

Správa soukromého klíče

Verze: 1.1

Global Payments Europe, s.r.o.

Vytvořeno **19.2.2016**

Poslední změna **15.4.2016**



SERVICE. DRIVEN. COMMERCE

globalpaymentsinc.com

Autor dokumentu	Dimitrij Holovka
Správce dokumentu	
Schválil	
Verze	1.1
Stupeň utajení	Důvěrné

Historie dokumentu:

Verze	Datum	Provedl	Komentář
1.0	19.2.2016	D. Holovka	První verze dokumentu
1.1	29.3.2016	D. Holovka	Drobné opravy

Obsah

1.	Právní doložka	3
2.	Úvod	4
2.1	Obecný princip zabezpečení GP webpay	4
2.1.1	Získání soukromého klíče	4
2.1.2	Účely využití PKI	4
2.2	Využití PKI v GP webpay	5
2.2.1	Způsoby použití	5
2.2.2	Ověření integrity zprávy	5
2.2.3	Ověření identity zaslatele zprávy	5
3.	Soukromý klíč a jeho správa	7
3.1	Soukromý klíč obecně	7
3.2	Získání soukromého klíče	7
3.2.1	Historie	7
3.2.2	Současnost	8
3.3	Správa soukromého klíče	9
3.3.1	Aktualizace formátu	10
3.3.2	Změna hesla	14
3.3.3	Pro vývojáře	17



1. Právní doložka

Tento dokument včetně všech případných příloh a odkazů je určen výhradně pro potřeby poskytovatele služeb e-shopu (dále jen „Zákazník“).

Informace v tomto dokumentu obsažené (dále jen „Informace“) jsou předmětem duševního vlastnictví a ochrany autorských práv společnosti Global Payments Europe, s.r.o. (dále jen „GPE“) a mají povahu obchodního tajemství v souladu s ust. § 504 zák. č. 89/2012 Sb., Občanský zákoník. Zákazník si je vědom právních povinností ve vztahu k nakládání s Informacemi.

Informace nebo kterákoliv její část nesmí být bez předchozího výslovného písemného souhlasu GPE poskytnuty nebo jakýmkoliv způsobem zpřístupněny třetí straně. Informace nesmí být zároveň využity Zákazníkem pro jiné účely, než pro účely ke kterému slouží. Pro vyloučení všech pochybností nesmí být Informace nebo kterákoliv část bez předchozího výslovného písemného souhlasu GPE poskytnuty nebo jakýmkoliv způsobem zpřístupněny ani společností poskytujícím služby zpracování plateb v prostředí internetu.

GPE si v rozsahu dovoleném platným právem, vyhrazuje veškerá práva k této dokumentaci a k Informacím v ní obsažených. Jakékoliv rozmnožování, použití, vystavení či jiné zveřejnění nebo šíření Informací nebo její části metodami známými i dosud neobjevenými je bez předchozího písemného souhlasu společnosti GPE přísně zakázáno. GPE není jakkoliv odpovědná za jakékoliv chyby nebo opomenutí v Informacích. GPE si vyhrazuje právo, a to i bez uvedení důvodu, jakoukoliv Informaci změnit nebo zrušit.

2. Úvod

Dokument popisuje princip zabezpečení zakládání plateb v prostředí platební brány GP webpay a autorizace následných operací s platbami.

2.1 Obecný princip zabezpečení GP webpay

Systém GP webpay pro své zabezpečení používá tzv. PKI (Public Key Infrastructure) model. Tento model využívá asymetrickou kryptografii, při které se používají dva rozdílné klíče.

1. Soukromý klíč – tato část je tajná a vlastní ji pouze oprávněná osoba
2. Veřejný klíč – veřejná část, kterou lze volně distribuovat jakýmkoli (i nezabezpečeným) kanálem – e-mail, veřejné úložiště klíčů ...

Hlavní vlastností soukromého klíče je to, že žádné dva klíče na světě se neshodují – tj. každý klíč je originál.

2.1.1 Získání soukromého klíče

- Veřejná certifikační autorita – obecně přijímaná důvěryhodná komerční instituce zajišťující správu klíčů (vydávání, zneplatnění, obnovování ...). Její veřejný klíč bývá umístěn přímo ve webových prohlížečích, popř. v různých run-timech (běhová prostředí pro ostatní software – např. Java, .NET ...). Klíče vydané takovouto institucí jsou obecně přijímány jako důvěryhodné a používají se pro komunikaci s bankami a veřejnými institucemi – např. Thawte (<https://www.thawte.com/>), První certifikační autorita a.s. (<http://www.ica.cz/>).
- Různá obecná řešení – soukromé klíče nejsou všeobecně akceptovány, ale jsou postaveny na důvěře mezi klientem a konkrétním poskytovatelem klíče – např. Komerční banka má svoji certifikační autoritu a poskytuje klíče svým klientům pro komunikaci s internetovým bankovníctvím.
- GP webpay umožňuje svým klientům získání soukromého klíče prostřednictvím webového portálu. Tento klíč je možné použít pouze v prostředí GP webpay.

2.1.2 Účely využití PKI

- autentizace přístupu (ověření totožnosti uživatele)
- prověřování integrity zpráv (zpráva nebyla žádným způsobem změněna)
- nepopiratelnost – využití elektronického podpisu
- privátnost – šifrování zpráv, symetrické a asymetrické šifry

GP webpay využívá z těchto účelů pouze dva – ověření integrity a nepopiratelnost.

2.2 Využití PKI v GP webpay

2.2.1 Způsoby použití

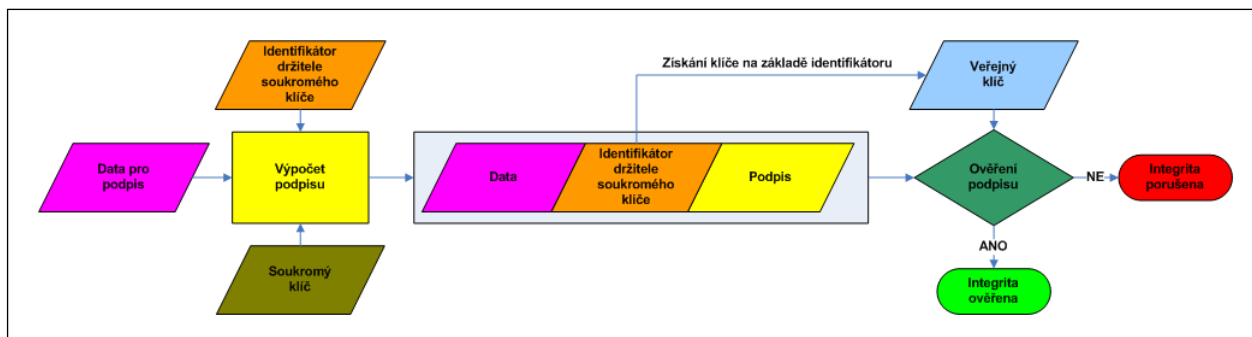
Soukromý klíč se používá pro výpočet podpisu veškerých zpráv umožňujících manipulaci s platbami. Ověřený podpis zaručuje integritu přenesených dat a správnou identitu (nepopíratelnost identity) zaslatele zprávy – neexistuje možnost vytvoření podpisu pomocí veřejné části klíče.

