Elektronická evidence tržeb

Formát a struktura údajů o evidované tržbě

Popis datového rozhraní pro příjem datových zpráv evidovaných tržeb

Verze 3.1.1

Datum poslední verze dokumentu: 13.10.2016

Změny vůči publikované verzi 1.0)*

Změna číslo	Popis
1	Byla vložena další omezující podmínka na finanční částky: nesmějí obsahovat nevýznamné vedoucí nuly a nulová hodnota nesmí mít znak minus – viz odst. *3.3.3.11 Finanční položky tržby*
2	Byla přidána nová kritická kontrola: maximální délka datové zprávy evidované tržby (tj. včetně SOAP obálky) nesmí přesáhnout 12 kB – viz odst. *2.2.3 Kritické kontroly*
3	Byla přidána 2 nová chybová hlášení s kódy 7 (překročena maximální délka datové zprávy evidované tržby) a 8 (technická chyba nebo chyba v datech) – viz odst. *3.5.4 Seznam chybových kódů a chybových zpráv*

Změny vůči publikované verzi 2.0)*

Změna číslo	Popis	Kapitola
1	Přidání varování (text a kód varování) do Potvrzovací zprávy, doplněna tabulka varování	*3.4 Potvrzovací datová zpráva*
2	Upřesnění požadavků na plnění položky UUID	*3.3.3.1 UUID zprávy (uuid_zpravy)*
3	Upřesnění požadavků na plnění položky dat_trzby vzhledem k časové zóně	*3.3.3.10 Datum a čas přijetí tržby (dat_trzby)*
4	Vysvětlení povinných a nepovinných položek	*3.3.2 Přehled položek datové zprávy o evidované tržbě*
5	Upřesnění finančních položek	*3.3.3.11 Finanční položky tržby*
6	Doplněna nová kategorie kontrol a chyb při přijetí datové zprávy: propustné kontroly a propustné chyby. Uveden výčet prováděných propustných kontrol.	*2.2.4 Propustné kontroly (propustné chyby)*
7	Upřesněna označení pokladního zařízení poplatníka	*3.3.3.8 Označení pokladního zařízení poplatníka (id_pokl)*
8	Doplnění požadavků na údaje uváděné na účtence	*3.6 Údaje uváděné na účtence*
9	Upřesněny požadavky na elektronický podpis datové zprávy evidované tržby	*6.2 Podpis datových zpráv evidovaných tržeb*
10	Upřesnění jednoznačné identifikace evidované tržby	*5 Identifikace evidované tržby - volba položek pro PKP*

Změny vůči publikované verzi 3.0)*

Změna číslo	Popis	Kapitola
1	Upřesněn popis položek, které nemají definovanou hodnotu (prázdné položky) – tyto položky nesmí být ve zprávě uvedeny s prázdnými hodnotami	*3.3.2 Přehled položek datové zprávy o evidované tržbě* *3.3.3.11 Finanční položky tržby*
2	Úprava popisu výpočtu PKP – výpočet elektronického podpisu (odkaz na RFC 3447)	*4.1 Podpisový kód poplatníka (PKP)*
3	Prodloužení délky pořadového čísla účtenky (porad_cis) z 20 na 25 znaků	*3.3.3.9 Pořadové číslo účtenky (porad_cis)*

4	Zařazení varování o propustných kontrolách do odpovědi v ověřovacím módu	*2.2.2 Produkční a neprodukční prostředí* *2.2.4 Propustné kontroly (propustné chyby)* *3.5 Chybová datová zpráva*
5	Přesun informací platných pro všechna prostředí z dokumentu Přístupové a provozní informace Playground	*1.1 Číslování verzí rozhraní* *2.3 Standardy síťové komunikace* *2.4 Certifikáty*
6	Úprava definice pojmu Chybová datová zpráva	*1.3 Přehled základních pojmů*
7	Doplnění informace, že zaslání zprávy v ověřovacím módu není splněním evidenční povinnosti	*2.2.1 Mód odeslání datové zprávy*
8	Doplnění podmínky vazby 1:1 mezi evidovanou tržbou a datovou zprávou evidované tržby	*1.3 Přehled základních pojmů*
9	Doplnění podmínky unikátnosti označení provozovny v rámci poplatníka, a to konkrétně na dvojici položek: (dic_popl, id_provoz)	*3.3.3.7 Označení provozovny (id_provoz)*
10	Doplnění podmínky unikátnosti označení pokladny v rámci poplatníka, a to konkrétně na čtveřici položek: (dic_popl, id_provoz, id_pokl, dat_trzby)	*3.3.3.8 Označení pokladního zařízení poplatníka (id_pokl)*
11	Doplnění (upřesnění) popisu položek datové zprávy o podmínky unikátnosti, a to konkrétně na pětici položek: (dic_popl, id_provoz, id_pokl, porad_cis, dat_trzby)	*3.3.3.9 Pořadové číslo účtenky (porad_cis)*

Změny vůči poslední publikované verzi 3.1)*

Změna číslo	Popis	Kapitola
1	Úprava popisu výpočtu PKP – výpočet elektronického podpisu – žádná z úprav oproti verzi dokumentu 2.0 nijak nemění způsob výpočtu PKP, jde pouze o úpravu vysvětlujícího textu na základě připomínek veřejnosti	*4.1 Podpisový kód poplatníka (PKP)*

)* Tabulka změn nepopisuje drobné formální úpravy textu.

Vymezení obsahu dokumentu

Dokument popisuje datové rozhraní pro příjem a potvrzování datových zpráv obsahujících údaje o tržbě, které jsou poplatníci EET povinni zasílat pro každou uskutečněnou tržbu, která je předmětem evidence dle zákona č. 112/2016 Sb., o evidenci tržeb.

Soubory obsahující definici XML schematu a webové služby (WSDL), které formálně popisují strukturu datových zpráv evidovaných tržeb a webovou službu pro jejich příjem, jsou přílohou tohoto dokumentu.

Obsah

1 ÚVODNÍ INFORMACE

1.1 ČÍSLOVÁNÍ VERZÍ ROZHRANÍ

Verze rozhraní je číslována dvojicí čísel: hlavní (první) a vedlejší (druhé), např. 1.0, 1.1, 1.2 atd. Hlavní číslo verze rozhraní je součástí URL adresy ve všech cílových prostředích (např. v3 pro verzi 3.x). Změny v rozhraní jsou zveřejňovány následujícím způsobem:

1. V případě drobných změn, které nemají mít vliv na implementaci v pokladních zařízeních poplatníků (tzv. kompatibilní změny), dojde ke změně pouze vedlejšího čísla verze: 1.0 -> 1.1 -> 1.2 -> ... atd. Verze XML schématu a WSDL dokumentu v jejich hlavičce se analogicky změní z 1.0 na 1.1, 1.2, atd. Naproti tomu uvnitř XML schématu a WSDL dokumentu se URL jmenných prostorů, cílová URL adresa služby apod. nezmění - na konci zůstane /v1.
2. Pokud dojde ke změnám struktury datových zpráv, které vyžadují změnu implementace v pokladních zařízeních poplatníků (tzv. nekompatibilní změny – změny formátu datových položek apod.), dojde ke změně čísla hlavní verze: např. 1.2 -> 2.0. Následné drobné změny (viz bod 1.) budou opět číslovány: 2.1, 2.2, atd. Uvnitř XML schématu a WSDL dokumentu se URL adresa jmenných prostorů, cílová URL služby apod. změní na /v2.

1.2 PŘEHLED ZKRATEK

Zkratka	Definice
BKP	Bezpečnostní kód poplatníka
CA	Certifikační autorita
CRL	Certificate Revocation List
DIČ	Daňové identifikační číslo
DPH	Daň z přidané hodnoty
DŘ	Daňový řád
EET	Elektronická evidence tržeb
FIK	Fiskální identifikační kód
FS, FSČR	Finanční správa České republiky
GFŘ	Generální finanční ředitelství
PKP	Podpisový kód poplatníka
SEČ	Středoevropský čas (CET)
SELČ	Středoevropský letní čas (CEST)
SOAP	Protokol pro výměnu zpráv založených na XML dle specifikace https://www.w3.org/TR/soap/
WS-security	Web Services Security – rozšíření SOAP standardu o zabezpečení WWW služeb dle specifikace publikované https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

Zkratka	Definice
WSDL	Web Services Description Language –jazyk založený na XML určený pro popis funkcí, jež nabízí WWW služba, dle specifikace https://www.w3.org/TR/wsdl
XML Schema	Jazyk založený na XML, určený pro definici struktury XML dokumentů, dle specifikace https://www.w3.org/TR/xmlschema11-1/ a https://www.w3.org/TR/xmlschema11-2/
ZoET	Zákon o evidenci tržeb

1.3 PŘEHLED ZÁKLADNÍCH POJMŮ

V tomto odstavci uvádíme definice základních pojmů, které jsou používány v textu tohoto dokumentu.

Pojem	Definice
Účtenka	Účtenkou rozumíme doklad vystavený (v papírové podobě nebo elektronicky) poplatníkem tomu, od koho tržba plyne, který obsahuje údaje o evidované tržbě definované v ustanovení § 20 ZoET.
e-tržba	Datová struktura v definovaném formátu stanoveném finanční správou, která obsahuje všechny datové údaje evidované tržby tak, jak je stanoví ZoET a příslušné vyhlášky Ministerstva financí. Jedná se o samotná data o tržbě, tedy bez SOAP obálky a jejího zabezpečení, tedy tzv. SOAP payload.
Datová zpráva evidované tržby	Datová struktura v definovaném formátu stanoveném finanční správou, která obsahuje e-tržbu a další potřebné údaje technického charakteru. Jedná se o kompletní XML zprávu, obsahující údaje popsané příslušnými standardy pro webové služby: SOAP/WSDL/WS-Security atd. Datová zpráva evidované tržby je pokladním zařízením zasílána na společné technické zařízení správce daně. Každé evidované tržbě odpovídá právě jedna datová zpráva evidované tržby, pokud se nejedná o opakované zaslání téže evidované tržby.
Potvrzovací datová zpráva	Datová struktura v definovaném formátu stanoveném finanční správou, která obsahuje fiskální identifikační kód (FIK) a současně slouží jako potvrzení přijetí a formální správnosti)* zaslané *datové zprávy evidované tržby*.
Chybová datová zpráva	Datová struktura v definovaném formátu stanoveném finanční správou, která obsahuje

Pojem	Definice
	chybový kód a jeho případný slovní popis pro případ, že – přijatá *datová zpráva* obsahující údaje o *evidované tržbě* obsahuje kritické chyby, které neumožňují její zpracování, – nebo došlo k jiné chybě, znemožňující další zpracování na straně správce daně – nebo byla *datová zpráva* obsahující údaje o *evidované tržbě* bez kritických chyb zaslána v tzv. ověřovacím módu.
Pokladní zařízení poplatníka	Zařízení na straně poplatníka, které zasílá údaje o evidované tržbě. Může tím být dle kontextu myšleno samotné koncové zařízení, například pokladna, ale i následný SW a HW, který datové zprávy o tržbě skutečně zasílá. V datové zprávě je položka „Označení pokladního zařízení“, která identifikuje koncové zařízení (pokladnu). Jinde v textu je většinou myšleno koncové zařízení i následný SW a HW zasílající datovou zprávu.
Evidovaná tržba	Evidovanou tržbou je platba, která splňuje formální náležitosti pro evidovanou tržbu a která zakládá rozhodný příjem. Evidovanou tržbou je také platba, která splňuje formální náležitosti pro evidovanou tržbu a je určena k následnému čerpání nebo zúčtování, které zakládají rozhodný příjem, nebo následným čerpáním nebo zúčtováním té platby, která zakládá rozhodný příjem (viz § 4 ZoET).

