

Integrovaný informační systém Státní pokladny (IISPP)

Centrální systém účetních informací státu (CSÚIS)

Šifrovací utilita pro účetní jednotky

(Uživatelská dokumentace)

Obsah

1. Instalace aplikace	3
1.1 Požadavky na pracovní stanici	3
1.2 Instalace.....	3
1.3 Aktualizace.....	5
1.4 Ověřování integrity aplikace.....	5
2. Procesy aplikace	6
2.1 Dekódování identifikačních údajů	6
2.2 Příprava dat k odeslání	10
2.3 Dešifrování přijatých dat	13
3. Využití zdrojových kódů aplikace.....	16

1. Instalace aplikace

1.1 Požadavky na pracovní stanici

Aplikace je dodávána pro platformu Java 6 a je tedy funkční všude tam, kde je možné mít nainstalováno a funkční Java Runtime Environment verze 6 (tj. platformy Windows, Linux, MacOSX). JRE 6 lze zdarma stáhnout a nainstalovat ze stránek <http://java.com/en/download/index.jsp> a k instalaci stačí běžná uživatelská oprávnění.

Vzhledem k tomu, že vyhláškou definované šifrovací algoritmy vyžadují použití tzv. nelimitované kryptografie v JRE, je nutné upravit konfiguraci standardní instalace JRE – nakopírovat do instalace JRE soubory politik neomezujičích sílu kryptografie (tzv. Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6). Tyto soubory je možné stáhnout přímo ze stránek dodavatele Java – např. <http://java.sun.com/javase/downloads/index.jsp>.

Po rozbalení staženého ZIP souboru je nutné obsažené soubory local_policy.jar a US_export_policy.jar nakopírovat do adresáře \$JAVA_HOME\lib\security, kde \$JAVA_HOME představuje domovský adresář JRE (obvykle C:\Program Files\Java\jre6). Při instalaci těchto souborů je nutné dodržet restriktce pro export silné kryptografie, které jsou součástí instalačního balíčku v souboru COPYRIGHT.html.

Aplikace si při spouštění ověřuje, zda používaná verze JRE má upravenou konfiguraci tak, aby používala nelimitovanou kryptografii, a pokud nemá, zobrazí upozornění a ukončí se.



Požadavky na výkonnost počítače jsou dány především zvolenou verzí operačního systému, JRE neklade na HW počítače žádné zvýšené nároky. Minimální konfigurace počítače pro nejrozšířenější platformu Windows x86 tak odpovídá požadavkům pro nejstarší podporovanou verzi operačního systému - MS Windows 2000, což předpokládá procesor min. 300 MHz a min. 128 MB RAM. Úplný přehled podporovaných HW platforem, verzí operačních systémů a konfigurací je k dispozici na internetu na adrese <http://java.sun.com/javase/6/webnotes/install/system-configurations.html>.

1.2 Instalace

Uživatel si aplikaci nainstaluje kliknutím na odkaz na stránkách Ministerstva financí. Po stažení a úspěšném nainstalování aplikace se uživateli na ploše vytvoří ikona, pomocí které může spouštět nainstalovanou aplikaci (a to i v off-line módu, bez připojení k internetu).

Detailní popis procesu instalace přitom probíhá následujícím způsobem:

- Uživatel na webové stránce MFCR zvolí odkaz **Stahování Šifrovací utility**.
- Po spuštění bude uživateli zobrazeno dialogové okno s průběhem stahování a informací o vydavateli utility (Obrázek č. 1 Stahování utility ze stránek MFCR).



Obrázek č. 1 Stahování utility ze stránek MFCR


- Po úspěšném stažení je uživateli zobrazen dialog, ve kterém je opět zobrazen vydavatel této utility a uživatel již v tomto kroku provádí vlastní instalaci aplikace z lokálně stažené kopie. (Obrázek č. 2 Potvrzení instalace šifrovací utility). Pokračování instalace je nutné potvrdit tlačítkem Run (následně dojde k prvnímu spuštění aplikace). Případné detailnější informace o vydavateli a jeho certifikátu lze získat po kliknutí na odkaz *More Information*



Obrázek č. 2 Potvrzení instalace šifrovací utility

- Dialogové okno požadující potvrzení spuštění aplikace podepsané níže uvedeným vydavatelem (LogicaCMG Code Sign) je zobrazováno při každém spuštění aplikace. Pro odstranění

zobrazování tohoto dialogu je nutné zařadit certifikát vydavatele mezi důvěryhodné certifikáty. To lze učinit zaškrtnutím volby *Always trust content from this publisher*.