Typy zpráv:

- Zakládání nových plateb prostřednictvím standardního rozhraní HTTP
- Správa plateb v Portálu – stržení/vrácení peněžních prostředků držitele platební karty
- Správa plateb prostřednictvím služeb web-services – používá se při přímém propojení systému GP webpay s platebním systémem obchodníka

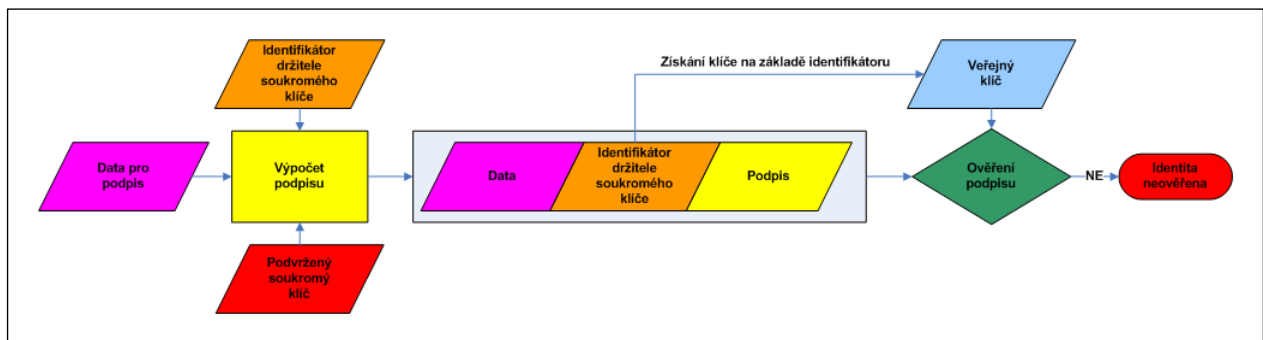
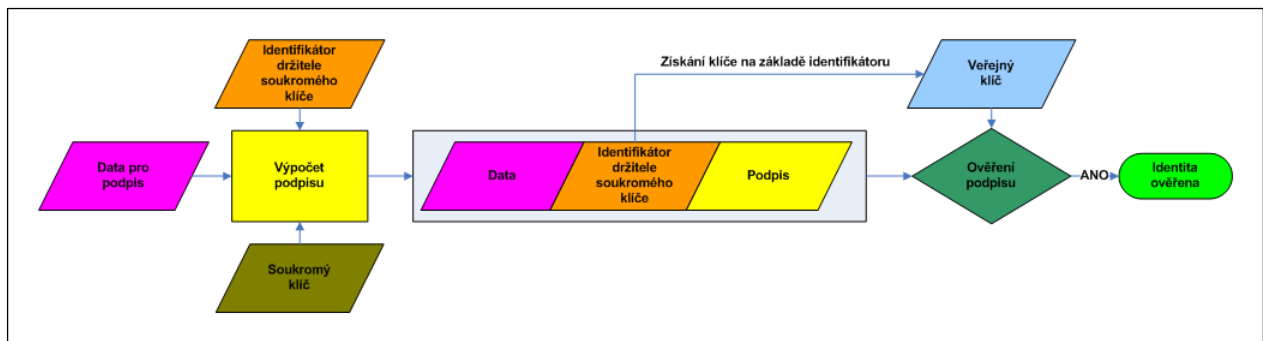
2.2.2 Ověření integrity zprávy

Každá zpráva modifikující data (ať jde o zakládání nebo operace s platbami) obsahuje kromě vlastních dat i pole pro podpis. Podpis vznikne na straně vlastníka soukromého klíče na základě vstupních dat a soukromého klíče s využitím obecného algoritmu pro výpočet podpisu. Po odeslání dat na server tento provede ověření obdobným způsobem, ale s využitím odpovídajícího veřejného klíče (veřejný klíč je vyhledán na základě identifikátoru původce zprávy zasláního ve zprávě). Pokud se výpočet liší, tak došlo během přenosu dat k jejich narušení.



2.2.3 Ověření identity zaslatele zprávy

Součástí přenášených dat je také identifikátor původce zprávy. Na základě tohoto identifikátoru je vybrán odpovídající veřejný klíč na serveru. Pokud bylo možné podpis ověřit a za předpokladu, že neexistují dva shodné soukromé klíče, lze konstatovat, že daná data opravdu zaslal držitel soukromého klíče.



3. Soukromý klíč a jeho správa

3.1 Soukromý klíč obecně

Soukromý klíč je základem bezpečnosti systému GP webpay. Tento klíč je ve výhradním vlastnictví držitele klíče a je nutné maximálně dodržovat bezpečnostní požadavky na jeho utajení:

- Uchovávat jej na bezpečném místě
- Vždy jej mít zabezpečen heslem
- Pokud dojde k jeho vyzrazení, je nutné získat klíč nový a o kompromitaci informovat všechny subjekty využívající ověřování identity pomocí jeho veřejné části

Soukromý klíč je uložen v datovém souboru. Tento soubor nazýváme úložiště, popř. keystore. Úložiště může obsahovat více soukromých i veřejných klíčů. Aby bylo možné jednotlivé klíče v úložišti odlišit, jsou k nim přiřazeny názvy – tzv. aliasy. Úložiště bývá chráněno centrálním heslem a každý soukromý klíč ještě svým vlastním heslem.

Existuje několik formátů úložišť. Pro naše účely budou postačovat tyto (dále popsaná konverzní aplikace podporuje právě tyto formáty):

JKS – úložiště ve formátu podporované programovacím jazykem JAVA

PFX – úložiště ve formátu podporované společností Microsoft (PKCS12)

PEM – úložiště ve formátu podporované programovacím jazykem PHP

K těmto typům se ještě váží formáty pro distribuci veřejného klíče:

PEM – úložiště v textovém formátu

DER – úložiště v binárním formátu

3.2 Získání soukromého klíče

Jak již bylo zmíněno, lze soukromý klíč získat několika způsoby. Pro komerční využití, popř. pro komunikaci s veřejnou správou, je nutné klíč získat od uznávané certifikační autority.

Pro účely provozu systému GP webpay je dostačující jeho získání prostředky dostupnými v GP webpay.

Pokud již máte nějaký soukromý klíč zakoupen (existuje několik komerčních certifikačních autorit, které vydávají/prodávají soukromé klíče), je možné použít ten.

3.2.1 Historie

Od samého počátku fungování GP webpay byla možnost získání soukromého klíče pomocí samostatně dodávané aplikace „Generování klíče a certifikátu“. Tato aplikace byla dostupná ke stažení z uživatelského prostředí GP webpay GUI a také jako součást distribučního balíčku dokumentace.

Výsledkem generování jsou následující soubory:

<jméno>.ks – soubor keystore v Java formátu – obsahuje soukromý i veřejný klíč

<jméno>.pfx – soubor keystore ve formátu PKCS#12 – obsahuje soukromý i veřejný klíč

<jméno>.pem – soubor keystore ve formátu PEM – obsahuje soukromý i veřejný klíč – např. pro PHP aplikace

<jméno>.cer – soubor s veřejným klíčem

3.2.2 Současnost

Nové grafické rozhraní pro správu objednávek Portál GP webpay má v sobě zakomponovanou správu soukromých a veřejných klíčů jednotlivých e-shopů. Jejich součástí je také možnost vygenerování soukromého klíče prostřednictvím webového prohlížeče.

Výsledkem generování je soubor „gpwebpay-pvk.key“ v textovém formátu PEM.

Tento klíč lze přímo vložit do používaného webového prohlížeče (prostřednictvím importu v Portálu).

Současně je nutné jej zachovat pro další použití – např. v jiném prohlížeči.

3.3 Správa soukromého klíče

Aby bylo možné pracovat s platbami ve webové aplikaci Portál GP webpay (dále pouze Portál), je nutné nahrát soukromý klíč do webového prohlížeče. Toto nahrání možné provést, po úspěšném přihlášení, přímo v prostředí Portálu. Soukromý klíč je nutné mít uložen v textovém formátu PEM, tento formát také vzniká při generování klíče v Portálu (soubor „gpwebpay-pvk.key“).

