Popis datové struktury souboru o čerpání z IISSP pro EIS prostřednictvím WS

Verze 2.2

EDS/SMVS

SYSCOM Software spol. s r.o.

Datum: 25. 2. 2014

Popis datové struktury souboru o čerpání z IISSP pro EIS Verze 2.2

Dokumentace EDS SMVS

Datum předání: elektronicky: **3. 3. 2014**

EZI:EDS /AN 18/2

Zpracovala: Bc. Martina Sovková
Grafická úprava: Alena Davidová

Rozdělovník:

Jan Zikl	MF
Martin Pejša	SSW

Pro tvorbu dokumentu byl použit textový editor Microsoft Word 2013

Obsah

1 Úvod

Dokument popisuje datovou strukturu souboru .xml, který je exportován z Evidenčního dotačního systému a ze systému Správa majetku ve vlastnictví státu (dále jen EDS/SMVS) a zasílán do Externích Informačních Systémů (dále jen EIS). V souboru budou zasílána data finančním čerpání akcí (projektů).

Datová struktura bude zcela jistě doplňována a upřesňována podle požadavků zadavatele, (tj. MF), které budou vyplývat zejména z pilotního provozu. Proto konečný popis datové struktury s daty o finančním čerpání akcí (projektů) pro externí informační systémy může vzniknout až po ukončení a vyhodnocení pilotního provozu.

Tento dokument nedefinuje XML schémata a XSLT šablony pro objekty popsané v kapitole 3. Specifikace datových objektů, XML schémata a šablony budou uloženy na adrese:

- http://xml.ssw.cz/eds/bankyCerpaniIISSP_v_1_0.xsd (schéma pro export dat o čerpání v bankovních ústavech z EDS/SMVS pro EIS)
- http://xml.ssw.cz/eds/bankyCerpaniIISSP.xslt (šablona pro export dat o čerpání v bankovních ústavech z EDS/SMVS pro EIS)
- http://xml.ssw.cz/eds/EDS_dataTypesIISSP.xsd (definice datových typů)

Šablony budou vytvořeny a předány po schválení této detailní analýzy.

Pokud je vydána nová verze tohoto dokumentu, jsou XML schémata a šablony pro novou verzi uložena na adrese http://xml.ssw.cz/eds/test/

- http://xml.ssw.cz/eds/test/bankyCerpaniIISSP_v_1_0.xsd (testovací schéma pro export dat o čerpání v bankovních ústavech z EDS a SMVS pro EIS)
- http://xml.ssw.cz/eds/test/bankyCerpaniIISSP.xslt (testovací šablona pro export dat o čerpání v bankovních ústavech z EDS/SMVS pro EIS)
- http://xml.ssw.cz/eds/test/EDS_dataTypesIISSSP.xsd (testovací definice datových typů)

Schémata a šablony jsou zde umístěny pro dobu, kdy stále platí původní verze dokumentu, ale je vydána nová verze, kterou je nutné zapracovat a otestovat její správnou funkčnost předtím, než bude spuštěna do ostrého provozu. Poté jsou tato schémata a šablony uloženy na adresu http://xml.ssw.cz/eds/ k danému datu, kdy se již používá nová verze čerpání v bankovních ústavech z EDS a SMVS pro EIS.

Tento dokument je členěn na následující kapitoly:

Úvod	Formuluje cíle řešení a definuje strukturu dokumentu
Způsob a principy předávání dat	Definuje a popisuje způsoby a principy předávání dat z EDS a SMVS externím informačním systémům o čerpání v bankovních ústavech.
Specifikace datových objektů	Definuje obsah, návaznosti a kontroly jednotlivých datových objektů, tvořící datovou strukturu:

2 Způsob a principy předávání dat

2.1 Přenosový formát dat

Navrhovaný přenosový formát dat především vychází z požadavku zadavatele na denní automatizované zasílání dat z EDS/SMVS do EIS. Z tohoto důvodu budou data mezi EDS/SMVS a EIS předávána ve formě XML struktur.

XML struktury musí být vytvořeny podle standardu XML 1.0, Second Edition. Přenášené XML struktury musí splňovat všechny požadavky standardu. XML soubor používá kódování UTF – 8.

2.2 Obsah dat

Vybrané údaje akcí (projektů) vystupujících z bankovního ústavu (např. ČNB a IISSP) **a vstupujících do EDS/SMVS.** Jedná se o údaje o čerpání (tj. skutečného proplacení) peněz na akcích (projektech).

Vystupující soubor bude vždy obsahovat veškeré údaje předávaných dat akcí (projektů), (podle níže uvedené datové struktury), které jsou v okamžiku tvorby souboru (exportu) v informačním systému EDS/SMVS k dispozici za **dané období**.

3 Základní přehled komunikace s EDS/SMVS

3.1 Obecný popis komunikace

Veškeré zprávy mezi externími informačními systémy integrovanými s EDS/SMVS (dále pouze EIS) a EDS/SMVS, které jsou v tomto dokumentu definovány, budou komunikovat jedním základním způsobem nebo doplňkovým:

- Na základě výměny zpráv mezi volajícím systémem (klientem, který vystupuje buď v roli odesílatele, nebo příjemce, dat) a systémem zprostředkujícího serveru (dále jen Proxy server). K volání je využito standardního protokolu SOAP (Simple Object Access Protocol), který umožňuje vzdálené volání procedur, také nazývané jako webové služby.
- Doplňkový způsob na základě výměny XML souborů mezi odesílatelem a příjemcem dat.
- Doplňkový způsob na základě výměny XML zpráv pomocí webových služeb, které jsou vystaveny jak na straně EDS/SMVS, tak i na straně EISů. Tato varianta ale předpokládá vystavení webové služby pro příjem na každé jednotlivé instanci systémů účastnící se integrace.

Detailní specifikaci SOAP protokolu je možné nalézt na http://www.w3.org/TR/soap/. Pro přenos dat mezi systémy bude využito verze protokolu SOAP 1.2.

3.2 Komunikace s použitím Proxy serveru

Komunikace nikdy neprobíhá přímo mezi EISem a EDS/SMVS, ale jako prostředník komunikace je použit Proxy server – server je umístěn v hostingovém centru a je viditelný prostřednictvím internetu pro všechny systémy integrace. Tím je vyřešena situace, kdy některý z EISů nemůže komunikovat se systémem EDS/SMVS přímo.

