Specifikace projektu

Elektronická evidence tržeb

Verze: 1.22

Únor 2015 /dílčí revize MF 01-2016/

Tento dokument obsahuje 185 stran.

Obsah

Manažerské shrnutí ... 9
Cíle projektu ... 9
Principy projektu ... 9
Koncepční popis projektu ... 10
Základní finanční ukazatele ... 11
PR vnímání a koncept ... 12
Úvod ... 14
Účel dokumentu ... 14
Metodologie a přístup ... 14
Potřeba zpracování dokumentu ... 15
Omezení zpracování dokumentu ... 15
Specifikace projektu ... 16
Účel a cíle projektu ... 16
Výchozí situace ... 16
Kvantitativní odhad objemu transakcí ... 17
Legislativní východiska ... 20
Základní procesy evidence tržeb ... 23
Registrace a evidence údajů a certifikátů o povinném subjektu ... 24
„Registrace“ poplatníka ... 26
Ověření poplatníka ... 32
Změny údajů poplatníka ... 35
Ukončení evidence (deaktivace) poplatníka ... 35
„Registrace“ provozovny ... 36
Změny údajů provozovny ... 37
Zrušení provozovny ... 38
Evidence tržeb ... 39
Procesy Evidence tržeb ... 45
Dávková evidence tržeb ... 50
Přístup poplatníka k vlastním agregovaným údajům ... 51
Kontrola účtenky zákazníkem ... 55
Nahlášení neobdržené účtenky zákazníkem ... 60
Kontrola ze strany FS a CS ... 65
Specifikace ochranných prvků EET ... 70
Technické a technologické řešení projektu ... 79
Logická architektura aplikace ... 80
Metriky systému ... 83
Požadované provozní a SLA parametry ... 84

Specifikace provedení detailní analýzy ... 87
Funkční dekompozice ... 91
Komponenty Projektu EET ... 91
Certifikační autorita ... 95
Požadavky na hardwarové prvky prostředí ... 106
Předběžný rozpočet systému EET a infrastruktury ... 118
Řešení procesu správy a provozu služeb ... 121
Řešení bezpečnosti systému EET ... 123
Požadavky na monitoring a prostředí datových sálů pro systém EET ... 137
Specifikace požadavků na testování systému ... 142
Požadovaná architektura připojení do Internetu pro systém EET ... 144
Analýza rizik ... 151
Identifikace rizik ... 151
Hodnocení rizik ... 153
Mapa rizik ... 156
Eliminace rizik ... 157
Projektové řízení a projektový tým ... 160
Organizace Projektu ... 161
Orgány projektu ... 161
Řídící komise a sponzor Projektu ... 162
Seznam projektových rolí a jejich základní specifikace: ... 162
Kompetence jednotlivých projektových týmů ... 163
Řízení Projektu ... 167
Řízení rizik ... 167
Řízení dodavatelů ... 167
Řízení problémů ... 168
Principy akceptace ... 168
Reporting a monitoring ... 169
Komunikace v rámci projektu ... 169
Schvalování výstupů ... 170
Řízení kvality ... 170
Ověřování výstupů projektu ... 172
Správa a dokumentace projektu ... 172
Účtenková loterie ... 175
Harmonogram projektu ... 177
Analýza přínosů a nákladů ... 178
Přínosy ... 178
Identifikace přínosů ... 178
Náklady ... 180

Návratnost projektu v čase 183
Přílohy 184
Příloha č. 1 – Návrh obsahu datové věty účtenky 184

Seznam obrázků

Obrázek 1: Rozložení transakcí v týdnu ... 18
Obrázek 2: Průměr počtu transakcí za sekundu ... 18
Obrázek 3: Základní procesy evidence tržeb ... 23
Obrázek 4: Případy užití poplatníka ... 25
Obrázek 5: Případy užití Czech POINTu ... 26
Obrázek 6: Proces registrace poplatníka a jeho provozoven do EET ... 31
Obrázek 7: Proces ověření poplatníka ... 33
Obrázek 8: Evidence tržeb - základní proces zaevidování tržby pokladníkem ... 47
Obrázek 9: Evidence tržeb - zaevidování tržby v době 48 hodin po vystavení účtenky (v případě zjednodušeného režimu 120 hodin) pokladníkem ... 48
Obrázek 10: Evidence tržeb - zaevidování tržby v době 48 hodin po vystavení účtenky (v případě zjednodušeného režimu 120 hodin) automatizovaně na straně koncového zařízení ... 49
Obrázek 11 Zobrazení agregovaných dat ... 53
Obrázek 12: Kontrola účtenky zákazníkem ... 58
Obrázek 13: Proces nevydané účtenky zákazníkovi ... 63
Obrázek 14: Proces kontrolní nákup ... 68
Obrázek 15: Logická architektura EET ... 80
Obrázek 16: Vazby komunikačních a ostatních informačních systémů na systém EET a okolí ... 89
Obrázek 17: Funkční dekompozice EET ... 91
Obrázek 18: Enterprise Service Bus ... 94
Obrázek 19: Blokové schéma CA EET ... 95
Obrázek 20: Řešení CA EET ... 96
Obrázek 21: Požadované použití rozhraní CA ... 100
Obrázek 22: Procesy probíhající v Interní Certifikační Autoritě ... 100
Obrázek 23: minimální požadavek na síťovou konfiguraci CA EET ... 102
Obrázek 24: Základní schéma zón systému EET ... 107
Obrázek 25: Schéma logické komunikační infrastruktury systému EET ... 108
Obrázek 26: Schéma aplikační a databázové vrstvy Varianty 1 ... 115
Obrázek 27:Schéma aplikační a databázové vrstvy Varianty 2 ... 116
Obrázek 28: Pojetí řešení procesu správy a provozu služeb ... 121
Obrázek 29: Schéma bezpečnostních činností a související dokumentace ... 124
Obrázek 30: Schéma etapy 1 řešení bezpečnosti Systému EET ... 126
Obrázek 31: Schéma etapy 2 řešení bezpečnosti Systému EET ... 131
Obrázek 32: Schéma etapy 3 řešení bezpečnosti Systému EET ... 135
Obrázek 33: Monitoring systému EET ... 138
Obrázek 34 : Schéma zapojení s použitím adres více ISP ... 144
Obrázek 35 : Schéma přístupu POSu k serverům ... 145
Obrázek 36 : Schéma zapojení pouze s IP adresami jednoho z ISP ... 145
Obrázek 37 : Schéma zapojení s použitím směrovacího protokolu BGP ... 146
Obrázek 38 : Schéma toku dat za normálního stavu sítě ... 146
Obrázek 39 : Schéma toku dat při výpadku linky k ISP ... 147
Obrázek 40 : Schéma toku dat při výpadku zahraniční konektivity ISP ... 148
Obrázek 41 : Schéma zapojení s vlastním AS ... 149
Obrázek 42 : Schéma toku dat za normálního stavu sítě ... 149
Obrázek 43 : Schéma toku dat při výpadku linky k ISP ... 150
Obrázek 44 : Schéma toku dat při výpadku zahraniční konektivity ISP ... 150
Obrázek 45: Organizační struktura projektu ... 161
Obrázek 46: Roční náklady na projekt a výnosy z projektu v čase ... 183
Obrázek 47: Kumulativní náklady na projekt a výnosy z projektu v čase ... 183

Pojmy a zkratky

pojem	význam	ust. ZoET
A		
autentizační údaje	údaje sloužící k ověření identity účastníka pro komunikaci se serverem EET, jedná se o údaje, na jejichž základě je systém EET schopen bezpečně rozeznat poplatníka, který se jimi identifikuje jedná se o přihlašovací údaje a certifikát	ČÁST DRUHÁ Hlava II, Díl 1 § 6 - § 9
B		
běžný režim	viz evidence tržeb běžným způsobem	
BKP	„bezpečnostní kód poplatníka“ vytvořený poplatníkem, který prokazuje jednoznačnou vazbu mezi poplatníkem a účtenkou	ČÁST DRUHÁ Hlava II, Díl 3 § 12
C		
D		
datová zpráva/datová věta	specificky definovaný způsob elektronické komunikace mezi pokladním zařízením poplatníka a serverem EET obsahuje údaje stanovené ZoET a prováděcím předpisem	ČÁST DRUHÁ Hlava II, Díl 3 § 11 odst. 1 písm. a)
DIČ	daňové identifikační číslo slouží k identifikaci účastníka při styku se správcem daně	ČÁST DRUHÁ Hlava II, Díl 2 § 10
E		
EET	„elektronická evidence tržeb“ pojem běžně užívaný	
IS EET	Informační systém elektronické evidence tržeb	
ET	„evidence tržeb“ pojem z legislativy	název
evidence tržeb běžným způsobem	evidenční povinnost, tj. odeslat nejpozději při uskutečnění transakce on-line datovou zprávu a vydat účtenku o transakci	ČÁST DRUHÁ Hlava II, Díl 3 § 11
evidenční povinnost	kumulativní povinnost zaslat datovou zprávou/datovou větou údaje o této tržbě systému EET (správci daně) a vydat účtenku tomu, od koho evidovaná tržba plyne	ČÁST DRUHÁ Hlava II, Díl 3 § 11
evidenční povinnost ve zjednodušeném režimu	Taková evidenční povinnost, kdy povinnost odeslat systému EET (správci daně) datovou zprávu/datovou větu nemusí být splněna v okamžiku uskutečnění transakce, nýbrž nejpozději do 5 dnů od uskutečnění tržby	ČÁST DRUHÁ Hlava II, Díl 3 Oddíl 3 § 16
evidovaná tržba	platba poplatníkovi, která je provedena stanoveným způsobem úhrady („hotovostí“) a zároveň se jedná o příjem z podnikání (resp. ze samostatné činnosti), který je předmětem daně z příjmů, není nahodilý, nepodléhá dani vybírané srážkou podle zvláštní sazby daně druhy: - platba hotovostí (bankovky, mince) - platba poukázkou, směnkou, šekem - platba uskutečněná plátcem prostřednictvím příjemce (typicky platba kartou)	ČÁST DRUHÁ Hlava I § 4
F		
FIK	„fiskální identifikační kód“ identifikátor vytvořený systémem finanční správy na základě obdržené datové zprávy poplatníka, prokazuje zaevidování tržby v systému EET	ČÁST DRUHÁ Hlava II, Díl 3 § 1 odst. 2 písm. c)
G		
GFŘ	Generální finanční ředitelství	
GŘC	Celní správa České republiky	

H		
I		
informační oznámení	informuje v pokladním místě na viditelném místě o tom, že osoba, od které plyne tržba, je povinna převzít účtenku	ČÁST TŘETÍ § 20 odst. 1
informační povinnost	povinnost vyvěsit informační oznámení za podmínek a s náležitostmi stanovenými zákonem a prováděcím předpisem	ČÁST TŘETÍ
ISMS	Systém řízení bezpečnosti informací	
J		
K		
koncové zařízení	Informační systém nebo elektronické zařízení poplatníka, které zasílá datové věty a přijímá FIK	
kontrolní nákup	nákup zboží nebo služeb za účelem zjištění plnění povinností poplatníkem	ČÁST DRUHÁ Hlava IV § 19
L		
M		
mezní doba odezvy	časový úsek mezi pokusem o odeslání údajů o evidované tržbě z pokladního (koncového) zařízení a přijetím FIK na zařízení stanoví poplatník tak, aby nemařil průběh evidence tržeb se zohledněním druhu a kvality internetového připojení při stanovení musí poplatník zohlednit čas na zpracování odezvy v systému EET v délce 2 s	ČÁST DRUHÁ Hlava II, Díl 3 Oddíl 2 § 15
MFČR	Ministerstvo financí České republiky	
N		
O		
ověření účtenky	právo osoby disponující údaji z účtenky způsobem umožňujícím dálkový přístup ověřit, zda byla konkrétní účtenka vydána k tržbě evidované v evidenci tržeb a zda poplatník eviduje tržby ve zjednodušeném režimu	ČÁST DRUHÁ Hlava III § 18
oznamovací povinnost	povinnost oznámit změnu v údajích, které jsou součástí žádosti o autentizační údaje	ČÁST DRUHÁ Hlava II, Díl 2 § 9
P		
pokladna, pokladní zařízení	Viz koncové zařízení	
pokladní místo	místo v provozovně, kde se evidované tržby přijímají „běžně“ (je umístěno pokladní (koncové) zařízení)	ČÁST TŘETÍ § 20 odst. 3
povolovací řízení	směřuje k vydání povolení plnit evidenční povinnost ve zjednodušeném režimu u určitých typů tržby rozhoduje správce daně na návrh poplatníka	ČÁST ČTVRTÁ
provozovna	místo, na kterém dochází k provozování činnosti, a které je účelové pro daný subjekt; vychází ze zákona č. 455/1991 Sb., živnostenský zákon, ve znění pozdějších předpisů (dále jen „živnostenský zákon“), kde je stanoveno, že provozovnou se pro účely zákona rozumí prostor, v němž je živnost provozována za provozovnu je považován taktéž automat nebo obdobné zařízení sloužící k prodeji zboží nebo poskytování služeb a mobilní provozovna	DZ, Zvláštní část, k § 35
překročení mezní doby odezvy	situace, kdy v důsledku technické závady, či dočasného výpadku připojení, prostého zhoršení úrovně přenosu, atp. poplatník neobdrží v jím stanovené lhůtě uběhlé od uskutečnění pokusu o odeslání údajů FIK a proto na jeho straně v daném případě není možné provést evidenci tržeb „on-line“ a poplatník má právo vydat účtenku bez FIK	ČÁST DRUHÁ Hlava II, Díl 3 Oddíl 2 § 14

původce tržby	ten, kdo poskytuje tržbu - uhradil platbu za obdržené zboží nebo poskytnuté služby, zjednodušeně zákazník	ČÁST DRUHÁ Hlava III § 17
R		
registrační pokladna	certifikované zařízení opatřené fiskální pamětí, (pozn. není záměrem projektu EET evidovat tržby pouze prostřednictvím těchto zařízení)	
S		
SPCS	Státní pokladna centrum sdílených služeb, s. p.	
T		
U		
účtenka	doklad o transakci splňující náležitosti stanovené ZoET a prováděcím předpisem	ČÁST DRUHÁ Hlava II, Díl 3 Oddíl 1 § 13
účtenková loterie	hra, které se lze účastnit pouze na základě zaslání účtenek, doplňkové opatření jako pozitivní motivace příjemců účtenek	ČÁST SEDMÁ Hlava I § 41
V		
W		
X		
Y		
Z		
zjednodušený režim evidence	viz evidenční povinnost ve zjednodušeném režimu	
ZoET	zákon o evidenci tržeb	

Manažerské shrnutí

V EU dochází každoročně v důsledku daňových podvodů, daňových úniků, vyhýbání se daňovým povinnostem a agresivního daňového plánování ke skandální ztrátě potenciálního daňového příjmu v odhadované výši 1 bilionu EUR, což představuje přibližně 2 000 EUR na každého evropského občana za rok. Česká republika není v tomto výjimkou.

Hlavní cíl téměř všech členských států EU je řešení daňového deficitu. Je cestou k postupnému vytváření podstatně vyšších příjmů z daní bez nutnosti zvyšování jejich sazeb.

Evropský parlament vyzval členské státy, aby vyčlenily odpovídající lidské zdroje, odborné poradenství a rozpočtové prostředky pro své vnitrostátní systémy daňové správy a pro pracovníky provádějící daňové audity a také zdroje pro odbornou přípravu zaměstnanců daňové správy v oblasti přeshraniční spolupráce týkající se daňových podvodů a vyhýbání se daňovým povinnostem a aby zavedly účinné protikorupční nástroje[1].

Dále EP vybídl členské státy k vyhledávání „podezřelých“ údajů o daňových únicích z dalších registrů vedených státní správou, jako jsou databáze motorových vozidel, pozemků, jachet a dalších hmotných statků, a ke sdílení těchto údajů s ostatními členskými státy a Komisí.

Řešení daňového deficitu je jednou z priorit Vlády ČR obsažené v rámci programového prohlášení vlády ČR.

Jedná se mimo jiné o navržení legislativních a technických opatření směřujících k efektivní kontrole vykazovaných tržeb z maloobchodního prodeje zboží a služeb. Tato opatření zahrnou u vybraných subjektů online hlášení tržeb, povinnost vystavovat doklady s unikátním číslem a „účtenkovou loterii“ – tato opatření lze shrnout pod pojem Elektronická evidence tržeb.

Cíle projektu

- Narovnání podnikatelského prostředí v České republice prostřednictvím eliminace nekalé konkurenční výhody subjektů, které krátí daňovou povinnost prostřednictvím nevykazování plné výše tržeb v rámci podnikatelské činnosti při prodeji zboží a služeb.
- Získání dodatečného výnosu daní a pojistných od subjektů, které tyto povinnosti krátí prostřednictvím nevykazování plné výše tržeb.

Principy projektu

- Otevřené řešení bez omezení z pohledu použitého hardware a software, neexistence povinné certifikace
- Jednoduchost a rychlost zavedení, fungování v režimu 24/7
- Minimalizace administrativní zátěže a nákladů podnikatelů
- Minimalizace zpomalení či omezení podnikání v konkrétním oboru
- Minimalizace nákladů státu, nikoliv však na úkor administrativní zátěže či nákladů podnikatelů
- Zapojení veřejnosti
- Pozitivní vnímání ze strany veřejnosti i podnikatelů
- Vnímání projektu EET jako součást širší iniciativy zaměřené k narovnání podnikatelského prostředí a zlepšení daňové disciplíny

[1] Zpráva o boji proti daňovým podvodům, daňovým únikům a daňovým rájům 3. května 2013 (2013/2060(INI)

Koncepční popis projektu

1. Hotovostní tržby za prodej zboží a služeb budou podléhat elektronické evidenci.
2. Příjemce tržby bude povinen tržbu [v reálném čase] elektronicky předem definovaným způsobem nahlásit finanční správě.
3. Finanční správa z nově vybudovaného IT systému EET vygeneruje unikátní kód a odešle ho zpět příjemci tržby.
4. Příjemce tržby má povinnost tento kód uvést na dokladu vystaveném zákazníkovi.
5. Budou existovat řešení pro případ dočasné nemožnosti spojení i trvalé evidence v off-line režimu
6. Doklad bude možné využít pro „účtenkovou loterii“ a jeho kontrolu bude moci přes internet provést i zákazník.
7. Za hotovostní tržby se považují i platby platebními kartami, poukázkami a obdobnými prostředky.
8. Příjemce tržby bude mít možnost ověřit si rozsah tržeb zaevidovaných pod jeho identitou.
9. Příjemcům tržeb i dodavatelům SW/HW řešení bude k dispozici testovací prostředí a podpůrná hot line, a to v dostatečném předstihu před spuštěním povinné evidence tržeb i po celou dobu existence povinné evidence tržeb.

Základní finanční ukazatele

Přínosy

Očekává se, že projekt EET přinese ročně až **10 – 15 mld. Kč**. Tento předpoklad vychází z následujících odhadů:

Náklady

Jednorázové kapitálové investice se očekávají v rozmezí **od 317 mil. Kč do 331 mil. Kč** v návaznosti na zvolené řešení, která jsou uvedena v tabulce

Název položky	IBM	ORACLE	MICROSOFT
Hardware	96	86	125
Software	102	115	62
Vývoj SW	32	32	32
Bezpečnost	15	15	15
PR	21	21	21
Školení	3	3	3
Certifikace subjektů	15	15	15
Call centrum	5	5	5
Implementace projektu	8	8	8
Ostatní	31	31	31
CELKEM v mil. Kč	**328**	**331**	**317**

Roční provozní náklady se odhadují v rozmezí **od 390 mil. Kč do 396 mil. Kč** v návaznosti na zvolenou variantu. Jednotlivé varianty řešení jsou zobrazeny v následující tabulce

Název položky	IBM	ORACLE	MICROSOFT
Mzdové náklady	199	199	199
Údržba hardware	79	80	75
Call centrum	34	34	34
Kontrolní nákupy	30	30	30
PR	3	3	3
Údržba software	7	7	7
Housing	7	7	7
Ostatní	36	36	35
CELKEM v mil. Kč	**395**	**396**	**390**

Legenda:

Software: nastavení systémů ČP, procesní ICT, úpravy ADIS, aplikace EET

Ostatní investiční: auta, mobilní kanceláře, výstroj, technické prostředky, vybavení kanceláří, výzbroj, znalecké posudky, správní poplatky, osobní vozidla, mzdové náklady, poradenství

Ostatní provozní: obnova a provoz vozidel, obnova výstroje, obnova technických prostředků, nájmy, vybavení pracovišť

PR vnímání a koncept

Projekt EET bude vyvolávat velkou pozornost veřejnosti. Hladký průběh implementace ovlivní vnímání veřejností. Proto komunikace projektu počítá s aktivními media relations, informační kampaní ATL, spoluprací s oborovými svazy a opinion makery a informační podporou pro daňové subjekty (Call centrum). Těžištěm komunikace v první fázi je obhájení projektu – jeho smyslu (primárním cílem je narovnání podmínek férové soutěže a tržního prostředí v České republice). Druhá fáze začíná krátce před možností daňových subjektů se registrovat do systému a bude zaměřena na awarness a informační podporu hladkého startu systému. Veškerá komunikace se bude snažit přirozeným a nenásilným způsobem přesvědčit občany, že vyžadování placení daní je pro ně přínosné a využívání cest jak „ušetřit“ díky krácení daní v konečném důsledku poškodí životní komfort každého občana České republiky. Komunikační tým počítá i s krizovým komunikačním scénářem při selhání systému.

Externality

Komunikace projektu počítá s využitím většiny dostupných komunikačních kanálů

Media relations

systematická práce s medii. Tiskové konference, tiskové zprávy, autorské komentáře představitelů resortu, využívání třetích stran, vystoupení představitelů resortu v elektronických mediích, příprava podkladů pro autory zabývající se problematikou EET, reakce na kritické nebo zavádějící materiály.

ATL

tisková reklama, omezeně outdoor, TV a rozhlasová reklama na základě dohody s veřejnoprávními medii.

Elektronická media

www stránky projektu, bannerová reklama, reklama na FB. S ohledem na nízkou míru kontroly neuvažujeme s vlastní FB, Twitter stránkami projektu.

Spolupráce s významnými svazy

využití komunikačních kanálů významných profesních a oborových svazů (Horeka, SOCR, AMSP, Hospodářská komora ad.)

Informační linka/Call centrum

zajištění dvousměnného informačního servisu pro daňové subjekty.

Vytvoření značky/jména projektu

Testováním navrhovaných názvů ve dvou focus groups jsme dospěli ke značce **e-tržby.** S tímto názvem se bude operovat ve veškeré komunikaci.

Součástí komunikačního konceptu je i maximální využití 15 tisíc zaměstnanců resortu financí jako ambasadorů projektu. Proto počítáme s kontinuání interní komunikací na všechny zaměstnance resortu, a to formou newsletteru a podkladů a prezentací určených pro vedoucí pracovníky (ke kaskádování do organizace).

Termín spuštění 1. 1. 2016 může být ohrožen kvůli následujícím aspektům:

a) Způsob zadání a z toho vyplývající délka dodání jednotlivých částí systému EET
b) Způsob zadání a z toho vyplývající délka dodání hardware (platformy) pro systém EET
c) Realizace a zaškolení „front office“ činností (FÚ, Česká Pošta, Czechpointy)
d) Nezbytná doba potřebná na úpravu stávajících pokladních systémů (odhadovaná doba 5-6 měsíců)

e) Neexistence prověrky SPCSS na stupeň utajení “Důvěrné“, které požaduje NBÚ na dodavatele

Úvod

Ministerstvo financí České republiky jako ústřední orgán státní správy zodpovědné za koordinaci Finanční správy. Finanční správa ČR je zřízena zákonem č. 456/2011 Sb., o Finanční správě České republiky, ve znění pozdějších předpisů (dále jen „zákon č. 456/2011 Sb.“) a je tvořena soustavou orgánů finanční správy, které jsou podřízené Ministerstvu financí. Klíčovou součástí kompetence Finanční správy ČR je správa daní, ale zároveň vykonává široké spektrum dalších agend.

Ministerstvo financí ČR má zájem ve spolupráci s GFŘ pro zlepšení podnikatelského prostředí a zvýšení efektivity fungování Finanční správy a kontrolních mechanismů plnění daňových povinností zavést elektronickou evidenci tržeb (dále i jako EET) a evidovat příjem a výdej jednotlivých plateb ve formě bankovek a mincí nebo prostřednictvím elektronického platebního prostředku, ceniny nebo šeku. Tuto snahu projevilo i předložením návrhu zákona o evidenci tržeb.

Hlavním cílem evidence tržeb z pohledu finanční správy je získání informací, které zabezpečí lepší správu daní (zejména daní z příjmů a daně z přidané hodnoty). Základním cílem je narovnání podnikatelského prostředí tak, aby se minimalizovala konkurenční nevýhoda poctivých podnikatelů způsobená krácením daňových povinností ostatními daňovými subjekty.

Na základě zkoumání existujících modelů evidování transakcí, byl shledán jako nejvhodnější systém evidence tržeb, který v maximální možné míře preferuje kritérium jednoduchosti a nízké nákladovosti na straně povinných subjektů při zajištění spolehlivého a plnohodnotného plnění předpokládané funkce.

Cílem aktivit směřujících k vytvoření tohoto dokumentu bylo pochopit kvalitativní ale i kvantitativní rozměr projektu a specifikovat základní charakteristiky projektu ale i technického řešení.

Účel dokumentu

Účelem dokumentu je analyzovat východiskovou situaci a aspekty ovlivňující projekt EET a navrhnou způsob řešení, resp. specifikovat projekt.

Kromě projektových aspektů jako jsou rizika, organizační zabezpečení apod., obsahuje dokument i návrh základních principů řešení a jeho specifikací.

Dokument bude sloužit jako část zadávací dokumentace anebo dokumentace potřebné pro přípravu projektu.

Metodologie a přístup

Pro oblast analýz byly využity následující metodologie:

- Analýza požadavků
- Projektové řízení (část analýzy východiska projektů)
- Řízení a správa rizik
- Rešerše technologických trendů
- Řízení přínosů (Benefit Management).

Pro oblast specifikace projektu byly využity následující metodologie:

- Projektové řízení (část, plánování projektu)
- Řízení organizačních změn
- Řízení změn procesů.

Přístup byl zvolen minimalistický, tj. realizace minimálně nutného rozsahu pro identifikaci nejvýznamnějších vlivů na projekt, při zachování konzistentnosti a kvalitativní úrovně i možnosti dalšího rozvoje projektu podle budoucích potřeb.

Shodně byl i v návrhové části, v specifikaci projektu, zvolen minimalistický přístup a jsou uváděny jenom významné charakteristiky či aspekty projektu. Jsou však zahrnuty všechny charakteristiky a aspekty, které jsou klíčové pro naplnění cílů projektu a pro fungování systému v požadovaném rozsahu.

Minimalistický přístup by zvolen z důvodů realizace dalších analýz za účelem větší detailizace a podrobnější specifikace v následujících fázích projektu, např. v průběhu specifikace technického řešení realizátorem, nastavení plánu projektu projektovým týmem, následné legislativy atd.

Potřeba zpracování dokumentu

Specifikace projektu této úrovně je potřebná pro realizaci dalších kroků v přípravě projektu, realizaci obstarání či k vytvoření podzákonné legislativy – vyhlášek Ministerstva financí ČR.

Omezení zpracování dokumentu

Omezení zpracování dokumentu byli zejména:

- Omezení časem. Z časových důvodů nebylo možné vykonat některé podrobné zkoumání, např. ověření odhadů materializovaných přínosů, či odhad přijetí projektu okolím projektu, zejména veřejností.
- Omezení dostupností informací. Vzhledem k relativně novátorskému přístupu k řešení problematiky evidence tržeb nebyly dostupné informace a zkušenosti z více států s odstupem času jako faktoru ověřujícího koncept dlouhodobě. Odhad dopadů projektu a jejich materializace není možno porovnat s relevantním vzorkem obdobných projektů.

Omezení vedla k relativně vysoké míře abstrakce a použití obecně platných nejlepších odvětvových zkušeností, zejména v návrhové části - ve specifikaci potenciálních průvodních organizačních a podpůrných opatřeních projektu.

Navzdory omezením, je možno konstatovat, že rozsah posouzení a analýz je dostatečný pro přijetí manažerských rozhodnutí o projektu a realizaci následných aktivit.

Specifikace projektu

Účel a cíle projektu

Hlavním cílem evidence tržeb je z pohledu finanční správy **získání informací, které zabezpečí lepší správu daní** (zejména daní z příjmů a daně z přidané hodnoty). Základním cílem je narovnání podnikatelského prostředí tak, aby se minimalizovala konkurenční nevýhoda poctivých podnikatelů způsobená krácením daňových povinností ostatními daňovými subjekty.

Dopadem naplnění hlavního cíle bude mít předpokládaný dopad ve formě zlepšeného výběru dani, zejména daní z příjmů podnikatelů a DPH. Samozřejmě je možno počítat i s nárůstem daní z příjmů zaměstnanců, odvodů pojistného nebo spotřebních daní. Blíže viz Analýza přínosů a nákladů.

Dle metody stanovení cílů s kritériem SMART[2] možno definovat cíl projektu následovně:

Zavést systém a podmínky pro elektronickou evidenci tržeb na straně finanční správy umožňující evidenci tržeb povinnými subjekty od začátku roku 2016.

Výchozí situace

Pro ukotvení projektu do prostředí je nutné vzít v potaz všechny důležité aspekty projektu. Jejich zhodnocení je uvedeno v následujících částech.

[2] SMART – cíle jsou specifické (Specific), měřitelné (Measurable), vykonatelné / realizovatelné (Attainable), směřující k výsledku / záměru (Relevant) a ve specifickém čase (Time-bound).

Kvantitativní odhad objemu transakcí

Technologická východiska úzce souvisí s objemem zpracovaných transakcí.

Objem transakcí není v ČR nijak prozkoumán a žádné použitelné statistiky nejsou dostupné. Pro kvantifikaci jsme použili data z geograficky a kulturně blízké krajiny – Rakouska.

Ty jsme následně extrapolovali podle počtu obyvatel a zapracovali odchylku ve výši 20 %.

V rámci výzkumu[3] objemu transakcí realizovaných obyvateli Rakouska byly zjištěny následující údaje:

Rakousko	**Počet obyvatel**	**8 400 000**
	Podíl	Počet v mil.
Hotovostní platby	82%	12 110,68
Platby debetními a kreditními kartami	16%	2 363,06
Ostatní formy	2%	295,38
	Celkem	14 769,13

Propočtem se dá určit průměrný počet transakcí jednoho obyvatele Rakouska na hodnotu 4,76 transakce denně. Propočtem dat z jiných zdrojů[4] byl počet transakcí stanoven na hodnotu 4,28 transakce na obyvatele a den. Pro porovnání, uvádíme i jiné země:

Země	AT	DE	NL	FR	ČR*
Počet transakcí na obyvatele a den	4,28	3,74	2,15	2,30	4,52

* propočet

Aproximací průměrné hodnoty Rakouska jsme získali hodnoty pro Českou republiku - objem cca 17 – 20 mld. transakcí ročně. Z tohoto propočtu jsme dále vycházeli.

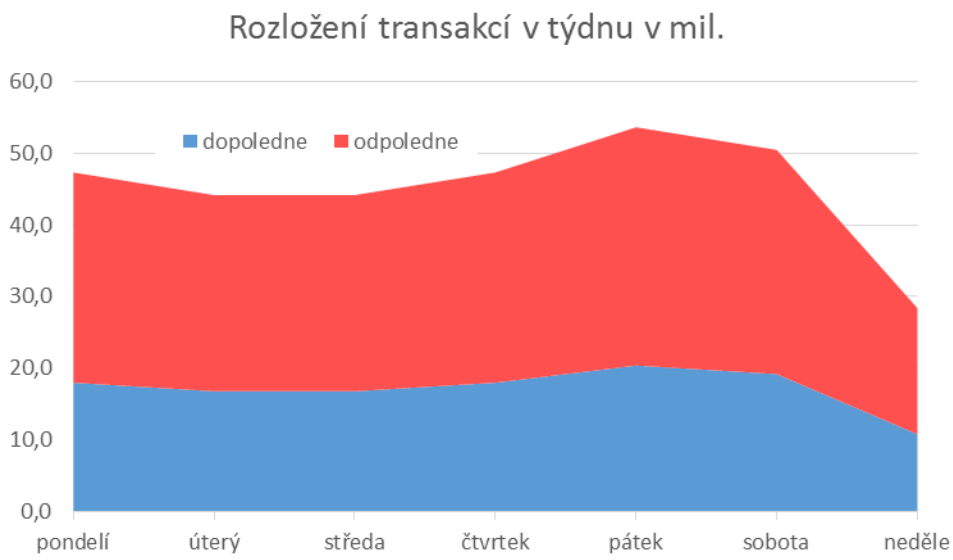
Kromě kvantifikace počtu transakcí je nutné vzít potaz jejich rozložení v čase. Pro tenhle účel posloužili údaje z výše zmiňovaného průzkumu v Rakousku.

Počet transakcí byl rozložen do jednotlivých dní a rozdělen na dopolední a odpolední část na základě dat průzkumu.

	pondělí	**úterý**	**středa**	**čtvrtek**	**pátek**	**sobota**	**neděle**
podíl na transakcích v týdnu	15%	14%	14%	15%	17%	16%	9%
z toho dopoledne	20,0	18,7	18,7	20,0	22,7	21,3	12,0
z toho odpoledne	32,6	30,5	30,5	32,6	37,0	34,8	19,6

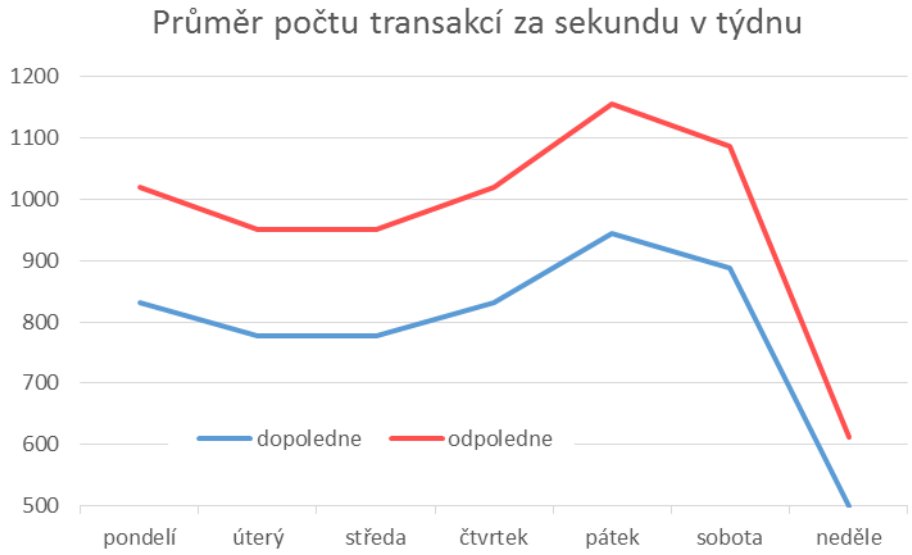
Graficky znázorněno:

[3] http://www.eea-esem.com/files/papers/EEA-ESEM/2014/1502/capd_masterfile.pdf
[4] https://www.worldpaymentsreport.com/reports/noncash_inhabitant



Obrázek 1: Rozložení transakcí v týdnu

Rozložení v průběhu dne je opět nerovnoměrné. Den rozdělený do dvou stejných částí (do 12:00 a od 12:00) nekoresponduje s typickou křivkou lidské aktivity. Důkazem je např. spotřeba elektrické energie, která začíná stoupat od 6:00 a utlumuje se po 22:00. Z tohoto důvodu jsme odhad počtu transakcí za sekundu rozdělili nerovnoměrně, s předpokladem transakcí jenom v čase od 6:00 do 22:00. Kumulace předpokládaných transakcí do tohoto času je rovněž uplatněním skeptického odhadu a ve prospěch kalkulace se špičkami. Výchozí počet transakcí, které bude muset systém zpracovat za jednu sekundu je ilustrován na následujícím grafu.



Obrázek 2: Průměr počtu transakcí za sekundu

Dalším aspektem, který je nutno zohlednit při identifikaci počtu transakcí v čase je charakteristika maximální kumulace transakcí v čase, tzv. špičky. Pro stanovení odchylky špičkového objemu transakcí vůči průměrnému jsme použili data z transakcí platebními kartami. Předpokladem je obdobná charakteristika špičky i pro hotovostní platby.

Jak se dá odhadovat, špička v roce se v prostředí Evropy vyskytuje v předvánočním čase, nejčastěji v průběhu víkendu před Vánocemi. Podle statistik společnosti VISA, špičkový objem transakcí

odpovídá 4,54 násobku průměrných hodnot. Obráceně, v průměrný den je 22% transakcí oproti dni ve špičce roku. Jednalo se o tzv. Black Friday (čtvrtý pátek v listopady), což je tradičně den věnovaný nákupům v USA a Kanadě.

V české republice si prvenství v celkovém objemu tržeb však nadále drží platby uskutečněné prostřednictvím platební karty v kamenných obchodech. Podle společnosti Global Payments Europe byl počet transakcí v průběhu vánočních nákupů vyšší dvojnásobně.

GE Money Bank informovala, že počet transakcí byl v prosinci 2014 4,6 mil. Nejvyšší počet transakcí zaznamenán 22. prosince (332 tis.), to znamená, že k průměru za prosinec (148 tis.) byl počet transakcí v tento den na úrovni něco více než dvojnásobku (224%).

Rozložení transakcí v průběhu špičky není známo. Dá se ovšem předpokládat, že bude ještě zvýrazněno a nebude kopírovat rozložení průměrného dne. To znamená, že špička může být 3 a vícenásobná oproti běžným objemům transakcí.

Z tohoto důvodu je vhodné upravit výkonovou kapacitu centrálního systému na kapacitu osmi násobku předpokládané zátěže.

Propočtem na kapacitu zpracovaných transakcí systémem, s ohledem na špičky, je určena

cílová hodnota výkonnosti systému na 10 tisíc transakcí za sekundu.

S touto hodnotou je potřebné v projektu pracovat a projektovat technické a jiné výkonnostní kapacity systémů.

Legislativní východiska

Základním východiskem pro specifikaci projektu jsou:

- Návrh zákona o evidenci tržeb
- Důvodová zpráva k návrhu zákona
- Analýza evidence tržeb elektronickými prostředky
- Programové prohlášení vlády
- Ostatní právní předpisy ČR
- Vyhláška

Návrh zákona

Navrhovaná právní úprava de facto doplňuje existující platné normy stanoveným směrem, a to zejména z hlediska způsobu a formy navazující na již dnes běžně prováděné úkony (zejména vedení určité evidence transakcí a vydávání dokladů zákazníkovi).

Obsahem navrhované právní úpravy, relevantní k specifikaci projektu jsou:

a) Vytvoření úložiště dat získaných v rámci evidence tržeb
b) Vytvoření aplikační části systému EET a jejich modulů sloužících pro realizaci všech procesů v rámci evidence tržeb od vstupu povinných subjektů do systému, testování, řešení změn, plnění i ukončení povinností, včetně portálu a certifikační autority
c) Zajištění adekvátní komunikační infrastruktury a dostatečně dimenzovaného připojení k internetu ze strany SPCSS pro zvládnutí výkonnostních provozních parametrů systému EET
d) Zajištění podmínek a prostředků pro orgánů Finanční správy a Celní správy ČR pro plnění jejich kompetencí v rámci EET včetně kontrolní a analytické činnosti
e) Poskytnutí autentizačních údajů pro evidenci tržeb a získání údajů o povinném subjektu

Samozřejmě jsou navrhované právní úpravy, které jsou nutné pro vytvoření legislativního rámce projektu EET, zejména:

f) Stanovení obecné evidenční povinnosti
g) Evidence tržeb probíhajících mezi stanovenými subjekty, za stanovených okolností a stanoveným způsobem
h) Uložení povinnosti vydání evidenčního dokladu povinným subjektem a povinnosti převzetí
i) Sankce za nesplnění povinností daňovými subjekty
j) Spolupráce orgánů veřejné moci při kontrole plnění vybraných povinností
k) Účtenková loterie

V téhle části budeme vycházet z předpokladu, že návrh zákona o evidenci tržeb bude schválen tak, jak je předložen. Návrh zákona má následující dopady na projekt a definuje charakter projektu:

Navrhovaný stav / oblast	Dopad na projekt
Platba poplatníkovi	Široce pojatá definice platby znamená prakticky všechny hotovostní platby nebo i platy prostřednictvím platebního nástroje (např. kreditní karta) nebo i stravenek. Předpokládaný počet transakcí je uveden v části **Chyba! Nenalezen zdroj odkazů.**.
Autentizační údaje	Součástí projektu musí být i systém pro evidenci registrací provozoven povinných subjektů. Bude se jednat o několik stovek tisíc provozoven a rovněž povinných subjektů. Systém proto bude muset být automatizovaný. Povinnému subjektu budou automatizovaně zaslány autentifikační údaje pro přístup na samoobslužný portál EET, v případě kdy je držitelem datové schránky ISDS, následně pro přihlášení na portál EET může povinný subjekt zaevidovat své provozovny a získat elektronickou značku (certifikát) pro komunikaci

	se systémem EET. V případě kdy povinný subjekt nedisponuje datovou schránkou ISDS, bude nezbytné získat autentifikační údaje prostřednictvím příslušné pobočky České pošty, pracoviště Czechpoint nebo výjimečně prostřednictvím na určeného pracoviště finančního úřadu. Tento proces bude nezbytné perfektně zvládnout z důvodu potřeby registrace většího počtu povinných subjektů během krátkého období.
Evidenční povinnost	Evidenční povinnost podle § 11, ods. 1, písm. b) ustanovuje povinnost vydat účtenku. Dále však účtenku blíže nespecifikuje. Teoreticky je tedy možné vydat i účtenku ručně psanou, obsahující však všechny náležitosti požadované právními předpisy. Znamená to, že i živnostník, který vydává účtenku např. párkrát denně, může tržbu zaevidovat, např. prostřednictvím aplikace v telefonu, a „ručně vypsat“ účtenku obsahující fiskální identifikační kód.
Údaje na účtence	V zákonu jsou definovány jenom dva údaje – bezpečnostní kód povinného subjektu a fiskální identifikační kód. V případě nedostupnosti systému EET a nemožnosti zaevidování účtenky systémem EET (off-line režim) bude nezbytné zavést i Off-line kód povinného subjektu (OKP). OKP je pomocným ochranným prvkem, který umožňuje kontrolu integrity a prokazuje odpovědnost povinného subjektu za vystavení tištěné účtenky. OKP je vždy předáván v elektronické komunikaci a na účtenku je tištěn pouze v případě, kdy je vydávána v off-line režimu.
Nemožnost evidování tržeb	Zákon pamatuje i na tyto situace. Blíže však neurčuje podrobnosti. (budou určené prováděcí vyhláškou). Viz také Návrh obsahu
Mezní doba odezvy	Důležitý údaj pro specifikaci parametrů systému. Technický návrh musí zohledňovat stanovené doby.
Zjednodušený režim	Nutno je zohlednit při specifikaci parametrů systému (kontrola splnění povinnosti do 5 dnů zaslat údaje v zjednodušeném režimu).
Ověření účtenky	Nutno je zohlednit při specifikaci parametrů systému.
Účinnost	Účinnost je stanovena na 1. ledna 2016. Pro § 6 - § 10 je účinnost stanovena na 1. listopad 2015. Což znamená, pilotní provoz evidence žádostí a vydávání autentizačních údajů musí začít 1.10. 2015.

Dle vyjádření Ministerstva financí je záměrem postupný náběh povinností u poplatníků, (celkem odhadováno až 600 000 povinných subjektů) s čtvrtletními intervaly, a to následovně:

Leden 2016 – restaurace, stravování, ubytování (cca **10 %** z celkového počtu povinných subjektů)

Duben 2016 – maloobchod, velkoobchod (cca **40 %** z celkového počtu povinných subjektů)

Červenec 2016 – Postupně by byly zapojeny další skupiny podnikatelů na základě analýz míry rizika zkreslování tržeb v jednotlivých segmentech trhu a významnosti odhadovaného objemu krácení daní, tak, aby všechny povinné subjekty podléhaly evidenci tržeb nejpozději do tří let od účinnosti zákona (zbylých cca **50 %** z celkového počtu povinných subjektů)

S ohledem na stanovené povinnosti, je nutno v projektu počítat s postupným spouštěním funkcí systému i v pilotním / ověřovacím provozu minimálně 60 dní před řádným provozem. To znamená:

k 1.7.2015 – zahájit pilotní provoz systému EET a CA EET pro vývojáře software pro povinné subjekty

k 1.10.2015 – zahájit pilotní provoz evidence žádostí a vydávání autentizačních údajů

k 1.11.2015 - zahájit pilotní provoz evidence tržeb, ověřování účtenky, evidence dat v zjednodušeném režimu

Důvodová zpráva

Důvodová zpráva (dále i jako DZ) podrobněji vysvětluje smysl a principy evidence tržeb.

Poznámka: Důvodová zpráva není sice právně závazná, avšak její obsah je důležitý z hlediska výkladu smyslu zákona a úmyslu zákonodárce, resp. předkladatele zákona.

DZ uvádí některé základní principy EET (pilíře) na kterých má stát:

1. Elektronizace a on-line přístup správce daně k údajům,
2. Umožnění dobrovolného zapojení veřejnosti do kontroly dodržování zákona,
3. Otevřené řešení (SW i HW).

Samostatně uvádí bezpečnost EET, tu však vzhledem k charakteru projektu není zapotřebí zdůrazňovat, vysokou úroveň bezpečnosti proto budeme považovat za samozřejmost.

Vyhláška

Ve vyhlášce bude dle současného návrhu zákona o evidenci tržeb upraveno:

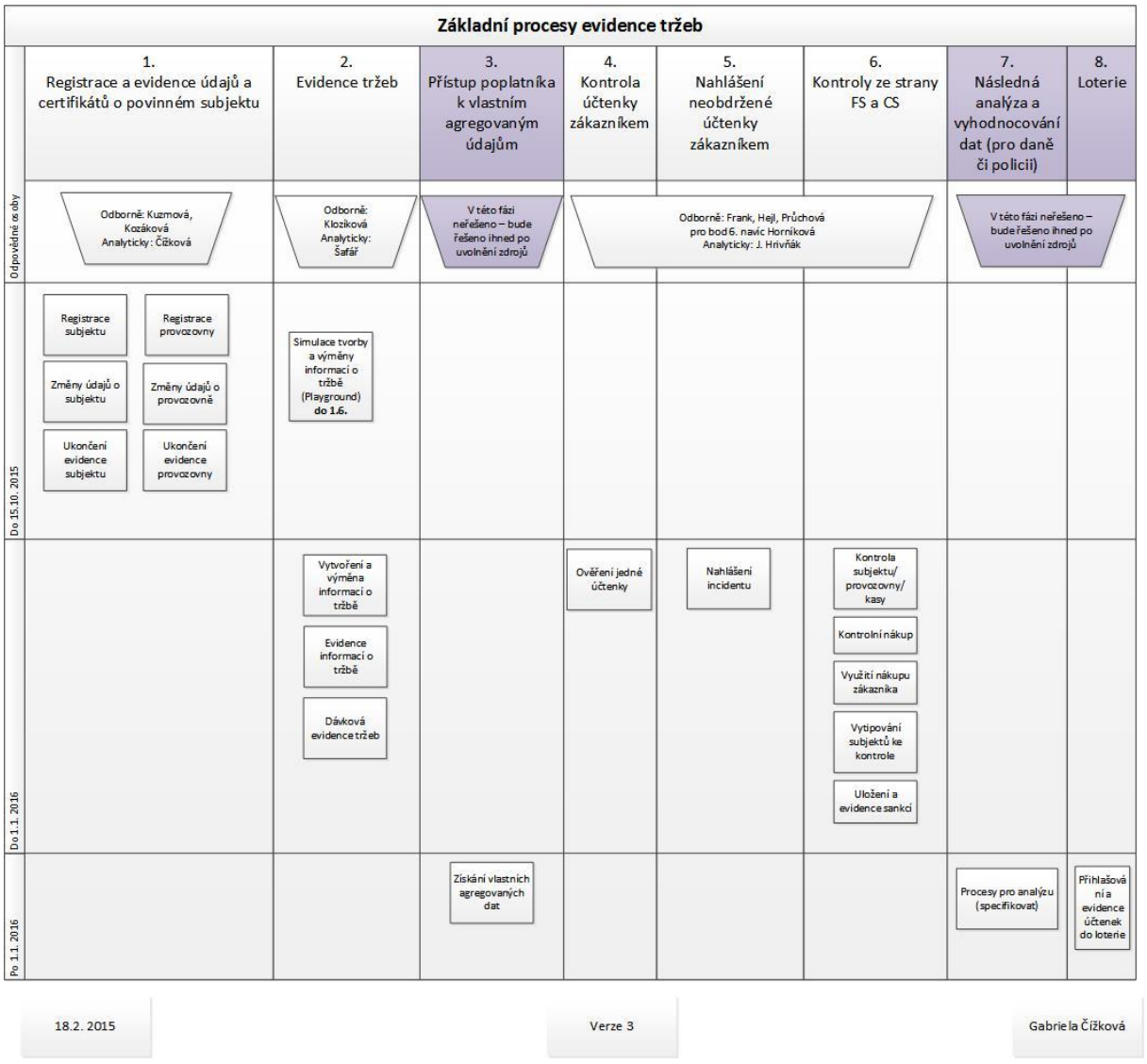
- výjimky z evidováni tržeb (para.5)
- tržby evidované ve zjednodušeném režimu (para.5)
- způsob tvorby BKP (para. 12)
- zasílané údaje k účtence (para.12)
- údaje uváděné na účtence (para. 13)
- obsah a forma informačního oznámení (para. 20)
- přechodný režim - tzv. fázování (para.43)

Základní procesy evidence tržeb

Základní procesy evidence tržeb jsou rozděleny do následujících 8 procesních oblastí:

1. Registrace a evidence údajů a certifikátů o povinném subjektu, změny v údajích
2. Evidence tržeb
3. Přístup poplatníka k vlastním údajům, a to v agregované podobě za definované období a na žádost v plném rozsahu zaevidovaných údajů za určené období
4. Kontrola účtenky zákazníkem
5. Nahlášení neobdržené účtenky zákazníkem
6. Kontrola ze strany FS a CS
7. Analýza a vyhodnocování dat, včetně možnosti poskytování dat pro statistické účely
8. Loterie

Obsahem tohoto dokumentu je detailní popis procesní oblasti 1, 2, 4, 5 a 6. Oblast 3, 7 a 8 budou zpracovány v následující analytické fázi, budou však součástí zadání projektu, tak, aby bylo možné jejich spuštění k datu spuštění systému.



Obrázek 3: Základní procesy evidence tržeb

Registrace a evidence údajů a certifikátů o povinném subjektu

Požadavky na IS EET

ID	IS/Portál	Požadavek	Popis
EP-1	RS-IS	Umožnit registraci poplatníka	IS EET musí při splnění podmínek umožnit založit poplatníka v systému EET
EP-2	IS	Ověřit technickou korektnost podané žádosti	IS EET musí dokázat ověřit formát a strukturu žádosti a vyhodnotit, zda žádost splňuje požadavky
EP-3	P, IS	Umožnit registrovat provozovnu a spravovat její údaje	IS EET musí při splnění podmínek umožnit vznik jedné i více provozoven poplatníka a správu údajů o provozovně v souladu s právy přihlášeného uživatele

Požadavky na portál EET

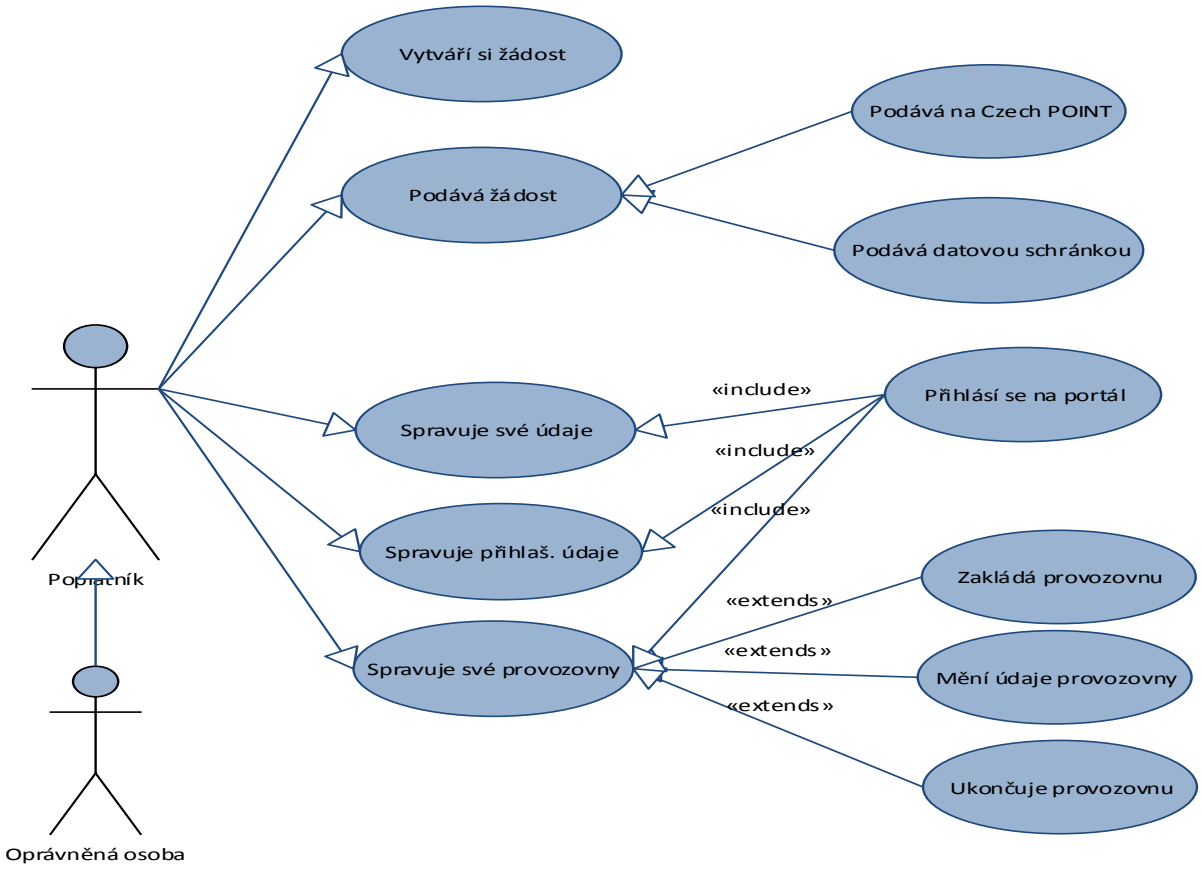
EP-4	P	Vytvořit poplatníkovi účet na webovém portálu EET	Účet je zakládán s odpovídající rolí dle požadavku poplatníka. Pozn.: poplatník může mít více uživatelských účtů, např. pro různé uživatele, které pověří (zejm. u právnických osob).
EP-5	P	Generovat autentizační údaje pro přístup k portálu	IS EET musí vytvořit autentizační údaje pro oprávněný přístup poplatníka k jeho údajům prostřednictvím portálu EET. (pozn. Portál slouží jako rozhraní pro přístup poplatníka k jeho údajům v EET.)
EP-6	P	Zobrazit údaje poplatníka na portálu	IS EET musí zobrazit vybrané údaje o poplatníkovi (pozn. většinu z ADIS na základě jeho DIČ, ostatní jsou vlastní údaje EET k poplatníkovi)
EP-7	P	Umožnit vytvořit žádost o autentizační údaje	Umožnit komukoli vytvořit žádost o autentizační údaje v požadovaném formátu a struktuře.
EP-8	P	Umožnit odeslat žádost o autentizační údaje za datovou schránku	Umožnit přímé odeslání žádosti datovou schránkou pouze po korektním přihlášení údaji datové schránky
EP-9	P	Autentizovat uživatele pro přístup do datové schránky	Pro přímé odeslání žádosti
EP-10	P	Paralelní přístup k jednomu účtu poplatníka	Umožnit přístup prostřednictvím portálu více uživatelům k účtu jednoho poplatníka v IS EET a to i paralelně
EP-11	P	Systém musí rozlišovat práva a role uživatelů portálu.	Systém musí rozlišovat práva přihlášených uživatelů na základě jejich role.
EP-12	P	Umožnit připomenutí hesla	Při zapomenutém hesle musí portál umožnit průběh procesu připomenutí hesla.
EP-13	P	Umožnit správu autentizačních údajů pro portál	Při splnění podmínek umožnit správu uživatelských údajů (obsluhou). Změny i zneplatnění.
EP-14	P	Zpřístupnit historii změn oprávněnému uživateli	Umožnit zjistit, jak byl který údaj nastaven ve zvolené době, kdo a kdy jej změnil.

Systémové a bezpečnostní požadavky

Předpokladem je, že systémové a bezpečnostní požadavky budou definovány globálně, mimo tyto parciální procesy. Zde jsou jen vybrané požadavky, přímo vyplývající z potřeb procesu.