)* Formální správností datové zprávy se rozumí její shoda s předepsanou datovou strukturou a splnění veřejně dokumentovaných kritických kontrol, které jsou podmínkou přijetí datové zprávy evidované tržby, nikoliv věcná správnost příslušné evidované tržby.

2 KOMUNIKAČNÍ SCÉNÁŘ ZASÍLÁNÍ DATOVÝCH ZPRÁV

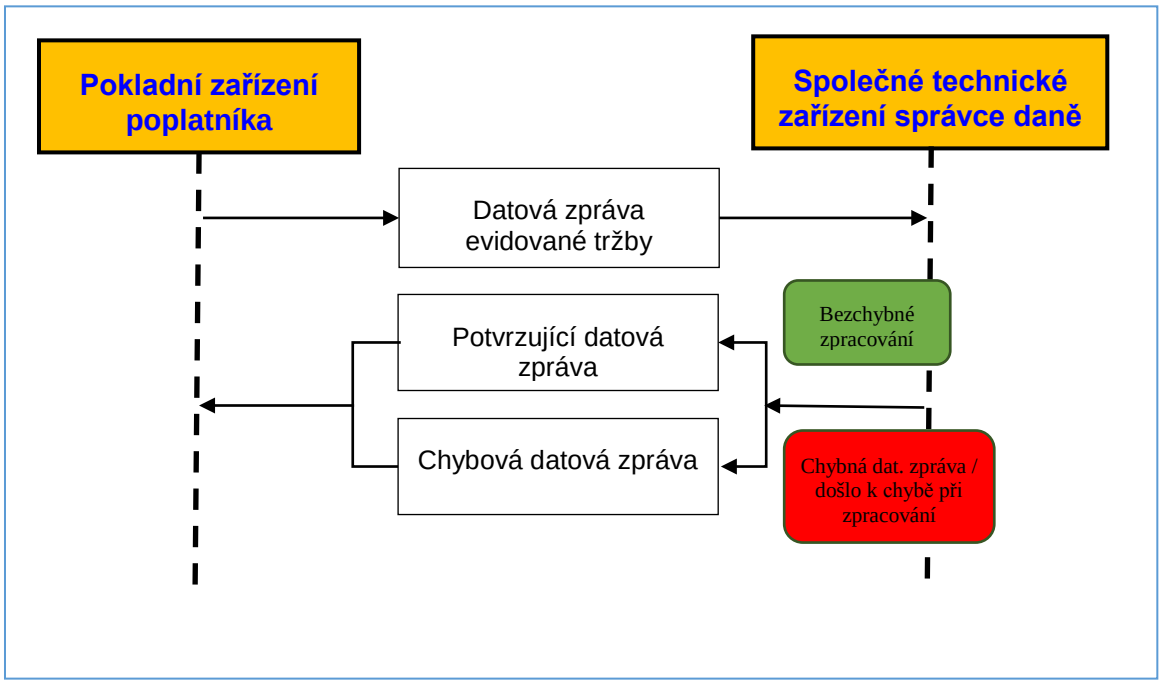
2.1 ZÁKLADNÍ SCHÉMA KOMUNIKACE

Pokladní zařízení zasílá jednotlivé datové zprávy evidovaných tržeb na společné technické zařízení správce daně určené správcem daně. V případě, že *datová zpráva evidované tržby* odeslaná pokladním zařízením poplatníka vyhovuje kritickým kontrolám – viz kapitola *2.2.3 Kritické kontroly* a je možno na straně finanční správy datovou zprávu uložit, je na straně společného technického zařízení správce daně bezprostředně vytvořena *potvrzovací datová zpráva*, kterou toto zařízení odešle zpět na pokladní zařízení poplatníka, jež *datovou zprávu evidované tržby* předtím odeslalo.

Komunikace tedy probíhá v režimu: *požadavek/odpověď* (*request/response*). Účelem potvrzovací datové zprávy je potvrdit přijetí a formální správnost přijaté datové zprávy pokladnímu zařízení poplatníka. Potvrzovací datová zpráva je s původní datovou zprávou svázána bezpečnostním kódem poplatníka (BKP) a kromě toho číslem datové zprávy přiděleným poplatníkem – viz *3 Struktura datových zpráv* a obsahuje fiskální identifikační kód (FIK) generovaný společným technickým zařízením správce daně. FIK je pro každou správně přijatou datovou zprávu evidované tržby unikátní.

V případě, že datová zpráva evidované tržby nevyhoví kritickým kontrolám nebo nastane technická chyba na straně společného technického zařízení správce daně, která znemožní další zpracování datové zprávy, bude pokladní zařízení poplatníka, jež *datovou zprávu evidované tržby* předtím odeslalo, informováno chybovou datovou zprávou, pokud to povaha chyby umožní.

Komunikační scénář je znázorněn na *Obr. 1*.



Obr. 1 – Komunikační scénář

2.2 MÓDY ODESÍLÁNÍ DATOVÝCH ZPRÁV, PRODUKČNÍ A NEPRODUKČNÍ PROSTŘEDÍ

2.2.1 Mód odeslání datové zprávy

Poplatník EET bude mít možnost odeslat datovou zprávu s údaji o evidované tržbě v jednom ze dvou módů. Požadovaný mód lze zvolit nastavením příznaku ověřovacího módu odesílání (atribut *overeni*) v hlavičce datové zprávy:

- **Ostrý mód** bude sloužit pro běžné odesílání datových zpráv s údaji o evidované tržbě a získání fiskálního identifikačního kódu. V ostrém módu hlavička datové zprávy buď neobsahuje příznak ověřovacího módu odesílání, nebo je atribut nastaven na hodnotu *false*.
- **Ověřovací mód** bude sloužit poplatníkům EET k ověření správného nastavení a funkčnosti spojení pokladního zařízení se systémem EET. Datová zpráva v takovém případě bude obsahovat příznak ověřovacího módu odesílání s hodnotou *true*. Zaslání datové zprávy v ověřovacím módu není zasláním údajů o evidované tržbě ve smyslu §18 ZoET.

2.2.2 Produkční a neprodukční prostředí

GFŘ zveřejní adresy webové služby v produkčním prostředí a v jednom nebo více neprodukčních prostředích systému EET:

- **Produkční prostředí** je určeno pro poplatníky EET a bude sloužit pro rutinní provoz, tj. především příjem a potvrzování datových zpráv s údaji o evidovaných tržbách.
- **Neprodukční prostředí (playground)** bude (budou) sloužit výhradně vývojářům softwaru pro pokladní zařízení, tedy nikoli koncovým uživatelům pokladních zařízení. Zaslání datové zprávy do neprodukčního prostředí není zasláním údajů o evidované tržbě ve smyslu §18 ZoET, tj. FIK vrácený neprodukčním prostředím není platným fiskálním identifikačním kódem.
  V neprodukčním prostředí mohou být certifikáty pokladních zařízení vydávány zjednodušeným způsobem.

S oběma prostředími bude možné komunikovat jak v ostrém, tak v ověřovacím módu. Následující tabulka popisuje, jaká odpověď bude systémem EET odeslána v závislosti na:

1. Módu, ve kterém byla datová zpráva odeslána. Mód je určen hodnotou atributu *overeni* v elementu *Hlavicka* datové zprávy s údaji o evidované tržbě.
2. Cílovém prostředí. Prostředí je učeno adresou webové služby, na kterou byla datová zpráva odeslána. Adresy jednotlivých prostředí budou zveřejněny správcem daně.
3. Validitě datové zprávy, tj. zda datová zpráva obsahuje kritické chyby.

Mód datové zprávy evidované tržby	Cílové prostředí	Scénář použití	Validita datové zprávy evidované tržby	Odpověď systému EET
Ostrý Datová zpráva v elementu *Hlavicka* **ne**obsahuje atribut *overeni*, nebo obsahuje atribut *overeni="false"*	**Produkční**	Poplatník EET zasílá datovou zprávou údaje o evidované tržbě	Validní	- potvrzovací datová zpráva, obsahuje FIK a ev. i varování o propustných chybách - přidělený FIK je unikátní a je platným fiskálním identifikačním kódem - odpověď obsahuje el. podpis (podepsáno produkčním certifikátem) - **evidovaná tržba byla přijata, zaevidována a bude dále uchovávána systémem EET)***
			Nevalidní	- chybová datová zpráva - nenulový kód chyby, textový popis chyby - odpověď neobsahuje el. podpis
	Neprodukční (playground)	Vývojář SW testuje svou aplikaci v ostrém módu	Validní	- potvrzovací datová zpráva, obsahuje FIK a ev. i varování o propustných chybách - přidělený FIK bude mít specifickou hodnotu („-ff“, na konci), **ale není platný** - odpověď obsahuje příznak neprodukčního prostředí (*test="true"*) - odpověď obsahuje el. podpis (podepsáno testovacím certifikátem)
			Nevalidní	- chybová datová zpráva - nenulový kód chyby, textový popis chyby - odpověď obsahuje příznak neprodukčního prostředí (*test="true"*) - odpověď neobsahuje el. podpis
Ověřovací Datová zpráva v elementu *Hlavicka* obsahuje atribut *overeni="true"*	**Produkční**	Poplatník EET ověřuje funkčnost spojení mezi svým pokladním zařízením a systémem EET	Validní	- chybová datová zpráva, obsahuje kód chyby 0, a ev. i varování o propustných chybách - kód chyby 0 – tj. žádné věcné chyby nebyly nalezeny - popis chyby „Datovou zpravu evidovane trzby v overovacim modu se podarilo zpracovat“ - odpověď neobsahuje el. podpis
			Nevalidní	- chybová datová zpráva - nenulový kód chyby, textový popis chyby - odpověď neobsahuje el. podpis
	Neprodukční (playground)	Vývojář SW testuje svou aplikaci v módu ověření funkčnosti spojení mezi pokladním zařízením a systémem EET	Validní	- chybová datová zpráva, obsahuje kód chyby 0, a ev. i varování o propustných chybách - kód chyby 0 – tj. žádné věcné chyby nebyly nalezeny - popis chyby „Datovou zpravu evidovane trzby v overovacim modu se podarilo zpracovat“ - odpověď obsahuje příznak neprodukčního prostředí (*test="true"*) - odpověď neobsahuje el. podpis
			Nevalidní	- chybová datová zpráva - nenulový kód chyby, textový popis chyby - odpověď obsahuje příznak neprodukčního prostředí (*test="true"*) - odpověď neobsahuje el. podpis
)* ve všech ostatních případech v této tabulce evidovaná tržba byla přijata systémem EET, ale nebude zaevidována ani dále uchovávána systémem EET				

Tabulka 1: Varianty odpovědi systému EET

2.2.3 Kritické kontroly (kritické chyby)

V systému EET jsou na přijatých datových zprávách evidovaných tržeb prováděny kritické kontroly. Pokud jakákoliv z kritických kontrol neprojde, datová zpráva o evidované tržbě nebude přijata a FIK nebude vydán.