- Po dokončení instalace bude uživateli vytvořena na ploše ikona  s popisem „Šifrovací utilita pro přípravu dat pro odeslání do CSÚIS“. Zároveň s tím bude vytvořena i nová položka ve start menu (MF Státní pokladna).

1.3 Aktualizace

Je-li počítač, na kterém je aplikace instalována, připojen k internetu, aplikace si při každém spuštění zkontroluje, zda není na serveru MF dostupná její novější verze, a v případě potřeby se sama zaktualizuje.

Pokud je počítač off-line (bez připojení k internetu), kontrola verzí neproběhne a spustí se verze, která je na počítači nainstalována.

1.4 Ověřování integrity aplikace

Instalovaná aplikace je vytvořena pomocí technologie Java WebStart. Tato technologie zajišťuje, kromě jednoduché instalace a aktualizace i vysokou bezpečnost provozování aplikace rozšířením technologie používané Java Applet. Aplikace Java WebStart jsou provozovány v řízeném prostředí, ze kterého mohou přistupovat k lokální síti nebo k souborovému systému pouze pokud je aplikace podepsána důvěryhodným certifikátem a uživatel instalaci této aplikace výslovně potvrdil. Tím je zamezeno možnému podvržení kódu.

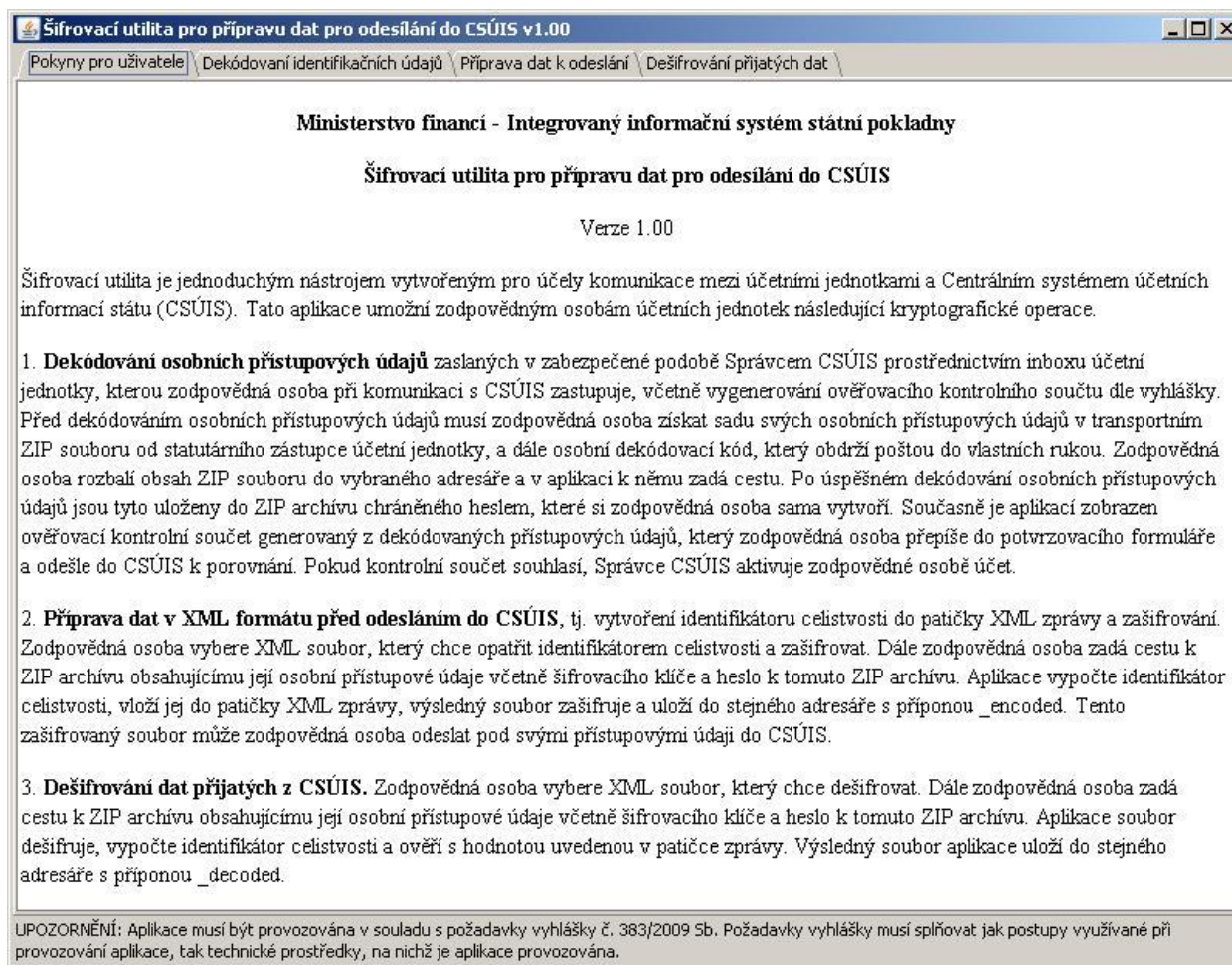
Nainstalovaná aplikace je v podepsané podobě uložena i na lokálním disku počítače a integrity aplikace (validita elektronického podpisu binárního souboru) je ověřována při každém spuštění aplikace. V případě, že dojde k narušení integrity aplikace (např. vlivem náhodného poškození souboru na disku nebo záměrnou nežádoucí úpravou aplikace), je uživatel při startu aplikace vyzván ke stažení nové verze aplikace z původní distribuční URL adresy (Obrázek č. 3 Vynucení stažení aktualizované verze aplikace). Spuštění nevalidní (např. poškozené) aplikace je tak vyloučeno.