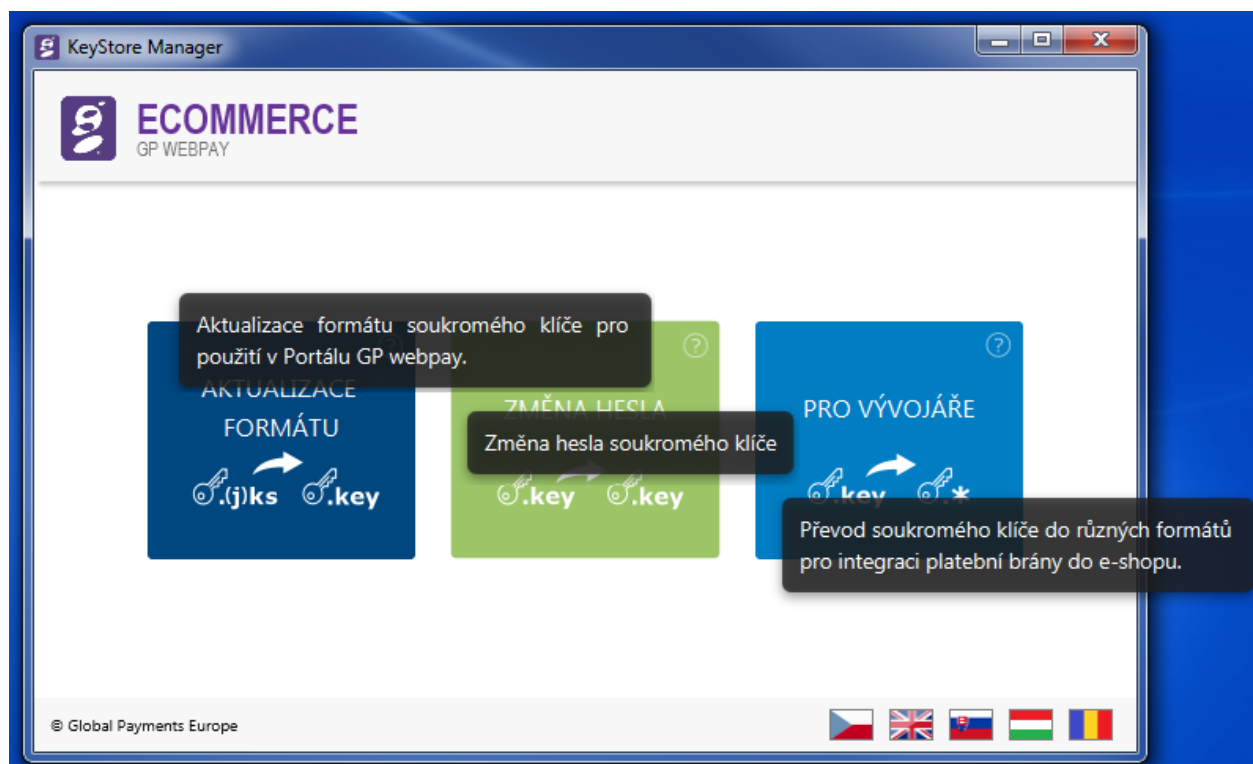
Pokud ovšem již máte soukromý klíč z dřívějška, je nutné původní formát aktualizovat do formátu nového. K této aktualizaci formátu slouží aplikace GP webpay Keystore Manager. Aplikace je dostupná v sekci „Ke stažení“ v Portálu a pro svůj běh vyžaduje nainstalované běhové prostředí jazyku Java (ke stažení z Oracle webu <http://www.java.com>).

Aplikace GP webpay Keystore Manager obsahuje tyto funkčnosti:

- Aktualizace formátu – konverze formátu původního souboru se soukromým klíčem
- Změna hesla – změna hesla soukromého klíče v novém formátu
- Pro vývojáře – automatická konverze soukromého klíče v novém formátu do formátů podporovaných různými vývojářskými nástroji



Po najetí myší na „dlaždici“ se zobrazí stručný popis funkcionality:



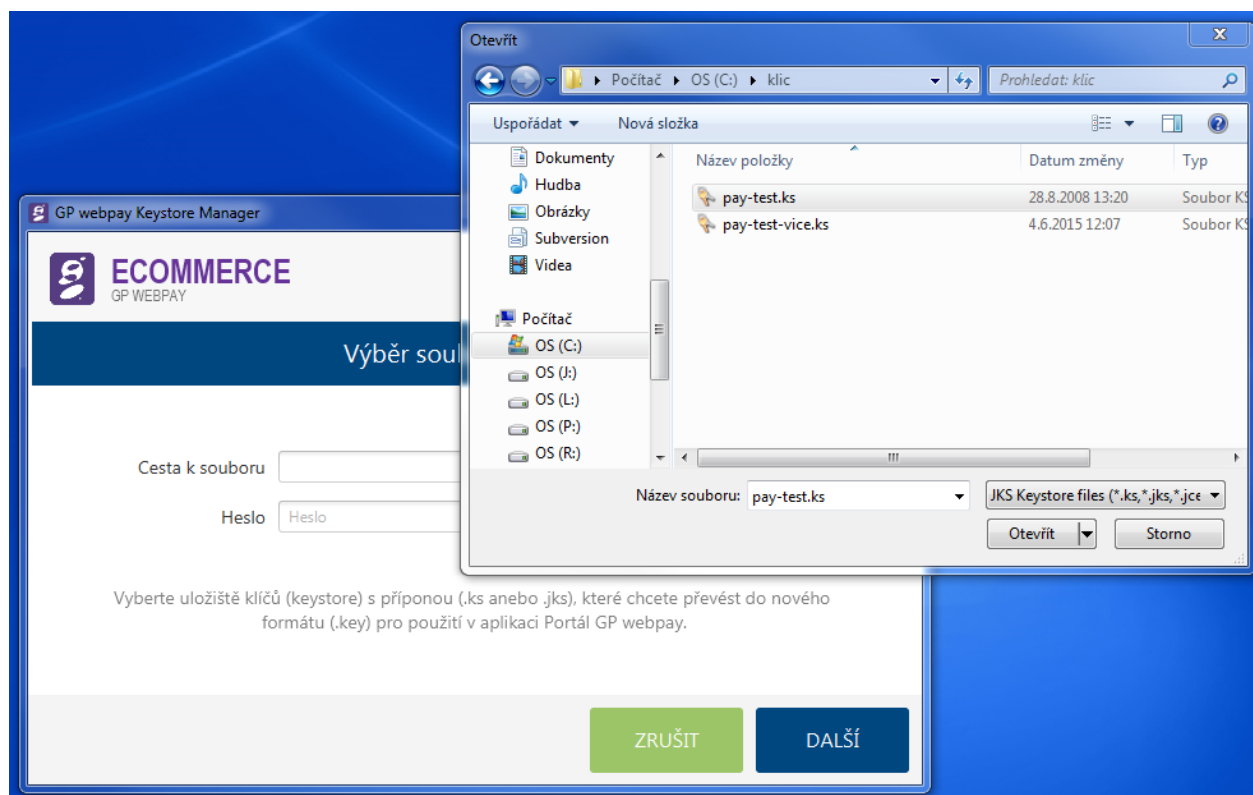
Aplikace podporuje několik jazykových variant. K jejich přepnutí slouží ikonky vlajek ve spodní části obrazovky.

3.3.1 Aktualizace formátu

Tato „dlaždice“ slouží k aktualizaci formátu původního soukromého klíče, který se používal ve starém GUI pro obchodníky. Původní formát je v JAVA struktuře a má, většinou, příponu souboru „.ks“ nebo „.jks“. Nový formát je v PEM struktuře a soukromý klíč je uložen v souboru s názvem „gpwebpay-pvk.key“.

Po kliknutí na dlaždici „AKTUALIZACE FORMÁTU“ je zobrazeno okno pro výběr souboru se starým formátem soukromého klíče:

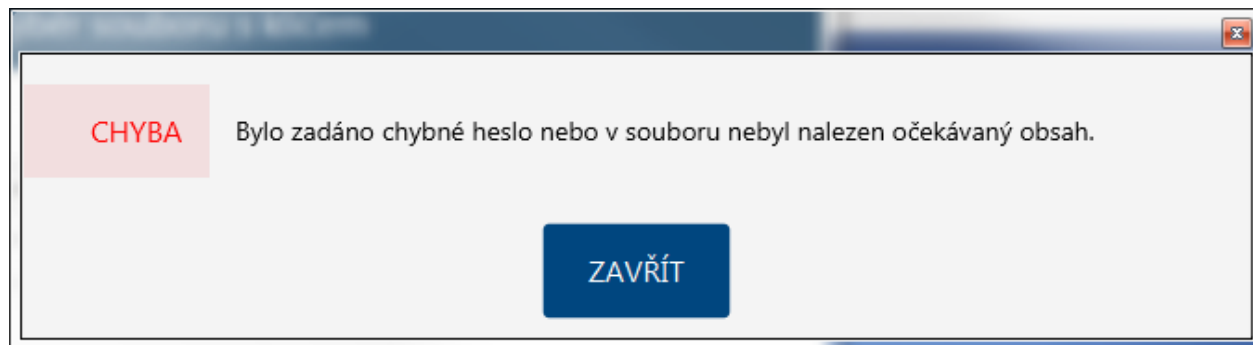
Ve vstupním poli „Cesta k souboru“ je potřeba, pomocí procházení adresářové struktury, najít soubor původního klíče.