Systém EET bude při nalezení kritické chyby vracet chybovou datovou zprávu obsahující číselný kód chyby a textový popis chyby – viz odst. *3.5.4 Seznam chybových kódů a chybových zpráv*.

Při nalezení chyb, které by systém EET mohl vyhodnotit jako kybernetický útok, systém EET žádnou odpověď klientovi (v našem případě pokladnímu zařízení poplatníka) nedává.

Kritické kontroly jsou následující:

1. kontrola kódování XML dokumentu – předepsáno je kódování UTF-8
2. kontrola na konkrétní XML schema (*.xsd) datové zprávy evidované tržby, které obsahuje přesnou definici struktury dat a formátů jednotlivých datových položek a kontrola přítomnosti povinných položek
3. kontrola elektronického podpisu datové zprávy (certifikát poplatníka je součástí SOAP obálky datové zprávy dle standardu WS-Security):
    a. kontrola vydavatele certifikátu
    b. kontrola platnosti certifikátu včetně kontroly CRL, které jsou aktuálně technickému zařízení dostupné
    c. kontrola správnosti podpisu
4. kontrola toho, že BKP přísluší k uvedenému PKP
5. kontrola integrity DIČ poplatníka
6. kontrola na celkovou délku datové zprávy evidované tržby (tj. zpráva včetně SOAP obálky), která nesmí přesáhnout 12 kB

2.2.4 Propustné kontroly (propustné chyby)

Propustné kontroly prováděné transakčním systémem EET nejsou důvodem k odmítnutí vydání FIK. Jedná se tedy o kontroly, jejichž výsledek bude pouze uložen do úložiště datových zpráv pro další případné zpracování.

Propustné kontroly jsou následující:

1. kontrola shodnosti DIČ poplatníka uvedeného v datové struktuře e-tržba (XML element <Trzba>) s DIČ uvedeným v certifikátu, pomocí kterého byla podepsána datová zpráva evidované tržby
2. kontrola integrity DIČ pověřujícího poplatníka
3. kontrola správnosti hodnoty PKP
4. kontrola data a času přijetí tržby (uvedené v datové zprávě) vůči datu a času přijetí zprávy na společné technické zařízení správce daně. Pokud bude datum a čas přijetí tržby o více než 2 hodiny novější, nebo naopak bude o více než 2 roky starší než datum a čas přijetí zprávy, bude označeno kontrolou jako chybné. Jako chybné bude označeno i datum a čas přijetí tržby starší než *minimální datum a čas přijetí tržby* vztahující se k příslušnému cílovému prostředí ve smyslu odst. *2.2.2 Produkční a neprodukční prostředí*.

    Předpokládané minimální datumy a časy přijetí tržby dle cílových prostředí:
    a. neprodukční prostředí (playground) verze 3: 1.8.2016
    b. produkční prostředí před 1.12.2016: 1.11.2016
    c. produkční prostředí: 1.12.2016.

Pokud jakákoliv z propustných kontrol neprojde (a současně nenastane žádná kritická chyba), datová zpráva o evidované tržbě bude přijata a FIK bude vydán, jako kdyby všechny kontroly prošly.
Chyby spočívající v nesplnění propustných kontrol budeme nazývat *propustné*. Potvrzovací datová zpráva bude v případě, že nastane jedna nebo více propustných chyb, doplněna o příslušná textová varování a jim odpovídající číselné kódy. Stejným způsobem budou příslušná varování zařazena i do chybové odpovědi s kódem 0 v ověřovacím módu.

2.3 STANDARDY SÍŤOVÉ KOMUNIKACE

2.3.1 HTTPS/TLS

Použití protokolu HTTPS je povinné, bez autentizace klientskými certifikáty. Podporované verze TLS jsou TLS 1.1 a vyšší, doporučená verze TLS je 1.2.

2.3.2 HTTP

Použití protokolu HTTP/1.1 je povinné.

2.4 CERTIFIKÁTY

Certifikáty používané pro účely zabezpečení HTTPS spojení, pro podpis datových zpráv evidované tržby a potvrzovacích datových zpráv jsou popsány v dokumentu „Přístupové a provozní informace“ příslušném pro dané prostředí.

3 STRUKTURA DATOVÝCH ZPRÁV

3.1 KÓDOVÁNÍ DATOVÝCH POLOŽEK

Všechny položky ve všech datových zprávách budou využívat pouze vybrané znaky kódované jedním bajtem ve standardní ASCII znakové sadě. Dekadické kódy povolených znaků mají hodnoty 9, 10, 13 nebo od 32 do 126.

Kódování datových zpráv jakožto XML dokumentů bude povinně UTF-8, tj. 1. řádek XML SOAP obálky bude mít vždy tvar:

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

Všechny XML elementy e-tržby patří do jmenného prostoru (namespace), který je specifikován v definici webové služby (WSDL), např.:

```
xmlns:eet="http://fs.mfcr.cz/eet/schema/v3"
```

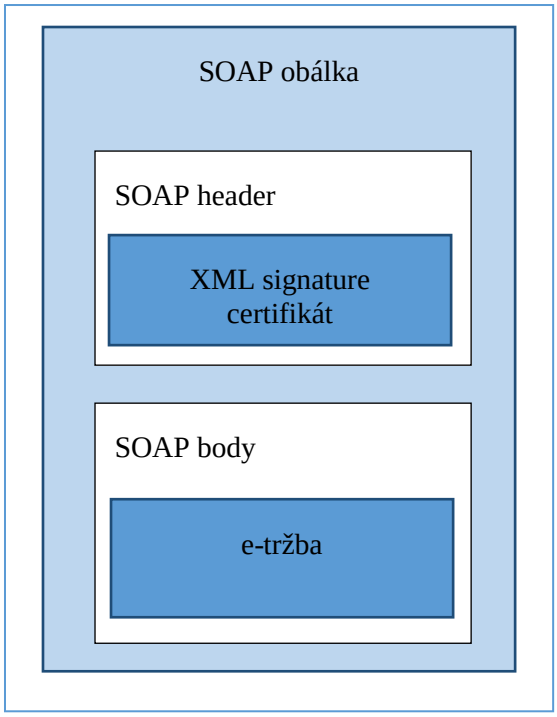
Maskou datového formátu jednotlivých položek, která je uvedena u jejich detailního popisu níže, rozumíme regulární výraz ve smyslu XML schematu, který přesně definuje požadovanou syntaxi položky. Pro jednoznačnost je v tomto dokumentu navíc explicitně uveden metaznak pro začátek textového řetězce (^) a pro konec textového řetězce ($).

Hexadecimální číslice větší než 9 („a“ až „f“) je možno uvádět malými nebo velkými písmeny, tj. alternativně „A“ až „F“.

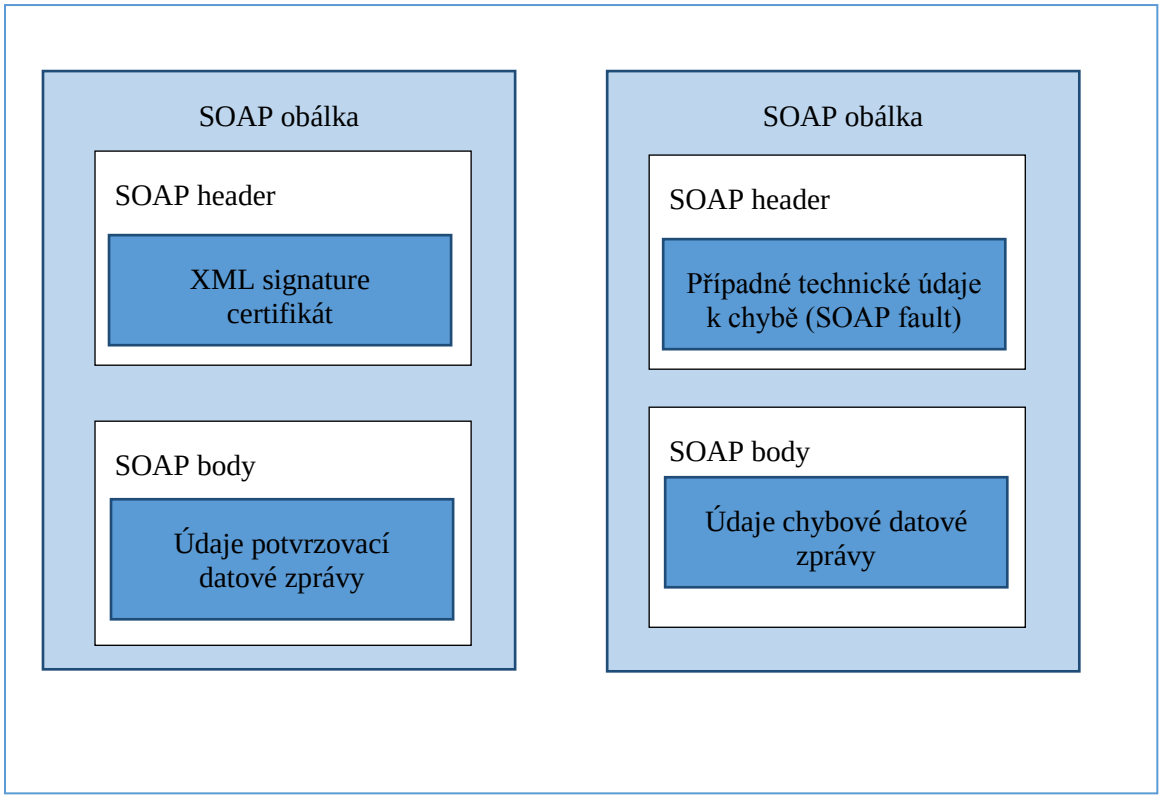
3.2 PŘEHLED STRUKTURY DATOVÝCH ZPRÁV

Všechny 3 datové zprávy (datová zpráva evidované tržby, potvrzovací datová zpráva, chybová datová zpráva) mají společný základní datový formát daný protokolem SOAP (Simple Object Access Protocol), tj. aplikační XML datové struktury jsou vloženy do tzv. těla SOAP obálky (<SOAP Envelope Body>).

Datová zpráva evidované tržby (viz *Obr. 2*) a potvrzovací datová zpráva budou podepsány (viz *Obr. 3* vlevo), chybová datová zpráva nikoliv (viz *Obr. 3* vpravo).



Obr. 2 Struktura datové zprávy evidované tržby



Obr. 3 Struktura potvrzovací a chybové datové zprávy

3.3 DATOVÁ ZPRÁVA EVIDOVANÉ TRŽBY

Datová zpráva včetně SOAP obálky je SOAP XML struktura obsahující všechny údaje, které jsou stanoveny pro odeslání údajů o evidované tržbě. Vlastní data evidované tržby jsou uložena ve vnořené

struktuře *e-tržby* (XML element <Trzba>), která bude obsažena v XML elementu <SOAP Envelope Body>.