Obrázek č. 3 Vynucení stažení aktualizované verze aplikace

2. Procesy aplikace

Aplikace při spuštění zobrazuje stručné pokyny pro uživatele.



2.1 Dekódování identifikačních údajů

Funkce slouží pro dekódování osobních přístupových údajů zaslaných v zabezpečené podobě Správcem CSÚIS prostřednictvím inboxu účetní jednotky, kterou zodpovědná osoba při komunikaci s CSÚIS zastupuje, včetně vygenerování ověřovacího kontrolního součtu dle vyhlášky. Před dekódováním osobních přístupových údajů musí zodpovědná osoba získat sadu svých osobních přístupových údajů v transportním ZIP souboru od statutárního zástupce účetní jednotky, a dále osobní dekódovací kód, který obdrží poštou do vlastních rukou.

Jako první krok rozbalte obsah ZIP souboru do vybraného adresáře a v aplikaci na záložce „**Dekódování identifikačních údajů**“ k němu zadejte cestu. Tento adresář musí obsahovat následující soubory:

AESKEY_C.TXT

UJEID.TXT

LOGIN_C.TXT

DATNAR.TXT

PASSWD_C.TXT

JMEZO.TXT

DTRANS_PWD.TXT

PRIZO.TXT

PAC_PWD.TXT

Uživatel musí mít nastavené právo zápisu do tohoto adresáře.

Šifrovací utilita pro přípravu dat pro odesílání do CSÚIS v1.00

Pokyny pro uživatele Dekódování identifikačních údajů Příprava dat k odeslání Dešifrování přijatých dat

Zadejte prosím cestu k adresáři, ve kterém je rozbalen obsah ZIP souboru, který jste obdržel(a) od statutárního zástupce účetní jednotky.