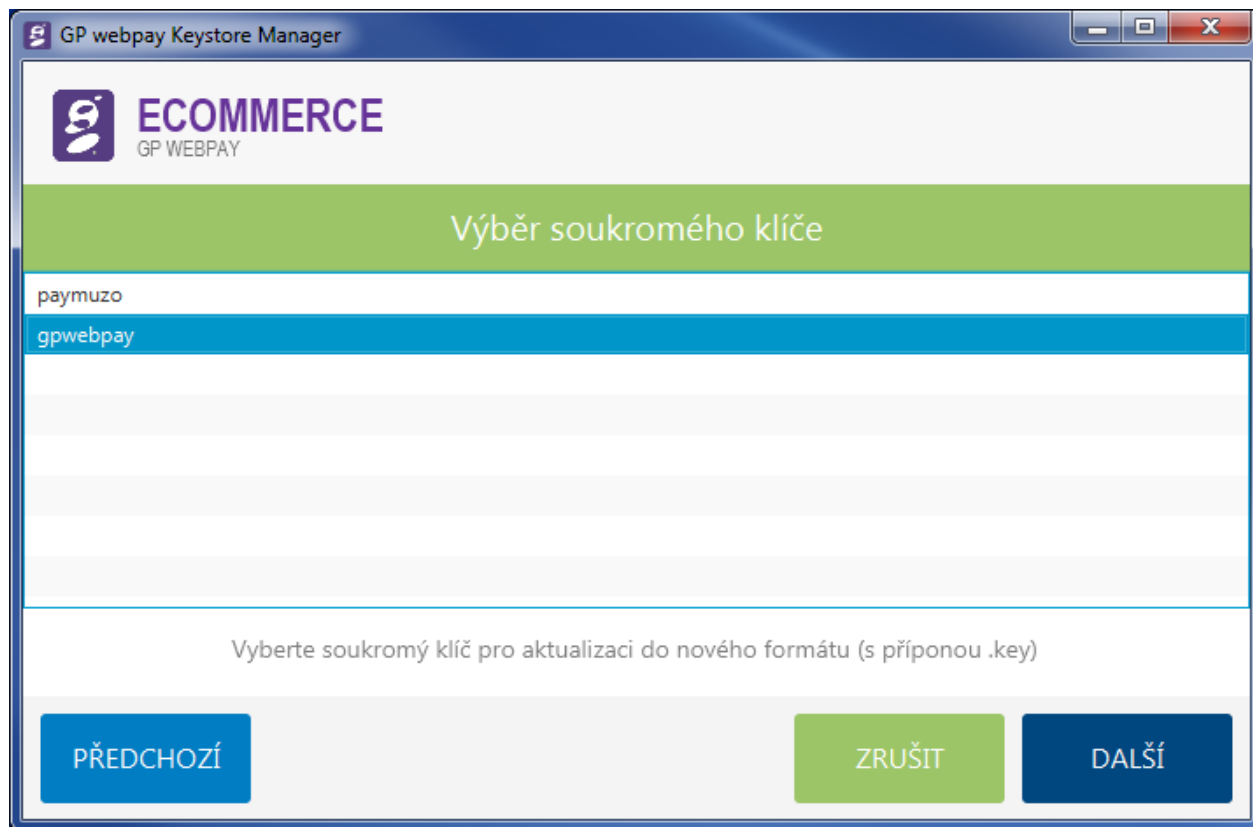
Potvrdit výběr souboru tlačítkem „Otevřít“.

Výběrové okno se uzavře a aplikace čeká na zadání hesla k původnímu úložišti soukromého klíče a stisk tlačítka „Další“. Následuje pokus o načtení obsahu souboru.

Pokud je chybně zadáno heslo, popř. soubor neobsahuje soukromý klíč, je zobrazeno hlášení:



V případě, že soubor úložiště obsahuje více soukromých klíčů, dojde k zobrazení seznamu klíčů a je potřeba vybrat správný soukromý klíč:



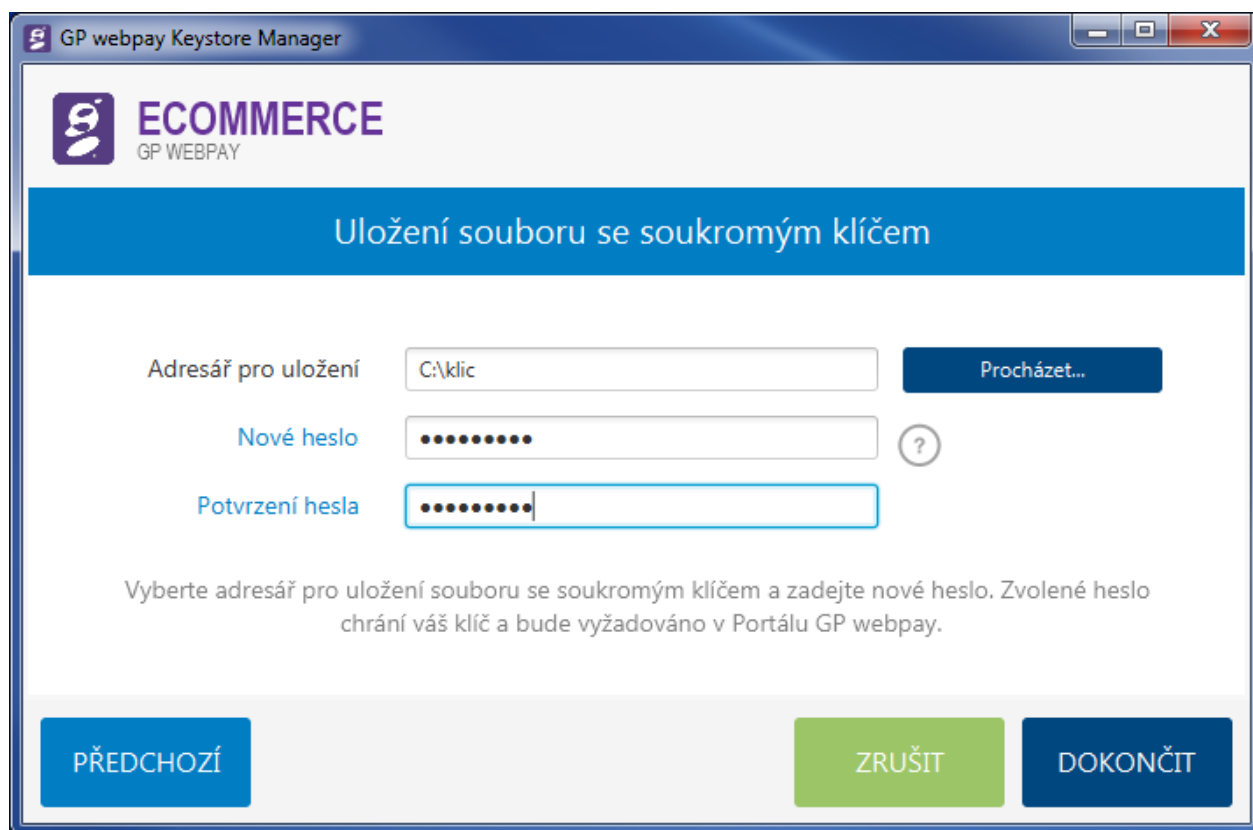
a pokračovat tlačítkem „Další“. V případě existence pouze jednoho soukromého klíče je tato obrazovka přeskočena.

Po ověření správnosti vstupního souboru, popř. potvrzení výběru klíče, je zobrazena výzva pro výběr cílového adresáře pro uložení konvertovaného souboru a požadavek na zadání nového hesla k soukromému klíči. Heslo musí být zadáno 2x, aby se předešlo překlepům.