V tomto případě vystupuje Proxy server jako buffer zpráv, do kterého odesílatelé zprávy ukládají a příjemci si zprávy vyzvedávají. Komunikaci zahajuje vždy buď odesílatel, nebo příjemce, zpráv. Dále jsou na Proxy serveru vystaveny webové služby sloužící ke komunikaci s jednotlivými systémy integrace – jsou to jediné webové služby integrace, žádný z EISů a ani EDS/SMVS nemusí vystavovat vlastní webové služby.

Aplikační část Proxy serveru obsahuje minimum aplikační logiky – udržuje pouze jednotlivé uzly (systémy) integrace a k nim přiřazené otisky jejich klientského certifikátu – slouží pro identifikaci účastníka komunikace.

Dále udržuje zásobník zpráv (Buffer), do kterého ukládá doručené zprávy a jejich identifikaci – odesílatele, jeho systém, datum uložení, vnitřní identifikaci zprávy (např. kapitola a finanční místo, kterých se zpráva týká) a seznam příjemců, kteří si mohou danou zprávu vyzvednout. Uložené zprávy čísluje nepřetržitou řadou pro každý typ zprávy a příjemce. Naopak ze zásobníku vybírá zprávy podle požadavků systému příjemce (typ zprávy a číslo poslední přijaté zprávy daného typu) a vytvořený seznam zpráv zasílá jako odpověď na tento požadavek. Daný Uzel příjemce si nemůže vyzvednout zprávy, které nejsou určeny pro něho.

Během, nebo po ukončení, určitého vnitřního procesu v jednom ze systémů integrace, jehož logickou součástí je komunikace s jiným systémem integrace, vytvoří tento systém XML zprávu v předepsané struktuře a odešle ji na vstup Proxy serveru. Proxy server uloží zprávu do svého bufferu a čeká, dokud si ji nevyzvedne oprávněný příjemce zprávy. Příjemce zprávy vytvoří XML zprávu v předepsané struktuře, ve které uvede požadavek na odběr zpráv z Proxy serveru – stažení zprávy doposud příjemci nezaslaných. Proxy server na základě požadavku vybere požadované zprávy ze svého bufferu a zašle je v odpovědi volání příjemci.

Po zpracování dat na straně příjemce se tento příjemce stane odesílatelem zprávy s výsledkem zpracování (nebo případně dalšími daty) a v minulém kroku z odesílatele se stane příjemcem dat. Komunikace s vyměněnými rolemi pak již pokračuje podobně.

3.2.1 Zjednodušený popis postupu předání dat z jednoho systému do druhého

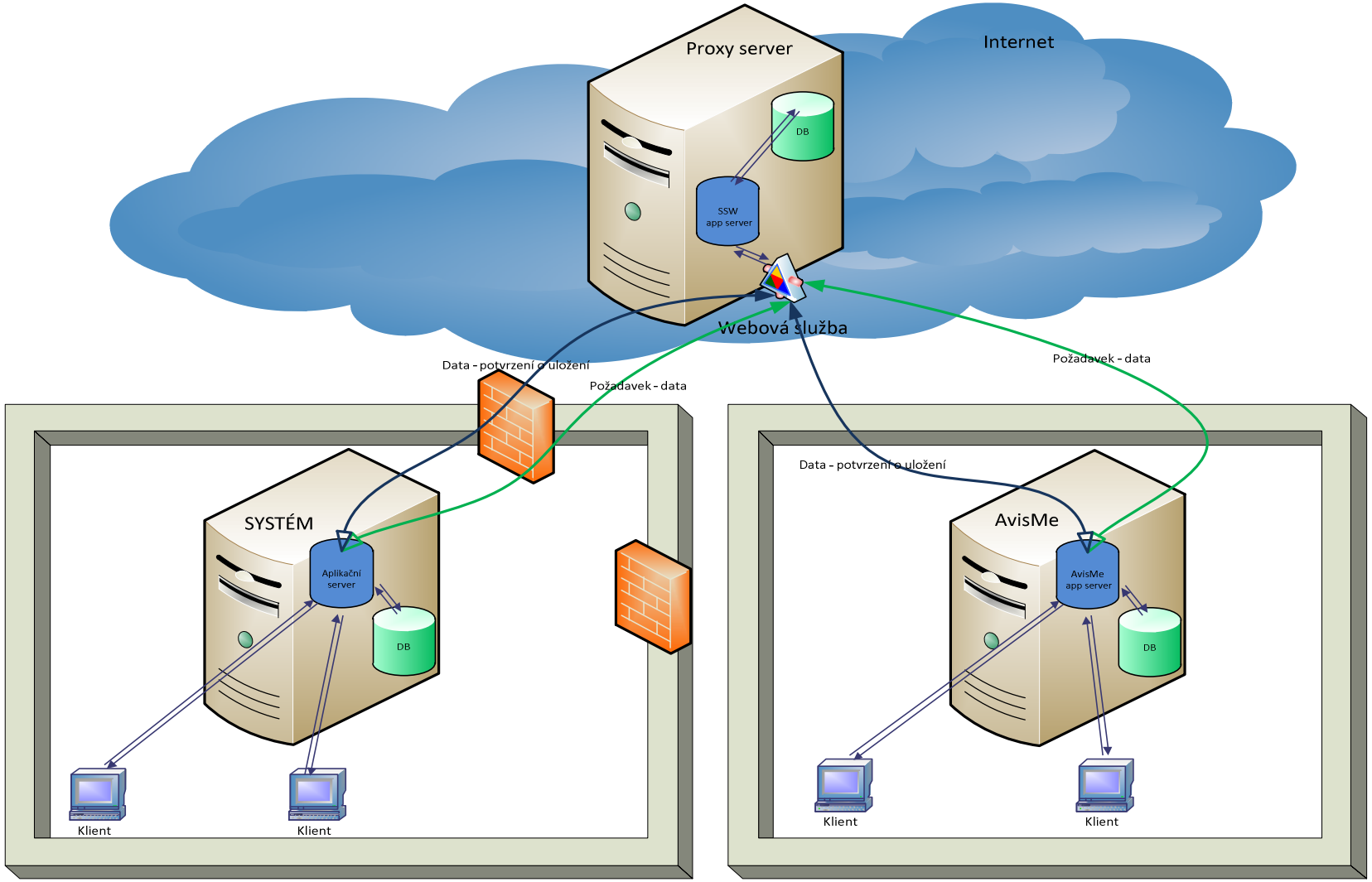
Odesílatel – EDS/SMVS /EIS/Systém	Událost v aplikaci EDS/SMVS/Sytému vyvolá požadavek na předání dat daného typu do druhého systému.
	Systém odesílatele vytvoří zprávu daného typu a uloží ji do svého outboxu – buffer odchozích zpráv. Zároveň systém vytvoří identifikační data pro samotnou identifikaci zprávy a pro její další směrování. Podle identifikačních dat směrování určí systém uzly příjemců, jímž je zpráva určena.
	Odesílatel odešle zprávu na Proxy server buď okamžitě (online), nebo až v určitý okamžik (v EDS/SMVS pravidelně zprávy zasílá služba SSW Scheduler). Pokud systém zasílá zprávu online, obsahuje komunikační obálka pouze tuto jednu zprávu. V případě, že jsou zprávy zasílány pravidelně v určitý okamžik, obsahuje obálka všechny zprávy, které doposud nebyly předány z aktuálního uzlu na Proxy server (mohou být různého typu).
	Systém odesílatele volá webovou službu Proxy serveru. Součástí volání je klientský certifikát uzlu odesílatele.
Proxy server	Webová služba Proxy serveru autentifikuje odesílatele (serverový a klientský certifikát) a načte obálku se zprávami.
	Připojený klientský certifikát slouží k jednoznačné identifikaci uzlu, ze kterého data přišla. Je volána metoda zpracovávající došlou zprávu.
	V DB je založena hlavička komunikace (obálka odesílatele) – kdo zaslal, kdy, apod.