D:\mf_client\yzorkyD

Zadejte prosím osobní dekodovací kód, který jste obdržel(a) od CSÚIS poštou do vlastních rukou (64 znaků).

1347673496429813229487444172809179634786492440515305912220341357

Zadejte prosím heslo k ZIP archivu, do kterého budou vaše přístupové údaje po dekodování bezpečně uloženy. Heslo musí vyhovovat požadavkům vyhlášky, tj. minimální délka hesla je 8 znaků, musí obsahovat písmena i čísla, všechny číslice nesmí být na pozicích, které spolu sousedí, písmena nesmí tvořit srozumitelné slovo v českém či anglickém jazyce. Heslo není citlivé na velká a malá písmena.

Nové heslo k ZIP archivu

Potvrzení hesla k ZIP archivu

Dekóduj

UPOZORNĚNÍ: Aplikace musí být provozována v souladu s požadavky vyhlášky č. 383/2009 Sb. Požadavky vyhlášky musí splňovat jak postupy využívané při provozování aplikace, tak technické prostředky, na nichž je aplikace provozována.

Následně zadejte osobní dekodovací kód a dvakrát nové heslo k ZIP archivu, do kterého se úspěšně dekodované přístupové údaje ukládají. Pro vytváření hesla platí následující podmínky:

- může obsahovat pouze písmena a číslice
- musí obsahovat minimálně 8 znaků
- musí obsahovat 2 až 5 číslic, které ale nesmí následovat bezprostředně za sebou

Všechny zadané znaky se v aplikaci následně automaticky převádějí na velká písmena a heslo k ZIPu tak obsahuje vždy pouze velká písmena.

Heslo k ZIP archivu si zapamatujte. Budete ho potřebovat při přípravě a zpracování dat pro komunikaci s CSÚIS (viz procesy 2.2 a 2.3).

Pak klikněte na tlačítko „**Dekóduj**“.

Po odkliknutí informační hlášky se na obrazovce zobrazí dešifrované přístupové údaje spolu s ověřovacím kontrolním součtem, který je generován z dešifrovaných přístupových údajů.

Tento kontrolní součet zodpovědná osoba přepíše do potvrzovacího formuláře (viz Vyhláška, příloha č. 10) a odešle do CSÚIS k porovnání. Pokud kontrolní součet souhlasí, Správce CSÚIS aktivuje zodpovědné osobě účet a vyrozumí o tom účetní jednotku prostřednictvím zprávy zaslané do inboxu.

Zároveň se v zadaném adresáři vytvoří ZIP archiv PersonalCodesStorage.zip chráněný heslem, které si zodpovědná osoba vytvořila. Tento ZIP archiv obsahuje dešifrovaný AES klíč a další dešifrované přístupové údaje.

Upozornění: Pokud budete ZIP archiv otvírat i v jiné aplikaci, je nutné všechna písmena v hesle zadávat velkými písmeny!

Šifrovací utilita pro přípravu dat pro odesílání do CSÚIS v1.00

Pokyny pro uživatele Dekódování identifikačních údajů Příprava dat k odeslání Dešifrování přijatých dat

Zadejte prosím cestu k adresáři, ve kterém je rozbalen obsah ZIP souboru, který jste obdržel(a) od statutárního zástupce účetní jednotky.

D:\mf_client\vozorkyD

Zadejte prosím osobní dekodovací kód, který jste obdržel(a) od CSÚIS poštou do vlastních rukou (64 znaků).

1347673496429813229487444172809179634786492440515305912220341357

Zadejte prosím heslo k ZIP archívu, do kterého budou vaše přístupové údaje po dekódování bezpečně uloženy. Heslo musí vyhovovat požadavkům vyhlášky, tj. minimální délka hesla je 8 znaků, musí obsahovat písmena i čísla, všechny číslice nesmí být na pozicích, které spolu sousedí, písmena nesmí tvořit srozumitelné slovo v českém či anglickém jazyce. Heslo není citlivé na velká a malá písmena.