Heslo musí být dlouhé min. 8 znaků a obsahovat nejméně 3 typy z následujících požadovaných typů znaků:

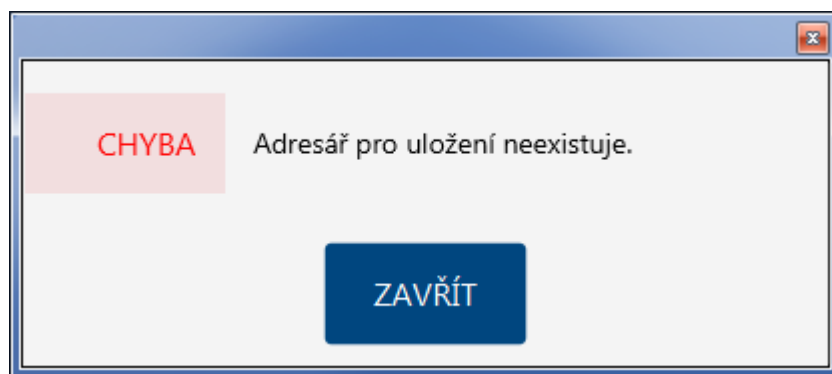
- velké písmeno

- malé písmeno
- číslice
- speciální znak

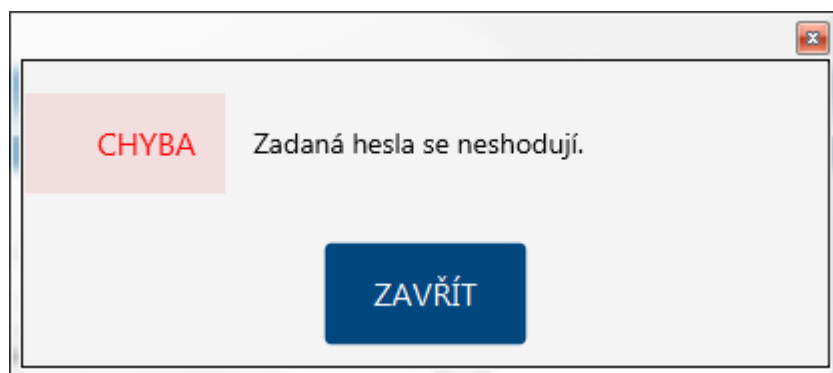


Po zadání všech potřebných informací je možné akci dokončit stiskem tlačítka „Dokončit“. Také je možno se vrátit k minulému kroku tlačítkem „Předchozí“, popř. pomocí tlačítka „Zrušit“ skočit zpět na úvodní obrazovku.

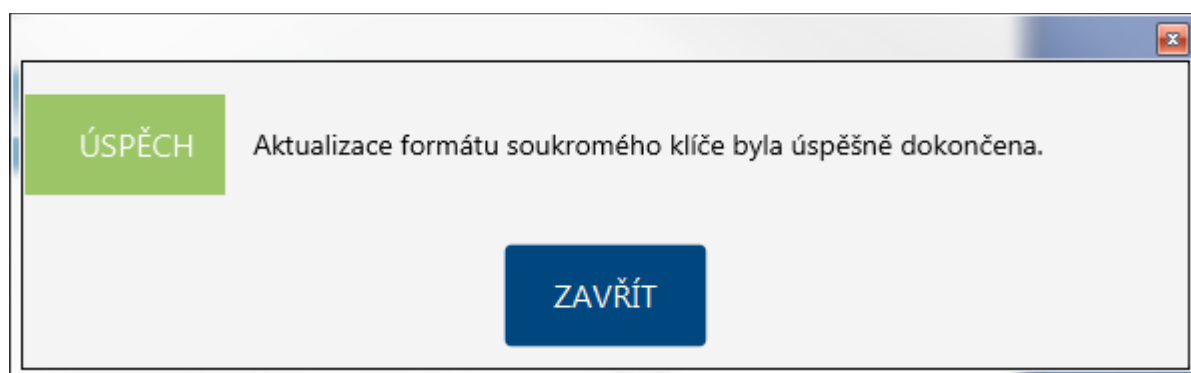
Pokud je zadán neexistující adresář, je při pokusu o pokračování zobrazeno hlášení:



V případě nerovnosti hesel je zobrazena informace:



Jestliže bylo vše zadáno v pořádku, dojde ke konverzi klíče a zobrazí se hlášení:



Ve zvoleném cílovém adresáři vznikne soubor se jménem „gpwebpay-pvk.key“. Soubor obsahuje soukromý klíč v textovém formátu PEM.

A po stisku tlačítka „Zavřít“ se aplikace vrátí na úvodní obrazovku.

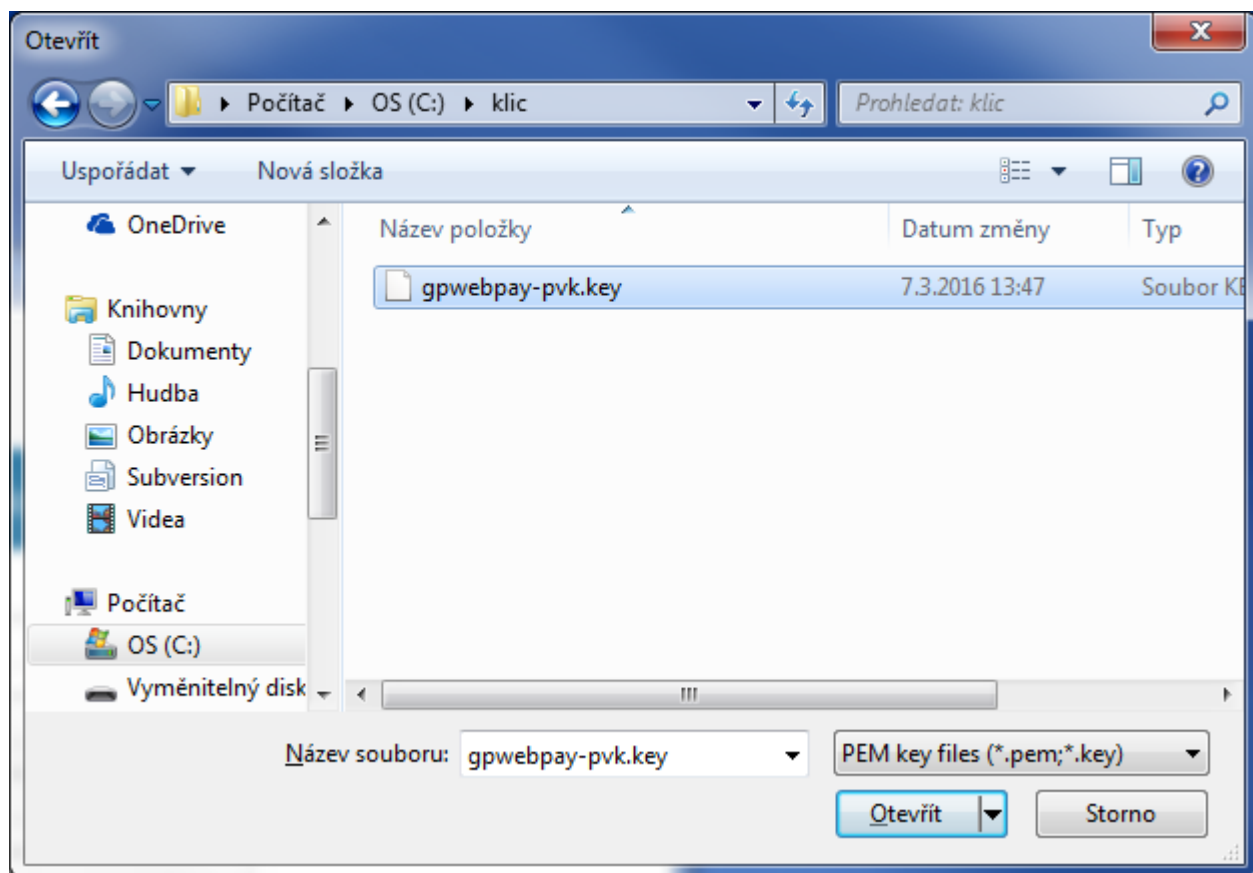
3.3.2 Změna hesla

Tato volba pracuje s novým formátem úložiště soukromého klíče a je nutné nejdříve soubor úložiště aktualizovat – viz předchozí kapitola, nebo použít soubor v novém tvaru získaný z Portálu GP webpay.