V XML elementu <SOAP Envelope Header> bude uložen XML signature a certifikát, k němuž příslušný privátní klíč byl použit k vytvoření XML signature. V situaci, kdy certifikát klíče použitý v době vydání účtenky (tj. vytvoření PKP a BKP) již není platný v okamžiku odeslání datové zprávy evidované tržby, použije poplatník pro XML signature aktuálně platný certifikát – viz též *4.1 Podpisový kód poplatníka (PKP).*

Datová zpráva evidované tržby bude formálně přesně popsána v definici příslušné webové služby – viz *6 Upřesnění XML zprávy ve tvaru SOAP a její zabezpečení*

Vlastní *datová zpráva evidované tržby* je uložena v XML elementu <SOAP Envelope Body> jako element <Trzba>.
Tento element obsahuje 3 vnořené elementy, které reprezentují datové oblasti: <Hlavicka>, <Data> a <KontrolniKody>.
Tyto datové oblasti obsahují vlastní datové položky – viz odstavec *3.3.2 Přehled položek datové zprávy o evidované tržbě.*

3.3.1 XML formát e-tržby

XML formát e-tržby v přehledu:

```
<eet:Trzba>
      <eet:Hlavicka atributy … />
      <eet:Data atributy … />
      <eet:KontrolniKody>
            hodnoty …
      </eet:KontrolniKody>
</eet:Trzba>
```

Atributy a hodnoty XML elementů jsou podrobně popsány níže.

3.3.2 Přehled položek datové zprávy o evidované tržbě

Datová oblast		Název položky	Povinná)**	XML jméno)*
Hlavička	1	UUID zprávy	Ano	uuid_zpravy
	2	Datum a čas odeslání zprávy	Ano	dat_odesl
	3	První zaslání údajů o tržbě	Ano	prvni_zaslani
	4	Příznak ověřovacího módu odesílání	Ne	overeni
Data	5	DIČ poplatníka	Ano	dic_popl
	6	DIČ pověřujícího poplatníka	Ne	dic_poverujiciho
	7	Označení provozovny	Ano	id_provoz
	8	Označení pokladního zařízení	Ano	id_pokl
	9	Pořadové číslo účtenky	Ano	porad_cis
	10	Datum a čas přijetí tržby	Ano	dat_trzby
	11	Celková částka tržby	Ano	celk_trzba
	12	Celková částka plnění osvobozených od DPH, ostatních plnění	Ne	zakl_nepodl_dph
	13	Celkový základ daně se základní sazbou DPH	Ne	zakl_dan1
	14	Celková DPH se základní sazbou	Ne	dan1
	15	Celkový základ daně s první sníženou sazbou DPH	Ne	zakl_dan2
	16	Celková DPH s první sníženou sazbou	Ne	dan2
	17	Celkový základ daně s druhou sníženou	Ne	zakl_dan3

Datová oblast		Název položky	Povinná)**	XML jméno)*
		sazbou DPH		
	18	Celková DPH s druhou sníženou sazbou	Ne	dan3
	19	Celková částka v režimu DPH pro cestovní službu	Ne	cest_sluz
	20	Celková částka v režimu DPH pro prodej použitého zboží se základní sazbou	Ne	pouzit_zboz1
	21	Celková částka v režimu DPH pro prodej použitého zboží s první sníženou sazbou	Ne	pouzit_zboz2
	22	Celková částka v režimu DPH pro prodej použitého zboží s druhou sníženou sazbou	Ne	pouzit_zboz3
	23	Celková částka plateb určená k následnému čerpání nebo zúčtování	Ne	urceno_cerp_zuct
	24	Celková částka plateb, které jsou následným čerpáním nebo zúčtováním platby	Ne	cerp_zuct
	25	Režim tržby	Ano	rezim
Kontrolní kódy	26	Podpisový kód poplatníka (PKP)	Ano	pkp
	27	Bezpečnostní kód poplatníka (BKP)	Ano	bkp

)* XML jméno znamená buď jméno XML elementu, nebo XML atributu.

)** Položky označené jako povinné musí být vyplněny v každé datové zprávě. Položky označené jako nepovinné musí být vyplněny, pokud jsou k evidované tržbě relevantní (např. plátci DPH musí mít vyplněny položky o DPH, které jsou relevantní k tržbě). Nejsou-li nepovinné položky uvedeny, jsou považovány za prázdné. Položky s prázdnou hodnotou jsou v XML zprávě nepřípustné.

Příklad:

Uvedení následujících prázdných položek ve zprávě je chybné:

```
dic_poverujiciho=""
cest_sluz=""
```

3.3.3 Podrobný popis položek e-tržby

V této kapitole jsou popsány položky e-tržby z hlediska technického formátu a struktury. Další informace k jejich věcnému obsahu jsou v dokumentu „*Popis položek datové zprávy a příklady situací při evidenci tržeb*“. Jako příklady konkrétních DIČ byly v dalším textu použity DIČ GFŘ a MF ČR.

3.3.3.1 UUID zprávy (uuid_zpravy)

Je atributem XML elementu <Hlavicka>. UUID (Universaly Unique Identifier) datové zprávy evidované tržby je generováno pokladním zařízením poplatníka. UUID bude mít formát dle RFC 4122:

```
xxxxxxxx-xxxx-Mxxx-Nxxx-xxxxxxxxxxxx
```

kde „x“, „M“ a „N“ značí hexadecimální číslici. Číslice „M“ značí *verzi* UUID a má povolené hodnoty 1 až 5. Doporučená *verze* UUID je 4. Jde o univerzální jedinečný identifikátor v hlavičce datové zprávy evidované tržby, který je generován pokladním zařízením poplatníka. Jednoznačně identifikuje datovou zprávu (nikoli e-tržbu). I při opakovaném zaslání datové zprávy má být vytvořeno nové UUID zprávy. Hodnota dvou nejvyšších bitů číslice N je povinně 1 0 (označuje *variantu* UUID), tj. tato číslice má povolené hexadecimální hodnoty: 8, 9, A, B.

Maska datového formátu:

```
^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[1-5][0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}$
```

kde znak "-" je pomlčka (znak s dekadickým kódem 45 v ASCII znakové sadě).

Délka: 36 znaků.

Příklad:

```
b3a09b52-7c87-4014-a496-4c7a53cf9125
```

3.3.3.2 Datum a čas odeslání zprávy (dat_odesl)

Je atributem XML elementu <Hlavicka>. Datum a čas odeslání zprávy je okamžik, kdy pokladní zařízení odeslalo datovou zprávu evidované tržby.

Datový formát je určen datovým typem DateTime dle ISO 8601, jak je předpokládá příslušná W3C specifikace: https://www.w3.org/TR/xmlschema11-2/#dateTime:

rrrr-*mm*-*dd*T*hh*:*mm*:*ss*±*hh*:*mm*

kde „*rrrr*-*mm*-*dd*“ je datum ve tvaru „rok-měsíc-den“, „*hh*:*mm*:*ss*“ je čas ve tvaru „hodina:minuta:sekunda“ a „±*hh*:*mm*“ značí časovou zónu jako rozdíl vůči světovému času (UTC/GMT) v hodinách a minutách. Znak „±“ je buď „+“ (plus) nebo „-“ (minus) podle toho, zda rozdíl proti světovému času je kladný nebo záporný. Jako speciální hodnotu rozdílu lze uvést řetězec „Z“, který má stejný význam jako „+00:00“.

Datum a čas odeslání datové zprávy se uvádí jako lokální čas v dané časové zóně s povinným vyznačením časové zóny podle následujícího pravidla:

- +01:00 v případě, že hodnota spadá do období zimního času v ČR – tj. časová zóna je SEČ
- +02:00 v případě, že hodnota spadá do období letního času v ČR – tj. časová zóna je SELČ
- +*hh*:*mm*, nebo –*hh*:*mm* nebo Z v případě, že hodnota je uvedena v jiné časové zóně (mimo ČR).

Délka: 25 znaků.

Příklad – zimní čas:

```
2016-11-09T04:25:28+01:00
```

Tento časový okamžik znamená 4 hodiny, 25 minut a 28 sekund SEČ, tedy 3 hodiny 25 minut 28 sekund UTC/GMT.

Příklad – letní čas:

```
2017-06-09T05:25:28+02:00
```

Tento časový okamžik znamená 5 hodin, 25 minut a 28 sekund SELČ, tedy 3 hodiny 25 minut 28 sekund UTC/GMT.

3.3.3.3 První zaslání údajů o tržbě (prvni_zaslani)

Je atributem XML elementu <Hlavicka>. Je to příznak s hodnotami *true* nebo *false* (též *1* nebo *0*), který určuje, zda jde o první zaslání konkrétní evidované tržby (hodnota: *true* nebo *1*) nebo o opakované zaslání téže tržby (hodnota: *false* nebo *0*).

Datový formát je určen příslušnou W3C specifikací, viz: https://www.w3.org/TR/xmlschema11-2/#boolean).

Délka: 1 až 5 znaků.

Příklad:

```
true
```

3.3.3.4 Příznak ověřovacího módu odesílání (overeni)

Je atributem XML elementu <Hlavicka>. Je to příznak, kterým si pokladní zařízení poplatníka může nastavit ověřovací mód odesílání datových zpráv evidovaných tržeb.

Je-li tento příznak uveden a má-li hodnotu *true* (nebo *1*), je datová zpráva zpracována v ověřovacím módu – viz *2.2 Módy odesílání datových zpráv, produkční a neprodukční prostředí*.

Není-li tento příznak uveden nebo má-li hodnotu *false* (nebo *0*), je datová zpráva zpracována v ostrém módu.

Datový formát je určen příslušnou W3C specifikací, viz https://www.w3.org/TR/xmlschema11-2/#boolean).

Délka: 1 až 5 znaků.

Příklad:

```
true
```

3.3.3.5 DIČ poplatníka (dic_popl)

Je atributem XML elementu <Data>. Je to DIČ poplatníka, který odesílá datovou zprávu evidované tržby, platné k okamžiku přijetí tržby nebo vydání příkazu k jejímu provedení, pokud byl tento příkaz vydán dříve. Povinnou součástí DIČ je kód státu: CZ. Hodnota atributu se shoduje s DIČ uvedeným v certifikátu použitém pro elektronický podpis datové zprávy (certifikát je součástí SOAP obálky datové zprávy evidované tržby). Poplatník EET, kterému bylo změněno DIČ, může odesílat datové zprávy evidovaných tržeb s novým DIČ v atributu *dic_popl* podepsané původním certifikátem, dokud mu není vystaven certifikát nový.

Maska datového formátu:

```
^CZ[0-9]{8,10}$
```

Délka: 10 až 12 znaků.

Příklad (DIČ GFŘ a MF):

```
CZ72080043
CZ00006947
```

3.3.3.6 DIČ pověřujícího poplatníka (dic_poverujiciho)

Je atributem XML elementu <Data>. Je to platné DIČ poplatníka, kterému tržba plyne, ale který pověřil jiného poplatníka, aby za něj tuto tržbu evidoval. Datový formát je identický jako pro *DIČ poplatníka*.

3.3.3.7 Označení provozovny (id_provoz)

Je atributem XML elementu <Data>. Jedná se o číselné označení provozovny, která byla přidělena poplatníkovi na portálu EET. Označení provozovny je unikátní v rámci poplatníka. Unikátní označení provozovny v systému je dáno touto dvojicí položek:

```
(dic_popl, id_provoz).
```

Maska datového formátu:

```
^[1-9][0-9]{0,5}$
```

Délka: 1 až 6 znaků, tj. číselný rozsah je od 1 do 999999.