Nové heslo k ZIP archívu

Potvrzení hesla k ZIP archívu

Dekóduj

Dekódované osobní přístupové údaje:
Přístupové jméno pro přihlášení k CSÚIS: 0010000050
Přístupové heslo pro přihlášení k CSÚIS: hn8yo7ui

Tyto údaje byly současně uloženy do souboru PersonalCodesStorage.zip.

Ověřovací kontrolní součet pro odeslání do CSÚIS:
eb8be2f81c99006d867bb40e843253b1021f031cf6e88638e5f54b1ea271246c

UPOZORNĚNÍ: Aplikace musí být provozována v souladu s požadavky vyhlášky č. 383/2009 Sb. Požadavky vyhlášky musí splňovat jak postupy využívané při provozování aplikace, tak technické prostředky, na nichž je aplikace provozována.

V případě, že Správce CSÚIS oznámí účetní jednotce prostřednictvím zprávy zaslané do inboxu, že zaslany ověřovací kontrolní součet nesouhlasí, postupuje zodpovědná osoba následovně:

1. Zopakuje postup Dekódování osobních přístupových údajů počínaje rozbalením získaného ZIP souboru s přístupovými údaji v zabezpečené podobě a ověří, že ověřovací kontrolní součet odeslaný do CSÚIS k ověření byl správný (že nedošlo k chybě při přepisování do formuláře).
2. V případě, kdy původně odeslaný ověřovací kontrolní součet do CSÚIS byl chybný, odešle zodpovědná osoba správný ověřovací kontrolní součet na novém formuláři stejným způsobem do 24 hodin od přijetí zprávy o neúspěšném ověření a aktivaci účtu. Správce CSÚIS následně ověří nově zaslany ověřovací kontrolní součet a pokud souhlasí, aktivuje zodpovědné osobě účet.
3. V případě, kdy původně odeslaný ověřovací kontrolní součet do CSÚIS byl správný, zodpovědná osoba nedělá nic a vyčká, až Správce CSÚIS pro ní vygeneruje novou sadu osobních přístupových údajů dle vyhlášky. Správce CSÚIS nové generování osobních přístupových údajů provede automaticky, pokud do 24 hodin po oznámení chyby při ověření kontrolního součtu neobdrží od zodpovědné osoby opravený ověřovací kontrolní součet.
4. Pro urychlené řešení problémů s ověřením kontrolního součtu může rovněž zodpovědná osoba kontaktovat Helpdesk IISSP.