Po stisku „dlaždice“ dojde otevření nového okna pro zadání potřebných údajů:

The screenshot shows the 'GP webpay Keystore Manager' application window. The title bar includes standard Windows window controls. The main header features the 'ECOMMERCE GP WEBPAY' logo. Below this, a blue banner displays the title 'Změna hesla soukromého klíče' (Change private key password). The interface contains four input fields: 'Cesta k souboru' (File path) with a 'Procházet...' (Browse...) button, 'Heslo' (Password), 'Nové heslo' (New password) with a help icon, and 'Potvrzení hesla' (Confirm password). A text instruction below the fields reads: 'Vyberte soubor se soukromým klíčem (s příponou .key), u kterého chcete změnit heslo.' (Select a file with a private key (with extension .key), for which you want to change the password). At the bottom right, there are two buttons: 'ZRUŠIT' (Cancel) in green and 'DOKONČIT' (Finish) in blue.

Nejdříve je nutné, pomocí funkce „Procházet“ najít na souborovém systému adresář se souborem soukromého klíče:

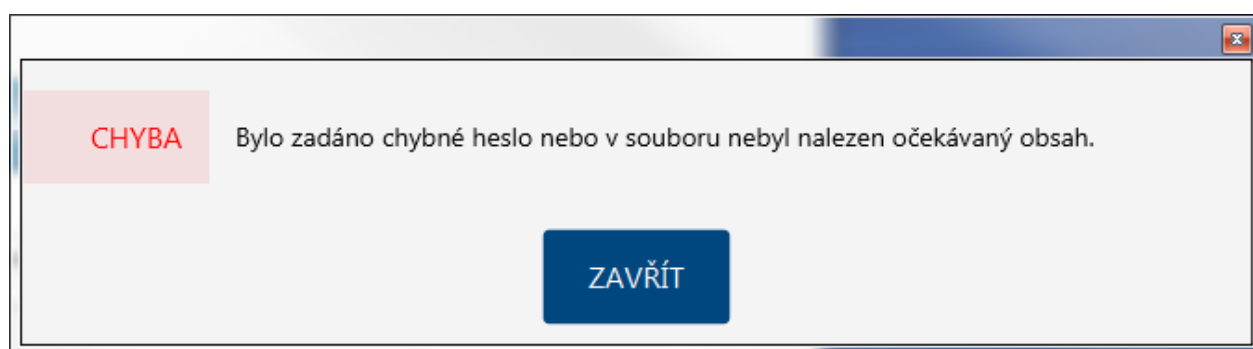


a patřičný soubor „Otevřít“. Dále je potřeba zadat heslo k původnímu klíči a heslo nové (samozřejmě je ověření nového hesla duplicitním zadáním).

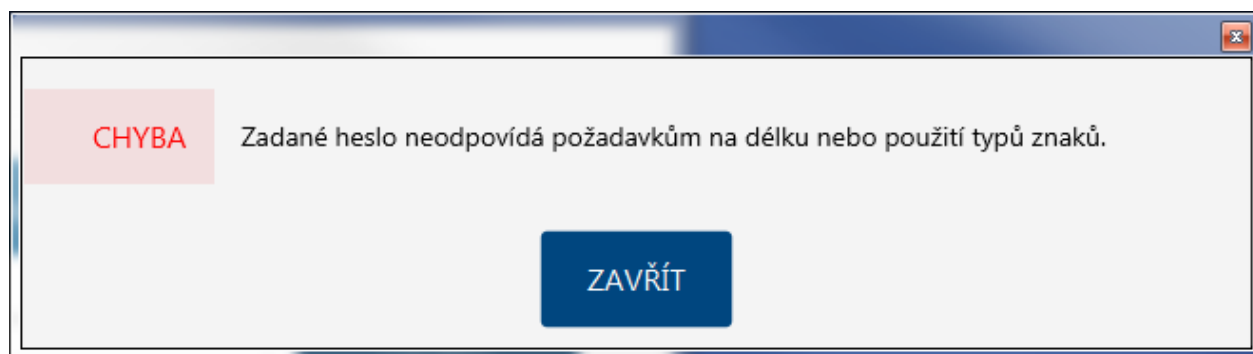
Heslo musí být dlouhé min. 8 znaků a obsahovat nejméně 3 typy z následujících požadovaných typů znaků:

- velké písmeno
- malé písmeno
- číslice
- speciální znak

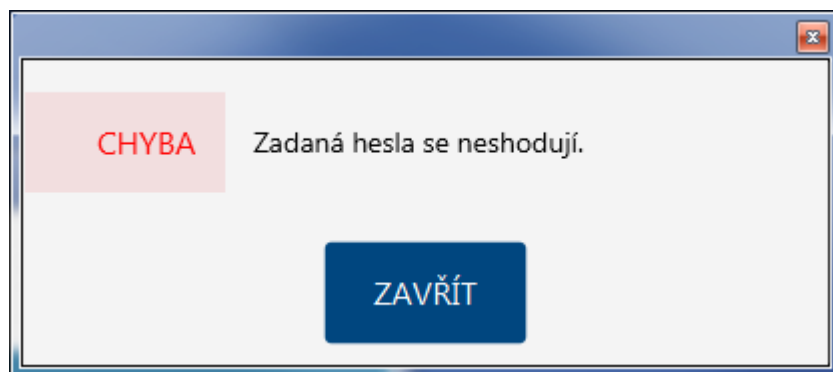
Při chybném starém heslu nebo špatném formátu souboru je zobrazeno hlášení:



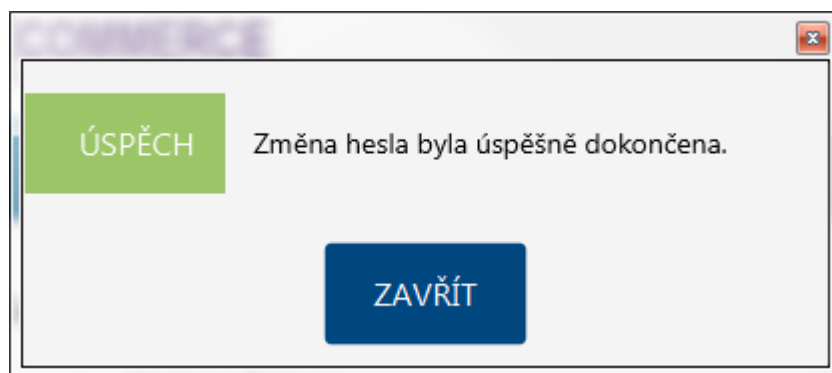
Pokud není zadáno nové heslo nebo nesplňuje potřebné bezpečnostní požadavky, tak je zobrazeno hlášení:



Jestliže se nové heslo neshoduje s potvrzením hesla, je tato situace indikována hlášením:



V případě správně zadaných hodnot je zobrazeno potvrzení o úspěšné změně hesla:



a následuje návrat na úvodní obrazovku.

3.3.3 Pro vývojáře

Sekce „PRO VÝVOJÁŘE“ je primárně určena pro programátory implementující platební bránu do e-shopu obchodníka.

Volba spustí proces konverze formátu úložiště soukromého klíče do další nejpoužívanějších formátů úložišť a současně uloží veřejnou část klíče do obecně použitelných formátů.