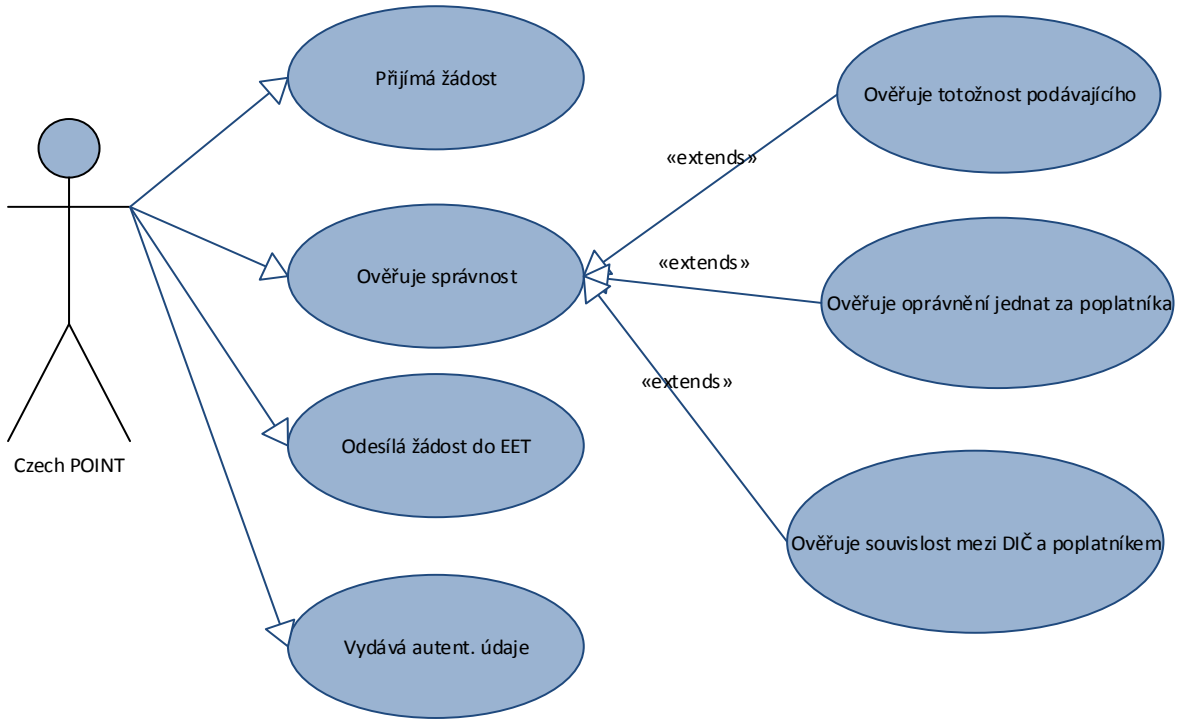
EP-15	IS, P	Evidovat historii vzniku a změn údajů	Při změně údaje musí být zaznamenána původní hodnota, nová hodnota, kdo a kdy údaj změnil.
EP-16	P	Logovat přihlášení na portál	úspěšná i neúspěšná přihlášení
EP-17	P	Správa rolí a práv	Portál musí umožňovat správu definovaných rolí a práv v rámci portálu. Dosud identifikováno: role administrátor, role editor provozoven a role pouze pro čtení.

Případy užití poplatníka



Obrázek 4: Případy užití poplatníka

Případy užití Czech POINTu



Obrázek 5: Případy užití Czech POINTu

„Registrace“ poplatníka

„Registrace“ poplatníka je proces, kterým poplatník vstupuje do elektronické evidence tržeb.

Smyslem registrace je, aby se poplatník zaregistroval do elektronické evidence tržeb. Při kladně vyřízené žádosti o autentizační údaje je poplatník zaregistrován v systému EET a zároveň jsou mu přiděleny autentizační údaje pro vstup na portál a minimálně jeden certifikát.

Aktéři

Aktér v kontextu „registrace“ poplatníka	Popis
Poplatník	Daňový poplatník, přijímající tržby dle § 4 zákona o EET. V jeho roli může vystupovat i oprávněná osoba.
Oprávněná osoba	Osoba oprávněně jednající za poplatníka
Czech POINT	Kontaktní místo veřejné správy, oprávněné k úkonům pro EET (předpokládá se přepážka na České poště)
IS EET	Informační systém EET, který přijímá a eviduje registrovaného poplatníka, jeho atributy a historii akcí.
Portál EET	Webový portál, mj. umožňující správu údajů v IS EET

Předpoklady

Seznam předpokladů, na jejichž základě byl proces navržen a popsán. Zdrojem předpokladů je platná legislativa, připravovaný zákon o EET, dále vstupy odborného a technického teamu, týkající se omezení a reálných možností za daných časových a technických podmínek.

Název	Popis předpokladu
Poplatník v procesu má vždy DIČ	Před vydáním DIČ se poplatníka zákon netýká, pracujeme tedy s předpokladem, že poplatník v procesu má vždy DIČ

Poplatník a IČO	Má-li poplatník přiděleno IČO, pak IČO uvádí v žádosti a systém jej zobrazuje jako jeden z údajů poplatníka
Terminologie žádosti	Dle terminologie zákona se jedná o **Žádost o autentizační údaje**, ačkoli věcně znamená mnohem více požadavků (zejm. se jedná o registraci – založení - poplatníka v IS EET)
Obsah žádosti	Dle zákona musí být součástí žádosti **vše**, co potřebujeme k celému procesu evidence tržeb, jinak následně nemůžeme požadovat evidenci, ani hlášení změn potřebných údajů (tzn. i údaje o provozovnách)
Kontrola DIČ	Předpokládáme spolupráci s ADIS (rozhraní), pomocí kterého by se daly údaje o poplatníkovi porovnat s údaji v žádosti (vazba na DIČ)
Datum přidělení DIČ	Je nutné vědět, kdy bylo přiděleno subjektu DIČ, jelikož zákon stanoví, že je nutné evidovat až tržby vzniklé 10 dní po přidělení DIČ. Datum přidělení DIČ poskytuje ADIS, nikoli poplatník.
Náležitosti podání	Žádost musí splňovat náležitosti pro podání dle § 70 daňového řádu (zák. č. 280/2009), tj.: kdo podání činí, čeho se podání týká, co se navrhuje a podpis
Autentizace podání	Podání musí být autentizováno způsobem dle § 71 daňového řádu.
Spisová služba	Dokument/y podání bude nutné evidovat ve spisové službě
Neposkytování informací	Pokud v procesu žádosti zjišťujeme jakékoli údaje o poplatníkovi, které nám v rámci žádosti neposkytl sám, neposkytujeme je žadateli
Vadné podání	Vadné podání je takové, které nesplňuje náležitosti § 70, resp. § 71 daňového řádu

Žádost

Vznik žádosti

Předpokládá se, že žádost si poplatník může vytvořit na veřejné části portálu EET (pomocí formuláře) a výstupem bude datová věta v potřebné struktuře. Dle zákona je možné žádost podat pouze datovou zprávou v určeném formátu a struktuře.

Obsah žádosti

Žádost o autentizační údaje poplatníka musí obsahovat tyto vstupní údaje:

1. DIČ poplatníka, pro kterého se žádá
2. Čeho se podání týká* – žádost o autentizační údaje
3. Co navrhuje* - žádá o registraci v EET a autentizační údaje na portál
4. Údaje podatele (Kdo podání činí*):
    - identifikace podatele
        - FO: jméno, příjmení, datum narození, adresa,
        - PO: název a IČO, má-li jej přiděleno
    - Podpis podatele*
5. Údaje poplatníka:
    - Zda je fyzická nebo právnická osoba a dále
        a) když je poplatník totožný s podatelem, tak ještě IČO, má-li jej přiděleno
        b) když není zároveň podávající, tak potřebujeme všechny údaje jako u podatele
6. Povinné údaje minimálně jedné provozovny (viz dále podrobněji v bodě 4. až 6.)
   Pozn.: Ze zákona vyplývá, že součástí žádosti musí být i údaje o provozovnách, abychom následně mohli požadovat jejich správu. Další důvod, proč požadujeme zadat alespoň jednu provozovny přímo při registraci je, že poplatník bez aktivní provozovny není v principu funkční. Poplatník je totiž povinen identifikovat tržby na konkrétní provozovnu (ID provozovny je součástí datové věty účtenky).

* Povinné náležitosti pro podání dle § 70 daňového řádu (zák. č. 280/2009).

Určený formát je XML. Struktura datové věty bude definována po schválení potřebných údajů.

Podání žádosti

Poplatník žádost podá a tím žádá o zavedení do systému EET a zároveň o přihlašovací údaje na portál.

Žádost může podávat:

a) fyzická osoba - podnikatel (pro sebe)
b) oprávněný zástupce právnické osoby (např. statutární orgán, …)
c) zástupce (zmocněnec) fyzické osoby na základě plné moci
d) zástupce (zmocněnec) právnické osoby na základě plné moci

Pozn. Zástupcem může být fyzická i právnická osoba.

Podání žádosti na Czech POINT

Czech POINT ověřuje:

1) totožnost podatele,
2) oprávněnost podatele jednat za uvedeného poplatníka a
3) příslušnost DIČ k poplatníkovi, uvedenému v žádosti (ověření ale provádí IS EET)

Proces ověření je popsán samostatně. Výstupem ověření pro potřeby procesu registrace je závěr, zda všechny ověřované skutečnosti odpovídají požadavkům pro podání a zpracování korektní žádosti nebo nikoli.

Pokud je závěr, že odpovídají, Czech POINT zasílá žádost systému EET. Systém EET ověří, zda již tento poplatník (toto DIČ) nebylo zaregistrováno. Pokud nebylo, systém EET poplatníka zaregistruje a vytvoří mu autentizační údaje na portál. Poplatník obdrží autentizační údaje.

Autentizační údaje musí být dle zákona přiděleny obratem.

Podání datovou schránkou

Rozdíly proti podání na Czech POINT

- Reakční doba je ze zákona delší (24 hod). Zpracování a odpověď musí tedy proběhnout do 24h od podání
- Odpadá ověření totožnosti podatele, jelikož totožnost je daná již datovou schránkou
- Ověření souvislosti mezi podatelem a poplatníkem, pro jehož DIČ se žádá, bude probíhat stejně jako u podání na Czech POINTU

Porovnání údajů u žádosti podané datovou schránkou vyhodnocuje na shodu systém EET proti údajům poskytnutým ADIS. Při dokonalé shodě potvrdí oprávněnost žádosti.

Při nesrovnalostech odkáže žadatele na Finanční úřad k manuálnímu zpracování žádosti.

Podání zástupcem (na základě plné moci) – není dořešeno a bude patrně muset spadat do ručního zpracování.

Tam, kde jsou potřeba dva podpisy – není problém, je vyřešeno novelou.

Údaje zástupce k ověření:

- FO: jméno, příjmení, rodné příjmení, datum narození
- PO: název, IČO, sídlo

Při ověření zástupce musí být Plná moc k dispozici (dostupná v ADIS).

Riziko při ověření zástupce: ověření není jednoznačné, ale je to současná praxe. Námět: ISDS má i pole „Místo narození“, které by se dalo využít.

Alternativní cesta

Vyplněný formulář žádosti na webu systém může odesílat přímo za svou datovou schránku po úspěšném zadání autentizačních údajů ke své datové schránce. Jednalo by se o obdobný proces jako

v aplikaci elektronická podání na Daňovém portálu (EPO). Tato cesta ale nyní není zákonem o EET umožňována.

Výsledky a výstupy žádosti

Podání žádosti může skončit jedním z následujících způsobů:

A) Žádost bude ověřena s kladným výsledkem
Výstupy:

- Autentizační údaje pro přístup na portál
- Potvrzení pro poplatníka, že žádost podal (na vyžádání)
- Potvrzení pro finanční správu, že poplatník vše převzal (aby bylo doloženo, že mu byly autentizační údaje přiděleny v zákonné lhůtě)

Předpokládáme, že elektronicky podaná žádost musí vygenerovat papírovou formu podání k podpisu.

B) Žádost bude ověřena se záporným výsledkem

Výstup: zamítnutí žádosti a přesměrování podatele na finanční úřad k dořešení situace

C) Ověřeno, účet založen, ale certifikáty nebyly vydány bez zavinění poplatníka (např. tech. potíže, dostupnost rozhraní)
Výstup: Autentizační údaje na portál a odkázání podatele na portál pro dořešení certifikátů

D) Žádost nebyla podána bez zavinění poplatníka
Výstup: Potvrzení pro poplatníka, že chtěl podat

Autorizovaná konverze z moci úřední Plné moci; potvrzení, že převzal. Dále budou uloženy do systému k žádosti.

Potvrzení, že žádost podal, bude uloženo v EET, jelikož jej systém sám vytváří.

Vadné podání žádosti

V případě vadného podání žádosti o autentizační údaje. Důvodová zpráva k zákonu o evidenci tržeb na straně 34, v části k § 7 uvádí „V případě vadného podání se předpokládá automatická odpověď systému, která bude právně výzvou k odstranění vad. Výzva k odstranění vad dle ustanovení § 74 daňového řádu pak jednak přerušuje běh lhůty správce daně a zadruhé zajišťuje, aby tato lhůta neskončila dříve než 5 dní ode dne, kdy došlo k požadované součinnosti, tj. odstranění vad. Prakticky tedy dojde k prodloužení lhůty.“ Prakticky to znamená, že pokud systém umožní poplatníkovi učinit jakkoliv vadné podání, bude nutné, aby systém na základě vadného podání pro obě varianty (tj. podání datovou schránkou i prostřednictvím kontaktního místa):

1. vygeneroval automatickou odpověď, která bude nést všechny náležitosti výzvy k odstranění vad podání, včetně řádného odůvodnění (§ 74, § 101 a § 102 daňového řádu)
2. zajistil zaznamenání data doručení této výzvy
3. zaznamenal návaznost k podání, kterým se vady podání odstraní a poznal, zda vady byly či nebyly odstraněny
4. pořídil/umožnil pořízení úředního záznamu za situace dle ust. § 74 odst. 3 daňového řádu
5. všechny písemnosti (podání, výzva, odpověď na výzvu=opravné podání, úřední záznam o neúčinnosti podání) umožnil evidovat ve spisové službě.

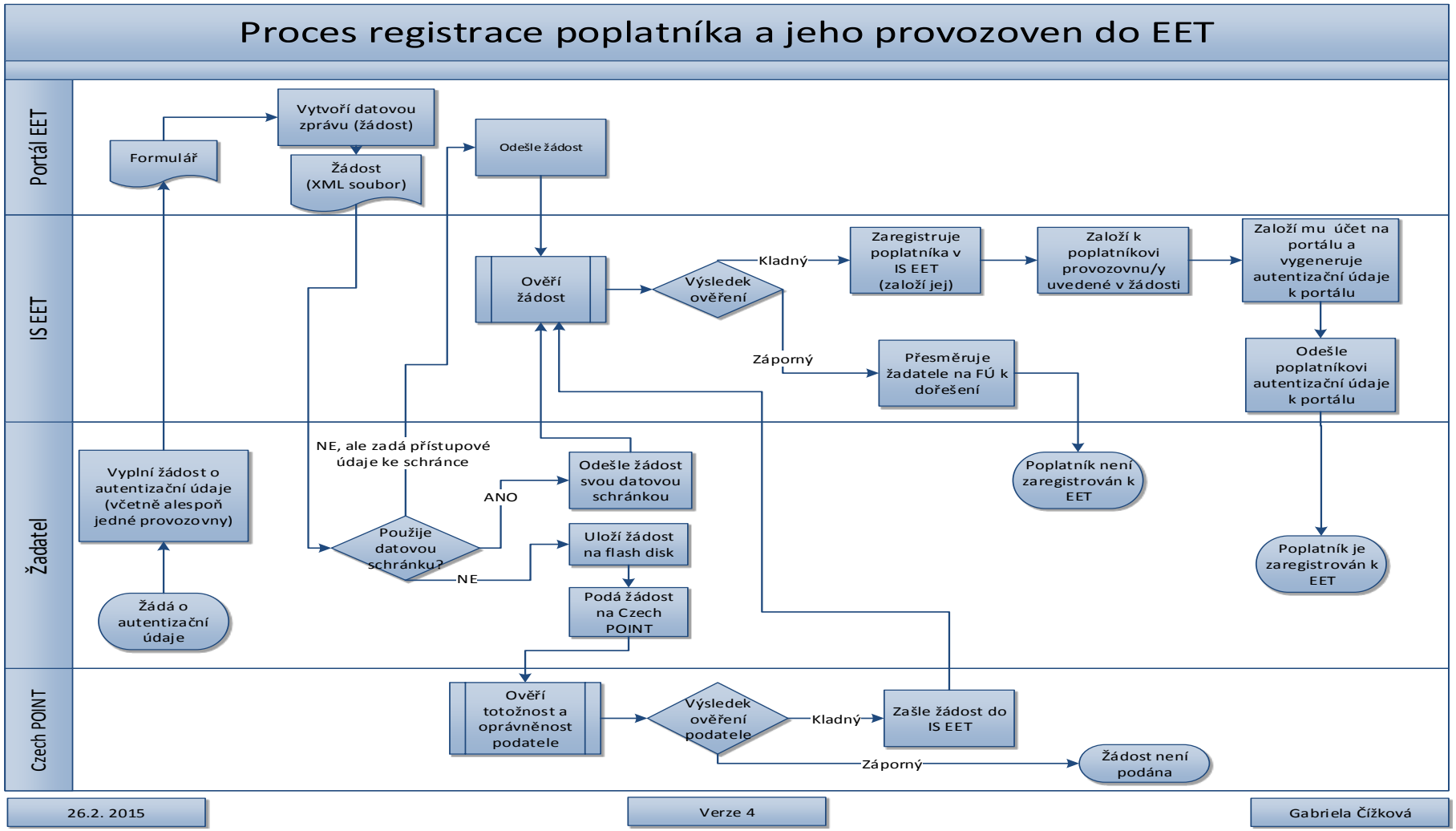
Alternativní scénáře

- Chybné DIČ
- ADIS rozhraní nezodpoví na ověřovací dotaz
- Neaktuální údaje v ADIS
- Podatel žádosti není oprávněná osoba

- Poplatník žádá na Czech Point o vydání autentizačních údajů ve stejný den, kdy mu bylo přiděleno DIČ, tj. ten samý den, kdy na FÚ vyzvedl osobně rozhodnutí o přidělení DIČ (nutno dořešit, zda budou údaje z ADIS přeneseny on-line v rámci jednoho dne)
- Duplicitní žádost – poplatník s tímto DIČ je již v EET registrován

Nalezená rizika

- Rozhraní ADIS – zda bude vytvořeno včas
- Kapacitní nároky na Czech POINT kolem počátku platnosti zákona (ev. v každé vlně)

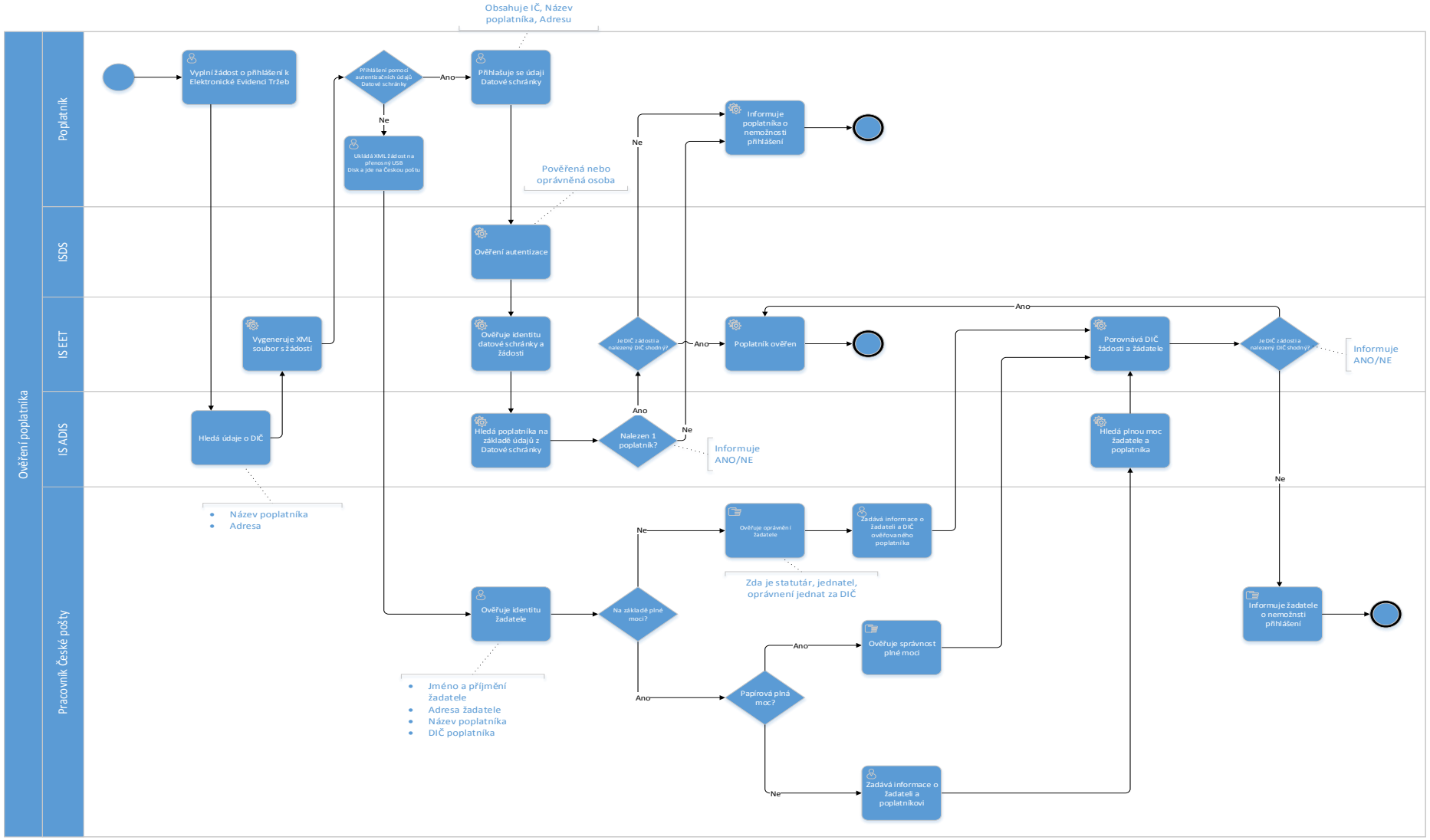


Obrázek 6: Proces registrace poplatníka a jeho provozoven do EET

Ověření poplatníka

Proces ověření poplatníka probíhá v několika krocích.

1. Na portálu žadatel vyplní informace o poplatníkovi a jeho provozovnách.
    a. Informace o poplatníkovi jsou automaticky získány z IS ADIS
2. V případě, že poplatník zvolí variantu pomocí datové schránky
    a. Žadatel zadá přihlašovací informace k datové schránce.
    b. Systém ISDS ověří, zda jsou údaje správné a předá informace o poplatníkovi (IČ, název poplatníka a jeho adresa).
    c. Systém ADIS dohledá k IČ a Názvu poplatníka (včetně jeho adresy) z ISDS DIČ.
    d. V případě, že existuje jenom jedno DIČ, ověření proběhlo správně. Když je nalezených výsledků víc než 1 nebo 0, proces končí a poplatník musí navštívit pobočku CzechPOINT nebo Finanční úřad.
    e. Když existuje jednom jedno DIČ, systém EET ověří, zda DIČ ze žádosti zodpovídá DIČ z ADIS a na základě výsledků ověří poplatníka.
3. V případě, že poplatník zvolí variantu pomocí návštěvy CzechPOINT.
    a. Pracovník pobočky ověří totožnost žadatele.
    b. V případě, že žadatel je osobou oprávněnou jednat na základě plné moci.
        i. V případě, že má žadatel papírovou plnou moc, pracovník ověří správnost plné moci (podepsání oprávněnou osobou za poplatníka) a odešle údaje o poplatníkovi do systému.
        ii. V případě, že je plná moc již zavedena v ADISu, systém vyhledá její existenci k poplatníkovi v systému ADIS. Když neexistuje, proces ověření končí.
    c. V případě, že žadatel je osobou oprávněnou jednat za poplatníka bez plné moci.
        i. Pracovník ověří oprávněnost jednat (porovná totožnost žadatele s výpisem z OR, ŽR apod.).
    d. Systém EET porovná DIČ ze žádosti s DIČ, pro který je osoba oprávněna jednat a provede ověření.
4. Systém odpovídá, zda je žadatel ověřený.



Obrázek 7: Proces ověření poplatníka

Chybové stavy

V případě, že proces selže v jakémkoli bodě, je žadatel požádán o návštěvu Finančního úřadu.

Czech POINT

Žádost může podávat

e) fyzická osoba - podnikatel (pro sebe)
f) oprávněný zástupce právnické osoby (např. statutární orgán, …)
g) zástupce (zmocněnec) fyzické osoby na základě plné moci
h) zástupce (zmocněnec) právnické osoby na základě plné moci

Na Czech POINT probíhá:

1. Ověření totožnosti žadatele (občanský průkaz) – ve všech čtyřech případech (běžná agenda).
2. Ověření, že je žadatel oprávněn jednat za poplatníka – v případě b), c) a d) (běžná agenda) Kontroluje se proti obchodnímu rejstříku.
3. Ověření souvislosti žadatele s DIČ poplatníka, ke kterému se žádost podává:

Ověření dle bodu 3

Ověření totožnosti žadatele a zjištění jeho oprávněnosti jednat za (DIČ) poplatníka, pro kterého žádá, musí být velmi dobře ošetřeno, jelikož na základě této žádosti vydáváme žadateli přístup do portálu a v následných krocích certifikáty poplatníka.

Vybrané údaje muset vykazovat 100% shodu, aby výsledkem bylo ověření.

Ověření na CzechPOINT

Totožnost žadatele se prokazuje občanským průkazem (ve variantě CzechPOINT). Souvislost mezi žadatelem a poplatníkem, pro kterého žádost podává, se zjistí porovnáním údajů k uvedenému DIČ poplatníka v žádosti vůči údajům uvedeným v obchodním rejstříku. Pracovník Czech POINTu přijde do styku s údaji o totožnosti žadatele, případně s údaji z obchodního rejstříku. Údaje na žádosti systém na pozadí porovná a vyhodnotí shodu nebo neshodu mezi údaji uvedenými k DIČ v žádosti a údaji uvedenými k DIČ v ADIS a pouze odpoví, zda jsou totožné nebo ne. Důvodem je neposkytovat pracovníkům České pošty údaje, které není nutné.

Ověření prostřednictvím Datové schránky

Rozhraní s ADIS poskytne odpověď, zda informace z Datové schránky jsou navázány na konkrétní jeden DIČ. Systém EET ověří shodnost DIČ z ADIS s DIČ ze žádosti.

ADIS musí rovněž poskytovat rozhraní na zjištění, zda k požadovanému DIČ a identifikované osobě existuje plná moc. Rozhraní (nebo údaje) ADIS o plných mocech musí být dostupné dle otevírací doby CzechPOINT a trvale ověření DIČ.

Tabulka 1 - Kontrola údajů na CzechPOINT

Poplatník	Žádající osoba předkládá		Kontrola proti
	dokumenty	údaje	
Fyzická osoba	Žádost + průkaz totožnosti	DIČ, jméno a adresa, datum narození	OŘ údaje k DIČ (jméno, adresa, datum narození)
Právnická osoba	Žádost + průkaz totožnosti	DIČ, název, adresa, IČO	OŘ údaje k DIČ (název, adresa, IČO)

Změny údajů poplatníka

Předpoklady

- Většina údajů o poplatníkovi se v EET pouze zobrazuje (viz seznam níže; zdrojem údajů je ADIS)
- Údaje, pocházející z ADIS, nelze v EET nijak spravovat
- Údaje k poplatníkovi, vznikající v EET, jsou jen Stav a Datum registrace do EET.
- Poplatník si nemůže samostatně editovat žádné údaje poplatníka (ani na portálu, ani jinak). Při změně údajů oznámí změnu finančnímu úřadu standardním a existujícím postupem a změna proběhne v systému, který je zdrojem dat (ADIS). Aktualizace je bude předávat z ADIS do EET. Může jít například o existující proces „Globální změna DIČ“ poplatníka v ADIS, která bude mít dopad i do EET.
- V případě údajů poplatníka vedených pouze v EET může finanční správa změnit pouze Stav (aktivní/neaktivní) a to na základě žádosti poplatníka, nebo z moci úřední

Údaje poplatníka v EET

<table>
<tr><th colspan="2">Údaje každého poplatníka</th></tr>
<tr><td colspan="2">1. DIČ
2. Datum získání DIČ
3. Stav poplatníka: (Aktivní, Neaktivní)
4. Datum registrace do EET
5. Zda je fyzická nebo právnická osoba
6. Místní příslušnost správce daně dle § 13, odst. 1 daň. řádu = (číslo územ. pracoviště FÚ)
7. Plné moci*</td></tr>
<tr><th>Údaje navíc u fyzických osob</th><th>Údaje navíc právnických osob</th></tr>
<tr><td>8. Jméno a příjmení
9. Datum narození
10. IČO, pokud jej má přiděleno
11. Adresa místa pobytu (dle § 13 odst. 1a) Daňového řádu)</td><td>12. Název společnosti
13. IČO, pokud jej má přiděleno
14. Adresa sídla</td></tr>
</table>

*Plné moci jsou vždy v ADIS. Pro účely EET potřebujeme generální Plné moci (kvůli ověření) i speciální plné moci pro EET. Varianta je potvrzení plné moci ze strany ADIS.

Pozn.: zde se předpokládá zásah do ADIS – speciální kód plné moci – jen pro EET.

Ukončení evidence (deaktivace) poplatníka

Předpoklady

- Finanční správa může v EET deaktivovat poplatníka v odůvodněných případech (např. ukončení činnosti společnosti, po skončení řízení o pozůstalosti při úmrtí fyzické osoby apod.) buď z moci úřední, nebo na základě žádosti poplatníka
- V případě ukončení evidence poplatníka budou ukončeny také všechny jeho provozovny.
- Je třeba nastavit návaznost na zneplatnění jeho certifikátů
- Je třeba zablokovat jeho přístupové údaje na portál.

„Registrace“ provozovny

Předpoklady

- V zákoně není konkrétně ošetřena definice „provozovny“. Proto v dalších částech tohoto materiálu předjímáme „provozovnu“ dle dostupných informací a potřeb elektronické evidence tržeb a předjímáme, že bude definice do zákona doplněna. Dále předjímáme, že bude povinnost provozovny přijímající hotovostní tržby dle § 4 registrovat a spravovat
- Vzniká nový registr provozoven! Nikde jinde není registr provozoven, který by vyhovoval potřebám evidence tržeb
- Provozovny by měly jít registrovat jak ručně (jednotlivě) – předpokládá se webový formulář pro zadání - tak i dávkově (v připravené strukturované podobě)
- Každý poplatník musí mít registrovánu alespoň jednu provozovnu
- Údaje provozovny může zadat a editovat pouze poplatník, nikoli Finanční správa správa

Údaje provozovny

O každé provozovně potřebujeme evidovat **DIČ provozovatele provozovny** (napojení na poplatníka) a dále tyto údaje:

- ID provozovny

  je číslo přidělené systémem, minimálně pětimístné, unikátní v rámci poplatníka, nikoli v rámci systému (z důvodu, že toto ID se uvádí na účtence a nesmí být příliš dlouhé)

- Datum registrace (vzniku) provozovny v EET

Typ provozovny

- Stálá (pozn. především kamenné obchody)
- Mobilní (např. taxi, autobusy)
- Semimobilní (např. stánek, cirkus)
- Virtuální (např. e-shop)

Mezi typy nelze přecházet. Pokud je třeba změnit typ provozovny, je nutné ukončit a založit novou provozovnu.

Lokalizace provozovny

(různá pole dle typu provozovny)

- Stálá: Adresa (konkrétní pole budou dle RUIAN)
- Mobilní: jiná identifikace (např. SPZ)
- Semimobilní: textový popis lokalizace (zde je výjimka, lze měnit lokalizaci provozovny)
- Virtuální: URL

Režim provozovny

- běžný
- zjednodušený ze zákona (+ výběr ze zákonných důvodů/podmínek)
- zjednodušený na základě povolení (+ číslo jednací příslušného povolení)

Běžný režim je nejpřísnější a měl by být i nejrozšířenější, takže bude zvolen jako defaultní.

Zákonné důvody pro použití zjednodušeného režimu bez nutnosti podat povolení budou dány vyhláškou.

„Povolovací řízení pro užití zjednodušeného režimu“ je samostatný proces, probíhající mimo EET. Jeho výstupem je povolení zjednodušeného režimu pro provozovnu/y, nebo zamítnutí žádosti. Kladný výsledek řízení zadá poplatník k provozovně – změní režim provozovny na „Zjednodušený na základě povolení“. Režim je také součástí datové věty účtenky.

Stav provozovny

- aktivní
- přerušená činnost
- zrušená

Pozn. Každý stav musí mít počáteční datum, a pokud se nejedná o aktuální stav, tak i koncové datum.

Každá nově založená provozovna má stav Aktivní. Mezi stavy Aktivní a Přerušená činnost lze přecházet oběma směry. Ze stavu Zrušena již nelze stav znovu změnit na žádný jiný.

Činnost provozovny

Seznam vybraných činností z NACE (obory – cca do 20). Konkrétní položky budou definovány. Činností může mít provozovna zvoleno i více najednou.

Obvyklá otevírací doba

Nepovinný údaj, zadávaný formou textové poznámky.

Provoz

- sezónní
- celoroční

Je zde požadavek držet historii stavů a změn údajů provozovny.

Otevřené otázky

1. Jaká definice provozovny bude použita pro výklad tohoto zákona?
2. Jaký je konkrétní seznam činností provozovny (výběr ze seznamu NACE)?
3. Na jakou dobu se povolení vydává? (určitou, neurčitou, po dobu trvání důvodů)

Změny údajů provozovny

Předpoklady

- Změna musí být dle zákona podána elektronickou cestou

Závěry

- Poplatník může měnit vybrané údaje o svých provozovnách výhradně prostřednictvím portálu a to jedině po úspěšném přihlášení
- Větší množství změn by mělo jít provést i dávkově
- Měnit nelze:
  - ID
  - Datum registrace
  - Typ provozovny
  - Lokalizace provozovny (kromě semimobilní)
- Provozovna je tak pevně vázaná (definována) na svou lokalizaci (u stálých provozoven adresou, u mobilních jinou …), že každé „přestěhování“ nebo změna SPZ, či URL adresy e-shopu bude znamenat ukončit a založit novou provozovnu
- Výjimku tvoří semimobilní provozovna, jejíž lokalizace se může měnit
- Za změnu se nepovažuje formální změna jako přejmenování či přečíslování ulice.

Zrušení provozovny

Předpoklady

Zrušení provozovny je věcně vázáno na zákonné důvody, které budou definovány.

Závěry

- Zrušení i Přerušení činnosti provozovny zadává poplatník na portálu – viz změny výše.
- Stav je třeba změnit pro konkrétní provozovnu.
- Ukončení může zadat i finanční správa, ale pouze v případě, kdy jde o deaktivaci poplatníka a tím i zrušení všech jeho provozoven. Samotné provozovny ne.
- Důvod zrušení bude povinně uváděn při změně stavu na „Zrušená“ výběrem jedné z možností.

Pozn. Uživatelsky vhodné nechat jej i uzavřít všechny provozovny „jedním krokem“, ale pak se v zásadě jedná o ukončení evidence poplatníka pro účely EET.

Evidence tržeb

Klíčová procesní oblast, která má na starosti komunikaci mezi koncovým zařízením poplatníka a informačním systémem EET (IS EET).

Tržby jsou zadávány do jednotlivých koncových zařízení (typicky pokladna). Každé koncové zařízení je vždy součástí jedné provozovny, přičemž provozovna může obsahovat více koncových zařízení. Provozovny jsou následně vztaženy k jednomu poplatníkovi. Poplatník je rozlišen na základě DIČ. Každé koncové zařízení je vybaveno certifikátem (i sdíleným přes více zařízení), kterým podepisuje datové věty směřující k IS EET.

Aktéři

Aktér v kontextu evidence tržeb	Popis
IS EET	Přijímá datové věty z koncových zařízení, provádí jejich validaci, ukládá je a generuje odpověď včetně FIK.
Koncové zařízení (také Pokladna)	Informační systém nebo elektronické zařízení poplatníka, které zasílá datové věty a přijímá FIK. Vytváří datové věty obsahující informace o tržbě, podepisuje je, zasílá směrem k IS EET, přijímá odpověď a tiskne účtenku. Koncové zařízení může být interně rozděleno na samotnou „pokladnu“ a centrální komunikační modul. Samotná pokladna tak nemusí být přístupná z Internetu.
Pokladník	Zadává vystavení účtenky.

Pravidla

Seznam pravidel, která se vztahují na evidenci tržeb (účtenek). Zdrojem těchto pravidel je aktuální znění zákona, statistické údaje finanční správy, technická a jiná omezení z hlediska návrhu finálního systému.

ID	Název pravidla	Popis
ET-P-1	Poplatník je povinen zaevidovat platbu v IS EET v okamžiku jejího vzniku.	IS EET potvrzuje přijetí platby do 2 vteřin (mezní doba odezvy). Jedná se o min. dobu, po kterou musí poplatník vyčkat. Maximální doba není omezena, může však být ukončena ze strany informačního systému. Pouze v případě technických problémů je poplatníkovi umožněno zaevidovat platbu do 48 hodin od jejího vzniku. Poplatník má i v takém případě povinnost předat zákazníkovi účtenku.
ET-P-2	Koncové zařízení, které je určeno pro zjednodušený režim evidence tržeb, musí zaevidovat platbu do 120 hodin od jejího přijetí směrem k IS EET.	Pro koncová zařízení ve zjednodušeném režimu neplatí pravidlo okamžitého zaevidování platby. Je dána maximální doba 120 hodin.
ET-P-3	Výměna informační o platbě vzniká na základě datové věty.	Datová věta je XML soubor obsahující informace v požadované struktuře a sémantice.
ET-P-4	Poplatník je povinen vyplnit veškeré relevantní údaje v datové větě, které se týkají konkrétní platební transakce.	Existuje min. sada povinných parametrů. Avšak na základě toho, jaká platba je provedena, poplatník vyplňuje patřičné části datové věty.
ET-P-5	Bude-li chybět jeden z povinných údajů v datové větě, taková zpráva bude odmítnuta.	Povinnými údaji je řádek 3, 4, 5, 6, 7 a 9 v datové větě.

ET-P-6	Datová věta musí být podepsána certifikátem poplatníka, který je vydán certifikační autoritou EET.	Každému poplatníku bude vygenerován jeden certifikát pro elektronické podepisování datových vět. Identifikátorem pro certifikát bude DIČ, obsažen přímo v certifikátu. Certifikát bude platný po dobu 2 let a bude možné ho obnovit. Poplatník může požádat o více certifikátů, vyžaduje-li to charakter jeho provozu (např. více provozních míst, více koncových zařízení apod.).
ET-P-7	Komunikace s IS EET probíhá pomocí zabezpečeného komunikačního kanálu.	Komunikace probíhá na základě webových služeb nad protokolem HTTPS (SSLv3).
ET-P-8	Poplatník je povinen předat koncovému zákazníkovi účtenku.	Účtenku předává jako evidenci proběhlé tržby.
ET-P-9	Součástí vystavené účtenky budou následující bezpečností údaje.	FIK – v případě, že dojde k okamžitému zaevidování platby IS EET, tento kód je navrácen zpět poplatníkovi a stává se součástí účtenky. V případě, že není možné okamžité zaevidování tržby, je tento FIK navrácen až ve chvíli zaevidování a nestává se tak součástí účtenky. BKP – bezpečností kód transakce, který je vypočítán dle vzorce provádějící MD5 funkci nad povinnými a certifikátem podepsanými údaji v datové zprávě. Elektronický podpis – v případě, že není k dispozici FIK, je součástí účtenky její podpis privátním klíčem.
ET-P-10	Rušení zaevidovaných tržeb	Poplatník provádí změny v již zaevidovaných tržbách tím způsobem, že vystaví tržbu novou se zápornou platbou. O této transakci vystavuje účtenku. V datové větě musí být evidována vazba na původní účtenku, i když byla vystavena v rámci jiného koncového zařízení.
ET-P-12	Každá zpráva musí být jednoznačně identifikovatelná.	Jak příchozí, tak odchozí zprávy mezi koncovým zařízením a IS EET budou obsahovat jednoznačný identifikátor UUID.
ET-P-13	Číselné řady účtenek se restartují vždy k 1. 1.	Vždy k 1. 1. dojde k zahájení číselné řady účtenek číslem 0.

Požadavky

Seznam funkčních a nefunkčních požadavků kladených na IS EET z pohledu evidence tržeb. Požadavky vycházejí z uvedených pravidel a dále je rozvíjejí do konkrétních funkčností či charakteristik celého systému. Součástí jsou také požadavky, které jsou kladené na koncová zařízení.

ID	Požadavek	Popis
ET-FP-1	Informační systém EET musí být schopen zaevidovat tržbu.	Tržbou je myšlena platební transakce. Koncové zařízení či poplatník, na kterého se nevztahuje zjednodušený režim je povinen zaevidovat tržbu okamžitě. V případě technických problémů v komunikaci s EET smí provést zaevidování do 48 hodin od vydání účtenky. Zaevidovaná tržba je identifikována na základě FIK.

ET-FP-2	V rámci každého kroku procesu musí docházet k logování klíčových informací.	Konkrétní seznam událostí k logování bude nutné specifikovat. Jedná se o logování událostí typu „koncové zařízení kontaktovalo IS EET“, „neplatný certifikát“, „chybějící povinné údaje“ atd. Předpokládá se, že tyto informace budou z hlediska objemu dat přibližně stejně, jako ukládané datové věty. Logovací soubory bude možné archivovat a zároveň komprimovat jejich velikost.
ET-NP-1	IS EET musí zajistit nepopiratelnost komunikace.	Musí být nepopiratelné, že tržbu zaevidoval konkrétní subjekt. Nepopiratelnost bude založena na podepisování datových vět certifikátem, který bude obsahovat DIČ poplatníka. Podepisování bude provedeno na základě privátního klíče, který je znám pouze poplatníkovi. Bude-li mít poplatník více certifikátů, bude rozlišeno minimálně sériovým číslem certifikátu.
ET-NP-2	IS EET musí zajistit integritu dat.	Musí být znemožněna jakákoli manipulace s datovou větou v rámci komunikace koncového zařízení a IS EET. Komunikace probíhá zabezpečeným kanálem. Může se stát, že tržba je zaevidována v IS EET, ale již nedošlo k přijetí potvrzující zprávy (obsahující FIK) směrem ke koncovému zařízení. V takovém případě koncové zařízení eviduje, že došlo k navázání spojení s IS EET, ale zpráva nebyla uložena. Zároveň se koncové zařízení pokouší o opakované odeslání dat.
ET-NP-3	IS EET musí být schopen zpracovat až 10.000.000.000 transakcí za rok.	Již k 1. 1. 2016 je zapotřebí mít vystavenu tuto infrastrukturu. Avšak počet transakcí bude postupně narůstat. V 1. fázi se počítá se zapojením kolem 10% všech subjektů (60 tis.).
ET-NP-4	IS EET musí být schopen odolat krátkodobému vytížení 4000 transakcí za vteřinu.	Počítá se s chvilkovým vytížením v řádu jednotek vteřin.
ET-NP-5	IS EET musí být schopen evidovat datové věty v obdržené podobě po dobu 10 let a 3 měsíců.	Datová věta, včetně podpisu, bude odpovídat zhruba velikosti 6kB. Za období 10 let, při očekávaném vytížení systému, lze předpokládat objem dat kolem 600 TB. Jednotlivé datové věty budou ukládány s časovým razítkem. Avšak jedno časové razítko bude aplikována na všechny transakce, evidované v jeden den. Za rok tak bude použito 365 časových razítek. Úložiště bude navrženo tak, aby bylo z hlediska kapacity rozšiřitelné. K 1.1.16 nebude zapotřebí plná kapacity.

ET-NP-6	IS EET musí zaevidovat tržbu do 0,33 vteřiny.	Tato doba se počítá od přijetí datové věty na rozhraní IS EET do odeslání datové věty s potvrzujícím FIK kódem. V rámci této dobu je nutné ověřit integritu a nepopiratelnost zprávy, provést extrakci dat, zkontrolovat povinné údaje, uložit do databáze, vygenerovat FIK, připravit odpověď, podepsat a odeslat. Očekává se, že celá transakce, včetně latence sítě má mezní dobu odezvy 2 vteřiny.
ET-FP-3	IS EET musí zvalidovat zaslané údaje, než dojde k zaevidování transakce.	Kontroluje se platnost certifikátu, který podepsal zprávu, platnost certifikátu certifikační autority, shoda identifikátoru certifikátu s DIČ subjektu obsaženého v datové větě, syntaxe údaje pro výpočet BKP. Veškeré další údaje jako návaznost číselné řady účtenek, správně vyplněné číselné hodnoty, správné formáty dalších dat atd. se kontrolují až v následné analýze dat.
ET-NP-7	IS EET musí umožnit rozšiřování datové věty o další parametry.	Z důvodu možnosti rozšiřování IS EET bez významných zásahů do komunikačního protokolu musí být umožněno, aby datová věta mohla být doplněna o další údaje, aniž by bylo zapotřebí upravovat způsob zpracování datové věty na straně IS EET či koncového zařázení. Předpokládá se, že bude dostatečné rezervovat 10 položek od každého typu (číslo, řetězec, true/false).
	Koncové zařízení	
ET-NP-8	Koncové zařízení musí být schopna komunikovat s IS EET na základě zabezpečené komunikace standardem webových služeb.	Jedná se o synchronní komunikaci zabezpečenou protokolem HTTPS. Protokol pro odeslání zpráv webových služeb SOAP 1.1.
ET-FP-4	Koncové zařízení umožní nastavení maximální dobu čekání na odpověď ze strany IS EET.	Maximální doba, po kterou bude koncové zařízení čekat na přidělení FIK k provedené transakci. Poplatník v takto stanoveném čase zohlední možnosti koncového zařízení a dostupnosti internetového připojení. IS EET podle vytížení může uzavřít spojení ještě před touto maximální čekací dobou. Minimální čekací doba (mezdní doba odezvy) je stanovena na 2 vteřiny.
ET-FP-5	Koncové zařízení musí být schopno generovat BKP kód.	Musí být použity stejné algoritmy. Zároveň musí být umožněno BKP kód vygenerovat zpětně a to buď na základě koncovým zařízením evidovanou účtenkou nebo na základě vstupních údajů nutných pro generování BKP kódu.
ET-FP-6	Koncové zařízení musí být schopno podepisovat a ověřovat datové věty.	Nutná podmínka pro správnou komunikaci s IS EET. Podepisování zpráv se děje na základě privátního klíče, který je vygenerován pro poplatníka. Ověřování zpráv se děje pomocí veřejného klíče vydaného pro IS EET.
ET-FP-7	Koncové zařízení musí být schopno notifikovat při blížící se době expirace certifikátu.	Po době expirace certifikátu nebude možné zaevidovat tržbu.
ET-FP-8	Koncové zařízení musí být schopno vygenerovat datovou větu dle pravidel pro její sestavování.	Vytvoření XML souboru s požadovanými údaji, generování UUID.

ET-FP-9	Koncové zařízení musí umožnit opětovné odeslání účtenky, jestliže při prvním odeslání neobdržela FIK (potvrzení).	Opětovné odeslání se může dít automaticky, kdy koncové zařízení pomocí volání rozhraní IS EET zjistí, že systém je funkční a dostupný. Případně se může jednat o ruční úkon na koncovém zařízení. Vždy je však zapotřebí dodržet max. dobu 48 hodin (případně 120 hodin ve zjednodušeném režimu) pro zaevidování tržby. Pokus o opětovné odeslání účtenky se rozlišuje příznakem. Stejně tak se liší doba zaevidování tržby a doba odeslání.
ET-FP-10	Koncové zařízení musí být schopno vytisknout veškeré požadované údaje na účtenku.	V případě, že neobdrží FIK, na účtenku vytiskne pouze BKP, elektronický podpis. V opačném případě obojí.
ET-FP-11	Koncové zařízení musí být schopno fungovat v plném či zjednodušeném režimu.	V případě fungování ve zjednodušeném režimu musí zaevidovat transakci do 120 hodin. V opačném případě do 48 hodin. I ve zjednodušeném režimu může koncové zařízení zaevidovat transakci okamžitě.
ET-FP-12	Koncové zařízení musí umožnit nastavit číslo koncového zařízení (pokladního místa).	Číslo koncového zařízení je jedním z důležitých údajů datové věty.
ET-FP-13	Koncové zařízení musí umožnit generování spojité řady čísel účtenek.	Spojitá řada musí být buď per koncové zařízení nebo per provozovna. Toto rozlišení je provedeno v datové větě.

Popis komunikace

Komunikace mezi koncovým zařízením a IS EET probíhá zabezpečeným HTTPS protokolem, pomocí webových služeb dle protokolu SOAP 1.1. Datové věty jsou XML soubory podléhající definovanému schématu. Podepisování XML dokumentů se děje dle W3C standardu XMLDsig (XML Signature). Před samotným podpisem dochází ke „kanonizaci“ XML zpráv, aby bylo zajištěno shodného podpisu u zpráv, mající identickou XML strukturu a obsah.

Datová věta

Slouží k zaevidování platební transakce. Specifikace datové věty je obsažena v samostatném dokumentu. Součástí je seznam položek, které se dělí na hlavičku a samotný obsah datové věty. Hlavička obsahuje základní údaje o zasílané zprávě směrem k IS EET. Tyto údaje nejsou podpisovány na straně koncového zařízení. Ostatní údaje podléhají podpisu ze strany koncového zařízení.

Potvrzující datová věta

Slouží k potvrzení evidence platební transakce a předání identifikátoru FIK. Specifikována je součástí samotného dokumentu.

Zabezpečení komunikace

Komunikace mezi koncovým zařízením a IS EET je na síťové vrstvě zabezpečena (šifrována) HTTPS protokolem. Jednotlivé zprávy jsou podepisovány primárními klíči svých odesílatelů (používá se asymetrické šifrování). Datová věta je podepisována privátním klíčem poplatníka (koncového zařízení), potvrzující datová věta naopak privátním klíčem IS EET. Veřejný klíč poplatníka je podepsán certifikační autoritou IS EET.

Pro šifrování dat na síťové vrstvě je využíván SSL akcelerátor. Za tímto akcelerátorem, v zabezpečené síti IS EET, jsou data zasílána v otevřené podobě z důvodu rychlosti zpracování.

Pro jednoznačnou identifikaci poplatníka obsahuje jeho certifikát údaj DIČ. Ten se musí shodovat s DIČ uvedeným v datové větě.

Způsob komunikace

Samotnou komunikaci (včetně podepisování, generování BKP, čísla účtenky atd.) s IS EET nemusí provádět jednotlivá pokladna. Ta může být zastoupena centrálním či jiným systémem na straně poplatníka. Zároveň procesní kroky v kontextu koncového zařízení mohou být realizovány jiným způsobem či v jiném pořadí (dle typy koncového zařízení, technických možností, softwarového vybavení atd.), např. zda bude na straně koncového zařízení docházet k ukládání kompletních a podepsaných datových vět pro pozdější odeslání nebo jestli s každým odesláním bude datová věta nově vytvářena a podepisována.

Konkrétní způsob vytváření a přijímání datových vět je vnitřní záležitostí poplatníka. Bezpodmínečně je však nutné každou tržbu zaevidovat a obdržet její FIK.

Generování BKP

Bezpečnostní kód poplatníka. Jedná se o kód generovaný veřejně dostupným algoritmem a prokazuje jednoznačnou vazbu mezi poplatníkem a účtenkou. Je součástí každé účtenky.

Chybové stavy

Níže uvedené chybové stavy popisují situace, kdy nedojde k řádnému zaevidování tržby. Způsob vypořádání chybového stavu je závislý na konkrétní příčině. Některé chybové mohou generovat notifikace do modulu *EETAuditSpojení*.

Koncovému zařízení se nepodaří spojit se IS EET

Výpadek na straně IS EET nebo jakákoli chyba sítě. Ukládá povinnost zaregistrovat tržbu nejpozději do 48 hodin, případně 120 ve zjednodušeném režimu evidence tržeb.

IS EET přijal chybnou datovou větu

Datová věta nebyla podepsána validním certifikátem nebo nesouhlasí identifikační údaj certifikátu a DIČ v datové větě.

IS EET přijal chybná data v datové větě

Chybný formát XML datové věty nebo chybná syntaxe povinných údajů. Sémantika informací (např. správnost data, existence provozovny, sekvenčnost číselné řady) se kontroluje až po zaevidování v rámci detailní analýzy vkládaných dat.

IS EET se nepodařilo uložit data

Chyba při ukládání dat nebo původní datové věty.

Koncové zařízení neobdrželo zpětnou potvrzující zprávu od IS EET

Případ, kdy bude vygenerován FIK, ale koncové zařízení či cokoli jiného uzavře spojení a potvrzující datová věta nebude koncovým zařízením přijata. Koncové zařízení při neobdrženém FIK provádí opětovné zaslání a nastavuje příznak opětovného zaslání tržby.

Koncové zařízení obdrželo chybnou zpětnou potvrzující zprávu od IS EET

Potvrzující datová věta nebyla řádně podepsána certifikátem IS EET nebo nastala chyba formátu dat.

Chybové zprávy

Kód chyby	Chybová zpráva
1	Zaslaná datová věta neodpovídá předepsanému formátu.
2	Datová věta byla podepsána certifikátem, který nebyl vystaven certifikační autoritou IS EET.
3	Certifikát, kterým byla podepsána datové věta, neobsahuje identifikaci poplatníka (DIČ).
4	Neplatný podpis datové věty.
5	Datová věta obsahuje jinou identifikaci poplatníka (DIČ), než je uvedena v certifikátu.
6	Chyba při zpracování datové věty.

Procesy Evidence tržeb

Požadavek na zaevidování tržby

Tímto krokem dává pokladník pokyn koncovému zařízení, aby před vytištěním účtenky provedlo zaevidování tržby do IS EET. Požadavek může být opakovaný a to ve chvíli, kdy dojde k chybě v rámci zaevidování a nebude přidělen FIK transakce. V takovém případě je poplatník povinen zaevidovat tržbu v rámci 48 hodin.

Vygenerování BKP

Koncové zařízení na základě dostupných údajů z účtované transakce proveden generování BKP kódu dle definovaného algoritmu. BKP kód je jednou z klíčových bezpečnostních mechanizmů evidence tržeb. BKP je součástí datové věty, jeho generování předchází tvorbě datové věty.

Vytvoření a podepsání datové věty

vytvoření datové věty dle XML schématu, vyplnění všech potřebných dat, čísla účtenky. Podepsání datové věty privátním klíčem.

Koncové zařízení na základě XML schématu vytvoří patřičnou datovou větu. Poplatník je povinen vyplnit veškeré relevantní údaje. V tomto kroku dochází také ke generování čísla účtenky dle modelu zvoleného poplatníkem (číselná řada pokladny nebo číselná řada skrze provozovnu). Datovou větou kanonizuje a podepisuje na základě standardu XMLDiag svým privátním klíčem.

Zaslání datové věty směrem k IS EET

Podepsanou datovou větu koncové zařízení zasílá směrem k IS EET pomocí standardu webových služeb (synchronní způsob komunikace). Komunikace je zabezpečena protokolem HTTPS. Hlavička zprávy webové služby obsahuje UUID (generovaný dle standardu) a čas odeslání datové věty. Bude-li koncové zařízení zasílat více datových vět (zejména když eviduje ve zjednodušeném režimu) je vhodné, aby pro komunikaci s IS EET vytvořila pouze jedno HTTPS spojení. Vytvoření a uzavření zabezpečeného komunikačního kanálu má významný vliv na dobu odpovědi.

U poplatníků/koncových zařízení, které jsou evidovány v režimu zjednodušené evidence tržeb, může tento krok být realizován v době do 120 hodin od vystavení účtenky. V ostatních případech musí dojít k pokusu zaslání datové věty směrem k IS EET v okamžiku vystavení účtenky.

V případě chyby při zaslání datové věty (koncové zařízení neobdrží FIK), jsou tyto datové věty evidovány k opětovnému odeslání, ke kterému může dojít automaticky nebo manuálně (na základě pokynu pokladníka).

Příjem a zpracování datové věty na straně IS EET

Při přijetí datové věty IS EET zkontroluje nepopiratelnost a integritu datové věty. Zároveň provede validaci XML formátu dat a syntaxe povinných údajů. Pouze korektně vytvořené datové věty budou přijaty k dalšímu zpracování a bude k nim vygenerován FIK.

Vstupní branou do IS EET bude SSL akcelerátor, který bude zabezpečovat HTTPS komunikaci. Za touto branou již veškerá data půjdou v nezašifrované formě. Nezašifrované XML zprávy příjme XML akcelerátor pro provedení základních validací.

Generování FIK

Příjme-li IS EET validní datovou větu, provede generování FIK.

Uložení a archivace

Extrahovaná data z datové věty jsou ukládány do databáze (včetně vygenerovaného FIK). Původní datové věty jsou ukládány do archivu. Jestliže se jedná o opětovně zaslanou větu (nastaveny element v datové větě, shodné BKP), která již byl přidělen FIK je použita poslední zaslaná datová věta a původní zpráva je odstraněna.

Vytvoření a podepsání datové věty

IS EET vytváří potvrzující datovou větu dle definovaného XML schématu. Bude-li vygenerován FIK, IS EET tuto datovou větu podepíše svým privátním klíčem. V opačném případě došlo k chybě. Datové věty chybového stavu podepisovány nejsou a odpovídají kapitole Chybové zprávy.

Zaslání datové věty zpět ke koncovému zařízení

Vytvořenou potvrzující datovou větu IS EET zasílá zpět vytvořeným HTTPS spojením zpět ke koncovému zařízení. Datová věta obsahuje UUID a čas odeslání.

Příjem a zpracování datové věty na straně koncového zařízení

Přijde-li podepsaný potvrzující datová věta, koncové zařízení provede kontrolu nepopiratelnosti a integrity. Získá z datové věty FIK.

Zaevidování datové věty pro pozdější odeslání

Obsahuje-li zpráva FIK, došlo k jejímu zaevidování a koncové zařízení již neeviduje tuto tržbu k opětovnému zaslání. V opačném případě ano a poplatník je povinen provést opětovný pokus o zaevidování. Nastane-li chyba v rámci komunikace s IS EET (např. spojení v době odesílání FIK směrem ke koncovému zařízení nebude dostupné) je i takto datová věta, která byla v této komunikaci zasílána, zaevidována pro opětovné odeslání (koncové zařízení může provést další pokus).

