Integrovaný informační systém Státní pokladny (IISSP)

Centrální systém účetních informací státu (CSÚIS)

Šifrovací utilita pro účetní jednotky

(Otázky a odpovědi)

Obsah

Šifrovací utilita

Otázka č. 1:

Šifrovací utilita vytváří soubor PersonalCodesStorage.zip, který je zabezpečen heslem. Problém je však jakým heslem. Nové heslo, které jsem zadával při Dekódovaní identifikačních údajů není platné.

Odpověď:

Heslo k ZIP archívu obsahuje vždy VELKÁ PÍSMENA, bez ohledu na to, jaká písmena zadával uživatel do hesla při dekódování identifikačních údajů. Bližší informace k práci se ZIP archívem jsou v aktuální verzi uživatelského manuálu na webu MF ČR:
http://www.mfcr.cz/cps/rde/xchg/mfcr/xsl/dane_ucetni_reforma_v_oblasti_vf_techinfo_51708.html

Otázka č. 2:

Po nainstalování Šifrovací utility a zkonfigurování JRE zadám veškeré požadované údaje pro dekódování přístupových údajů, tj.:

1. cestu k adresáři s rozbaleným ZIP
2. osobní dekódovací kód
3. nové heslo ZIP archivu a jeho potvrzení

a kliknu na tlačítko „Dekóduj“. Po kliknutí se nestane nic. Tlačítko se chová, jako by negenerovalo žádnou událost. Žádné varování ani jiné informační okno se neobjeví.

Odpověď:

Ukončete a znovu spusťte Šifrovací utilitu. Pokud restart aplikace nepomůže, může se jednat o chybu aplikace. Detaily o chybě je možné získat z výpisů z Java konsole. Zapnutí Java konzole se provádí v Control Panel - Java, záložka Advanced, Java console – Show. Pokud ani pomocí výpis z Java konzole nebudete schopni problém odstranit a jste přesvědčeni, že se jedná o chybu aplikace, proveďte její nahlášení (viz níže)

Otázka č. 3:

Chci zašifrovat vygenerovaný XML soubor s výkazem dle příslušných XSD schémat pomocí aplikace Šifrovací utilita. Zadám do Šifrovací utility cestu k souboru a cestu a heslo k souboru PersonalCodesStorage.zip. Po klepnutí na „Zašifruj“ vyskočí chybová hláška „Zašifrování XML souboru XXXXXXX se nezdařilo.“ Toto hlášení je dosti obecné, nevrací žádný konkrétní chybový kód. Jak diagnostikovat příčinu chyby?

Odpověď:

Pro získání detailnějšího výpisu aplikace je třeba zapnout Java konzoli. Následně spusťte Šifrovací utilitu a proveďte znovu operaci šifrování XML souboru, který vám nefunguje. Ve výpisu v Java konzoli uvidíte detailní výpis, k čemu při zpracování XML souboru došlo. Zapnutí Java konzole se provádí v Control Panel - Java, záložka Advanced, Java console - Show

Otázka č. 4:

Zkoušel jsem rozbalit archív PersonalCodesStorage.zip, který vznikne po dešifrování osobních přístupových kódů a ve kterém jsou uloženy mé identifikační údaje, heslo atd., ale nepovedlo se mi to, skončil jsem s chybou - neznámá metoda.

Odpověď:

Soubor je určen zejména jako interní úložiště Šifrovací utility. Formát souboru je ZIP s využitím šifrování AES s délkou klíče 256 bit. Tento způsob šifrování není podporován všemi nástroji pro práci se soubory ZIP. Ověřte si, že váš program podporuje AES enkrypci v ZIP archívu.

Otázka č. 5:

Po zadání všech požadovaných údajů a jejich kontrole nelze dekódování provést. Program hlásí " Dekódování se nezdařilo.”

Odpověď:

V první řadě je potřeba ověřit, zda jsou opravdu používány správné údaje (cesta k souboru ZIP, heslo apod.). Pokud ano a problém přetrvává, pak doporučujeme postupovat podle postupu popsaného níže jako řešení „zatuhlé“ aplikace Šifrovací utilita.

Otázka č. 6:

Při snaze o dekódování identifikačních údajů aplikace „zatuhla“ a nereaguje.