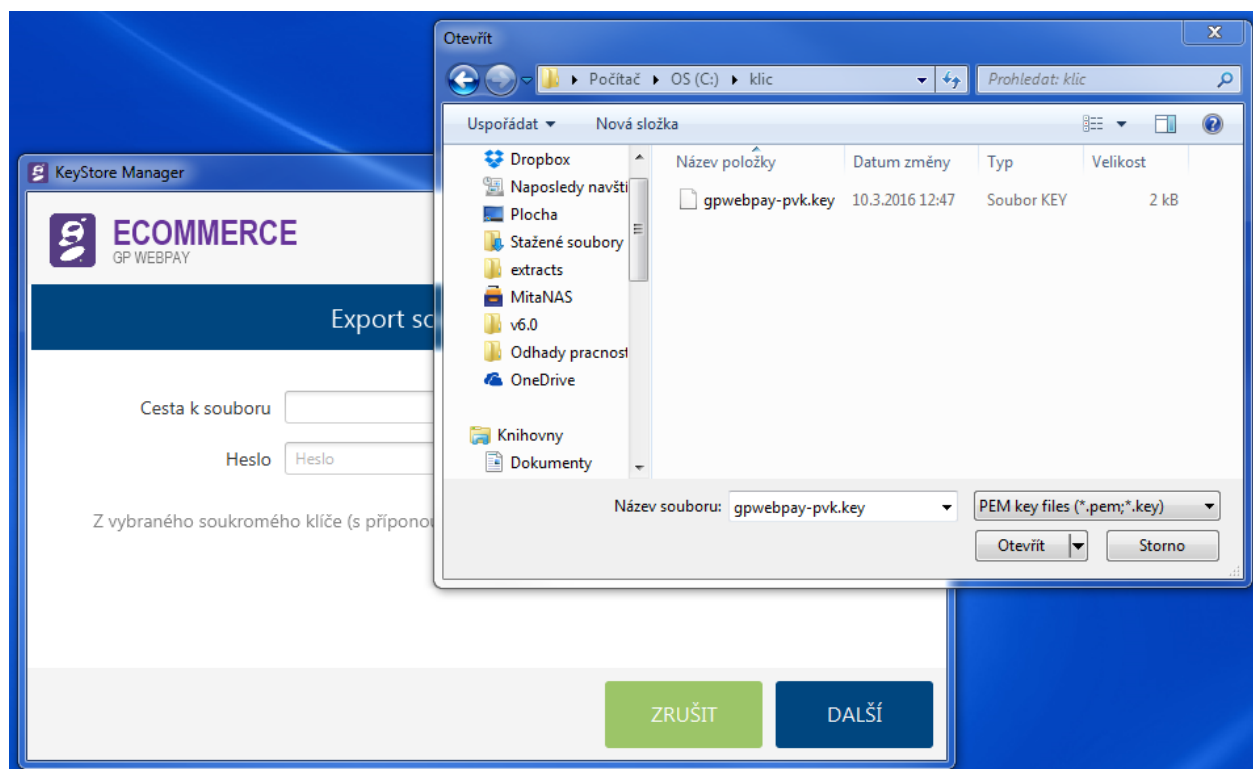
Vstupní formát úložiště soukromého klíče:

- textový formát PEM (PVK) – `gpwebpay-pvk.key`

Výstupní formáty úložišť a souborů:

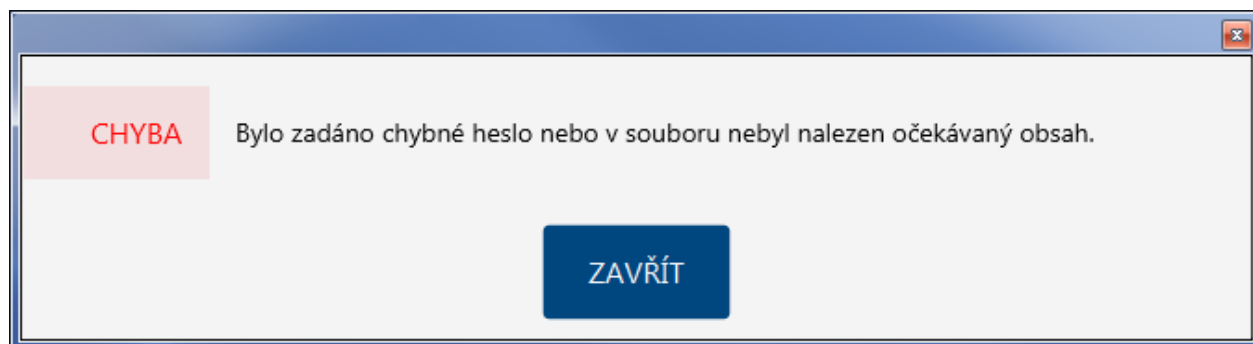
- úložiště soukromého klíče:
 - JAVA formát JKS – `gpwebpay-pvk.jks`
 - Microsoft PKCS12 – `gpwebpay-pvk.p12`
- soubor veřejného klíče:
 - textový formát PEM – `gpwebpay-pub.pem`
 - binární formát DER – `gpwebpay-pub.cer`

Prvním krokem konverze je výběr souboru úložiště soukromého klíče. Pomocí tlačítka „Procházet“ je nutné vybrat soubor s úložištěm soukromého klíče:



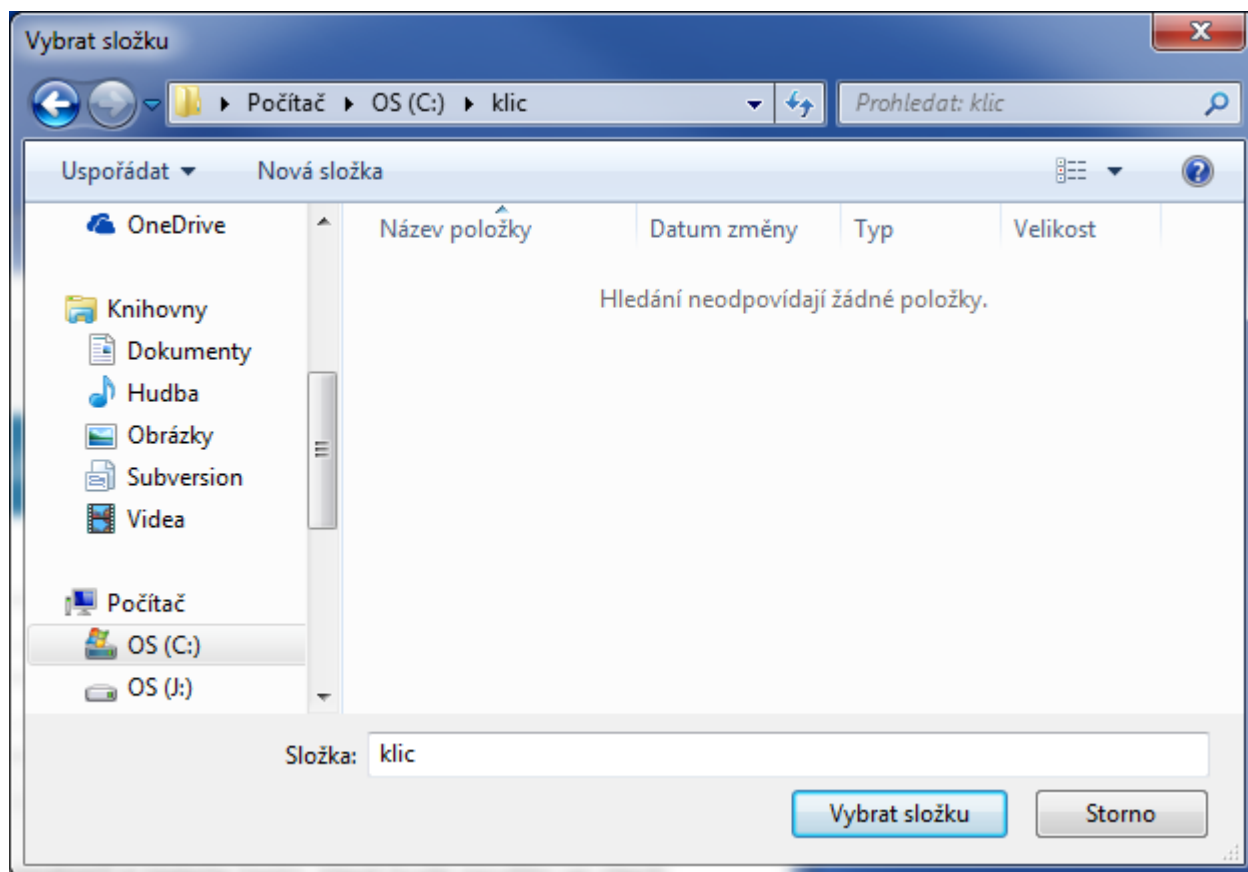
Soubor „Otevřít“, zadat heslo a stisknout tlačítko „Další“.

V případě chyby hesla nebo chybného vnitřního formátu souboru úložiště je zobrazeno hlášení:



V opačném případě následuje výzva k výběru výstupního adresáře pro uložení nově vzniklých souborů a zadání nového hesla k úložišti (to samé heslo se také použije k zabezpečení soukromého klíče v úložišti, lze použít i původní heslo).