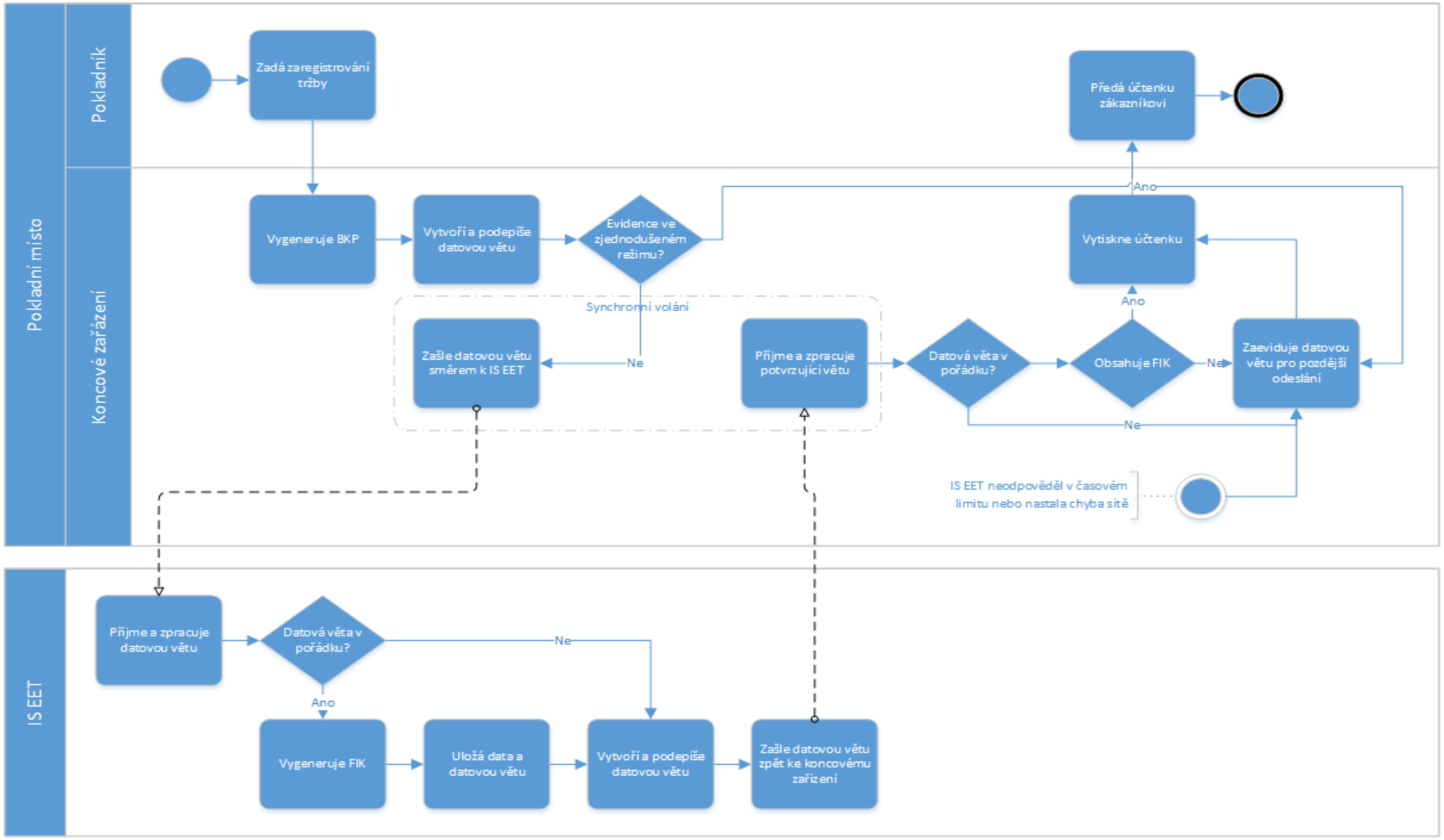
V případě, že koncové zařízení pracuje ve zjednodušeném režimu evidence tržeb, může k tomuto kroku přistoupit, aniž by provedlo zaevidování v IS EET. Tuto povinnost má do 120 hodin.

Uložení přijatých dat

Koncové zařízení může provést uložení přijatých dat pro svou vlastní evidenci.

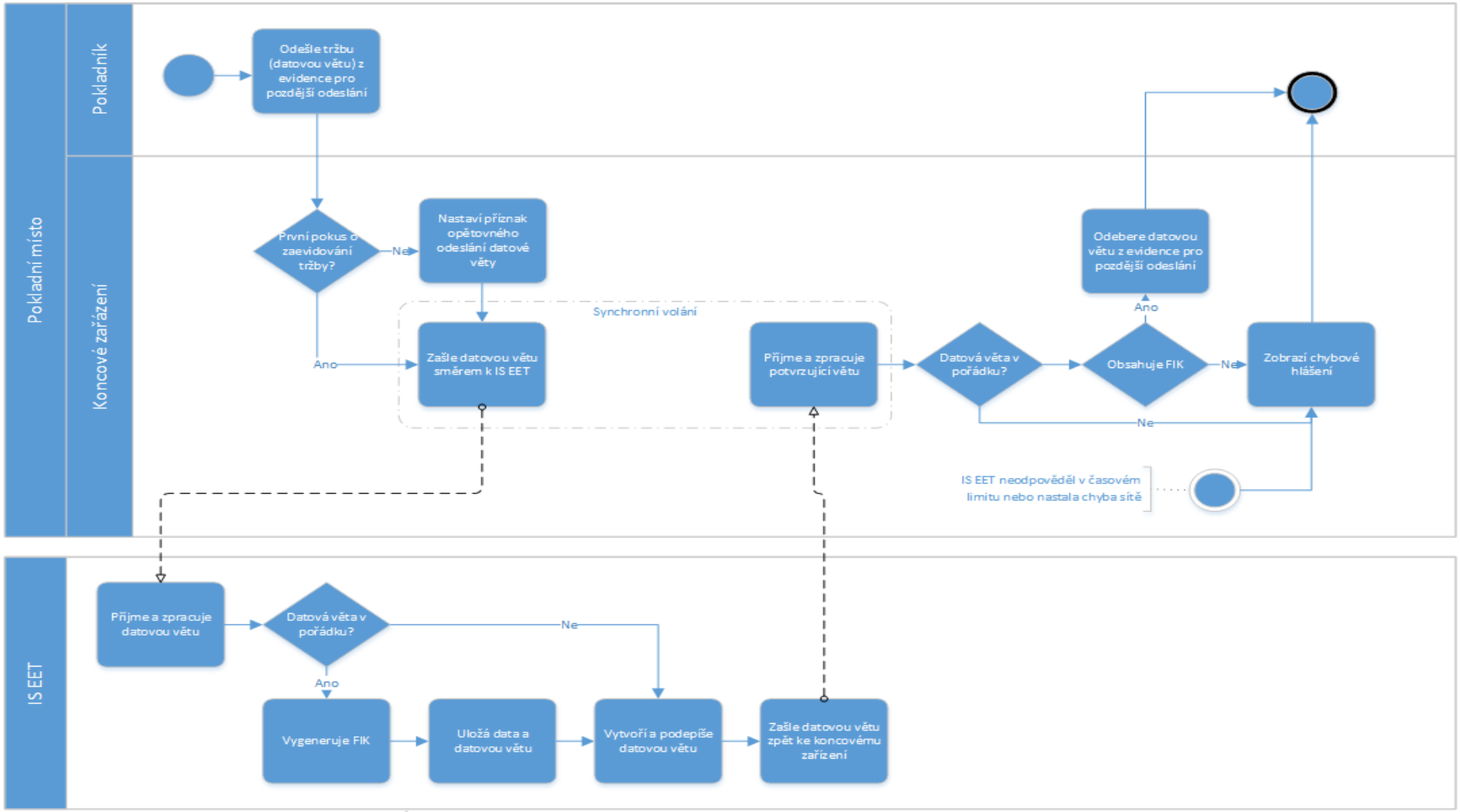
Vytištění a předání účtenky

K vytištění a předání účtenky zákazníkovi musí dojít vždy. V případě, že dojde k přijetí FIK, je na účtenku vytištěn společně s BKP kódem. V opačném případě je místo FIK na účtenku vytištěn podpis dané účtenky.



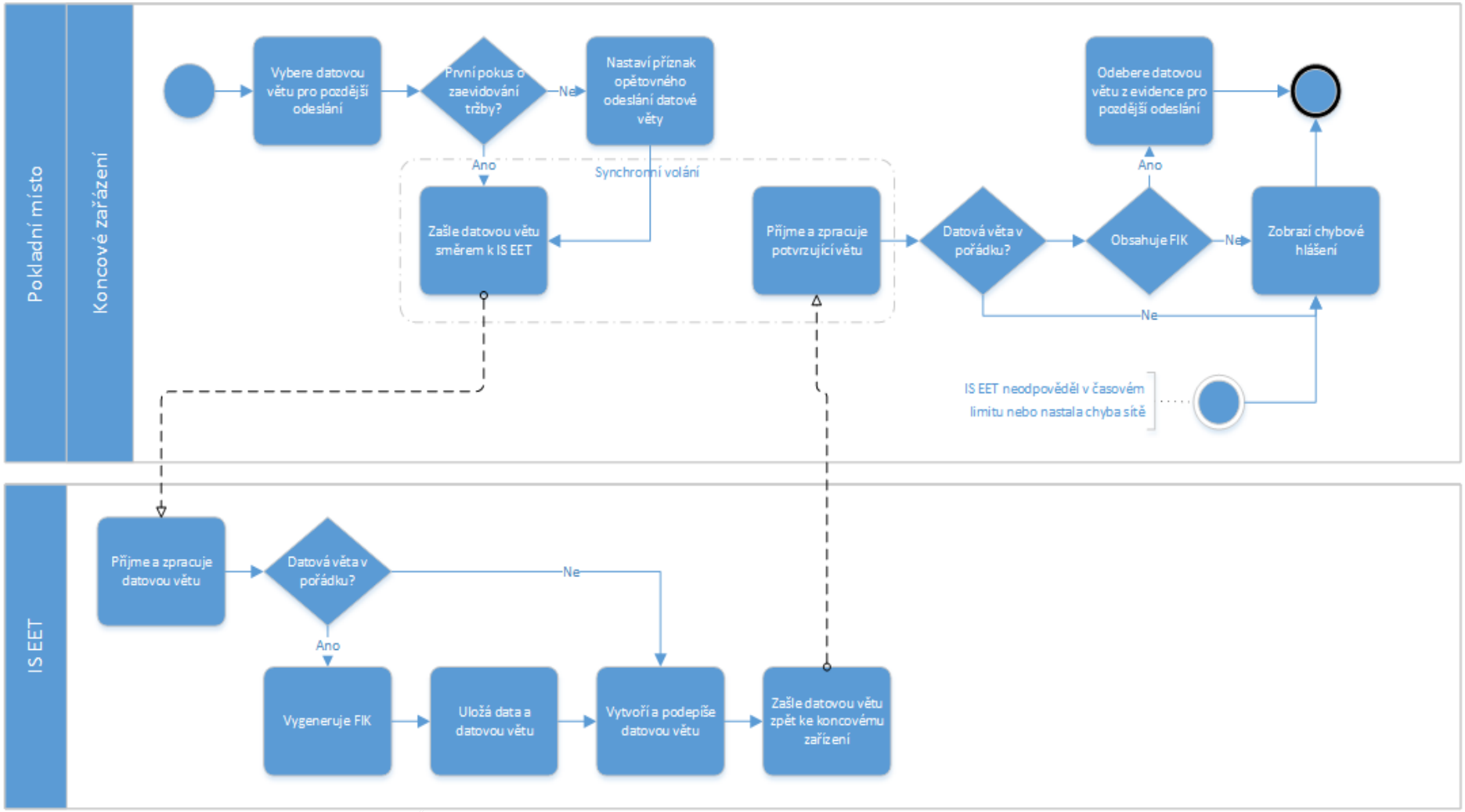
Obrázek 8: Evidence tržeb - základní proces zaevidování tržby pokladníkem

Evidence proběhne současně s vytištěním účtenky. Ve zjednodušeném režimu může dojít k zaevidování tržby pro pozdější odeslání.



Obrázek 9: Evidence tržeb - zaevidování tržby v době 48 hodin po vystavení účtenky (v případě zjednodušeného režimu 120 hodin) pokladníkem

První pokus je validní pouze v rámci zjednodušeného režimu evidence tržeb.



Obrázek 10: Evidence tržeb - zaevidování tržby v době 48 hodin po vystavení účtenky (v případě zjednodušeného režimu 120 hodin) automatizovaně na straně koncového zařízení

První pokus je validní pouze v rámci zjednodušeného režimu evidence tržeb. První pokus je validní pouze v rámci zjednodušeného režimu evidence tržeb.

Dávková evidence tržeb

Pro dávkové zpracování není vytvořeno samostatné rozhraní na straně IS EET. Veškeré datové věty je zapotřebí podepisovat a zasílat směrem k IS EET samostatně a sekvenčně.

Případy užití

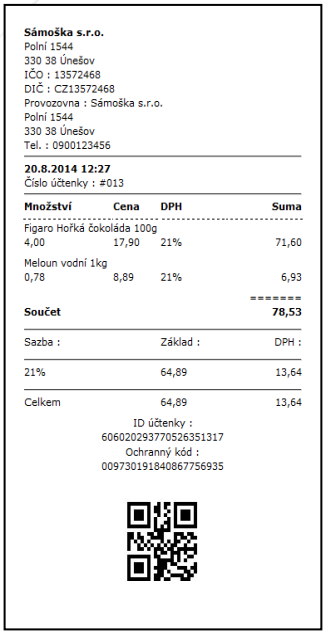
V rámci uvedených procesů je zapotřebí zohlednit následující případy užití.

- Zaevidování tržby v běžném režimu s obdržením FIK
- Zaevidování tržby ve zjednodušeném režimu s obdržením FIK
- Nedostupnost spojení k IS EET
- Chyba spojení při zpětném zasílání FIK
- Manuální pokyn pokladníka k opětovnému zaevidování tržby
- Automatické opětovné zaevidování tržby
- Hromadné zpracování tržeb
- Chyba při ověřování certifikátu datové věty
- Chyba při ověřování certifikátu potvrzující datové věty
- Chyba formátu XML datové věty
- Chyba při ukládání dat

Účtenka

Údaje, které musí být součástí účtenky, jsou řešeny patřičnou vyhláškou a jsou uvedeny v samostatném dokumentu. Každá účtenka musí mimo jiné obsahovat:

- BKP – tento údaj je obsažen při každém vystavení účtenky.
- FIK – pouze v případě, že IS EET tento údaj vrátí při zaevidování tržby.
- Podpis – není-li FIK k dispozici, účtenka je podepisována elektronickým podpisem (privátním klíčem) provozního místa (resp. poplatníka). V případě velkého množství znaků v podpisu je možné na účtenku vytisknout QR kód.
- Číslo účtenky – pořadové číslo účtenky, číslo provozovny a číslo pokladny.



Sámoška s.r.o.
Polní 1544
330 38 Únešov
IČO : 13572468
DIČ : CZ13572468
Provozovna : Sámoška s.r.o.
Polní 1544
330 38 Únešov
Tel. : 0900123456

20.8.2014 12:27
Číslo účtenky : #013

Množství	Cena	DPH	Suma
Figaro Hořká čokoláda 100g			
4,00	17,90	21%	71,60
Meloun vodní 1kg			
0,78	8,89	21%	6,93
Součet			**78,53**

Sazba :	Základ :	DPH :
21%	64,89	13,64
Celkem	64,89	13,64

ID účtenky :
606020293770526351317
Ochranný kód :
009730191840867756935

Přístup poplatníka k vlastním agregovaným údajům

Procesní oblast, která má za cíl informovat poplatníka o nashromážděných údajích týkajících se evidence vlastních tržeb. Veškeré údaje jsou získávány z procesu Evidence tržeb.

Aktéři

Aktér	Popis
IS EET	Poskytuje informace o agregovaných datech.
Poplatník	Prochází agregovaná data.

Požadavky

ID	Požadavek	Popis
SU-F-1	IS EET musí poskytovat poplatníkovi agregované údaje na denní, měsíční, kvartální a roční bázi.	Tržby poplatníka jsou agregována skrze denní, měsíční, kvartální a roční pohledy. U každého poplatníka je tak evidováno 382 číselných údajů, udávající tržbu (v datové větě položka Celková částka tržby), v jednom roce (365 dní + 12 měsíců + 4 kvartály + 1 rok).
SU-F-2	IS EET musí poskytovat agregované údaje na denní, měsíční, kvartální a roční bázi dle provozovny poplatníka.	U každé provozovny je evidováno 382 údajů o tržbě.
SU-F-3	Agregovaná data budou poplatníkovi poskytnuta skrze webové rozhraní.	Pro přístup poplatníka k vlastním agregovaným datům bude využito webové rozhraní IS EET (portál). Poplatníkovi bude na základě úspěšného přihlášení umožněno data procházet.
SU-F-4	IS EET musí při zobrazování agregovaných dat respektovat oprávnění přihlášeného uživatele.	Má-li přihlášený uživatel oprávnění zobrazovat agregované údaje pouze některých provozoven, nebude mu zobrazen zbytek dat, stejně tak agregovaná data skrze všechny provozovny.
SU-F-5	IS EET musí poskytovat možnost exportu zobrazených dat.	Pro konkrétní výpisy agregovaných dat (roční, kvartální, měsíční a denní) IS EET poskytne možnost exportu pro jejich stažení poplatníkem.
SU-N-1	Ukládání a výpočet agregovaných dat nesmí mít vliv na procesy určené k evidenci tržby.	Data pro poskytování agregovaných dat by měla být ukládána v datovém skladu, který je oddělen od databáze pro evidenci tržeb. Výpočet agregovaných dat a jejich poskytování tak nebude mít vliv na infrastrukturu určenou k evidenci tržeb (nebude ji zatěžovat či jinak zpomalovat).
SU-N-2	IS EET bude evidovat denní agregovaná data pouze v aktuálním roce.	Za předchozí roky tyto data nebudou dostupná, pouze měsíční, kvartální a roční.

Proces zobrazení vlastních agregovaných dat

Popis jednotlivých kroků procesu.

Zadání přihlašovacích údajů

Uživatel (poplatník) přistupuje na veřejně dostupný portál IS EET. Provádí přihlášení pomocí získaných přihlašovacích údajů.

Ověření uživatele a přihlášení

IS EET ověří (provede autentizaci) uživatelem zadané přihlašovací údaje a v případě úspěšného ověření provede přihlášení.

Zobrazení agregovaných dat poplatníka/provozovny

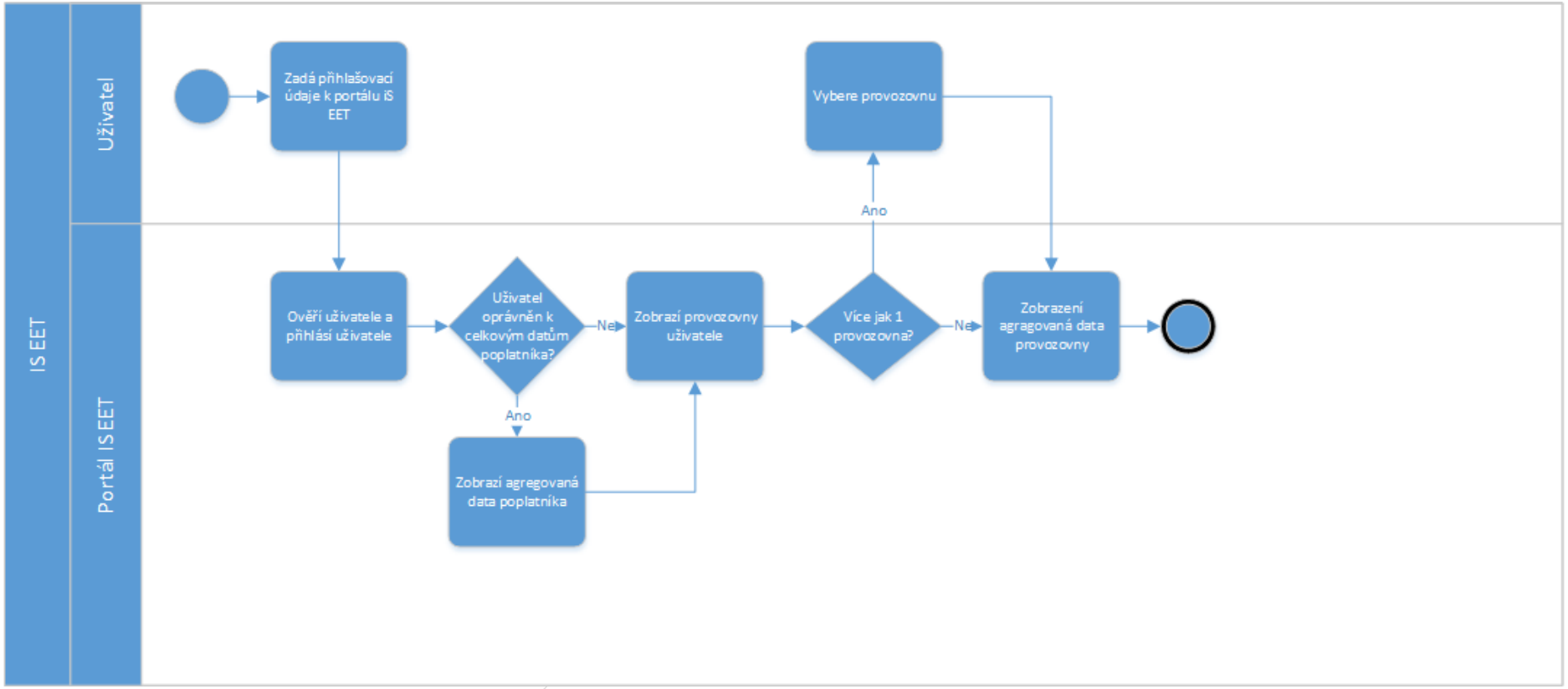
Má-li uživatel oprávnění (autorizace) k zobrazení veškerých agregovaných dat poplatníka, jsou mu zobrazeny. V opačném případě jsou mu zobrazena agregovaná data skrze jednotlivé provozovny.

Uživatel vybírá mezi denním, měsíčním, kvartálním či ročním pohledem.

Uživatel může zvolit zobrazení agregovaných dat v jiném, než aktuálním roce. V takovém případě jsou zobrazen pouze měsíční, kvartální a roční agregovaných údaj.

Zobrazení/výběr provozovny

Má-li uživatel oprávnění zobrazovat agregovaná data více provozoven, je mu zobrazen jejich seznam. Po výběru provozovny uživatelem jsou uživateli zobrazeny agregovaná data provozovny.

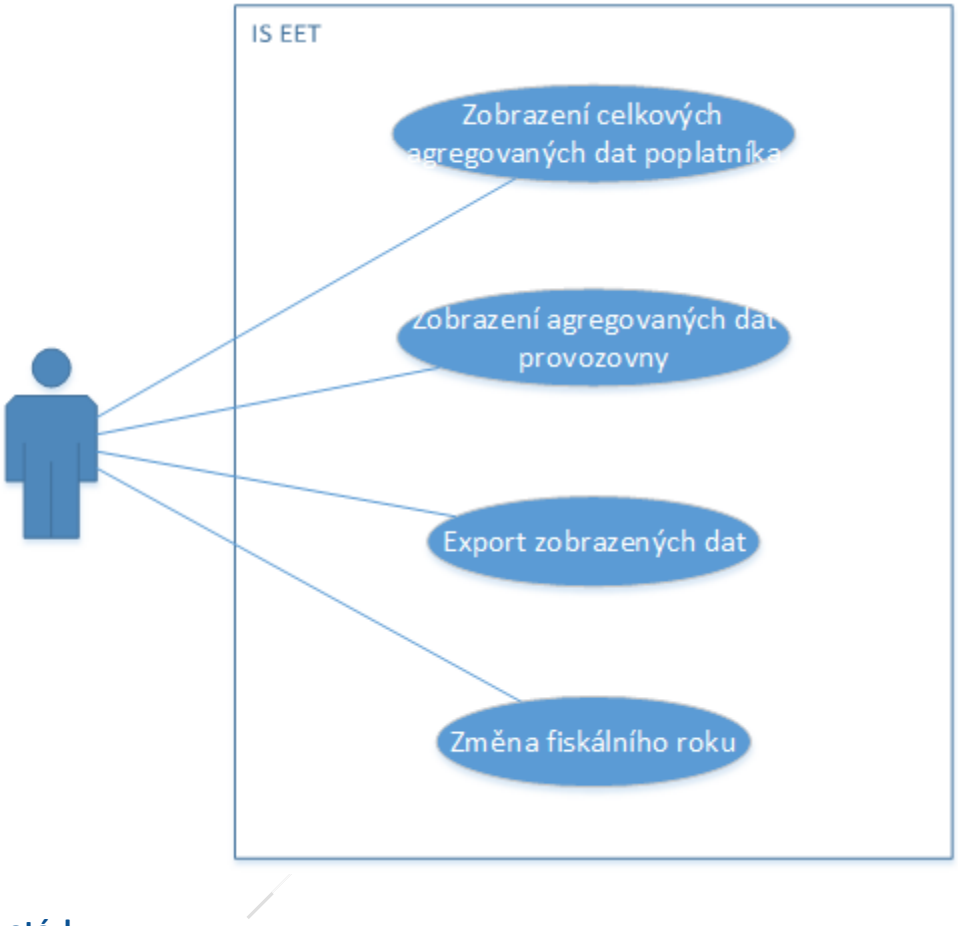


Obrázek 11 Zobrazení agregovaných dat

Případy užití

V rámci proces je zapotřebí zohlednit následující případy užití.

- Zobrazení celkových agregovaných dat poplatníka
- Zobrazení agregovaných dat jedné provozovny uživatele
- Zobrazení agregovaných dat v jiném fiskálním období
- Export zobrazených agregovaných dat



Otevřené otázky

1. Jak to bude s retencí dat? Budou se udržovat veškerá dat a jak dlouho? Nebo detail se bude držet pouze v aktuálním roce a pro předchozí roky bude k dispozici pouze 17 údajů (měsíce, kvartály a roky)?
2. Jakým způsobem bude realizován výpočet agregovaných dat? Denně to bude každý den. Měsíčně to bude 1. den v měsíci nebo to bude počítáno ode dne, kdy se poplatník registroval? To by mohlo být vhodné pro rozdělení zátěže (i když je otázkou jaká distribuce v rámci měsíce bude).
3. Bude nutné data filtrovat dle provozovny? Abych např. některým lidem ukázal pouze část dat a ne všechny? Půjdeme až na úroveň pokladny?
4. Je dostatečné agregovat skrze Celkovou částku tržby v datové větě? Nebo je nutné zahrnout i jiné cenové položky? Jak naložit s vouchery, SMS platbami, dobírkami apod.?
5. Bude umožněn export dat?

Kontrola účtenky zákazníkem

Procesní oblast, která má na starosti kontrolu validity účtenky informačním systémem EET (IS EET).

Tržby jsou evidovány v rámci jednotlivých POS (Point of Sale), dále pokladna. Poplatník má povinnost každou účtenku zaevidovat, tj. zadat její kód do IS EET, který vede evidenci účtenek (dále tržeb). Zákazník má možnost ověřit si, že byla tržba korektně zpracována. IS EET s případnými falešnými účtenkami dále pracuje, a odpovědné osoby, kontroloři, na základě těchto informací provedou případnou kontrolu poplatníka (další proces).

Aktéři

Aktér v kontextu evidence tržeb	Popis
IS EET	Přijímá informace kontrolované účtence, tyto informace zpracuje a vyhodnocuje, případně je ukládá a generuje data potřebná pro kontrolu.
Zákazník	Vkládá informace z účtenky.

Pravidla

Seznam pravidel, která se vztahují ke kontrole účtenky. Zdrojem těchto pravidel jsou aktuální postupy kontrolních úřadů, technická a jiná omezení z hlediska návrhu finálního systému.

Název pravidla	Popis
Zákazník kontroluje účtenku	IS EET musí umožnit kontrolu vydané účtenky.
Při nevalidní účtence musí IS EET poskytnout Zákazníkovi možnost identifikovat provozovnu, kde mu byla účtenka vydána.	IS EET po kontrole nevalidní účtenky poskytne možnost zadat informace nezbytné k identifikaci provozovny. Tyto informace budou zaznamenány pro ověření kontrolním orgánem.
IS EET dosud nezaevidovanou účtenku po uplynutí definovaného času zkontroluje.	IS EET musí v případě ještě neevidované účtenky tuto po uplynutí definovaného času zkontrolovat, zda byla dodatečně zaevidována.
Zákazník vyplňuje veškeré relevantní údaje, které se vztahují ke konkrétní účtence.	Při kontrole účtenky je povinen zákazník zadat FIK, případně BKP (společně s datem transakce a částkou) uvedené na účtence. Bez těchto informací nemůže být kontrola provedena. Pro zamezení opakovaného vydávání stejných BKP/FIK, které jsou již systémem potvrzeny (a účtenky by se zákazníkovi jevila jako validní a zaevidovaná) je nutné požadovat zadání data tržby a částky.

Požadavky

Seznam funkčních a nefunkčních požadavků kladených na IS EET v kontextu kontroly validity účtenky. Požadavky vycházejí z uvedených pravidel a dále je rozvíjejí do konkrétních funkčností či charakteristik celého systému.

ID	Požadavek	Popis
KU-1	Informační systém EET musí být schopen zkontrolovat účtenku.	Kontrolou účtenky je myšleno poskytnutí informací z účtenky pro ověření, zda poplatník tržbu zaevidoval.
KU-2	Po zadání FIK/BKP musí systém zákazníkovi odpovědět.	Systém po zadání dat pro kontrolu musí zákazníkovi odpovědět, zda je účtenka zaevidovaná nebo nikoli. V případě, že účtenka ještě nebyla do systému zadána a plyne zákonní doba, zákazník je na tuto skutečnost upozorněn.

KU-3	Neevidovaná účtenka musí být systémem zaznamenána.	V případě, že je kontrolovaná účtenka neevidovaná (FIK v systému neexistuje, BKP nebylo off-line do systému doplněno, případně jsou data falešná) IS EET musí toto zaevidovat a zpřístupnit pro zpracování kontrolním orgánem.
KU-4	IS EET musí zajistit notifikaci pro potřeby kontroly.	Po zaevidování účtenky systém zajistí notifikaci kontrolního orgánu, který bude věc dále prověřovat.
KU-5	IS EET nesmí odmítnout kontrolu.	IS EET musí přijat každou kontrolu účtenky, která bude mít vyplněné povinné informace.
KU-6	IS EET pro nezaevidované účtenky sbírá další informace.	Při kontrole nezaevidované účtenky se systém pokusí o získání dodatečných informací o transakci od zákazníka (název a lokace provozovny a poplatníka, datum tržby, částka, poznámka a další) pro potřeby kontroly.
KU-7	IS EET bude schopen ověřit účtenku, která je uložená v „rychlé“ části systému.	IS EET bude pracovat s účtenkami ve dvou částech. První část bude obsahovat nejnovější rychlá data, nad kterými bude možné provádět kontrolu. Starší účtenky budou přesouvány do archivní části systému (pro analýzy apod.), kde již účtenku nebude možné ověřit.

Popis komunikace

Kontrola účtenky

Zákazník v prvním kroku zadává následující informace:

- FIK případně BKP
  Informace jsou použity k verifikaci, zda daná tržba byla zaevidována systémem a zaznamenána.
- Částka
  Informace použita k verifikaci validity evidence tržby.
- Datum nákupu
  Informace použita k verifikaci validity evidence tržby.
- IČ/DIČ
  V případě, že je účtenka nezaevidovaná, je použito k identifikaci poplatníka.
- Název provozovny
  V případě, že je účtenka nezaevidovaná, je použito k identifikaci provozovny.
- Adresa provozovny
  V případě, že je účtenka nezaevidovaná, je použito k identifikaci provozovny.
- Poznámka a další údaje
  V případě, že je účtenka nezaevidovaná, je použito k identifikaci provozovny.

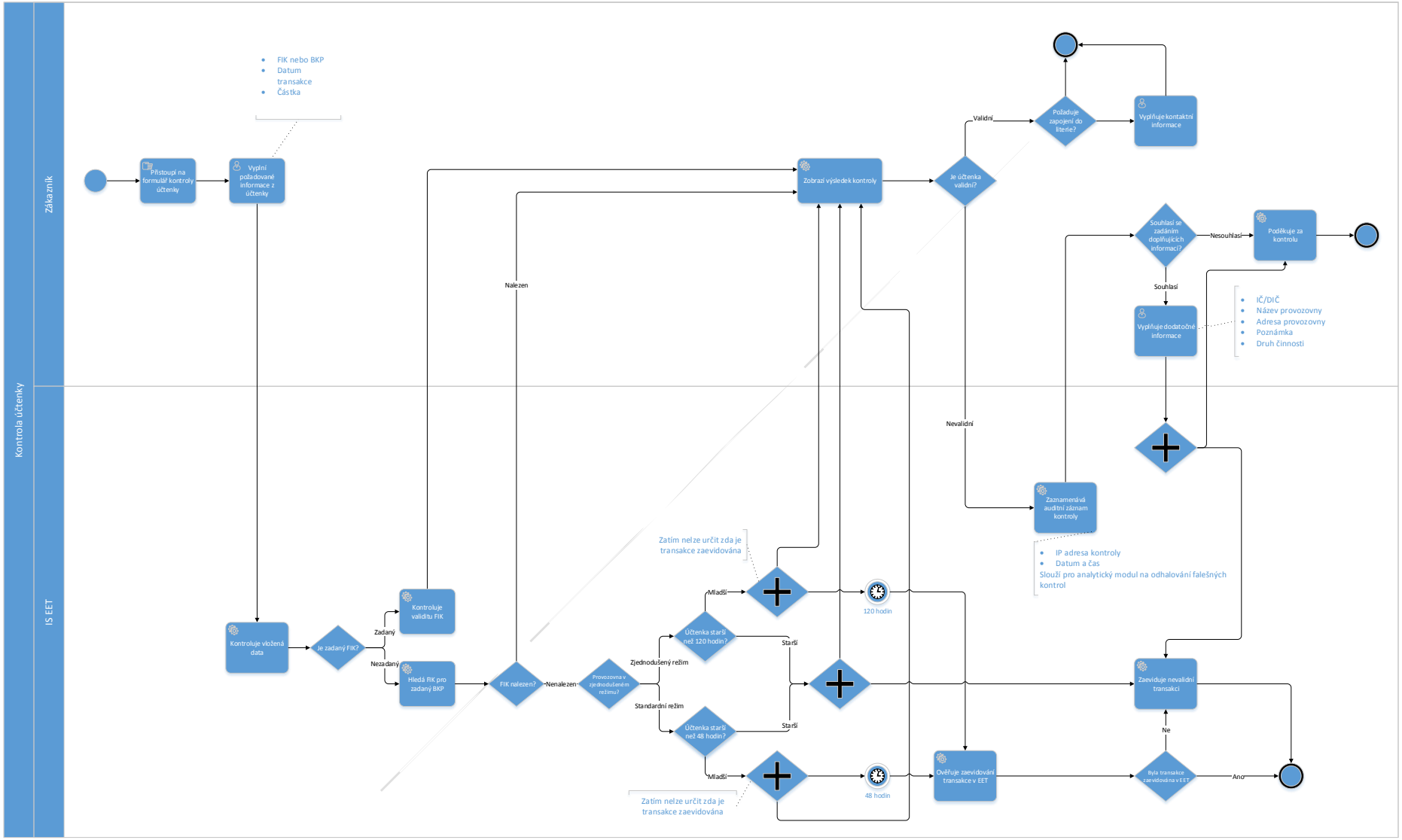
Logování událostí

Systém loguje různé technické informace kontroly nevalidních účtenek (IP adresa, User-agent, datum a další), které mohou být použity pro kontrolu „podvodného“ nahlašování (konkurence apod.). Tato funkcionalita bude předmětem analytického modulu.

Proces Kontrola účtenky zákazníkem

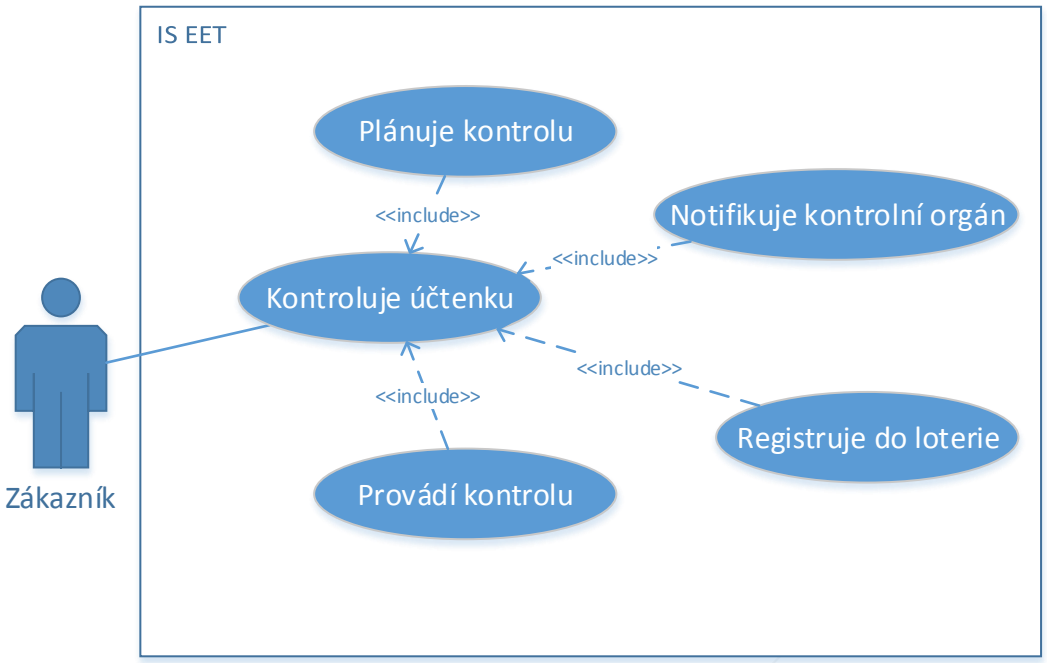
Popis kroků procesu

1. Zákazník přistoupí na formulář pro kontrolu účtenky. Formulář může být realizován na webovém portálu, případně součástí mobilní aplikace (která může účtenku ověřit pomocí fotoaparátu).
2. Zákazník vyplní požadované informace.
3. IS EET zkontroluje, zda byla účtenka zaevidována.
4. V případě korektní evidence je zákazník informován, požádán, zda souhlasí se zařazením do loterie. V případě souhlasu jsou vyžádány jeho kontaktní údaje a proces je ukončen.
5. V případě nemožné kontroly z důvodu časové prodlevy (při off-line zpracování pokladnou), systém identifikuje, zda provozovna pracuje ve zjednodušeném režimu a naplánuje kontrolu realizace evidence tržby. Zákazník je informován o faktu, že tržba není zatím zaevidována a je požádán o případné doplňující informace (pro případ že poplatník po uplynutí zákonem definovaného času tržbu nezaeviduje). Proces končí poděkováním.
6. V případě nesprávné evidence (od data nákupu uplynulo 48, případně 120 hodin a BKP v systému není zaevidováno, FIK je systémem neevidován) je zákazník požádán o další informace o transakci a poplatníkovi/provozovně (z důvodu možných falešných dat na účtence se systém pokusí o získání nejen DIČ z účtenky ale i dalších informací) a systém tyto data zaznamená.
7. Kontrolní orgán je notifikován o nové nekorektní účtence.



Obrázek 12: Kontrola účtenky zákazníkem

Případy užití



Základním případem užití je „Kontroluje účtenku“, který je blíže procesně rozpracován. Další případy užití jsou následující

- Plánuje kontrolu
  Systém na základě provozovny a jejího režimu naplánuje kontrolu evidenci tržby.
- Provede kontrolu
  Systém po uplynutí definované doby zkontroluje evidenci tržby a zaznamená případný nekorektní evidenci.
- Registruje do loterie
  Zákazník se při korektní účtence může zúčastnit loterie. Pro zapojení musí vyplnit kontaktní údaje, které jsou zaznamenány.
- Notifikuje kontrolní orgán
  Informační systém zašle notifikaci (konkrétní implementace není předmětem tohoto popisu, může se jednat o emailovou notifikaci, případně notifikaci v samotném systému) kontrolnímu orgánu o existenci nově zaznamenané nekorektní účtence.

Nahlášení neobdržené účtenky zákazníkem

Procesní oblast, která má na starosti zprostředkování oznámení o nevydané účtence zákazníkem do informačního systému EET (IS EET).

Tržby jsou evidovány v rámci jednotlivých POS (Point of Sale), dále pokladna. Poplatník má povinnost každou účtenku zaevidovat, tj. zadat její kód do IS EET, který vede evidenci účtenek. V případě, že poplatník zákazníkovi nevydá účtenku, co je jeho povinnost, musí IS EET umožnit tuto skutečnost oznámit. S těmito skutečnosti dále pracují odpovědné osoby, kontroloři, kteří na základě těchto informací provedou případnou kontrolu poplatníka (další proces).

Aktéři

Aktér v kontextu evidence tržeb	Popis
IS EET	Přijímá informace o nevydané účtence, tyto informace zpracuje, ukládá je a generuje data potřebná pro kontrolu.
Zákazník	Vkládá a upřesňuje informace o poplatníkovi, resp. provozovně, kde mu nebyla vydána účtenka.

Pravidla

Seznam pravidel, která se vztahují k ohlašování nevydání účtenky. Zdrojem těchto pravidel jsou aktuální postupy kontrolních úřadů, technická a jiná omezení z hlediska návrhu finálního systému.

Název pravidla	Popis
Zákazník nahlašuje nevydanou účtenku.	IS EET musí umožnit oznámení nevydané účtenky.
Zákazník identifikuje provozovnu, kde mu nebyla vydána účtenka.	IS EET sbírá informace nezbytné k identifikaci provozovny.
IS EET zpracuje a třídí oznámení.	IS EET musí v maximální možné míře identifikovat provozovnu na základě informací poskytnutých Zákazníkem.
Zákazník vyplňuje veškeré relevantní údaje, které se týkají konkrétní provozovny.	Existuje min. sada povinných parametrů. Avšak na základě toho, jaké informace je zákazník schopen poskytnout, je přizpůsobena povinnost vyplnění údajů (např. nepožaduje se vyplnění názvu poplatníka, když je Zákazník schopen specifikovat IČ, případně DIČ).
Bude-li chybět jeden z povinných údajů, nebo se nepovede ztotožnění provozovny, takové oznámení bude zařazeno do fronty pro ruční zpracování.	V případě, že bude zadaná adresa, kde sídlí několik provozoven a nepovede se přesná identifikace poplatníka, bude oznámení určeno pro další ruční zpracování kontrolním orgánem.

Požadavky

Seznam funkčních a nefunkčních požadavků kladených na IS EET v kontextu ohlašování nevydané účtenky. Požadavky vycházejí z uvedených pravidel a dále je rozvíjejí do konkrétních funkčností či charakteristik celého systému.

ID	Požadavek	Popis
O-1	Informační systém EET musí být schopen přijat oznámení.	Oznámením je myšleno poskytnutí informací o provozovně, kde poplatník nevydal účtenku a porušil tím své povinnosti.
O-2	Po zadání oznámení musí systém provést ztotožnění informací a pokusit se o automatickou identifikaci poplatníka.	V případě zadání IČ/DIČ je možné přesné určení poplatníka a společně s adresou provozovny o její identifikaci. V tomto případě systém vytvoří záznam o oznámení, se kterým následně kontrolní orgán pracuje. V případě, že je zadaná adresa provozovny a název poplatníka (provozovny), systém se na základě zadaných adres všech provozoven pokusí identifikovat a ztotožnit poplatníka a provozovnu.
O-3	IS EET musí zajistit zpracování nepřesných oznámení.	V případě, že je oznámení nekompletní, IS EET musí toto zaevidovat a zpřístupnit pro další ruční zpracování.
O-4	IS EET musí zajistit notifikaci pro potřeby kontroly.	Po ztotožnění poplatníka a provozovny systém zajistí notifikaci kontrolního orgánu, který bude oznámení dále prověřovat.
O-5	IS EET nesmí odmítnout oznámení	IS EET musí přijat každé oznámení, které bude mít vyplněny povinné informace. V případě, že nebude možné provést ztotožnění, musí oznámení zachovat pro ruční zpracování.

Popis komunikace

Oznámení nevydané účtenky

Oznámení nevydané účtenky bude obsahovat následující informace:

- Identifikace poplatníka (IČ nebo DIČ)*
- Název provozovny*
- Adresa provozovny (město*, ulice*, číslo popisné)
- Druh činnosti
- Poznámka
- Datum nákupu
- Registrační značka
- Částka

Je nezbytné, aby systém EET byl schopen identifikovat poplatníka a provozovnu, kde nebyla účtenka vydána. Tato identifikace bude realizována prostřednictvím (daňového) identifikačního čísla, případně specifikací Názvu poplatníka. Provozovna je lokalizována prostřednictvím adresy (povinně města a ulice, nepovinně čísla popisného). Další informace jsou určeny na bližší identifikaci poplatníka a provozovny a jsou určeny pro posouzení kontrolorem.

Chybové stavy

Oznámení nevydané účtenky nelze zadat bez vyplnění kombinace povinných údajů, které jsou určeny na přesnou identifikaci poplatníka a provozovny. Proces dále neobsahuje další chybové stavy.

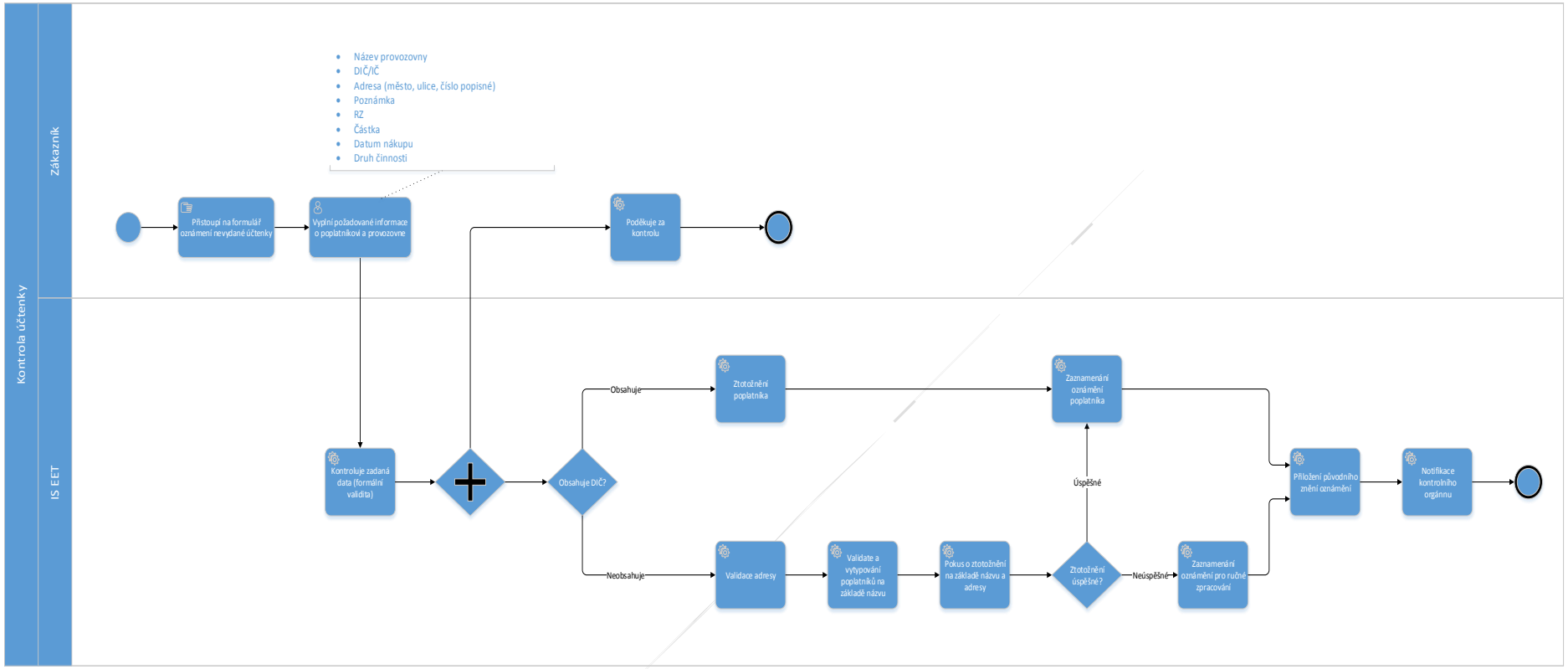
Logování událostí

Proces bude zaznamenávat jednotlivá oznámení přímo jako zájmové entity. Logování přístupu není nutné, doporučujeme logování přístupů a jejich četností pro analýzu případných falešných útoků (např. konkurence).

Proces Oznámení nevydání účtenky zákazníkovi

Popis kroků procesu

1. Zákazník přistoupí na formulář pro oznámení nevydané účtenky. Formulář může být realizován na webovém portálu, případně součástí mobilní aplikace.
2. Zákazník vyplní požadované informace.
3. IS EET zpracuje oznámení.
4. V případě přesné identifikace poplatníka a provozovny na základě poskytnutých dat je vytvořeno oznámení, které je poskytnuté kontrolnímu orgánu pro další zpracování.
5. V případě, že se identifikace nepovede (na adrese sídlí několik provozoven, adresa není přesná, zákazník neuvedl IČ/DIČ, ale název poplatníka, který není jednoznačný, je oznámení zaevidováno pro ruční zpracování kontrolním orgánem.
6. Kontrolní orgán je notifikován o novém oznámení.
7. Systém poděkuje zákazníkovi za oznámení.



Obrázek 13: Proces nevydané účtenky zákazníkovi

Případy užití

Základním případem užití je „Oznamuje nevydanou účtenku“, který je blíže procesně rozpracován. Další případy užití jsou následující

- Prohlíží oznámení (třídí, filtruje, nahlíží na detail)
  Kontrolor v tomto případě užití disponuje rozhraním, které mu umožní nahlížet na jednotlivé oznámení pro potřeby dalšího zpracování. Oznámení je možné třídit a filtrovat dle data oznámení, poplatníka, provozovny, lokace, případné dalších parametrů. Kontrolor má možnost nahlížet na detail oznámení, přiřadit oznámení kontroloru, případně označit jako zpracované.

- Označuje oznámení jako zpracované
  Kontrolor po realizaci kontroly u poplatníka a ověření vydávaní nebo nevydávání účtenek označuje oznámení jako zpracované a systém k danému oznámení přidá příznak. Toto oznámení není smazáno, je jej možné použít v další analytice, nicméně pro potřeby přímé kontroly již není potřebné.

- Přiřazuje oznámení pro zpracování
  Kontrolor konkrétní oznámení označuje příznakem, že je předmětem probíhající kontroly (naplánované, případně probíhající) a další kontrolor by neměl mít možnost s ním pracovat.

- Ztotožňuje nezpracované oznámení
  oznámení, které není možné automaticky přiřadit poplatníkovi (a jeho provozovně) na základě informací zadaných Zákazníkem (oznamovatelem), je připraveno pro další ruční zpracování kontrolorem, který může ztotožnění vykonat s využitím svých schopností.

- Notifikuje kontrolní orgán
  Informační systém zašle notifikaci (konkrétní implementace není předmětem tohoto popisu, může se jednat o emailovou notifikaci, případně notifikaci v samotném systému) kontrolnímu orgánu o existenci nového oznámení.

Kontrola ze strany FS a CS

Procesní oblast, která má na starosti kontrolní nákup. Kontrolor provede nákup a kontroluje, zda byl správně zaevidována.

Aktéři

Aktér v kontextu evidence tržeb	Popis
IS EET	Přijímá a kontroluje informace o nákupu, tyto informace zpracuje, ukládá evidenci o kontrole.
Kontrolor	Kontroluje zaevidování tržby, vkládá a upřesňuje informace o vykonané kontrole.
IS ADIS	Ověřuje registraci poplatníka k daním.

Pravidla

Seznam pravidel, která se vztahují ke kontrolnímu nákupu. Zdrojem těchto pravidel jsou aktuální postupy kontrolních úřadů, technická a jiná omezení z hlediska návrhu finálního systému.

Název pravidla	Popis
Kontrolor ověřuje požadované registrace poplatníka.	IS EET musí umožnit zjištění informace, zda je poplatník registrován k dani a registrován v EET.
IS EET integruje IS ADIS.	Pro získaní informace o registraci k dani je IS EET integrován na rozhraní IS ADIS, kde jsou tyto informace vedeny.
Kontrolor zadává a ověřuje informace z účtenky	IS EET sbírá informace z účtenky pro kontrolu.
IS EET informuje o stave fiskalizace.	IS EET na základě zadaných dat informuje, zda byla tržba zaevidována.
IS EET naplánuje kontrolu, když provozovna nebyla v online režimu.	IS EET po kontrole účtenky s BKP naplánuje kontrolu po uplynutí nezbytného času (dle režimu, ve kterém provozovna funguje) a informuje kontrolora o výsledku.
IS EET umožní evidenci kontrol.	IS EET umožní vedení a evidenci probíhajících a ukončených kontrol poplatníků, včetně informací o udělených sankcích.
IS EET poskytne možnost integrace evidence kontrol pro další subjekty.	IS EET musí obsahovat integrační rozhraní, prostřednictvím kterého budou další subjekty (Celní správa) schopny zasílat informace o kontrolách poplatníků. Toto rozhraní je nutné pro informaci zejména o uložených sankcích.

Požadavky

Seznam funkčních a nefunkčních požadavků kladených na IS EET v kontextu kontrolního nákupu. Požadavky vycházejí z uvedených pravidel a dále je rozvíjejí do konkrétních funkčností či charakteristik celého systému.

ID	Požadavek	Popis
KN-1	Informační systém EET musí být schopen ověřit registraci poplatníka k dani.	IS EET musí umožnit na základě IČ ověření, zda je poplatník registrován k dani.
KN-2	Informační systém EET musí být schopen ověřit registraci poplatníka k EET.	IS EET musí umožnit na základě IČ ověření, zda je poplatník registrován k EET.
KN-3	Informační systém EET musí umožnit ověření informací z účtenky.	IS EET po zadání informací z účtenky (FIK/BKP, IČ a další) ověří, zda byla transakce fiskalizovaná.
KN-4	IS EET musí pod zadání podpisu (při off-line nákupu umístěn na účtence) ověřit jeho validitu.	V případě, že byl nákup proveden v off-line režimu, bude účtenka obsahovat část podpisu. IS EET musí být schopen ověřit, zda poplatník vlastní certifikát

		patřící k tomuto podpisu (jinými slovy zda byla tržba podepsána certifikátem náležícím kontrolovanému poplatníkovi).
KN-5	IS EET musí zajistit zpracování nezaevidovaných tržeb.	V případě, že tržba proběhla v off-line režimu, IS EET musí naplánovat kontrolu budoucího zaevidování po uplynutí zákonem definované doby.
KN-6	IS EET musí vést evidenci kontrol.	IS EET musí obsahovat evidenční modul, kde jsou jednotlivé kontroly evidovány. Důležité informace jsou zejména historie kontrol poplatníka, udělené sankce a jejich důvod.
KN-7	IS EET musí obsahovat rozhraní pro zápis do evidence kontrol.	Z důvodu vykonávání kontrol elektronické evidence tržeb externími orgány (zejména Celní správou), které využívají vlastní IS pro vedení evidencí kontrol, musí IS EET obsahovat rozhraní, které umožní zapsání proběhlé kontroly, aby bylo možné zákonné udělování sankcí.
KN-8	IS EET musí zajistit notifikaci pro potřeby kontroly.	Po dodatečné verifikaci off-line transakce systém zajistí notifikaci kontrolního orgánu, který bude dále pokračovat v kontrole dle výsledku.

Popis komunikace

Kontrolní nákup

Kontrolor bude do IS EET zadávat tyto informace:

- IČ/DIČ poplatníka
  Bude použito pro ověření registraci k dani a registraci v EET
- FIK/BKP
  Bude použito pro kontrolu správné evidence tržby poplatníkem.
- Datum transakce, částka, podpis, číslo pokladny, číslo provozovny
  Bude použito pro kontrolu správné evidence tržby poplatníkem.
- Informace o kontrole
  Evidenční záznam obsahující informace o proběhlé kontrole, udělených sankcích včetně důvodu, případně poznámek.

Logování událostí

Systém zaznamená při evidenci kontroly identifikaci kontrolora, který kontrolu provedl.