	Do DB jsou uloženy jednotlivé zprávy, které jsou uloženy v komunikační obálce a každá zpráva má v identifikaci typ zprávy a bližší identifikaci dat, kterých se zpráva týká. Dále zpráva obsahuje seznam uzlů, pro které je ta která zpráva určena – tato informace je součástí dané zprávy a vytváří ji aplikace odesílatele. Proxy server vygeneruje pro každou konkrétní zprávu její číslo a to ze sekvence, která je definována pro kombinaci typu zprávy a konkrétního příjemce.
	Jako návratová hodnota volání webové služby je zaslán výsledek zpracování zprávy na Proxy serveru a případná chybová hláška. V případě chyby se žádné zprávy na Proxy server neukládají.
Příjemce – EIS/ EDS/SMVS Systém	Zprávy čekají na Proxy serveru, dokud si je nevyzvedne jejich příjemce (EIS nebo EDS/SMVS) – příjemce musí začít komunikaci požadavkem na zaslání relevantních zpráv. To se na straně EDS/SMVS děje pomocí služby SSW Scheduleru, vznikem události na straně EDS/SMVS vyvolávající stažení zpráv nebo manuálním požadavkem uživatele.
	Příjemce vytvoří zprávu, která obsahuje požadavek na zaslání zpráv z Proxy serveru. Tento požadavek obsahuje seznam typů zpráv a poslední přijaté číslo zprávy daného typu – podle těchto dat Proxy server vyhledává zprávy ve svém zásobníku a zasílá je zpět.
	Příjemce volá webovou službu Proxy serveru. Součástí volání je klientský certifikát uzlu příjemce.
Proxy server	Webová služba Proxy serveru autentifikuje příjemce (serverový a klientský certifikát) a načte zprávu obsahující požadavek.
	Připojený klientský certifikát slouží k jednoznačné identifikaci uzlu, ze kterého požadavek přišel. Je volána metoda zpracovávající došlý požadavek.
	Do DB je uložena hlavička požadavku (obálka příjemce) – kdo, kdy, vlastní požadavek.
	Systém vyhledá v zásobníku zpráv ty zprávy, které vyhovují zaslanému požadavku (typ zprávy číslo zprávy je větší jak číslo poslední přijaté zprávy příjemcem) a jsou určeny pro uzel příjemce. Tyto zprávy jsou sloučeny pod komunikační obálku příjemce.
	Tato obálka je vrácena v návratové hodnotě volání webové služby
Příjemce – EIS/ EDS/SMVS/Systém	Po příjmu obálky systém daného uzlu uloží jednotlivé zprávy do svého inboxu (buffer došlých zpráv). EDS/SMVS zároveň zašle informační zprávu zadaným uživatelům o příjmu zprávy daného typu.
	Další zpracování je již záležitostí daného systému.

3.2.2 Terminologie

- Uzel integrace – seznam systémů, které se účastní integrace dat s EDS/SMVS. Tento číselník musí být společný pro všechny uzly, aby každý uzel mohl správně přiřadit ke každé zprávě kód uzlu příjemce, kterému je zpráva určena.
- Typy zpráv – číselník jednotlivých typů zpráv, které si vyměňují jednotlivé uzly integrace mezi sebou.
- Zpráva – nejnižší úroveň předávaných dat. Zpráva je určitého typu a byla vytvořena na určitém uzlu integrace. Každá jednotlivá zpráva je identifikována svým GUID, které musí být jedinečné ve všech systémech účastnících se integrace. Ke každé zprávě odesílající systém generuje seznam příjemců, pro které je zpráva určena, a seznam identifikačních údajů, které se týkají dané zprávy.
- Komunikační obálka – soubor zpráv, které můžou být různého typu. Pokud obálka obsahuje zprávy odesílatele, pak každá zpráva může být určena jinému příjemci, nebo více příjemcům. Pokud obálka obsahuje zprávy pro příjemce, může být každá zpráva jiného typu, ale každá zpráva je určena danému příjemci. Obálka je identifikována svým GUID, které musí být jedinečné ve všech systémech účastnících se integrace.
- Bližší identifikace zprávy – univerzální pole, které blíže identifikuje data v dané zprávě – může to být identifikátor dokladu, kapitola, finanční místo apod. Tato data mohou sloužit např. Pro hledání uzlu příjemce dané zprávy – pokud více uzlů pracuje se zprávami stejného typu XXX, ale jen jeden z nich zpracovává tyto zprávy z kapitoly YYY a jiný uzel z ostatních kapitol. Dále tato identifikace slouží pro kontrolu, zda může uživatel zpracovat zprávu mimo pořadí.