Tlačítkem „Procházet“ se otevře okno pro výběr výstupního adresáře, po vyhledání potřebného místa v souborovém systému je potřeba volbu potvrdit tlačítkem „Vybrat složku“:



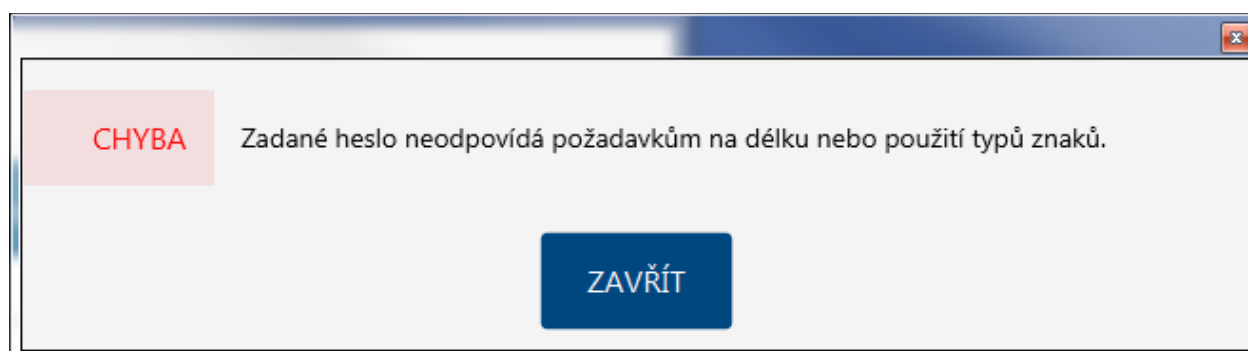
dále je potřeba zadat heslo a jeho potvrzení.

Heslo musí být dlouhé min. 8 znaků a obsahovat nejméně 3 typy z následujících požadovaných typů znaků:

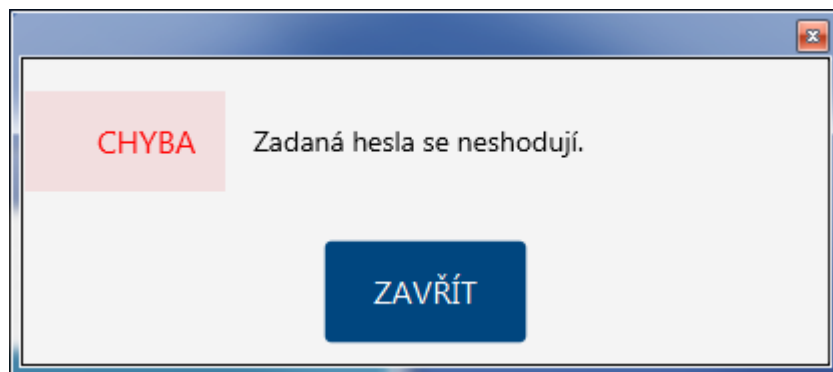
- velké písmeno
- malé písmeno
- číslice
- speciální znak

Následuje stisk tlačítka „Dokončit“.

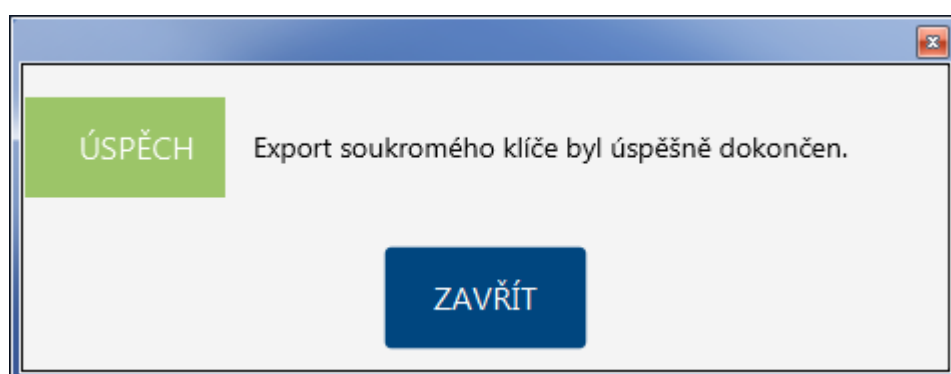
Pokud není zadáno nové heslo nebo nesplňuje potřebné bezpečnostní požadavky, tak je zobrazeno hlášení:



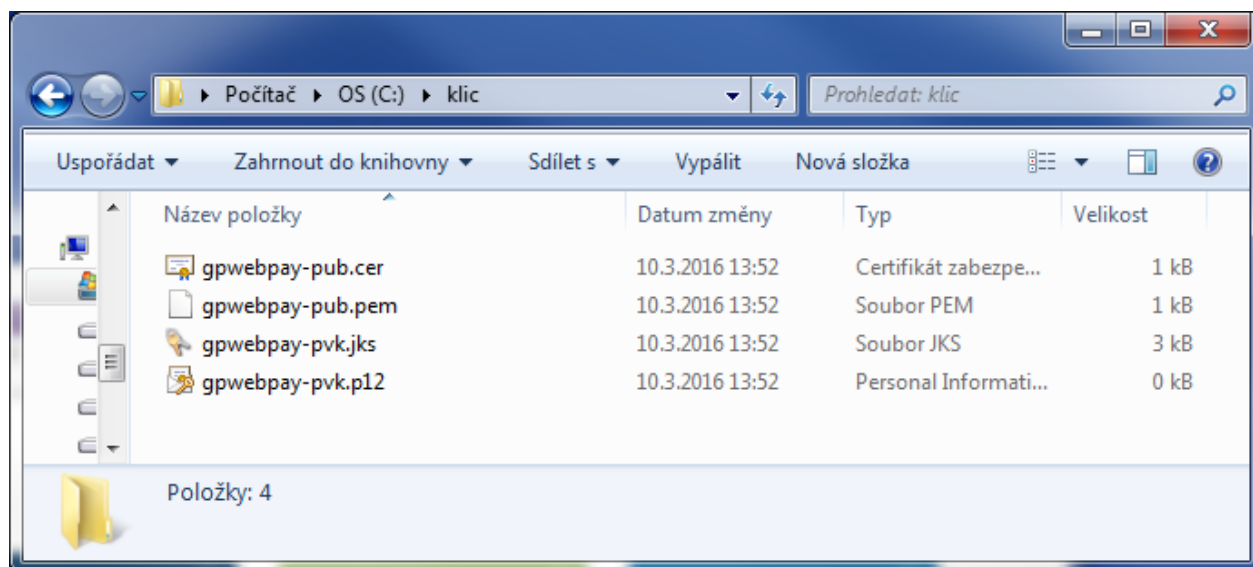
Jestliže se nové heslo neshoduje s potvrzením hesla, je tato situace indikována hlášením:



V případě správně zadaných hodnot je zobrazeno potvrzení o úspěšném exportu soukromého klíče:



Tímto je proces exportu soukromého klíče ukončen a v zadaném výstupním adresáři jsou vytvořeny tyto soubory:



- gpwebpay-pvk.jks – soukromý klíč v úložišti jazyku JAVA (JKS)
 - použitelný pro JSP/JAVA aplikace
- gpwebpay-pvk.p12 – soukromý klíč v úložišti ve struktuře Microsoft (PKCS12 – P12)
 - použitelný pro aplikace .NET

- `gpwebpay-pub.pem` – textový PEM (PVK) formát veřejného klíče
 - použitelný pro PHP aplikace na ověření správnosti hodnoty podpisu vytvořeným pomocí soukromého klíče
- `gpwebpay-pub.cer` – binární DER formát veřejného klíče
 - použitelný pro .NET aplikace na ověření správnosti hodnoty podpisu vytvořeným pomocí soukromého klíče
 - formát pro zaslání veřejného klíče aplikační podpoře GP webpay, pokud selže nahrání veřejného klíče prostřednictvím Portálu GP webpay

Po stisku tlačítka „Zavřít“ se aplikace vrátí na úvodní obrazovku.