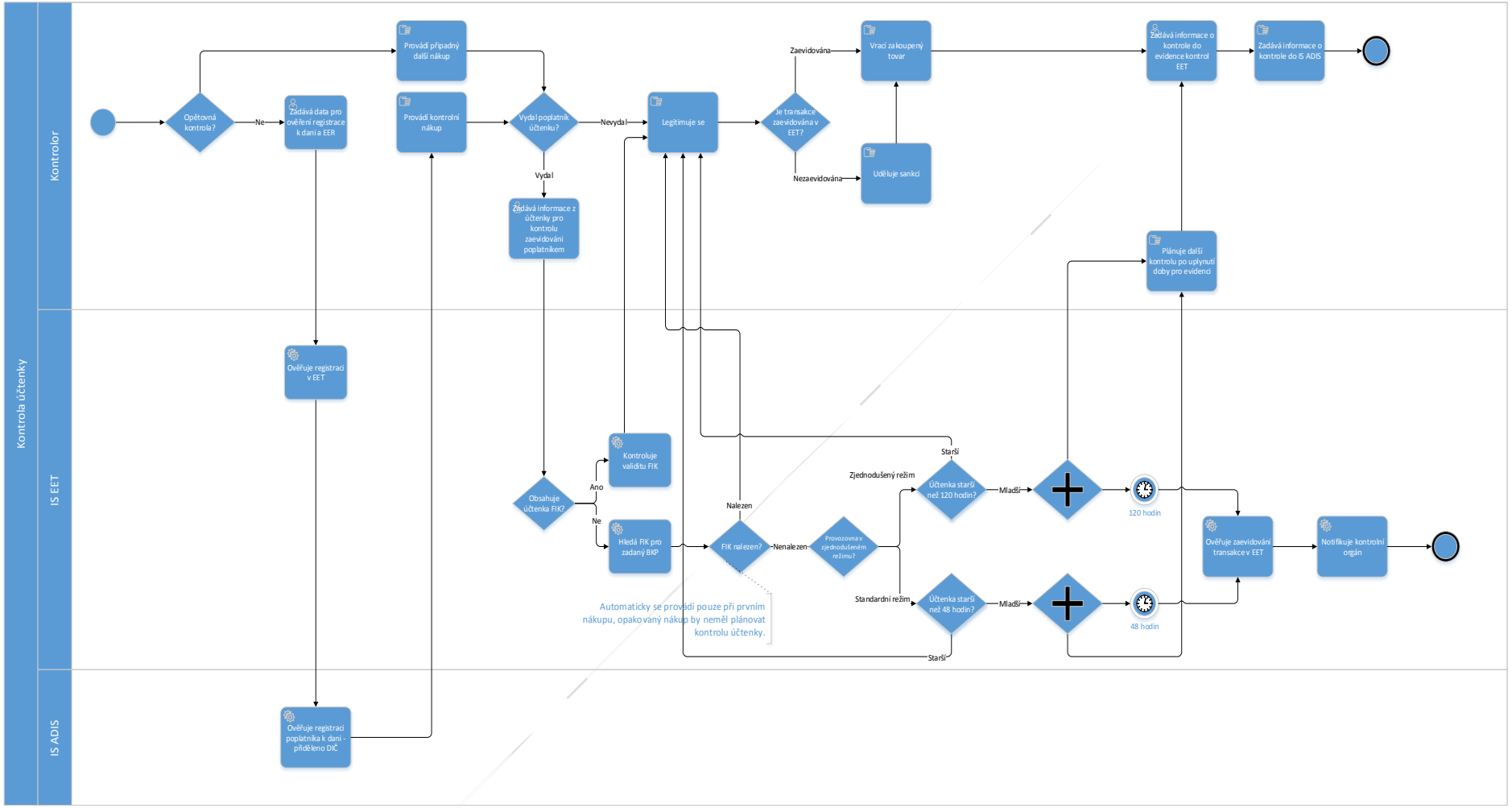
Proces Kontrolní nákup

Popis kroků procesu

1. Kontrolor přistoupí na formulář pro kontrolu registrace. Formulář může být realizován na webovém portálu, případně součástí mobilní aplikace.
2. Kontrolor vyplní požadované informace.
3. IS EET ověří registraci k dani a EET.
4. Kontrolor provede kontrolní nákup
5. V případě nevydání účtenky se legitimuje a udělí sankci.
6. V případě vydání účtenky:
   a. Účtenka byla správně zaevidována – kontrolor se legitimuje, vrací zboží a zaznamenává průběh kontroly.
   b. Účtenka nebyla správně zaznamenána (obsahuje nevalidní FIK, podpis je falešný, DIČ se neshoduje apod.) – kontrolor se legitimuje, uděluje sankci, vrací zboží a zaznamenává průběh kontroly.

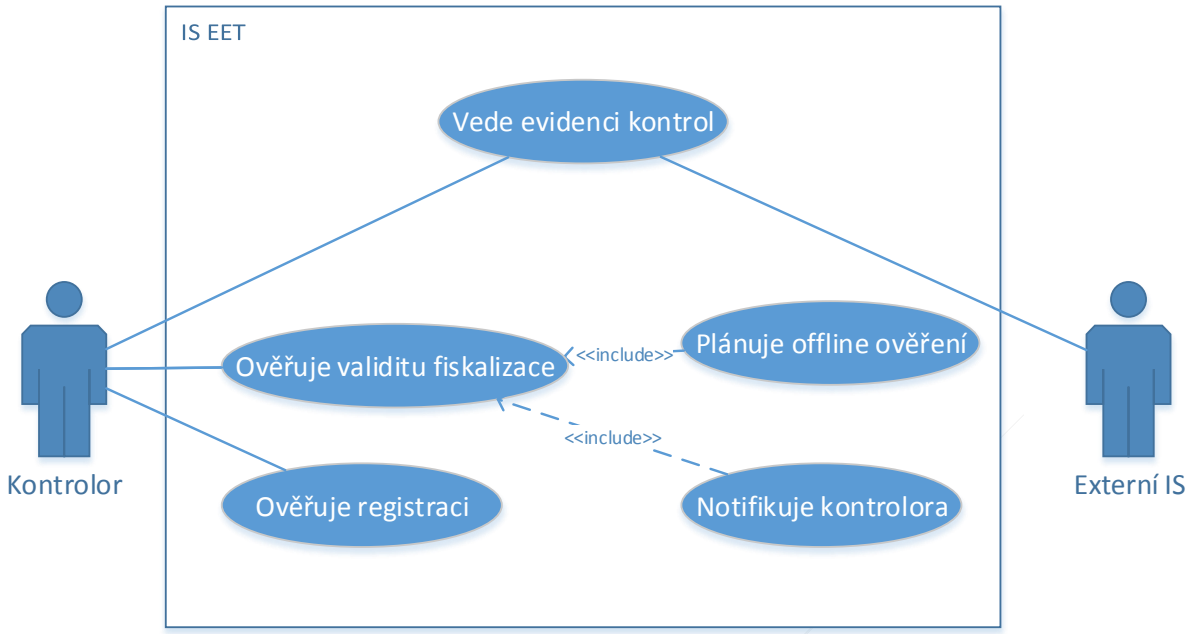
c. Účtenka byla vydána v off-line režime – kontrolor zaznamenává průběh kontroly a plánuje další kontrolu. Systém paralelně naplánuje kontrolu pozdní evidence. Kontrolor je informován o výsledku, vrací se do provozovny, kde může zrealizovat další nákup (systém v tomto případě zkontroluje validitu FIK, případně podpis a validitu BKP a neplánuje pozdní kontrolu off-line evidence), legitimuje se a uděluje případnou sankci. Následně zaznamenává a doplňuje informace k evidenčnímu záznamu kontroly.

7. Kontrolor zadává informace o kontrole do systému ADIS.



Obrázek 14: Proces kontrolní nákup

Případy užití



Základním případem užití je „Ověřuje validitu fiskalizace“, který je blíže procesně rozpracován. Další případy užití jsou následující

- Ověřuje registraci
  Kontrolor v tomto případě užití ověřuje, zda je poplatník registrován k dani a k elektronické evidenci tržeb. Tento případ užití využívá integrované rozhraní informačního systému ADIS.
- Vede evidenci kontrol
  Kontrolor (případně externí informační systém integrující rozhraní EET) po vykonání kontroly u poplatníka zaznamenává průběh kontroly a eviduje udělené sankce.
- Plánuje off-line ověření
  IS EET při off-line transakci naplánuje ověření po uplynutí zákonem definované lhůty.
- Notifikuje kontrolora
  Informační systém zašle notifikaci (konkrétní implementace není předmětem tohoto popisu, může se jednat o emailovou notifikaci, případně notifikaci v samotném systému) kontrolnímu orgánu o proběhnuté validaci a jejím výsledku.

Specifikace ochranných prvků EET

Vymezení rozsahu

Předmětem specifikace ochranných prvků EET je vymezení klíčových ochranných informací souvisejících s účtenkou a to jak v její fyzické („vytištěné“) formě, tak v její elektronické formě (datová věta). Daná specifikace obsažená dále v tomto dokumentu zahrnuje:

- stanovení požadavků na ochranné prvky
- stanovení výchozího konceptu ochranných prvků
- stanovení ochranných prvků
- stanovení postupu tvorby a validace vybraných ochranných prvků
- stanovení algoritmů použitých pro ochranné prvky a jejich síly
- stanovení způsobu prezentace ochranných prvků.

Požadavky na ochranné prvky EET

Stanovení požadavků na ochranné prvky EET vychází ze základního koncepčního modelu EET kdy:

1. pro vydání účtenky zasílá povinný subjekt elektronicky účtenku do systému EET a očekává potvrzení jejího přijetí a přidělení ID
2. obdrží-li potvrzení, vystaví účtenku opatřenou získaným ID zákazníkovi.
3. obdrží-li zamítnutí, (například z důvodu neplatné elektronické značky), musí zjednat nápravu a následně se pokusí zaslat účtenku znovu.
4. Neobdrží-li odpověď, vystaví off-line účtenku bez ID, které neobdržel.

Požadavky na ochranné prvky EET elektronické formy účtenky

Požadavky na ochranné prvky EET respektující výše naznačený koncepčního modelu EET jsou pro elektronickou formu účtenky stanoveny následovně:

ID požadavku	Specifikace požadavku
OP.E.PV.POS.integrita	Vystavitel účtenky je povinen ji potvrdit takovým způsobem, aby toto potvrzení umožňovalo zjistit modifikaci či poškození informací účtenky oproti stavu, ve kterém ji vystavitel potvrzoval. (Integrita elektronické účtenky na straně vystavitele)
OP.E.PV.POS.Odpovednost	Vystavitel účtenky je povinen ji nezpochybnitelně potvrdit takovým způsobem, aby bylo následně možno ověřit, že dané potvrzení pochází od daného vystavitele a že se vztahuje k účtence ve stavu, ve kterém ji vystavitel potvrzoval. (Neodmítnutelnost odpovědnosti za vystavení elektronické účtenky na straně vystavitele)
OP.E.PV.POS.Uplnost	Vystavitel účtenky je povinen ji nezpochybnitelně potvrdit takovým způsobem, aby se toto potvrzení vztahovalo na všechny významné informace účtenky včetně informací souvisejících s jejím vystavením (např. čas vystavení, DIČ, provozovna, apod.)[5]. (Pokrytí všech důležitých informací účtenky vystavitelovým potvrzením na straně vystavitele – úplnost)
OP.E.PV.POS.Implementace	Požadované potvrzení vystavitele musí být reálně implementovatelné běžně dostupnými prostředky. Reálné provádění potvrzování nesmí nad nezbytně nutnou úroveň narušovat běžnou oprávněnou činnost vystavitele účtenky. (Implementovatelnost vystavitelova potvrzení dostupnými prostředky)

[5] Tyto povinné informace jsou vymezeny samostatně v rámci struktury datových vět předávaných mezi vystaviteli účtenek (povinnými subjekty) a EET

OP.E.PV.POS.Validace	Vystavitel účtenky musí mít možnost ověřit si ze svého potvrzení, že je skutečně vystavitelem dané účtenky a že nedošlo k modifikaci či poškození informací účtenky oproti stavu, ve kterém ji vystavitel potvrzoval. (Ověření/validace vystavitelova potvrzení elektronické účtenky na straně vystavitele)
OP.E.PV.POS.Stop	Vystavitel musí mít možnost (a povinnost) v případě okolností (ukončení činnosti, ztráta zařízení, podezření na nekalou činnost zaměstnance apod.) oznámit „nevalidnost“ dalšího vydávaní potvrzení vystavitele, ke které by mohlo dojít v důsledku daných okolností.
OP.E.PV.EET.validace	EET musí mít možnost ověřit si z vystavitelova potvrzení účtenky, že zasílající či kontrolovaný subjekt je skutečně vystavitelem dané účtenky a že nedošlo k modifikaci či poškození informací účtenky oproti stavu, ve kterém ji vystavitel potvrzoval. (Ověření/validace vystavitelova potvrzení elektronické účtenky na straně EET)
OP.E.PV.EET.Stop	EET musí mít možnost (a povinnost) v případě okolností (ukončení činnosti, oznámení vystavitele apod.) zajistit kroky, které zajistí, „nevalidnost“ dalšího vydávaní potvrzení vystavitele, ke které by mohlo dojít v důsledku daných okolností.
OP.E.PE.EET.integrita	EET je povinno předanou validní účtenku potvrdit takovým způsobem, aby toto EET potvrzení umožňovalo zjistit modifikaci či poškození informací zaslané účtenky potvrzované ze strany EET oproti stavu, ve kterém ji EET potvrzovalo. (Integrita přijaté elektronické účtenky na straně EET)
OP.E.PE.EET.Odpovednost	EET je povinno opatřit předanou validní účtenku potvrdit takovým způsobem, aby toto EET potvrzení následně umožňovalo ověřit, že pochází od EET a že se vztahuje k potvrzované účtence ve stavu, ve kterém ji EET potvrzovalo. (Neodmítnutelnost odpovědnosti za potvrzení přijaté elektronické účtenky na straně EET)
OP.E.PE.EET.Uplnost	EET je povinno opatřit předanou validní účtenku potvrdit takovým způsobem, aby se toto potvrzení vztahovalo na všechny významné informace potvrzované účtenky včetně informací souvisejících s jejím potvrzením na straně EET (např. čas přijetí/potvrzení, apod.)[6]. (Pokrytí všech důležitých informací přijaté elektronické účtenky EET potvrzením EET na straně EET – úplnost)
OP.E.PE.EET.validace	EET musí mít možnost ověřit si z EET potvrzení účtenky, že je skutečně potvrzovatelem dané účtenky a že nedošlo k modifikaci či poškození informací účtenky oproti stavu, ve kterém ji EET potvrzovalo. (Ověření/validace EET potvrzení přijaté elektronické účtenky na straně EET)
OP.E.PV.OST.validace	Třetí strany musí mít (vyžaduje-li to provoz a používání EET) možnost ověřit si z potvrzení účtenky vystavitelem, že daný subjekt je skutečně vystavitelem dané účtenky a že nedošlo k modifikaci či poškození informací účtenky oproti stavu, ve kterém ji daný subjekt potvrzoval. (Ověření/validace EET potvrzení přijaté elektronické účtenky třetí stranou)

[6] Tyto povinné informace jsou vymezeny samostatně v rámci struktury datových vět předávaných mezi vystaviteli účtenek (povinnými subjekty) a EET.

OP.E.PE.OST.validace	možnost ověřit si z potvrzení účtenky od EET, že EET je skutečně potvrzovatelem dané účtenky a že nedošlo k modifikaci či poškození informací potvrzované účtenky oproti stavu, ve kterém ji EET potvrzoval. (Ověření/validace EET potvrzení přijaté elektronické účtenky třetí stranou)
OP.E.PE.OST.validace	Třetí strany musí mít (vyžaduje-li to provoz a používání EET) možnost ověřit si z EET potvrzení účtenky, že potvrzovatelem dané účtenky je skutečně EET a že nedošlo k modifikaci či poškození informací účtenky oproti stavu, ve kterém ji EET potvrzovalo. (Ověření/validace EET potvrzení přijaté elektronické účtenky třetí stranou)

Požadavky na ochranné prvky EET fyzické formy účtenky

Požadavky na ochranné prvky EET respektující výše naznačený koncepčního modelu EET jsou pro fyzickou formu účtenky stanoveny následovně:

ID požadavku	Specifikace požadavku
OP.F.POS.Vazba	Vystavitel fyzické účtenky je povinen na ní jednoznačným a srozumitelným způsobem uvést veškeré relevantní významné informace účtenky včetně informací souvisejících s jejím vystavením (např. čas vystavení, DIČ, provozovna, apod.)[7] ve shodě s údaji, které jsou předávány v elektronické podobě účtenky. (Srozumitelná tištěná prezence, úplnost a jednoznačná vazba informací na fyzické účtence na informace uvedené v elektronické formě účtenky)
OP.F.PV.POS.integrita	Vystavitel účtenky je povinen opatřit ji takovým potvrzením (potvrzovacím údajem), aby tento údaj umožňoval zjistit modifikaci či poškození informací účtenky oproti stavu, ve kterém ji vystavitel vystavil. (Integrita fyzické účtenky na straně vystavitele)
OP.F.PV.POS.Odpovednost	Vystavitel účtenky je povinen opatřit ji takovým potvrzením (potvrzovacím údajem), aby bylo následně možno s podporou dodatečných informací určit, že daný údaj pochází od daného vystavitele a vztahuje se k dané účtence ve stavu, ve kterém byla vystavena. (Neodmítnutelnost odpovědnosti za vystavení fyzické účtenky na straně vystavitele)
OP.F.PV.POS.Uplnost	Vystavitel účtenky je povinen opatřit ji takovým potvrzením (potvrzovacím údajem), aby se tento potvrzovací údaj vztahoval na všechny významné informace účtenky včetně informací souvisejících s jejím vystavením. (Pokrytí všech důležitých informací fyzické účtenky vystavitelovým potvrzovacím údajem na straně vystavitele – úplnost)
OP.F.PV.POS.Implementace	Požadované potvrzení vystavitele (potvrzovací údaj) musí být reálně implementovatelný a na fyzické účtence prezentovatelný běžně dostupnými prostředky. Reálné potvrzování nesmí nad nezbytně nutnou úroveň narušovat běžnou oprávněnou činnost vystavitele účtenky. (Implementovatelnost vystavitelova potvrzení fyzické účtenky dostupnými prostředky)

[7] Tyto povinné informace jsou vymezeny samostatně v rámci struktury fyzického výtisku účtenky vystavované povinnými subjekty zákazníkům.

OP.F.PV.POS.validace	Vystavitel účtenky musí mít možnost ověřit si, že dané potvrzení (potvrzovací údaj) je skutečně pořízen jím a že nedošlo k modifikaci či poškození informací fyzické účtenky oproti stavu, ve kterém ji vystavitel potvrzoval. (Ověření/validace vystavitelova potvrzení fyzické účtenky na straně vystavitele)
OP.F.PE.EET.ID	EET je povinno poskytnout vystaviteli na základě předané validní elektronické účtenky potvrzovací identifikační údaj, kterým opatří vydavatel příslušnou fyzickou účtenku. (Poskytnutí ID účtenky ze strany EET)
OP.F.PV.OST.validace	Třetí strany musí mít (vyžaduje-li to provoz a používání EET) možnost ověřit si z potvrzení účtenky vystavitelem, že daný subjekt je skutečně vystavitelem dané účtenky a že nedošlo k modifikaci či poškození informací účtenky oproti stavu, ve kterém ji daný subjekt potvrzoval. (Ověření/validace elektronické účtenky třetí stranou)

Stanovení výchozího konceptu ochranných prvků EET

Koncept řešení ochranných prvků je s ohledem na potřeby EET, stanovené požadavky na ochranné prvky EET a dostupnou legislativní oporu (zejména zákon o elektronickém podpisu a související), založen na:

- jednoznačně specifikovaných datových větách pro elektronické předávání účtenek mezi vystaviteli účtenek a EET jakožto příjemcem účtenek (struktura a obsah elektronicky předávané účtenky).
- jednoznačně specifikovaných povinných položkách vytištěné účtenky předávané jejím vystavitelem zákazníkovi jakožto jejímu příjemci (stanovení povinných položek fyzicky vytištěné účtenky a požadavků na ně).
- využití konceptu PKI a to zejména elektronického podpisu [8] (s využitím asymetrické kryptografie) k zajištění integrity předávaných informací a odpovědnosti za předávané informace. Podepisujícími stranami jsou jak vystavitelé účtenek, tak EET jakožto příjemce účtenek a vystavitel potvrzení o jejich příjmu.
- využití vybraných informací (z datových vět elektronicky předávané formy účtenek) k ochraně fyzického výtisku účtenky tak, aby ji bylo možno samostatně ověřovat z hlediska zachování integrity vybraných klíčových dat a z hlediska odpovědnosti vystavitele za její vystavení.
- dostupnosti přijatelných forem prezentace ochranných prvků či jejich částí na fyzickém výtisku účtenky. Kritériem přijatelnosti jsou zejména délka informace v dané prezentované podobě (možnost jejího reálného vytištění) a přehlednost (především se jedná o volbu dostatečně čitelné znakové sady, ve které je informace prezentována a dále použitelná zákazníkem a dalšími subjekty). Blíže viz kapitola 0 „Stanovení způsobu prezentace ochranných prvků V rámci prezentace jsou využívány hashovací funkce[9].

[8] V textu je užíváno pojmu elektronický podpis s tím, že ve smyslu zákona o elektronickém podpisu by se jednalo o použití ve smyslu elektronické značky vytvářené systémy na straně EET a povinných subjektů.

[9] Hašovací funkce náleží mezi kryptografické funkce, poskytující pro jakýkoliv přípustný vstup (např. pro algoritmy typu SHA jsou dle typu vstupy omezeny délkou 2^{64} až 2^{128} bitů) poskytují výstup (tzv. hash resp. „heš“) konstantní omezené délky (např. pro algoritmy typu SHA se výsledné hashe dle typu pohybují od 160 do 512 bitů).
Klíčové jsou pro kvalitní hashovací funkce následující vlastnosti:

- Jedná se o funkci: hashovací funkce vrací pro stejný vstup vždy stejnou hodnotu - výstup.
- Jedná se o jednosměrnou funkci: pro daný výstup hašovací funkce (daný hash) není výpočetně možné zpětně stanovit jeho vstup (původní zprávu). Tato vlastnost se nazývá jednosměrnost.
- Bezkoliznost: není výpočetně možné efektivně nalézt libovolné dva vstupy (zprávy), jejichž hodnoty (hashe) jsou shodné – není tzv. možné nalézt výpočetně efektivně kolize.

Stanovení ochranných prvků

Pro potřeby EET v souladu s požadavky na ochranné prvky EET a na základě výchozího konceptu ochranných prvků EET, budou v rámci EET používány následující ochranné prvky:

Ochranné prvky zaměřené na elektronickou výměnu datových vět mezi povinnými subjekty a POS	
XML zprávy	Informací jsou předávány formou zpráv v XML formátu, jejichž obsahem jsou definované datové věty.
Elektronické podpisy	Informace předávané v rámci zpráv jsou oběma stranami elektronicky podepisovány tak, aby byla zajištěna integrita těchto informací (resp. detekovatelnost jejího případného narušení) a odpovědnost odesilatelů za jejich zaslání.
Identifikátor zpráv	Jednotlivé zprávy jsou opatřeny vhodnými identifikátory tak, aby bylo možno identifikovat a řešit případné opakované zaslání zpráv či následné vazby mezi zprávami.
Časové údaje	Jednotlivé zprávy jsou opatřovány časových údaji.

Ochranné prvky zaměřené primárně na ochranu informací fyzického výtisku účtenky	
BKP	Bezpečnostní kód povinného subjektu, který umožňuje spolu s kódem OKP přiměřenou ochranu integrity (resp. detekovatelnost jejího případného narušení) významných údajů uvedených na výtisku účtenky a prosazuje odpovědnost povinného subjektu za její vystavení. Úlohou BKP je především prezentovatelná a použitelná podoba daného ochranného prvku. Bez použití OKP není samostatně schopen výše uvedené zajistit. BKP má též vlastnosti dostatečně unikátního identifikátoru účtenky se silnou vazbou na jejího vystavitele a její obsah. BKP je vždy přenášeno elektronicky i tištěno na výtisk účtenky.
OKP	Offline kód povinného subjektu, je pomocným ochranným prvkem, který umožňuje kontrolu integrity a prosazuje odpovědnost povinného subjektu za vystavení tištěné účtenky. Kód je určen pro specifické potřeby kontroly (kontrolních orgánů/pracovníků) a není běžně manipulován zákazníkem. OKP je vždy předáván v elektronické komunikaci a na účtenku je tištěn pouze v případě, kdy je tato vydávána v offline režimu.

Obecné ochranné prvky	
FIK	Kód přidělovaný systémem EET. Daný kód je řešen samostatně a není předmětem této specifikace. Nicméně bez ohledu na svou povahu a vlastnosti plní daný kód též úlohu identifikátoru přidělovaného zaslané účtence ze strany systému EET. FIK je vždy přenášen elektronicky i tištěn na výtisk účtenky.

Stanovení postupu tvorby a validace vybraných ochranných prvků

Ochranné prvky zaměřené na elektronickou výměnu datových vět mezi povinnými subjekty a POS budou použity v souladu se standardy a standardními postupy. Jedná se o použití standardního formátu XML, v němž budou prezentovány přenášené datové věty. Elektronické podpisy zpráv budou vytvářeny dle doporučení W3C XML s preferencí „XML enveloped signature“.

Identifikátory zpráv budou generovány dle standardních postupů s vyžitím UUID. Časové údaje budou přenášeny v jednoznačné reprezentaci zahrnující datum a čas s přesností na vteřiny.

- Je výpočetně nemožné najít efektivně k dané zprávě jakoukoli jinou zprávu, pro kterou by funkce vracela stejnou hodnotu (hash).

Kód FIK je řešen samostatně a není předmětem této specifikace.

Ochranné prvky zaměřené primárně na ochranu informací fyzického výtisku účtenky jsou založeny na dvojici kódů BKP a OKP. Oba tyto kódy jsou vždy zasílány elektronickou cestou systému EET v rámci datových vět. Na fyzickou účtenku je vždy tištěn BKP a v případě vydání v offline řežimu též OKP.

Při offline vydání účtenky poskytuje kód OKP možnost kontroly integrity a původce účtenky i za stavu, kdy nebyla účtenka v elektronické podobě doručena do systému EET a je možno použít pouze fyzický výtisk účtenky.

OKP zaslané elektronicky při online vydání umožňuje ověření BKP na straně systému EET.

Kód OKP je hodnotou elektronického podpisu vybraných významných údajů, prezentovaných následně na fyzickém výtisku účtenky. Je vytvořen standardním postupem:

1. M = vybrané významné údaje prezentované následně na fyzickém výtisku účtenky
2. H = hash (M) : hash kód dat D
3. OKP = Encrypt (M,$PrivKey_{POS}$) : zašifrování H soukromým klíčen povinného subjektu.

Kód BKP je následně odvozen jako hash kód OKP, tedy:

1. BKP = hash (OKP).

Ověření integrity a původu fyzické účtenky (vyžaduje nástroj – např. lokální aplikaci či službu poskytovanou kontrolujícímu systémem EET) má dvě základní etapy:

- ověření integrity a původu fyzické účtenky dle OKP
  ověření integrity a původu fyzické účtenky dle OKP je provedeno následovně:
  - je sestavena zpráva M z vybraných významných údajů uvedených na fyzickém výtisku validované účtenky
  - je spočten hash kód H zprávy M
  - je získán hash kód H1 uložený v kódu (elektronickém podpisu) OKP. H1 je získán dešifrování elektronického podpisu za použití správného veřejného klíče podepisujícího povinného subjektu[10]
  - Je-li H = H1, pak je validace úspěšná (účtenka si zachovala integritu a byla vydána držitelem použitého veřejného klíče resp. certifikátu, který daný klíč obsahuje). V opačném případě není účtenka validní (je narušena její integrita, nebo není vystavena daným povinným subjektem).
- validace BKP
  validace BKP je provedena spočtení hodnoty BKP1 = hash (OKP). Je-li BKP = BKP1, pak je validace úspěšná. V opačném případě není kód BKP validní.

Stanovení algoritmů použitých pro ochranné prvky a jejich síly

S ohledem na aktuální stav a doporučení v oblasti kryptografie a s ohledem na korekce dané potřebami zadavatele řešení (zejména s ohledem na reálnou použitelnost a implementovatelnost) jsou

[10] S ohledem na nutnost zajistit co nejkratší délku prezentovaných informací neobsahuje OKP informace o identifikaci certifikátu a tedy veřejného klíče povinného subjektu, který odpovídá vytvořenému podpisu. Z tohoto důvodu je nutno při validaci ověřovat veškeré veřejné klíče (obsažené v certifikátech) daného povinného subjektu, dokud není validace úspěšná, nebo nejsou neúspěšně vyčerpány všechny klíče daného povinného subjektu.
Úpravou této skutečnosti může být uvedení údaje o sériovém čísle certifikátu, který obsahuje relevantní veřejný klíč povinného subjektu („podpisový certifikát dané účtenky“). Při této variantě by bylo postačující ověření vůči tomuto jednomu specifikovanému klíči/certifikátu.

stanoveny následující pro klíčové použité ochranné prvky dále v této kapitole stanovené algoritmy a jejich síla.

Elektronické podpisy

Pro elektronické podpisy bude v rámci řešení EET použito schématu **SHA-256/RSA2048.** Tvorba a ověřování elektronických podpisů v systému EET bude jakožto asymetrického algoritmu používat algoritmus RSA s délkou kryptografických klíčů 2048 bitů a jakožto hashovací funkci algoritmus SHA-256 z rodiny algoritmů SHA2. Toto paradigma se vztahuje též na elektronické podpisy v rámci certifikátů. Konkrétně potom:

- elektronický podpis kořenového certifikátu CA ve schématu SHA-256/RSA2048 (případně může být použito větší délky klíče – 4096 bitů - v případě víceúrovňové struktury CA)
- elektronický podpis certifikátů systému EET ve schématu SHA-256/RSA2048
- elektronický podpis certifikátů POS ve schématu SHA-256/RSA2048
- elektronické podpisy vytvářené na straně EET se schématem SHA-256/RSA2048
- elektronické podpisy vytvářené na straně POS (včetně elektronických podpisů pro potřeby tvorby kódů OKP a z nich odvozených kódů BKP) se schématem SHA-256/RSA2048.

Hashovací algoritmus pro tvorbu kódu BKP

Pro tvorbu bezpečnostního kódu BKP z kódu OKP bude s ohledem na nutnost přijatelné a pro občana motivující délky vytištěné podoby BKP použito hashovacího algoritmu **SHA1**.

Identifikátory

Pro tvorbu identifikátorů bude primárně využito vhodné formy UUID dle příslušných standardů. Jedná se zejména o případy typu identifikátory zasílaných zpráv. Ve vybraných případech mohou mít identifikátory či prvky, které mají též funkci identifikátorů i jinou konstrukci (viz např. BKP).

Stanovení způsobu prezentace ochranných prvků

K prezentaci ochranných prvků v rámci datových vět není nutno řešit prezentaci daných údajů s ohledem na jejich délku a lze používat standardním norem a doporučení. Rozhodující je zejména zvolený rámec pro reprezentaci a přenos dat XML.

Prezentace je klíčová v případě ochranných prvků na fyzickém výtisku účtenky. Zde je nutno respektovat následující předpoklady a omezení:

- prvky musí být prezentovány pouze tehdy, je-li to účelné, tedy nepoužívat prezentaci prvků v případech, kdy tento ochranný prvek není nutný
- prvky musí být reprezentovány v dostatečně přehledné a čitelné podobě, tedy zejména z pohledu volené znakové sady a struktury zápisu
- prvky musí být prezentovány úsporným způsobem tak, aby výsledná délka tištěného ochranného prvku umožňovala stále jeho využití fyzickými osobami, případně od použití tyto fyzické osoby neodrazovala nad míru nezbytně nutnou
- je vhodné využívat také alternativních (neznakových) tištěných forem prezentace, pakliže tyto mohou usnadnit nakládání s reprezentovanými informacemi pro občany a zjednodušovat a zrychlovat pořizování účtenek pro povinné subjekty.

Jak stanoví kapitola 0 „Stanovení ochranných prvků“, je nutno na fyzickém výtisku účtence prezentovat:

- BKP
- OKP v případě potřeby vydání účtenky v off-line módu
- FIK v případě vydání účtenky v online módu (reprezentace daného kódu je řešena samostatně a není předmětem této specifikace).

S ohledem na volené algoritmy stanovené kapitolou 0 „Stanovení algoritmů použitých pro ochranné prvky a jejich síly“ je základní binární délka ochranných prvků BKP a OKP následující:

Ochranný prvek	Kryptografické schéma	Binární délka v bytech
BKP	SHA1	20
OKP	SHA-256/RSA2048	256

Oba ochranné prvky mají charakter binární informace resp. řetězce bytů a nejsou tedy přímo reprezentovatelné na fyzickém výtisku účtenky. Oba ochranné prvky BKP a OKP tedy vyžadují specifickou formu prezentace.

Znaková reprezentace kódů

S ohledem na jejich délku a požadavek na úspornou reprezentaci není vhodné použití standardně nejlépe přehledné a čitelné prezentace ve formě hexadecimálního zápisu v 16 znakové sadě [0 – 9, a -f], neboť hexadecimální prezentace zdvojnásobuje binární délku vstupu. Proto je volena prezentace kódováním BASE64.

Vychází se ze standardní 64 znakové sady [0 – 9, a –f, A – Z, ‘/’, ‘+’]. Standardní kódování BASE64 je dále redukováno o použití potenciálních závěrečných zarovnávacích znaků ‚=‘, které by jinak byly pro dané délky vstupů vkládány (výstupy by byly standardně doplňovány jedním zarovnávacím znakem v případě BKP a dvěma zarovnávacími znaky v případě OKP). Výsledná prezentace kódu ve znakové podobě bude přijatelně přehledná a čitelná a současně oproti hexadecimálnímu zápisu výrazně úspornější.

Výsledná prezentace ochranných prvků je tedy volena následovně:

Ochranný prvek	Kódování	Výsledný počet prezentovaných znaků
BKP	BASE64	43
OKP	BASE64	342

Ve fázi návrhu řešení je možné dále zvážit úpravu základní znakové sady z pohledu odstranění znaků, které jsou „kolizní/zaměnitelné z hlediska čitelnosti“. Jedná se o případy typu velké O a nula („O“ vs „0“) či malé l a jednička („l“ vs „1“). Odstranění těchto kolizí lze docílit náhradou kolizních znaků (např. velké O a malé l) jinými z tohoto pohledu nekolizními znaky, které jsou současně tištitelné na fyzickou účtenku na straně povinných subjektů.

Alternativní reprezentace QR kódem

Vhodnou alternativní reprezentací údajů na fyzickém výtisku účtenky je použití **QR kódu**. Jeho použití v rámci EET je motivováno snahou:

- Současná případně alternativní reprezentace ochranných prvků a optimálně dalších významných informací účtenky jedním QR kódem
- zjednodušit skrze QR kód načtení klíčových informací fyzického výtisku účtenky pro občany a kontrolní orgány
- reprezentací velkých informací typu OKP.

Vzhledem k tomu, že QR kód není použitelný a "přepsatelný" bez použití prostředků jako jsou např. aplikace pro zařízení typu SmartPhone či tablet, není pro člověka, který takovým prostředkem nedisponuje reálně využitelný. Z důvodu zajištění přístupu občana/zákazníka k jím použitelné informaci je nutno při použití QR kódu nakládat s modelem, kdy:

- v případě potřeby vydání účtenky v off-line módu bude fyzická účtenka obsahovat BKP a FIK ve znakové podobě a případně současně QR kód

- v případě potřeby vydání účtenky v online módu bude fyzická účtenka obsahovat BKP ve znakové podobě a dále variantně OKP ve znakové podobě nebo QR kód obsahující též OKP.

Kapacita QR kódů (objem reprezentovatelné informace - počet "znaků") se výrazně liší dle jednotlivých typů (1 až 40), dle velikosti znakové sady ukládané informace a dle úrovně korekce chyb (schopnost výsledného QR kódu odolávat chybám/kvalitě/poškození výtisku či následného čtení/skenování). QR kódy s vysokou kapacitou stovek až tisíců znaků jsou "husté" a vyžadují vyšší kvalitu vytištění a/nebo větší plochu vytištění. Použitelná kapacita QR kódu pro potřeby systému EET bude do značné míry dána dostupnou kvalitou tisku a dostupným tiskovým prostorem u zařízení vydávajících na straně povinných subjektů fyzické účtenky.

Optimálním cílem, je zajistit QR kódem reprezentaci nejen kódů BKP, OKP a FIK, ale také vlastních významných údajů účtenky. V takovém případě je nutno uvažovat s kapacitou cca 1000 znaků širší znakové sady.

Příklad reprezentace

Výše specifikovaná forma reprezentace vede k řetězcům, jejichž podoba je uvedena na následujícím příkladu, který je též doplněn o alternativní reprezentaci QR kódem (kódováno je spojení BKP a OKP pro potřeby příkladu v podobě „BKP:…. OKP:…“):

Ochranný prvek	Kódování	Výsledný řetězec k tisku	Výsledný QR kód
BKP	BASE64	X0Z2l7LsLJcBUPhUGW2tWc6CTmM	
OKP	BASE64	hiTtrr/D5uv1GxhXhoSrfwvfY96XpZy1HNQeE88i3y4jD0Xyj2zkGKWVY/tGKJJWb6QTRbdAV2vGT0lgxcM0CFy5bSMfh6jP1W7qGCiD9RAKzXS0T8cd5DpjuqeQHfZFdNz8DaA/eJS7tWvv8oy1z2tzLGYIc+Q3KSudCs2/KP4piwhIafJSFqiegr4GrlNpQ/q6LUahP9B6fUtu7DHD+YFhWTINt5rJni+qxdKQ4cYWGaHvG0U+VqoIsLo5gez6FVMpw40kUX+xpgBcPNx7NOz21MNmA4uEyGtigRSI+2dUFnmwfQ5J76kxdFF3PlUnEdCJjFjah71Ami7IvmLZtw	

Technické a technologické řešení projektu

Logické aplikační schéma aplikace EET je definováno požadavky jednotlivých definic procesů, které mají být v rámci funkcionality aplikace zajištěny.

V první fázi realizace projektu EET se zajišťuje prostředí pro následující procesy:

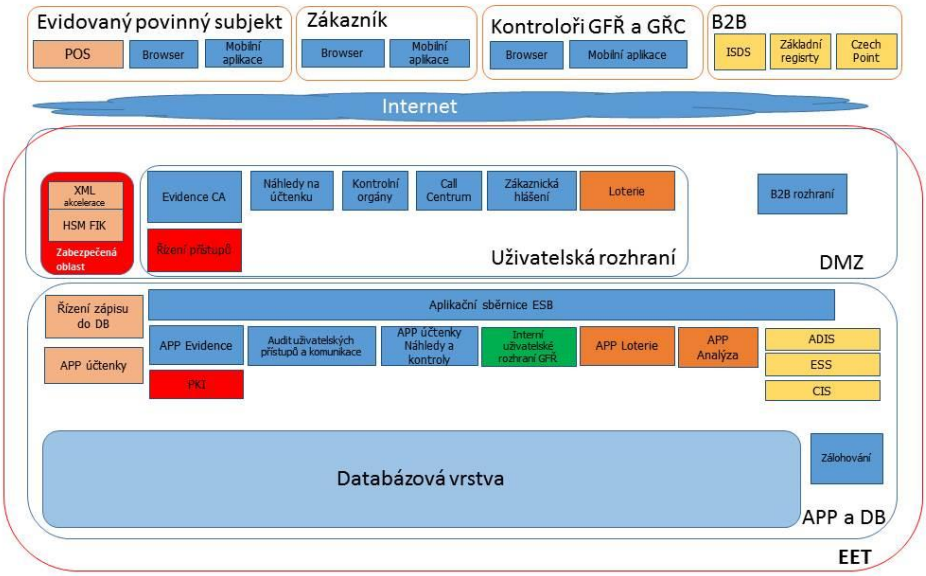
1. Registrace a evidence údajů a certifikátů o povinném subjektu
2. Evidence tržeb
3. Přístup poplatníka k vlastním statistickým údajům
4. Kontrola účtenky zákazníkem
5. Nahlášení neobdržené účtenky zákazníkem
6. Kontroly ze strany FS a CS
7. Následná analýza a vyhodnocování dat
8. Loterie

Jednotlivé procesy a jejich požadavky jsou rozepsány v samostatné části zadávací dokumentace.

V rámci požadovaných procesů je nutné zajistit další následující související služby:

- Interní certifikační autorita
- Auditní záznamy
    - Evidence auditních záznamů z komunikačního rozhraní
    - Evidence auditních záznamů o přístupech evidovaných osob
- Evidence přístupových údajů povinných subjektů
- Zálohování provozního prostředí
- Zabezpečená část technického řešení v úrovni Důvěrné

Logická architektura aplikace



Obrázek 15: Logická architektura EET

Uživatelé prostředí EET

Uživatelé EET jsou děleni do následujících skupin

- Evidovaný povinný subjekt
  - POS – prodejní místo, pokladna
  - Browser – přístup na portálové rozhraní EET
  - Mobilní aplikace - přístup na portálové rozhraní EET
- Zákazník (držitel účtenky)
  - Browser - přístup na portálové rozhraní EET
  - Mobilní aplikace - přístup na portálové rozhraní EET
- Kontrolní orgány GFŘ a GŘC
  - Browser - přístup na portálové rozhraní EET
  - Mobilní aplikace - přístup na portálové rozhraní EET
- B2B
  - Externí systémy státní správy
    - ISDS – Informační Systém Datových Schránek
    - Základní Registry
    - Czech Point

Uživatelská rozhraní portálu EET

- Zabezpečená oblast
  - XML akcelerace - Zpracování zasílaných účtenek
  - HSM FIK - Vystavení bezpečnostního evidenčního kódu FIK

- Evidence CA
  - Uživatelské rozhraní evidence povinných subjektů
  - Uživatelské rozhraní vystavení požadovaných certifikátů
- Řízení přístupů
  - Evidence uživatelských přístupů evidovaných povinných subjektů
- Náhledy na účtenku
  - Uživatelské rozhraní náhledů na účtenky
- Kontrolní orgány
  - Uživatelské rozhraní pro kontrolní orgány GFŘ a GŘC
- Call Centrum
  - Uživatelské rozhraní pro potřeby pracovníků CallCentra
- Zákaznická hlášení
  - Uživatelské rozhraní zákaznických hlášení o chybách účtenek
- Loterie
  - Uživatelské rozhraní účastníků loterie
- B2B rozhraní – rozhraní pro napojení na ISDS, Základní registry, CzechPoint

Datová a aplikační vrstva

Z hlediska datové vrstvy jsou v současné době data ukládána:

- v datovém úložišti vybudovaném v rámci projektu EET s požadavkem replikace dat mezi dvěma datovými úložišti. Datová úložiště budou umístěna ve dvou oddělených technologických prostorech v lokalitě datového centra SPCSS

Hlavním cílem v datové oblasti je konsolidovat, sjednotit a integrovat technologie datových úložišť (dále DÚ) na bázi nově budovaného datového úložiště při dodržení zásady ochrany již vynaložených investic, sjednocení zabezpečeného přístupu k datům.

V oblasti aplikační vrstvy a datových úložišť jsou vybudována dvě provozní prostředí – **integrační/testovací** pro integraci a testování POS aplikací a doladění jejich vazeb a prostředí **produkční**.

Aplikační vrstva bude tvořena serverovou farmou, na které bude provozováno aplikační prostředí EET s požadovanou redundancí a funkcionalitou.

- Řízení zápisu do DB – zápis účtenek do databáze
- APP účtenky – zpracování účtenek
- APP evidence – evidence povinných subjektů
- PKI – interní certifikační autorita
- Audit uživatelských přístupů a komunikace – zpracování auditních záznamů systému
- APP účtenky, Náhledy na účtenky – realizace zpracování přístupů na účtenky
- Interní uživatelské rozhraní – aplikační rozhraní EET pro pracovníky GFŘ
- APP loterie – aplikační část EET loterie
- APP analýza – zpracování analýz v systému EET
- ADIS – napojení na vybrané služby ADIS
- ESS – napojení na elektronickou spisovou službu
- Aplikační sběrnice ESB – orchestrace jednotlivých služeb systému EET
- Zálohování – provozní zálohy dat EET a aplikačních, databázových serverů
- Databázová vrstva
  - Rychlá data – evidence účtenek (2-4 měsíce)
  - Dlouhodobé úložiště – evidence účtenek na dobu 10 let
  - Evidence povinných subjektů, provozoven a XML podání

  - Kontroly a sankce
  - Auditní záznamy
  - Loterie
- Rozhraní GFŘ – interní uživatelské rozhraní pro zaměstnance GFŘ a GŘC, Servicedesk SPCSS, Call centrum pro veřejnost
  - Agregované a analytické údaje

Prezentační vrstva

Aplikační vrstva bude tvořena serverovou farmou, na které bude provozováno aplikační prostředí EET s požadovanou redundancí a funkcionalitou.

Základem prezentační vrstvy je uživatelský portál prezentující jednotlivé uživatelská rozhraní pro několik skupin uživatelů systému a rozhraní B2B pro realizaci služeb evidence účtenek. Uživatelský portál a B2B rozhraní je od sebe logicky a fyzicky odděleno tak, aby nedocházelo k ovlivňování provozu navzájem.

Rozhraní:

- **B2B** – komunikační rozhraní dedikované pro komunikaci s POS
- **Evidence a CA** – autorizované uživatelské rozhraní pro evidenci povinných subjektů a certifikační autoritu
- **Access management** – správa uživatelských přístupů
- **Náhled na účtenku** – neautorizované rozhraní pro náhledy na jednotlivé účtenky
- **CallCentrum** – autorizované rozhraní pro služby poskytované externím dodavatelem služeb
- **Kontroly** – autorizované rozhraní pro kontrolní orgány GFŘ
- **Audit-** evidence auditních záznamů

Metriky systému

Dále je uvedena základní sada metrik:

- Dostupnost klientského rozhraní v režimu 24/7,
- Dostupnost datových služeb v režimu 24/7,

Popis	Počet	Jednotka	Poznámka
Počet účtenek za rok	10 500 000 000,00	ks	
Počet účtenek za den	30 000 000,00	ks	
Průměrná velikost účtenky (s el. podpisem)	8,50	kB	
B2B rozhraní pro sběr účtenek			
Průměrný počet přijímaných účtenek	347,00	Ks/sec	
Špičková požadovaná propustnost přijímaných účtenek	4 000,00	Ks/sec	
Průměrná odezva centrálního systému na vystavení účtenky	0,33	sec	Jedná se o odezvu systému na vystavení FIK a uložení účtenky
Maximální odezva centrálního systému na vystavení účtenky při špičkovém zatížení	2,00	sec	Jedná se o odezvu systému na vystavení FIK a uložení účtenky
Požadavky na úložiště			
Rychlé úložiště po dobu	3	měsíců	S rezervou okamžitého rozšíření úložiště na 5 měsíců
Dlouhodobé úložiště na dobu	4	roky	S možností rozšíření na 10 let
Certifikační autorita			
Minimální počet evidovaných certifikátů	2 000 000	ks	Rozšiřitelné na 5 000 000
Počet vystavovaných certifikátů	200	ks/min	
Uživatelské rozhraní, aplikační vrstva			
Počet současně pracujících uživatelů webového rozhraní	200	uživatelů	
Průměrná odezva na dotaz	0,5	sec	
Obnova systému po incidentu Recovery Time Objective (RTO)			
Pro rychlé úložiště evidence účtenek a B2B aplikační rozhraní	12	hod	Čas potřebný pro obnovu systému a zprovoznění B2B aplikačního rozhraní, obnova dat
Pro dlouhodobé úložiště účtenek a uživatelské webové rozhraní	48	hod	Čas potřebný pro obnovu systému a zprovoznění aplikačního rozhraní
Obnova dat dlouhodobého úložiště účtenek	až 30	dní	Obnova dat ze zálohy dlouhodobého úložiště účtenek
Recovery Point Objective (RPO)	10	min	Možná ztráta dat při obnově havarovaného systému. Hodnota určuje pravděpodobnou ztrátu dat v časovém období předcházejícím havárii.

Požadované provozní a SLA parametry

- Portál pro povinné subjekty a veřejnost
  - provozní doba 24x7
  - dostupnost v provozní době 99,9%
- WS rozhraní pro fiskalizaci
  - provozní doba 24x7
  - dostupnost v provozní době 99,99%
- Rozhraní pro front-office
  - provozní doba 8,5x5
  - dostupnost v provozní době 99,9%

V rámci návrhu architektury jsou požadovány následující provozní parametry služeb jednotlivých vrstev architektury (SLA parametry):

- Datová vrstva
  - provozní doba 24x7
  - dostupnost v provozní době 99,99%
- Aplikační vrstva
  - provozní doba 24x7
  - dostupnost v provozní době 99,99%
- Prezentační vrstva (Frontend)
  - provozní doba 24x7
  - dostupnost v provozní době 99,9%
- Komunikační infrastruktura
  - provozní doba 24x7
  - dostupnost v provozní době 99,99%.

SLA pro zajištění provozu systému EET

Základní návrh parametrů pro stanovení provozního SLA systému EET

Seznam služeb

Následuje přehled služeb a jejich významných parametrů:

Číslo služby	Kategorie služby	Popis
1	Provoz služeb komunikační infrastruktury	Provoz infrastruktury systému EET
2	Provoz HW a SW infrastruktury	Provoz HW a SW infrastruktury tvořící systémy EET
3	Podpora povinných subjektů (service desk)	HW, SW a aplikační podpora povinných subjektů

Parametry služeb:

Číslo služby	Kategorie služby	Garantovaná celková dostupnost %	Garantovaná celková doba obnovy [hod]	Provozní doba služby
1	Provoz služeb komunikační infrastruktury	99,99	2	Po – Ne 0:00 – 24:00
2	Provoz HW a SW infrastruktury	99,99	2	Po – Ne 0:00 – 24:00
3	Podpora povinných subjektů	99,9	4	Po – Ne 7:00 – 17:00

Definice dostupnosti

Dostupností služby se rozumí:

Poskytovatel garantuje, že všechny požadované *systémy* dle definovaných služeb, tedy jednotlivý SW a HW a komunikace budou dostupné, tedy schopné provozovat danou službu.

Hlavní kritérium dostupnosti :

Služba je považována za nedostupnou když:

I. Uživatelé oznámí tuto skutečnost Provozovateli
II. Provozovatel potvrdí nedostupnost služby

Vysvětlení definice nedostupnosti:

I. Uživatele oznámí tuto skutečnost Provozovateli

Oznámení o incidentu je nezbytnou podmínkou pro to, aby byl systém považován za nedostupný.

II. Provozovatel potvrdí nedostupnost serverů

Tuto akceptaci provozovatelem je možno použít pro zjednodušení procesu potvrzení nedostupnosti. Předpokládá se na základě historie incidentů, že naprostá většina incidentů ohlášených jako nedostupná služba bude uznána jako oprávněná. Je tomu tak proto, že nedostupnost *služeb* je v převážné většině případů evidentní a nezpochybnitelná.

Požadované parametry systémů

Provozovatel aplikace dodá prokazatelně požadované parametry systémů. Tyto požadované parametry budou jakékoliv vlastnosti, procesy, konfigurace či soubory na *Systémech*. Požadovaným parametrem nesmí být funkčnost vlastní aplikace ale pouze podmínky pro její provoz.

Požadované parametry systémů jsou vlastnosti systémů, které musí být splněny, aby všechny požadované *služby* byly dostupné, tedy schopné provozovat aplikace.

Vzorec dostupnosti

Služba se skládá ze jednotlivých *Systémů*.

Dostupnost jednotlivého systému $dost_i$ je :

$$dost_i = [\ 1 - T_{nedost} / (\text{počet hodin v měsíci})\ ] * 100\ \%$$

kde

T_{nedost} doba po kterou je jednotlivý *Systém* nedostupný v hodinách za měsíc. Doba nedostupnosti je započtena z období požadované provozní doby služby. Požadovaná provozní doba služby je 0:00 – 24: 00 ve všechny dny

Začátek T_{nedost} Doba se začíná měřit v okamžiku ohlášení. Pokud tento okamžik není v požadované provozní době služby, počítá se od nejbližšího (časově následujícího) zahájení provozní doby služby.

Konec T_{nedost} Incident se ukončí v okamžiku kdy systém či služba je opět dostupná podle definice dostupnosti. Rozhodující je čas evidovaný na ServiceDesku. Opětovná dostupnost služby musí být doložitelná na základě monitoringu a splnění požadovaných parametrů systémů. V případě že ukončení incidentu nastane mimo rozsah požadované provozní doby služby, pak se započítává ukončení nejbližšího (časově předchozího) ukončení provozní doby služby.

Celková dostupnost služby je:

$$DOST = \sum dost_i / n$$

Kde

$dost_i$ je dostupnost jednotlivého systému služby

n je počet systémů služby

Specifikace provedení detailní analýzy

První oblasti realizace veřejné zakázky je provedení detailní analýzy vztažené k realizaci Projektu EET respektive realizaci jednotlivých funkcionalit Projektu EET.

Obsah analýzy

Obsahem analýzy a výstupů bude zpřesnění způsobu realizace této zakázky, zejména potom:

- Detailní popis identifikace v informačních systémech Zadavatele pro informační služby publikované v prostředí EET.
- Detailní popis procesu realizace jednotlivých dotazů ve vazbě na služby poskytované Projektem EET:
    - B2B přístup, GUI přístup, WS (web services) přístup,

  Jedná se o detailní specifikaci technické realizace. Popis procesu realizace informačních služeb publikovaných na EET.
- Detailní způsob realizace jednotlivých informačních služeb –
    - kategorie informačních služeb (evidence, dotaz rychlý, dotaz pomalý, atd.),
    - potřebné datové zdroje pro realizaci informační služby,
    - způsob realizace odpovědi pro jednotlivé požadované informační služby,
    - definice rolí (skupiny uživatelů) včetně přiřazení k informačním službám,
    - počet uživatelů (klientů) a transakcí (dotazů) pro každou informační službu včetně předpokladu „náběhové“ křivky těchto počtů,
- Zpřesnění požadavků Projektu EET na infrastrukturu a její využití, zejména:
    - HW aplikační vrstvy,
    - diskového prostoru:
        - kapacita,
        - přiřazení pro jednotlivé komponenty Projektu EET,
        - tier resp. další parametry,
    - technický návrh rozložení zátěže,
    - verifikace výkonnosti infrastruktury ve vztahu k upřesnění informačních služeb Projektu EET (zaručená odezva, SLA…)
    - „projekce“ nárůstů požadavků na výkon a kapacitu u definovaných a implementovaných informačních služeb s výhledem na 4 roky s projekcí na navrženou infrastrukturu.
    - časové (harmonogram),
    - bezpečnostní požadavky a promítnutí na realizované řešení.
- Návrh základních provozních postupů, principů a požadavků na personální a smluvní zajištění.
- Návrh dalšího rozvoje a dalších informačních služeb realizovatelných po ukončení úvodní fáze Projektu EET.

Výstupy detailní analýzy

1. Detailního technického projektu celého Projektu EET.
2. Návrh jednotné registrace, identifikace a autorizace pro povinné subjekty a interních pracovníků GFŘ a GŘC.
3. Detailního implementačního plánu Projektu EET.

Nutná součinnost pro realizaci analýzy

Zadavatel předpokládá, že vybranému Uchazeči, který bude realizovat tuto zakázku, pro realizaci analýzy poskytne součinnost ze strany následujících organizačních jednotek a pracovníků:

- SPCSS,
- garantů odborných agend GFŘ,
- vlastníků dat odborných agend GFŘ zejména systému ADIS,
- právních a metodických odborů MFČR a GFŘ,

Dále Zadavatel zajistí součinnost ze strany SPCSS zejména v oblastech:

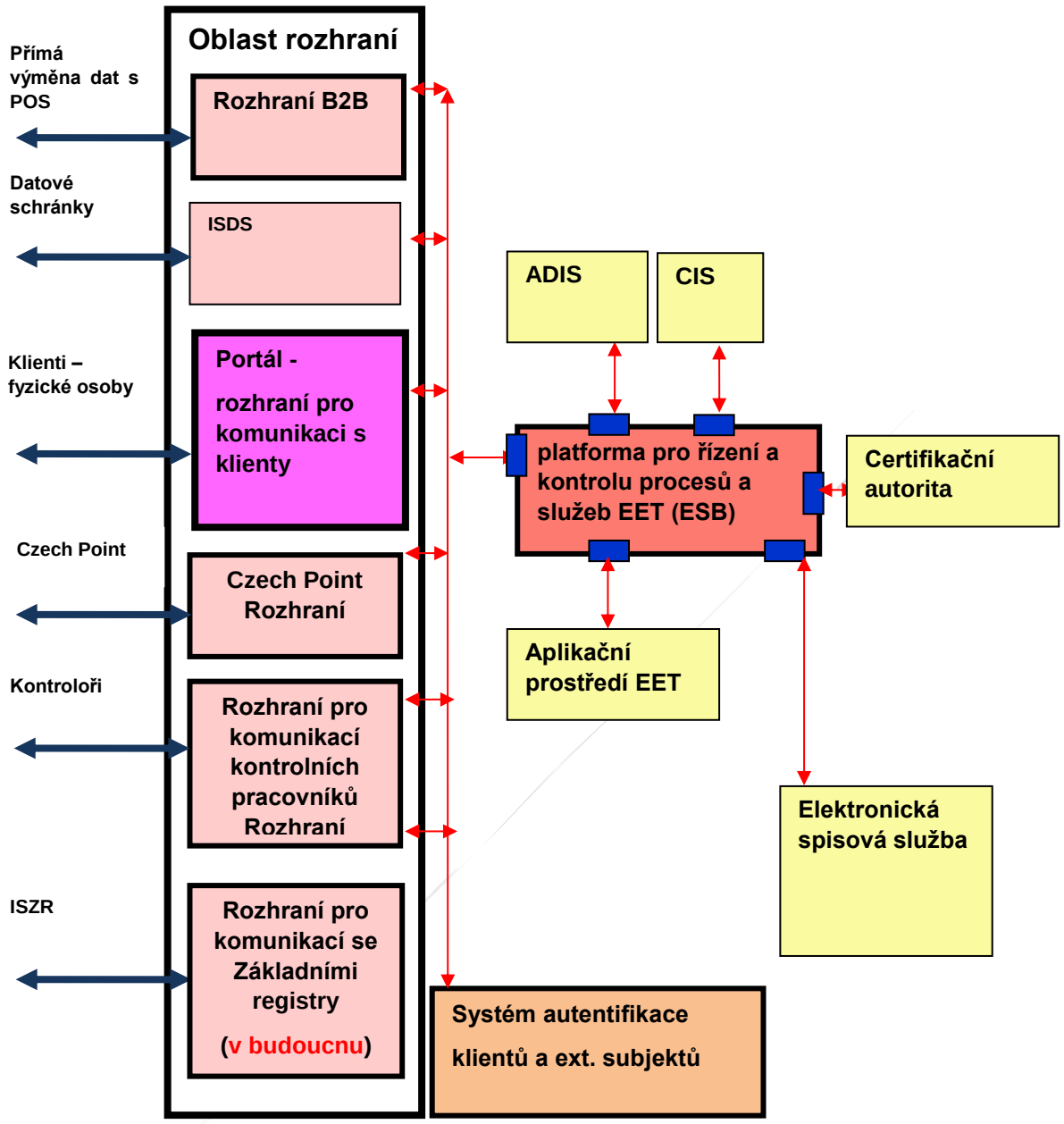
- komunikační infrastruktury,
- jednotné registrace, identifikace a autorizace pro pracovníky GFŘ a GŘC.

Technická specifikace EET

EET bude jedinou bezpečnou vstupně výstupní branou pro komunikaci v oblasti evidence účtenek. Klientské rozhraní bude poskytovat služby, data a informace pro zaměstnance GFŘ, veřejnost, povinné subjekty a současně bude umožňovat i komunikační kanály pro získávání informací od třetích stran (externích zdrojů) pro potřeby interních odborných aplikací. Napojení systému EET na systém Základních Registrů po potřebu ověřování adres registrovaných provozoven.