3.2.3 Schéma komunikace



3.2.4 Alternativní způsob přenosu dat – předávání dat pomocí souborů

Zjednodušený postup předávání dat:

- systém 1 připraví jednotlivé zprávy k odeslání a zabalí je do komunikační obálky.
- systém 1 exportuje komunikační obálku do XML souboru
- systém 1 předá XML soubor systému 2 emailem
- systém 2 importuje XML soubor
- systém 2 rozebere komunikační obálku a uloží jednotlivé zprávy do svého systému
- systém 2 zpracuje zprávy od systému 1
- z výsledků zpracování vytvoří systém 2 jednotlivé zprávy, které zabalí do komunikační obálky
- systém 2 exportuje komunikační obálku do XML souboru
- systém 2 předá XML soubor systému 1 emailem
- systém 1 importuje XML soubor
- systém 1 rozebere komunikační obálku a uloží jednotlivé zprávy do svého systému

Pro zabezpečení komunikace pomocí XML souborů je nutné, aby XML soubory byly podepsány elektronickým podpisem.

XML soubory používají pro přenos zpráv větev Obalka/ObalkaObsah/Odber/OdberZprava v XML schématu.

Emailová adresa test@ssw.cz je na straně EDS/SMVS určená k zasílání souborů pro otestování.

3.2.5 Alternativní způsob přenosu dat – direct webová služba

Zjednodušený postup předávání dat:

- systém 1 připraví jednotlivé zprávy k odeslání a zabalí je do komunikační obálky.
- systém 1 volá webovou službu vystavenou systémem 2 a té předá komunikační obálku se zprávami
- systém 2 rozebere komunikační obálku a uloží jednotlivé zprávy do svého systému
- systém 2 zpracuje zprávy
- z výsledků zpracování vytvoří systém 2 jednotlivé zprávy, které zabalí do komunikační obálky
- systém 2 volá webovou službu vystavenou systémem 1 a té předá komunikační obálku se zprávami
- systém 1 rozebere komunikační obálku a uloží jednotlivé zprávy do svého systému, které může následně zpracovat

Systémy se mezi sebou ověřují klientským certifikátem, který je přiložen ve volání webové služby.
Systém příjemce musí vystavit webovou službu pro příjem zpráv z ostatních systémů.

3.3 Technická specifikace rozhraní webových služeb, definice bezpečnostních prvků

3.3.1 Technická specifikace rozhraní webových služeb

Pro předání informace o přístupovém bodě webových služeb a struktuře přenášených dat v XML zprávě bude použita definice WSDL. Detailní specifikace je uvedena na adrese http://www.w3.org/TR/wsdl.

Pro komunikaci zpráv mezi systémy je definován WSDL soubor s konkrétním přístupovým bodem (URL adresou) a informací o struktuře dat.

Univerzální schéma XSD obsahující struktury XML zpráv pro veškeré zprávy je vloženo v příloze.

3.3.2 Pravidla přenosu protokolem SOAP

Pro SOAP komunikaci platí následující základní pravidla:

- přenos se provádí na stanovenou URL,
- přenos je zabezpečen na úrovni komunikačního kanálu pomoci SSL,
- volající systém se autentizuje svým komerčním serverovým certifikátem jako klient spojení (dále klientským certifikátem),
- přenos je považován za úspěšný, pokud se vrátí odpověď ve validní struktuře s http kódem 200,
- návratový HTTP kód <> 200 (menší, nebo větší 200) a SOAP: fault je považován za chybu přenosu resp. nepřijetí zprávy ke zpracování,
- přenášená XML zpráva obsahuje atributy potřebné pro autorizaci (tj. kód uzlu integrace popř. podpis zprávy) a ID komunikační obálky,
- ID obálky je generováno odesílatelem a je unikátní pro všechny typy rozhraní inicializované z daného EIS. Identifikátor je definován jako GUID – řetězec s délkou 36 znaků s použitím numerických znaků (0–9), znaků ‘a,b,c,d,e,f’ a znaku ´–´ (pomlčka). Musí být zachována unikátnost ID přenosu,
- přenášení datových souborů je realizováno pomocí SOAP zprávy s přílohou (specifikace na http://www.w3.org/TR/SOAP-attachments).

3.3.3 Způsob autorizace, zabezpečená komunikace

Pro zabezpečení SOAP komunikace se bude využívat transportní protokol HTTPS. Jedná se o zabezpečenou verzi protokolu HTTP (specifikace na http://www.ietf.org/rfc/rfc2616) rozšířenou o protokol TLS (specifikace na http://www.ietf.org/rfc/rfc5246.txt).

Bude využíváno oboustranně autentizované TLS spojení. Tzn., že obě strany se budou navzájem autentizovat svými komerčními systémovými (serverovými) certifikáty, které jsou primárně určeny pro bezpečnou komunikaci mezi servery. Princip vytvoření spojení mezi klientem a serverem lze popsat následujícími kroky:

1. klient (tj. EDS/SMVS nebo Systém) pošle serveru (Proxy) požadavek na SSL spojení spolu s doplňujícími informacemi (např. verze SSL, nastavení šifrování atd.),
2. server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informací a především certifikát serveru,
3. podle přijatého certifikátu si klient ověří autentičnost serveru. Certifikát obsahuje veřejný klíč serveru,
4. server si vyžádá zaslání veřejného klíče klientského certifikátu,

5. klient zašle svůj veřejný klíč certifikátu,
6. dle použitého typu kryptografického algoritmu si server vymění s klientem šifrovací klíč,
7. klient a server si navzájem potvrdí, že jejich další komunikace bude šifrována předaným klíčem z předchozího bodu,
8. je ustanoveno zabezpečené spojení šifrované vygenerovaným šifrovacím klíčem,
9. aplikace již komunikují přes šifrované spojení, je možné na server posílat požadavky.

Z důvodu bezpečnosti se bude každý systém autorizovat vlastním klientským certifikátem.

3.3.4 Elektronické podpisy datových zpráv, způsob podepisování

Z důvodu zajištění konzistence a důvěryhodnosti přenášených dat v případě přenosu XML souborů je vyžadováno, aby přenášená data byla podepsána zaručeným elektronickým podpisem.

