats.

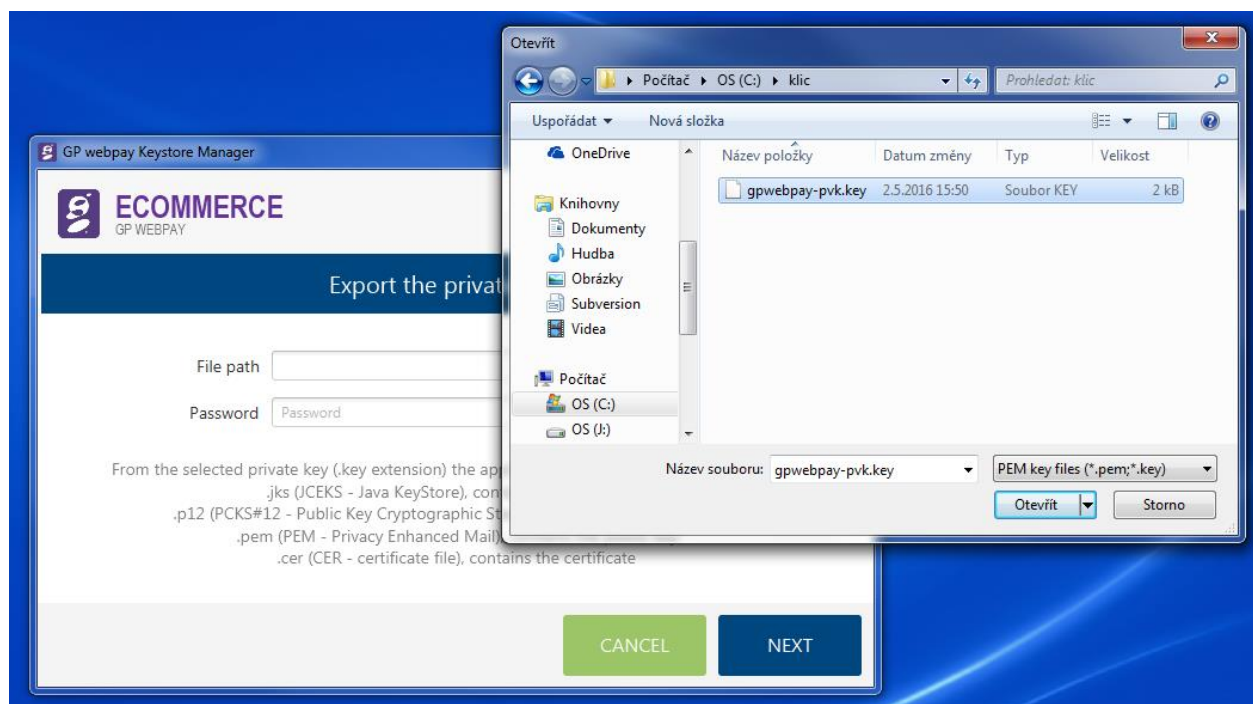
Input format of the keystore:

- text format PEM (PVK) – `gpwebpay-pvk.key`

Output formats of keystores and files:

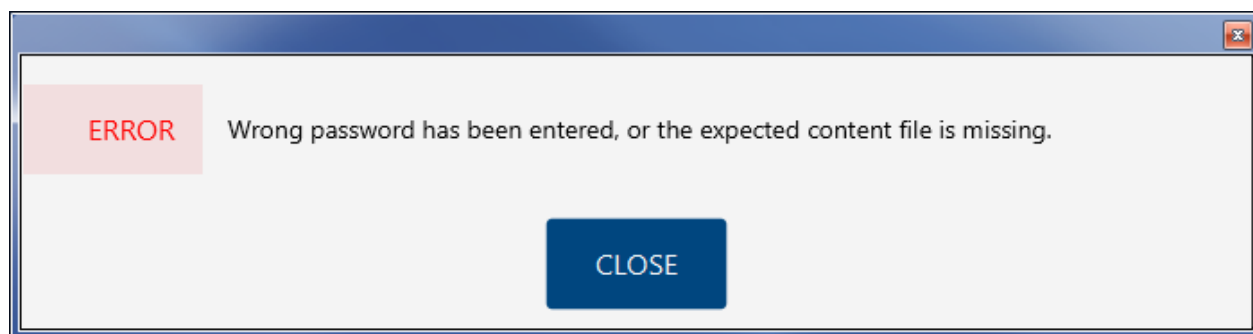
- keystore:
 - JAVA format JKS – `gpwebpay-pvk.jks`
 - Microsoft PKCS12 – `gpwebpay-pvk.p12`
- public key file:
 - text format PEM – `gpwebpay-pub.pem`
 - binary format DER – `gpwebpay-pub.cer`