Vazby a rozhraní systému EET

Vazby komunikačních a ostatních informačních systémů (na systém EET a okolí) jsou znázorněny v následujícím schématu:



Obrázek 16: Vazby komunikačních a ostatních informačních systémů na systém EET a okolí

Pro zajištění požadovaných služeb prostředí EET je zapotřebí zajištění rozhraní a vazeb na jiné systémy státní správy tak na interní systémy GFŘ (ADIS, spisové služby).

Rozhraní pro evidenci

Pro potřeby evidence povinných subjektů je požadováno napojení na systém datových schránek pro příjem požadavků na evidenci a ukládání těchto žádostí v prostředí spisové služby. Druhým rozhraním pro evidenci do prostředí EET, bude rozhraní na Czech Point pro povinné subjekty, které nemají datovou schránku.

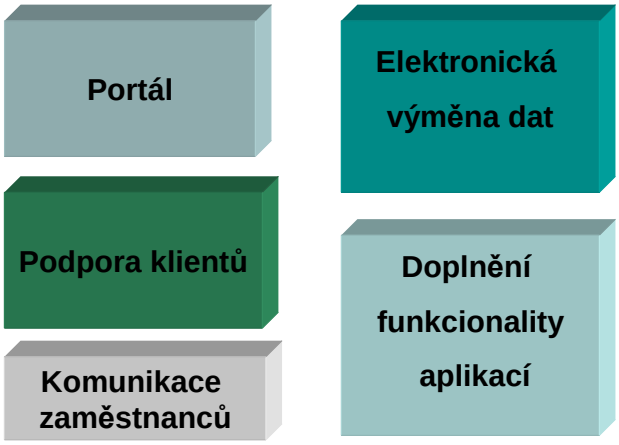
Dalším rozhraním je napojení na systém základních registrů (ISZR) pro potřeby ověřování existence adres evidovaných provozoven. Z tohoto důvodu musí systém EET být registrová jako agendový systém s oprávněním přístupu do základních registrů (tato funkcionalita bude realizována v etapě po spuštění systému do provozu).

Rozhraní pro realizaci sběru účtenek a jejich kontrolu a evidenci

B2B rozhraní je hlavním výkonným rozhraním na které jsou kladeny extrémní nároky. Rozhraní pro zákaznickou kontrolu a rozhraní pro kontrolní pracovníky GFŘ je realizováno v rámci portálového řečení a zajišťují přístup k jednotlivým údajům o evidovaných účtenkách.

Funkční dekompozice

Funkční dekompozice vychází ze zajištění hlavních cílů Projektu EET. Podrobnější popis funkcionality jednotlivých komponent je zřejmý z popisů procesů. Funkcionalitu Projektu EET tvoří 5 základních funkčních oblastí:



Obrázek 17: Funkční dekompozice EET

Komponenty Projektu EET

Dodávka a implementace řešení (prostředí) EET tj. výběr vhodné platformy pro realizaci klientského rozhraní, dodání vhodných SW komponent EET a implementace EET (provedení instalace, customizace, konfigurace, testování) do prostředí Zadavatele, zejména:

- Identity/Access Manager, který bude zajišťovat autentizaci a autorizaci povinných subjektů.
- Portálové řešení, které bude zajišťovat interaktivní webový přístup klientů a dalších subjektů k poskytovaným službám.
    - frontend API rozhraní,
    - integrační platforma pro EET,
    - rozhraní
    - nástroje pro správu portálu (redakční systém),
- Enterprise Service Bus
- Audit Manager, který bude zajišťovat logování veškerých přístupů pro potřeby:
    - statistik přístupů,
    - ověřování SLA poskytovaných služeb,
    - ověřování SLA využívaných služeb třetích stran (externích zdrojů).

Celkové řešení klientského rozhraní složené z jednotlivých definovaných komponent, které budou vzájemně integrovány a musí vytvářet homogenní řešení.

Řešení EET je napojeno na stávající komponenty SPCSS:

- Monitoring
- Bezpečnost
- Service desk
- Call centrum
- Posílání stavových a transakčních informací do úložiště pro potřeby auditu
- Autorizace a autentizace.

Portálové řešení

Portálové řešení musí umožňovat definovaným způsobem implementovat poskytované služby (funkčnosti), které pomocí webového rozhraní (WWW) budou dostupné definovaným skupinám uživatelů.

Primárně bude sloužit pro komunikaci B2C a B2B bude samostatný preferovaný komunikační kanál pro sběr účtenek.

Mezi základní požadované funkčnosti patří:

- Snadná a rychlá implementace uživatelského rozhraní pro nové interaktivní služby.
- Snadná definice a změna grafického manuálu uživatelského rozhraní.
- Jednoduchá změna uživatelského vzhledu na úrovni obsahu pro jednotlivé uživatelské skupiny a typy zařízení.
- Stránky budou plně kompatibilní minimálně pro prohlížeče

  Internetové rozhraní:
  - IE (od verze stávající mínus 1),
  - Firefox (od verze stávající mínus 1),
  - Google Chrome (od verze stávající mínus 1),
  - Apple Safari (od verze stávající mínus 1).

  Intranetové rozhraní
  - IE (od verze 10),
  - Firefox (od verze 30),

Další požadované funkcionality:

- Možnost prezentace informací formou portletů podle standardů JSR-168 a JSR-286.
- Podpora SOA – integrace s ostatními systémy.
- Identity/Access Manager - stávající user management pro přístupy pracovníků na interní aplikační rozhraní a externí kontrolní rozhraní.
- Řízený přístup k informacím prostřednictvím rolí nebo členstvím uživatele ve skupině (komunitě).
- Vyhledávání informací.
- Monitorování aktivit.

Poskytované služby WS

Poskytované služby musí být dostupné minimálně pomocí rozhraní webových služeb (WS) a budou primárně určeny pro komunikaci B2B (výměnu dat mezi systémy).

Požadované standardy:

- HTTP/HTTPS.
- SOAP.
- WSDL.

Doplňující standardy:

- XML, XSD, UDDI.
- REST.

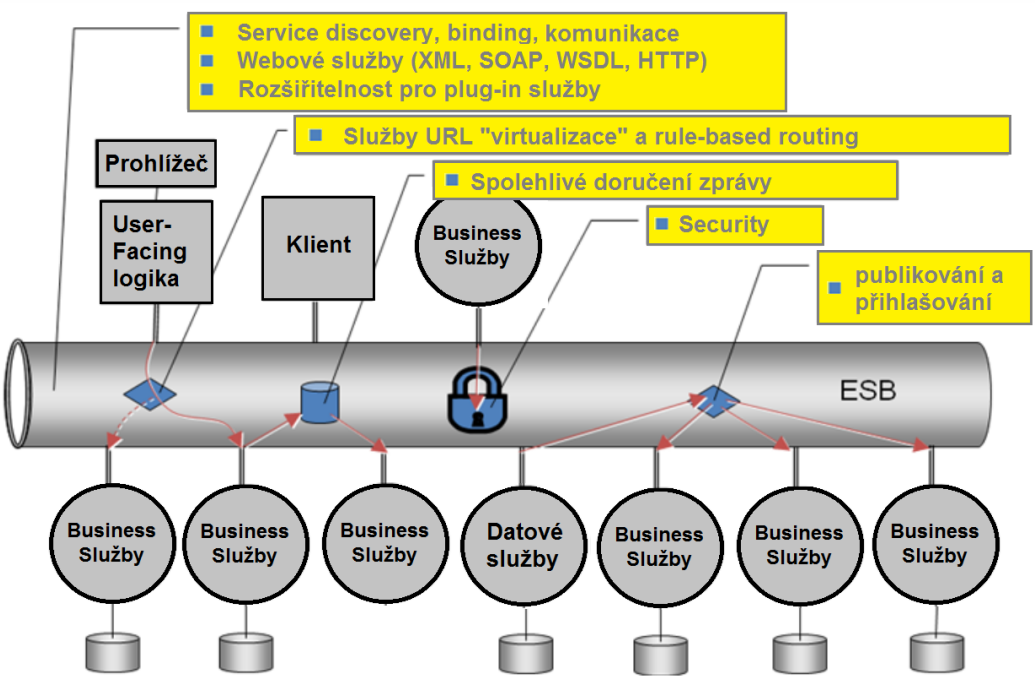
Access Manager musí umožňovat tyto základní typy autentizace:

- Uživatele webového klientského portálu na základě:
  - Login/Password Přístupového klíče s omezenou dobou platnosti (OTP),
- Uživatele (konzumenty) služby poskytované EET na základě:
  - Login/Password,
  - přístupového klíče s omezenou dobou platnosti (OTP),
  - klientského certifikátu.
- Uživatele rozhraní pro vzdálený přístup na základě:
  - Interního zaměstnaneckého certifikátu, čipové karty
- Systémových účtů komunikujících s aplikacemi třetích stran pro získávání externích dat na základě:
  - Login/Password,
  - systémového certifikátu.

Enterprise Service Bus (ESB)

Zadavatel pro realizaci Projektu EET resp. této veřejné zakázky požaduje, aby byla pro nabídky Uchazečů, a následnou realizaci vybraným Uchazečem, požaduje, aby byly využity principy SOA architektury a byla rozpracována rámcová architektura s využitím sběrnice (ESB) a těmito vlastnostmi a parametry:

- standardizovaná integrační aplikace, která podporuje všechny hlavní komunikační scénáře, včetně žádost/odpověď, jednosměrné přenosy zpráv s garantovaným doručením a vice komplexní přenosy událostí a zpráv,
- standardizace XML, HTTP, SOAP, WSDL , a JAX-RPC,
- standardizované konektory a možnost vytváření dalších konektorů,
- rozšiřitelnost a modularizace.



Obrázek 18: Enterprise Service Bus

B2B (dedikovaný pro sběr účtenek)

V rámci řešení EET bude B2B hlavní rozhraní prezentováno jako externí služba pro přijímání dat (účtenek).

Ošetření komunikace prostřednictvím B2B rozhraní musí být zabezpečeno pomocí TSSL/SSL a musí umožňovat komunikace pouze definovaným způsobem a formátem XML opatřeným příslušným platným certifikátem. Komunikace nevyhovující definovaným požadavkům bude zahazována.

Informace předané přes B2B rozhraní budou předávány přes standardní definované rozhraní EET.

Audit Manager

Další komponentou je Audit Manager, kterého úkolem bude logování veškerých datových toků vstupně výstupní brány. Současně musí umožňovat analýzu a prezentaci získaných dat pro:

- Provozní statistiky.
- Podklady k ověřování SLA poskytovaných služeb.
- Podklady k ověřování SLA využívaných služeb třetích stran.
- Podklady pro bezpečnostní audit a řešení případných bezpečnostních incidentů.

Audit manager bude napojen na centrální audit manager SPCSS

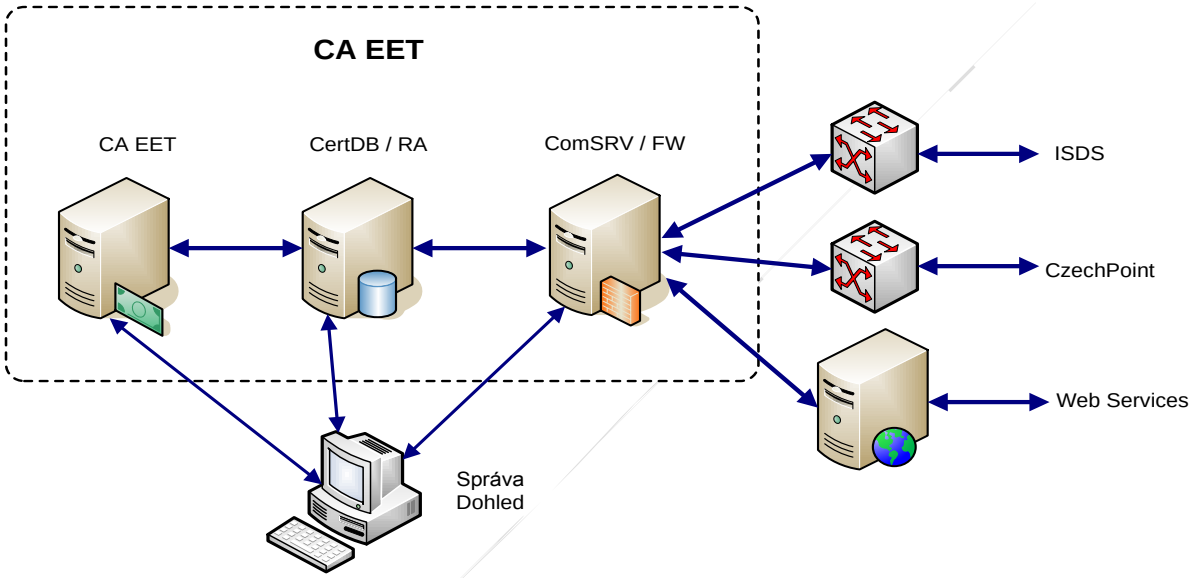
Certifikační autorita

Certifikační autorita (dále jen CA) je budována pro zajištění funkce systémů Elektronické evidence tržeb (dále jen EET). Účelem CA EET je vydávat certifikáty Povinným subjektům (dále jen POS) a centrálním systémům EET (dále jen CS). Tyto certifikáty jsou dále používány k podepisování (zajištění integrity a nepopiratelnosti) datových vět, odesílaných POSy do EET a naopak.

Certifikační autorita PKI a její řešení musí být navržena na základě bezpečnostních požadavků jako dvouúrovňová architektura se zajištěním ochrany klíčových prvků systému.

Základní softwarové komponenty PKI využívají open-source licence, což pozitivně ovlivňuje náklady na pořízení, provoz a upgrade. Zároveň musí být dbáno, že použité prvky nebudou mít negativní vliv na klíčové části systému, zejména na bezpečnost dat.

Blokové schéma



Obrázek 19: Blokové schéma CA EET

Dopady realizace CA EET na stávající IS GFŘ

CA EET je nově budovaný systém, který nebude využívat služeb ani nebude kooperovat se stávajícími IS MFČR. Jeho vliv na stávající IS MFČR bude minimální, pokud vůbec jaký.

Výkonové požadavky

CA EET a RA EET musí být dimenzovány na vydávání a správu jednotek milionů certifikátů. POSy se budou zapojovat do systému v několika vlnách, takže lze předpokládat, že ve špičkách budou vydávány statisíce certifikátů denně. Jelikož požadavky se budou shlukovat v pracovní době, musí CA a RA zpracovat řádově několik jednotek až několik desítek žádostí za sekundu.

Požadavky na dostupnost a odezvu

Přesto, že vydání certifikátu ve skutečnosti není časově kritické, s ohledem na udržení dobrého jména provozovatele systému a zamezení negativní publicity doporučujeme, aby CA EET i RA EET byly v provozu nepřetržitě a aby bylo použito řešení s vysokou dostupností. Odezva na žádost o vydání certifikátu nesmí překročit jednotky sekund, jinak hrozí zahlcení systému stále se prodlužujícími frontami požadavků.

Požadavky na přenos dat

Budeme-li předpokládat, že jedna žádost i jeden certifikát mají velikost 1 kB a sítí projde 10 žádostí a 10 certifikátů za sekundu, jedná se o přenos 20 kB/s, což je hodnota bez problému dosahovaná lokálními i rozsáhlými sítěmi.

Využití dohledu

CA EET musí být v provozu nepřetržitě. Naprostá většina operací však bude probíhat automaticky, bez nutnosti lidského zásahu. V mimopracovní době však musí být zajištěn dohled nad provozem CA a RA. Dohled musí mít možnost informovat osoby v důvěryhodných rolích, případně vyžadovat podporu dodavatele v případě mimořádné situace.

Požadavky na hardware

CA EET v uspořádání v principu odpovídajícím blokovému schématu bude realizována ve dvou identických instancích, nazývaných Hlavní a Záložní a třetí, funkčně shodnou instanci Testovací / Školící, avšak s nižšími výkonovými požadavky. Instalace Hlavní a Záložní instance je doporučeno na geograficky jiných lokalitách. Testovací / Školící CA EET bude obsahovat navíc i několik testovacích systémů POS na různých platformách. Tomu musí odpovídat návrh hardwarového řešení.

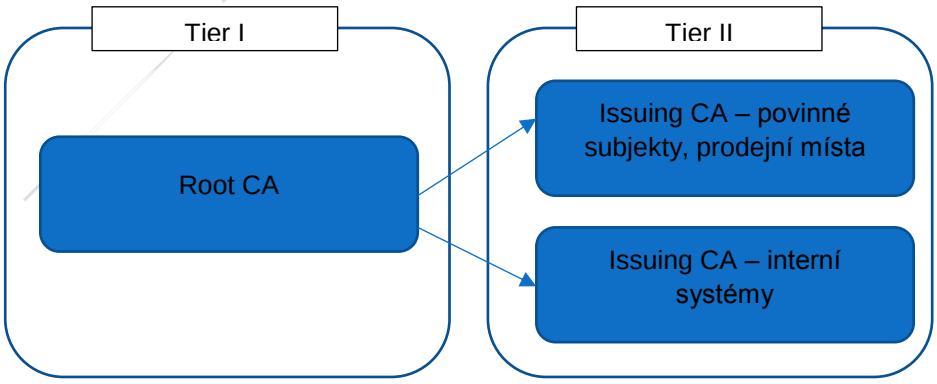
Předpokládá se, že každá CA EET bude řešena jako sada serverů a jiných zařízení, umístěných ve společné 19“ přístrojové skříni. Tato skříň bude umístěna v technologických prostorách s fyzickým a režimovým zabezpečením. Obsluha a dohled budou prováděny vzdáleně, pomocí pracovních stanic a napojením na funkce dohledového střediska.

Třetí, Testovací / Školící instance CA EET bude užívána pro testování software a pro školení obsluhy.

Struktura instancí certifikační autority PKI

Systém je navržen jako dvouúrovňová certifikační autorita, přičemž kořenová (root) CA slouží výhradně pro ukotvení hierarchie, tedy nevydává přímo klientské certifikáty. Účelem koncové CA (tzv. issuing CA) je naopak poskytovat požadovanou službu vydávání certifikátů.

Pro maximální flexibilitu jsou navrženy dvě instance koncových CA, přičemž jedna z nich poskytuje certifikáty pouze pro povinné subjekty EET (představitele subjektu, prodejní místa apod.) a druhá instance generuje certifikáty pouze pro interní IT zařízení (je-li potřeba). Požadované řešení je znázorněno na následujícím diagramu.



Obrázek 20: Řešení CA EET

Navržené řešení nesmí vylučovat možnost pro vybudování doplňkové Tier II CA, pokud bude existovat opodstatnění pro jejich vznik. Požadavek na řešení, aby případné CA určené pro případné vývojové/testovací/demonstrační účely nebyly zakotveny v hlavní hierarchii důvěry, tedy mezi jejich nadřazenými CA nebude figurovat výše uvedená Root CA.

Parametr systému	Metrika	Hodnota pro kořenovou CA	Hodnota pro koncovou CA
Architektura CA	Počet vrstev certifikačních autorit	dvě vrstvy	
Počet instancí	**Počet jednotlivých instancí certifikačních autorit v jednotlivých vrstvách**	**1**	**2**
Algoritmus pro tvorbu elektronických podpisů	Kombinace primitivních kryptografických mechanismů, pomocí nichž systém generuje elektronické podpisy.	RSA + SHA-256	RSA + SHA-256
Velikost klíče CA	Délka bitového řetězce, který tvoří soukromý klíč certifikační autority	4096 bitů	2048 bitů
Platnost certifikátu CA	Maximální doba platnosti certifikátu certifikační autority.	10 let	6 roky
Aktivní období certifikátu CA	Doba, po kterou jsou daným certifikátem CA podepisovány vystavované klientské certifikáty.	4 let	3 let
Platnost vydávaných klientských certifikátů	Doba, po kterou jsou platné vydávané certifikáty určené pro subjekty nebo IT systémy	N/A	max. 3 roky subjekt max. 2 roky systém

Provozní parametry

Parametr systému	Metrika	Hodnota pro kořenovou CA	Hodnota pro koncovou CA
Dostupnost služeb – ověřování certifikátů	Maximální délka časového intervalu v hodinách, kdy certifikační autorita neposkytuje služby související s ověřováním platnosti certifikátů.	6 hodin	0,5 hodin
Dostupnost služeb - ostatní	Maximální délka časového intervalu v hodinách, kdy certifikační autorita neposkytuje služby nesouvisející s ověřováním platnosti certifikátů.	96 hodin	2 hodin
Kapacita	Řádový počet vystavených certifikátů, který je CA schopná vygenerovat a evidovat, aniž by docházelo k degradaci výkonu.	jednotky až desítky	miliony

Požadavky na software a funkce

Subsystém CA EET představuje vlastní certifikační autoritu. Základním určením CA EET je vydat vlastní selfsigned kořenový certifikát a následně na základě identifikace a autentizace žádostí od POS a CS vydávat podepisovací certifikáty pro POSy a CS.

Subsystém CertDB / RA EET je komponenta podporující správu certifikátů a CRL. Subsystém zároveň plní funkce registrační autority CA EET. Tato podpora se předpokládá pro stejnou množinu klientů, kterou pokrývá CA EET.

Subsystém ComSRV / FW představuje komunikační a bezpečnostní rozhraní k vnějšímu světu. Aktuálně se předpokládá, že CA EET bude komunikovat třemi kanály: Informační systém datových schránek (ISDS), kontaktní místa CzechPoint a webové služby.

Registrační procedury

CA EET je certifikační autoritou pro POSy a CS. Registrační procedury CA EET realizuje subsystém RA EET.

Registrace povinných subjektu

O registraci a následně o certifikát mohou žádat POS podle připravovaného Zákona o evidenci tržeb a CS.

Zde je třeba uvést, že neplatí, že jeden POS = jeden certifikát. Zejména větší POS mohou žádat o více certifikátů, například pro jednotlivé provozovny nebo i jednotlivá místa pro příjem hotovosti (pokladny). Takovýto subjekt se samostatným certifikátem dále nazýváme Klient POS (KPOS).

Otázka registrace klientů je úzce spjata s problematikou prvotní žádosti o certifikát. Vzhledem k množství očekávaných klientů bude jejich registrace prováděna automatizovaně. Ztotožnění žadatele, kterým je právnická nebo fyzická osoba, se předpokládá následujícími způsoby:

- Zaslání žádosti o registraci prostřednictvím datové schránky (ISDS), to zejména v případě právnických osob,
- zaslání žádosti prostřednictvím služeb CzechPoint, to zejména pro fyzické osoby – OSVČ.
- zaslání žádosti podepsané kvalifikovaným elektronickým podpisem prostřednictvím webových služeb.

Z těchto údajů vytvoří registrační autorita CA EET jedinečný kód každého KPOS, který bude obsažen v poli CHR jeho certifikátu. RA EET vydá Rozhodnutí o registraci. V rozhodnutí o registraci je uvedena CAR identita systému CA EET a CHR identita KPOS. Naplnění polí CHR musí být upřesněno před započetím vývoje CA EET.

Pro podporu registrace KPOS musí být implementovány tyto postupy:

- Registrace KPOS – prvotní zavedení registračních údajů;
- Prohlížení KPOS – zobrazení registrovaných dat;
- Editace KPOS – možnost změnit registrační data klienta.

Vzhledem k očekávanému počtu KPOS musí být CE EET, resp. její registrační autorita, vybavena uživatelsky přívětivými nástroji pro správu velkého počtu klientů, jako seskupování, hromadné editace, dávkové příkazy, importy-exporty aj.

Prvotní žádost o vlastní certifikát

Bude-li jako kořenový certifikát CA EET použit vlastní selfsigned certifikát, musí být stanoven postup pro generování klíčového páru, žádosti a certifikátu.

Bude-li jako kořenový použit certifikát nadřízené autority, řídí se postup při žádosti o tento certifikát certifikační politikou příslušné CA.

Import vlastního certifikátu

Pro import vlastního certifikátu musí být implementovány tyto postupy:

- Manuální import certifikátu
- Automatizované přijetí certifikátu.

Po přijetí nového vlastního certifikátu se veškeré podpisové operace realizují s využitím nových párových dat náležejících tomuto certifikátu.

Správa KPOS

CA EET, resp. její registrační autorita, musí disponovat softwarovými nástroji na správu dat většího počtu registrovaných KPOS. Ve správě KPOS musí být zahrnuty tyto postupy:

- Registrace klienta – nástroj na zavedení nového klienta
- Prohlížení klientů
- Editace klienta – úprava registračních údajů
- Blokování klienta – zablokování klienta musí znemožnit vydání certifikátu pro klienta
- Odblokování klienta.

Zpracování žádosti o certifikát od KPOS, vydání certifikátu

Po registraci KPOS je možno zpracovávat žádosti o certifikát od ISY.

Důležitou otázkou je ověření identity žadatele a pravosti žádosti při prvotní žádosti o certifikát. Naskýtá se několik možností řešení.

- Zaslání žádosti o registraci prostřednictvím datové schránky (ISDS), to zejména v případě právnických osob
- Zaslání žádosti prostřednictvím služeb CzechPoint, to zejména pro fyzické osoby – OSVČ
- Zaslání žádosti podepsané kvalifikovaným elektronickým podpisem prostřednictvím webových služeb.

Vydání následného certifikátu v době platnosti certifikátu

Ověření identity při zpracování žádosti o následný certifikát je provedeno s využitím předchozího certifikátu vydaného témuž KPOS či CA. Žádost musí být ve tvaru, kdy je opatřena vnějším podpisem. Tento podpis musí být vytvořen pomocí soukromého klíče odpovídajícího certifikátu. Tento certifikát musí být v době zpracování žádosti a vydání následného certifikátu platný.

Vydání následného certifikátu po době platnosti certifikátu

Pokud nebude vnější podpis žádosti o následný certifikát úspěšně ověřen, bude žádost zamítnuta a žadatel musí podstoupit proceduru vydání prvotního certifikátu.

Modifikace certifikátu

CA EET neumožňuje modifikaci certifikátu. Při potřebě změny obsahu certifikátu je nutno vydat nový certifikát a původní uvést v CRL.

CA EET rovněž neumožňuje prodloužení platnosti certifikátu a příslušného klíčového páru změnou položky Certificate Expiration Date. Prodloužení platnosti certifikátu je možné pouze cestou vydání následného certifikátu k novému klíčovému páru.

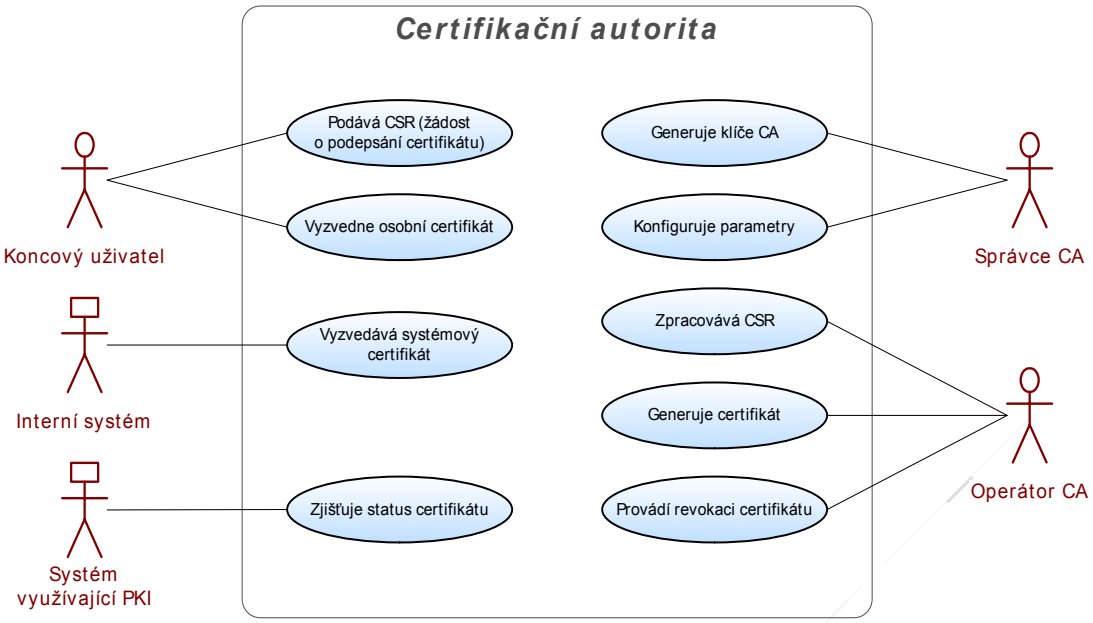
Požadavky na nastavení a kontrolu času

Certifikáty obsahují položky vymezující časové údaje označované jako:

- Certificate Effective Date – datum generování certifikátu
- Certificate Expiration Date – datum vypršení platnosti certifikátu.

Systém CA EET vyžaduje násobnou kontrolu časového údaje (více NTP serverů, dohledové centrum).

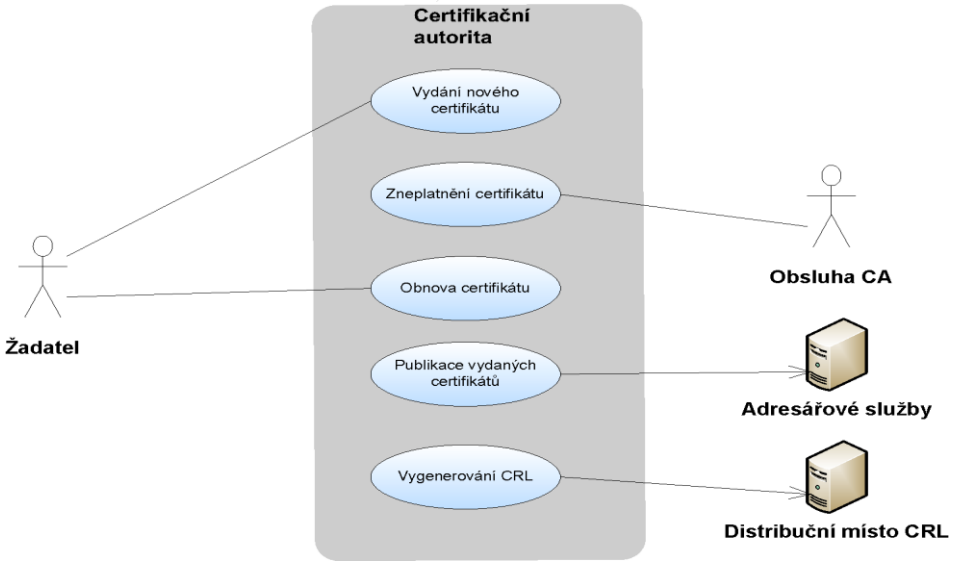
Požadovaná užití rozhraní CA



Obrázek 21: Požadované použití rozhraní CA

Procesní specifikace

Procesy probíhající v Interní Certifikační Autoritě (ICA) jsou znázorněny na následujícím diagramu případů užití:



Obrázek 22: Procesy probíhající v Interní Certifikační Autoritě

Uživatelé z hlediska vydávání certifikátů

V systému budou tito uživatelé:

- Žadatel o certifikát (povinný subjekt) - prostřednictvím CA získává certifikát, následně si jej může obnovit. Žádá o zneplatnění certifikátu.

- Obsluha CA - přijímá žádosti o zneplatnění certifikátů - tuto roli zastává administrátor CI.
- Adresářové služby - představují úložiště vydávaných certifikátů.
- Distribuční místo - představuje úložiště aktuálního CRL (Certificate revocation list - Seznam zneplatněných certifikátů) generovaného ICA.

Předpisová základna

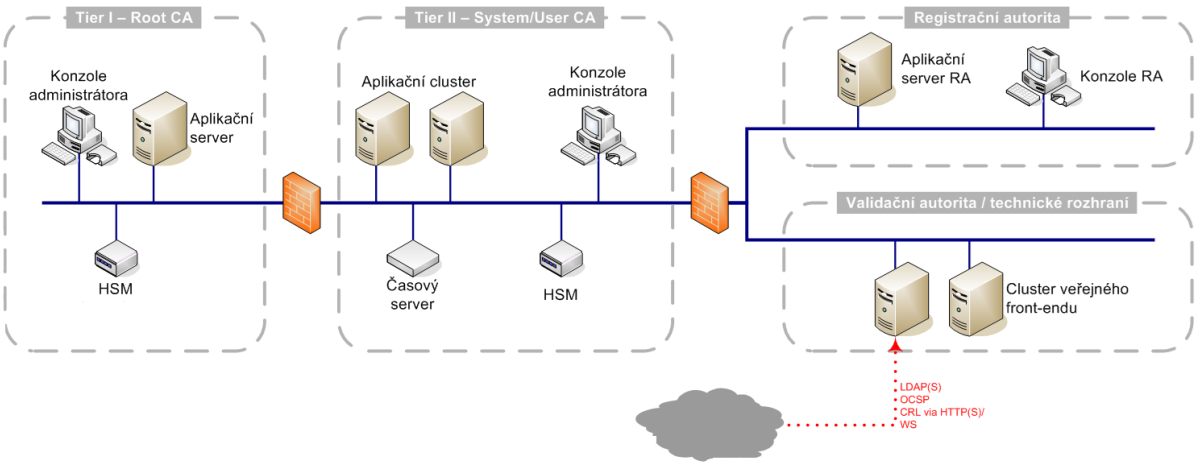
V průběhu implementace Certifikační autority (CA) budou zpracovány nezbytné dokumentace a předpisy.

Předpisová základna musí minimálně tvořit:

1. Certifikační politika – zásady uplatňované při vydávání certifikátů a specifikaci obsahu vydávaných certifikátů v souladu s „RFC 3647 – Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework“:
    - Výklad základních pojmů
    - Přehled poskytovaných služeb (vydávání certifikátů, CRL)
    - Přehled typů poskytovaných certifikátů
    - Základní práva a povinnosti
2. Certifikační prováděcí směrnice – postupy používané při vydávání certifikátu v souladu s RFC 3647:
    - Obecná ustanovení (práva, povinnosti, odpovědnost)
    - Identifikace a autorizace (pravidla registrace, obnovení klíče)
    - Provozní požadavky a postupy (vydávání, zneplatňování, audit, archivace, správa klíčů)
    - Bezpečnostní mechanismy – netechnické (fyzická, procedurální a personální bezpečnost)
    - Bezpečnostní mechanismy – technické (generování a ochrana klíčů, počítačová bezpečnost, komunikační bezpečnost)
    - Profily certifikátů a CRL
    - Další administrativní postupy (změny, schvalování)
3. Systémová bezpečnostní politika – způsob uplatnění celkové bezpečnostní politiky v systému, způsob ochrany dat systému pro vydávání certifikátů, popis bezpečnostních opatření a vyhodnocení analýzy rizik:
    - Základní popis systému
    - Popis bezpečnosti prostředí (předpoklady, hrozby, pravidla)
    - Bezpečnostní cíle
    - Aplikovaná bezpečnostní opatření
4. Příručka správce – návod pro používání a správu systému:
    - Pravidla a postupy instalace
    - Provozní pravidla a postupy
    - Bezpečnostní pravidla a postupy
    - Pravidla a postupy pro zajištění kontinuity
    - Nastavení provozních a bezpečnostních parametrů

Požadavky na technologické řešení

Na obrázku níže je zobrazen minimální požadavek na síťovou konfiguraci. Tato konfigurace zohledňuje požadavky na bezpečnost (oddělení jednotlivých zón firewally) a dostupnost (clusterování klíčových komponent).



Obrázek 23: minimální požadavek na síťovou konfiguraci CA EET

Auditní záznamy

Systém musí zaznamenávat do auditního logu údaje, vážící se k bezpečnosti provozu.

V rámci provozu CA EET jsou zaznamenávány provozní události následujících typů:

- Události spojené s operacemi v rámci životního cyklu certifikátu
- Události spojené s řízením přístupu k systému CA EET
- Události spojené se změnami konfigurace systémů CA EE
- Události spojené s životním cyklem klienta
- Jiné významné události spojené s provozem systémů CA EET.

V rámci událostí, spojených s operacemi životního cyklu certifikátu, jsou zaznamenávány:

- Zavedení certifikátu
- Generování vlastní žádosti o certifikát
- Zpracování žádosti o certifikát klienta
- Vydání certifikátu
- Export certifikátů.

V rámci událostí, spojených s řízením přístupu k systému CA EET, jsou zaznamenávány:

- Zavedení uživatele
- Správa uživatele (zneplatnění, atd.)
- Úspěšné přihlášení uživatele
- Neúspěšný pokus o přihlášení
- Odhlášení uživatele.

V rámci jiných významných událostí, spojených s provozem systému CA EET, jsou zaznamenávány zejména:

- Spuštění systému CA EET
- Ukončení / přerušení provozu systému CA EET
- Provedení záloh
- Generování párových dat CA EET a certifikátů
- Provozní chyby.

Pro všechny události jsou zaznamenávány identifikace události, čas výskytu události a uživatele, závažnost události.

Události jsou zaznamenávány:

- Elektronicky, v databázi nebo logovacím souboru
- Případně současně v papírové formě (provozní deníky).

V rámci událostí, spojených se změnami konfigurace systému CA EET, jsou zaznamenávány zejména:

- Změny politiky CA EET (událost vedena v provozním deníku)
- Změny konfigurace systémů CA EET (událost vedena v provozním deníku).

Auditní záznamy jsou ukládány v textové podobě s následující strukturou:

- Závažnost události
- Datum a čas vzniku události
- Kategorie typu události (skupina a typ)
- Zdroj – komponenta generující auditní záznam
- Identifikace uživatele
- Identifikace role
- Unikátní číslo události
- Data – údaje blíže popisující zaznamenanou událost (vstupní údaje, výsledek operace apod.).

Integritu auditních záznamů garantuje jejich uložení se zabezpečením přístupových práv.

Po exportu auditních záznamů do archivu bude zachována struktura dat v textové podobě, data bude možno prohlížet standardními editory.

Zálohování, obnova, replikace dat

Dodavatel musí v rámci vývoje systému navrhnout procesy pro:

Replikace kryptografických klíčů

Při návrhu koncepce správy klíčů zvážit metody automatické replikace kryptografických klíčů, které by garantovaly sdílení stejných kryptografických klíčů ve všech HSM pracujících ve společném clusteru.

Replikace obsahu databáze

Za provozu musí být replikována databáze na oba uzly clusteru, případně bude cluster pracovat nad sdíleným diskovým polem.

Při ukončení činnosti na aktivním systému CA EET daného dne musí být provedena replikace (záloha) obsahu relevantních tabulek databáze pro přenos na Záložní systém.

Možnosti konfigurace

Z hlediska možností konfigurace musí CA EET:

- být konfigurovatelná pro použití všech přípustných kryptografických algoritmů
- mít konfigurovatelná uživatelská oprávnění
- být vybavena konfigurovatelným firewallem pro vytváření bezpečných komunikačních kanálů
- mít možnost ručně korigovat nastavení systémového času
- mít možnost konfigurovat profil vydávaného certifikátu
- musí mít možnost konfigurovat vytváření záznamů o provozu systému a činnostech uživatelů.

Požadavky na role a procesy

Dodavatel CA EET navrhne:

- strukturu důvěryhodných rolí pro obsluhu CA EET,
- jejich náplň činnosti,
- požadavky na slučitelnost a neslučitelnost rolí,
- procesy vyžadující součinnost více rolí

Dále dodá odhad pracovního vytížení pro jednotlivé role.

Požadavky na dokumentaci

Dodavatel CA EET zhotoví:

- Analytickou dokumentaci, tj:
  - Analýza technického řešení CA EET
  - Analýza rizik
  - Analýza bezpečnostních požadavků
  - Bezpečnostní projekt
  - Systémová bezpečnostní politika
  - Projekt technického řešení CA EET
- Provozní dokumentaci, tj.
  - Systémová příručka
  - Uživatelské příručky pro jednotlivé role
- Bezpečnostní dokumentaci, t.j.
  - Směrnice pro technickou bezpečnost
  - Směrnice pro netechnickou bezpečnost
  - Směrnice pro reakci na incidenty
  - Směrnice pro kontinuitu činností.

Bezpečnostní směrnice pro jednotlivé role.

Pro případ, že by byl považován CA EET za obecný informační systém veřejné správy ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy, je pro splnění požadavků tohoto zákona požadováno:

- Systémová příručka popisuje způsob instalace, uvedení do provozu, pravidelné údržby a administrátorských úkonů na systému. Plní zároveň úlohu Systémové příručky ve smyslu zákona č. 365/2000 Sb., a vyhlášky č. 529/2006 Sb.

- Uživatelské příručky pro jednotlivé role popisují provádění jednotlivých úkonů v běžném provozu CA EET pracovníky v příslušných rolích. Pro každou roli je zpracována samostatná příručka. Plní zároveň úlohu Uživatelské příručky ve smyslu zákona č. 365/2000 Sb., a vyhlášky č. 529/2006 Sb.

Požadavky na školení

Součástí dodávaného systému bude příprava a provedení školení uživatelů a administrátorů jednotlivých částí dodávaného systému.

Součástí přípravy školení bude vytvoření dokumentace pro účastníky jednotlivých školení.

Veškerá školení budou provedena v dohodnutých termínech před zahájením ostrého provozu.

Součástí dodávaných školení nejsou konkrétní produktová školení dodávaná jednotlivými dodavateli hardware a software. Pokud objednatel uzná za nutné, aby obsluha a uživatelé byli vyškoleni v těchto produktech, doporučujeme přímo kontaktovat jednotlivé dodavatele, kteří nabízejí celou řadu školení a certifikačních programů.

Požadavky na hardwarové prvky prostředí

Aplikační server

Předpokládá se využití virtualizovaného řešení v rámci realizace samostatných serverů a jejich redundance. Umístění Certifikační autority bude logicky odděleno od ostatních systémů s využitím bezpečnostních aktivních prvků realizovaných v rámci komunikační infrastruktury EET.

Minimální konfigurace jednoho serveru:

Parametr	Doporučená hodnota
Virtualizace	Virtualizační prostředky schodné s celkovým pojetím virtualizace EET
Operační systém	systém unixového typu (RHEL, SUSE Linux ES, Debian Linux apod.)
CPU	architektura x86/x86-64, parametry dle doporučení pro operační systém
Paměť	Minimálně 8 GB na server
Disková kapacita	Vyhrazená disková kapacita , minimálně 1000 GB v RAID I konfiguraci
Síťové připojení	100/1000 MBit/s

HSM

Hardwarový bezpečnostní modul je základním kamenem návrhu certifikační autority. Zařízení musí být schopno generovat, ve spolupráci s hlavním HSM modulem, náhodné soukromé klíče a bezpečně je uchovávat. Veškeré operace vyžadující tyto klíče probíhají ve vnitřním výpočetním prostředí HSM, a tudíž klíče v čitelné podobě nikdy HSM neopouštějí.

Zálohování/obnova vnitřních dat HSM je citlivou operací a musí umožnit duplikaci dat na záložní zařízení pro potřeby zajištění vysoké dostupnosti anebo export obsahu zašifrovaného pomocí klíčů.

HSM zařízení musí mít odpovídající úroveň certifikace.

Požadovaná infrastruktura pro aplikační prostředí EET

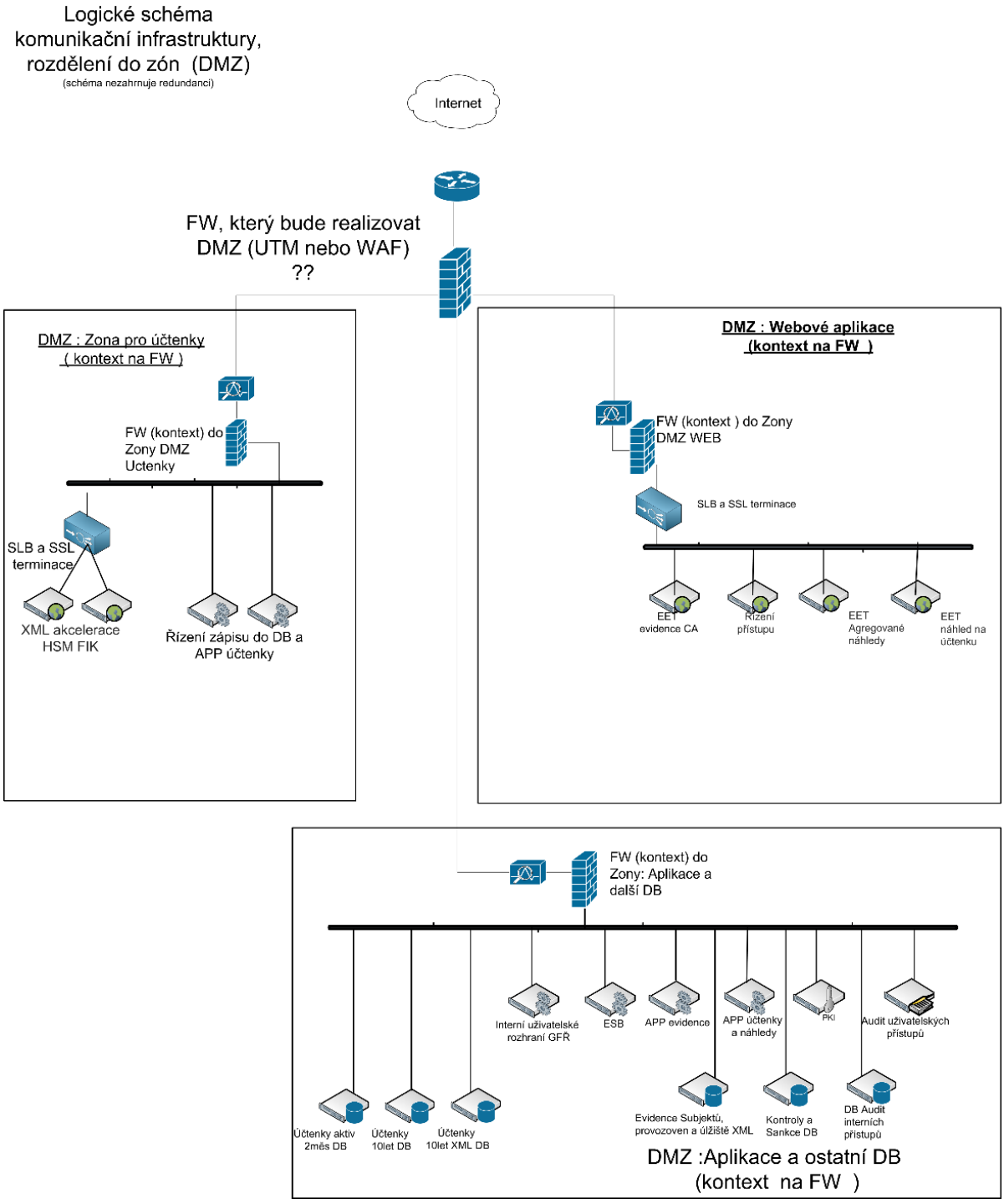
Aplikační prostředí a potřebná infrastruktura bude dělena minimálně do následujících zón:

1. DMZ 1 – Zóna pro zpracování účtenek a vystavování evidenčního bezpečnostního kódu FIK
2. DMZ 2 – Webové aplikace. Webový uživatelský portál pro potřeby aplikačního rozhraní EET
3. APP a DB – realizace ESB sběrnice pro orchestraci služeb, aplikační servery pro jednotlivé požadované služby, interní uživatelské rozhraní, databázové prostředí
4. CA – certifikační autorita

Základní požadavkem na infrastrukturu EET je maximální virtualizace zdrojů, redundance jednotlivých částí infrastruktury v jednotlivých zónách. Pro virtualizované prostředí je předpokládáno možnost přesouvání jednotlivých virtualizovaných zdrojů mezi jednotlivými zónami.

Schéma základních zón

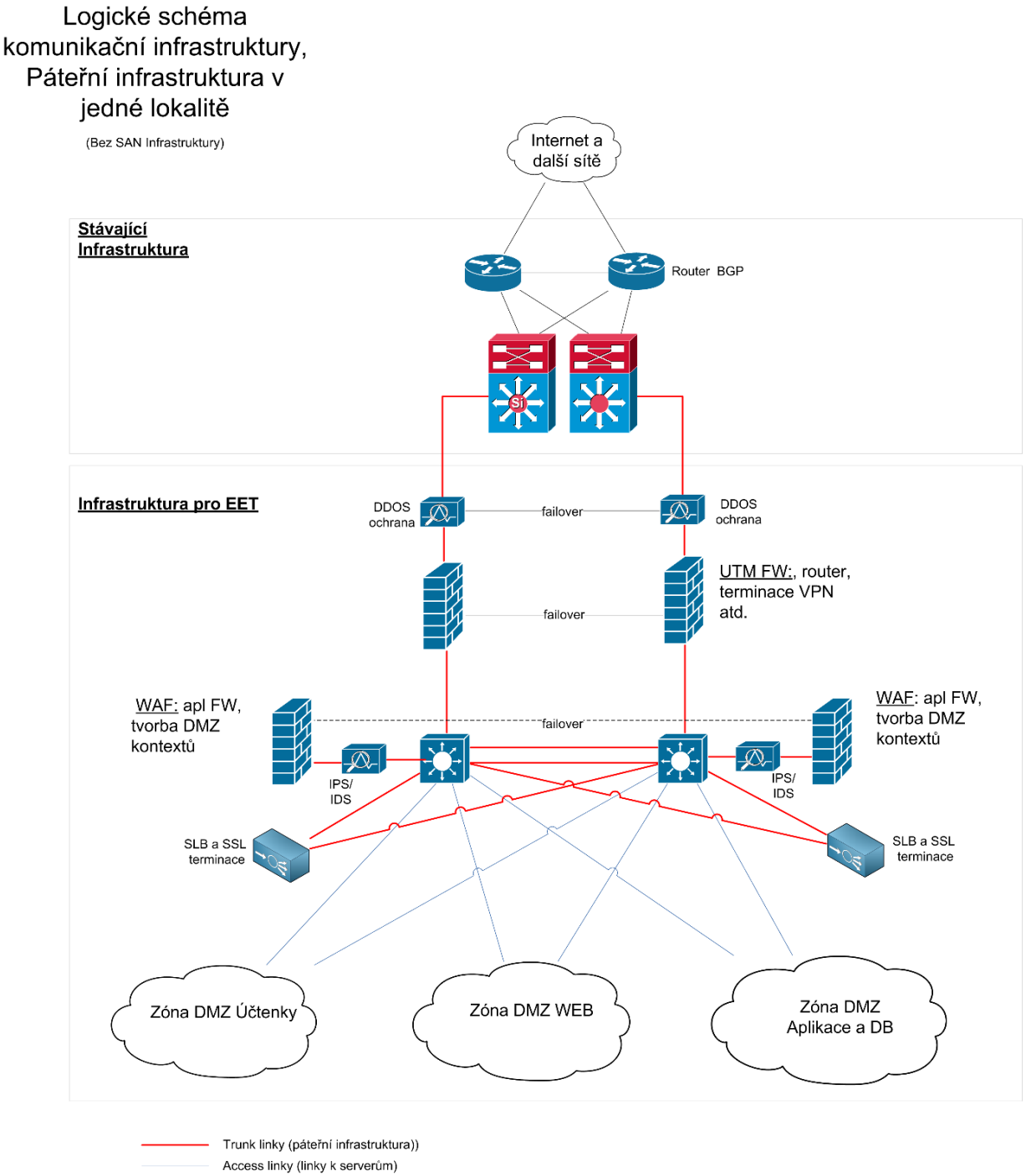
Základní schéma zón s rozdělením požadované funkcionality je patrné z následujícího obrázku:



Obrázek 24: Základní schéma zón systému EET

Schéma logické komunikační infrastruktury

Základní schéma logické komunikační infrastruktury je uvedeno na následujícím obrázku:



Obrázek 25: Schéma logické komunikační infrastruktury systému EET

Komunikační infrastruktura

- Propustnost prvků 4 Gbps
- Páteřní switche s propustností 10 Gbps na portech s možností použití 1/10 Gbps rozhraní (optika, metalika)
- Zdvojená architektura
- Použití UTM - routovací funkce, Firewall, ukončení VPN – žádné další funkce nelze použít z důvodu garantování propustnosti zařízení
- Použití IPS/IDS – na základě požadavků zákona o kybernetické bezpečnosti a pro ochranu operačních systémů a midleware před sofistikovanými útoky.
- SSL terminace na Loadbalancerech (LB),
- Pro přístup na webové rozhraní použít WAF – ve spolupráci s LB
- SIEM – analýza nebezpečného chování/pokusů o průnik – viz zákon o kybernetické bezpečnosti
- Out of band management všech prvků z bezpečnostních důvodů (OOB).

Požadavek na použití **dedikovaných zařízení** pro následující funkce

- **DDOS ochrana** - je specifická, protože musí rozeznat SSL fload od regulérního SSL provozu aplikace. Toho lze dosáhnout jedině tak, že IPS nebo WAF dokáže pracovat jako sonda DDOS ochrany a indikovat včas pakety, které jsou vadné a svědčí o SSL útoku. DDOS podle indikace vytvoří pravidlo a škodlivé SSL pakety odfiltruje.
- **Firewall & routing** (ASIC na akceleraci) jsou to hlavní dvě funkce používané z UTM, UTM musí mít alespoň 100 virtuálních nezávislých firewallů s centrálním managementem a reportingem (vhodné realizovat separátními zařízeními)
- **Switching** (VLAN separace)
- **Switching pro OOB** (management prvků mimo provozní komunikační kanály – garantuje bezpečnost a navíc umožňuje spravovat jednotlivé prvky bez ohledu na jejich vytížení/zatížení/zahlcení v provozních kanálech, stačí porty 100/1000 Gbps
- **IPS/IDS** (60000 connections /s) – chrání operační systémy a midleware před útoky/zneužitím jejich slabin
- **LoadBalancing** – Ukončení SSL (7000 connections a ASIC akcelerací pro ukončení SSL) – rozkládá zátěž
- **WAF** – chrání webové aplikační servery před zneužitím slabin v aplikacích (např. vytváření neregulérních komunikačních jader přes které lze vyčítat data), dataminingem, zneužitím SQL jazyka, může ukončovat SSL sizing odpovídá IPS/IDS, loadbalancerům a očekávané zátěži webových aplikačních serverech.
- **SIEM** – korelační analýza logů prováděná za účelem odhalení nebezpečných jevů vedoucích k odhalení útoků a zneužití.

XML appliance - B2B, webové a aplikační servery

Pro oblast řešení B2B komunikace s v rámci komunikace pokladních systémů s prostředím EET je požadována takové řešení, která bude sjednocovat potřebnou funkcionalitu spojenou s příjmem účtenky ve formátu XML certifikátem, kontrola certifikátu ve vztahu k účtence, kontrola správnosti XML, vystavení bezpečnostního kódu (FIK) a jeho odeslání v rámci kompaktního řešení a splňovat požadavky spojené se zabezpečením vystavování FIK odpovídající certifikacím pro HSM zařízení a uložení účtenky s FIK do databáze společně s podepsaným XML. Detailní popis procesu je součástí popisu požadovaných procesů.

Zařízení musí splňovat minimálně bezpečnostní certifikaci Common Criteria (EAL4) FIPS 140-2 level 3. Řešení musí splňovat požadavky vysoké dostupnosti a výkonnostní požadavky definované pro EET.

Pro **zabezpečenou oblast** zpracování XML dat v rámci evidence zaslaných účtenek je potřeba zpracovávat masivní datové toky generované vysokým počtem povinných subjektů a jejich pokladních systémů zasílajících XML soubory podepsané příslušným certifikátem. Pro náročnou úlohu ověřování XML a certifikátů je nutné zařízení, které maximálně akceleruje prováděné operace, které je schopno kumulovat několik funkčních požadavků oblasti propustnosti a bezpečnosti. Pro oblast bezpečnosti je nutné zajištění takových podmínek, aby byla zajištěna ochrana vložených **bezpečnostních kódů, nutných pro požadovanou funkcionalitu v rámci vystavování bezpečnostního kódu FIK**. Podmínkou oddělení zmíněných generických úkonů s aplikačními daty z aplikačního serveru na HW zařízení tzv. **SOA appliance, je vysoký výkon při zpracování XML dat a vysoká míra zabezpečení**. **DataPower SOA appliance** koncentruje požadovanou funkcionalitu tak, že zpracování XML je podpořeno HW akcelerátorem a integrovanými bezpečnostními vlastnostmi včetně integrovaného HSM modulu. Požadované užití v prostředí EET je typické případem, kdy zařízení DataPower zajišťuje zejména integrací systémů s externími entitami (B2B/B2G):

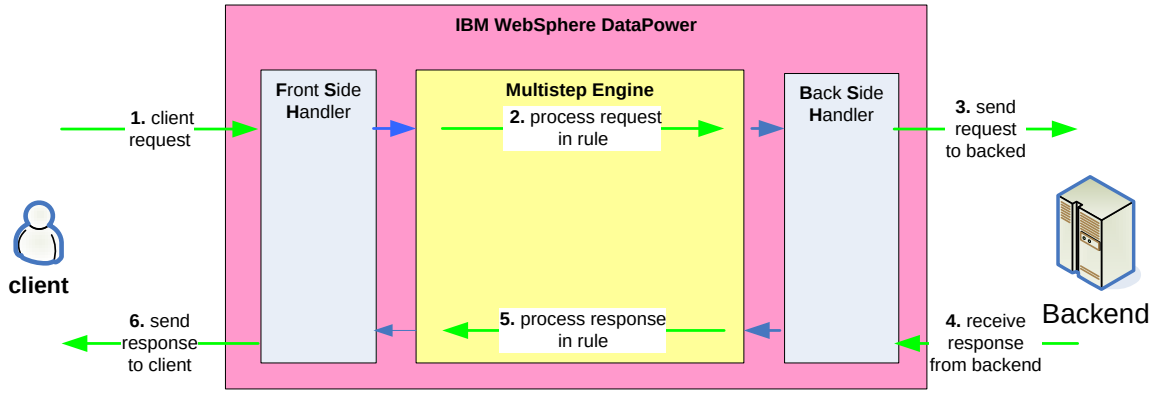
- Při implementaci B2B, B2G a B2C řešení založených na výměně XML zpráv např. s využitím WebServices a protokolem SOAP, DataPower plní významné bezpečnostní funkce v demilitarizované zóně (DMZ)
    - **Autentizace** & **Autorizace** požadavků a případné vytváření **SSO** tokenů pro propagaci identit od proprietárních řešení jako je LTPA až po standard SAML
    - **Validace zpráv** – např. zpráva musí být validní XML, následně validní SOAP, a také obsah (přenášená data) musí být validní podle XML schématu
    - **Digitální podpis** a **validace digitálního** podpisu pro zajištění **nepopiratelnosti zprávy**
    - **Šifrování** a **dešifrování** obsahu zprávy za pomoci integrovaného HSM modulu tak, aby byla uchráněna citlivá data před zneužitím
    - **Ochrana před XML útoky – při tvorbě B2B řešení a obecně je nutno uvažovat, že se často vystavují služby systémů, které nikdy nebyly k podobnému účelu určeny**!
    - Terminace **HTTPs** protokolu
    - Transformace formátu dat pro komunikaci s externí entitou na interní formát a opačně
    - Audit zpráv
- V rámci implementace portálového řešení EET, je žádoucí využít DataPower v demilitarizované zóně k řešení:
    - **Autentizace** & **Autorizace** požadavků a případné vytváření **SSO** tokenů pro propagaci identit od proprietárních řešení jako je LTPA až po standard SAML.
    - **Validace zpráv** – např. zpráva musí obsahovat data validní XML podle definovaného XML schématu.
    - Akcelerace **XSLT** transformací a snížení latencí spojených se zpracováním digitálního podpisu.
    - Ochrana před různými útoky (**XML threats**) – např. SQL injection.
    - **Loadbalancingu** požadavků na backend systémy.
- Implementace portálových a reportovacích řešení postavených na **XSLT**
    - Síla HW akcelerátoru pro XSLT v zařízení DataPower může pomoci ušetřit zdroje aplikačního serveru a snížit latence zpracování požadavků.

