Integrovaný informační systém Státní pokladny (IISSP)

Centrální systém účetních informací státu (CSÚIS)

Testování třetích stran

(Pracovní postup)

Obsah

Úvod

Účel testování

Testování třetích stran a související technické prostředky uvedené v dalším textu jsou určeny zástupcům účetních jednotek nebo softwarových společností a slouží k otestování schopnosti jejich software komunikovat se systémy CSÚIS. Testovací infrastruktura je volně dostupná všem a po účastnících nevyžaduje registraci ani povolení Ministerstva financí ČR.

Při testování budou ověřeny následující činnosti:

1. Schopnost účetní jednotky odeslat data pomocí webových služeb (v případě použití SOAP klienta), alternativně pomocí Webové aplikace
2. Ověření správnosti postupu použitého pro zašifrování zaslané zprávy (za použití testovacího šifrovacího klíče) dle Vyhlášky č. 383/2009 Sb. (Technická vyhláška) ve znění pozdějších předpisů
3. Ověření syntaktické správnosti zaslané zprávy na technické úrovni (kontrola XML dle definic)
4. Schopnost účetní jednotky přistupovat k inboxu pomocí webových služeb (v případě použití SOAP klienta), alternativně pomocí Webové aplikace umožňující stažení stavové zprávy o výsledku zpracování zaslaných dat

Při testování nebude kontrolována obsahová správnost zasílaných údajů (výkazů) ani oprávněnost použité zodpovědné osoby zasílat data za použitou účetní jednotku.

Organizační pokyny

Dostupnost testovací Webové aplikace a testovacího prostředí

Pro účely testování budou na webových stránkách CSÚIS administrátorem CSÚIS uveřejněna časová pásma, ve kterých budou přijímány testovací soubory. Mimo tato pásma není zaručena odpověď na testovací zprávu. Není-li na webových stránkách CSÚIS stanoveno jinak, je zajištěna dostupnost testovací Webové aplikace v pracovní dny od 8 – 17 hodin.

Frekvence zasílaných zpráv do testovacího provozu je omezena na jednu zprávu za minutu. Přístup k Webové aplikaci není omezen. Pro testování nebude poskytována telefonická podpora.

Na webových stránkách CSÚIS budou vždy uveřejněny aktuální informace o provozu či plánovaných odstávkách testovacího prostředí.

Přihlašovací údaje

Pro přihlášení k testovacímu komunikačnímu serveru, tj. testovací Webové aplikaci nebo testovacímu komunikačnímu kanálu SOAP pro volání webových služeb je nutné použít výhradně testovací přihlašovací údaje zveřejněné na webových stránkách CSÚIS:

Uživatelské jméno pro přihlášení: **`0010000050`**

Heslo pro přihlášení: **`nl7jbu5o`**

Tyto přihlašovací údaje jsou shodné pro testovací Webovou aplikaci i pro testovací komunikační kanál SOAP.

Testovací přihlašovací údaje nelze použít pro produktivní zasílání výkazů ani pro přihlášení k produktivnímu komunikačnímu serveru CSÚIS.

URL pro testování třetích stran:

Přístup k testovací Webové aplikaci pro testování třetích stran: https://portal5.statnipokladna.cz/csuis

Adresa webové služby (SOAP) pro zasílání výkazů: https://portal5.statnipokladna.cz/csuis/wstest/vykazy

Adresa webové služby (SOAP) pro přístup k inboxu: https://portal5.statnipokladna.cz/csuis/wstest/inbox

Poznámka: Výše uvedená URL testovacích webových služeb jsou rovněž uvedena ve WSDL souborech uveřejněných společně s XSD popisy zpráv.

Šifrovací klíče

Šifrovací klíče pro testovací provoz jsou zveřejněny administrátorem CSÚIS na webových stránkách CSÚIS v podobě balíku Zajišťovacích a identifikačních souborů (ZaIS) testovací zodpovědné osoby (ZO). Obsah šifrovacího klíče musí být před použitím nejprve dekódován. Tuto funkci poskytuje dále popsaná Šifrovací utilita.

Zajišťovací a identifkační soubory včetně šifrovacího klíče jsou dostupné na webových stránkách CSÚIS v souboru nazvaném „**ZaIS_0010000050.zip**“.

Pro dekódování ZaIS slouží následující dekódovací kód:

6604 7279 1985 2504 9275 8722 2182 5440 5117 6636 0008 7452 2868 4891 4716 4751

Bližší popis postupu pro dekódování ZaIS je uveden v uživatelské příručce Šifrovací utility, která byla na webu MF zveřejněna již dříve.