Příklad:

```
25
```

3.3.3.8 Označení pokladního zařízení poplatníka (id_pokl)

Je atributem XML elementu <Data>. Je to identifikační kód pokladního zařízení poplatníka, které zasílá datovou zprávu evidované tržby na společné technické zařízení správce daně. Tento kód je tvořen na straně poplatníka alfanumerickými znaky a vybranými speciálními znaky. Pro konkrétního poplatníka musí být označení pokladního zařízení unikátní na jedné provozovně v jednom okamžiku. Přesně to znamená, že musí být unikátní čtveřice položek:

```
(dic_popl, id_provoz, id_pokl, dat_trzby).
```

Maska datového formátu:

```
^[0-9a-zA-Z\.,:;/#\-_ ]{1,20}$
```

kde poslední znak v hranaté závorce je mezera (znak " " s dekadickým kódem 32 v ASCII znakové sadě) a znak "`-`" je pomlčka (znak s dekadickým kódem 45 v ASCII znakové sadě).

Délka: 1 až 20 znaků.

Příklad:

```
5a/A-q/5:22d_2
```

3.3.3.9 Pořadové číslo účtenky (porad_cis)

Je atributem XML elementu <Data>. Jde o pořadové číslo účtenky, které je tvořeno na straně poplatníka alfanumerickými znaky a vybranými speciálními znaky. Tento kód je tvořen alfanumerickými znaky a vybranými speciálními znaky.

Pro konkrétního poplatníka musí být pořadové číslo účtenky unikátní na jedné provozovně, pro jedno pokladní zařízení v jednom okamžiku. Přesně to znamená, že musí být unikátní pětice položek:

```
(dic_popl, id_provoz, id_pokl, porad_cis, dat_trzby).
```

Účtenkou rozumíme doklad vystavený (v papírové podobě nebo elektronicky) poplatníkem tomu, od koho tržba plyne, který obsahuje údaje o evidované tržbě definované v ustanovení § 20 ZoET (viz *1.3 Přehled základních pojmů*).

Maska datového formátu:

```
^[0-9a-zA-Z\.,:;/#\-_ ]{1,25}$
```

kde poslední znak v hranaté závorce je mezera (znak " " s dekadickým kódem 32 v ASCII znakové sadě) a znak "`-`" je pomlčka (znak s dekadickým kódem 45 v ASCII znakové sadě).

Délka: 1 až 25 znaků.

Příklad:

```
#25/c-12/1A_2/2016
```

3.3.3.10 Datum a čas přijetí tržby (dat_trzby)

Je atributem XML elementu <Data>. Jde o datum a čas uskutečnění evidované tržby, případně datum vystavení účtenky, pokud byla vystavena dříve.

Formát je identický jako u položky – viz *3.3.3.2 Datum a čas odeslání zprávy*, tj. uvádí se datum a čas rozhodného okamžiku v lokální časové zóně, která byla použita při uvedení časového údaje na tištěné účtence, a k tomu povinně jednoznačné určení této časové zóny.

3.3.3.11 Finanční položky tržby

Všechny finanční položky tržby jsou atributy XML elementu <Data>. Jedná se o následující číselné položky, které představují finanční hodnoty v českých korunách:

11	Celková částka tržby
12	Celková částka plnění osvobozených od DPH, ostatních plnění
13	Celkový základ daně se základní sazbou DPH
14	Celková DPH se základní sazbou
15	Celkový základ daně s první sníženou sazbou DPH
16	Celková DPH s první sníženou sazbou
17	Celkový základ daně s druhou sníženou sazbou DPH
18	Celková DPH s druhou sníženou sazbou
19	Celková částka v režimu DPH pro cestovní službu
20	Celková částka v režimu DPH pro prodej použitého zboží se základní sazbou
21	Celková částka v režimu DPH pro prodej použitého zboží s první sníženou sazbou
22	Celková částka v režimu DPH pro prodej použitého zboží s druhou sníženou sazbou
23	Celková částka plateb určená k následnému čerpání nebo zúčtování
24	Celková částka plateb, které jsou následným čerpáním nebo zúčtováním platby

Číselné hodnoty všech částek jsou uvedeny v dekadické soustavě s právě dvěma povinnými desetinnými místy a řádovou tečkou v souladu se specifikací https://www.w3.org/TR/xmlschema11-2/#decimal. Hodnoty mohou být kladné, nulové nebo záporné.

Aby byla zaručena jednoznačná korespondence mezi číselnou hodnotou finanční položky a řetězcem znaků dekadické reprezentace této hodnoty, jsou zakázány číselně nevýznamné vedoucí nuly a znak minus (znak pomlčky s dekadickým kódem 45 v ASCII znakové sadě) před nulovou hodnotou.

Finanční položky, které datová zpráva neobsahuje, nebo nemají vyplněnou hodnotu, budou považovány za prázdné, tj. nedefinované (pozor: takové položky nebudou považovány za číselnou hodnotu 0). Položky s prázdnou hodnotou jsou v XML zprávě nepřípustné – viz *3.3.2 Přehled položek datové zprávy o evidované tržbě*.

Maska datového formátu:

```
^((0|-?[1-9]\d{0,7})\.\d\d|-0\.(0[1-9]|[1-9]\d))$
```

Délka:

- pro nezáporné hodnoty: 4 až 11 znaků, tj. minimální nezáporná hodnota je 0,00 Kč a maximální nezáporná hodnota je 99 999 999,99 Kč
- pro záporné hodnoty: 5 až 12 znaků, tj. minimální záporná hodnota je -99 999 999,99 Kč a maximální záporná hodnota je -0,01 Kč.

To znamená, že finanční položky jsou v absolutní hodnotě omezeny na čísla menší než 100 milionů Kč.

Příklady:

250.00

-187.20

0.56

Příklady chybné textové reprezentace:

Číselná hodnota	Chybná reprezentace	Správná reprezentace
20,45	020.45	20.45
10,25	00010.25	10.25
0	-0.00	0.00
0	-00.00	0.00
0,2	.20	0.20
-100	-00100.00	-100.00

3.3.3.12 Režim tržby (rezim)

Je atributem XML elementu <Data>. Režim evidované tržby je buď běžný, nebo zjednodušený. Je kódován následujícím způsobem:

- 0 běžný režim
- 1 zjednodušený režim.

Maska datového formátu:

```
^[01]$
```

Délka: 1 znak.

3.3.3.13 Podpisový kód poplatníka (pkp)

Je hodnotou XML elementu <pkp>, který je obsažen v XML elementu <KontrolniKody>. PKP je elektronickým podpisem vybraných údajů z e-tržby. Atributy elementu <pkp> definují:

- Použitý algoritmus otisku (message digest, hash): SHA256
- Použitý algoritmus elektronického podpisu: RSA2048
- Použitý způsob kódování PKP jakožto hodnoty XML elementu: Base64, tj. řetězec znaků: „0“ až „9“, „a“ až „z“, „A“ až „Z“, „/“, „+“ a „=“.

Typ je definován dle https://www.w3.org/TR/xmlschema11-2/#base64Binary.

Délka: délka binárních dat je 256 bajtů, tedy délka jejich Base64 reprezentace je 344 znaků.

Podrobný popis generování a výsledného formátu PKP je uveden v kapitole *4.1 Podpisový kód poplatníka (PKP).*

3.3.3.14 Bezpečnostní kód poplatníka (bkp)

Je hodnotou XML elementu <bkp>, který je obsažen v XML elementu <KontrolniKody>. BKP je otisk neboli tzv. message digest (hash) kódu PKP. Atributy elementu <bkp> definují:

- Použitý algoritmus otisku (message digest, hash): SHA1

- Použitý způsob kódování BKP jakožto hodnoty XML elementu: Base16, tj. řetězec hexadecimálních číslic.

Pozor – nejedná se o běžný typ https://www.w3.org/TR/xmlschema11-2/#hexBinary, ale upravenou hodnotu dle specifikace níže.

Délka: délka binárních dat 20 bajtů, tedy 40 hexadecimálních číslic. Pro lepší čitelnost budou hexadecimální číslice BKP odděleny pomlčkou (znak "-" s dekadickým kódem 45 v ASCII znakové sadě) po osmi číslicích. Celková délka textové reprezentace BKP tedy bude 44 znaků.

Maska datového formátu:

```
^([0-9a-fA-F]{8}-){4}[0-9a-fA-F]{8}$
```

kde znak "-" je pomlčka (znak s dekadickým kódem 45 v ASCII znakové sadě).

Podrobný popis generování a výsledného formátu BKP je uveden v kapitole *4.2 Bezpečnostní kód poplatníka (BKP)*.

3.3.4 Příklad e-tržby

V následujícím textu uvádíme příklad XML elementu <Trzba> zasílaném v běžném produkčním módu:

```
<eet:Trzba>
      <eet:Hlavicka
            uuid_zpravy="e23e5a5a-08d7-4a08-844d-2b6c6b60621d"
            dat_odesl="2016-12-08T21:19:40+01:00"
            prvni_zaslani="true" />
<eet:Data dic_popl="CZ72080043" dic_poverujiciho="CZ00006947"
      id_provoz="181" id_pokl="00/2535/CN58" porad_cis="0/2482/IE25"
      dat_trzby="2016-12-07T22:01:00+01:00" celk_trzba="87988.00"
      zakl_nepodl_dph="5922.00" zakl_dan1="-7083.74" dan1="-1487.59"
      zakl_dan2="-7605.28" dan2="-1140.79" zakl_dan3="-7172.54"
      dan3="-717.25" cest_sluz="4267.00" pouzit_zboz1="956.00"
      pouzit_zboz2="424.00" pouzit_zboz3="131.00"
      urceno_cerp_zuct="343.00" cerp_zuct="237.00" rezim="1" />
      <eet:KontrolniKody>
      <eet:pkp digest="SHA256" cipher="RSA2048" encoding="base64">
Ca8sTbURReQjjgcy/znXBKjPOnZof3AxWK5WySpyMrUXF0o7cz1BP6adQzktODKh2d8s
oAhn1R/S07lVDTa/6r9xTuI3NBH/+7YfYz/t92eb5Y6aNvLm6tXfOdE3C94EqmT0SEEz
9rInGXXP1whIKYX7K0HgVrxjdxCFkZF8Lt12XbahhAzJ47LcPxuBZZp6U6wJ2sWI5os3
KY9u/ZchzAUaCec7H56QwkMnu3U3Ftwi/YrxSzQZTmPTpFYKXnYanrFaLDJm+1/yg+VQ
ntoByBM+HeDXigBK+Shaxx+Nd0sSmm1Im4v685BRVdUId+4CobcnSQ3CBsjAhqmIrtWT
GQ==
      </eet:pkp>
      <eet:bkp digest="SHA1" encoding="base16">
            03ec1d0e-6d9f77fb-1d798ccb-f4739666-a4069bc3 </eet:bkp>
      </eet:KontrolniKody>
</eet:Trzba>
```

