Vybrané technické informace pro předávání účetních záznamů do centrálního systému účetních informací státu

verze k 30.10.2009

OBSAH:

A. Datové prvky a jejich struktura

Komunikační obálka

Význam komunikační obálky

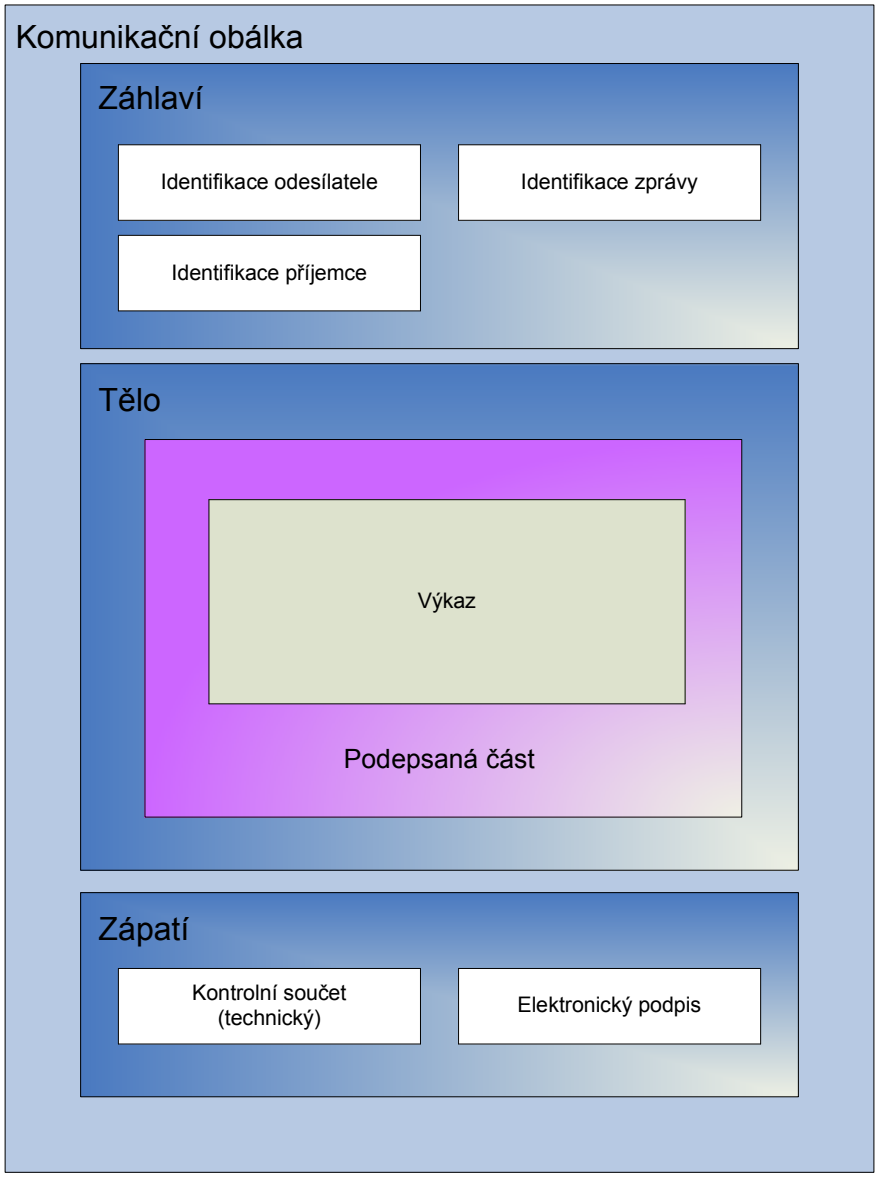
Všechny zprávy vyměňované mezi ÚJ a CSÚIS mají shodnou strukturu. Ta sestává ze společné komunikační obálky a kontextově závislého obsahu. Komunikační obálka je vytvořena s ohledem na obecné použití v rámci celého systému IISSP Ministerstva financí ČR.

Komunikační obálka obsahuje mimo jiné jednotné identifikační a bezpečnostní mechanizmy, které bylo vhodné implementovat pro obecné řešení komunikace s IISSP.

Před přenosem komunikačním kanálem mezi UJ a CSÚIS je vyžadováno, aby byla zpráva zašifrována, pokud není stanoveno jinak. Dle požadavků specifikovaných v Technické vyhlášce je v tomto případě zašifrována celá komunikační obálka včetně vložené zprávy.

Struktura komunikační obálky

Následující diagram přibližuje strukturu komunikační obálky.