K podepisování lze použít kvalifikovaný osobní certifikát, který je vydán osobě oprávněné k činnosti spojené s určitým úkonem v jednom systému a následným odesláním důvěrných dat do druhého systému.

Funkcionalita podepisování:

Pro podepisování aplikačních dat přenášených přes rozhraní se bude využívat standardní postup pro podepisování XML zpráv verze 1.0 dle definice konsorcia W3C s rozšířením o další funkcionality podepisování XML zpráv verze 1.1 pro potřebu pokrytí využití certifikátu rodiny SHA-2. Popis funkcionality je k dispozici na adresách:
http://www.w3.org/TR/xmldsig-core/ a http://www.w3.org/TR/xmldsig-core1/.

Další informace lze nalézt na adrese: http://www.w3.org/Signature/.

Postup podepisování:

Před nebo při sestavování XML zprávy vyzve systém uživatele ke zvolení certifikátu, který má být použit pro podepsání odesílaných aplikačních dat.

Po sestavení XML struktury pro dané rozhraní dle specifikace provede systém odesílatele podepsání aplikačních dat, tzn., že se jako reference podpisu použije XML element (XPath výraz) **//Obalka/ObalkaObsah**.

Po vykonání procedury podepsání se informace o podpisu vloží do elementu **//Obalka/ObalkaPaticka/Signature**, který dle standardní definice typu „http://www.w3.org/2000/09/xmldsig#SignatureType“ obsahuje všechny potřebné elementy.

Systém odesílatele dat je povinen přiložit i veřejnou část certifikátu tak, aby příjemce mohl před vlastním zpracováním dat provést validaci podpisu. K uložení informace o veřejném klíči je určen element **//Obalka/ObalkaPaticka/Signature/KeyInfo/X509Data**.

Podpisy jednotlivých zpráv:

V rámci každé jednotlivé zprávy může existovat element „Dokument“ – V tomto elementu je možné předat dokument PDF/A, který je opatřený kvalifikovaným elektronickým podpisem, vydaným ve shodě se zákonem o elektronickém podpisu v platném znění.

3.4 Definice datových struktur

3.4.1 Definice komunikační obálky

Pro přenášení datových zpráv mezi jednotlivými systémy byla definována jednotná XML struktura. Definovaná XML struktura (dále nazývaná jako „komunikační obálka“) bude využívána pro veškeré přenosy dat.

Komunikační obálku lze charakterizovat těmito vlastnostmi:

- podpora více typů zpráv při přenosu dat
- možnost zasílat více zpráv různých typů v jedné komunikační obálce
- dodržena syntaktická pravidla jazyka XML
- formální definice struktury na základě XML schématu využívající syntaxi jazyka XSD
- možnost podepsání aplikační části zprávy oprávněnou osobou a tedy kontrolu celistvosti celého XML souboru
- datové prvky elementů budou v maximální míře vycházet z informačního systému o datových prvcích dle zákona 365/2000 Sb.

3.4.2 Struktura komunikační obálky

Komunikační obálka je součástí všech datových zpráv předávaných mezi systémy integrace. Jinak řečeno, každá datová zpráva je SOAP XML zprávou, jejíž kořenový element je tvořen komunikační obálkou, která má následující části:

- hlavička – identifikační údaje zprávy, identifikace odesílatele a příjemce zprávy,
- obsah – vlastní datový obsah přenášející samotná aplikační data,
- patička – elektronický podpis (povinné pouze v případě přenosu XML souborů).

Použitím formátu XML pro přenos dat je možné ještě před zpracováním zprávy provést tzv. XML validaci. Porovnáním zasílané XML zprávy vůči definici XML struktury (ve formátu XSD) se ověří, že zpráva splňuje všechny syntaktické požadavky, tj. že její struktura, názvy a obsahy XML elementů odpovídají definici.

3.4.2.1 Hlavička

Hlavička obsahuje následující elementy:

Název	**Povinnost**	**Význam**
ObalkaID	Ano	Unikátní identifikátor obálky (přiděluje odesílatel)
ObalkaUzel	Ano	Kód uzlu odesílatele
ObalkaSmer	Ano	Směr komunikace (OP = odesílatel – Proxy, PP = příjemce – Proxy)
ObalkaDatum	Ano*	Datum a čas vytvoření zprávy
ObalkaUzelPrijemce	Ne/Ano	Uzel příjemce obálky – použito a povinný v případě komunikace se souborem nebo direct webovou službou

3.4.2.2 Obsah

Struktura obsahu zprávy je závislá na typu přenášených aplikačních dat (zpráv).

Při vystavování (odesílání) zpráv na Proxy server je použit element *Obalka/ObalkaObsah/Vystaveni*, který obsahuje jeden element *ZpravaPocet* a 1–n elementů *Zprava,* obsahující již data konkrétních zpráv.

Proxy server vrací výsledek uložení zpráv do svého bufferu v elementu *Obalka/ObalkaObsah/ZpracovaniVysledek.*

Při odběru (příjmu) zpráv z Proxy serveru je použit element *Obalka/ObalkaObsah/Odber/OdberPozadavek* na zaslání požadavku na odběr zpráv a element *Obalka/ObalkaObsah/Odber/OdberZprava* na zaslání zpráv z Proxy serveru k příjemci.

Pokud Proxy server nemá pro příjemce žádné požadované zprávy, pak je místo elementu *Obalka/ObalkaObsah/Odber/OdberZprava* použit element

Obalka/ObalkaObsah/ZpracovaniVysledek, ve kterém je naplněn element *Vysledek* hodnotou OK a element *Hlaska* hodnotou „Žádná data k odběru“.

Detailní struktura hlavičky zprávy a požadavku na zaslání zpráv je uvedena v kapitole 4 Popis struktury obecných zpráv přenosu.

3.4.2.3 Patička

Patička obsahuje následující elementy:

Název	Povinnost	Význam
Signature	Ne	Elektronický podpis XML dle standardu XML Signature

3.5 Pravidla kontroly zabezpečení, pravidla kontroly přenášených dat

Po přijetí zaslaných dat budou prováděny různé typy kontrol ve stanoveném pořadí.