IBM WebSphere DataPower je SOA appliance, kterou je možno použít v závislosti na požadavcích zejména jako:

- Enterprise Service Bus (ESB) nebo jako jeho doplněk
- Bezpečnostní zařízení v demilitarizované zóně k ochraně interních systémů

Základni funkcionalita DataPower

IBM WebSphere DataPower je možno si představit jako prostředníka (intermediary) ve zpracování požadavků. Klient (service requester) komunikuje na jedné straně se zařízením DataPower a na druhé straně zařízení DataPower komunikuje s poskytovatelem služby (service provider) na backend systému.



Princip práce zařízení DataPower

Na obrázku je vidět, že zařízení DataPower pracuje na principu Proxy.

Front **S**ide **H**andler (FSH) zajišťuje komunikaci s klientem. DataPower se tak může přizpůsobit protokolu, který klient používá – např. http/https, ftp nebo MQ, WebSphere JMS, Tibco EMS. Komunikaci s backend systémem zajišťuje **B**ack **S**ide **H**andler. Vlastní logika zpracování zprávy je prováděna v tzv. **Multistep Engine**, který leží mezi **F**ront **S**ide **H**andlerem a **B**ack **S**ide **H**andlerem. **Multistep Engine** tak může zpracovat jak příchozí požadavek klienta před jeho propuštěním na backend system tak i odpověď vrácenou backend systémem před odesláním klientovi. Je například možno provést při zpracování požadavku autentizaci a autorizaci a rozhodnout, zda bude požadavek na backend system předán. Podobně při zpracování odpovědi je možno zprávu **digitálně podepsat**.

1) **DataPower: Multistep Engine** zpracuje zprávu požadavku nakonfigurovanou bezpečnostní a integrační logikou:
   a) autentizace a autorizace
   b) validace XML (metriky XML, validace schématu, externí reference…)
   c) kryptografie (digitální podpis a šifrování na úrovni zprávy)
   d) obohacení zprávy na základě volání jiné webové služby (enrichment)
   e) Service Level Management (SLM)
   f) content based routing
   g) transformace obsahu zprávy
   h) záznam požadavku pro účely auditu
2) **DataPower: Multistep Engine** předá výsledek zpracování na **B**ack **S**ide **H**andler (**BSH**).
3) **DataPower: B**ack **S**ide **H**andler (**BSH**) přepošle zpracovanou zprávu na backend systém
   a) Předávají se jen a pouze validní požadavky splňující nastavená pravidla – požadavky nesplňující nastavenou politiku služby se na backend nepropouštějí (firewalling).
4) **Backend:** Zpracování požadavku, vytvoření odpovědi a její zaslání zpět na **B**ack **S**ide **H**andler
5) **DataPower: B**ack **S**ide **H**andler (**BSH**) Akceptování odpovědi backend systému a přijetí dat/zprávy.

6) **DataPower: B**ack **S**ide **H**andler (**BSH**) Předání zprávy odpovědi na **Multistep Engine.**
7) **DataPower: Multistep Engine** zpracuje zprávu odpovědi nakonfigurovanou aplikační logikou (např. digitální podpis, šifrování nebo transformace obsahu). U synchronních operací má k dispozici Mutlistep Engine i data (zprávu) požadavku.
   a) validace XML (metriky XML, validace schématu, externí reference…)
      i) validace odpovědí patří k důležité best practice v bezpečnosti webových služeb
   b) obohacení zprávy na základě volání jiné webové služby (enrichment)
   c) transformace obsahu
   d) kryptografie (digitální podpis a šifrování na úrovni zprávy)
   e) audit
      i) Často se DataPower využívá k auditování vybraných dat ze zprávy požadavku a odpovědi (případně komunikačních metadat jako je identita klienta)
8) **DataPower: Multistep Engine** předá výsledek zpracování zprávy odpovědi na **F**ront **S**ide **H**andler.
9) **DataPower: F**ront **S**ide **H**andler (**FSH**) předá výslednou zprávu odpovědi pomocí komunikačního protokolu (např. SOAP message pomocí protokolu HTTP).
10) **Klient:** Zpracuje data odpovědi od zařízení **DataPower**

Variace vlastností DataPoweru je využita při návrhu B2B rozhraní systému EET pro sběr účtenek.

Podporované protokoly a standardy

1. Transport a konektivita
   - HTTP, HTTPS, WebSocket Proxy
   - FTP, FTPS
   - SFTP
   - WebSphere MQ and WebSphere MQ File Transfer Edition (MQFTE)
   - TIBCO EMS (Integration and B2B appliances)
   - WebSphere Java™ Message Service (JMS)
   - IBM IMS™ Connect, IMS Callout
   - NFS
   - DB2®, Microsoft SQL Server, Oracle, Sybase, and IMS database connectivity
   - IPv4, IPv6
   - Link Aggregation Control Protocol (LACP) IEEE 802.1ax, 802.3ad
   - Virtual LAN (VLAN) IEEE 802.1q
   - 10G Ethernet IEEE 802.3-2008
   - 1G Ethernet IEEE 802.3ab
   - Dynamic Host Configuration Protocol (DHCP)
   - SSH File Transfer Protocol (SFTP) Support

   Podporované protokoly jsou následující:

   - SSH-2 protocol definovaný IETF RFC 4251
   - SFTP verze 3 definovaný podle draft-ietf-secsh-filexfer-02.txt Internet-Draft

2. Enforcement bezpečnostní politiky

   - OAuth 2.0
   - SAML 1.0, 1.1 and 2.0, SAML Token Profile, SAML queries
   - XACML 2.0
   - Kerberos, SPNEGO
   - RADIUS
   - LDAP versions 2 and 3
   - Lightweight Third-Party Authentication (LTPA)
   - Microsoft Active Directory

- Federal Information Processing Standard (FIPS) 140-2 Level 3 (with optional Hardware Security Module)
- FIPS 140-2 Level 1 (with built-in cryptographic software module)
- SAF and IBM RACF® integration with z/OS®
- Internet Content Adaptation Protocol (ICAP)
- W3C XML Encryption
- W3C XML Signature
- S/MIME encryption and digital signature
- WS-MediationPolicy, versions 1.6, 1.7, 1.8, and 1.9
- WS-Security 1.0, 1.1
- WS-I Basic Security Profile 1.0, 1.1
- WS-SecurityPolicy
- WS-SecureConversation 1.3

3. Webové služby

- WS-I Basic Profile 1.0, 1.1
- WS-I Simple SOAP Basic Profile
- WS-Policy Framework
- WS-Policy Attachments: Message Content Filters 1.3 (IBM standard)
- WS-Policy 1.2, 1.5
- WS-Trust 1.3
- WS-Addressing
- WS-Enumeration
- WS-Eventing
- WS-Notification
- Web Services Distributed Management (WSDM)
- WS-Management
- WS-I Attachments Profile
- SOAP Attachment Feature 1.2
- SOAP with Attachments (SwA)
- Direct Internet Message Encapsulation (DIME)
- Multipurpose Internet Mail Extensions (MIME)
- XML-binary Optimized Packaging (XOP)
- Message Transmission Optimization Mechanism (MTOM)
- Universal Description, Discovery, and Integration (UDDI versions 2 and 3), UDDI version 3 subscription
- WebSphere Service Registry and Repository (WSRR)

4. Transport Layer Security (SSL and TLS)

- SSL version 2 (deprecated)
- SSL version 3
- TLS versions 1.0, 1.1, and 1.2 (hardware accelerated on physical appliances)

5. Public key infrastructure (PKI)

- RSA, 3DES, DES, AES, SHA, X.509, CRLs, OCSP
- PKCS#1, PKCS#5, PKCS#7, PKCS#8, PKCS#10, PKCS#12
- XKMS for integration with Tivoli® Security Policy Manager

6. Management

- Simple Network Management Protocol (SNMP)
- SYSLOG

- Secure Shell (SSH)
- Intelligent Platform Management Interface (IPMI)

Realizace webových a aplikačních serverů je doporučeno řešit na virtualizované platformě x86 se zajištěním požadavku vysoké dostupnosti. Žádný server nebude mít lokální diskový systém a musí být napojen do SAN/NAS via FC za pomocí běžně používaných protokolů.

Navržené řešení musí umožňovat horizontální škálovatelnost.

Databázové servery a úložiště

Databázové servery musí splňovat požadavky vysoké dostupnosti včetně diskového úložiště umožňujícího „tierování" jednotlivých diskových prostor v automatickém režimu. Databázové prostředí musí umožňovat ukládání velkého objemu dat jak co do počtu ukládaných záznamů tak co do velikosti uložených dat. Databázové nebo storage funkcionalita musí umožnit online replikaci dat do druhého úložiště.

Požadavky na minimální konfiguraci

		Platforma	Minimální počet jader fyzického serveru	Minimální paměť fyzického serveru	Minimální celkový počet jader virtuálního prostředí	Minimální velikost paměti virtuálního prostředí	
Webové a aplikační servery	Varianta 1	x86	16	64 GB	80	320 GB	
	Varianta 2	RISC	20	256GB	60	768 GB	
Databázové servery	Varianta 1	x86	72				Exadata
	Varianta 2	RISC	24	1TB	48	2TB	IBM
Virtualizovaná platforma (CPS)	Varianta 3	X86	-	-	270	552GB	MS

Minimální konfigurace aplikačních a databázových serverů je počítána bez výkonových nároků virtualizačních řešení.

Minimální kapacita Storage je požadována na 4-leté období provozu systému včetně diskových prostorů přiřazení pro jednotlivé virtualní stroje a virtualizační platformu s kapacitou 144 TB s možností rozšíření celkové kapacity na deseti násobek. Pro potřeby zajištění vysoké propustnosti je požadovaná minimální kapacita 2 TB na SSD. Požadované kapacity jsou netto kapacity dostupné pro systémy. Raw kapacita je závislá na konkrétním řešení diskových systémů.

SAN switching

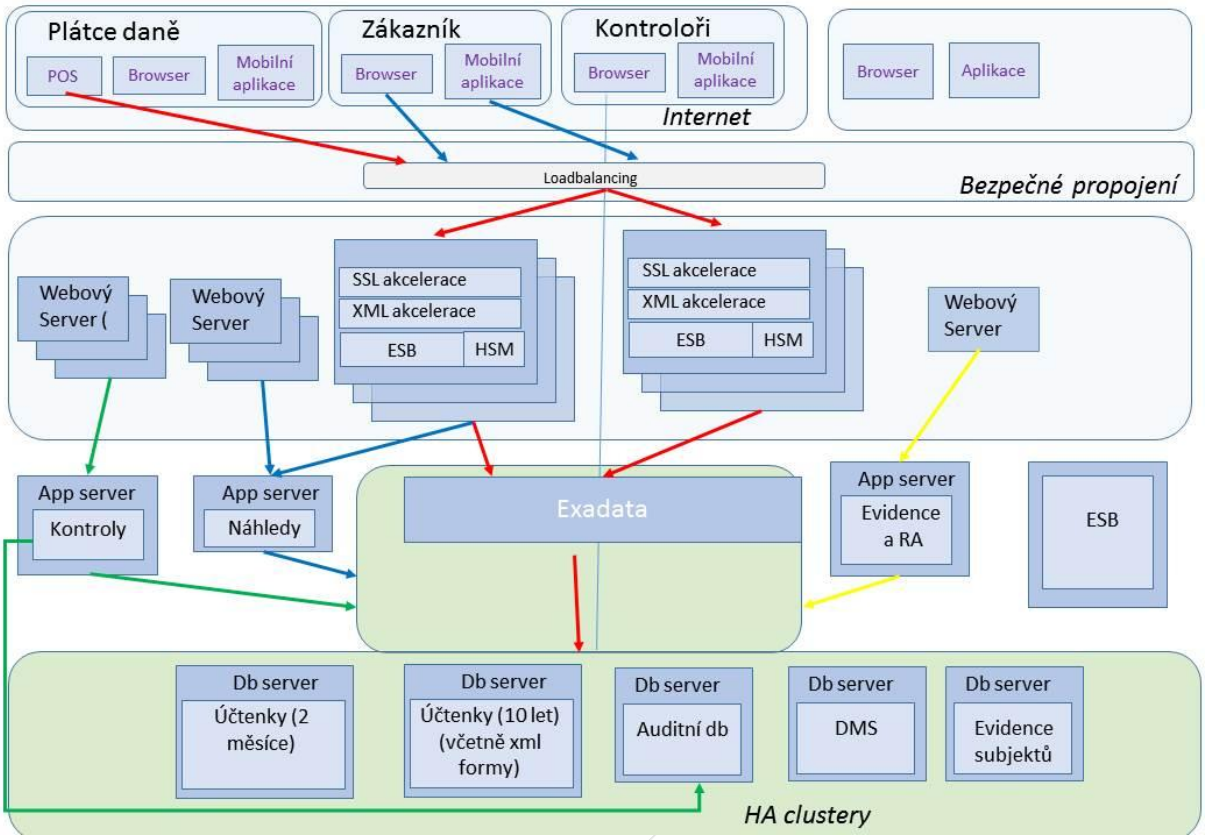
V rámci dodávky je požadováno dodání 4x SAN switch 48 port 8/16Gb.

Zapojení SAN switchů bude zajišťovat SAN FC redundantní infrastrukturu a to v každém ze dvou datových sálů datového centra SPCSS. To Znamená, že každý sever bude mít vždy dvě FC spojení na datové úložiště.

Kabeláž

Požadavky na kabeláž musí být definovány v první fázi realizace projetu.

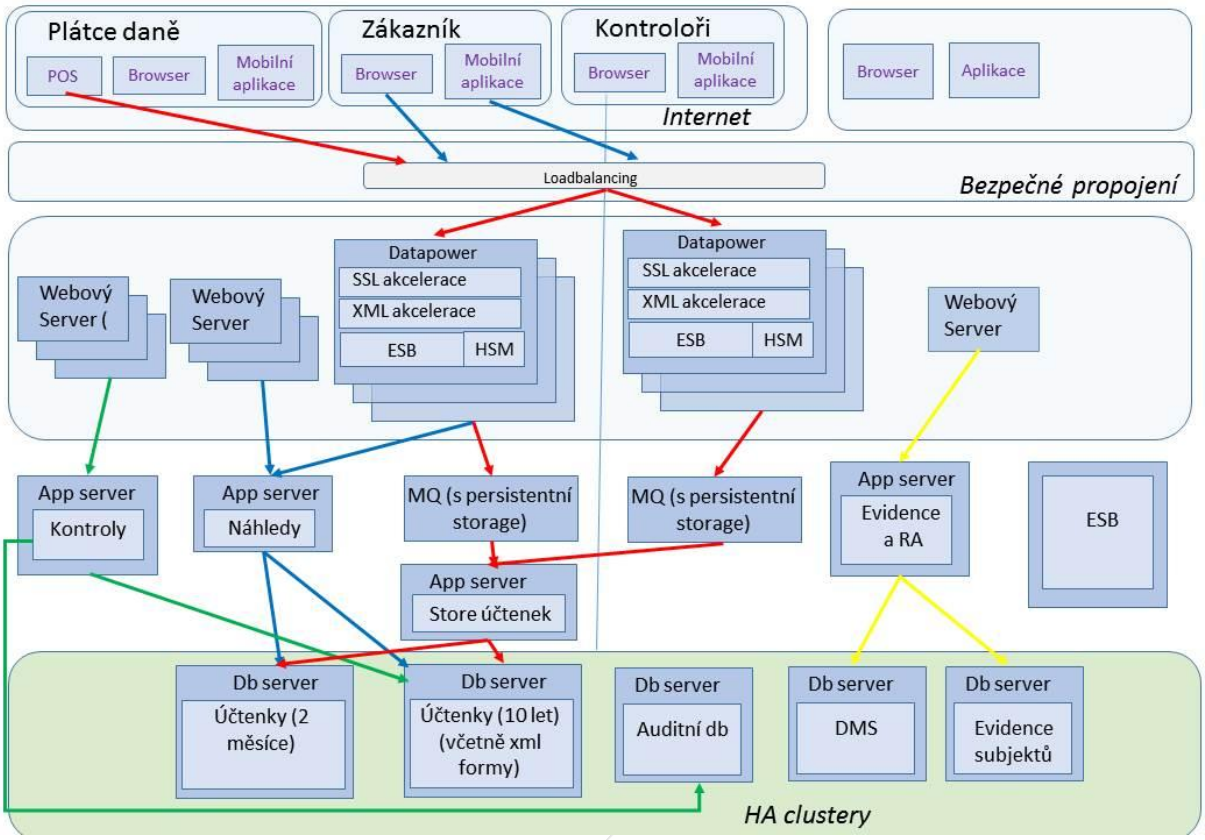
Varianta 1 aplikační vrstvy a Varianta 1 databázové vrstvy



Obrázek 26: Schéma aplikační a databázové vrstvy Varianty 1

Varianta 1 je postavena na platformě x86 a na konsolidovaném produktu ExaData, který realizuje kompaktní databázové prostředí. Aplikační a databázová oblast je řešena jako samostatné celky, kde aplikační oblast je plně virtualizována umožňuje dynamicky alokovat potřebný výkon určeným aplikačním virtuálním serverům. Databázové prostředí ExaData s databází Oracle umožňuje pracovat konfigurovat potřebná databázová prostředí dle aktuálních požadavků aplikace.

Vizualizace možného řešení pro Variantu 2 aplikační vrstvy a Varianty 2 databázové vrstvy kombinace



Obrázek 27:Schéma aplikační a databázové vrstvy Varianty 2

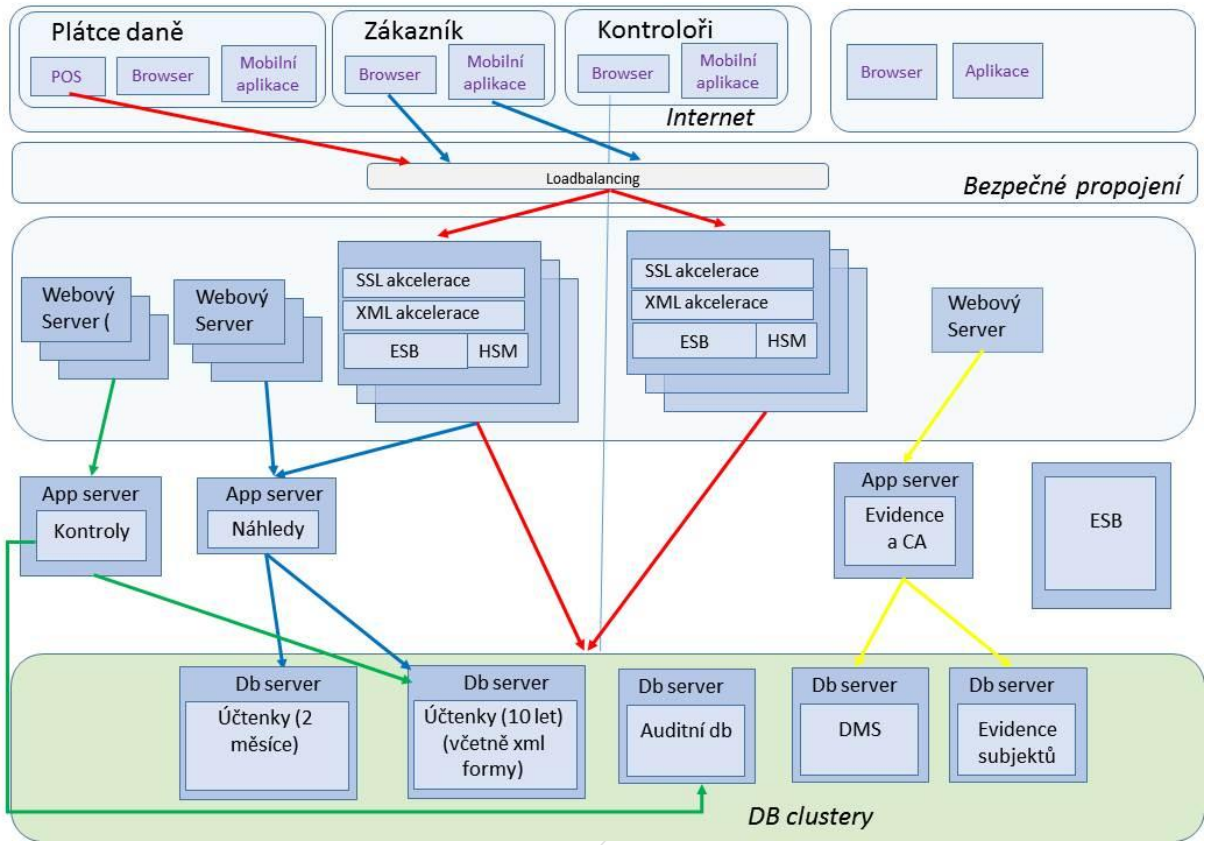
Varianta 2 řeší realizaci na procesorové platformě RISC a produktech IBM. Varianta konsoliduje potřebný výpočetní výkon do jednotného virtualizačního prostředí a umožňuje dynamicky alokovaný výkon do příslušných částí systému dle aktuálních požadavků. Databázové prostředí je řešeno na platformě databázových serverů Informix nebo DB2.

Hlavní částí řešení pro B2B rozhraní jsou XML akcelerátory s integrovanými moduly HSM pro zajištění požadované propustnosti pro evidenci účtenek a vystavování bezpečnostního kódu FIK.

Varianta 3 - Virtualizovaná Platforma (CPS)

1. **Konvergovaný systém** – úplné HW&SW řešení dodávané na klíč, škálovatelné dle požadavků projektu EET
2. V současné době se jedná o řešení Microsoft a DELL, připravuje se v2: MS a HP
3. Řešení vychází ze zkušeností při návrhu, realizaci a provozu datových center
4. Podpora je zajištěna prostřednictvím služeb Premier Support, případné požadavky na integraci CPS do prostředí zákazníka zajišťují Microsoft Services
5. Řešení je postaveno na normalizovaném HW Dell s garantovanou kompatibilitou všech HW a SW komponent řešení
6. Řízené aktualizace: SW opravy a aktualizace všech komponent jsou nejprve testovány na totožné HW konfiguraci v laboratořích MS a následně jsou uvolněny pro nasazení na prostředky
7. Doporučovaný životní cyklus je v závislosti na způsobu nasazení odhadován na 3 - 5let
8. Řešení využívá technologii Microsoft.
9. CPS nabízí služby: IaaS, PaaS a DBaaS

CPS Stamp:



Škálovatelnost (stručně)

Řešení je flexibilní dle výkonových požadavků zákazníka. CPS je dodáváno v jednotkách, tzv. Stamp Stamp znamená rovněž jednu management doménu provozované CPS instance.

Škálovatelnost Stamp:

- V rámci Stamp je možné zajistit efektivní škálování a rozšiřitelnost o sdílený výpočetní výkon, diskové úložiště.

Zálohování

Pro potřeby provozních záloh je požadováno zajištění zálohování na média s minimalizací dopadů na zdrojové systémy, které by mohli mít dopad na celkové zpomalení odezvy primárního systému. Systém a zvolený způsob zálohování musí splňovat požadavky na recovery time plynoucí z parametru RTO a RPO definovaným pro jednotlivé části informačního systému. Zařízení musí splňovat parametry pro možnost obnovitelnosti dat po celou dobu životního cyklů použitých zálohovacích médií.

Pro všechny HW a SW prostředky je požadována tříletá maintenance (HWMA 3y 24x7 Response time 4h).

Předběžný rozpočet systému EET a infrastruktury

V rámci **Varianty 1** jsou použity produkty Oracle a to jak HW tak SW. Prostředí je řešené na platformě x86 a řešení ExaData. Replika (online) dat je provedena na samostatný storage v druhém datovém sále.

Varianta 1	počet	SW/HW	cena	funkce	poznámka
			218 850 615,96 Kč		
Oracle Database Enterprise Edition	1	SW	23 573 523,85 Kč	DB	
Paritioning	1	SW	5 707 274,19 Kč	DB	
Real Application Clusters	1	SW	11 414 548,39 Kč	DB	
Multitenant	1	SW	8 684 982,47 Kč	DB	
Tuning Pack	1	SW	2 481 423,56 Kč	DB	
Diagnostics Pack	1	SW	3 722 135,34 Kč	DB	
Exadata Storage Server Software	1	SW	4 962 847,13 Kč	DB	
WebLogic + service bus	1	SW	21 216 399,20 Kč	sběrnice služeb	
storage pro replikaci	1	HW	2 000 000,00 Kč		
Exadata 5-2 Quarter rack	1	HW	7 649 056,80 Kč	DB	
X5-2 server	1	HW	115 894,80 Kč	správa	
DataPower Gateway Appliance	4	HW	16 495 498,67 Kč	XML akcelerace, ESB, FIK,	
x3550 16 way 64 GB	4	HW	1 096 024,20 Kč	Aplikační servery	
x3550 16 way 64 GB	4	HW	1 096 024,20 Kč	Middleware servery	
CA s HSM	3	HW	2 426 891,78 Kč	Certifikační autorita	
Switch 48 port	2	HW	1 146 398,16 Kč	SAN Infrastruktura	
Diskove pole	2	HW	2 312 177,42 Kč	Diskove pole	
TS3500	1	HW	4 730 187,80 Kč	Pásková jednotka	
TSM	1	SW	1 759 664,00 Kč	Zálohování	
Implementace	1		20 000 000,00 Kč	cena implementace	
DDOS	2	Network	4 000 000,00 Kč	síťové prvky	
UTM	2	Network	6 000 000,00 Kč	síťové prvky	
Switch	2	Network	2 000 000,00 Kč	síťové prvky	
Switch OOB	2	Network	2 000 000,00 Kč	síťové prvky	
IPS/IDS	2	Network	3 000 000,00 Kč	síťové prvky	
Loadbalancing	2	Network	4 000 000,00 Kč	síťové prvky	
WAF	4	Network	2 000 000,00 Kč	síťové prvky	
SIEM	1	Network	2 000 000,00 Kč	síťové prvky	
Implementace	200 MD		2 500 000,00 Kč	implementace sít prvků	
EET			32 000 000,00 Kč	vývoj a implementace SW	
Tomcat		SW	- Kč	Aplikační servery	
TSM		SW	1 759 664,00 Kč	Zálohování	
bezpecnost			15 000 000,00 Kč		

Varianta 2 vychází z předpokladu existence smlouvy ISLO s IBM..

Varianta 2	počet	SW/HW	cena	funkce	poznámka
			212 839 106,85 Kč		
S822 20c 256GB RAM	3	HW	3 277 085,36 Kč	Aplikační servery	
S824 24c 1TB RAM	2	HW	6 848 058,72 Kč	DB servery	
CA s HSM	2	HW	2 426 891,78 Kč	Certifikační autorita	
Storvize v7000	2	HW	9 248 709,68 Kč	Diskové pole	
TS3500	1	HW	4 730 187,80 Kč	Pásková knihovna	
Switch 48 port	2	HW	1 146 398,16 Kč	SAN Infrastruktura	
DataPower Gateway Appliance	4	HW	22 828 832,00 Kč	XML akcelerace, ESB, FIK,	ISLO
TSM		SW	1 759 664,00 Kč	Zálohování	ISLO
Informix nebo DB2		SW	35 152 038,40 Kč	Databázový systém	ISLO
Tomcat		SW	- Kč	Aplikační servery	ISLO
WebSphere MQ		SW	6 321 120,00 Kč	Message Queue	ISLO
Integration Bus		SW	24 600 120,95 Kč	ESB	ISLO
Implementace	1		20 000 000,00 Kč	cena implementace	
DDOS	2	Network	4 000 000,00 Kč	síťové prvky	
UTM	2	Network	6 000 000,00 Kč	síťové prvky	
Switch	2	Network	2 000 000,00 Kč	síťové prvky	
Switch OOB	2	Network	2 000 000,00 Kč	síťové prvky	
IPS/IDS	2	Network	3 000 000,00 Kč	síťové prvky	
Loadbalancing	2	Network	4 000 000,00 Kč	síťové prvky	
WAF	4	Network	2 000 000,00 Kč	síťové prvky	
SIEM	1	Network	2 000 000,00 Kč	síťové prvky	
Implementace	200 MD		2 500 000,00 Kč	implementace sít prvků	
Bezpečnostní projekt			15 000 000,00 Kč	Komplexní bezpečnostní dokumentace, bezpečnostní testy	
EET		SW	32 000 000,00 Kč	vývoj a implementace SW	

Varianta 3 je založena na virtualizované platformě CPS. Platforma je dodávána jako kompletní připravené řešení společností Microsoft včetně HW a SW prostředků. Virtualizované prostředí je schopné realizovat prostředí pro OS Microsoft a Linux.

Varianta 3	počet	SW/HW	cena	funkce	poznámka
			202 245 575,58 Kč		
CPS - APP,DB	2	HW	57 800 000,00 Kč	Aplikační a databázové servery	
TS3500	1	HW	4 730 187,80 Kč	Pásková knihovna - zálohování	
DataPower Gateway Appliance	4	HW	22 828 832,00 Kč	XML akcelerace, ESB, FIK,	
TSM		SW	1 759 664,00 Kč	Zálohování	
SQL server		SW	23 500 000,00 Kč	Databázový systém	

Integration Bus		SW	4 700 000,00 Kč	ESB	
CA s HSM	3	HW	2 426 891,78 Kč	Certifikační autorita	
Implementace	1		10 000 000,00 Kč	cena implementace	
DDOS	2	Network	4 000 000,00 Kč	síťové prvky	
UTM	2	Network	6 000 000,00 Kč	síťové prvky	
Switch	2	Network	2 000 000,00 Kč	síťové prvky	
Switch OOB	2	Network	2 000 000,00 Kč	síťové prvky	
IPS/IDS	2	Network	3 000 000,00 Kč	síťové prvky	
Loadbalancing	2	Network	4 000 000,00 Kč	síťové prvky	
WAF	4	Network	2 000 000,00 Kč	síťové prvky	
SIEM	1	Network	2 000 000,00 Kč	síťové prvky	
Implementace	200 MD		2 500 000,00 Kč	implementace sít prvků	
Bezpečnostní projekt			15 000 000,00 Kč	Komplexní bezpečnostní dokumentace, bezpečnostní testy	
EET		SW	32 000 000,00 Kč	vývoj a implementace SW	

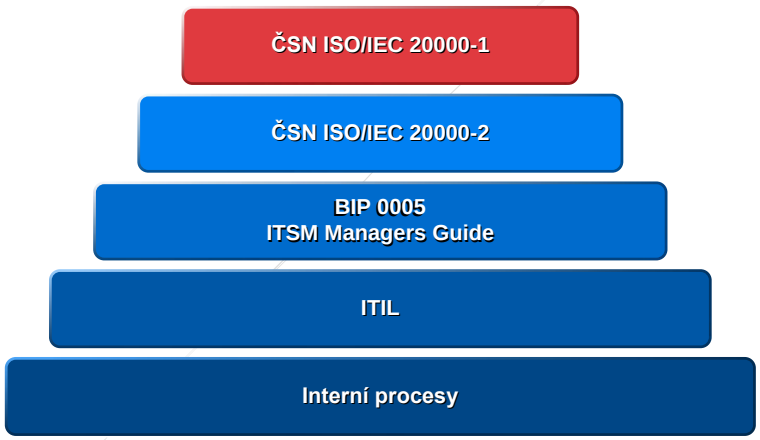
Řešení procesu správy a provozu služeb

Řešení procesů provozu a správy služeb systém EET bude řešeno v souladu s normou ISO/IEC 20000. Důraz bude kladen na procesy životního cyklu jednotlivých služeb poskytovaných koncovým uživatelům a na procesy dohledu, monitorování, podpory uživatelů a řešení incidentů.

Bude provedeno stanovení rozsahu a cílů řešení, provedena analýza rizik služeb (bude zajištěna úzká koordinace a propojení s analýzou rizik v rámci řešení bezpečnosti), příprava politiky IT služeb, katalogu služeb, plánu managementu služeb, provozních politik, návrhu SLA, provozních plánů, plánu a politiky zlepšování služeb a plánu školení a vzdělávání.

Procesy správy a provozu služeb

Zajištění shody s požadavky průmyslové normy ISO/IEC 2000 (respektive doporučení normy ISO/IEC 2000-2) je nezávislé na organizační struktuře. Poskytovatel služby musí použít strukturu, která je nejvhodnější pro efektivní službu. V návaznosti na to, nabízené řešení procesu správy a provozu služeb vhodně kombinuje ISO/IEC 20000 obsahujícím povinnosti a ITIL (aktuálně ve verzi 3), který zahrnuje nejlepší doporučení (best practices) správy služeb IT, která mohou být přizpůsobena potřebám organizací rozdílných velikostí a která jsou zaměřena na služby a na neustálé měření a zlepšování kvality dodávaných služeb IT a to jak z pohledu poskytovatele tak zákazníka.



Obrázek 28: Pojetí řešení procesu správy a provozu služeb

Řešení procesu správy a provozu služeb ve výše uvedeném pojetí bude tedy zaměřeno na následující (dále stručně vymezené) procesy:

Strategie služeb (Service Strategy)	• Správa financí (Financial Management) • Správa portfolia služeb (Service Portfolio Management) • Správa požadavků (Demand Management)
Návrh služeb (Service Design)	• Správa katalogu služeb (Service Catalogue Management) • Správa úrovně služeb (Service Level Management) • Správa kapacit (Capacity Management) • Správa dostupnosti (Availability Management) • Správa kontinuity služeb IT (IT Service Continuity Management) • Správa bezpečnosti informací (Information Security Management) • Správa dodavatelů (Supplier Management)

Přechod služeb (Service Transition)	• Správa změn (Change Management) • Správa aktiv a konfigurace (Service Asset and Configuration Management) • Správa znalostí (Knowledge Management) • Plánování a podpora přechodu (Transition Planning and Support) • Správa releasů a nasazení (Release and Deployment Management) • Ověření a testování služby (Service Validation and Testing) • Vyhodnocení (Evaluation)
Provoz služeb (Service Operation)	• Správa událostí (Event Management) • Správa incidentů (Incident Management) • Provádění požadavků (Request Fulfilment) • Správa přístupů (Access Management) • Správa problémů (Problem Management)
Neustálé zlepšování služby (Continual Service Improvement)	• Zlepšovací proces v 7 krocích • Měření služby (Service Measurement) • Vykazování služby (Service Reporting)

Řešení bezpečnosti systému EET

Řešení bezpečnosti Systému EET musí vycházet z předpokladu, že vzhledem k významu Systému EET bude tento zařazen mezi významné informační systémy dle písmena d) §2 dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dále je předpoklad, že některá dokumentace Systému EET, obsahující popisy mechanismů zajišťujících bezpečnost celého systému může být klasifikovaná jako utajovaná informace až do stupně „Důvěrné“ dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Pro Systém EET je tedy požadováno zavedení systému řízení bezpečnosti informací.

Řešení bezpečnosti Systému EET bude zahrnovat posouzení vstupních podmínek a bezpečnostních požadavků a řešení bezpečnostních požadavků v souladu s normou ISO/IEC 27001 a požadavky zákona. Při řešení bezpečnosti Systému EET musí Poskytovatel sledovat tři základní cíle:

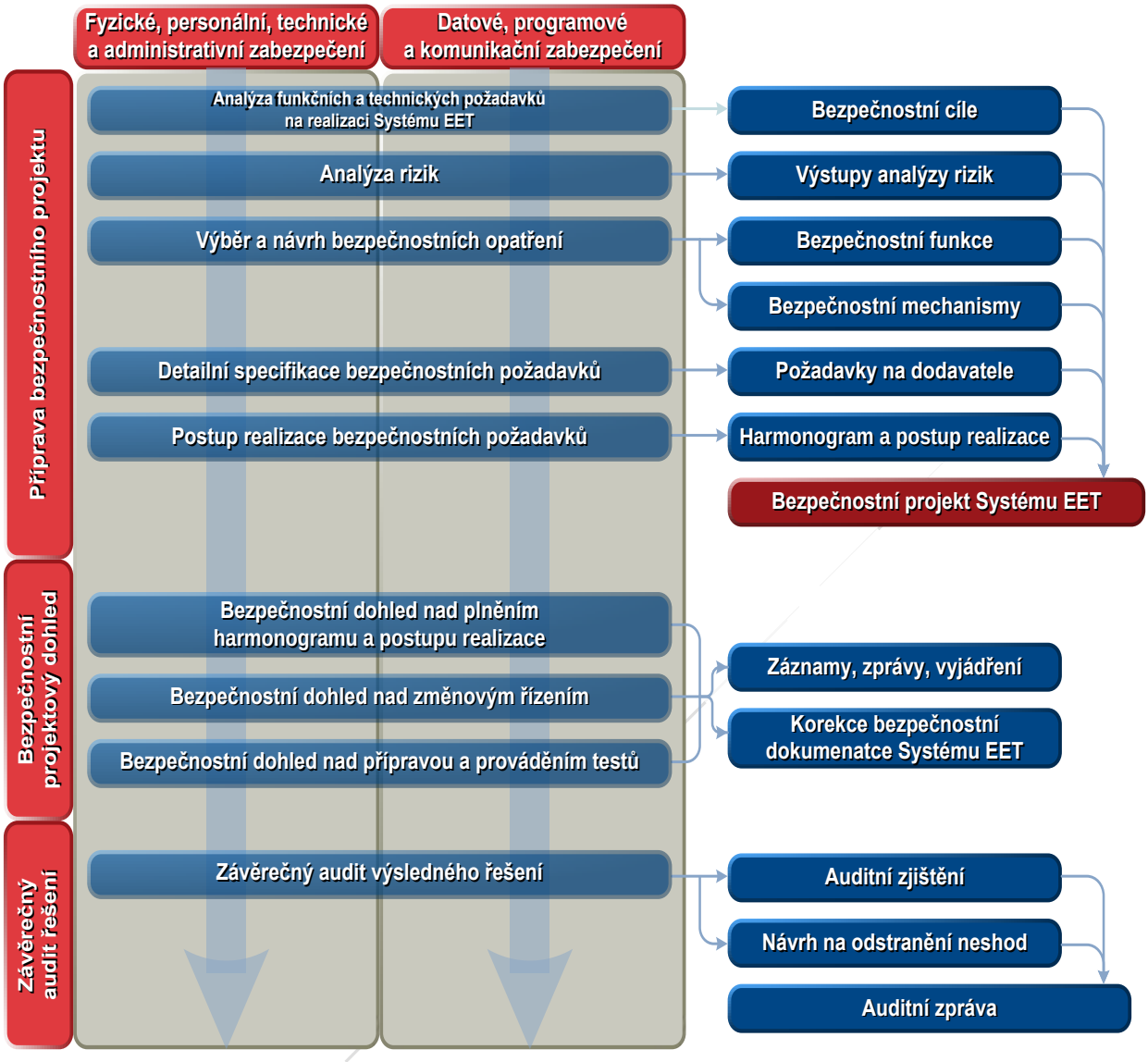
1. Zajistit zapracování bezpečnostních požadavků na Systém EET od návrhu až po implementaci celého systému bezpečnosti.
2. Vytvořit funkční systém řízení bezpečnosti informací Systému EET tak, aby bylo možné tento systém bezpečně provozovat.
3. Navrhnout a zavést systém řízení bezpečnosti a návrh bezpečnostních funkcí tak, aby byl v souladu s požadavky:
    - normy ČSN ISO/IEC 27001:2014,
    - zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a navazujících vyhlášek NBÚ (dále také „zákon č. 181/2014 Sb., a vyhlášky NBÚ“),
    - zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (pro některé části dokumentace),
    - požadavky kladenými na systémy veřejné správy a požadavky dalších relevantních právních norem.

Na základě výše uvedených cílů a požadavků zadávací dokumentace je požadováno, aby Poskytovatel řešení bezpečnosti Systému EET realizoval zavedení bezpečnosti Systému EET ve 3 po sobě jdoucích etapách následovně:

- **Etapa 1** – Analýza a návrh bezpečnosti Systému EET
- **Etapa 2** – Implementace bezpečnosti Systému EET
- **Etapa 3** – Monitorování a přezkoumání bezpečnosti Systému EET

Systém řízení bezpečnosti Systému EET musí být Poskytovatelem navržen a implementován tak, aby ho bylo možné, v případě potřeby, certifikovat podle normy ČSN ISO/IEC 27001:2014.

Bezpečnostní funkce budou navrženy ve formě Typizovaných bezpečnostních profilů s využitím ISO 15408.



Obrázek 29: Schéma bezpečnostních činností a související dokumentace

Při realizaci řešení bezpečnosti Systému EET bude se vycházet a řídit ustanoveními standardu ČSN ISO/IEC 27001:2014 s tím, že bude dále akcentovat další relevantní zákony, normy a standardy, zejména potom:

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- zákon č. 101/2000 Sb., o ochraně osobních údajů v platném znění
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
- zákon č. 227/2000 Sb., o elektronickém podpisu v platném znění
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy v platném znění
- zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

Dále je požadováno realizovat řešení bezpečnosti EET v následujících krocích:

- **Příprava bezpečnostního projektu Systému EET** zahrnujícího analýzu bezpečnostních aspektů projektu včetně stanovení bezpečnostních cílů a analýzy rizik, návrh efektivních bezpečnostních opatření s následnou specifikací bezpečnostních funkcí a návrh jejich realizace ve formě bezpečnostních mechanismů na úrovni jednotlivých komponent Systému EET.
- **Bezpečnostní projektový dohled Systému EET** zahrnující dohled nad realizací a prosazováním bezpečnostních funkcí a bezpečnostních mechanismů v souladu s obsahem bezpečnostního projektu Systému EET.
- **Závěrečný bezpečnostní audit řešení Systému EET** za účelem ověření funkčnosti bezpečnostních funkcí a bezpečnostních mechanismů včetně jejich prosazení do relevantních interních procesů Systému EET.
- **Řízení a údržba bezpečnosti při provozu Systému EET**, která bude zahrnovat zejména udržení souladu stavu bezpečnost s bezpečnostními požadavky prostředí a udržení souladu stavu bezpečnosti s bezpečnostními potřebami Systému EET v souvislosti s jeho změnami prováděnými v rámci jeho implementace a provozu.

Jednotlivé složky, jejich návaznosti a postup realizace řešení bezpečnosti Systému EET jsou znázorněny na schématu uvedeném na následující straně.

Řešení bezpečnosti Systému EET musí být zajištěno v koordinaci s návrhem a implementací celého systému tak, aby bylo zajištěno okamžité zapracování bezpečnostních požadavků do implementovaného systému.

Vzhledem k tomu, že některá dokumentace systému EET, zejména část obsahující popisy mechanismů zajišťujících bezpečnost celého systému, může být klasifikována jako utajovaná informace až do stupně „Důvěrné“ dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, jsou na Poskytovatele kladeny tyto požadavky:

- Poskytovatel musí být držitelem Osvědčení podnikatele pro přístup k utajované informaci, která u něho vzniká nebo je mu poskytnuta, nejméně pro stupeň „Důvěrné“.
- Zaměstnanci Poskytovatele, zpracovávající části dokumentace, obsahující popisy mechanismů zajišťujících bezpečnost celého systému, musí být držiteli Osvědčení fyzické osoby pro přístup k utajované informaci nejméně pro stupeň „Důvěrné“.
- Poskytovatel musí disponovat prostředky fyzické a administrativní bezpečnosti a bezpečnosti informačních systémů pro zpracování dokumentace v režimu utajované informace do stupně „Důvěrné“ dle zákona č. 412/2005 Sb., a prováděcích vyhlášek.

Dále následuje rozklad činností a obsah výstupů realizovaných v jednotlivých etapách řešení bezpečnosti.

Etapa 1 – Analýza a návrh bezpečnosti systému EET

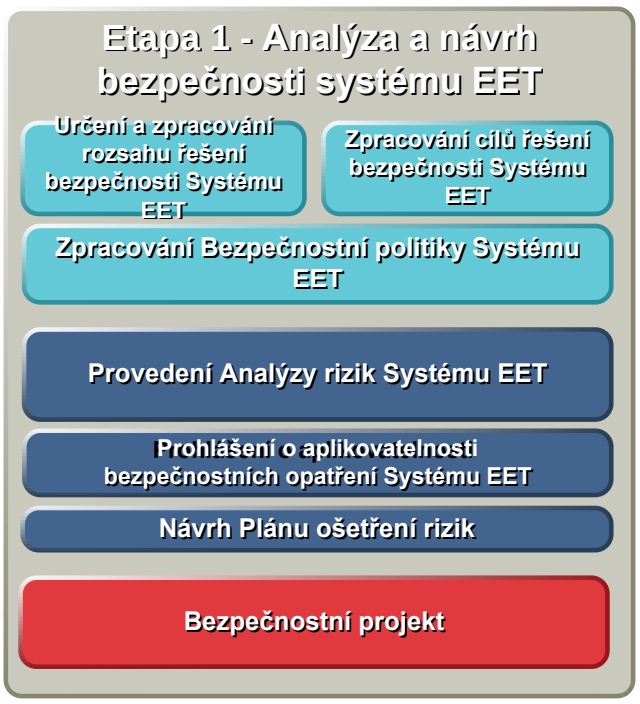
Analýza a návrh bezpečnosti systému EET bude mít za cíl identifikovat požadavky na bezpečnost systému EET a navrhnout bezpečnostní řešení Systému EET počínaje návrhem celého systému a konče jeho předáním do provozu.

V rámci této etapy bude provedeno stanovení rozsahu a cílů řešení bezpečnosti, analýza rizik, zpracování bezpečnostní politiky Systému EET včetně bezpečnostní strategie, připravení Prohlášení o aplikovatelnosti a Plánu ošetření rizik Systému EET. V závěru etapy bude zpracován bezpečnostní projekt Systému EET.

Etapa 1 musí obsahovat následující fáze:

1. Určení základních parametrů řešení bezpečnosti Systému EET
2. Hodnocení a řízení rizik Systému EET
3. Zpracování Bezpečnostního projektu Systému EET

Grafické znázornění činností požadovaných realizovat v této etapě je uveden na následujícím obrázku.



Obrázek 30: Schéma etapy 1 řešení bezpečnosti Systému EET

Fáze 1.1 – Určení základních parametrů řešení bezpečnosti systému EET

V první fázi řešení bezpečnosti Systému EET bude provedeno upřesnění rozsahu řešení bezpečnosti Systému EET, návrh cílů řešení bezpečnosti a následně zpracuje Bezpečnostní politiku informací systému EET.

V této fázi se provedou úkony důležité pro realizaci řešení bezpečnosti Systému EET:

- Analýzu funkčních a legislativních bezpečnostních požadavků na Systém EET a prostředí, v němž bude provozován.
- Definování rozsahu řešení bezpečnosti systému EET, který bude obsahovat interní a externí aspekt dle ČSN ISO/IEC 27001:2014.

Popis požadovaných základních výstupů:

1. ***Rozsah řešení bezpečnosti Systému EET*** – ***upřesní*** rozsah řešení bezpečnosti Systému EET z hlediska zapojených organizačních složek, vybraných prostor, definovaných aktiv a technologií. Rozsah bude mít následující strukturu:
    a. organizační struktura ve vztahu k řešení bezpečnosti Systému EET
    b. umístění organizačních útvarů a zařízení pokrývaných v rámci k řešení bezpečnosti Systému EET
    c. základní aktiva a technologie pokrývaní v rámci k řešení bezpečnosti Systému EET
    d. rozhraní řešení bezpečnosti Systému EET
    e. závislosti k řešení bezpečnosti Systému EET.
2. ***Cíle řešení bezpečnosti Systému EET*** – budou obsahovat stručný výčet cílů, kterých má být dosaženo řešením bezpečnosti v určeném rozsahu řešení bezpečnosti Systému EET. Cíle budou konkrétně stanoveny na období implementace s výhledem na zajištění provozu systému EET.
3. ***Bezpečnostní politiku informací systému EET*** je požadováno zpracovat ve formě koncepčního dokumentu shrnujícího strategii a zásady bezpečnosti systému EET ve všech oblastech bezpečnosti informací s důrazem na uvedení odpovědností za oblast bezpečnosti a popis zaváděných bezpečnostních zásad v rámci jednotlivých oblastí bezpečnosti. Pro Bezpečnostní politiku systému EET je požadována následující struktura:
    a. Strategie bezpečnosti Systému EET
    b. popis systému EET
    c. funkční bloky systému EET
    d. bezpečnost prostředí systému EET
    e. regulatorní, právní a smluvní požadavky na řešení bezpečnosti Systému EET
    f. kritéria hodnocení rizik
    g. zásady bezpečnosti informací v Systému EET:
        - organizace bezpečnosti informací
        - bezpečnost lidských zdrojů
        - řízení aktiv
        - řízení přístupu
        - kryptografie
        - fyzická bezpečnost a bezpečnost prostředí
        - bezpečnost provozu
        - bezpečnost komunikací
        - dodavatelské vztahy
        - řízení incidentů bezpečnosti informací
        - kontinuita bezpečnosti informací
        - soulad s požadavky
    h. způsob řízení bezpečnostní dokumentace Systému EET
    i. způsob vyčleňování a řízení zdrojů pro zajištění bezpečnosti Systému EET
    j. způsob monitorování a měření efektivity řešení bezpečnosti Systému EET.

Fáze 1.2 – Hodnocení a řízení rizik systému EET

Cílem hodnocení a řízení rizik bude identifikovat aktiva Systému EET, a zjistit úroveň rizik možného uplatnění hrozeb, které na aktiva mohou působit.

V počátku fáze bude navržena metodika hodnocení a řízení rizik Systému EET. V návaznosti na vybranou metodiku identifikuje aktiva, která budou zahrnuta do rozsahu řešení bezpečnosti Systému EET, spolu s určením jejich bezpečnostních parametrů (důvěrnost, integrita, dostupnost). Dále budou identifikovány a hodnoceny hrozby a zranitelnosti působící na aktiva Systému EET a následně navržena opatření k pokrytí rizik. Zdůvodnění výběru opatření bude provedeno v dokumentu Prohlášení o aplikovatelnosti bezpečnostních opatření Systému EET. Způsob řízení rizik bude následně popsán v Plánu ošetření rizik Systému EET.

V závěru analýzy rizik bude zajištěno provedení zvládání a řízení rizik prostřednictvím návrhu přiměřených bezpečnostních protiopatření pokrývajících zjištěná rizika. Pro naplnění bezpečnostních cílů a snížení bezpečnostních rizik bude vybrána vyvážená kombinace technických a netechnických bezpečnostních opatření pro Systému EET.

V této fázi budou provedeny úkony, vyžadované normou ČSN ISO/IEC 27001:2014:

- stanovení kritérií rizik bezpečnosti informací, která zahrnují:
  - kritéria akceptace rizik
  - kritéria pro provádění posouzení rizik bezpečnosti informací
- identifikace rizika bezpečnosti informací:
  - používá proces posuzování rizik bezpečnosti informací k identifikaci rizik spojených se ztrátou důvěrnosti, integrity a dostupnosti informací v rozsahu systému řízení bezpečnosti informací
  - identifikuje vlastníky rizik
- analýza rizika bezpečnosti informací:
  - posuzuje potenciální následky, které by nastaly, pokud by se realizovala identifikovaná rizika
  - posuzuje reálnou pravděpodobnost výskytu rizik
  - určuje úroveň rizik
- hodnocení rizika bezpečnosti informací:
  - porovnává výsledky analýzy rizik s kritérii rizik
  - stanovuje priority analyzovaných rizik pro ošetření rizika
- Definování procesu ošetření rizik bezpečnosti informací pro:
  - výběr vhodných variant pro ošetření rizika bezpečnosti informací s ohledem na výsledky posuzování rizik
  - určení všech opatření nezbytných k implementaci vybrané varianty (variant) pro ošetření rizika bezpečnosti informací
  - verifikace opatření určených výše s cílem ověřit, že žádné nezbytné opatření nabylo vynecháno
  - vytvoření Prohlášení o aplikovatelnosti, které obsahuje nezbytná opatření a zdůvodnění pro jejich zahrnutí, ať už jsou nebo nejsou implementována
  - formulace Plánu ošetření rizik bezpečnosti informací
  - získání souhlasu vlastníků rizik ohledně plánu ošetření rizik bezpečnosti informací a přijetí zbytkových rizik bezpečnosti informací.

Metodika analýzy rizik musí zároveň odpovídat zákonu č. 181/2014 Sb., a jeho prováděcím vyhláškám.

Popis požadovaných základních výstupů

1. ***Zpráva o hodnocení rizik Systému EET*** – souhrnný dokument, který musí obsahovat:
    a. základní pravidla a postupy analýzy rizik a příslušná hodnotící kritéria včetně metodologie
    b. přehled aktiv včetně určení bezpečnostních parametrů a vlastníků
    c. výčet hrozeb a zranitelností, která na aktiva (skupiny aktiv) působí
    d. výsledky analýzy pro jednotlivá aktiva
    e. stanovení variant pro ošetření rizika
    f. stanovení priorit pro ošetření rizik
    g. přehled vlastníků rizik
    h. detailní výsledky analýzy rizik.

2. ***Prohlášení o aplikovatelnosti bezpečnostních opatření Systému EET*** – uvede ***souhrnný*** přehled opatření dle přílohy A normy ČSN ISO/IEC 27001:2014, která jsou aplikována při řešení bezpečnosti Systému EET a případné důvody, pro které nebyla nevhodná opatření aplikována. Součástí prohlášení o aplikovatelnosti bude specifikace a rozhodnutí o výši zbytkových rizik.

3. ***Návrh Plánu ošetření rizik Systému EET*** – bude obsahovat ***stanovení*** cílů bezpečnosti Systému EET, relevantních jednotlivým funkcím a úrovním řízení. Při plánování jak dosáhnout cílů bezpečnosti informací musí Poskytovatel určit:
    a. co bude vykonáno
    b. jaké zdroje budou vyžadovány
    c. kdo bude odpovědný
    d. kdy to bude dokončeno
    e. jak budou výsledky vyhodnoceny.

Fáze 1.3 – Zpracování Bezpečnostního projektu Systému EET

Cílem přípravy bezpečnostního projektu Systému EET bude zpracovat souhrnný podkladový dokument **Bezpečnostní projekt systému EET** přehled posuzovaných bezpečnostních funkcí, přehled a odůvodnění bezpečnostních funkcí vybraných k realizaci a postup a způsob jejich realizace.

Úkolem bezpečnostního projektu Systému EET bude **navrhnout bezpečnostní profily** (sady bezpečnostních funkcí), které budou snadno a jednoznačné implementovatelné.

Bezpečnostní profil systému je specifikací konkrétních bezpečnostních funkcí, které jsou definovány na základě určení systému, analýzy prostředí, v kterém bude provozován, a požadovaných bezpečnostních cílů. Bezpečnostní funkce jsou směrovány do všech oblastí bezpečnosti, včetně bezpečnosti provozního prostředí. Hlavním cílem bezpečnostních profilů tedy je výběr bezpečnostních funkcí pro funkční celky systému EET a jejich komponenty podle normy ČSN ISO/IEC 15408 a určení navazujících profilů ochrany.

Norma ČSN ISO/IEC 15408 stanovuje následující strukturu bezpečnostního profilu, jeho obsahu a významu jednotlivých dílčích částí:

- **úvod** – vymezuje základní charakteristiky bezpečnostního profilu,
- **charakteristika systému** – obecný popis systému, pro který je bezpečnostní profil určen,

- **bezpečnost prostředí** – rozbor bezpečnosti prostředí, ve kterém je systém provozován, zde jsou upřesněny základní aktiva, předpoklady pro bezpečné fungování systému, bezpečnostní zásady a hrozby, kterým systém musí čelit,
- **bezpečnostní cíle** – upřesnění bezpečnostních cílů, které musí být při řešení bezpečnosti dosaženy, ty jsou rozděleny na bezpečnostní cíle pro informační technologie a na bezpečnostní cíle pro prostředí, ve které jsou systémy provozovány,
- **požadavky na bezpečnost** – naplnění cílů návrhem bezpečnostních požadavků, tyto požadavky jsou rozděleny na požadavky na bezpečnostní funkce, které jsou prosazovány informačními technologiemi, na požadavky na záruky, kde je upřesněna míra záruk za správnost, a na požadavky na bezpečnost prostředí, které upřesňuje opatření v přímém okolí informačních technologií.

V této fázi budou provedeny následující úkony, které jsou důležité pro realizaci řešení bezpečnosti Systému EET:

- výběr relevantních bezpečnostních profilů pro funkční celky systému EET a jejich komponenty;
- konkretizace bezpečnostních funkcí;
- návrh realizace bezpečnostních funkcí v rámci systému EET.

Popis požadovaných základních výstupů

1. ***Bezpečnostní projekt*** – bude ***zpracován*** dle formální struktury profilu ochrany dle normy ČSN ISO/IEC 15408. Budou rozpracovány výchozí bezpečnostní cíle stanovené v souladu s Bezpečnostní politikou informací systému EET do bezpečnostních funkcí. Bezpečnostní projekt bude zahrnovat:
    a. Popis systému EET na úrovni vymezení účelu, hranic a struktury;
    b. Specifikaci bezpečnostního prostředí Systému EET na úrovni základních aktiv, služeb, bezpečnostních předpoklad, hrozeb a zásad bezpečnostní politiky;
    c. Vymezení bezpečnostních cílů Systému EET na úrovni cílů bezpečnosti pro informační technologie a cílů bezpečnosti pro prostředí;
    d. Stanovení požadavků na bezpečnost Sytému EET na úrovni požadavků na bezpečnost jednotlivých klíčových komponent, požadavků na bezpečnost prostředí, interpretace bezpečnostních požadavků a záruk;
    e. Mapování vzájemných vztahů mezi cíli, předpoklady a hrozbami.