Obsahem komunikační obálky jsou tyto části:

1. Záhlaví (EnvelopeHeader) – Identifikační údaje o odesílateli a příjemci zprávy, identifikace zprávy
2. Tělo (EnvelopeBody) – Vlastní datový obsah, tj. konkrétní datová zpráva (např. rozvaha, finanční výkaz apod.)
3. Zápatí (EnvelopeFooter) – Technické a zabezpečovací údaje: identifikátor celistvosti zprávy, elektronický podpis

Identifikátory

Všechny identifikátory týkající se zprávy a partnerů komunikace jsou obsaženy v záhlaví komunikační obálky. Povinnost jednotlivých elementů je dána XML schema definicí. U identifikace ÚJ a ZO doporučujeme uvádět i nepovinné položky, zejména kontaktní informace.

Identifikátor přenosu

U přenosu zpráv je vyžadováno uvedení identifikace přenosu, tzv. Transaction Id. Tato identifikace je generována odesílatelem a musí být *jedinečná pro každou zprávu* odeslanou danou ÚJ. Pro jednoznačný identifikátor přenosu doporučujeme použít tzv. GUID – globálně unikátní identifkátor ve tvaru hexadecimálního čísla o délce 32 znaků.

Identifikace ÚJ

Účetní jednotka je pro potřeby komunikace s CSÚIS jednoznačně identifikována svým přiděleným Identifikačním číslem (IČ). Nemá-li komunikující subjekt přidělen identifikátor IČ, nebo je-li to v odůvodněných případech vyžádáno správcem CSÚIS, může účetní jednotka pro svou identifikaci v hlavičce zprávy použít alternativní identifikátor SubjectId přidělený správcem CSÚIS.

Kromě tohoto údaje je potřeba v záhlaví uvést rovněž název a sídlo ÚJ.

Identifikace ZO

ZO je pro potřeby komunikace s CSÚIS jednoznačně identifikován numerickým ID přiděleným CSÚIS.

Kromě tohoto údaje je potřeba v záhlaví uvést rovněž plné jméno a kontaktní informace ZO, především platnou emailovou adresu ZO.

Identifikace CSÚIS

Pro potřeby odesílání zpráv z UJ do CSÚIS musí být v záhlaví zprávy subjekt CSÚIS identifikován jako příjemce následujícím způsobem:

```
<iissp:Recipient>
       <iissp:SubjectId>1</iissp:SubjectId>
       <iissp:SubjectName>Ministerstvo financí ČR</iissp:SubjectName>
       <iissp:Module>CSÚIS</iissp:Module>
</iissp:Recipient>
```

Tělo zprávy

Aplikační data jsou přenášená ve vnořené struktuře elementu EnvelopeBody. Dle typu přenášených dat obsahuje tento element vždy jeden specifický element se strukturou potřebnou k přenesení dané informace.

Dle typu je možné zprávy rozdělit na:

- Datové zprávy – nesoucí obchodní data (účetní záznamy, finanční výkazy apod.)
- Stavové zprávy – předání informace o stavu zpracování Účetní jednotce
- Žádost o data - vyžádání jiných účetních záznamů od Účetní jednotky

Ukázka záhlaví

Příklad záhlaví zprávy:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<msg:Envelope xmlns:cus="http://mfcr.cz/iissp/cus/v1.0"
       xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:iissp="http://mfcr.cz/iissp/common/v1.0"
xmlns:msg="http://mfcr.cz/iissp/messaging/v1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://mfcr.cz/iissp/messaging/v1.0 iissp_messaging.xsd ">

<msg:EnvelopeHeader>
       <!-- Záhlaví zprávy -->
       <iissp:TransactionId>A970E763D149462BB1EBB0E7831996DB</iissp:TransactionId>
       <msg:DateTimeCreated>2009-09-17T13:03:42</msg:DateTimeCreated>
              <iissp:Sender>
                     <iissp:IC>0000075370</iissp:IC>
                     <iissp:SubjectName>Obecní úřad Plzeň</iissp:SubjectName>
                     <iissp:ResponsiblePerson>
                            <iissp:PersonName>Jan Novák</iissp:PersonName>
                            <iissp:Email>novak@plzen.cz</iissp:Email>
                            <iissp:UserId>99010101</iissp:UserId>
                            <iissp:PhoneNumber>337900900</iissp:PhoneNumber>
                     </iissp:ResponsiblePerson>
              </iissp:Sender>
              <iissp:Recipient>
                     <iissp:SubjectId>1</iissp:SubjectId>
                     <iissp:SubjectName>Ministerstvo financí ČR</iissp:SubjectName>
                     <iissp:Module>CSÚIS</iissp:Module>
              </iissp:Recipient>
</msg:EnvelopeHeader>