Odpověď:

Doporučujeme následujíci postup:
- vyčistit cache webstart pomocí nástrojů webstart nebo
- vyčistit cache webstart přímo na disku
- znovu spustit aplikaci ze stranek MF

Čištění cache nástrojem webstart:
Start -> Spustit ... -> javaws -viewer
Označit řádek s šifrovací utilitou
Pomocí ikonky červeného křížku (X) smazat soubory cache dané aplikace.

Čištění cache přímo na disku:
POZOR: tento postup odstraní rovněž položky náležející jiným webstart aplikacím
V Průzkumníku nebo jiném správci souborů najděte následující složku odpovídající následující (vzhledem k různým lokalizacím a různým uživatelským jménům nelze uvést přesný název)
c:\Documents and Settings\jmeno-uzivatele\Application Data\Sun\Java\Deployment\cache\6.0\
V této složce smažte veškerý obsah.

Otázka č. 7:

Zkopíroval jsem z vašich stránek zdrojové kódy šifrovací utility v jazyce Java (http://www.mfcr.cz/cps/rde/xchg/mfcr/xsl/dane_ucetni_reforma_v_oblasti_vf_techinfo_51709.html). Bohužel se mi tyto zdrojové kódy nepodařilo zkompilovat. Kompilátor hlásí, že tam chybějí nějaké balíčky, konkrétně: com.logica.common.logging.LLogger; com.logica.common.logging.LLoggerFactory; com.logica.cz.namespace.state_treasury.kvs.*; com.logica.cz.namespace.state_treasury.kvs.VerifCode; com.logica.cz.namespace.state_treasury.kvs.VerifResult;

Můžete mi prosím sdělit, kde je možné chybějící soubory získat?

Odpověď:

Zdrojové kódy dodávané současně se šifrovací utilitou jsou publikovány zejména jako reference pro vývojáře na jiných platformách, než je Java, nejsou určeny pro přímé využití v aplikacích. Pokud mají vývojáři zájem o funkcionalitu, která je ve zdrojových kódech publikována, pak již zkompilované třídy najdou v JAR souborech, které jsou součástí instalace šifrovací utility.

Odkazy na původní JAR soubory na webu MF ČR je možné najít v JNLP deskriptoru šifrovací utility (soubor mf_client.jnlp). V současné verzi aplikace jde o tyto URL:

http://www.mfcr.cz/sys/iissp/kvsclient/KVSClient_signed.jar
http://www.mfcr.cz/sys/iissp/kvsclient/KVSCommon_signed.jar
http://www.mfcr.cz/sys/iissp/kvsclient/xalan.jar
http://www.mfcr.cz/sys/iissp/kvsclient/log4j-1.2.8.jar
http://www.mfcr.cz/sys/iissp/kvsclient/bcprov-jdk16-144.jar
http://www.mfcr.cz/sys/iissp/kvsclient/bcmail-jdk16-144.jar
http://www.mfcr.cz/sys/iissp/kvsclient/xmlsec-1.4.3.jar
http://www.mfcr.cz/sys/iissp/kvsclient/commons-logging.jar
http://www.mfcr.cz/sys/iissp/kvsclient/serializer.jar
http://www.mfcr.cz/sys/iissp/kvsclient/forms.jar
http://www.mfcr.cz/sys/iissp/kvsclient/looks.jar

V těchto JAR souborech se nalézá kompletní funkcionalita aplikace Šifrovací utilita včetně kódů uvolněných v zdrojové podobě.

DOPORUČUJEME využít zveřejněné části zdrojového kódu jako základ pro vlastní vývoj, přičemž po začlenění kódu do vlastních produktů doporučujeme nadále pracovat s kódem jako s vlastním bez vazby na zdroj na stránkách MF ČR.

NEDOPORUČUJEME výše uvedené knihovny využívat jako základ pro vývoj vlastního řešení. Pro toto využití nejsou určeny a v budoucnu se bez upozornění může měnit rozhraní komponent, názvy JAR souborů a další vlastnosti, jejichž stabilita je nutná pro využití v produkčním systému.

KVS

Otázka č. 1/KVS:

Při odeslání šifrovaných dat dochází k chybě s kódem DECRYPT_FAILED.