The first step of conversion is selection of the keystore file. Use the “Browse” button to select the keystore file:



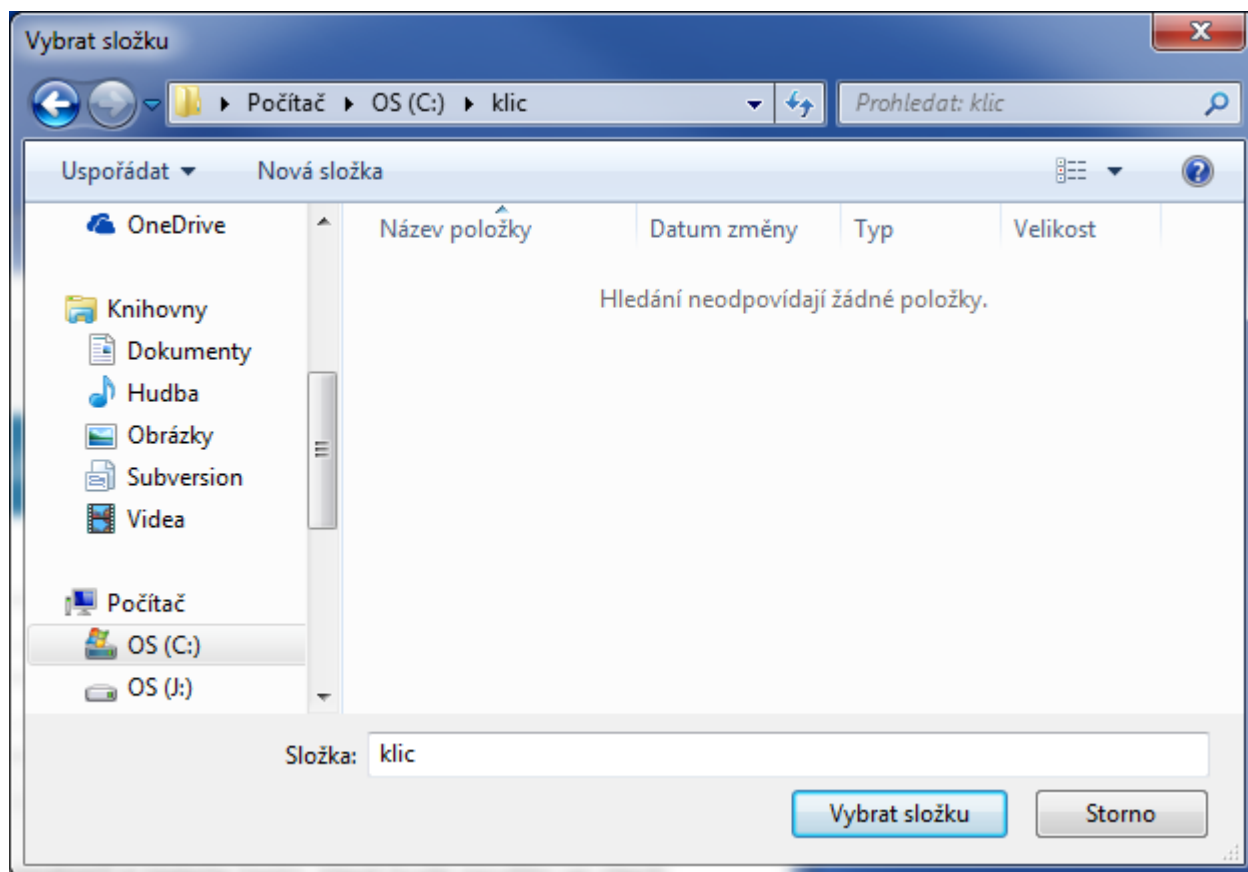
“Open” the file, enter password and press the “Next” button.