<msg:EnvelopeBody>
              <cus:Message xmlns:cus="http://mfcr.cz/iissp/cus/v1.0">
              <!-- Data zprávy -->
              </cus:Message>
</msg:EnvelopeBody>

<msg:EnvelopeFooter>
              <!-- Data zápatí -->
</msg:EnvelopeFooter>

</msg:Envelope>
```

Definice jednotlivých zpráv

Strukura každého vnořeného typu zprávy je popsána odpovídajícím XML schématem (soubor XSD) dle následující tabulky. Základním schematem popisujícím komunikační obálku včetně vnořených elementů je pak soubor iissp_messaging.xsd.

V některých případech jsou struktury jednotlivých výkazů rozlišeny podle typu reportující organizace. V tomto případě se používá následujících zkratek:

OSS	Organizační složka státu
SF	Státní fond
PO	Příspěvková organizace
USC	Územní samosprávný celek

Zpráva	XML schéma
Rozvaha	CV1_Rozvaha_*.xsd[1]
Výkaz zisku a ztrát	CV2_Vysledovka_*.xsd[2]
Přehled o peněžních tocích a o změnách vlastního kapitálu	CV3_PenezniToky.xsd CV4_ZmenyVlastnihoKapitalu.xsd
Příloha	CV4_UcetniZaverkaPriloha.xsd
Pomocný konsolidační přehled k účetní závěrce	
Statistický přehled	
Výkaz majetku a závazků za dílčí konsolidační celek státu	
Výkaz nákladů a výnosů za dílčí konsolidační celek státu	
Výkaz peněžních toků za dílčí konsolidační celek státu	
Příloha účetního výkazu za dílčí konsolidační celek státu	
Pomocný konsolidační přehled za dílčí konsolidační celek státu	
Statistický přehled za dílčí konsolidační celek státu	
Vyžádaný primární účetní záznam z účetních knih	
Vyžádaný jiný účetní záznam	
Inventarizační zpráva	
Vyžádaný konkrétní účetní doklad	
Vyžádaný seznam primárních účetních záznamů a účetních dokladů dle bližší specifikace	

[1] Dle typu organizace (OSS, SF, PO, USC)

[2] Dle typu organizace (OSS, SF, PO, USC)

Soupis pohledávek	CV18_SoupisPohledavek.xsd
Soupis závazků	CV19_SoupisZavazku.xsd
Soupis podmíněných závazků	CV20_SoupisPodminenychPohledavek.xsd
Peněžní prostředky	CV21_SoupisPodminenychZavazku.xsd
Krátkodobý finanční majetek	CV22_SoupisPeneznichProstredku.xsd
Žádost o data	ZadostZaznamUcetni.xsd
Stavová zpráva	iissp_messaging.xsd
Práce se schránkou (výpis a stažení zpráv)	iissp_messaging.xsd

Tab1. XSD schémata jednotlivých zpráv

Kromě těchto souborů s XSD definicemi je potřeba k vytvoření zpráv pro potřeby CSÚIS použití XML Schema sdílených prvků. Jedná se především o datové typy standardizovaného slovníku datových prvků Informačních systémů ve státní správě (ISDP) vytvořeného Ministerstvem informatiky a nyní ve správě Ministerstva vnitra. Tento slovník obsahuje definice základních datových typů používaných ve všech referenčních rozhraních veřejné správy v České republice – viz https://www.sluzby-isvs.cz/ISDP.

Další skupinou jsou sdílené definice datových prvků vytvořených pro technické a komunikační potřeby CSÚIS, resp. IISSP. Tyto XSD soubory jsou pojmenovány iissp_*.xsd

Aktuální verze všech těchto XSD souborů jsou přílohou tohoto dokumentu. Jejich verze v elektronické podobě je rovněž udržována a přístupná na webových stránkách Ministerstva financí ČR.

Použití XML formátu a připojených XML schema definic umožňuje snadnou kontrolu správnosti syntaxe dat. Tato kontrola je prováděna jako součást kontroly vstupu dat do CSÚIS. Je však žádoucí, aby před zasláním dat do CSÚIS provedla tuto syntaktickou kontrolu i samotná ÚJ a předešla tak chybám zabraňujícím převzetí dat v CSÚIS. Další informace o těchto kontrolách jsou uvedeny v kapitole **Error! Reference source not found.**.

Hlavička účetního záznamu

Všechny zprávy odpovídající jednotlivým typům účetních záznamů obsahují hlavičku výkazu (element VykazHlavicka) s obvyklými informacemi o sestavení výkazu a jeho původci. Hlavička je společná pro všechny typy účetních záznamů.