Odpověď:
Ověřte, zda data, která zasíláte (base64) jsou dešifrovatelná pomocí Šifrovací utility. Pokud ano, ověřte, že nedochází k chybě při konstrukci SOAP zprávy. Ověřte, zda používáte správné identifikační údaje a správnou webovou službu (produkční vs. testovací).

Otázka č. 2/KVS:

Při odeslání šifrovaných dat dochází k chybě s kódem HMAC_VERIF_FAILED

Odpověď:
XML zpráva byla dešifrována, ale nepodařilo se ověřit integritu zprávy (identifikátor celistvosti). Důvodem může být např.: změna zprávy mezi generováním identifikátoru celistvosti a zašifrováním, nevhodně zvolené parametry identifikátoru celistvosti (Id, algoritmus), nesprávně vypočtený identifikátor celistvosti, nesprávné jmenné prostory apod. Jako test, zda je zpráva generována korektně lze využít Šifrovací utilitu a funkcionalitu dešifrování zprávy.

Otázka č. 3/KVS:

Při odeslání šifrovaných dat dochází k chybě s kódem: SIGN_VERIF_FAILED

Odpověď:
Dešifrování XML zprávy i ověření integrity zprávy (identifikátoru celistvosti) bylo úspěšné, ale některý z vnořených elektronických podpisů nebyl úspěšně ověřen.

Důvodem může být např.

- Změna podepsané části dokumentu (např. je podepsán celý dokument a byl přidán identifikátor celistvosti)
- Použití neplatného certifikátu (různé důvody neplatnosti)
- Použití certifikátu od nedůvěryhodné certifikační autority
- Chybný výpočet el. podpisu

Hlášení problémů

V následujících odstavcích najdete postup, jak nahlásit problém, na který jste narazili v šifrovací utilitě nebo při vývoji SW pro komunikaci s CSÚIS. Pokud nebude dodržena níže popsaná forma hlášení problému, vyřízení vašeho požadavku se zpomalí nebo muže být pro nedostatek údajů zamítnut.

Uživatel šifrovací utility

Pokud jste uživatelem šifrovací utility a při použití narazíte na problém, kontaktujte nejprve vašeho správce počítače, který by se měl i s využitím výše uvedených řešení nejčastějších problémů pokusit odstranit váš problém.
Pokud se nepodaří problém odstranit ani s odbornou pomocí a jste přesvědčeni, že se jedná o chybu Šifrovací utility, zašlete chybové hlášení na servicedesk@sd-stc.cz . Aby bylo vyřízení vašeho požadavku co nejefektivnější, zařaďte do hlášení následující údaje, které získáte s pomocí vašeho správce:

- Typ a verze operačního systému (např. Windows Vista Ultimate SP1 32 bit, česká verze)
- Typ a verzi Java prostředí (např. SUN Java v 1.6.0_17)
- Typ a verzi internetového prohlížeče (Firefox 3.5.7 nebo MS IE 8.0.601.18702)
- Snímek obrazovky problematické situace (pokud je dostupný)
- Kompletní záznam z Java konzole
- Detailní popis vyvolání chyby
- E-mail kontakt pro případné získání dalších informací

Vývoj třetích stran

Pokud při vývoji narazíte na problém, ověřili jste postupy popsané výše, pak je možné, že jste narazili na chybu aplikace.
V tomto případě zašlete chybové hlášení na servicedesk@sd-stc.cz . Chybové hlášení musí obsahovat následující údaje:

- Rozhraní, kterého se chyba týká - web aplikace nebo webservices rozhraní
- Určení, zda se požadavek týká produkčního nebo testovacího prostředí
    - U produkčního pak zadejte uživatelské přihlašovací jméno
- Datum a čas, kdy operace selhala (s přesností na minuty)
- Detailní popis, jak bylo chybné chování vyvoláno
- Pokud k chybě došlo při zpracování dat a nejde o data produkční, přiložte tato data k požadavku
- Web aplikace
    - Snímek obrazovky webové aplikace, pokud je k dispozici a nese informaci
- Webservices rozhraní
    - Vstupní SOAP zprávu a výstupní SOAP zprávu resp. HTTP odpověď (např. záznam komunikace pomocí nástroje SOPAUI,webscarab, burp)