Dále uvádíme příklad XML elementu <Trzba> zasílaném v ověřovacím módu:

```
<eet:Trzba>
      <eet:Hlavicka
```

```
            uuid_zpravy="e23e5a5a-08d7-4a08-844d-2b6c6b60621d"
            dat_odesl="2016-12-08T21:19:40+01:00"
            prvni_zaslani="true" overeni="true" />
<eet:Data dic_popl="CZ72080043" dic_poverujiciho="CZ00006947"
      id_provoz="181" id_pokl="00/2535/CN58" porad_cis="0/2482/IE25"
      dat_trzby="2016-12-07T22:01:00+01:00" celk_trzba="87988.00"
      zakl_nepodl_dph="5922.00" zakl_dan1="-7083.74" dan1="-1487.59"
      zakl_dan2="-7605.28" dan2="-1140.79" zakl_dan3="-7172.54"
      dan3="-717.25" cest_sluz="4267.00" pouzit_zboz1="956.00"
      pouzit_zboz2="424.00" pouzit_zboz3="131.00"
      urceno_cerp_zuct="343.00" cerp_zuct="237.00" rezim="1" />
      <eet:KontrolniKody>
      <eet:pkp digest="SHA256" cipher="RSA2048" encoding="base64">
Ca8sTbURReQjjgcy/znXBKjPOnZof3AxWK5WySpyMrUXF0o7cz1BP6adQzktODKh2d8s
oAhn1R/S07lVDTa/6r9xTuI3NBH/+7YfYz/t92eb5Y6aNvLm6tXfOdE3C94EqmT0SEEz
9rInGXXP1whIKYX7K0HgVrxjdxCFkZF8Lt12XbahhAzJ47LcPxuBZZp6U6wJ2sWI5os3
KY9u/ZchzAUaCec7H56QwkMnu3U3Ftwi/YrxSzQZTmPTpFYKXnYanrFaLDJm+1/yg+VQ
ntoByBM+HeDXigBK+Shaxx+Nd0sSmm1Im4v685BRVdUId+4CobcnSQ3CBsjAhqmIrtWT
GQ==
      </eet:pkp>
      <eet:bkp digest="SHA1" encoding="base16">
            03ec1d0e-6d9f77fb-1d798ccb-f4739666-a4069bc3 </eet:bkp>
      </eet:KontrolniKody>
</eet:Trzba>
```

3.4 POTVRZOVACÍ DATOVÁ ZPRÁVA

Potvrzovací datová zpráva je SOAP XML struktura obsahující potvrzovací údaje o přijetí evidované tržby společným technickým zařízením správce daně. Potvrzovací data evidované tržby jsou uložena v XML elementu <SOAP Envelope Body>.

V XML elementu <SOAP Envelope Header> bude uložen XML signature a certifikát společného technického zařízení správce daně, k němuž příslušný privátní klíč byl použit k vytvoření XML signature.

Vlastní potvrzení je uloženo v XML elementu <SOAP Envelope Body> jako element <Odpoved>. Tento element obsahuje 2 vnořené elementy, které reprezentují datové oblasti: <Hlavicka> a <Potvrzeni>. Tyto datové oblasti obsahují vlastní datové položky – viz odstavec *3.4.2 Přehled datových položek potvrzení*.

Jednotlivé varianty odpovědi systému EET v závislosti na módu, validitě datové zprávy a cílovém prostředí jsou popsány v tabulce *Tabulka 1: Varianty odpovědi systému EET*.

V případě, že nastane jedna či více propustných chyb (viz odst. *2.2.4 Propustné kontroly (propustné chyby)*, bude potvrzovací datová zpráva doplněna o textová varování a příslušné číselné kódy varování.

3.4.1 XML formát potvrzení

XML formát potvrzení v přehledu:

```
<eet:Odpoved>
      <eet:Hlavicka atributy … />
      <eet:Potvrzeni atributy … />
      <eet:Varovani atributy ... >
            hodnoty ...
      </eet:Varovani>
```

```
    <eet:Varovani          atributy          ...          >
        hodnoty                                           ...
    </eet:Varovani>
    ...
</eet:Odpoved>
```

XML element <Varovani> může být uveden vícekrát pro různá varování. Atributy a hodnoty XML elementů jsou podrobně popsány níže.

3.4.2 Přehled datových položek potvrzení

Datová oblast		Název položky	Povinná	XML jméno)*
Hlavička	1	UUID zprávy	Ano	uuid_zpravy
	2	Datum a čas přijetí zprávy	Ano	dat_prij
	3	Bezpečnostní kód poplatníka	Ano	bkp
Potvrzeni	4	Fiskální identifikační kód	Ano	fik
	5	Příznak neprodukčního prostředí	Ne	test
Varování	6	Kód varování	Ne	kod_varov)**
	7	Textový popis varování	Ne	Varovani)**

)* XML jméno znamená buď jméno XML elementu, nebo XML atributu.

)** XML element <Varovani> s atributem kod_varov se v potvrzovací zprávě může vícekrát opakovat.

3.4.2.1 UUID zprávy (uuid_zpravy)

Je atributem XML elementu <Hlavicka>. Jedná se o UUID datové zprávy evidované tržby, která byla zaslána pokladním zařízením poplatníka – popis viz *3.3.3.1 UUID zprávy*.

3.4.2.2 Datum a čas přijetí zprávy (dat_prij)

Je atributem XML elementu <Hlavicka>. Datum a čas přijetí potvrzované zprávy je okamžik, kdy společné technické zařízení správce daně přijalo datovou zprávu evidované tržby.

Datový formát této položky je identický s formátem data a času odeslání zprávy – viz *3.3.3.2 Datum a čas odeslání zprávy*.

3.4.2.3 Bezpečnostní kód poplatníka (bkp)

Je atributem XML elementu <Hlavicka>. Jedná se o BKP potvrzované datové zprávy evidované tržby, která byla zaslána pokladním zařízením poplatníka – popis viz *3.3.3.14 Bezpečnostní kód poplatníka (bkp)*.

3.4.2.4 Fiskální identifikační kód (fik)

Je atributem XML elementu <Potvrzeni>. Jedná se o fiskální identifikační kód (FIK) generovaný společným technickým zařízením správce daně, který je unikátní pro každou potvrzovanou datovou zprávu evidované tržby, jež byla zaslána pokladním zařízením poplatníka.

Datový formát FIK je následující:

```
uuid_prijem-Id_zarizeni
```

Kde `uuid_prijem` je UUID číslo generované konkrétním zařízením transakčního systému EET, které zprávu přijalo, a `Id_zarizeni` je 2-místné hexadecimální číslo tohoto zařízení.

Maska datového formátu:

```
^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-4[0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}-[0-9a-fA-F]{2}$
```

Délka: 39 znaků.

Příklad:

```
b3a09b52-7c87-4014-a496-4c7a53cf9125-03
```

Pokud je FIK přidělen v neprodukčním prostředí a nejedná se tedy o skutečný FIK dle ZoET, potom mají poslední dva znaky FIK speciální hodnotu ff (mnemotechnická pomůcka: Fiktivní FIK=ff)

Příklad:

```
b3a09b52-7c87-4014-a496-4c7a53cf9125-ff
```

3.4.2.5 Příznak neprodukčního prostředí (test)

Je atributem XML elementu <Potvrzeni>. Je to příznak, kterým společné technické zařízení správce daně informuje pokladní zařízení poplatníka, zda datová zpráva evidované tržby byla zaslána do produkčního nebo neprodukčního prostředí.

Je-li tento příznak uveden a má-li hodnotu *true* (nebo *1*), byla datová zpráva přijata do neprodukčního prostředí – viz *2.2 Módy odesílání datových zpráv, produkční a neprodukční prostředí.*

Není-li tento příznak uveden, byla datová zpráva přijata do produkčního prostředí.

Datový formát je určen příslušnou W3C specifikací, viz: https://www.w3.org/TR/xmlschema11-2/#boolean.

Délka: 1 až 5 znaků.

Příklad:

```
true
```

3.4.2.6 Kód varování (kod_varov)

Je atributem XML elementu <Varovani>. Jedná se o celé max. 3-ciferné kladné dekadické číslo, které dle stanoveného číselníku označuje konkrétní varování.

Maska datového formátu:

```
^[1-9]\d{0,2}$
```

Délka: 1 až 3 znaky.

Příklady:

1

3

3.4.2.7 Textový popis varování (Varovani)

Je hodnotou XML elementu <Varovani>. Jedná se o znakový řetězec, který v českém jazyce stručně popisuje, k jaké propustné chybě při zpracování datové zprávy evidované tržby došlo.

Z důvodu konzistence všech datových zpráv budou povolené znaky v dolní ASCII sadě XML povolených znaků, tj. jejich dekadické kódy budou mít hodnoty 9, 10, 13 nebo od 32 do 126. To znamená, že textový popis chyby nebude používat diakritiku.

Délka: max. 100 znaků.

3.4.3 Příklad potvrzení

V následujícím textu uvádíme příklad XML elementu <Odpoved> z produkčního prostředí, bez propustných chyb:

```
<eet:Odpoved>
      <eet:Hlavicka uuid_zpravy="123e4567-e89b-42d3-a456-
426655440000"
      dat_prij="2017-03-04T18:25:21+01:00"
      bkp="01234567-89abcdef-01234567-89abcdef-01234567" />
      <eet:Potvrzeni fik="987a6be5-6af5-44f3-b4fc-987654321000-02" />
</eet:Odpoved>
```

Dále uvádíme příklad XML elementu <Odpoved> z neprodukčního prostředí, kde odpověď obsahuje varování o propustných chybách:

```
<eet:Odpoved>
      <eet:Hlavicka uuid_zpravy="123e4567-e89b-42d3-a456-
426655440000"
      dat_prij="2017-03-04T18:25:21+01:00"
      bkp="01234567-89abcdef-01234567-89abcdef-01234567" />
      <eet:Potvrzeni fik="987a6be5-6af5-44f3-b4fc-987654321000-03"
      test="true" />
      <eet:Varovani kod_varov="1" >
            DIC poplatnika v datove zprave se neshoduje s DIC
v certifikatu
      </eet:Varovani>
      <eet:Varovani kod_varov="2" >
            Chybny format DIC poverujiciho poplatnika
      </eet:Varovani>
      <eet:Varovani kod_varov="3" >
            Chybna hodnota PKP
      </eet:Varovani>
</eet:Odpoved>
```

3.4.4 Seznam kódů a textů varování

Kód varování	Text varování)*
1	DIC poplatnika v datove zprave se neshoduje s DIC v certifikatu
2	Chybny format DIC poverujiciho poplatnika
3	Chybna hodnota PKP
4	Datum a cas prijeti trzby je novejsi nez datum a cas prijeti zpravy
5	Datum a cas prijeti trzby je vyrazne v minulosti
6 – 999	**)****

)* Texty varování budou v souladu s kódováním znaků ve všech datových zprávách EET uvedeny bez diakritiky – viz *3.1 Kódování datových položek*.

)** Rezervováno pro budoucí použití.

3.5 CHYBOVÁ DATOVÁ ZPRÁVA

Chybová datová zpráva je SOAP XML struktura obsahující chybový kód a textové chybové hlášení o:

1. kritické chybě přijaté datové zprávy evidované tržby nebo
2. dočasné technické chybě zpracování na straně společného technického zařízení správce daně (nutnost odeslat datovou zprávu evidované tržby později).