Rozvaha

Kořenovým elementem tohoto ÚZ je RozvahaOSS, RozvahaPO, RozvahaSF, RozvahaUSC (dle typu subjektu). Tento element obsahuje podelement VykazHlavicka a dale již elementy Aktiva a Pasiva (názvy elementů) obsahující samotné účetní informace.

Další členění elementů Aktiva a Pasiva je dle jednotlivých „ukazatelů“ (sloupců výkazu) na Období běžné brutto, Období běžné korekce, Období běžné netto, Období minulé pro které existují odpovídající

podelementy. Tyto se dále člení na elementy jednotlivých položek (řádků) účetního záznamu které již přenáší svoji hodnotou hodnoty jim nadřazených ukazatelů a jsou definovány i ve slovnících ISDP.

Výkaz zisků a ztrát

Kořenovým elementem tohoto ÚZ je VykazZiskuAztratOSS, VykazZiskuAztratPO, VykazZiskuAztratSF, VykazZiskuAztratUSC. Tento element obsahuje podelement VykazHlavicka a dale již elementy Naklady a Vynosy (názvy elementů) obsahující samotné účetní informace.

Další členění elementů Aktiva a Pasiva je dle jednotlivých „ukazatelů" (sloupců výkazu) na Období běžné činnost hlavní, Období běžné činnost hospodářská, Období minulé činnost hlavní, Období minulé činnost hospodářská, pro které existují odpovídající podelementy. Tyto se dále člení na elementy jednotlivých položek (řádků) účetního záznamu které již přenáší svoji hodnotou hodnoty jim nadřazených ukazatelů a jsou definovány i ve slovnících ISDP.

Přehled o peněžních tocích a o změnách vlastního kapitálu

Kořenovým elementem tohoto ÚZ je PenezniToky. Tento element obsahuje podelement VykazHlavicka a dale element Vykaz obsahující samotné účetní informace. Podelementy elementu Vykaz odpovídají jednotlivým položkám výkazu, přenáší svoji hodnotou požadované ukazatele a jsou definovány i ve slovnících ISDP.

Kořenovým elementem tohoto ÚZ je ZmenyVlastnihoKapitalu. Tento element obsahuje podelement VykazHlavicka a dale element Vykaz který se dále člení na ukazatele (sloupce výkazu) Období minulé, Stav zvýšení, Stav snížení, Období běžné, pro které existující odpovídající podelementy. Tyto se dále člení na elementy jednotlivých položek (řádků) účetního záznamu které již přenáší svoji hodnotou hodnoty jim nadřazených ukazatelů a jsou definovány i ve slovnících ISDP.

B. Komunikační rozhraní

Komunikační rozhraní CSÚIS je založeno na využívání otevřených standardů a je postaveno na bázi webových služeb. Veškerá data předávaná mezi účetní jednotkou a CSÚIS jsou vytvořena ve formátu XML. Struktura jednotlivých výkazů ve formátu XML je popsána výše.

Pro komunikaci účetních jednotek s CSÚIS je připraven SOAP komunikační kanál pro vytvoření rozhraní typu A2A (aplikace s aplikací). Detailní popis komunikačního kanálu a technické realizace komunikace je uveden v kapitole Komunikační protokoly.

Komunikace účetní jednotky směrem do CSÚIS probíhá formou zasílání zpráv přes komunikační kanál. Všechna data, jež CSÚIS zasílá účetní jednotce, jsou uložena v takzvané schránce ZO, která je přístupná voláním služeb stejného komunikačního kanálu CSÚIS. Systém CSÚIS tedy nenavazuje žádné spojení s libovolným systémem účetní jednotky.

Pro manuální komunikaci je vytvořeno uživatelské rozhraní v prostředí Webové aplikace, pomocí které lze zasílat připravená data do CSÚIS a rovněž přistupovat k datům (např. stavovým zprávám) uloženým ve schránce ZO. Bližší popis naleznete v kapitole Webová aplikace.

Realizace přenosů SOAP kanálem

V případě SOAP komunikačního kanálu je komunikace vždy iniciována (a řízena) stranou účetní jednotky (klient). Oproti tomu přenos dat je obousměrný, tj. tímto komunikačním kanálem mohou být data