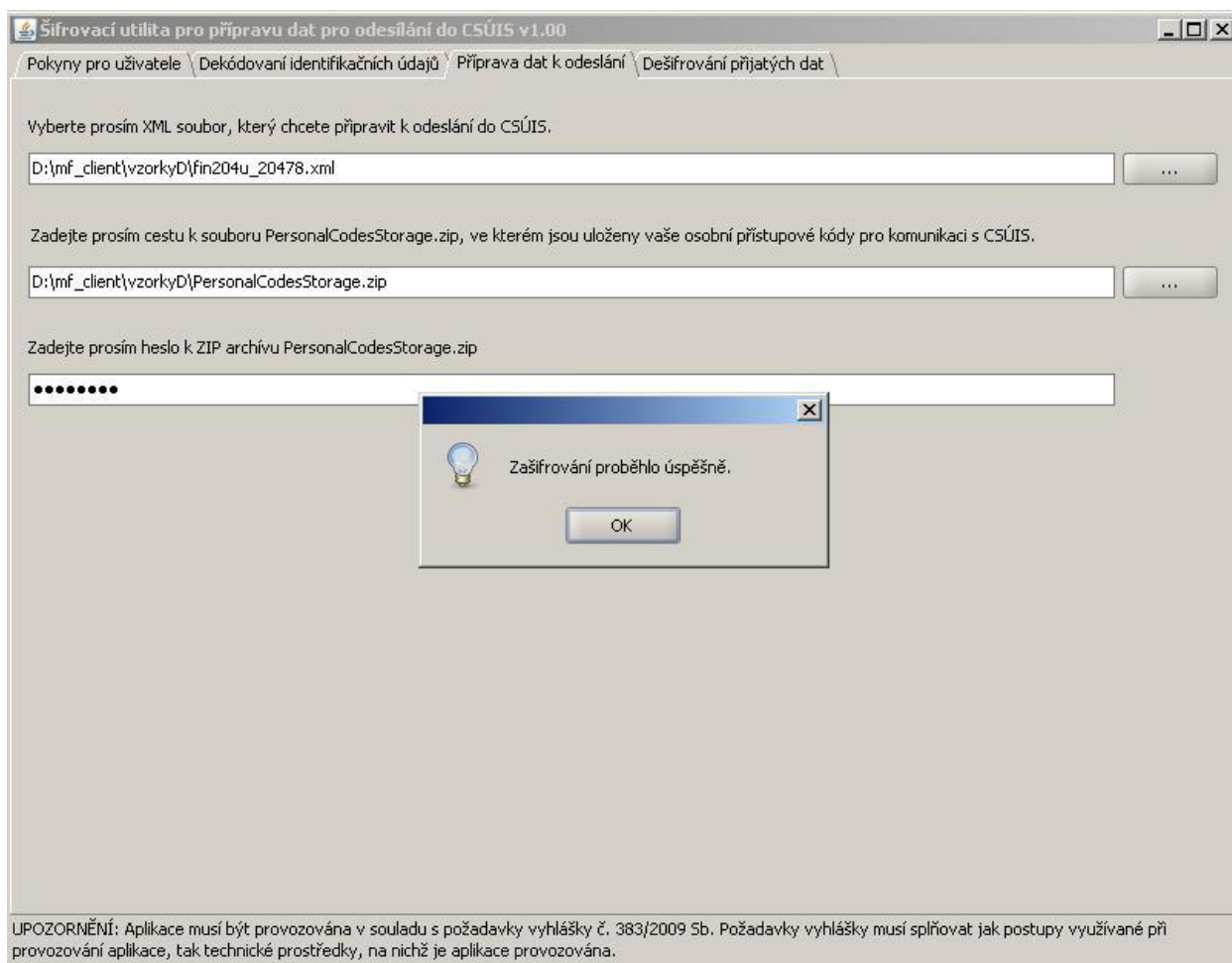
2.2 Příprava dat k odeslání

Tato funkce slouží k přípravě dat v XML formátu před odesláním do CSÚIS, tj. k vytvoření identifikátoru celistvosti do patičky XML zprávy a zašifrování XML zprávy.

Na záložce „**Příprava dat k odeslání**“ vyberte XML soubor, který má být opatřen identifikátorem celistvosti a zašifrován.

Dále zadejte cestu k ZIP archívu (vytvořený procesem 1) obsahujícímu vaše osobní přístupové údaje, včetně šifrovacího AES klíče, a zadejte heslo k ZIP archívu (zadávaní hesla není citlivé na velká a malá písmena – aplikace si všechny zadané znaky automaticky převádí na velká písmena). Nakonec klikněte na tlačítko „**Zašifruj**“.

Aplikace vypočte identifikátor celistvosti, vloží jej do patičky XML zprávy, výsledný XML soubor zašifruje a uloží ho s příponou *_encoded* do stejného adresáře, v kterém se nachází původní soubor. Tento zašifrovaný soubor může zodpovědná osoba odeslat pod svými přístupovými údaji do CSÚIS.



Příklad: Ze souboru *pohledavky.xml* vznikne soubor *pohledavky_encoded.xml*

Šifrovací utilita pro přípravu dat pro odeslání do CSÚIS v1.00

Pokyny pro uživatele Dekódování identifikačních údajů Příprava dat k odeslání Dešifrování přijatých dat

Vyberte prosím XML soubor, který chcete připravit k odeslání do CSÚIS.

D:\mf_client\vizorkyD\fin204u_20478.xml

Zadejte prosím cestu k souboru PersonalCodesStorage.zip, ve kterém jsou uloženy vaše osobní přístupové kódy pro komunikaci s CSÚIS.

D:\mf_client\vizorkyD\PersonalCodesStorage.zip

Zadejte prosím heslo k ZIP archívu PersonalCodesStorage.zip

.....