Proces testování

Pro účely testování je možné využít Šifrovací utilitu pro zašifrování dat a testovací Webovou aplikaci pro odeslání zprávy a přístup do Inboxu pro ověření výsledku zpracování testovací zprávy nebo přístup pomocí volání webových služeb.

U všech zaslaných zpráv je nutné uvádět jako IČ odesílatele (účetní jednotky) IČ organizace, která provádí testování nebo IČ účetní jednotky, v jejímž pověření je testování prováděno. Toto IČ je nutné uvádět na všech relevantních místech odesílané zprávy, tj. v komunikační obálce a v hlavičce výkazu. Pro zašifrování zpráv zasílaných do CSÚIS je nutné použít testovací šifrovací klíč zveřejněný k tomuto účelu na webových stránkách CSÚIS.

Pro testování bude vytvořen v testovací Webové aplikaci jeden univerzální inbox pro všechny Účetní jednotky (ÚJ). Z tohoto důvodu je nutné při přístupu do inboxu použít filtr zobrazení podle IČ organizace použitého v testovací zprávě. V inboxu bude po zpracování zprávy dostupná stavová zpráva s výsledky kontrol. Stavová zpráva o výsledku testu bude dostupná v univerzálním inboxu po dobu 24 hodin.

Předpokladem pro úspěšné testování je znalost Technického manuálu, který detailněji popisuje základní principy pro zasílání zpráv do CSÚIS a jejich kontroly.

Přehled odkazů

Hlavní stránka pro Státní pokladnu:	http://www.statnipokladna.cz
Webové stránky CSÚIS:	http://www.statnipokladna.cz/csuis
Technický manuál:	http://www.statnipokladna.cz/csuis/tech-manual
Webová aplikace:	http://www.statnipokladna.cz/csuis/webaplikace

Postup testování

Zjednodušený popis postupu testování

Při testování se typicky postupuje dle následujících kroků:

1. Stažení testovacího šifrovacího klíče z webových stránek CSÚIS. Šifrovací klíč je distribuován jako součást Zabezpečovacích a identifikačních souborů dle Vyhlášky č. 383/2009 Sb. (Technická vyhláška) ve znění pozdějších předpisů a Technického manuálu. Obsah šifrovacího klíče musí být před použitím nejprve dekódován. Tuto funkci poskytuje popsaná Šifrovací utilita.
2. Vytvoření výkazu ve formátu XML včetně komunikační obálky v podobě vyžadované vyhláškou č. 383/2009 Sb. (Technická vyhláška) ve znění pozdějších předpisů a Technickým manuálem. Jako IČ účetní jednotky musí být vyplněno IČ subjektu provádějícího testování, případně IČ účetní jednotky, v jejímž pověření je testování prováděno. Identifikátor zodpovědné osoby může být použit libovolný (odpovídající XML schematu).
3. Zašifrování zprávy testovacím šifrovacím klíčem pomocí Šifrovací utility nebo jiným způsobem dle požadavků Vyhlášky č. 383/2009 Sb. (Technická vyhláška) ve znění pozdějších předpisů.
4. Odeslání zašifrované zprávy pomocí Webové aplikace nebo SOAP komunikačního kanálu; k přihlášení ke komunikačnímu serveru je nutné použít přihlašovací údaje testovacího uživatele.
5. Po úspěšném odeslání zprávy je možné zkontrolovat výsledek zpracování v inboxu. Přístup do inboxu je možný po přihlášení testovacím uživatelem do Webové aplikace nebo za použití webových služeb. V zobrazení seznamu zpráv v inboxu je nutné zadat do filtru účetní jednotky použitou hodnotu IČ. Zprávy v inboxu jsou dostupné po dobu 24 hodin.

V následujících kapitolách jsou jednotlivé činnosti prováděné pro testování podrobně popsány.

Příprava dat

- ÚJ připraví data pro zvolený výkaz (např. Rozvahu) dle vzoru ve Vyhlášce č. 410/2009 Sb. ve znění pozdějších předpisů.
- ÚJ (ZO/NZO) připraví podle postupů v Technickém manuálu soubor pro zaslání dat do CSÚIS (podle aktuálních uveřejněných XSD schémat).