přenášena jak z účetní jednotky do CSÚIS (typicky sběr účetních záznamů) tak obráceně (typicky stažení číselníku, stavové zprávy, požadavku na data z CSÚIS). Podle požadovaného směru toku dat jsou tedy tato přenášena v zprávě typu SOAP:request nebo SOAP:respons. V případě přenosu dat v SOAP:respons pak hovoříme o synchronním komunikačním scénáři.

Přenos zpráv (účetních záznamů) do CSÚIS

Zprávy z ÚJ do CSÚIS jsou přenášeny vždy asynchronně. To znamená, že klient (ÚJ) po odeslání dat pomocí SOAP komunikačního kanálu neobdrží okamžitou odpověď s výsledkem zpracování. Vzhledem k množství kontrol prováděných nad daty jsou všechny informace o výsledku zpracování vytvářeny jako tzv. stavové zprávy a zpřístupněny ÚJ, resp. ZO v její schránce.

Do CSÚIS se přenáší typy zpráv odpovídající výkazům uvedeným v kapitole

Popis scénáře:

- Zašifrovaná zpráva je odeslána účetní jednotkou pomocí protokolu SOAP (tj. v SOAP obálce) na komunikační server CSÚIS
- Komunikační server provede bezpečnostní a syntaktické kontroly a předá zprávu ke zpracování obsahových kontrol
- Podle výsledku kontrol je vytvořena ve schránce ZO stavová zpráva informující odesílatele o úspěšném či neúspěšném přijetí zprávy ke zpracování
- Při ukončení obsahových kontrol a zpracování zaslaných dat je opět vytvořena stavová zpráva o výsledku zpracování, která je uložena ve schránce ZO
- ÚJ, resp. ZO se výpisem zpráv ze své schránky může přesvědčit o výsledku zpracování a případných chybách

Stažení zpráv z CSÚIS

Tento scénář slouží pro přenos zpráv typu Stavová zpráva a dalších požadavků směrem z CSÚIS do účetní jednotky. Veškerá komunikace tímto směrem probíhá přes tzv. schránku ZO. Veškeré zprávy určené pro ZO jsou uloženy na komunikačním serveru. ZO se pomocí SOAP komunikačního kanálu může dotázat na seznam zpráv čekajících ve schránce a vybranou zprávu si stáhnout.

Jedná se o synchronní scénář kdy ZO odešle zprávu typu žádost o výpis zpráv ve schránce nebo žádost o download dat ze schránky a v synchronní odpovědi obdrží od komunikačního serveru odpověď. Konkrétně se jedná o následující typy zpráv:

- Seznam zpráv ve schránce ZO a jejich identifikace
- Obsah konkrétní zprávy z inboxu

Veškeré zprávy pro komunikaci se schránkou ZO nebo odpovědi komunikačního serveru obsahují komunikační obálku, uvnitř které je vložena příslušná zpráva. Dle typu zprávy a požadavcích na její zabezpečení bude stažená zpráva zašifrována dle požadavků Technické vyhlášky.

V případě chyby při zpracování žádosti obdrží klient standardním způsobem chybovou zprávu (SOAP Fault).

Výpis seznamu zpráv ve schránce

K výpisu seznamu zpráv ve schránce je třeba použít zprávu SeznamZpravPozadavek definovanou v souboru iissp_messaging.xsd.

Stažení zprávy ze schránky

Ke stažení vybrané zprávy ze schránky je potřeba použít zprávu SeznamZpravVypis definovanou v souboru iissp_messaging.xsd.

Webová aplikace

Pro zasílání zpráv do CSÚIS nebo pro přístup ZO do schránky k získání výpisu uložených zpráv nebo jejich stažení je rovněž možné využít uživatelské rozhraní webové aplikace. Bližší informace jsou uvedeny v kapitole Webová aplikace.

C. Způsob hlášení závad datových přenosů

D. Metodika provádění přenosů dat

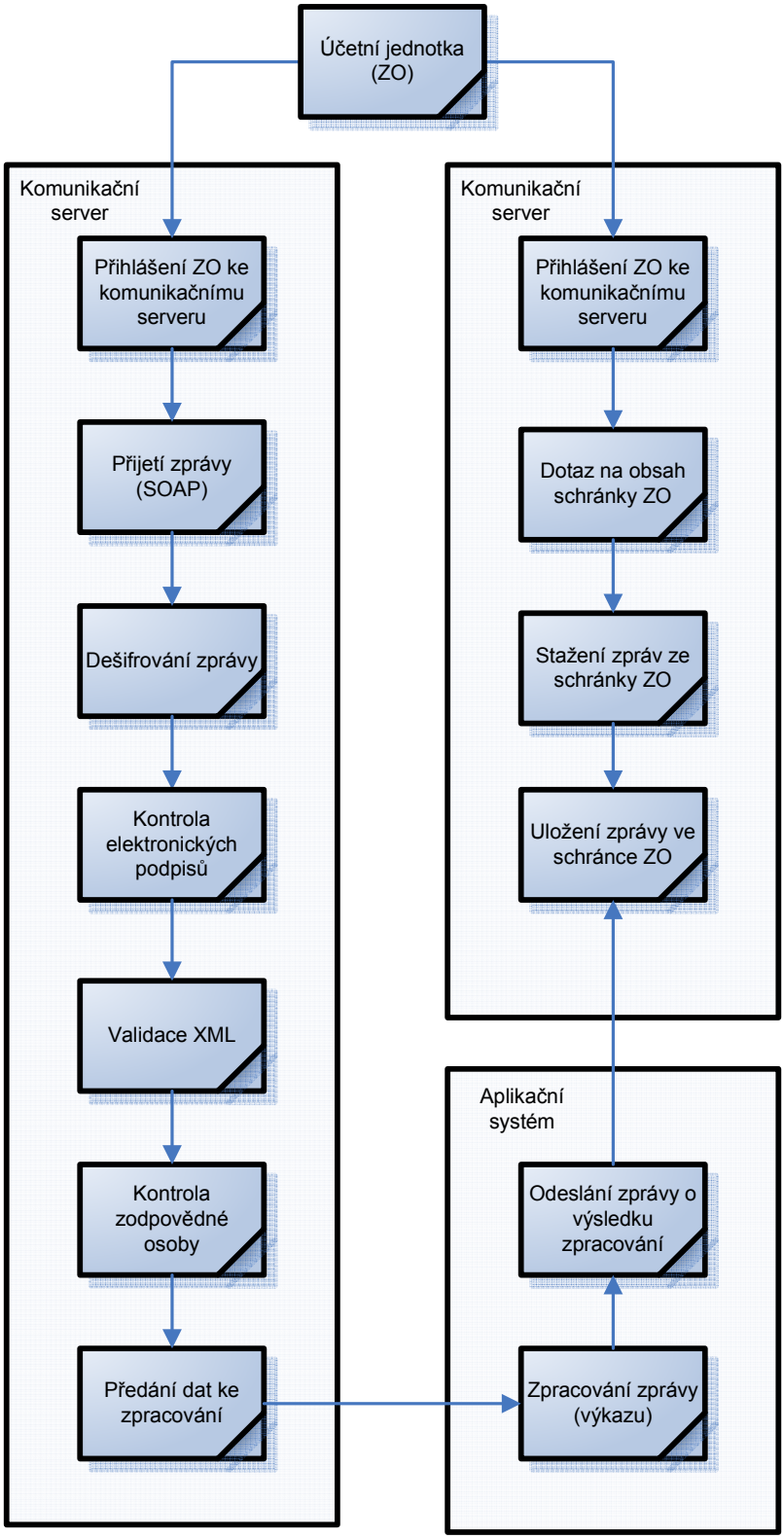
Účetní jednotka zasílá do CSÚIS požadované informace dle termínů stanovených Technickou vyhláškou v přílohách č.4, 5, 6 a 16.

Účetní jednotka předává data do CSÚIS co nejdříve po jejich sestavení, aby bylo možné případné opravy resp. opakované přenosy provést ještě v předepsaném termínu.