Při přenosu dat mezi systémy jsou prováděny následující kontroly:

- kontrola platnosti elektronického podpisu (u přenosu pomocí XML souboru),
- validace struktury zprávy oproti definici XSD,
- kontrola věcné správnosti dat.

3.5.1 Kontrola platnosti elektronického podpisu

U rozhraní přenášených XML souborem je prováděna kontrola platnosti elektronického podpisu. Kontrolnímu modulu je předána kompletní XML zpráva k ověření elektronického podpisu.

Modul následně provede:

- Ověření podpisu elementu <SignedInfo> tak, že přepočítá hash elementu <SignedInfo> (použitím „Message-Digest“ algoritmu uvedeného v elementu <SignatureMethod>) a použije veřejnou část certifikátu k ověření, zda hodnota elementu <SignatureValue> odpovídá hash hodnotě elementu <SignedInfo>.
- Následně přepočítá hash pro element uvedený v elementu <Reference> (vyskytující se v elementu <SignedInfo>) a porovná s hash hodnotami, které se nacházejí v elementu <DigestValue> uvnitř elementu <Reference>.

Služba po vyhodnocení elektronického podpisu předá integračnímu serveru odpověď, zda je elektronický podpis platný.

3.5.2 Validace struktury zpráv oproti definici XSD

Úlohou validace XML zprávy se rozumí ověření, že zaslaná XML data jsou dobře formátovaná (tj. dodržují syntaktická pravidla jazyka XML) a navíc odpovídají danému XML schématu.

XML schéma se definuje pomocí jazyka XSD, který vytváří pravidla struktury validních dokumentů. Jinak řečeno – definuje elementy, atributy a vztahy mezi nimi. XSD přitom též využívá jazyk XML. Podrobnější informace lze najít na http://www.w3.org/TR/xmlschema-2/, případně http://www.w3.org/XML/Schema.

3.5.3 Pravidla věcné kontroly

Na vstupu do systému příjemce probíhá vždy při přijetí zprávy kontrola věcné správnosti dat. Vstupní data procházejí jednotlivými kontrolami, přičemž případně nalezené chyby jsou zaznamenávány. Po ukončení vstupních kontrol projde systém jejich výsledek. Pokud zjistí alespoň jednu zaznamenanou chybu, přeruší další zpracování a označí celkový výsledek zpracování jako chybný.

K validaci mohou být použity následující typy kontrol:

Číselník – kontrola ověřuje, že vstupní hodnota existuje v systémovém číselníku, na který se vstupní pole odkazuje.

Unikátnost – kontrola ověřuje, že pro dané vstupní pole v systému neexistuje stejná hodnota (např. dvě stejná čísla dokladů).

Existence – kontrola ověřuje, že pro dané vstupní pole v systému existuje vstupní hodnota.

3.6 Pravidla hlášení chyb na komunikační úrovni

3.6.1 Způsoby hlášení závad datových přenosů

Tato sekce popisuje pravidla při hlášení závad datových přenosů a jejich následném ošetření. Jednotlivé závady mohou vzniknout před přenosem zprávy do systému, při přenosu nebo v systému při provádění definovaných kontrol. Pokud přenos dat proběhne bez závad, v hlavičce zpětné zprávy je HTTP kód 200. V případě, že během přenosu dojde k chybě, je tato zaslána zpět odesílajícímu systému. Jednotlivé chybové stavy jsou poté rozděleny podle místa vzniku následovně:

- Technické chyby – odpověď obsahující SOAP Fault element a HTTP kód 4xx nebo 5xx.
- Bezpečnostní a syntaktické chyby – odpověď obsahuje element ZpracovaniVysledek s popisem chyby a HTTP kód 200.
- Sémantické chyby aplikačních dat – odpověď obsahuje element ZpracovaniVysledek s popisem chyby a HTTP kód 200.

3.6.2 Technické chyby

Tento druh chyb vzniká při inicializaci nebo přenosu zprávy. Jinými slovy – jedná se o chyby při komunikaci se systémem. Obvykle se projeví při chybné autorizaci klientského certifikátu, zadáním špatné URL adresy, rozpadnutím spojení během přenosu dat, případně nedostupností webové služby či aplikace. Odpověď obsahuje HTTP kód 4xx nebo 5xx a zpráva s odpovědí obsahuje element SOAP Fault element s popisem chyby. Ve výjimečných případech je informace o chybě publikována ve formátu HTML.

Přehled a příčina jednotlivých systémových chyb, které mohou nastat:

- kód 400 „ICM_HTTP_CONNECTION_FAILED“
- Příčina: Chyba může být způsobena zatížením serveru, na který dorazilo v jednom okamžiku velké množství požadavků.
- Řešení: Pokud se jedná o tento typ chyby, zkuste zaslání dat opakovat.
- kód 401 „Unauthorized“
- Příčina: Chyba může být způsobena zadáním špatného uživatelského jména nebo hesla, případně nedostatečným oprávněním.
- Řešení: Zkontrolujte autorizační údaje
- kód 403 „Forbidden“
- Příčina: Chyba může být způsobena zadáním špatné URL adresy. Případně nefunkčností adaptéru.
- Řešení: Opravte URL adresu
- kód 404 „Not Found“
- Příčina: Chyba může být způsobena zadáním špatné části URL adresy. Požadavek byl doručen na server, který ho nedokázal rozpoznat.
- Řešení: Opravte URL adresu

- kód 500 „Internal Server Error“
- Příčina: Existuje několik příčin chyby. Možné příčiny mohou být: nefunkční komunikační kanál, "No SOAP envelope", "invalid channel", "no receiver agreement".
- Řešení: Pokud se jedná o tento typ chyby, zkuste zaslání dat opakovat.
- kód 503 „Service unavailable application stopped!“
- Příčina: Web server je dostupný, ale z důvodu zastavení některé z volaných komponent nelze požadavek odbavit.
- Řešení: Pokud se jedná o tento typ chyby, zkuste zaslání dat opakovat.
- V případě jiné chyby kontaktujte Hotline EDS/SMVS.