If the password or the inner keystore format is incorrect, the following message is displayed:



Otherwise, you are prompted for selection of output directory to save the new created files and to enter the new keystore password (the same password is used also to protect the private key in the keystore; the original password can be used as well).

The “Browse” button opens the window for selection of the output directory; after the necessary space in the file system is found, it is necessary to confirm the selection by the “Select folder” button:



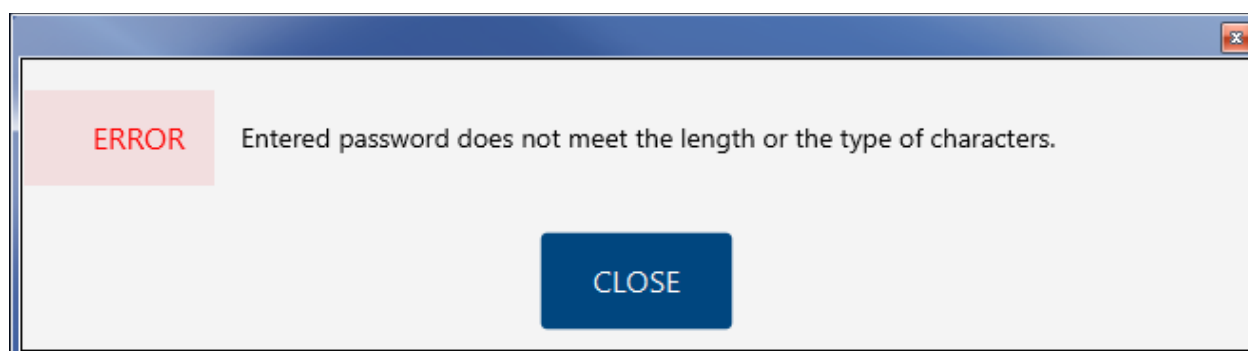
then it is necessary to enter the password and confirm it.

The password must be min. 8 characters and contain at least 3 types of the following requested types of characters:

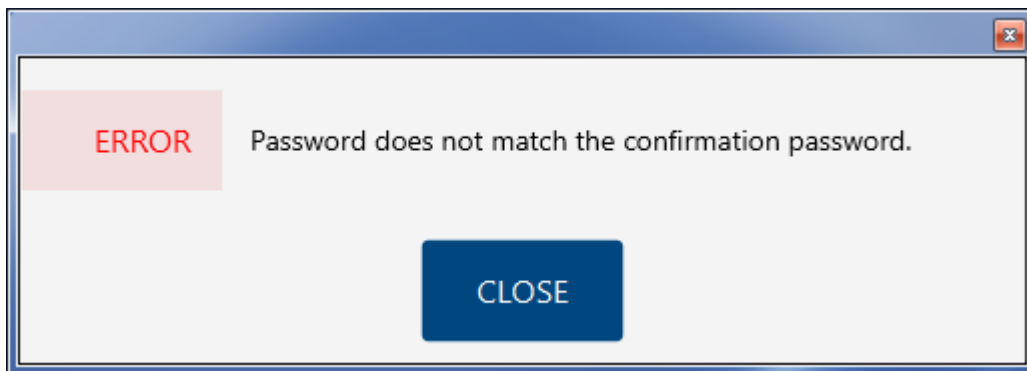
- upper case letter
- lower case letter
- figure
- special character

Then the “Finish” button is to be pressed.