Při opakovaném přenosu či jakémkoliv vícenásobném zaslání dat (typu UZ k danému datu/období) se jako platná zpráva bere poslední předaná zpráva obsahující očekávaný výkaz. Předchozí zprávy nebudou systémem dále zpracovávány, a to bez ohledu na výsledky obsahových kontrol poslední zaslané zprávy.

Zpráva je předána ke zpracování, tj. k obsahovým kontrolám pouze při úspěšném dokončení všech kontrol zabezpečení a syntaxe. Výkaz neodpovídající svým zabezpečením a syntaxí požadavkům CSÚIS je systémem brána jako nedoručená – tj. zaslání výkazu s nesprávnou strukturou nebo zabezpečením je chápáno stejně jako nedoručení výkazu.

Popis procesu pro přenos dat z ÚJ do CSÚIS a obráceně je obsahem následujícího diagramu. Při komunikaci z CSÚIS směrem do ÚJ se ovšem nenavazuje přímé spojení ze strany CSÚIS do ÚJ, ale zpráva je pouze uložena v takzvané schránce ZO na komunikačním serveru CSÚIS. ZO musí iniciovat spojení s komunikačním serverem ke stažení připravených zprávy ze schránky CSÚIS.


Účetní jednotka (ZO)
Komunikační server
Přihlášení ZO ke komunikačnímu serveru
Přijetí zprávy (SOAP)
Dešifrování zprávy
Kontrola elektronických podpisů
Validace XML
Kontrola zodpovědné osoby
Předání dat ke zpracování
Komunikační server
Přihlášení ZO ke komunikačnímu serveru
Dotaz na obsah schránky ZO
Stažení zpráv ze schránky ZO
Uložení zprávy ve schránce ZO
Aplikační systém
Odeslání zprávy o výsledku zpracování
Zpracování zprávy (výkazu)

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 (např. rozvaha, výkaz zisku a ztrát)
2. Pokud je relevantní, zabezpečení účetních záznamů 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 Technickou vyhláškou

Takto vytvořená zpráva bude následně vložena do SOAP obálky dle WSDL definice webové služby a zaslána pomocí protokolu SOAP na komunikační server CSÚIS – viz kapitola SOAP komunikace.

E. Rejstříky a číselníky

F. Parametry zabezpečení a šifrování

Zprávy přenášené mezi ÚJ a CSÚIS musí být zašifrovány symetrickou šifrou Rijndael s délkou klíče 256 bitů. Konkrétní specifikace šifrování a odkaz na použitou dokumentaci jsou obsahem přílohy číslo 10 Technické vyhlášky. Šifrování není použito pouze v případě následujících druhů zpráv zasílaných z CSÚIS účetní jednotce:

- stavová zpráva o zpracování účetního či finančního výkazu nebo jiného dokumentu
- veřejně distribuovaný číselník

Všechny zprávy, které účetní jednotka zasílá do CSÚIS musejí být šifrovány.

Proces zašifrování a dešifrování dat je podrobně popsán v příloze číslo 7 Technické vyhlášky.

Kromě zabezpečení zpráv jejich předáváním v zašifrovaném tvaru je zabezpečen i přenosový kanál SOAP pomocí SSL použitím transportního protokolu HTTPS.

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.

Vložená XML signatura může vypadat například takto (použité transformace a algoritmy jsou závazné):

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
       <SignedInfo>
              <CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
              <SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#hmac-sha256">
<HMACOutputLength>256</HMACOutputLength>
</SignatureMethod>
              <Reference URI="">
                     <Transforms>
                            <Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                            <Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
                     </Transforms>
                     <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                     <DigestValue>tvEZ/FYL87EFYgJAKSFDIMqnu6ZMurItSNBSn6QgwrM=</DigestValue>
              </Reference>
       </SignedInfo>
       <SignatureValue>JAKSFDIMqnu6ZMuJAKSFDIMqnu6ZMuJAKSFDIMqnu6ZMu=</SignatureValue>
</Signature>
```