3.6.3 Bezpečnostní a syntaktické chyby

Před vlastním zpracováním aplikačních dat jsou prováděny bezpečnostní a syntaktické kontroly nebo akce:

- Validace zprávy – dochází k syntaktické kontrole zaslaných dat. Jedná se zejména o formální validaci XML struktury a obsahu zaslané zprávy. Kontroluje se, zda obsah zprávy odpovídá požadavkům na syntaxi uvedených v XSD definici pro daný typ zprávy. Pokud při této kontrole dojde ke zjištění chyby, bude zpracování zprávy odmítnuto.
- Kontrola klientského certifikátu s vazbou na odesílatele.
- Kontrola případných elektronických podpisů v XML zprávě – služba pro validaci elektronického podpisu vrátí odpověď, zda je elektronický podpis platný.

V případě, že během kontrol dojde k nalezení chyby, sestaví se hlášení o chybě. Hlášení je vloženo do komunikační obálky. V dalším zpracování zprávy již ke kontrolám nedochází a nedojde ani k uložení aplikačních dat do systému příjemce. Hlášení o chybě je zasláno zpět odesílajícímu systému jako synchronní odpověď s hlášením o chybě s HTTP kódem 200.

Zároveň je chyba zaznamenána do centrální logovací komponenty spolu s vazbou na původní datovou zprávu pro potřeby pozdějšího dohledání příčiny problému.

3.6.4 Sémantické chyby

Pokud všechny kontroly proběhly v pořádku, zpracování zprávy dále pokračuje spuštěním funkcionality věcné kontroly dat. Po úspěšném ukončení věcné kontroly jsou data teprve uložena do systému příjemce.

V případě, že během kontrol dojde k nalezení chyby, je tato zaslána zpět odesílajícímu systému v synchronní odpovědi. Aplikační chybové hlášení bude odesláno jako synchronní hlášení o chybě s HTTP kódem 200. Vlastní informace o chybě je předávána v elementu //Obalka/ObalkaObsah/ ZpracovaniVysledek.

Zpráva nese ve strukturovaném formátu informaci o chybě, která vznikla při ukládání původních zdrojových dat dále určených ke zpracování.

Zároveň je chyba zaznamenána do centrální logovací komponenty spolu s vazbou na původní datovou zprávu pro potřeby pozdějšího dohledání příčiny problému.

3.7 Certifikáty, zásady jejich použití a správy

Certifikáty budou na projektu IISSP využívány k následujícím účelům:

- elektronické podepisování aplikačních dat (vybraných transakcí),
- navázání šifrované komunikace mezi systémy (oboustranně autentizované TLS spojení)

3.7.1 Zabezpečení automatické komunikace mezi systémy

Pro zabezpečení SOAP komunikace se bude využívat aplikační protokol HTTPS s využitím oboustranně autentizovaného TLS spojení. Tzn., že obě strany se budou navzájem autentizovat svými komerčními systémovými (serverovými) certifikáty, které jsou primárně určeny pro bezpečnou komunikaci mezi servery.

Každý systém účastnící se integrace musí předat otisk svého klientského certifikátu, aby podle tohoto otisku byl systém EDS/SMVS schopen ztotožnit původce komunikace.

3.7.2 Elektronické podepisování aplikačních dat

Zaručený elektronický podpis (aplikačních dat, transakcí, zpráv apod.) se používá pro zajištění integrity, autenticity a nepopiratelnosti autorství přenášených dat. Z tohoto důvodu je vyžadováno použití kvalifikovaných osobních certifikátů založených na kvalifikovaných systémových certifikátech, které byly vydány akreditovanými certifikačními autoritami.

4 Popis struktury obecných zpráv přenosu

4.1 Standardní položky hlavičky zprávy

Název	Povinnost	Výskyt	Význam
ZpravaID	Ano	1	Unikátní identifikátor zprávy (přiděluje odesílatel)
ZpravaTyp	Ano	1	Typ zprávy z číselníků typů zpráv
ZpravaUzel	Ano	1	Kód uzlu integrace, který zprávu vytvořil
ZpravaDatum	Ano	1	Datum a čas vytvoření zprávy
ZpravaNadrizenaID	Ne	0 .. 1	Identifikátor nadřízené zprávy
ZpravaCislo	Ano/Ne	1	Číslo zprávy u příjemce
Zprava	Ano	1 .. n	Seznam konkrétních zpráv, popis struktury viz dokument popisující struktury jednotlivých zpráv
ZpravaPrijemce	Ano	1 .. n	Seznam příjemců zprávy
PrijemceUzel	Ano	1 .. n	Kód uzlu příjemce zprávy
ZpravaIdentifikace	Ne	0 .. n	Seznam identifikačních dat zprávy
Identifikace	Ano	1 .. n	Element identifikace
IdentifikaceTyp	Ano	1	Typ identifikace – I = identifikace zprávy (default), S = směrování zprávy
IdentifikaceNazev	Ano	1	Popis identifikační hodnoty – např. Akce
IdentifikaceHodnota	Ano	1	Hodnota identifikace – např. 112V010010011

4.2 Struktura požadavku na odběr zpráv z Proxy serveru

Požadavek na odběr zpráv je uložen v elementu Obalka/ObalkaObsah/Odber/OdberPozadavek

Název		Povinnost	Výskyt	Význam
PozadavekPocet		Ano	1	Počet následujících elementů „Pozadavek“ – kontrolní hodnota
Pozadavek		Ano	1 .. n	
	ZpravaTyp	Ano	1	Kód typu zprávy, které mají být zaslány příjemci
	ZpravaCisloPosledni	Ne	0 .. 1	Číslo poslední zprávy daného typu, které je evidováno u příjemce. Z Proxy serveru jsou zaslány zprávy s číslem větším než uvedené. Pokud číslo není zadáno (default), zasílají se doposud neodeslané zprávy.

5 Specifikace datových objektů

5.1 Struktura pro přenos žádosti na předání aktuálního stavu čerpání rozpočtu

EIS zašle požadavek na předání stavu čerpání z EDS/SMVS. Součástí požadavku bude mimo jiné rozmezí data, za které má být čerpání předáváno.