Zašifruj

Identifikátor celistvosti byl úspěšně vygenerován a vložen do XML zprávy.

XML zpráva byla úspěšně zašifrována a uložena do souboru:
D:\mf_client\vizorkyD\fin204u_20478_encoded.xml

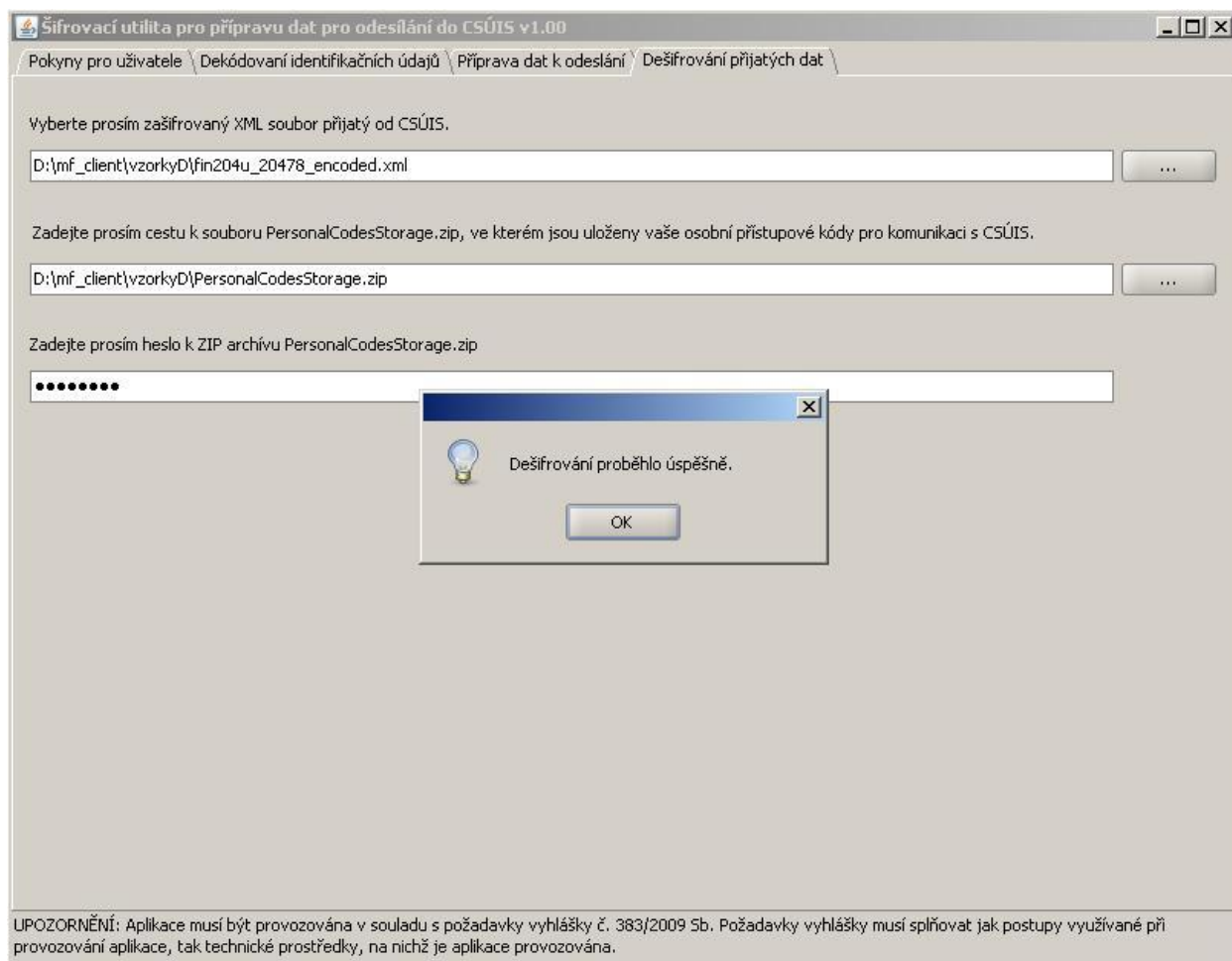
UPOZORNĚNÍ: Aplikace musí být provozována v souladu s požadavky vyhlášky č. 383/2009 Sb. Požadavky vyhlášky musí splňovat jak postupy využívané při provozování aplikace, tak technické prostředky, na nichž je aplikace provozována.