Pro tvorbu XML podpisu jsou závazné následující algoritmy:

- Metoda kanonikalizace: **http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments**
- Algoritmus podpisu: **http://www.w3.org/2001/04/xmldsig-more#hmac-sha256**
- Reference
  - **URI=””** – celý aktuální XML dokument
  - Transformace 1 - **http://www.w3.org/2000/09/xmldsig#enveloped-signature**
  - Transformace 2 - **http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments**
  - DigestMethod – **http://www.w3.org/2001/04/xmlenc#sha256**

Zašifrování zprávy

Přesný postup pro zašifrování zprávy je uveden v Technické vyhlášce, příloze číslo 7. 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).

Všem komunikujícím subjektům bude na veřejných webových stránkách CSÚIS k dispozici nástroj pro zašifrování a dešifrování zprávy.

Dešifrování zprávy

Přesný postup pro dešifrování zprávy je uveden v Technické vyhlášce, příloze číslo 7. Výstupem po dešifrování je XML zpráva tvořená kořenovým elementem Envelope (společná komunikační obálka) obsahující data předávaná z CSÚIS.

Všem komunikujícím subjektům bude na veřejných webových stránkách CSÚIS k dispozici nástroj pro zašifrování a dešifrování zprávy.

G. Způsob a termíny předávání hesel a šifrovacích klíčů

Popis procesu je uveden v Technické vyhlášce, příloze číslo 7, 12 a 13.

H. Způsob tvorby osobních přístupových kódů a jejich předávání zodpovědným osobám a náhradním zodpovědným osobám

Popis procesu je uveden v Technické vyhlášce, příloze číslo 7, 12 a 13.