5.1.1 Obsah datové věty

5.1.1.1 isp_eCerpaniPozadavek

Element	Datový typ	Min	Max	Výčet	Povinnost elementu	Klíč	Popis a kontroly
IdentifikatorExternihoSystemu	xs:string				Ano		Unikátní identifikátor externího informačního systému, který dávku odesílá.
DavkaIdentifikatorExterni	xs:string	36	36		Ano	PK	GUID. Hodnota generovaná na straně EIS. Unikátní identifikátor konkrétní dávky s aktuálním požadavkem na předání stavu čerpání.
DatumOd	xs:datetime				Ano		Počátek rozmezí data, za které mají být data vygenerována (včetně). Datum může nabývat hodnot 1.1. daného roku – 31.12. daného roku.
DatumDo	xs:datetime				Ano		Konec rozmezí data, za které mají být data vygenerována (včetně). Datum může nabývat hodnot 1.1. daného roku – 31.12. daného roku.
Kapitola	xs:unsignedShort	3	3		Ano		Kód kapitoly z číselníku kapitol. Čerpání je zasíláno vždy maximálně za jednu kapitolu.

Element	Datový typ	Min	Max	Výčet	Povinnost elementu	Klíč	Popis a kontroly
VydajTypKod	xs:string	1	9		Ne		Kód typu výdajů z číselníku typů výdajů. Bude-li vyplněn konkrétní kód typu výdaje, odpověď bude obsahovat informace o čerpání pouze pro daný titul, subtitul, nebo podmnožinu subtitulu. Pokud je vyplněný kód typu výdaje, není možné zaslat požadavek na akci EDS/SMVS, nebo středisko.
EdsSmvsAkce	xs:string	13	13		Ne		Identifikační číslo akce (projektu). Bude-li vyplněna konkrétní akce EDS/SMVS, odpověď bude obsahovat informace o čerpání pouze pro danou akci EDS/SMVS. Pokud je vyplněná akce EDS/SMVS, není možné zaslat požadavek na kód typu výdaje nebo středisko.
Stredisko	xs:unsignedLong	3	9		Ne		Kód střediska z číselníku středisek. Bude-li vyplněno konkrétní středisko, odpověď bude obsahovat informace o čerpání pouze pro dané středisko. Pokud je vyplněné středisko, není možné zaslat požadavek na kód typu výdaje nebo akci EDS/SMVS.

5.2 Vybrané údaje o aktuálním čerpání projektů vystupujících z EDS/SMVS do EIS za data IISSP

Ze systému EDS/SMVS budou poskytována data o finančním čerpání akcí (projektů), která budou předávána do EIS. Pokud budou vyexportována data z EDS/SMVS pomocí exportu čerpání za UCB a zároveň za IISSP, mohou data nabývat duplicitních záznamů (UCB – ČNB „IISSP“). Kódy

Účelových znaků a Účelů mohou být průběžně doplňovány. Odpověď bude obsahovat všechny informace o čerpání, které bylo modifikováno v průběhu požadovaného období.

5.2.1 Obsah datové věty

5.2.1.1 isp_eCerpani

Element	Datový typ	Min	Max	Výčet	Povinnost elementu	Klíč	Popis a kontroly
DavkaIdentifikatorExterni	xs:string	36	36		Ano	PK	GUID. Hodnota generovaná na straně EIS. Unikátní identifikátor konkrétní dávky s požadavkem na předání aktuálního stavu čerpání.
Id	xs:string	36	36		Ano	FK	GUID. Jednoznačný identifikátor položky čerpání.
ZpracovaniDatumIISSP	xs:datetime				Ne		Datum, kdy došlo ke zpracování konkrétní operace v IISSP. Datum není uvedeno u čerpání na kódech řádků, které vznikly v systému EDS/SMVS.
DatumZapisu	xs:datetime				Ano		Datum, ke kterému došlo k aktualizaci čerpání rozpočtu v EDS/SMVS. Odpovídá dotazu isp_eCerpaniPozadavek DatumOd a DatumDo.
CerpaniDatumIISSP	xs:datetime				Ne		Datum, ke kterému došlo k aktualizaci čerpání rozpočtu v IISSP.
VypisDatumIISSP	xs:datetime				Ne		U pohybů, které byly účtovány při zpracování bankovního výpisu, bude element vyplněn datem daného bankovního výpisu.
Rok	xs:unsignedShort	4	4		Ano		Rok SR, ke kterému se čerpání vztahuje.
KodRadku	xs:string	4	5		Ano		Kód řádku bilance.
Zdroj	xs:unsignedShort	7	7		Ano		Kód zdroje z číselníku zdrojů SR.

Element	Datový typ	Min	Max	Výčet	Povinnost elementu	Klíč	Popis a kontroly
Paragraf	xs:unsignedShort	7	7		Ano		Kód odvětvového třídění z číselníku odvětvového třídění.
PolozkaRozpoctova	xs:unsignedShort	4	4		Ano		Kód druhového třídění z číselníku druhového třídění.
StrukturaPrijmovaVydajova	xs:string	1	10		Ano		Kód příjmové a výdajové struktury z číselníku kódů činností.
EdsSmvsAkce	xs:string	13	13		Ano		Identifikační číslo akce (projektu).
Ucel	xs:string	9	9		Ne		Kód účelů z číselníku účelů IISSP.
ZnakUcelovy	xs:unsignedShort	6	6		Ne		Kód odvětvového třídění z číselníku odvětvového třídění.
Castka	xs:decimal (18,8)				Ano		Částka čerpaná za daný PK. Vždy se jedná o hodnotu v CZK a pokud nabývá záporné hodnoty, jedná se o snížení.
Spolufinancovani	xs:string	2	4	NEUZ UZ VSR	Ne		Spolufinancování. VSR – Výdaj SR, UZ – Výdaj uznatelný EU, NEUZ – Výdaj neuznatelný EU.

Příloha A – použité pojmy, zkratky a symboly

Hesla jsou uvedena v abecedním řazení.

Zkratka, pojem	Význam
EDS	Evidenční dotační systém
EIS	Externí informační systém, nebo Ekonomický informační systém
IISSP	Integrovaný informační systém Státní pokladny
MF	Ministerstvo financí
NEUZ	Výdaj neuznatelný EU
SMVS	Správa majetku ve vlastnictví státu
SP	Spárovaná platba
SN	Snížení (záporná částka)
URN	Uniform Resouce Name
UTF	UCS Transformation Format
UZ	Výdaj uznatelný EU
VSR	Výdaj SR
XML	Extensible Markup Language
XSLT	eXtensible Stylesheet langure transformations – transformace v jazyce XSL