2.3 Dešifrování přijatých dat

Tato funkce slouží k dešifrování dat přijatých z CSÚIS.

Na záložce „**Zpracování přijatých dat**“ vyberte zašifrovaný soubor přijatý od CSÚIS.

Dále zadejte cestu k ZIP archívu (vytvořený procesem 1) obsahujícímu vaše osobní přístupové údaje, včetně šifrovacího AES klíče (vytvořený procesem 1). Zadejte heslo k ZIP archívu (zadávání hesla není citlivé na velká a malá písmena – aplikace si všechny zadané znaky automaticky převádí na velká písmena) a klikněte na tlačítko „**Dešifruj**“.



Aplikace dešifruje daný soubor a uloží ho s příponou *_decoded* do stejného adresáře, v kterém se nachází původní soubor.

Příklad: Ze souboru *pohledavky.xml* vznikne *pohledavky_decoded.xml*

Šifrovací utilita pro přípravu dat pro odesílání do CSÚIS v1.00

Pokyny pro uživatele \ Dekódování identifikačních údajů \ Příprava dat k odeslání \ **Dešifrování přijatých dat**

Vyberte prosím zašifrovaný XML soubor přijatý od CSÚIS.

D:\mf_client\ vzorkyD\ fin204u_20478_encoded.xml ...

Zadejte prosím cestu k souboru PersonalCodesStorage.zip, ve kterém jsou uloženy vaše osobní přístupové kódy pro komunikaci s CSÚIS.

D:\mf_client\ vzorkyD\ PersonalCodesStorage.zip ...

Zadejte prosím heslo k ZIP archivu PersonalCodesStorage.zip

.....

Dešifruj

XML zpráva byla úspěšně dešifrována a uložena do souboru:
D:\mf_client\ vzorkyD\ fin204u_20478_encoded_decoded.xml
Ověření integrity dešifrované XML zprávy proběhlo úspěšně.

UPOZORNĚNÍ: Aplikace musí být provozována v souladu s požadavky vyhlášky č. 383/2009 Sb. Požadavky vyhlášky musí splňovat jak postupy využívané při provozování aplikace, tak technické prostředky, na nichž je aplikace provozována.

3. Využití zdrojových kódů aplikace

K aplikaci jsou poskytovány zdrojové kódy ve formě jar knihoven a dokumentace API pro případné využití integrátory a výrobci SW řešení v jejich vlastních produktech. Zdrojové kódy a dokumentace API této aplikace je uveřejněna na webu MF.

Zdrojové kódy jsou poskytnuty pod licencí [Apache verze 2.0](#), což mimo jiné znamená, že

- SW pod touto licencí je dáván k dispozici komukoliv pro nekomerční i komerční využití
- SW pod touto licencí je možné libovolně upravovat či měnit, používat jako celek nebo jeho části
- SW pod touto licencí je dáván k dispozici bez jakýchkoli záruk či podmínek
- v odvozených dílech musí být ve zdrojových kódech ponecháno označení původu zdrojového kódu
- k odvozeným dílům musí být přikládána kopie Apache licence, která informuje o využití zdrojového kódu třetí strany
- využitím zdrojového kódu nevzniká právo či možnost využívání obchodního jména či značky poskytovatele licence.

Kompletní text licence je zveřejněn na adrese <http://www.apache.org/licenses/LICENSE-2.0>

Poskytovatel licence - společnost [Logica Czech Republic s.r.o.](#) neposkytuje žádnou podporu třetím stranám v souvislosti s používáním či úpravami tohoto zdrojového kódu.

Copyright 2009 Logica Czech Republic s.r.o.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