Příslušné dokumenty jsou zveřejněny na adrese:

http://www.statnipokladna.cz/csuis

Postup při vytváření datové zprávy

V následujících bodech je uveden proces při vytváření datové zprávy, která má být ÚJ zaslána do systému CSÚIS:

1. Vytvoření obsahu zprávy (účetní záznamy, finanční výkaz apod.) ve formátu XML, odpovídajícím příslušné definici XSD
2. Pokud je to relevantní, je nutné zabezpečit účetní záznamy pomocí elektronického podpisu dle požadavků Zákona o účetnictví
3. Vytvoření obecné komunikační obálky a vyplnění identifikátorů zpráv a komunikujících subjektů (příjemce, odesílatel)
4. Vložení vytvořeného výkazu do těla připravené komunikační obálky
5. Vytvoření identifikátoru celistvosti obsahu zprávy a jeho vložení do komunikační obálky

6. Zašifrování celé zprávy, tj. komunikační obálky i v ní obsažených dat dle postupu definovaného Vyhláškou č. 383/2009 Sb. (Technická vyhláška) ve znění pozdějších předpisů – viz následující kapitola.

Zašifrování zprávy

Přesný postup pro zašifrování zprávy je uveden ve vyhlášce č. 383/2009 Sb. (Technická vyhláška) ve znění pozdějších předpisů, v příloze číslo 6. Vstupem do šifrovacího procesu je tedy XML zpráva vytvořená dle popisu v kapitole Datové prvky a jejich struktura – XML dokument s kořenovým elementem Envelope (společná komunikační obálka) obsahující uvnitř elementu EnvelopeBody XML reprezentaci příslušného výkazu, účetního záznamu či jiného dokumentu a opatřená příslušnými bezpečnostními prvky v elementu EnvelopeFooter (identifikátor celistvosti, elektronický podpis).

K zašifrování zprávy lze použít Šifrovací utilitu poskytovanou Ministerstvem financí (viz Použití Šifrovací utility).

Tvorba identifikátoru celistvosti

Vzhledem k tomu, že identifikátor celistvosti má prokazovat, že data nebyla přenosem změněna či poškozena, je potřeba přesně definovat, z jakých dat a jakým způsobem se identifikátor vypočte. Vzhledem k povaze dat (XML) bude identifikátor celistvosti vytvořen pomocí postupů definovaných ve standardu XML Signature 1.1. Identifikátor celistvosti bude vytvořen ve formě elementu Signature s využitím mechanizmu HMAC-SHA256. Pro výpočet HMAC nebude použit utajený klíč a identifikátor celistvosti tak nebude sloužit k autentizaci. Jako hodnota klíče pro HMAC bude použito 32 nulových bajtů.

K zašifrování zprávy a vytvoření identifikátoru celistvosti lze použít Šifrovací utilitu poskytovanou Ministerstvem financí (viz Použití Šifrovací utility).

Použití Šifrovací utility

Ministerstvo financí zpřístupňuje Šifrovací utilitu, kterou je možno použít pro zašifrování připravené zprávy ve formátu XML dle požadavků Vyhlášky 383/2009 Sb. (Technické vyhlášky) ve znění pozdějších předpisů. Při zašifrování bude zpráva rovněž opatřena vyžadovaným identifikátorem celistvosti. Zároveň umožňuje Šifrovací utilita dekódování testovacích Zajišťovacích a identifikačních souborů uveřejněných pro účely testování na webových stránkách CSÚIS.

Ministerstvo financí poskytuje Šifrovací utilitu ve formě instalačního balíčku Java WebStart aplikace včetně uživatelského manuálu. Dále se pro dodavatele, kteří chtějí využít zdrojové kódy Šifrovací utility ve svých aplikacích, se zveřejňují podklady - zdrojové kódy aplikace a dokumentace API ve formátu javadoc (ZIP).

Podrobné informace o Šifrovací utilitě včetně uživatelské příručky jsou na adrese:

http://www.statnipokladna.cz/cs/CSUIS-Sifrovaci-utilita.html

Odeslání zprávy pomocí Webové aplikace

Účelem specializované Webové aplikace pro komunikaci s CSÚIS je umožnit účetním jednotkám (ÚJ), respektive zodpovědné osobě (ZO), která je zastupuje dle Vyhlášky č. 383/2009 Sb. (Technická vyhláška) ve znění pozdějších předpisů, obousměrně komunikovat se systémy CSÚIS bez nutnosti úprav lokálního software účetní jednotky pro automatizovanou komunikaci.

Pro testování ÚJ převezme na stránkách CSÚIS informace (uvedené výše) vyžadované pro zaslání testovací zprávy:

- URL testovací Webové aplikace
- Uživatelské jméno pro přihlášení
- Heslo pro přihlášení
- Šifrovací klíč

Uvedené přístupové kódy jsou univerzální a jsou pro všechny účetní jednotky totožné.

Před započetím práce s testovací Webovou aplikací se uživatel musí k serveru přihlásit uživatelským jménem a heslem testovací ZO (testovacího uživatele).