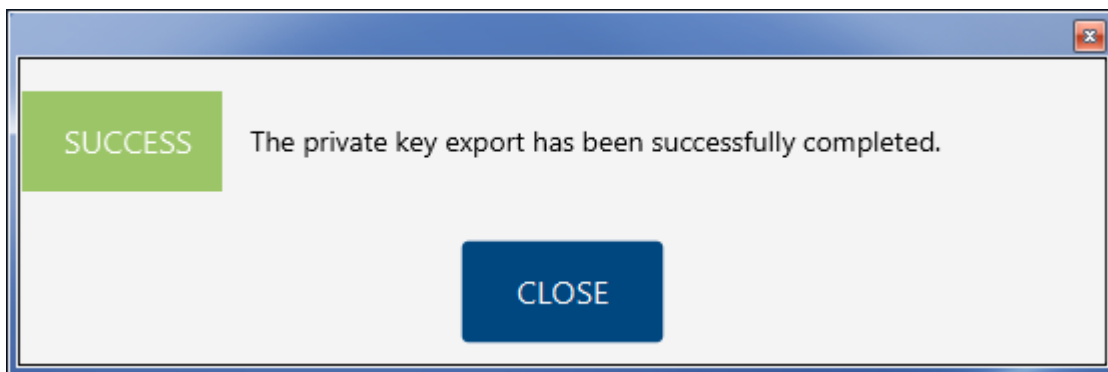
If a new password is not entered, or if it does not meet the necessary security requirements, the following message is displayed:



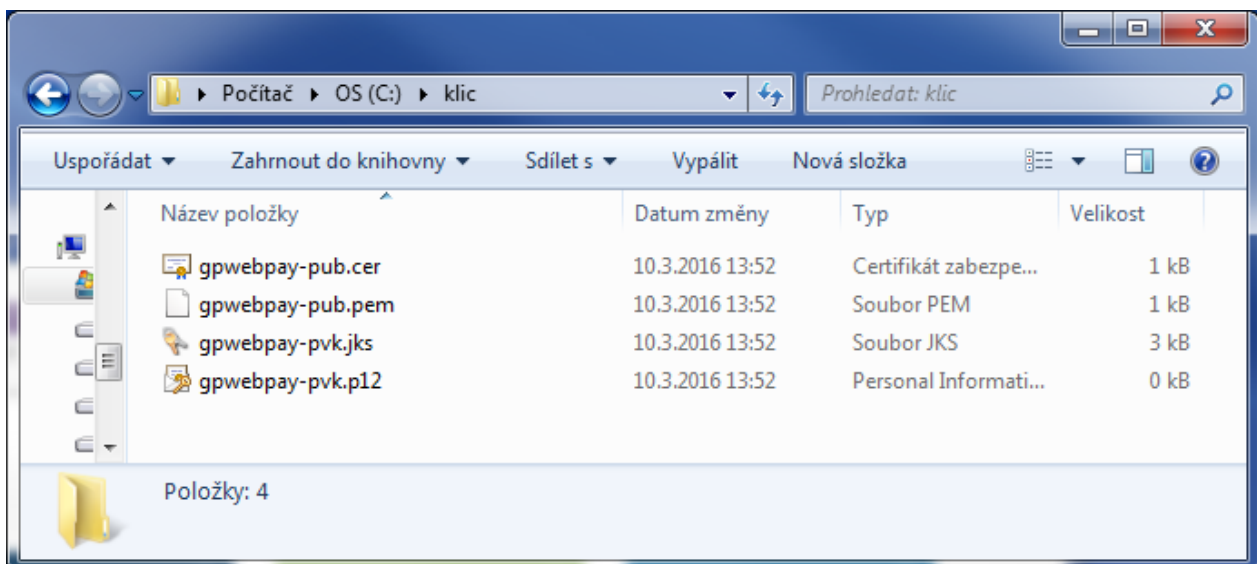
If the new password is not identical to the password confirmation, the situation is indicated by the following message:



If all the values are entered correctly, the successful export of the private key is confirmed by the following message:



This concludes the process of export of the private key, and in the selected output directory are created the following files:



- `gpwebpay-pvk.jks` – private key in the keystore in JAVA language (JKS)
 - applicable for JSP/JAVA applications
- `gpwebpay-pvk.p12` – private key in the keystore in Microsoft structure (PKCS12 – P12)

- applicable for .NET applications
- `gpwebpay-pub.pem` – text PEM (PVK) format of the public key
 - applicable for PHP applications for verification of the accuracy of the signature value created by the private key
- `gpwebpay-pub.cer` – binary DER format of the public key
 - applicable for .NET applications for verification of the accuracy of the signature value created by the private key
 - format for sending the public key to the GP webpay application support, if recording of the public key by means of the GP webpay Portal fails

After pressing the “Close” button the application returns to the start screen.