Etapa 2 – Implementace bezpečnosti Systému EET

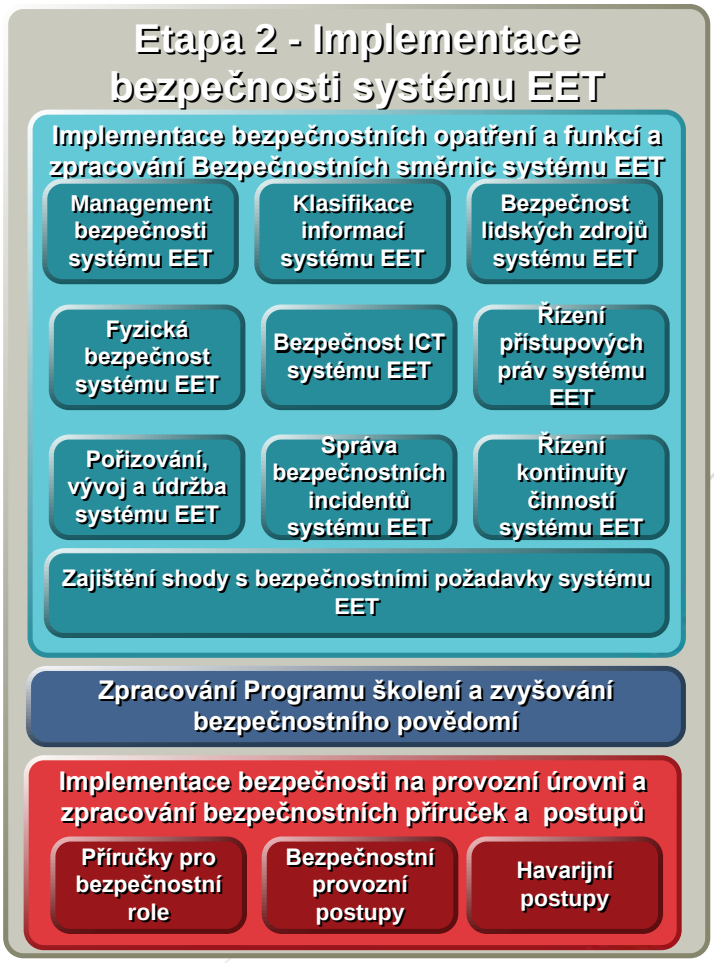
Cílem této fáze bude rozpracovat vybraná bezpečnostní opatření a bezpečnostní funkce do bezpečnostních pravidel a postupů Systému EET.

V návaznosti na výsledky analýz a bezpečnostního projektu musí poskytovatel zpracovat bezpečnostní směrnice Systému EET, bezpečnostní příručky a navazující postupy (případně návazností na jiné existující či zpracované postupy) včetně příručky/bezpečnostní směrnice pro činnost bezpečnostního správce.

Etapa 2 obsahuje následující fáze:

- 2.1 Implementace bezpečnostních opatření Systému EET
- 2.2 Bezpečnostní školení a vzdělávání v Systému EET.
- 2.3 Zpracování bezpečnostních příruček a zajištění kontinuity Systému EET

Grafické znázornění činností požadovaných realizovat Poskytovatelem v této etapě je uveden na následujícím obrázku.



Obrázek 31: Schéma etapy 2 řešení bezpečnosti Systému EET

Fáze 2.1 – Implementace bezpečnostních opatření Systému EET

V této fázi budou rozpracovány cíle a opatření bezpečnosti informací do postupů ve formě směrnic (dle ČSN ISO/IEC 27001:2014 – Příloha A - bezpečnostních profilů dle ISO/IEC 15408).

Nedílnou součástí bezpečnostních činností bude návrh a popis nástrojů relevantních pro Systém EET dle odst. 3) § 5 zákona č. 181/2014 Sb.

Ve směrnicích Poskytovatel stanoví ve spolupráci se Zadavatelem Systému EET role, navrhne úpravu pracovních náplní a odpovědnosti v procesu řízení bezpečnosti Systému EET. Bezpečnostní směrnice Systému EET budou zařazeny do systému řízení dokumentace provozovatele.

Způsob, formální uspořádání směrnic a jejich počet navrhne Poskytovatel na základě zpracovaného bezpečnostního projektu Systému EET. Směrnice však vždy budou obsahovat zapracování všech oblastí a náležitostí normy ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., včetně vyhlášek NBÚ.

V této fázi budou provedeny následující úkony, které jsou důležité pro realizaci řešení bezpečnosti Systému EET:

- zavedení a zdokumentování vybraných bezpečnostních opatření (ČSN ISO/IEC 27001: 2014;)
- určení a zdokumentování způsobu měření účinnosti vybraných bezpečnostních opatření.

Popis požadovaných základních výstupů

1. ***Směrnice řízení bezpečnosti Systému EET*** bude *zpracována* v rozsahu:
    a. Management bezpečnosti informací definující pravidla a postupy pro management bezpečnosti informací a bezpečnosti informací v projektovém řízení včetně určení odpovědností za průběh celého cyklu ISMS a uvedení způsobu měření účinnosti ISMS.
    b. Bezpečnost lidských zdrojů definující bezpečnostní pravidla a postupy pro oblast personální bezpečnosti.
    c. Klasifikace informací určující způsob klasifikace informací včetně klasifikačního schématu a způsob manipulace s citlivými informacemi.
    d. Fyzická bezpečnost a bezpečnost prostředí definující bezpečnostní pravidla a postupy, jejichž cílem je předcházet neautorizovanému přístupu, poškození, znehodnocení, zničení či jiným zásahům do informací a do prostor, ve kterých se nacházejí zařízení pro zpracování informací.
    e. Shoda s bezpečnostními požadavky rozpracovávající konkrétní postupy v oblasti zajištění souladu přijímaných opatření s legislativou a bezpečnostními či technologickými postupy dle přijatých norem a standardů.
2. ***Směrnice bezpečnosti informačních a komunikačních technologií Systému EET*** bude zpracována v rozsahu:
    a. Bezpečnost provozu a bezpečnost komunikací stanovující opatření zaměřená na řádný a bezpečný provoz prostředků pro zpracování informací a služeb a procesů s tím souvisejících.
    b. Řízení přístupu stanovující opatření zaměřená na ochranu a kontrolu přístupu k informacím, službám a procesům.
    c. Akvizice, vývoj a údržba informačních systémů definující pravidla a postupy pořizování, vývoje a údržby Systému EET k prosazení bezpečnosti informací do celého životního cyklu Systému EET od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu.
3. ***Směrnice řízení incidentů bezpečnosti informací a zajištění kontinuity činností Systému EET*** bude zpracována v rozsahu:
    a. Řízení incidentů bezpečnosti informací stanovující postupy hlášení bezpečnostních incidentů, reakce na ně a jejich vyhodnocování.
    b. Řízení kontinuity činností a základní rámec řízení kontinuity podnikatelských činností, zahrnující stanovení rolí, procesů, struktury dokumentace a odpovědností.

Fáze 2.2 – Bezpečnostní školení a vzdělávání v Systému EET

V této fázi bude provedeno seznámení pracovníků provozovatele Systému EET se zaváděnými bezpečnostními opatřeními. Bude vytvořen program budování bezpečnostního povědomí, jehož úkolem bude zabezpečit znalost a pochopení postupů a činností v oblasti bezpečnosti Systému EET zaměstnanci provozovatele.

Dále budou vyškoleni pracovníci provozovatele Systému EET, kteří jsou zahrnuti do rozsahu řešení bezpečnosti Systému EET. Tito zaměstnanci budou seznámeni s pravidly a úkoly, které jím ze zajištění bezpečnosti Systému EET vyplývají. Zvláštní pozornost musí být věnována přípravě zaměstnanců, kteří budou provádět interní audity bezpečnosti Systému EET. Pro školení pracovníků bude vytvořen e-learningový portál.

V této fázi budou provedeny následující úkony, které jsou důležité pro realizaci řešení bezpečnosti informací Systému EET:

- zpracování programu školení a zvyšování bezpečnostního povědomí (dle ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., včetně vyhlášek NBÚ)
- zpracování podkladů pro školení zainteresovaných zaměstnanců provozovatele Systému EET – upřesnění kategorií, pro které bude školení provedeno, příprava prezentace a Desatera

bezpečnosti informací (ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., včetně vyhlášek NBÚ)

- proškolení zaměstnanců provozovatele Systému EET, po určených kategoriích (ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., včetně vyhlášek NBÚ).

Popis základních požadovaných výstupů

1. ***Program školení a zvyšování bezpečnostního povědomí*** – obsahuje koncepci tvorby a budování bezpečnostního povědomí subjektů účastnících se správy, provozu a užívání Systému EET. Rozsah programu bude následující:
    a. Způsob budování bezpečnostního povědomí:
        - základní cíl budování bezpečnostního povědomí,
        - strategie budování bezpečnostního povědomí,
        - kategorie zaměstnanců,
        - plánování budování bezpečnostního povědomí,
        - odpovědnost za budování bezpečnostního povědomí,
        - odpovědnost zaměstnanců,
        - odpovědnost za organizaci a provedení školení zaměstnanců provozovatele Systému EET,
        - odpovědnost za seznámení zaměstnanců třetích stran s bezpečnostními postupy Systému EET

    b. Obsahová náplň budování bezpečnostního povědomí“
        - školení k systému řízení bezpečnosti Systému EET,
        - Vstupní školení bezpečnosti Systému EET,
        - Periodické školení bezpečnosti Systému EET,
        - Mimořádné proškolení bezpečnosti Systému EET,
        - vzdělávání v oblasti bezpečnosti Systému EET.
2. ***Materiály školení bezpečnosti Systému EET*** – tvoří ppt prezentace a podkladové materiály pro provedení školení k zajištění bezpečnosti Systému EET pro jednotlivé kategorie zaměstnanců provozovatele Systému EET.
3. ***E-learningový* portál** – Vlastní školení bude pro vhodné kategorie zaměstnanců provedeno formou e-learningu. Poskytovatel zajistí vytvoření standardního e-learningového portálu včetně vhodného obsahu.

Fáze 2.3 – Zpracování bezpečnostních příruček a zajištění kontinuity Systému EET

V této fázi budou rozpracovány bezpečnostní postupy a pravidla Systému EET do nejnižší provozní úrovně.

Rozsah činností a konkretizace výstupů bude upřesněna na počátku fáze a musí vycházet z implementovaných bezpečnostních opatření vybraných na základě provedené analýzy rizik, bezpečnostního projektu Systému EET.

V rámci fáze musí být vytvořena bezpečnostní provozní dokumentace zejména v oblastech:

- Informační bezpečnosti Systému EET;
- zajištění kontinuity činností Systému EET

Důraz musí být položen na zpracování **bezpečnostních příruček pro jednotlivé role**. Tvorba příruček pro oblast bezpečnosti se bude opírat o informace ve směrnicích a o informace ze schůzek

s pracovníky, kteří budou zastávat jednotlivé role. Struktura příruček musí vycházet ze struktury existujících směrnic.

V rámci této fáze musí být zapracována problematika bezpečnosti do uživatelské dokumentace Systému EET.

V této fázi musí být provedeny následující úkony, které jsou důležité pro realizaci řešení bezpečnosti Systému EET:

zavedení a zdokumentování vybraných bezpečnostních opatření (ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., včetně vyhlášek NBÚ).

Popis požadovaných základních výstupů

1. ***Bezpečnostní příručky a navazující postupy*** definující konkrétní činnosti a pravidla chování pro jednotlivé role a účastníky správy a provozu Systému EET. Základní rozsah jedné příručky (zde pro příklad bezpečnostního manažera systému EET) je následující:

    a. Bezpečnostní příručka bezpečnostního manažera Systému EET:
    - řízení bezpečnosti s důrazem na roli bezpečnostního manažera,
    - řízení a klasifikace aktiv Systému EET s důrazem na evidenci aktiv a zacházení s aktivy v závislosti na jejich klasifikaci.
    - zajištění bezpečnosti lidských zdrojů s důrazem na: povinnosti bezpečnostního manažera při přijímání, školení a bezpečném odchodu pracovníků provozu Systému EET.
    - řízení bezpečnosti komunikací a provozu Systému EET s důrazem na provozní postupy, řízení změn, zálohování a monitorování.
    - řízení přístupu k systémům Systému EET s důrazem na roli bezpečnostního manažera a dohled a kontrolu přístupových práv.
    - akvizice, vývoj a údržba informačních systémů v rámci Systému EET s důrazem na stanovení bezpečnostních požadavků a dokumentace.
    - fyzická bezpečnost a bezpečnost prostředí s důrazem na pravidla práce v zabezpečených oblastech.
    - správa incidentů a řízení kontinuity s důrazem na povinnosti bezpečnostního manažera.
    - Bezpečnostní příručka bezpečnostního správce Systému EET bude zpracována v obdobném rozsahu jako příručka bezpečnostního manažera Systému EET.

Etapa 3 – Monitorování a přezkoumání bezpečnosti Systému EET

Cílem etapy bude zavést postupy pro zajištění efektivního řízení bezpečnosti Systému EET a jeho zlepšování. V rámci etapy musí Poskytovatel navrhnout a zavést metriky pro měření účinnosti bezpečnosti Systému EET, postupy interního auditu bezpečnosti a postupy pro pravidelná přezkoumání bezpečnosti Systému EET.

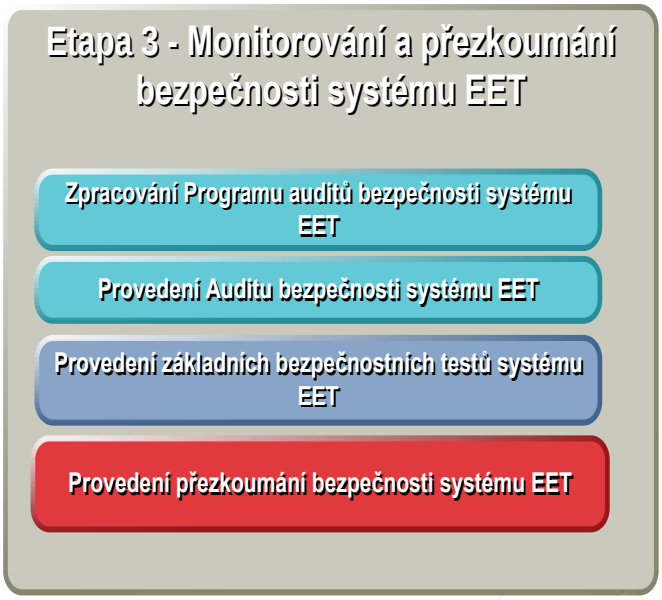
V rámci této etapy budou provedeny základní bezpečnostní testy Systému EET v rozsahu konfiguračních a penetračních testů k ověření výsledné implementace řešení před spuštěním Systému EET do produkčního provozu.

Etapa 3 musí obsahovat následující fáze:

- 3.1 Příprava a provedení auditu bezpečnosti Systému EET

- 3.2. Povedení přezkoumání bezpečnosti Systému EET

Grafické znázornění činností požadovaných realizovat v této etapě je uveden na následujícím obrázku.



Obrázek 32: Schéma etapy 3 řešení bezpečnosti Systému EET

Fáze 3.1 – Příprava a provedení auditu bezpečnosti Systému EET

Cílem této fáze bude zajistit provádění kontrolní a auditní činnosti k posouzení efektivního provozu bezpečnosti Systému EET. Fáze bude zahrnovat přípravu a provedení interního auditu bezpečnosti Systému EET.

V rámci fáze bude zpracován plán interních auditů bezpečnosti Systému EET, včetně popisu způsobu provádění interních auditů bezpečnosti Systému EET a metrik měření účinnosti přijatých opatření. V tomto dokument Poskytovatel uvede:

- vstupy pro zhodnocení, které budou mimo jiné zahrnovat výsledky auditů a analýz bezpečnosti Systému EET, zajištění zpětné vazby od zainteresovaných stran, stavu preventivně nápravných činností a doporučení pro zlepšení bezpečnosti Systému EET (dle ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., a vyhlášky NBÚ);
- výstupy zhodnocení, které budou zahrnovat jakákoliv rozhodnutí a činnosti vztahující se k zlepšování efektivnosti, změny postupů a potřeby zdrojů na zajištění bezpečnosti Systému EET (dle ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., a vyhlášky NBÚ);
- interní audity bezpečnosti Systému EET, které zajistí, že cíle a opatření bezpečnosti Systému EET vyhovují požadavkům na systém, normě ČSN ISO/IEC 27001, legislativě a požadavkům na bezpečnost informací a jsou funkční a jsou zavedeny a udržovány efektivně ((dle ČSN ISO/IEC 27001:2014 a zákon č. 181/2014 Sb., a vyhlášky NBÚ).

V rámci této fáze bude zpracován program pro první audit, provede vzorový interní audit s vyčleněnými pracovníky Zadavatele bezpečnosti Systému EET dle normy ČSN ISO/IEC 27001:2014 a zpracuje zprávu z tohoto auditu. Dále budou připraveni a vyškoleni interní auditoři pro oblast bezpečnosti Systému EET Strukturu auditu je požadována v následující:

- zpracování programu auditu,
- zahájení a příprava auditu – ustavení jeho základního rámce,

- příprava auditu – příprava auditních podkladů, upřesnění rámce a průběhu auditu a příprava jeho účastníků na straně provozovatele Systému EET,
- provedení auditu – shromáždění relevantních informací z auditovaných oblastí, jejich posouzení, zpracování a schválení ve formě auditních záznamů a příprava závěrů auditu z auditovaných oblastí.
- vyhodnocení auditu – bude zjištěna úroveň shody aktuálního stavu auditovaných oblastí se zvolenými kritérii auditu – požadavky na bezpečnost Systému EET a normou ČSN ISO/IEC 27001:2014. Výsledky budou uvedeny ve Zprávě z interního auditu bezpečnosti Systému EET.

Popis požadovaných základních výstupů

1. ***Plán auditů bezpečnosti Systému EET*** – stanoví způsob provádění pravidelných přezkoumávání a ověřování bezpečnosti Systému EET k zajištění účelnosti, dostatečnosti a efektivnosti celého řešení bezpečnosti.
2. ***Materiály školení interních auditorů*** – budou tvořit ppt prezentace a podkladové materiály pro provedení interního auditu bezpečnosti Systému EET spolu s přípravou modulu do e-learningového školení.
3. ***Program interního auditu bezpečnosti Systému EET*** – bude tvořit dokument propisující způsob provedení, kritéria a organizační zajištění konkrétního (prvního) auditu stavu bezpečnosti Systému EET.
4. ***Zpráva z interního auditu bezpečnosti Systému EET*** – bude tvořit dokument, jehož cílem bude poskytnout komplexní zprávu o stavu bezpečnosti Systému EET.

Fáze 3.2 – Provedení přezkoumání bezpečnosti Systému EET

Cílem fáze bude zpracovat Přezkoumání bezpečnosti Systému EET, které bude tvořit základní hodnotící dokument pro další provoz a zlepšování bezpečnosti Systému EET.

Návrh Přezkoumání bezpečnosti Systému EET bude zpracován ve spolupráci s bezpečnostním managementem resortu MFČR v následující struktuře:

- návrh na zlepšení bezpečnosti Systému EET do dalšího přezkoumání bezpečnosti Systému EET
- doporučení ke zlepšení efektivity bezpečnosti Systému EET a k aktualizaci hodnocení rizik
- návrh změny postupů zajištění bezpečnosti Systému EET
- zdroje potřebné pro zlepšování bezpečnosti Systému EET
- doporučení ke zlepšení účinnosti opatření bezpečnosti Systému EET
- návrh cílů ISMS pro další cyklus provozu bezpečnosti Systému EET.

Přezkoumání bezpečnosti Systému EET – bude tvořit dokument, jehož cílem bude zhodnotit úroveň zavedení bezpečnosti Systému EET a navrhnout další postup při provozování a zlepšování bezpečnosti Systému EET.

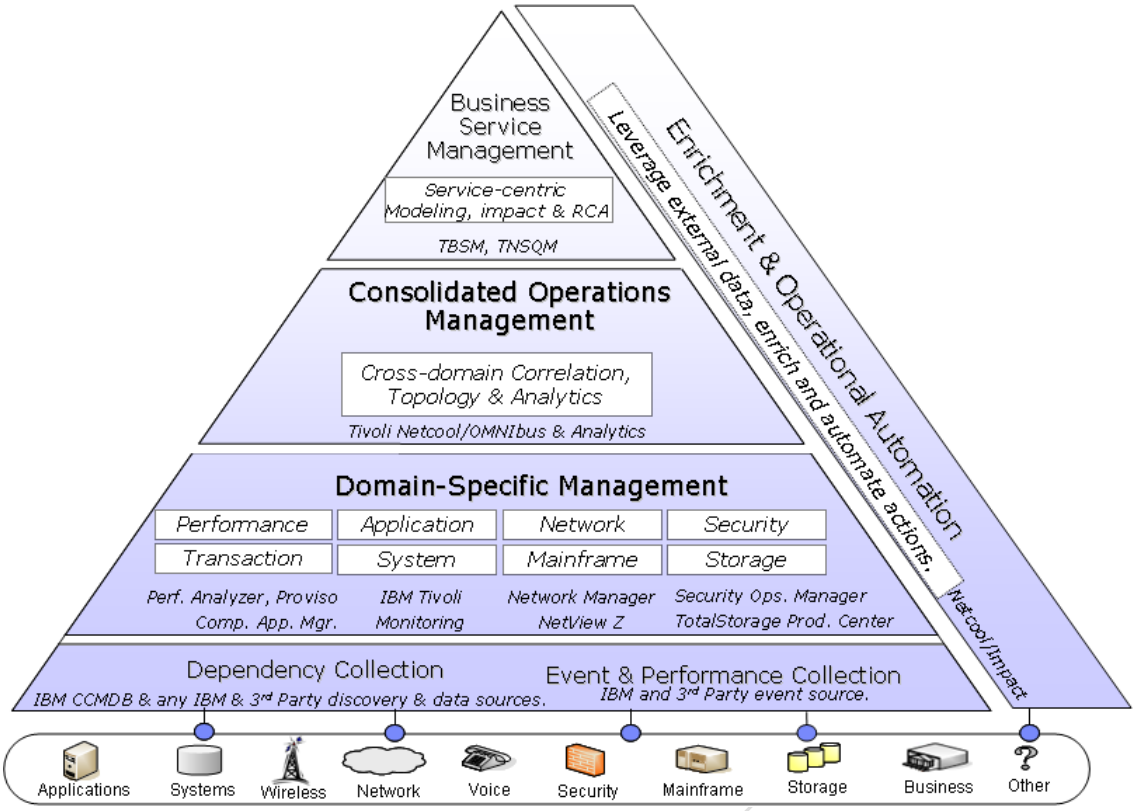
Požadavky na monitoring a prostředí datových sálů pro systém EET

Monitoring systému EET

- provádí nepřetržitý dohled provozního stavu a datové průchodnosti aktivních prvků
- průběžně monitoruje zejména kvalitu a dostupnost služeb EET, odchylky parametrů od normálního stavu, sleduje trendy a reportuje dosažení prahových hodnot
- provádí primární vyhodnocení alarmů a nestandardních provozních stavů a jejich eskalace
- pořizuje záznamy provozních událostí do Trouble Ticket System (TTS)
- zpracovává a distribuuje periodická hlášení a reporting o dostupnosti služeb a datovém zatížení infrastruktury
- provádí zálohování dat podle schválené dokumentace
- dohlíží na dodržování postupů Řízení změn (Change management), Řízení konfiguračních položek (Configuration management) HW a SW a jejich dokumentace
- plánuje a provádí ověřovací a profylaktické činnosti
- provádí správu a uchovávání logů
- klasifikuje poruchy a odchylky od provozního stavu, spoluvytváří postupy pro jejich odstraňování a provádí jejich dokumentaci prostřednictvím TTS (trouble ticket systém)
- spolupracuje s administrátory při řešení incidentů

Všeobecné vlastnosti monitoringu:

- Konsolidace a korelace systémových událostí v reálném čase a “root-cause“
- Kompletní viditelnost všech KPI a SLA napříč aplikacemi, síťovými segmenty nebo provozními jednotkami.
- Jednotné grafické prezentační prostředí a single-sign on
- Integrace s externími systémy a tzv. business context - tedy jak jsou technologie napojeny na podnikové/obchodní funkce
- Drill-down – vizualizace od přehledových pohledů až po detailní pohledy pro konkrétní technologie
- Nativní provázanost s ostatními moduly – síťový a aplikační performance management, Service Desk, Storage, atd.



Obrázek 33: Monitoring systému EET

Koncepčně existují tyto funkční bloky:

- **Business Service Management:** Nejvyšší vrstva, která poskytuje celkový přehled o službách, aplikacích, transakcích a procesech. Tato vrstva sleduje agregované KPI a vyhodnocuje SLA a celkovou výkonnost IT organizace
- **Consolidated Operations Management:** Konsolidace fault a performance dat a tzv. umbrella management, tedy jednotná správa nad celou heterogenní technologickou a aplikační infrastrukturou
- **Domain Management:** Správa jednotlivých technologických domén jako jsou sítě, aplikace, security, storage, VoIP atd.

Metriky:

- Objem transakcí
- Transakční chyby
- Výkonnost procesů a jejich degradace
- Celkový zisk služby, dostupnost, SLA a případná penalizace
- Záznamy o incidentech a problémech
- Žádosti o změnu (‘change request’)

SLA Monitoring

- Aktuální stav SLA
- Procentuální poměr, kdy je služba dostupná

- Celkový down-time služby pro dané SLA
- Zbývající čas do překročení SLA
- Celková cena (penalizace) za nedostupnost služby
- Systémová architektura

Monitoring infrastruktury

Prostředky pro správu a dohled EET budou připojeny k infrastruktuře SPCSS prostřednictvím nezávislé administrativní sítě.

Do jednotlivých VLAN logických sítích jsou připojovány jednotlivé komponenty admin (Out-Of-Band) sítě.

Pro vzdálené připojení administrátorů z prostředí Internetu nebo Intranetu slouží tentýž hardware ve funkci VPN koncentrátoru. Autentizace administrátorů je možná prostřednictvím AAA serveru umístěným v jednom z bezpečných segmentu admin sítě nebo prostřednictvím „master“ AAA serveru SPCSS. Vlastní autentizace je realizována prostřednictvím hesla a certifikátu pro identifikaci uživatele resp. klíč pro IPSEC komunikaci.

Pro větší bezpečnostní oddělení administrátorů bude mezi administrátora a vlastní spravované prostředky vložen server s terminálovými službami. Vlastní nástroje pro administraci pak mají jednotliví uživatelé umístěny na těchto aplikačních terminálových serverech. Přenášená data mezi administrátorem a terminálovým serverem jsou data „o obrazovce a klávesnici“.

Síťové prvky v admin síti musí podporovat technologii PVLAN (Private VLAN).

Každý dohlížený prvek je do OOB sítě zapojen samostatným Ethernet portem s možností nastavení protokolových pravidel na tomto portu (síťové prostředky Access-list, servery lokální firewally jako je např. iptables v linuxu apod.)

Každý síťový prvek je navíc připojen do OOB sítě ještě jedním nezávislým kanálem a to je konzolový port. Konzolové porty z admin sítě jsou dostupné přes síťový terminálový server.

Požadavky na fyzické a technologické zabezpečení datový sálů EET

Prostory, kde bude datový sál EET umístěn, musí odpovídat následujícím požadavkům:

a) teplota prostředí se pohybuje v rozmezí od 19°C do 25°C, relativní vlhkost v rozmezí 35% - 65%,
b) v místnostech, kde je datový sál EET umístěn, jsou instalována požární čidla na kouř a teplotu,
c) tyto prostory jsou napojeny na systém elektronické protipožární signalizace a elektronické zabezpečovací signalizace, a jsou vybaveny kamerovým systémem hlídající vstup do prostor a jednotlivé uličky mezi stojany s možností přisvětlení ve tmě
d) prostory jsou vybaveny stabilním hasicím zařízením s hasícím médiem FM 200, Novec 1230 či obdobným
e) technologické prostory datového sálu EET musí mít instalovaný dveřní systém v bezpečnostní třídě WK 2 podle EN 1627 s mechanickým zavíračem dveří, včetně přidržovacího elektromagnetického zařízení a elektronického zámku s napojením na stávající systém EKV
f) požadavky zajištění silnoproudých rozvodů:
    a. všechny technologické prostory jsou vybaveny mezilehlým rozvaděčem se dvěma samostatnými okruhy:
        i. nezálohovaná AC síť 230V,

ii. AC síť 230V zálohovaná generátorem,

b. technologické prostory jsou vybaveny distribučním stojanem se dvěma samostatnými okruhy určeným pro napájení zařízení ve stojanových řadách, jeden okruh bude napájen ze zálohované sítě generátorem a druhý bude napájen ze záložního generátoru přes centrální UPS jako zdroj nepřerušitelného napájení.,

g) požadavky zajištění zálohování silnoproudého napájení:
   a. technologické prostory jsou vybaveny nepřerušitelným zdrojem v kapacitě min. 50 kVA v modulární výstavbě s možností výkonového rozšíření na 80 kVA, s umístěním co nejblíže distribučního stojanu, na překlenutí náběhu generátoru max. 5 min.,
   b. modulární řešení UPS předpokládá redundaci N+1, jak řídících, tak výkonových modulů, včetně řešení redundance baterií (2 okruhy). Požadujeme možnost výměny výkonových modulů i baterií bez přerušení provozu. UPS vybavit modulem pro vzdálený dohled (SNMP a WWW přístup) ,
h) požadavky zajištění klimatizace
   a. všechny technologické prostory požadujeme vybavit klimatizačním systémem na plánovanou kapacitu.
   b. návrh řešení komplexního chladicího systému musí obsahovat flexibilní a modulární systém klimatizačních prvků, modulů s možností reakce na změny zátěže v jednotlivých místnostech i stojanových řadách v průběhu doby dle požadavků provozovatele.
   c. řešení klimatizace musí umožňovat redundanci N+1 a střídání základních modulů, jak chladícího systému, tak ventilačního systému, včetně možnosti výměny vadného modulu bez přerušení provozu. Systém vybavit modulem pro vzdálený dohled (SNMP a WWW přístup)
   d. řešení chladícího systému musí zohledňovat uzavřenou stojanovou řadu se stojany 800 x 1000 mm s chladicím výkonem 8 kW na každý stojan, určené pro technologická zařízení s příkonem přesahujícím 2,5 kW.
i) v datovém sálu EET musí být instalované stojany modelově „řady DK-TS8“, určené pro zařízení s montáží do 19“ lišt o hloubce 1 m a montážní výškou 42U s následujícími vlastnostmi: robustní svařovaný rám, statická zatížitelnost 1000 kg, čtyřbodové zamykání, včetně bezpečnostního zámku vpředu i vzadu, 19“ montážní rám vpředu i vzadu, zemnění všech částí stojanu,
j) v datovém sálu EET je instalován systém zvýšené podlahy pro aplikaci komunikační kabeláže a silnoproudých rozvodů s zátěží dimenzovanou minimálně na 850 kg/m2, při požadavku na vyšší nosnost - možnost instalace roznášecích roštů
k) je zajištěna vnější ochrana budovy bezpečnostní službou nepřetržitě 24 hodin denně a 7 dní v týdnu, přičemž jsou prokazatelně evidovány osoby vstupující do objektu, v němž se prostory s datovým sálem EET nacházejí,
l) datový sál EET splňují podmínky Vyhlášky č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. pro **stupeň utajení Důvěrné**,
m) prostory, v nichž se datový sál EET nachází, leží mimo zátopovou oblast tzv. stoleté vody,
n) datové sály EET jsou z hlediska geografické lokalizace umístěny ve dvou různých lokalitách, které splňují podmínku, že jsou od sebe vzdáleny více než 6000 metrů a méně jak 30000 metrů a jsou napájeny z různých rozvoden elektrické energie,

o) možnost instalace systému datových komor s možností rozšíření nebo demontáže a následné montáže, splňující fyzickou bezpečnost dle *Certifikátu technického prostředku NBÚ, třída 2, požadované krytí IP56),*

p) datové sály EET jsou redundantně připojeny na páteřní infrastrukturu MFČR a Internet

Kapacita datových sálů

V datovém sále EET je požadováno umístění minimálně 5 stojanů modelově „řady DK-TS8“, určené pro zařízení s montáží do 19“ lišt o hloubce 1 m a montážní výškou 42U.

Specifikace požadavků na testování systému

Testování je nedílnou součástí životního cyklu vývoje webových služeb a výstavby prostředí pro provoz systému EET. Zabezpečuje udržování kvality celého řešení. Testování se řídí podobnými pravidly jako tvorba aplikace. Z pohledu RUP jako obecné metodiky pro tvorbu aplikací je na začátku testování nutné vytvořit testovací případy (testcase). Je to obdoba tvorby případů užití (usecase) v rámci návrhu aplikace.

Test Case je obvykle tvořen jedním nebo vícero kroky. Test case obsahuje následující údaje:

- test case ID,
- test case popis,
- testovací kroky nebo pořadí testování,
- nutné požadavky k výkonu testu,
- síla testu,
- test kategorie,
- autor,
- označení, jestli test je automatizován, nebo ne (jestli je možno jej pravidelně spouštět),
- výsledek testu (úspěšný/neúspěšný),
- poznámky.

V případě testování celého řešení EET budou jednotlivé testy rozděleny do několika oblastí:

- Testování infrastruktury (non-functional test)
- Testovaní webových služeb (functional test)

Testování infrastruktury v sobě zahrnuje:

- Výkonnostní testování
- Integrační testování
- Bezpečnostní testování
- Disaster-Recovery testy
- Load test

Cílem testování samotné infrastruktury je:

- ladění systémových parametrů,
- odstranění potencionálních problémů z pohledu bezpečnosti, výkonnosti,
- nastavení spodních prahových hodnot pro další testování, při postupné instalaci jednotlivých aplikačních komponent,
- otestování obnovy systému při jeho pádu (single-point-of-failure)
- testování rozkládaní zátěže mezi jednotlivé komponenty v rámci clusteru
- otestování přepnutí do záložní lokality a obnova primární lokality
- otestování monitorování prostředí
- otestování zálohování prostředí a obnova jednotlivých komponent

Test Disaster Recovery

Speciálním typem funkčního testu z pohledu funkcionality EET je test disaster-recovery. Tento test bude proveden k otestování:

1. fyzické kapacity infrastruktury,
2. validaci postupů navrhnutých pro účely disaster-recovery,
3. validaci týmu pro provedení jednotlivých procesů,
4. validaci časového plánu,
5. zjištění možných ztrát dat při ztrátě jedné lokality,
6. validaci postupů návratu zpět do primárná lokality,
7. validaci času potřebného pro návrat do primární lokality.

Tyto testy budou prováděny pravidelně podle stanoveného plánu těchto testů.

K tomu, abychom mohli dostatečně kvalitně otestovat infrastrukturu, bude zapotřebí vytvořit vlastní testovací služby, které běží na jednotlivých komponentách a zároveň vytvoření vlastních “pokladen” simulujících reálný provoz.

Zátěžový test (load test)

Zátěžový test patří mezi nefunkcionální testy, slouží pro validaci výkonnosti:

- samotných služeb,
- provozního prostředí.

Pro správně otestování zátěže bude nutné vytvořit sadu klientů (pokladen), kteří budou simulovat reálný provoz. To znamená vytvořit zhruba až 4000 transakcí za sekundu simulujících pokladní systémy povinných subjektů, které nám vytvoří zátěž s následujícími parametry:

- 4000 dotazů za 1s na fiskalizační rozhraní
- 100 editačních dotazů za 1s na portále.

Výsledky této zátěže budou zpracovány do formy výstupního reportu. Zátěžové testy budou prováděny za přítomnosti monitorovacích nástrojů. Důvodem je zjištění jednotlivých časových zpoždění, která vznikají na komponentách infrastruktury nebo konkrétních služeb.

Nutnou podmínkou zátěžového testu je monitorování jednotlivých komponent na úrovni:

- hardware (využití CPU, paměť),
- propustnost sítě,
- výkonnosti samotné služby,
- výkonnosti aplikačních platforem.

Na základě výsledku zátěžového testování, bude identifikováno, kde jsou slabá místa v rámci infrastruktury EET a jednotlivých služeb implementovaných v rámci EET.

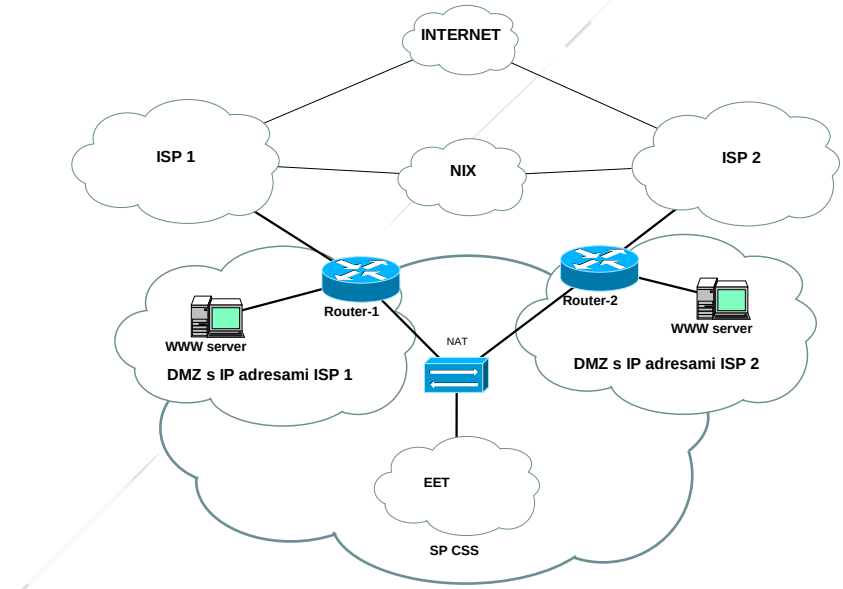
Požadovaná architektura připojení do Internetu pro systém EET

K poskytování služby EET, u které je zapotřebí udržet vysokou dostupnost fiskalizačních serverů, je nutné mít zálohované připojení. Vícenásobné připojení k jednomu poskytovateli (ISP - Internet Service Provider) je nejjednodušší variantou. Připojení SPCSS k síti Internet je v současné době realizováno prostřednictvím poskytovatele T-Mobile, dvěma nezávislými optickými spoji o rychlosti 100 Mbit/s.

Takovéto připojení však neřeší zajištění dostupnosti služby v případě problému na hraničních zařízeních ISP. Zajištění velmi vysokých nároků na dostupnost je možné dosáhnout pouze při připojení na více poskytovatelů. Pro realizaci projektu EET bude zapotřebí navýšit kapacity a způsob připojení SPCSS k síti Internet. Kapacitu připojení bude zapotřebí navýšit na 2 x 1Gb/s (1Gb/s dvěma optickými spoji). Architektura a možné způsoby realizace připojení SPCSS k síti Internetu pro potřeby projektu EET jsou rozebrány níže. Jedná se o připojení SPCSS do dvou nezávislých přístupových bodů internetu a 3 možné varianty připojení na vícero poskytovatelů připojení k síti Internet. Jako nejvhodnější se jeví poslední varianta připojení prostřednictví vlastního autonomního směrovacího systému.

Připojení s použitím adres od více ISP

Tato možnost je často používána. Organizace obdrží od každého poskytovatele blok adres, který použije při adresaci svých serverů.



Obrázek 34 : Schéma zapojení s použitím adres více ISP

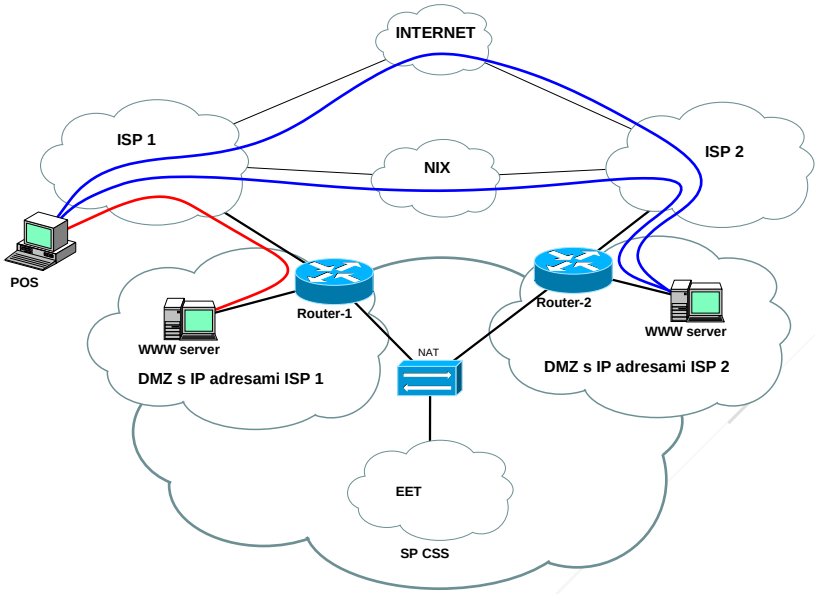
Pojmenování serverů je možné v DNS provést dvěma způsoby:

- každé IP adrese je přiřazeno jméno
- všem IP adresám je přiřazeno pouze jediné jméno

Pokud je každé IP adrese přiřazeno jiné jméno je pokladní systém povinného subjektu (dále jen POS) nucen si vybrat z různých připojení to, u kterého má nejlepší odezvu. Sám POS si vybírá nejlepší cestu (Obrázek 35). V případě nedostupnosti sám musí zkusit připojení na další server.

Pokud je adresám přiřazeno pouze jediné jméno nemusí sice POS vyhledávat nejlépe dostupný server, ale jmenné servery mu vrací IP adresy serverů v cyklu (tzv. round robin). Stává se tedy, že přestože stále vstupuje na tentýž odkaz, mívá různou odezvu podle toho, kterou IP adresu dostane od

jmenného serveru. Nejlepší připojení je přímo u ISP (Obrázek 35 - červená cesta). U ostatních cest (Obrázek 35 - modré cesty) již dochází ke zpoždění. Při připojení přes NIX nemusí být zpoždění nijak dramatické, ale zpoždění na vytížených zahraničních linkách již může být pro POS obtěžující.

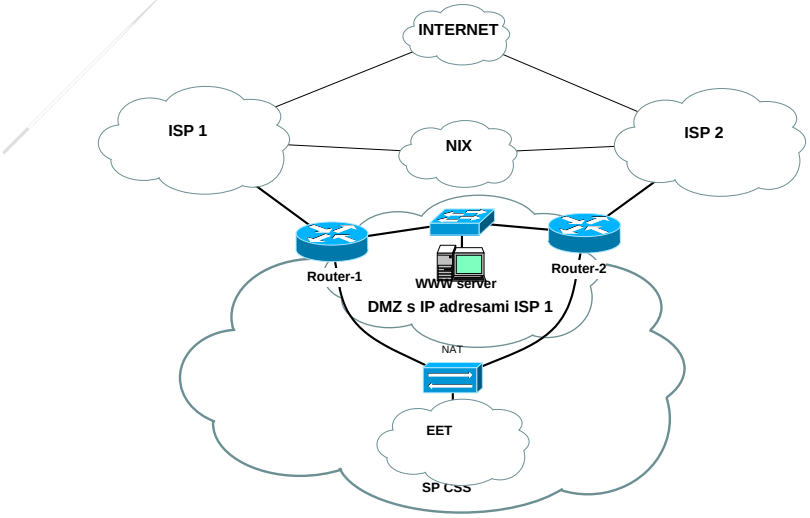


Obrázek 35 : Schéma přístupu POSu k serverům

Tato varianta tudíž není příliš vhodná pro poskytování služeb EET. Její výhodou je však jednoduchost a možnost provozování bez nutnosti nadstandardní spolupráce s ISP.

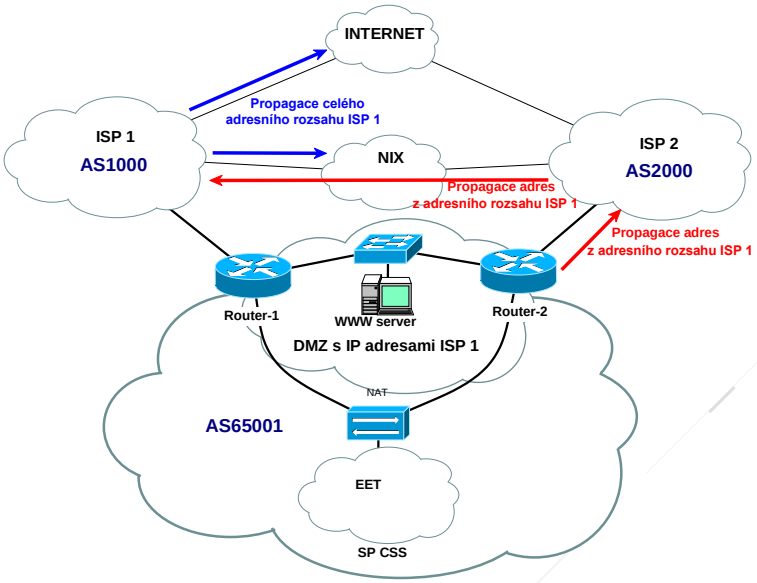
Připojení s použitím adres jednoho z ISP

Mnohem efektivnější než předchozí varianta je využít připojení s adresním prostorem pouze jediného poskytovatele připojení (Obrázek 36). Díky jedinému adresnímu prostoru je zajištěno, že POS vždy k serverům přistupuje pouze jedinou cestou, která se za normálního stavu nemění.



Obrázek 36 : Schéma zapojení pouze s IP adresami jednoho z ISP

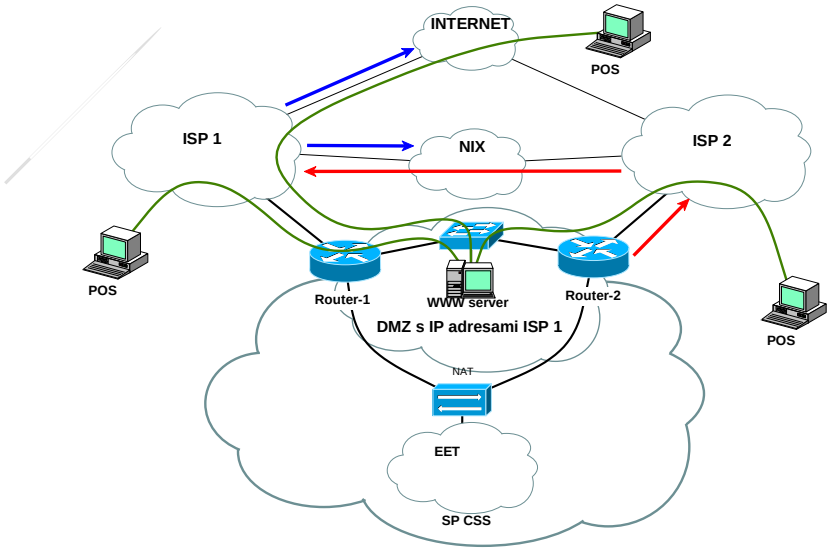
Tato varianta je mnohem vhodnější pro komunikaci mezi systémem EET a POSem, ale vyžaduje nadstandardní spolupráci s poskytovateli připojení. Také již vyžaduje použití vnějšího směrovacího protokolu. Z důvodu zamezení nežádoucího propojení mezi sítěmi ISP je téměř nezbytné použití BGP (Border Gateway Protocol).



Obrázek 37 : Schéma zapojení s použitím směrovacího protokolu BGP

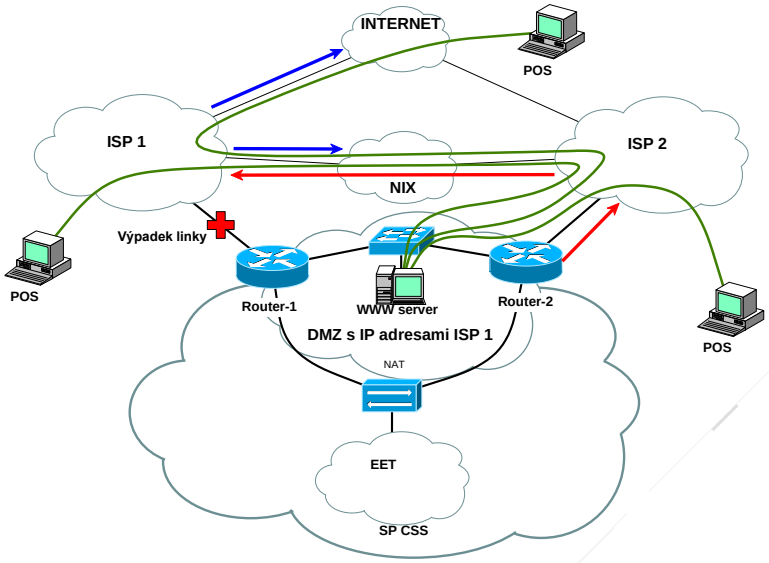
Je nutné zajistit domluvu a souhlas ISP k šíření bloku adres, který je přidělen jednomu z poskytovatelů i v ostatních sítích (Obrázek 37). ISP 1 jehož adresy jsou použity šíří směrovací informace do internetu standardním způsobem(modré šipky). Do sítě dalších poskytovatelů se po dohodě šíří směrovací informace o bloku adres z privátního autonomního systému AS65001, v němž jsou použity adresy přidělené poskytovatelem ISP1. Tito ostatní poskytovatelé mohou tyto směrovací informace předávat hraničním směrovačům ISP1 (červené šipky).

Poskytování směrovacích informací z privátního AS dalším poskytovatelům umožní přímý přístup k serverům i POSům připojeným prostřednictvím těchto ISP (Obrázek 38).



Obrázek 38 : Schéma toku dat za normálního stavu sítě

Předávání směrovacích informací o bloku adres použitém v privátním AS na hraniční směrovače poskytovatele ISP1 vytváří záložní spojení pro případný výpadek linky mezi organizací a ISP (Obrázek 39).



Obrázek 39 : Schéma toku dat při výpadku linky k ISP

Poskytování směrovacích informací jiným poskytovatelům nebo do obecně internetu je sice možné, ale nemusí vždy fungovat. Většina ISP totiž kontroluje a filtruje směrovací informace, které neodpovídají doporučení a informacím uvedených v databázích organizace RIPE (Réseaux IP Européens).

Mimo jiné akceptují směrovací informace s minimálním prefixem /19 případně /20 (Tabulka 2) a menší bloky ignorují. Dále mohou akceptovat směrovací informace o síti pokud přichází z AS uvedeného v databázích organizace RIPE.

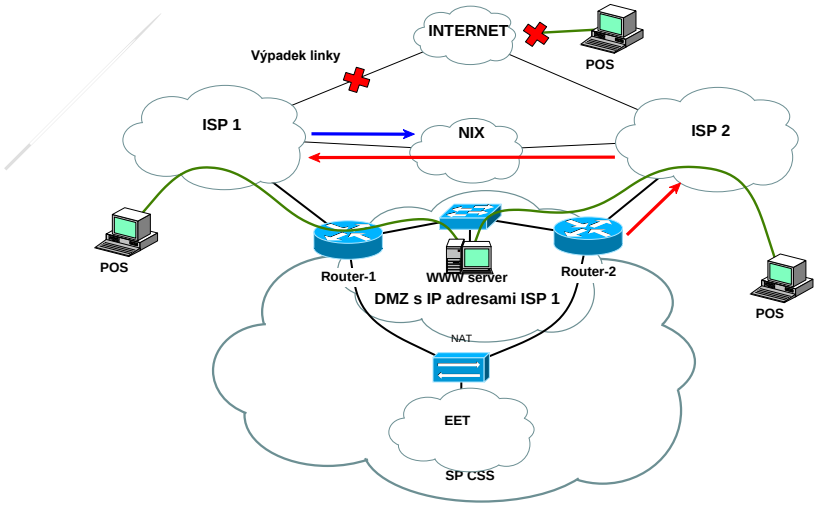
Počet adres	Počet bitů	Prefix	Maska
1	0	/32	255.255.255.255
2	1	/31	255.255.255.254
4	2	/30	255.255.255.252
8	3	/29	255.255.255.248
16	4	/28	255.255.255.240
32	5	/27	255.255.255.224
64	6	/26	255.255.255.192
128	7	/25	255.255.255.128
256	8	/24	255.255.255.0
512	9	/23	255.255.254.0
1K	10	/22	255.255.252.0
2K	11	/21	255.255.248.0
4K	12	/20	255.255.240.0
8K	13	/19	255.255.224.0
16K	14	/18	255.255.192.0
32K	15	/17	255.255.128.0

Počet adres	Počet bitů	Prefix	Maska
64K	16	/16	255.255.0.0
128K	17	/15	255.254.0.0
256K	18	/14	255.252.0.0
512K	19	/13	255.248.0.0
1M	20	/12	255.240.0.0
2M	21	/11	255.224.0.0
4M	22	/10	255.192.0.0
8M	23	/9	255.128.0.0
16M	24	/8	255.0.0.0
32M	25	/7	254.0.0.0
64M	26	/6	252.0.0.0
128M	27	/5	248.0.0.0
256M	28	/4	240.0.0.0
512M	29	/3	224.0.0.0
1024M	30	/2	192.0.0.0

Tabulka 2 : Označování velikosti adresního prostoru a směrovacího předčíslí (routing prefix)

počet bitů	Velikost přiřazeného adresního prostoru v bitech
počet adres	Množství dostupných adres při použité masce. Je však nutné mít na paměti, že normálně je počet stanic o 2 nižší, protože nejnižší a nejvyšší adresy (samé nuly, samé jedničky v části označující stanici) jsou rezervovány.
prefix	Délka směrovacího předčíslí (routing prefix) adresního prostoru.
maska	Síťová maska definující směrovací předčíslí (routing prefix) ve formě čtyř čísel oddělených tečkou.

Při dodržování pravidel a doporučení je tedy možné, v případě ztráty konektivity ISP1 do internetu, že se zákazníci nebudou moci připojit (Obrázek 40). Obdobné problémy by mohly nastat i v případě ztráty konektivity do NIXu.



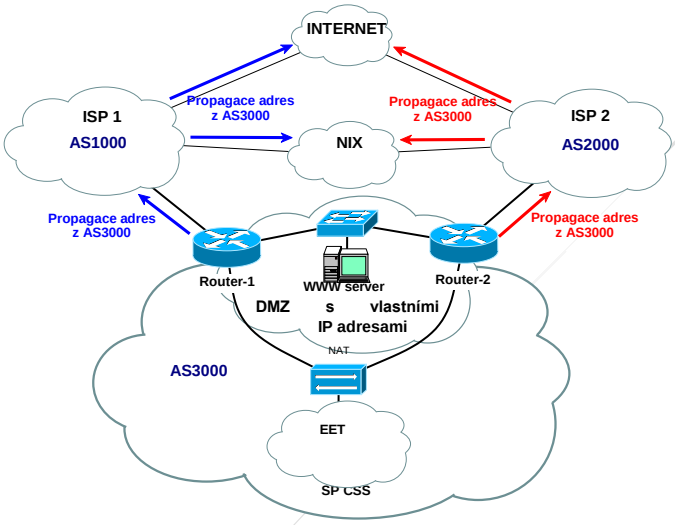
Obrázek 40 : Schéma toku dat při výpadku zahraniční konektivity ISP

Při použití této varianty je potřeba velice dobře vybírat poskytovatele, z jehož adresního prostoru budou adresy použity. Je velice žádoucí aby tento ISP měl zálohovanou konektivitu do internetu i do NIXu přes více směrovačů. Potom nebezpečí nedostupnosti serveru klesá na minimum.

V případě potřeby je možné požádat o „provider independent“ adresy, které umožní rychle změnit poskytovatele bez nutnosti přeadresování. Při přechodu stačí pouze změnit záznamy v databázích RIPE.

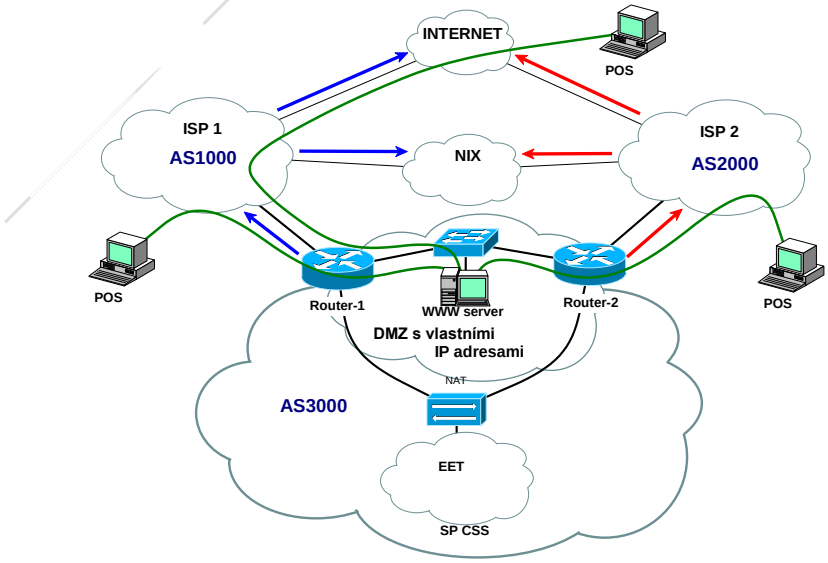
Připojení s vlastním autonomním systémem

Z hlediska technického se jeví varianta s vlastním autonomním systémem jako nejlepší. Tato varianta řeší všechny nevýhody předchozích variant. Směrovací informace jsou propagovány od všech ISP, se kterými je toto domluveno. Za všech okolností jsou dodrženy doporučení RIPE a není zapotřebí jiné nastavení směrování než je uvedeno v databázích RIPE.