Testovací Webová aplikace nevyžaduje na straně klienta instalaci žádných dodatečných programů nebo speciálních nastavení. Ke svému běhu potřebuje pouze běžný webový prohlížeč se zapnutou podporou cookies. Webovou aplikaci je možné provozovat na systémech s prohlížečem Internet Explorer 6 a vyšší, Mozilla Firefox 3.0 a vyšší nebo Safari 3.0 a vyšší.

Uživatelská dokumentace k Webové aplikaci (tedy i k testovací Webové aplikaci) je na adrese:

http://www.statnipokladna.cz/csuis/webaplikace

Přístup k testovací Webové aplikaci je na adrese:

https://portal5.statnipokladna.cz/csuis

Přístup k Webové aplikaci

Při přístupu na server testovací Webové aplikace https://portal4.statnipokladna.cz/může prohlížeč zobrazit varování o nedůvěryhodném certifikátu serveru. Důvodem je to, že vydavatel serverového certifikátu - První certifikační autorita, a.s. - není pro prohlížeč uživatele důvěryhodným vydavatelem certifikátů. Defaultní instalace prohlížečů obsahují certifikáty sady světových certifikačních autorit, mezi nimiž ovšem není zastoupena žádná certifikační autorita z České republiky.

Při první návštěvě, resp. před první návštěvou je tedy vhodné nainstalovat certifikát vydavatele (takzvaný kořenový certifikát) do prohlížeče.

Kořenové certifikáty I.CA jsou ke stažení zde:

http://www.ica.cz/cz/menu/112/prace-s-certifikaty/korenove-certifikaty-i-ca-sha-2/

Instalace proběhne pouhým kliknutím na odkaz s certifikátem a je okamžitá.

Bližší popis o účelu kořenového certifikátu je uveden zde:
http://www.ica.cz/cz/menu/7/casto-kladene-otazky/clanek-90-k-cemu-slouzi-korenovy-certifikat-nebo-li-tzv-certifikat-certifikacni-autority-quot-/

Účelem kořenového certifikátu je "důvěryhodným způsobem" potvrdit uživateli, že server, s nímž komunikuje pomocí zabezpečeného přenosu, je skutečně tím, za koho se vydává.
Neexistence kořenového certifikátu certifikační autority na počítači uživatele neznamená žádnou bezpečnostní hrozbu; prohlížeč v tomto případě pouze zobrazí varování a umožní uživateli další práci se zabezpečenými stránkami. Úroveň zabezpečení je vždy stejně vysoká.

Odeslání zprávy pomocí webových služeb

K odeslání zprávy do CSÚIS je rovněž možné použít rozhraní webových služeb SOAP protokolem. Informace o rozhraní jsou popsané v souboru csuis.wsdl uveřejněném společně s XSD definicemi zpráv na webových stránkách CSÚIS. K odeslání na testovací komunikační server je nutné použít správné URL, ve WSDL definici označené jako testovací port ENCRYPTED_MESSAGE_Test_Port.

URL pro zasílání testovacích zpráv je následující:

https://portal5.statnipokladna.cz/csuis/wstest/vykazy
Uvedené volání vyžaduje standardní Basic autentizaci pomocí zveřejněných přihlašovacích údajů testovacího uživatele.

Převzetí výsledku

Výsledek o testu obdrží ÚJ do univerzálního inboxu, který je přístupný opět pomocí webových služeb nebo Webové aplikace. Pro zobrazení relevantní zpráv je nutné přihlásit se pomocí zveřejněných přístupových údajů testovací ZO a v inboxu zobrazeném Webovou aplikací vyfiltrovat pouze zprávy určené pro použité IČ účetní jednotky. Stavové zprávy v testovacím inboxu jsou dostupné pouze po dobu 24 hodin.

Text stavové zprávy obsahuje informace o průběhu jejího zpracování a výpisy případnych chybových nebo informačních hlášení.

K přístupu do univerzálního inboxu je rovněž možné použít rozhraní webových služeb SOAP protokolem. Informace o tombo rozhraní jsou popsané v souboru inbox.wsdl uveřejněném společně s XSD definicemi zpráv na webových stránkách CSÚIS. K odeslání na testovací komunikační server je nutné použít správné url, ve WSDL definici je označené jako testovací port INBOX_ENVELOPE_Test_Port.

URL pro přístup k testovacímu univerzálnímu inboxu je následující:

https://portal5.statnipokladna.cz/csuis/wstest/inbox
Uvedené volání vyžaduje standardní Basic autentizaci pomocí zveřejněných přihlašovacích údajů testovacího uživatele.