I. Kontroly předávaných dat

J. Obsahové kontroly konsolidačních účetních záznamů

K. Poskytování součinnosti při odstraňování chyb v přenášených účetních záznamech

L. Komunikační protokoly

SOAP komunikace

Pro komunikaci mezi ÚJ a CSÚIS je použit pro výměnu zpráv standard SOAP ve verzi 1.1. Definice standardu SOAP je uvedena například na adrese http://www.w3.org/TR/2000/NOTE-SOAP-20000508/.

Konkrétní data jsou přenášena standardním způsobem uvnitř elementu SOAP:Body dle přiložené WSDL definice. Ostatní nepovinné elementy SOAP obálky nebudou vyplňovány.

Formát SOAP volání

Předávání zpráv do CSÚIS je prováděno formou asynchronního volání webové služby. SOAP volání je prováděno zprávou, která má tyto části:

SOAP Header

Není využíván.

SOAP Body

V části Body budou přenášena vlastní data a to v elementu EncryptedMessage obsahujícím datovou zprávu (přenášené účetní záznamy a jiné informace, zabalené v přenosové XML obálce) po zašifrování a zakódování pomocí base64.

Ukázka SOAP zprávy – zaslání dat do CSÚIS

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:iissp="http://mfcr.cz/iissp/messaging/v1.0">
<SOAP:Body>
<iissp:EncryptedMessage>
  base64 zakódovaná zašifrovaná zpráva
</iissp:EncryptedMessage>
</SOAP:Body>
</SOAP:Envelope>
```

Pro přenos a zpracování všech typů zpráv je k dispozici webová služba XXX. WSDL popis této webové služby je součástí tohoto dokumentu a rovněž je dostupný na adrese URL.

Formáty SOAP odpovědi

Na zprávu zaslanou pomocí SOAP protokolu může komunikační server odpovědět následujícím způsobem:

- Zpráva v SOAP obálce obsahující aplikační odpověď – v případě úspěšného synchronního zpracování
- Zpráva obsahující práznou SOAP obálku – v případě úspěšného přijetí asynchronní zprávy; alternativně
- Prázdná odpověď s HTTP kódem 200 – v případě úspěšného přijetí asynchronní zprávy
- Zrpáva obsahující SOAP Fault element a HTTP kód 500 – v případě neúspěšného přijetí synchronní či asynchronní zprávy

Typy odpovědí odpovídají standardu SOAP 1.1.

Pravidla SOAP komunikace

Pro SOAP komunikaci s komunikačním serverem CSÚIS platí následující obecná pravidla:

1. Přenos se provádí na stanovenou URL adresu webové služby
2. Komunikace je vždy zahájena ze strany účetní jednotky
3. Komunikace mezi ÚJ a komunikačním serverem probíhá zabezpečeným kanálem HTTPS
4. Komunikaci provádí Zodpovědná osoba (ZO), která se musí ke komunikačnímu serveru přihlásit svým osobním přístupovým kódem (přiděleným jménem a heslem). K autentizaci je použita HTTP Basic autentizace
5. Přenos dat do CSÚIS je považován za úspěšný, pokud se vrátí odpověď ve validní struktuře, tj. element SOAP Body s aplikační odpovědí, případně prázdná odpověď s HTTP kódem 200 nebo prázdný element SOAP Body pro asynchronní volání. Návratový kód protokolu HTTP 5xx nebo výskyt elementu SOAP Fault je považován za chybu přenosu resp. nepřijetí zprávy ke zpracování (viz standard SOAP).

Webová aplikace

Jako alternativní způsob výměny zpráv mezi ÚJ a CSÚIS poskytuje IISSP webovou aplikaci poskytující uživatelské rozhraní pro manuální činnosti zasílání zpráv do CSÚIS, výpis zpráv ze schránky ZO či jejich download.

Použití webové aplikace se předpokládá u ÚJ, kde náklady na vytvoření integračních vazeb mezi aplikacemi by převýšily přínos resp. míru využití tohoto rozhraní.

Pro přihlášení k webové aplikaci použije ZO přidělené uživatelské jméno a heslo totožné s přístupovými údaji pro standardní komunikační kanál SOAP.

Webová aplikace je dostupná na URL adrese ...

Pro všechny druhy zpráv zasílaných pomocí webové aplikace platí stejná pravidla na obsah, formát a zabezpečení jako při použití přenosového komunikačního kanálu SOAP.

M. Oznamování závažných skutečností