Data chybové datové zprávy jsou uložena v XML elementu <SOAP Envelope Body> jako element <Odpoved>. Tento element obsahuje 2 vnořené elementy, které reprezentují datové oblasti: <Hlavicka> a <Chyba>. Tyto datové oblasti obsahují vlastní datové položky – viz odstavec *3.5.2 Přehled datových položek chyby*.

V tomto případě <SOAP Envelope> nebude obsahovat ani XML signature ani certifikát.

Jednotlivé varianty odpovědi systému EET v závislosti na módu, validitě datové zprávy a cílovém prostředí jsou popsány v tabulce *Tabulka 1: Varianty odpovědi systému EET*.

V ověřovacím módu v chybové datové zprávě s chybovým kódem 0 (Datovou zpravu evidovane trzby v overovacim modu se podarilo zpracovat) bude v případě, že nastane jedna či více propustných chyb (viz odst. *2.2.4 Propustné kontroly (propustné chyby)*), chybová datová zpráva doplněna o textová varování a příslušné číselné kódy varování stejným způsobem, jako potvrzovací datová zpráva.

3.5.1 XML formát chyby

XML formát chyby v přehledu:

```
<eet:Odpoved>
      <eet:Hlavicka atributy … />
      <eet:Chyba atributy …>
            hodnoty …
      </eet:Chyba>
      <eet:Varovani atributy …>
            hodnoty …
      </eet:Varovani>
</eet:Odpoved>
```

Atributy a hodnoty XML elementů jsou podrobně popsány níže.

3.5.2 Přehled datových položek chyby

Datová oblast		Název položky	Povinná	XML jméno)*
Hlavička	1	UUID zprávy	Ne	uuid_zpravy
	2	Datum a čas odmítnutí zprávy	Ne	dat_odmit
	3	Bezpečnostní kód poplatníka	Ne	bkp
Chyba	4	Chybový kód	Ano	kod
	5	Textový popis chyby	Ano	Chyba
	6	Příznak neprodukčního prostředí	Ne	test
Varování	7	Kód varování	Ne	kod_varov)**
	8	Textový popis varování	Ne	Varovani)**

)* XML jméno znamená buď jméno XML elementu, nebo XML atributu.

)** XML element <Varovani> je relevantní v případě chybové zprávy pouze pro chybový kód 0 („Datovou zpravu evidovane trzby v overovacim modu se podarilo zpracovat“). XML element <Varovani> s atributem kod_varov se v chybové zprávě může vícekrát opakovat.

3.5.2.1 UUID zprávy (uuid_zpravy)

Je atributem XML elementu <Hlavicka>. Jedná se o UUID datové zprávy evidované tržby obsahující chybu, která byla zaslána pokladním zařízením poplatníka – popis viz *3.3.3.1 UUID zprávy*.

3.5.2.2 Datum a čas odmítnutí zprávy (dat_odmit)

Je atributem XML elementu <Hlavicka>. Datum a čas odmítnutí zprávy, která obsahuje chybu, je okamžik zpracování chybné datové zprávy evidované tržby na společném technickém zařízení správce daně.

Datový formát této položky je identický s formátem data a času odeslání zprávy – viz *3.3.3.2 Datum a čas odeslání zprávy*.

3.5.2.3 Bezpečnostní kód poplatníka (bkp)

Je atributem XML elementu < Hlavicka>. Jedná se o BKP tržby obsahující chybu, která byla zaslána pokladním zařízením poplatníka – popis viz *3.3.3.14 Bezpečnostní kód poplatníka (bkp)*.

3.5.2.4 Chybový kód (kod)

Je atributem XML elementu <Chyba>. Jedná se o celé max. 3-ciferné dekadické číslo, které dle stanoveného číselníku označuje konkrétní kritickou chybu. Hodnoty chybového kódu mohou být kladné, nulové nebo záporné.

Maska datového formátu:

```
^-?\d{1,3}$
```

Délka:

- pro nezáporné hodnoty: 1 až 3 znaky, tj. minimální nezáporná hodnota je 0, maximální nezáporná hodnota je 999
- pro záporné hodnoty: 2 až 4 znaky, tj. minimální záporná hodnota je -999, maximální záporná hodnota je -1

Příklady:

10

-1

560

3.5.2.5 Textový popis chyby (Chyba)

Je hodnotou XML elementu <Chyba>. Jedná se o znakový řetězec, který v českém jazyce stručně popisuje, k jaké chybě při zpracování datové zprávy evidované tržby došlo.

Z důvodu konzistence všech datových zpráv budou povolené znaky v dolní ASCII sadě XML povolených znaků, tj. jejich dekadické kódy budou mít hodnoty 9, 10, 13 nebo od 32 do 126. To znamená, že textový popis chyby nebude používat diakritiku.

Délka: max. 100 znaků.

3.5.2.6 Příznak neprodukčního prostředí (test)

Je atributem XML elementu <Chyba>. Je to příznak, kterým společné technické zařízení správce daně informuje pokladní zařízení poplatníka, zda datová zpráva evidované tržby byla zaslána do produkčního nebo neprodukčního prostředí.

Je-li tento příznak uveden a má-li hodnotu *true* (nebo *1*), byla datová zpráva přijata do neprodukčního prostředí – viz *2.2 Módy odesílání datových zpráv, produkční a neprodukční prostředí.*

Není-li tento příznak uveden, byla datová zpráva přijata do produkčního prostředí.

Datový formát je určen příslušnou W3C specifikací, viz: https://www.w3.org/TR/xmlschema11-2/#boolean).

Délka: 1 až 5 znaků.

Příklad:

```
true
```

3.5.3 Příklad chyby

V následujícím textu uvádíme příklady chybové odpovědi ve tvaru XML elementu <Odpoved> obsahujícího informaci o chybě.

Zde jsou příklady odpovědí produkčního prostředí ve tvaru XML elementu <Odpoved> obsahujícího informaci o chybě:

Příklad 1 (datovou zprávu evidované tržby se povedlo analyzovat):

```
<eet:Odpoved>
	<eet:Hlavicka
		uuid_zpravy="123e4567-e89b-42d3-a456-426655440000"
		bkp="01234567-89abcdef-01234567-89abcdef-01234567"
		dat_odmit="2017-03-04T18:25:21+01:00" />
	<eet:Chyba kod="5">
		Neplatny kontrolni bezpecnostni kod poplatnika (BKP)
	</eet:Chyba>
</eet:Odpoved>
```

Příklad 2 (datovou zprávu evidované tržby se nepovedlo analyzovat):

```
<eet:Odpoved>
	<eet:Hlavicka dat_odmit="2017-03-04T18:25:21+01:00" />
	<eet:Chyba kod="3">
		XML zprava nevyhovela kontrole XML schematu
	</eet:Chyba>
</eet:Odpoved>
```

Příklad 3 (technický problém na straně společného zařízení správce daně):

```
<eet:Odpoved>
	<eet:Hlavicka dat_odmit="2017-03-04T18:25:21+01:00" />
	<eet:Chyba kod="-1">
		Docasna technicka chyba zpracovani – odeslete prosim
datovou zpravu pozdeji
	</eet:Chyba>
</eet:Odpoved>
```

Dále uvádíme příklad chybové odpovědi ve tvaru XML elementu <Odpoved> z neprodukčního prostředí:

```
<eet:Odpoved>
      <eet:Hlavicka
            uuid_zpravy="123e4567-e89b-42d3-a456-426655440000"
            bkp="01234567-89abcdef-01234567-89abcdef-01234567"
            dat_odmit="2017-03-04T18:25:21+01:00" />
      <eet:Chyba kod="5" test="true" >
            Neplatny kontrolni bezpecnostni kod poplatnika (BKP)
      </eet:Chyba>
</eet:Odpoved>
```

3.5.4 Seznam chybových kódů a chybových zpráv

Kód	Text chybové zprávy)*
-999 – -2	)**
-1	Docasna technicka chyba zpracovani – odeslete prosim datovou zpravu pozdeji
0	Datovou zpravu evidovane trzby v overovacim modu se podarilo zpracovat
1	)**
2	Kodovani XML neni platne)***
3	XML zprava nevyhovela kontrole XML schematu
4	Neplatny podpis SOAP zpravy
5	Neplatny kontrolni bezpecnostni kod poplatnika (BKP)
6	DIC poplatnika ma chybnou strukturu
7	Datova zprava je prilis velka
8	Datova zprava nebyla zpracovana kvuli technicke chybe nebo chybe dat
9 – 999	**)****

)* Texty chybových zpráv budou v souladu s kódováním znaků ve všech datových zprávách EET uvedeny bez diakritiky – viz *3.1 Kódování datových položek.*

)** Rezervováno pro budoucí použití.

)*** Podle situace je možné na tuto chybu reagovat i navrácením technické chyby, např. tzv. SOAP fault, nebo dokonce ignorováním datové zprávy, pokud je podezření, že se jedná o kybernetický útok.

3.6 ÚDAJE UVÁDĚNÉ NA ÚČTENCE

Údaje uvedené na účtence musí odpovídat údajům uvedeným v datové zprávě zaslané poplatníkem správci daně a v případě fiskálního identifikačního kódu údaji zaslanému v potvrzení správce daně o jejím přijetí. Uspořádání údajů na účtence zákon o evidenci tržeb nestanovuje, nicméně je nutné, aby byly údaje uvedené na účtence čitelné a jednoznačně identifikovatelné. V případě data a času přijetí tržby nebo vystavení účtenky, pokud je vystavena dříve, není nutné uvádět časovou zónu. Datum musí vždy obsahovat rok, měsíc a den, čas pak hodinu, minutu a sekundu.

4 KONTROLNÍ KÓDY PKP A BKP

4.1 PODPISOVÝ KÓD POPLATNÍKA (PKP)

Podpisový kód poplatníka (PKP) je elektronickým podpisem vybraných údajů datové zprávy evidované tržby stanovených finanční správou.

Technicky je PKP elektronický podpis textového řetězce, který je definovaným způsobem vytvořen z vybraných datových položek e-tržby – viz kap. *5 Identifikace evidované tržby - volba položek pro PKP*. Podpis vytváří pokladní zařízení poplatníka pomocí svého privátního klíče. Tento privátní klíč tvoří jednoznačný pár s veřejným klíčem, jenž je součástí X509 certifikátu, který je vložen do SOAP elementu <SOAP Header> datové zprávy. To znamená, že k vytvoření PKP a XML signature datové zprávy musí být použit tentýž privátní klíč – jediná výjimka je v situaci, kdy certifikát klíče použitý v době vydání účtenky (tj. vytvoření PKP a BKP) již není platný v okamžiku odeslání datové zprávy evidované tržby. V tom případě použije poplatník pro vytvoření XML signature aktuálně platný certifikát.

Výpočet PKP v pokladním zařízení poplatníka probíhá v následujících krocích:

1. Podepisovaný text (`plaintext`) se vytvoří textovým zřetězením vybraných položek elementu <Trzba> v kódování ASCII s použitím oddělovače „|“ (ASCII znak s dekadickou hodnotou 124) mezi jednotlivými položkami.
2. Z takto vytvořeného textu `plaintext` se vypočte otisk (hash neboli message digest) algoritmem SHA256 a tento se následně elektronicky podepíše algoritmem RSASSA-PKCS1-v1_5 podle RFC 3447 (přesná definice způsobu výpočtu PKP je uvedena ve vyhlášce č. 269/2016 o způsobu tvorby podpisového kódu poplatníka a bezpečnostního kódu poplatníka: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=35066), s použitím téhož certifikátu a klíče, který bude použit pro elektronický podpis celé datové zprávy. Výsledkem je `rsa_text.`
3. Výsledný podpis `rsa_text` je pak zakódován algoritmem Base64 do textového řetězce `rsa_text_base64,` který je pak do datové zprávy uložen jako hodnota XML elementu <pkp> v elementu <Trzba>. Výsledný textový řetězec má délku 344 znaků.

4.1.1 Příklad výpočtu PKP

Následující kód v jazyku Java ilustruje způsob výpočtu PKP. Pro výpočet PKP jsou použity standardní třídy, které jsou součástí běhového prostředí Java.

```
import java.security.KeyStore;
import java.security.PrivateKey;
import java.security.Signature;
```

Níže uvedený příklad výpočtu PKP pracuje s proměnnými, jejichž naplnění závisí na konkrétním cílovém prostředí (tj. pokladním zařízení poplatníka).

```
KeyStore keystore; // úložiště klíčů obsahující certifikát pro podpis
String alias;      // alias certifikátu v úložišti klíčů
String password;   // heslo k privátnímu klíči certifikátu
```

Dále uvedený příklad výpočtu předpokládá, že proměnná `plaintext` bude naplněna dle popisu uvedeného v kapitole *4.1 Podpisový kód poplatníka (PKP)*.

```
String plaintext;       // podepisovaný text
```

Algoritmus zřetězení položek do podepisovaného textu je záležitostí konkrétní implementace klienta webové služby. Výsledný podepisovaný text bude mít následující tvar (údaje pro uvedený podepisovaný text byly převzaty z příkladu XML elementu <Trzba> v běžném produkčním módu uvedeného v *3.3.4 Příklad e-tržby*):

```
"CZ72080043|181|00/2535/CN58|0/2482/IE25|2016-12-07T22:01:00+01:00|87988.00"
```

Prvním krokem výpočtu je příprava objektu typu `java.security.Signature`, pomocí kterého bude PKP vypočten.

```
Signature signature = Signature.getInstance("SHA256withRSA");
signature.initSign((PrivateKey) keystore
        .getKey(alias, password.toCharArray()));
signature.update(plaintext.getBytes("UTF-8"));
```

V druhém kroku bude proveden samotný výpočet PKP (elektronický podpis).

```
byte[] rsa_text = signature.sign();
```

Proměnná `rsa_text` po provedení funkce `sign()` obsahuje binární data (řetězec oktetů), ze kterých vznikne PKP převodem do Base64 kódování. Konkrétní API funkce pro převod do Base64 kódovaného řetězce znaků závisí na příslušné implementaci klienta webové služby.

4.2 BEZPEČNOSTNÍ KÓD POPLATNÍKA (BKP)

Bezpečnostní kód poplatníka (BKP) je otisk (hash neboli message digest) hodnoty kódu PKP, kde PKP je použit ve formě řetězce oktetů (viz hodnota `rsa_text` výše) algoritmem SHA1. Z této definice je zřejmé, že při znalosti samotného PKP je možné BKP kdykoliv jednoznačně zrekonstruovat.

Přesná definice příslušného algoritmu je uvedena ve vyhlášce 269/2016 o způsobu tvorby podpisového kódu poplatníka a bezpečnostního kódu poplatníka: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=35066).

Popis kroků výpočtu BKP:

1. Je-li k dispozici původní řetězec oktetů `rsa_text`, postupujeme rovnou krokem 2 níže; je-li k dispozici PKP (tj. řetězec znaků v kódování Base64): `rsa_text_base64`, je nutné napřed provést dekódování na řetězec oktetů `rsa_text`
2. Z řetězce oktetů `rsa_text` se vytvoří otisk (hash neboli message digest) pomocí algoritmu SHA1. Tím vznikne řetězec oktetů `hash_sha1` o délce 160 bitů (tj. 20 bajtů).
3. Řetězec oktetů `hash_sha1` je pak zakódován hexadecimálně do textového řetězce `hash_sha1_base16`.
4. Textový řetězec `hash_sha1_base16` je následně upraven do cílového tvaru tak, že se mezi následující číslice zápisu hodnoty v šestnáctkové soustavě:
   8. a 9.
   16. a 17.
   24. a 25.
   32. a 33.
   vloží znak pomlčky (znak "-" s dekadickým kódem 45 v ASCII znakové sadě), tj. 40 hexadecimálních číslic BKP je rozděleno do 5-ti bloků po osmi číslicích oddělených znakem pomlčky.

Takto upravený textový řetězec je pak do datové zprávy uložen jako hodnota XML elementu <bkp> v elementu <Trzba>. Výsledný textový řetězec má délku 44 znaků.

5 IDENTIFIKACE EVIDOVANÉ TRŽBY - VOLBA POLOŽEK PRO PKP

Evidovaná tržba bude jednoznačně identifikována hodnotami základních datových položek XML elementu <Data> e-tržby, které jsou uvedeny v této tabulce:

Datová oblast		Název položky – základní	Povinná	XML jméno
Data	5	DIČ poplatníka	Ano	dic_popl
	7	Označení provozovny	Ano	id_provoz
	8	Označení pokladního zařízení	Ano	id_pokl
	9	Pořadové číslo účtenky	Ano	porad_cis
	10	Datum a čas přijetí tržby	Ano	dat_trzby
	11	Celková částka tržby	Ano	celk_trzba

Výchozí podepisovaný text (`plaintext`) pro výpočet PKP vznikne zřetězením výše uvedených položek datové zprávy evidované tržby v uvedeném pořadí v kódování ASCII s použitím oddělovače „|“ (ASCII znak s dekadickou hodnotou 124) mezi jednotlivými položkami.

Příklad:

Nechť příslušné hodnoty výše uvedených položek jsou následující:

	Název položky -základní	XML jméno	Hodnota
5	DIČ poplatníka	dic_popl	`CZ72080043`
7	Označení provozovny	id_provoz	`243`
8	Označení pokladního zařízení	id_pokl	`24/A-6/Brno_2`
9	Pořadové číslo účtenky	porad_cis	`#135433c/11/2016`
10	Datum a čas přijetí tržby	dat_trzby	`2016-12-09T16:45:36+01:00`
11	Celková částka tržby	celk_trzba	`3264.00`

Potom text (`plaintext`), z něhož bude spočítán PKP, bude mít hodnotu:

```
CZ72080043|243|24/A-6/Brno_2|#135433c/11/2016|2016-12-
09T16:45:36+01:00|3264.00
```

Bude-li přijata datová zpráva evidované tržby se stejnými hodnotami základních datových položek jako některá již dříve přijatá zpráva, bude nová zpráva považována za zaslání údajů o téže evidované tržbě.

6 UPŘESNĚNÍ XML ZPRÁVY VE TVARU SOAP A JEJÍ ZABEZPEČENÍ

Rozhraní webové služby je formálně definováno formou WSDL (Web Services Description Language). WSDL dokument odkazuje na příslušný dokument XML Schema, který popisuje vlastní XML strukturu e-tržby. XML struktura e-tržby bude jediným obsahem SOAP elementu <soap:Body>.

Soubory XML schema a WSDL jsou přílohou tohoto dokumentu.

Zabezpečení webové služby je realizováno v souladu se standardem Web Services Security (WSS) v následujících oblastech.

6.1 ŠIFROVÁNÍ KOMUNIKACE PROTOKOLEM HTTPS

Společné technické zařízení správce daně bude vybaveno SSL certifikátem serveru. Pokladní zařízení musí v rámci navázání spojení SSL spojení (SSL handshake) se společným technickým zařízením povinně kontrolovat platnost SSL certifikátu serveru, zda byl vystaven důvěryhodnou autoritou a zda se shoduje jméno, na které byl vydán, s adresou společného technického zařízení.

Autentizace klienta SSL (tedy pokladního zařízení) není v rámci navázání SSL spojení požadována.

6.2 PODPIS DATOVÝCH ZPRÁV EVIDOVANÝCH TRŽEB

Každá datová zpráva evidované tržby musí být povinně podepsána klíčem, k němuž je vydán X509 certifikát poplatníka. Certifikát poplatníka musí být platný k okamžiku zpracování datové zprávy evidované tržby na straně společného technického zařízení správce daně.

Kromě situace, která je popsána v odst. *4.1 Podpisový kód poplatníka (PKP)*, platí, že klíč a certifikát použitý pro elektronický podpis datové zprávy musí být shodný s klíčem a certifikátem použitým pro výpočet kódu PKP. Do elektronického podpisu SOAP zprávy musí být zahrnut právě jeden element, a to element <soap:Body> obsahující XML strukturu e-tržby (element <eet:Trzba>) sestavený dle platného XML Schema (XSD). Elektronický podpis musí být realizován dle standardu XML Signature Syntax and Processing (Second Edition) s následujícími požadavky:

- Pro realizaci elektronického podpisu zprávy je využito standardu WS-Security 1.0 a XML Digital Signature
- Vlastní digitální podpis musí být vložen do SOAP obálky datové zprávy a to v sekci hlaviček WS-Security. Odkaz na podepisovaný objekt (element <soap:Body>) je realizován referencí s využitím relativního odkazu v rámci SOAP zprávy.
- Je požadován algoritmus „Exclusive C14N“ kanonizace podepisovaného objektu (Exclusive XML Canonicalization Version 1.0, https://www.w3.org/TR/xml-exc-c14n/)
- Pro výpočet otisku (digest) podepisovaného objektu (element <soap:Body>) pro elektronický podpis SOAP zprávy je požadován hashovací algoritmus SHA256 (http://www.w3.org/2001/04/xmlenc#sha256)
- Pro elektronický podpis SOAP zprávy je požadován algoritmus RSA-SHA256 (http://www.w3.org/2001/04/xmldsig-more#rsa-sha256)
- X509 certifikát náležející k privátnímu klíči použitému pro realizaci elektronického podpisu datové zprávy evidované tržby včetně SOAP obálky musí být přiložen v elementu BinarySecurityToken v rámci sekce WS-Security hlavičky SOAP zprávy (typ http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary) ve formátu X509v3 (typ http://docs.oasis-open.org/wss/2004/01/oasis-

200401-wss-x509-token-profile-1.0#X509v3). Z digitálního podpisu je tento certifikát standardními prostředky referencován.

Datová zpráva by neměla obsahovat další hlavičky (jako např. Timestamp a WS-Addressing) a neměly by být podepisovány jiné elementy než <soap:Body>. V opačném případě roste velikost datové zprávy a takové zprávy by mohly být považovány za útok a následně odmítány.

Příklad očekávané struktury datové zprávy je zachycen na následujícím obrázku:

6.3 ELEKTRONICKÝ PODPIS POTVRZOVACÍCH DATOVÝCH ZPRÁV

Potvrzovací datové zprávy ve formátu SOAP budou opatřeny elektronickým podpisem společného technického zařízení správce daně.