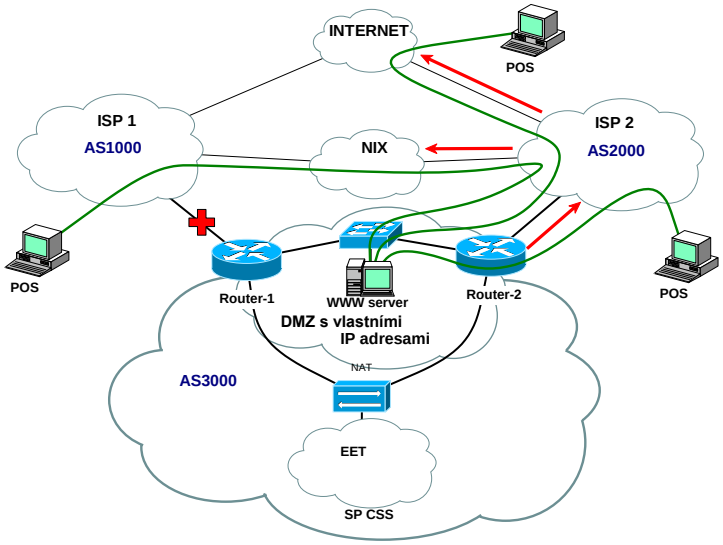


Obrázek 41 : Schéma zapojení s vlastním AS

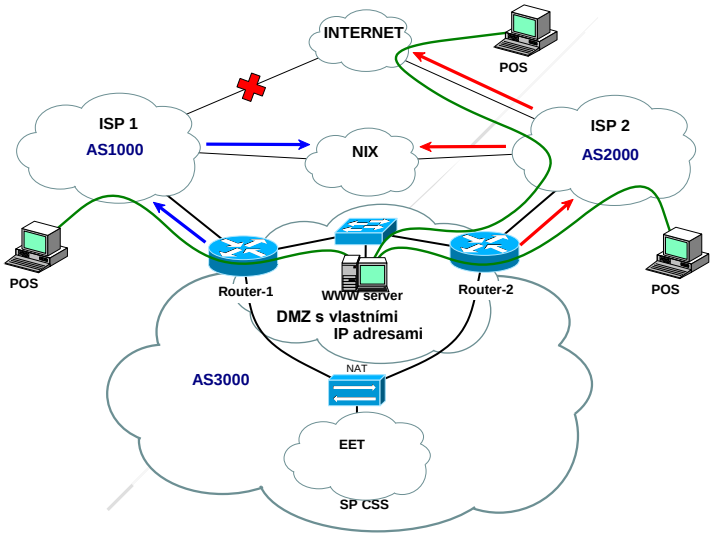
Za libovolného stavu je pro směrování provozu mezi POSem a EET hledána nejvýhodnější cesta (Obrázek 42, Obrázek 43 a Obrázek 44). Ani v případě ztráty zahraniční konektivity ISP nedojde k nedostupnosti služby EET.



Obrázek 42 : Schéma toku dat za normálního stavu sítě



Obrázek 43 : Schéma toku dat při výpadku linky k ISP



Obrázek 44 : Schéma toku dat při výpadku zahraniční konektivity ISP

Pro provozování vlastního AS je nutné podat žádost na RIPE NCC (Réseaux IP Européens Network Coordination Centre).

Tato varianta je z hlediska dodržování pravidel nesprávnější. Přináší však i některé problémy.

U menších sítí jsou přiděleny rozsahy adres jejichž samostatné směrování je doporučováno. Bohužel velcí poskytovatelé, především v USA, tato doporučení občas nerespektují a mohou nastat problémy s dostupností do těchto sítí.

Hraniční směrovače by měly mít plné směrovací tabulky. To klade vysoké nároky na paměť a výkon směrovačů. S rostoucími nároky roste cena zařízení.

Je nutné dosáhnout maximální stability hraničních směrovačů. Různé nestability mohou vést k přetěžování směrovačů. Proto má většina ISP nakonfigurovám ochranu proti „nestabilním sítím“ a v případě několikeré změny směrovacích informací v krátkém čase přestane, na nastavenou dobu, přijímat směrovací informace z těchto sítí. Po tuto dobu budou problémy s dostupností některých sítí.

Analýza rizik

Cílem řízení rizik je identifikace a specifikace jednotlivých rizik projektu včetně posouzení jejich dopadů a celkové závažnosti a vymezení vhodných opatření na prevenci daného rizika nebo omezení následků při reálném uplatnění daného rizika. Na základě identifikace a specifikace jsou následně vybraná opatření plánována v rámci projektu.

Některá identifikovaná rizika mohou být záměrně akceptována bez jakýchkoli opatření (nebo jen s omezenými opatřeními) s ohledem na přílišnou (danému riziku neadekvátní) náročnost některých opatření (zejména nároky na časové, finanční a lidské zdroje).

Řízení rizik projektu provádí průběžně Vedení řešitelských týmů a konsoliduje Vedení projektového týmu. Tuto činnost koordinuje projektový manažer tak, aby se plně prošetřila možná rizika. Zjištěná závažná rizika, jejich dopady a návrhy na jejich řešení či omezení jsou neprodleně předkládána a eskalována k posouzení a případnému rozhodnutí ŘK projektu.

Identifikace a vyhodnocení rizik a opatření přijatá pro jejich následnou eliminaci jsou obsahem následujících subkapitol.

První fází analýzy rizik je identifikace potenciálních rizik, která spočívá v zjištění a následné evidenci významných rizik. Následnou druhou fázi analýzy představuje vyhodnocení identifikovaných rizik, které je prováděno na základě hodnocení míry dopadu a pravděpodobnosti výskytu rizika.

Identifikace rizik

Jedním z významných aspektů řízení rizik je identifikace (definice) potenciálních rizik, která lze dle svého charakteru rozdělit do předem definovaných klasifikačních skupin:

A. právní rizika;
B. finanční rizika;
C. technická rizika;
D. personální rizika;
E. provozní rizika;
F. bezpečnostní rizika;
G. projektová rizika.

Následující tabulky představují výsledný seznam identifikovaných potenciálních rizik, která mohou nastat v průběhu přípravy či realizace předkládaného projektu, ale i v průběhu běžného provozu celkového projektu. Pro zvýšení přehlednosti byla jednotlivá rizika označena kódem (např. A.1, B.3, apod.).

Právní rizika		
Kód	**Riziko**	**Dopad**
A.1	Nedodržení právních norem ČR, EU.	Zpoždění projektu z důvodu nápravy stavu nebo protiprávnost části projektu a možné náhrady škody.
A.2	Neschopnost udržet legislativní shodu systému nebo jeho částí	Snížení nebo absence přínosů z důvodu nevymožitelnosti povinností poplatníků nebo kompromitace projektu samotného.
A.3	Nevhodné smluvní podmínky, např. autorské právo, sankce, náhrada škody atd.	Alternativní řešení technických a jiných projektových potřeb za zvýšenou cenu, nebo nevymožitelnost náhrady škody a sankcí.

Finanční rizika		
Kód	**Riziko**	**Dopad**
B.1	Nedostatečné údaje pro vyhodnocení předpokladů návratnosti	Nemožnost vyhodnotit projekt z finanční stránky, částečná kompromitace projektu.
B.2	Navýšení cen technologií, služeb a prací a dalších vstupů.	Zvýšení celkových nákladů projektu a zároveň zvýšení nároků na financování projektu v realizační fázi projektu.
B.3	Růst provozních nákladů v provozní fázi projektu.	Zvýšení provozní náročnosti.

Technická rizika		
Kód	**Riziko**	**Dopad**
C.1	Výběr nekvalitního dodavatele.	Ohrožení kvality výstupu projektu a prodloužení doby realizace. Riziko zvýšených nákladů (dodatečných) na nápravu stavu.
C.2	Výběr nevhodné technologie.	Ohrožení kvality výstupu projektu nebo projektu vůbec, prodloužení doby realizace. Riziko zvýšených nákladů (dodatečných) na nápravu stavu.
C.3	Riziko souvisící se zařízením (pře/poddimenzovaná kapacita / výkon)	Kompromitace projektu, neschopnost plnit legislativní povinnosti za strany státu.

Personální rizika		
Kód	**Riziko**	**Dopad**
D.1	Nedostatečná delegace kompetencí v projektovém týmu.	Neefektivní fungování projektového týmu. Ohrožení přípravy a realizace projektu či běžného provozu.
D.2	Nedostatečný vnitřní kontrolní systém.	Neefektivní fungování projektového týmu. Ohrožení realizace projektu či běžného provozu.
D.3	Nedostatek kvalifikované a kvalitní pracovní síly v provozní fázi.	Ohrožení běžného provozu.
D.4	Fluktuace zaměstnanců zapojených do provozu projektu.	Nedostatečně kvalitní personální zajištění fungování.
D.5	Závislost na specifických zaměstnancích / zaměstnancích dodavatele.	Ohrožení projektu, nebo běžného provozu. Zvýšené náklady na projekt nebo provoz.
D.6	Nedostatečné znalosti nebo potřeba specifického know-how.	Zvýšené náklady na projekt nebo provoz. Ohrožení kvalitativní úrovně projektu.

Provozní rizika		
Kód	**Riziko**	**Dopad**
E.1	Neschopnost koordinace rozvoje systému v požadovaném čase a rozsahu	Ohrožení běžného provozu.
E.2	Nenaplnění dodavatelských smluv v provozní fázi projektu.	Ohrožení běžného provozu.
E.3	Riziko spjaté s nastavením smluvního vztahu údržby a provozu systému (závislost na dodavateli)	Zvýšené náklady na provoz. Ohrožení kvalitativní úrovně provozu.

Bezpečnostní rizika		
Kód	**Riziko**	**Dopad**
F.1	Krádež technologií nebo jejich poničení.	Znemožnění provozování dané technologie, resp. nutnost její opravy.
F.2	Teroristický útok (včetně kybernetického útoku).	Ohrožení běžného provozu. Nebezpečí poničení technologií a systému. Možné ohrožení z hlediska reputace a důvěryhodnosti projektu.
F.3	Bezpečnostní rizika	Kompromitace bezpečnostních prvků; narušení bezpečnosti v oblasti dostupnosti, důvěrnosti nebo integrity dat.
F.4	Nedodržení povinností vyplývajících z legislativy, zejména zákonu o ochraně utajovaných skutečností.	Kompromitace bezpečnostních prvků; kompromitace projektu, změny projektu a zvýšené náklady. Škody značného rozsahu v případě prozrazení utajovaných skutečností.

Projektová rizika		
Kód	**Riziko**	**Dopad**
G.1	Nedostatky v projektové dokumentaci.	Může dojít k celkovému zpoždění realizace.
G.2	Neschopnost expertního zhodnocení kvality dodaných služeb (částečné přebíraní výstupů dodavatele)	Může dojít k akceptaci nekvalitního díla a služeb nebo jejich částí.
G.3	Dodatečné změny v projektu.	Dodatečné změny by mohly významně ovlivnit dobu realizace projektu a ohrozit jeho realizaci.
G.4	Špatná koordinace dodavatelských prací.	Zpoždění zahájení provozu. Riziko snížení kvality dodaných prací/služeb/technologií.
G.5	Zpochybnění validity projektu	Kompromitace projektu a nesplnění cílů projektu.
G.6	Škody z nedostatečné soutěže anebo škody spojené s reputací na základě medializovaného zpochybnění nezávislého výběru dodavatele	Zpochybnění realizátora projektu, případné opakování soutěží, nebo zpoždění projektu.
G.7	Nedodržení termínu realizace.	Zpoždění zahájení provozu. Nedosažení plánovaných přínosů. Neshoda s legislativou.

Hodnocení rizik

Druhou fází analýzy rizik je její **vyhodnocení**, které spočívá v určení **míry dopadu „D“** rizika a **pravděpodobnosti výskytu „P“** rizika. Obě veličiny jsou hodnoceny v kvalitativních bodových škálách (stupnicích) s definovaným významem jednotlivých bodů škály. Míra dopadu (vlivu) rizika „D“ a pravděpodobnost výskytu rizika „P“ jsou hodnoceny dle stupnice uvedené v následující tabulce:

Hodnota	Dopad	Pravděpodobnost výskytu	Míra dopadu/ pravděpodobnosti
1	Téměř neznatelný	Téměř nemožná	Velmi malá
2	Drobný	Výjimečně možná	Malá
3	Významný	Běžně možná	Střední
4	Velmi významný	Pravděpodobná	Vysoká
5	Nepřijatelný	Hraničící s jistotou	Velmi vysoká

Z hlediska efektivity řízení rizik je nutné pro každé riziko stanovit jeho význam (interpretovatelný jednou konkrétní hodnotou), který zahrnuje jak míru dopadu rizika, tak i pravděpodobnost jeho výskytu. Z tohoto důvodu byl pro každé riziko stanoven stupeň **významnosti rizika „V“**, který je definován jako součin bodového ohodnocení dopadu rizika „D“ a pravděpodobnosti výskytu rizika „P“.

$$V = D \times P$$

Významnost rizika „V“ lze na základě dosažitelných hodnot klasifikovat dle do 3 skupin (viz stupnice dle následující tabulky). Distribuce dosažených hodnot významnosti rizika „V“ u všech definovaných rizik je v grafické podobě zpracována formou mapy rizik (viz kapitola „Mapa rizik“).

Stupeň významnosti	Hodnota
Běžné	1 – 4
Závažné	5 – 11
Kritické	12 – 25

Pro úspěšné řízení rizik je nejdůležitější zaměřit se na rizika nejzávaznější (rizika spadající do kategorie „Kritická rizika“), která je nutné co nejdříve eliminovat nebo alespoň minimalizovat.

Cílem této podkapitoly tedy bylo vytvoření tzv. **katalogu rizik**, ve kterém jsou uvedeny hodnoty pro míru dopadu, pravděpodobnost výskytu a významnost rizik.

Následující tabulka představuje výsledný katalog rizik – souhrn potenciálních rizik, která mohou nastat v průběhu přípravy a realizace předkládaného projektu, ale i v průběhu běžného provozu.

Kód rizika	Riziko	Míra dopadu	Míra pravděp. výskytu	Stupeň významnosti
Právní rizika				
A.1	Nedodržení právních norem ČR, EU.	5	1	5
A.2	Neschopnost udržet legislativní shodu systému nebo jeho částí	5	1	3
A.3	Nevhodné smluvní podmínky, např. autorské právo, sankce, náhrada škody atd.	3	2	6
Finanční rizika				
B.1	Nedostatečné údaje pro vyhodnocení předpokladů návratnosti	1	3	3
B.2	Navýšení cen technologií, služeb a prací a dalších vstupů.	2	3	6
B.3	Růst provozních nákladů v provozní fázi projektu.	3	3	9
Technická rizika				
C.1	Výběr nekvalitního dodavatele.	3	3	9
C.2	Výběr nevhodné technologie.	4	4	16
C.3	Riziko souvisící se zařízením (pře/poddimenzovaná kapacita / výkon)	4	3	12

Kód rizika	Riziko	Míra dopadu	Míra pravděp. výskytu	Stupeň významnosti
Personální rizika				
D.1	Nedostatečná delegace kompetencí v projektovém týmu.	2	3	6
D.2	Nedostatečný vnitřní kontrolní systém.	2	2	4
D.3	Nedostatek kvalifikované a kvalitní pracovní síly v provozní fázi.	2	5	10
D.4	Fluktuace zaměstnanců zapojených do provozu projektu.	2	2	4
D.5	Závislost na specifických zaměstnancích / zaměstnancích dodavatele.	2	4	8
D.6	Nedostatečné znalosti nebo potřeba specifického know-how.	2	5	10
Provozní rizika				
E.1	Neschopnost koordinace rozvoje systému v požadovaném čase a rozsahu	3	1	3
E.2	Nenaplnění dodavatelských smluv v provozní fázi projektu.	2	2	4
E.3	Riziko spjaté s nastavením smluvního vztahu údržby a provozu systému (závislost na dodavateli)	1	5	5
Bezpečnostní rizika				
F.1	Krádež technologií nebo jejich poničení.	3	1	3
F.2	Teroristický útok (včetně kybernetického útoku).	5	2	10
F.3	Bezpečnostní rizika	3	5	15
F.4	Nedodržení povinností vyplývajících z legislativy, zejména zákonu o ochraně utajovaných skutečností.	5	2	10
Projektová rizika				
G.1	Nedostatky v projektové dokumentaci.	1	3	3
G.2	Neschopnost expertního zhodnocení kvality dodaných služeb (částkové přebíraní výstupů dodavatele)	4	3	12
G.3	Dodatečné změny v projektu.	3	5	15
G.4	Špatná koordinace dodavatelských prací.	3	3	9
G.5	Zpochybnění validity projektu	3	2	6
G.6	Škody z nedostatečné soutěže anebo škody spojené s reputací na základě medializovaného zpochybnění nezávislého výběru dodavatele	1	2	2
G.7	Nedodržení termínu realizace.	5	2	10

Mapa rizik

Mapa rizik slouží ke grafickému znázornění katalogu rizik – míry dopadu „D“, pravděpodobnosti výskytu „P“ a stupně významnosti „V“ identifikovaných rizik. Mapa rizik je promítnuta v následující tabulce, ve které je zobrazeno rozložení jednotlivých rizik do definovaných kategorií významnosti rizik. Nejvíce identifikovaných rizik spadá do kategorie „Běžná rizika. Přesto bude kladen důraz na eliminaci všech identifikovaných rizik, protože mohou v případě vzájemného souběhu negativně ovlivnit projekt.

Mapa rizik			Pravděpodobnost				
			Téměř nemožná	Výjimečně možná	Běžně možná	Pravděpodobná	Hraničící s jistotou
			1	2	3	4	5
Dopad	Nepřijatelný	5	A.1 A.2	F.2 F.4 G.7			
	Velmi významný	4			C.3 G.2	C.2	
	Významný	3	E.1 F.1	A.3 G.5	B.3 C.1 G.4		G.3F.3
	Drobný	2		D.2 D.4 E.2	B.2 D.1	D.5 D.6	D.3
	Téměř neznatelný	1		G.6	B.1 G.1		E.3

Eliminace rizik

Na analýzu rizik navazují opatření, jejichž cílem je úplná eliminace potenciálních rizik nebo alespoň jejich minimalizace do podoby, která již projekt zásadně neovlivní a neohrozí jeho průběh. Taktika řízení rizik spočívá ve výběru nejvhodnějšího postupu pro zvládání příslušného rizika. Zvládání rizika spočívá obecně ve snižování jeho dopadu anebo jeho pravděpodobnosti výskytu. Pro kritická rizika se stanovují tzv. generické taktiky k jejich zvládnutí výběrem jedné z dále uvedených metod:

- **vyloučení rizika** – zákaz vybraných rizikových aktivit a procesů;
- **snížení rizika** – snížení velikosti dopadu např. pojištěním rizika;
- **přenos rizika** – redukce rizika snížením pravděpodobnosti nežádoucích událostí;
- **přijetí rizika** – akceptace rizika na stávající úrovni bez dalších aktivit.

Volba základní taktiky vychází z disponibilních možností, jakými vůbec lze v principu snížit dopad a pravděpodobnost konkrétního rizika.

Smyslem základních taktik je především uvědomění si základního směru (resp. možnosti) pro snižování významností rizika (tj. směru zamýšleného posunu pozice rizika v mapě rizik a to prostřednictvím snižování jeho pravděpodobnosti anebo dopadu s cílem posunout „pozici“ rizika v mapě rizik co nejvíce k počátku).

Pro eliminaci identifikovaných rizik byla vždy zvolena vhodná taktika zvládání rizika, která vedla ke stanovení konkrétního opatření. Tato opatření jsou specifikována v následující tabulce „Opatření navržená pro eliminaci rizik projektu“:

Kód rizika	Riziko	Opatření vedoucí k eliminaci
Právní rizika		
A.1	Nedodržení právních norem ČR, EU.	Podrobná analýza legislativy a specifikace požadavků legislativy v úvodní fázi projektu.
A.2	Neschopnost udržet legislativní shodu systému nebo jeho částí	Průběžný monitoring změn legislativy v průběhu projektu a implementace změnového managementu.
A.3	Nevhodné smluvní podmínky, např. autorské právo, sankce, náhrada škody atd.	Návrh smluvních podmínek ze strany zadavatele a jejich ověření více právníky.
Finanční rizika		
B.1	Nedostatečné údaje pro vyhodnocení předpokladů návratnosti	Implementace metriky a systému pro vyhodnocování finančních dopadů projektu.
B.2	Navýšení cen technologií, služeb a prací a dalších vstupů.	Smluvní fixace cen za služby, standardizace technologií a otevřenost technologií, autorských práv a detailní dokumentace systémů.
B.3	Růst provozních nákladů v provozní fázi projektu.	Standardizace provozu, implementace systému řízení kvalitativní úrovně služeb provozu.

Kód rizika	Riziko	Opatření vedoucí k eliminaci
Technická rizika		
C.1	Výběr nekvalitního dodavatele.	Při výběrových řízeních bude kladen důraz na kvalitu uchazečů (realizované projekty, reference od zákazníků apod.) a nabízenou cenu. Žadatel má bohaté zkušenosti s prováděním výběrových řízení.
C.2	Výběr nevhodné technologie.	Určení kvalitativních kritérií technologií a testování technologií před / v průběhu jejich obstarání.
C.3	Riziko souvisící se zařízením (pře/poddimenzovaná kapacita / výkon)	Dimenzování podle zátěžových testů, opce na zvýšení / snížení kapacit technologií.
Personální rizika		
D.1	Nedostatečná delegace kompetencí v projektovém týmu.	Uplatnění standardní metodiky řízení projektů a definování kompetencí v projektovém týmu.
D.2	Nedostatečný vnitřní kontrolní systém.	Implementace kontrolního systému s vnějším prvkem pro nezávislost kontroly.
D.3	Nedostatek kvalifikované a kvalitní pracovní síly v provozní fázi.	Zahrnutí získání know-how pracovníků spolu s ověřením jejich znalostí do realizační fáze projektu.
D.4	Fluktuace zaměstnanců zapojených do provozu projektu.	Uplatnění struktury znalostí v týmu s redundantním výskytem znalostí.
D.5	Závislost na specifických zaměstnancích / zaměstnancích dodavatele.	Kvalitní dokumentace s podrobným popisem všech částí systémů a infrastruktury, obstarání paralelního rámce pro poskytování služeb z vnějšího prostředí, rotace pracovníků více poskytovatelů.
D.6	Nedostatečné znalosti nebo potřeba specifického know-how.	Zmapování znalostní báze a identifikace mezer v znalostech, zavedení plánu transferu / obstarání specifického know-how.
Provozní rizika		
E.1	Neschopnost koordinace rozvoje systému v požadovaném čase a rozsahu	Standardizace provozu, implementace systému řízení kvalitativní úrovně služeb provozu včetně systému řízení změn.
E.2	Nenaplnění dodavatelských smluv v provozní fázi projektu.	Standardizace provozu, implementace kontrolních mechanizmů a smluvní dohoda s náhradním poskytovatelem služeb.
E.3	Riziko spjaté s nastavením smluvního vztahu údržby a provozu systému (závislost na dodavateli)	Standardizace provozu, implementace kontrolních mechanizmů a smluvní dohoda s náhradním poskytovatelem služeb.

Kód rizika	Riziko	Opatření vedoucí k eliminaci
Bezpečnostní rizika		
F.1	Krádež technologií nebo jejich poničení.	Zajištění maximální úrovně ostrahy jak z hlediska personálního zabezpečení, tak i moderních zabezpečovacích systémů. Umístnění technologií do přiměřeného prostoru datacanetra.
F.2	Teroristický útok (včetně kybernetického útoku).	Uplatnění metodiky / standardu pro řízení bezpečnostních rizik a řízení bezpečnosti. Technická opatření pro eliminaci útoků.
F.3	Bezpečnostní rizika	Uplatnění metodiky / standardu pro řízení bezpečnostních rizik a řízení bezpečnosti. Technická opatření pro zabezpečení dostupnosti, integrity a důvěrnosti dat.
F.4	Nedodržení povinností vyplývajících z legislativy, zejména zákonu o ochraně utajovaných skutečností.	Postupování ve shodě se zákonem a příslušnými předpisy.
Projektová rizika		
G.1	Nedostatky v projektové dokumentaci.	Uplatnění standardní metodiky řízení projektů a kvalitativních kritérií na dokumentaci.
G.2	Neschopnost expertního zhodnocení kvality dodaných služeb (částkové přebíraní výstupů dodavatele)	Definice kvalitativních úrovní, jejich oponentura třetí stranou a kontrola / audit jejich uplatnění v průběhu projektu.
G.3	Dodatečné změny v projektu.	Uplatnění standardní metodiky řízení projektů a změnového řízení.
G.4	Špatná koordinace dodavatelských prací.	Uplatnění standardní metodiky řízení projektů a kontrolních mechanizmů postupu.
G.5	Zpochybnění validity projektu	Podpora prostřednictvím podporné komunikace s okolím projektu a příprava krizové komunikace - scénářů krizové komunikace.
G.6	Škody z nedostatečné soutěže anebo škody spojené s reputací na základě medializovaného zpochybnění nezávislého výběru dodavatele	Uplatnění principů transparentnosti a zákonných pravidel pro podporu soutěže v projektu nebo jeho částech.
G.7	Nedodržení termínu realizace.	Za dodržování termínu realizace (příp. etap) bude zodpovědný dodavatel, případné porušení sjednaného harmonogramu bude řešeno smluvní pokutou.

Projektové řízení a projektový tým

Pro realizaci Projektu EET je kladen velký důraz na úspěšné zvládnutí vhodných metod a nástrojů. Dobré a vžité praktiky projektového řízení se opírají především o následující zdroje:

- Norma ČSN ISO 10006 – Management jakosti – Směrnice jakosti v managementu projektu.
- Mezinárodní metodika Project Management Body of Knowledge.
- Metodiky, doporučení a Prince2.

Metodologie řízení projektu se skládá z následujících klíčových procesních oblastí, jež je nutné zásadním způsobem zvládat:

- Procesy vztahující se ke zdrojům.
- Procesy vztahující se k pracovníkům (řízení lidských zdrojů v rámci projektu).
- Procesy vztahující se k řízení vzájemných závislostí (řízení integrace projektu).
- Procesy vztahující se k záměru (řízení rozsahu prací projektu).
- Procesy vztahující se k časovým lhůtám (řízení času v rámci projektu).
- Procesy vztahující se k nákladům (řízení nákladů projektu).
- Procesy vztahující se ke komunikaci (řízení komunikace v rámci projektu).
- Procesy vztahující se k rizikům (řízení rizik projektu).
- Procesy vztahující se k nakupování (řízení obstarávání v rámci projektu).
- Procesy vztahující se ke zlepšování (řízení jakosti v rámci projektu).

Metodika řízení projektu je založena na definici organizace projektu a nastavení procesů projektového řízení. Metodika je navržena tak, aby poskytovala metodickou podporu a metodické nástroje pro:

- Řízení projektu tak, aby bylo efektivním způsobem dosaženo stanovených cílů projektu.
- Kontrolu plnění smluvních závazků a podmínek plynoucích ze Smluvních vztahů:
    - kvality, včasnosti a úplnosti plnění závazků smluvních stran,
    - identifikace případného neplnění smluvních závazků smluvními stranami,
    - identifikace zřejmých, jednoznačných a rychle aplikovatelných termínovaných postupů vedoucích k odstranění překážek plnění Smluvních závazků a k případné reflexi těchto postupů do znění Smluvní dokumentace.

Koncepce metodiky řízení projektu včetně organizace projektu vychází z následující základních prosazovaných zásad:

- **Racionálně navržená struktura orgánů řízení projektu**

  Organizační struktura projektu zahrnuje pouze nutné řídící orgány, jejichž struktura je minimalizována tak, aby mohly řádně plnit jim svěřené řídící funkce. Struktura řídících orgánů je navržena hierarchicky tak, aby se na příslušné úrovni řízení projektu nakládalo pouze s adekvátními a na nižších úrovních dostatečně předzpracovanými informacemi a tak, aby probíhaly pouze řídící činnosti, které jsou adekvátní dané úrovni řízení.

- **Racionálně navržené rozhodovací procesy**

  Rozhodovací procesy jsou navrženy takovým způsobem, aby byl minimalizován počet nutných kroků vedoucích ke konečnému rozhodování, ovšem při zachování kvality rozhodovacího procesu. V rámci rozhodovacích procesů je uplatněna zásada individuální rozhodovací odpovědnosti a zásada „rozhoduje jeden“ (ať již ve smyslu řídícího orgánu jako celku, tak jednotlivých účastníků projektu).

- **Prosazování cílené adresné odpovědnosti**

  V rámci projektu je jednoznačně určena odpovědnost jednotlivých účastníků. Jednotlivé úkoly jsou předávány k řešení těm účastníkům projektu, kteří mají předpoklady a potřebné zdroje k jejich vykonání. Provádění jednotlivých činností (plnění úkolů včetně kvality plnění) je důsledně sledováno.

- **Zajištění účelnosti a efektivity metodiky řízení projektu**

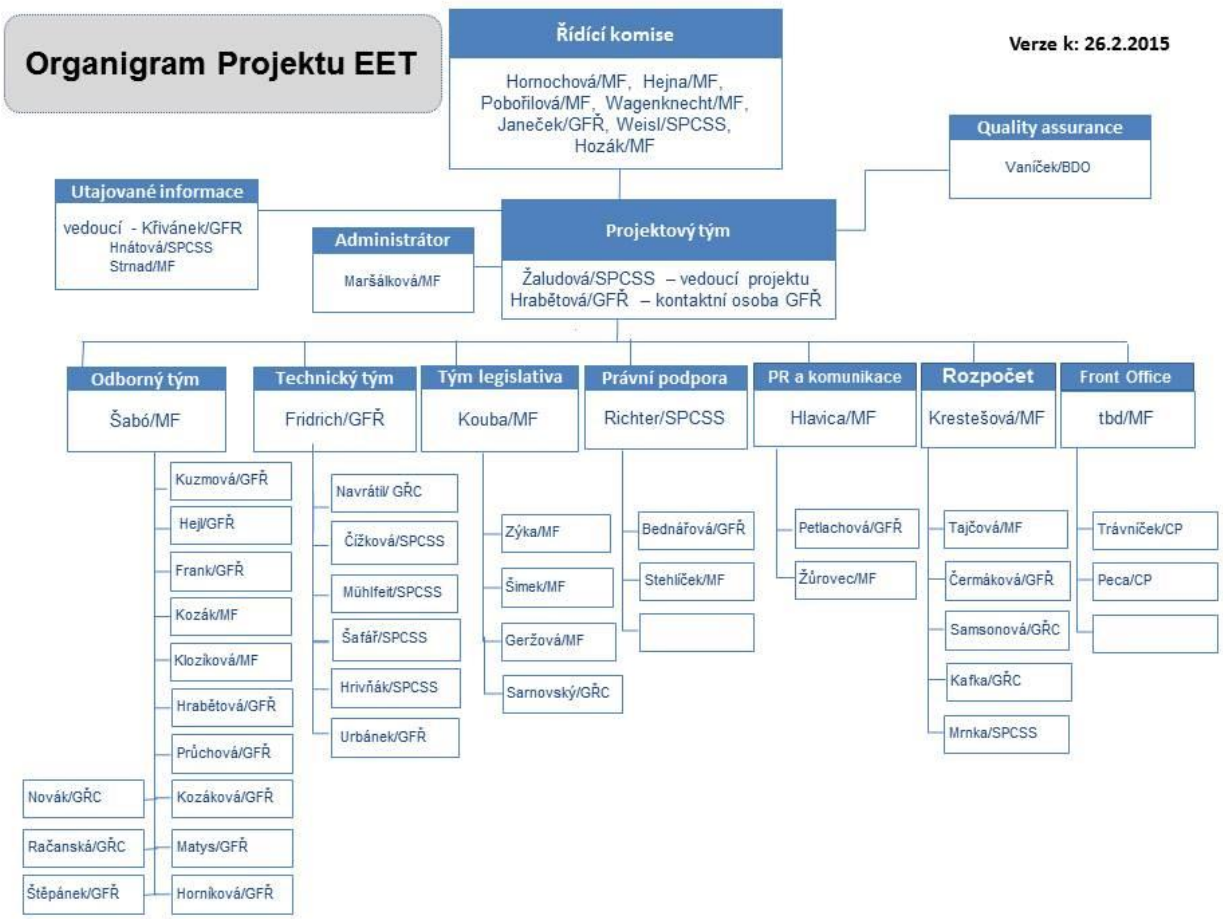
  Metodika řízení projektu není chápána staticky. V průběhu projektu, se může částečně měnit, a to vždy tak, aby vždy odpovídala aktuálnímu stavu projektu a byla účinná a efektivní při řešení aktuálních potřeb projektu včetně těch, které mohou plynout ze změny priorit projektového řízení. Soulad aktuální podoby metodiky se stavem a potřebami projektu je průběžně sledován.

Organizace Projektu

V této kapitole jsou popsány **orgány** Projektu EET z hlediska jejich **struktury a vzájemných vazeb**.

Orgány projektu

Organizační struktura Projektu EET je **graficky znázorněna** na schématu níže.



Obrázek 45: Organizační struktura projektu

Řídící komise a sponzor Projektu

Sponzor Projektu EET

Sponzorem projektu je statutární zástupce organizace, který je vybaven rozhodovací pravomocí a bude se zasazovat za realizaci projektu. Sponzor projektu především rozhoduje o způsobu financování projektu, provádí strategická rozhodnutí, která mají vliv na směřování projektu a řeší případné spory a problémy, které se nepodaří vyřešit na nižších úrovních. Sponzor projektu odpovídá především za:

- Oficiální zaštítění celého projektu.
- Řešení velkých změn projektu.
- Schvaluje výstupy projektu.

Sponzorem projektu je Ministr financí ČR.

Řídící komise

Řídící komise projektu (ŘK) má celkem **sedm členů**, předsedou komise je statutární zástupce GŘC. Jeho členy jsou zaměstnanci nejvyššího vedení MFČR a GŘC:

- Simona Hornochová
- Miroslav Hejna
- Michaela Pobořilová
- Lukáš Wagenknecht
- Martin Janeček (předseda)
- Hanuš Weisl
- Roman Hozák

Mezi hlavní úkoly ŘK patří především:

- Schvalování hlavních výstupů Projektu EET, tj. zejména Základní listiny Projektu EET, apod.
- Projednávání aktuálního stavu hlavních aktivit Projektu EET a přijímání případných zásadních rozhodnutí týkajících se Projektu, zejména schvalování podstatných změn.
- Řešení rizik a přijímání opatření k jejich eliminaci, respektive odstranění.
- Schvalování personálních změn projektového týmu a řešitelských týmů.

Řídící komise se bude v plném složení scházet minimálně **jednou za měsíc**, v případě potřeby častěji. Jednání ŘK se bude za účelem informování o aktuálním stavu Projektu účastnit rovněž projektový manažer. Projektový manažer nebude mít hlasovací právo. Konkrétní mechanismy jednání a schvalování na úrovni ŘK budou upraveny v Základní listině Projektu EET.

Seznam projektových rolí a jejich základní specifikace:

Role	Specifikace role
Zainteresovaná smluvní strana projektu	Zainteresovanou smluvní stranou se rozumí subjekt, který je v projektu přímo zastoupen a nějakým způsobem projekt přímo ovlivňuje. V tomto případě MFČR, GFŘ, GŘC, SPCSS.
Člen řídící komise	Člen řídící komise odpovídá spolu s ostatními členy řídící komise za dohled nad plněním celkového rámce projektu, zejména dohleduje projektové vedení. Člen řídící komise se podílí na rozhodování zásadních otázek a stavů projektu, které jsou mu k rozhodnutí předkládány z úrovně vedení projektu. Člen řídící komise plní úkoly uložené mu rozhodnutím řídící komise.

Vedoucí projektu/ projektového týmu	Vedoucí projektu odpovídá za vedení jemu podřízeného projektového týmu, zejména zadává úkoly a sleduje jejich plnění. Vedoucí projektu je hlavní odpovědnou osobou za projekt a je současně hlavní kontaktní osobou zajišťující komunikaci s ostatními řešitelskými projektovými týmy a řídící komisí.
Kontaktní osoba projektového týmu	Kontaktní osoba projektového týmu je hlavní odpovědnou osobou za projekt za danou zainteresovanou smluvní stranu. Zajišťuje komunikaci za svou smluvní stranu napříč mezi všemi projektovými týmy.
Členové projektového týmu	Členové projektového týmu jsou vedoucí jednotlivých řešitelských týmů a administrátor projektu. Předkládají projektovému vedoucímu výstupy za své řešitelské týmy. Jedná se o výkonnou složku projektu.
Administrátor projektu	Administrátor projektu zajišťuje některé běžné agendy projektu (např. zápisy z jednání řídící komise, zápisy z jednání projektového týmu, atp.) a zprostředkovává a zastřešuje další organizační požadavky plynoucí z projektového týmu.
Vedoucí řešitelského projektového týmu	Vedoucí řešitelského projektového týmu je zodpovědný za vedení jeho týmu. Organizuje schůzky svého týmu, zadává úkoly členům svého týmu, kontroluje plnění těchto úkolů, předkládá a zodpovídá za výstupy svého týmu směrem k projektovému vedoucímu. Každý vedoucí řešitelského týmu má povinnost delegovat svého zástupce, v případě nutnosti zastoupení při jednáních projektového týmu.
Člen řešitelského projektového	Člen řešitelského projektového týmu řádně a včas plní úkoly uložené nadřízeným vedoucím odborného týmu nebo jím pověřenou osobou. Každý člen řešitelského projektového týmu je zejména povinen neprodleně informovat nadřízeného vedoucího, nebo vedoucího projektu o skutečnostech, které mohou ohrozit projekt či naopak napomoci jeho realizaci.

Kompetence jednotlivých projektových týmů

Řídící komise Projektu EET (dále také „ŘKO“)

Řídící komise Projektu EET (dále jen ŘKO) je vrcholový řídící orgán Projektu EET, který rozhoduje o zásadních otázkách ovlivňujících směr a průběh realizace Projektu EET.

Člen ŘKO musí být vybaven potřebnými kompetencemi rozhodovat v zásadních otázkách Projektu EET, musí mít možnost alokovat potřebné projektové zdroje a musí mít možnost prosadit rozhodnutí v rámci příslušné smluvní strany.

Řídící komise Projektu je složena ze zástupců MFČR, GFŘ a SPCSS.

Na jednání ŘKO mohou být na žádost zástupců MFČR, GFŘ či zástupců SPCSS přizváni s poradním hlasem další externí odborníci nebo zástupci dalších stran participujících na realizaci Projektu.

ŘKO se schází dle potřeby tak, aby byla zabezpečena dostatečná kvalita sledování Projektu. V případě nutnosti rychlého a zásadního rozhodnutí se Řídící komise Projektu sejde v prvním možném termínu na vyžádání kterýmkoliv jejím stálým členem.

ŘKO svolává vedoucí projektu, pokud není domluveno jinak.

Kompetence ŘKO:

- Jmenuje členy ostatních týmů na návrh vedoucího projektu.
- Informuje vedení Ministerstva financí ČR o průběhu projektu; kontroluje stav a průběh projektu a vydává rozhodnutí za účelem podpory plnění cílů projektu.
- Rozhoduje o návrhu na změnu projektu (rozsah plnění, harmonogram, cena) včetně případných změn smlouvy.
- Řeší krizové situace projektu a rozhoduje o mimořádných opatřeních k jejich odstranění.

- Potvrzuje jednotlivá plnění projektu a schvaluje zahájení a ukončení projektu.
- Řídí a schvaluje součinnosti, které budou poskytnuty v rámci projektu (včetně třetích stran).
- Je eskalačním orgánem, který řeší případné spory, jež se nepodařilo vyřešit v rámci ostatních projektových týmů.

Quality assurance (QA)

Garant kvality dohlíží na všechny procesy, od návrhu, realizaci až po dokumentaci projektu. Cílem QA je dohlédnout na procesy projektu, tak aby byl projekt dokončen dle zadání a v požadovaném čase a kvalitě. Garant kvality (z BDO) je nominován dočasně a to do 27.2. 2015.

Projektový tým (PT)

Projektový tým, řeší aktuální problémy při přípravě a provozu Služeb, koordinuje činnost řešitelských týmů, které se podílejí na přípravě a realizaci služeb.

PT projednává a předkládá návrhy na optimalizaci a změnu, zpracovává zprávy o průběhu Projektu, identifikuje možná rizika, iniciuje jednání na mitigaci rizik.

PT schvaluje dokumenty, jež jsou součástí plnění, schvaluje dílčí harmonogramy jednotlivých etap Projektu.

Tým je složen ze zástupců SPCSS, MFČR a GFŘ a případně zástupců třetích stran.

Kompetence Projektového týmu

- Definuje a hodnotí požadavky na systém EET, určuje priority ve spolupráci s ostatními týmy.
- Předkládá výstupy Řídící komisi.
- Řídí a monitoruje kvalitu v průběhu všech etap projektu.
- Připravuje a projednává návrhy postupů k mitigaci rizik.
- Odpovídá za vedení aktuálního Registru rizik.
- Předkládá podklady Řídící komisi a poradě vedení (ZPV)

Odborný tým (OT)

Kompetence Odborného týmu:

- Specifikuje zadání - věcný popis fungování systému elektronické evidence tržeb z hlediska povinných subjektů a z hlediska správce daně, včetně souvisejících kontrolních postupů a udělování sankcí.
- Navrhuje a upravuje procesní postupy ve vztahu k zavedení EET ve spolupráci s ostatními týmy.
- Provádí věcné hodnocení vůči Chorvatskému modelu. Komunikuje s odbornými subjekty ze zahraničí.
- Spolupracuje také s ostatními týmy, zejména s týmem legislativy a technickým týmem, s týmem PR komunikuje propagační stránku projektu.
- Podílí se na vytvoření zadávací dokumentace pro projekt EET.
- Zodpovídá za formální i obsahovou správnost specifikace zadání

Technický tým (TT)

Kompetence Technického týmu:

- Vytváří funkční a technickou specifikaci pro zadání projektu EET.

- Provádí sběr požadavků od odborného a legislativního týmu a převádí věcné požadavky do technického řešení.
- Formalizuje požadavky a komunikuje požadavky s ostatními týmy.
- Připravuje návrh technického řešení EET.
- Připravuje podklady pro zadávací dokumentaci projektu EET.
- Zodpovídá za správnost vytvořené funkční a technické specifikace

Tým legislativa (TL)

Kompetence Týmu legislativa:

- Odpovídá za přenesení věcného řešení do legislativního textu, tj. při požadavku na regulaci, tým zváží, zda je ji třeba provádět zákonem, vyhláškou či postačí řešení v rovině metodické či správní. Pokud bude daný požadavek regulován zákonem či vyhláškou, pak je odpovědný za formulaci daného ustanovení do předmětného právního předpisu.
- Vyhodnocuje požadavky ostatních týmů zejména s ohledem na nutnost regulace zákonem, vyhláškou atd.
- Navrhuje formulace ustanovení zákona.
- Odpovídá za realizaci legislativního procesu přípravy zákona o EET, tj. realizace připomínkových řízení a procesů v rámci vlády a Parlamentu České republiky (tj. zajištění potřebné součinnosti ze strany předkladatele)
- Vede harmonogram legislativního procesu
- Zodpovídá za legislativní zachycení věcného řešení.

Tým právní a administrativní podpora (PP)

Kompetence Tým právní a administrativní podpora:

- Právní a administrativní podpora projektu, tj. organizuje přípravu pro zadání veřejných zakázek na realizaci EET včetně vedení dokumentace.
- Podílí se na vytvoření zadávací dokumentace pro projekt.
- Připravuje a vede harmonogram zadání veřejných zakázek.
- Komunikuje s dotčenými orgány (ÚOHS …).
- Zodpovídá za smluvní zajištění systému EET ve všech fázích projektu

Tým PR a komunikace (PR)

Kompetence Týmu PR a komunikace:

- Příprava strategického plánu komunikace, segmentace cílové skupiny, volba nástrojů, precizace hlavních sdělení, časový plán
- Příprava obsahu kampaně (název projektu, Corporate identity projektu, argumentář, tonalita sdělení)
- Sběr mediálně důležitých témat a informací z jednání týmů.
- Hodnotí získané informace z hlediska nutné komunikace směrem k veřejnosti či jiným zájmovým skupinám.
- Zpracovává manuál krizové dokumentace.
- Provádí analýzu mediálního obsahu.
- Navrhuje témata, která je nutné sdílet. Navrhuje postupy sdílení.
- Podporuje klíčové zaměstnance MFČR při prezentacích EET a veřejném vystupování

- Zodpovídá za komunikaci s médii a třetími stranami na podporu v médiích (on-line komunikace včetně zvláštní webové stránky)

Tým Rozpočet/controlling (RO)

Kompetence Týmu Rozpočet a controlling:

- Nastavuje a řídí rozpočet projektu a kontroluje jeho plnění ve 2 rovinách (rozpočet a controlling)
- Plánování zdrojů a řízení nákladů projektu (rozpočet)
- Příprava podkladů pro plánování zdrojů, rozpočtu a řízení nákladů projektu,
- Plánování zdrojů - určování, jaké zdroje (pracovníci, vybavení) a v jakých množstvích by měly být použity pro provedení projektových a provozních činností.
- Odhadování nákladů - stanovení přibližných nákladů potřebných k dokončení projektových a provozních činností.
- Rozpočtování nákladů – zpracování a rozdělování celkových odhadovaných nákladů mezi jednotlivé etapy projektu a provozu.
- Operativní řízení nákladů - operativní řízení změn rozpočtu projektu.
- Návrh, nastavení a zavedení systému controllingu projektu v za účelem pravidelného informování o stavu čerpání a rezerv finančních a dalších prostředků,
- Pravidelné zpracovávání výkazů čerpání rozpočtu a porovnání plánu a skutečnosti.
- Zodpovídá za řádné plnění rozpočtu

Tým Front Office (FO)

Kompetence Týmu Front Office:

- Komunikuje se zástupci a Ministerstva vnitra (ISDS, Czechpoint) a České pošty za účelem přípravy a realizace obslužných procesů EET prostřednictvím služeb ISDS (datové schránky) a kontaktních míst České pošty a Czechpoint.
- Zodpovídá za řádné a včasné zajištění procesů EET spojených s obsluhou povinných subjektů na kontaktních místech (FÚ, Česká pošta, Czech point) a prostřednictví ISDS.

Tým Utajované informace (UI)

Tým Utajované informace (UI) je složen z bezpečnostních ředitelů GFŘ a SPCSS a zástupce ředitele Odboru Bezpečnost a krizové řízení MFČR.

Kompetence Týmu Utajované informace:

- Komunikuje ve spolupráci s právním týmem s dotčenými orgány (NBÚ).
- Zodpovídá za realizaci veškeré agendy spojené s nakládáním se stávajícími utajovanými informacemi v rámci projektu EET i s těmi co vzniknou v průběhu realizace, jakož i dalšími bezpečnostními aspekty EET.
- Vede seznam poskytnutých utajovaných informací (utajovaných dokumentů), které v rámci projektu EET vznikly.
- Vede seznam pracovníků (členů projektových týmů) s přístupem k předmětným utajovaným informacím a provádí jejích poučení.
- Kontroluje nakládání s utajovanými informacemi v rámci projektu EET.

Řízení Projektu

Následující kapitoly popisují hlavní principy řízení Projektu. Detailní a aktuální specifikace řízení Projektu EET bude uvedena v **Základní listině Projektu**, která bude zpracována bezprostředně po schválení tohoto dokumentu.

Základní listina Projektu bude jasně **definovat aktivity řízení a implementace** Projektu EET, odpovědnosti a termíny plnění. Za zpracování Základní listiny Projektu a její případné změny odpovídá projektový manažer a schvaluje ji Řídící komise Projektu.

Základem metodiky řízení projektu je vyvážený a vzájemně provázaný systém procesů a postupů, jehož cílem je efektivní dosažení stanovených cílů v plánovaném rozsahu a s využitím plánovaných zdrojů. Tento systém zahrnuje následující procesní okruhy popsané dále v následujících podkapitolách:

- Řízení rizik.
- Řízení dodavatelů.
- Řízení změn.
- Kontrolu postupu projektu.
- Řízení problémů.
- Akceptační postupy.
- Komunikační strategie.
- Řízení kvality.
- Správa dokumentace.

Řízení rizik

- Hlavní **odpovědnost za řízení rizik** (monitorování a realizaci opatření k eliminaci / odstranění rizika) nese projektový manažer (PM).
- **Nástrojem pro řízení rizik** je Katalog rizik. Rizika uvedená v Katalogu budou předmětem monitorování a řízení na úrovni projektového týmu, respektive řešitelského týmu, který odpovídá za jeho eliminaci / odstranění.
- Za **identifikaci** případných dalších rizik Projektu EET jsou odpovědni všichni členové řešitelských týmů. O identifikovaném riziku, včetně návrhu nápravného opatření, je každý člen povinen informovat příslušného vedoucího týmu.
- Vedoucí řešitelského týmu **ohodnotí riziko** z hlediska jeho významnosti (tj. pravděpodobnost a dopad) a schválí navržené nápravné opatření. Pokud jde o riziko střední / vysoké významnosti, eskaluje jej na PM, který jej zařadí na nejbližší jednání projektového týmu.
- Projektový tým nově **identifikovaná rizika**, jejich významnost a návrh opatření projedná a rozhodne o začlenění do Katalogu rizik. Každému novému riziku PT následně přidělí osobu odpovědnou za sledování rizika a realizaci nápravného opatření. Nápravná opatření ve formě nepodstatných změn schvaluje PM, ve formě podstatných změn pak ŘK.
- Monitorování a řízení rizik je vždy **předmětem jednání** ŘK.

Řízení dodavatelů

- Za řízení dodavatelů odpovídá vedoucí projektového týmu. Na přípravě veřejných zakázek se budou podílet jednotlivé řešitelské týmy, každý za svojí oblast. Odpovědnost zahrnuje nastavení a kontrolu smluvních vztahů.
- Odpovědnost za **řízení změn** v rámci Projektu EET nese projektový manažer (PM).
- **„Podstatné“ změny** v Projektu na základě návrhu PM schvaluje ŘK. **„Nepodstatné“ změny** v projektu schvaluje PM a informuje na nejbližším jednání ŘK.

Řízení problémů

Cílem řízení problémů je včasná identifikace a řízené řešení faktorů (problémů), které ohrožují úspěšné dosažení cílů projektu (zejména pak lokálně jeho řádný průběh).

Na rozdíl od změny, která je řízenou (byť dodatečnou) změnou předmětu projektu či způsobu jeho realizace, může být problémem jakákoli skutečnost související s projektem, která má na jeho průběh a výsledek negativní vliv menšího i většího rozsahu.

Řešení problémů probíhá primárně uvnitř projektových týmů v pravomoci příslušného vedoucího řešitelského týmu. Vedoucí řešitelského týmu informují o problémech svého vedoucího řešitelského týmu a jejich řešení ostatní členy vedení řešitelského týmu. V případě zásadních problémů, které přesahují pravomoci vedení řešitelského týmu jsou tyto přenášeny na vedení projektového týmu a případně až na ŘK projektu.

Řešení některých problémů může vyústit do požadavku na změnu.

Identifikace problému

Kdokoliv z projektového týmu projektu může identifikovat problém. V tomto případě zašle hlášení problému (popis problému, jeho příčin, dopadů a možných řešení) elektronickou cestou nadřízenému vedoucímu řešitelského týmu.

Příslušný vedoucí řešitelského týmu potvrdí ohlašovateli elektronickou cestou přijetí hlášení problému.

Rozhodnutí o řešení problému

Vedoucí řešitelského týmu posoudí přijatý problém a je-li to třeba k řešení, konzultuje jej s vedením projektového týmu. Vyžaduje-li to situace, může být problém spolu s návrhy řešení a dalšími relevantními podklady předán vedení projektu případně následně řídící radě projektu. Následně rozhodne o způsobu řešení problému jedním z následujících způsobů:

- **Odložení problému**: neshledá-li potřebu řešit hlášený problém, pak jej uzavře.
- **Operativní řešení problému**: rozhodne-li o operativním řešení problému, pak stanoví způsob řešení včetně předpokládaných termínu a zdrojů a pověří příslušné členy řešitelského týmu úkoly a sleduje jejich plnění. Po operativním vyřešení problému uzavře tento problém s tím, že o uzavření informuje vedení projektového týmu a případně ŘK (jestliže došlo k eskalaci problému na dané úrovně).
- **Návrh na změnu**: shledá-li potřebu řešit problém formou změnového požadavku, pak připraví příslušný změnový požadavek.

Řešení problému

Problémy vedení řešitelských týmů a vedení projektového týmu sleduje nejméně s týdenní periodicitou a podle potřeby přijímá příslušná opatření. Informace o problémech a jejich řešení jsou dle závažnosti a úrovně eskalace zaznamenávány v rámci zápisů z jednání řešitelských týmů, vedení projektového týmu a ŘK.

Principy akceptace

- Akceptační řízení je činnost, která začíná protokolárním **předáním předmětu dílčího** plnění (etapy, fáze) a během které vedoucí projektového týmu a jednotlivými dodavateli ověřují, zda předaný předmět plnění odpovídá smluvním vztahům, a to prostřednictvím akceptačních kritérií a v dohodnutých lhůtách.
- Akceptační protokoly – v souladu s odevzdanými výstupy dodavatelů zajišťují vedoucí řešitelských týmů jejich vypracování a podepsání dotčenými stranami.

Reporting a monitoring

- Za průběžný monitoring Projektu na úrovni jednotlivých řešitelských týmu odpovídá **příslušný vedoucí**. Za monitoring na úrovni celého Projektu odpovídá projektový manažer. Aktuální stav realizovaných aktivit je předmětem pravidelných jednání projektového týmu. Projektový manažer pravidelně informuje o stavu Projektu ŘK.
- Etapové a **závěrečná monitorovací zpráva** – předkládá se poskytovateli po ukončení etap, respektive celkovém ukončení Projektu EET. Za zpracování zpráv odpovídá projektovému manažer, který zprávu předloží ke schválení ŘK. Po schválení je zpráva předána k podpisu statutárnímu zástupci.
- Všichni členové týmu budou povinni zpracovávat měsíční **pracovní výkazy**, které budou specifikovat počet hodin účelně strávených na realizaci Projektu (v souladu s popisem práce na Projektu) a realizovanou aktivitu. Výkaz práce je schvalován nadřízeným člena týmu.
- **Za řízení rozpočtu** Projektu a jeho aktuální čerpání odpovídá vedoucí řešitelského rozpočet a controlling. Řízení rozpočtu je předmětem jednání na úrovni projektového týmu. Změny rozpočtu schvaluje vždy projektový manažer. Tzv. podstatné změny rozpočtu musí být schváleny ŘK.

Komunikace v rámci projektu

Řídící komise

- Řídící komise Projektu se schází **minimálně jednou za měsíc**, v případě potřeby častěji. Na prvním jednání ŘK si členové zvolí předsedu.
- Jednání ŘK svolává **předseda ŘK** na podnět PM minimálně 1x za měsíc, respektive v případě eskalovaného problému. Agendu připravuje a zápis pořizuje PM Projektu EET.
- ŘK je **pravidelně informován** o aktuálním stavu a dalším vývoji v Projektu EET.
- V případě rozhodování hlasováním rozhoduje **prostá většina** hlasů, sponzor má právo veta, PM má hlas pouze poradní. Pro účely hlasování musí být přítomni členové ŘK, nebo jimi určení náhradníci. Pro zefektivnění realizace Projektu EET Základní listina Projektu dále specifikuje případy, kdy je možné hlasování / schvalování „per rollam“.
- Ze všech jednání ŘK jsou pořizovány **písemné zápisy**, které jsou archivovány v souladu s pravidly archivace.

Projektový tým

- Projektový tým se schází zpravidla **jednou za týden**, v případě potřeby častěji. Nastavení frekvence jednání bude předmětem úpravy v Základní listině Projektu.
- Jednání týmu **svolává PM**, agendu připravuje asistent PM.
- Účelem jednání projektového týmu je **zejména monitoring** stavu Projektu EET, **koordinace prací a činností řešitelských týmů**, řízení rizik, koordinace s ostatními projekty, které mají vazbu na Projekt EET, řízení změn apod.
- Ze všech jednání projektového týmu pořizuje asistent PM písemné zápisy, které jsou archivovány v souladu s pravidly archivace.

Řešitelské týmy

- Řešitelské týmy se schází zpravidla **jednou za týden**, v případě potřeby častěji. Nastavení frekvence jednání bude předmětem úpravy v Základní listině Projektu.
- Jednání týmu svolávají příslušní vedoucí řešitelských týmů.
- Účelem jednání řešitelského týmu je zejména **monitoring stavu Projektu** na úrovni týmu, **koordinace prací** a činností v rámci týmu, monitoring dodavatelských vztahů, řízení rizik, koordinace s ostatními řešitelskými týmy, apod.
- Ze všech jednání řešitelského týmu jsou pořizovány **písemné zápisy**, které jsou archivovány v souladu s pravidly archivace.

Schvalování výstupů

- ŘK schvaluje **změny v projektovém týmu**, podstatné změny v Projektu EET a monitorovací zprávy.
- PM **schvaluje výstupy** Projektu EET na úrovni projektového týmu (tzn. akceptační kritéria dílčích etap, akceptační protokoly z řešitelských týmů, nepodstatné změny v Projektu EET, návrhy podstatných změn v Projektu EET).
- Vedoucí řešitelských týmů schvalují **výstupy dodavatelů** dodané v rámci jimi věcně řízené oblasti.

Řízení kvality

Principy řízení kvality

Zajištění kvality jednotlivých klíčových výstupů projektu a projektu samotného patří mezi povinnosti vedoucích řešitelských týmů a je dohledováno manažerem kvality projektu z hlediska dodržování metodiky řízení projektu a souladu se smluvním rámcem stanoveným smlouvou o dílo. Zajišťování kvality výstupů projektu vychází ze dvou principů:

- **Zdokonalování kvality projektových postupů.**
- **Kontroly kvality klíčových výstupů projektu.**

PM společně s manažerem kvality vypracovávají plán zajišťování kvality projektu. Mezi nástroje k zajištění kontroly kvality patří:

- Osvědčený projektový postup, jehož použití je na závěr projektu (a případně i v jeho průběhu) posuzováno a který je soustavně zdokonalován.
- Pokud na úkolu pracuje více zdrojů, je stanoveno, který z nich za splnění úkolu zodpovídá a role/úloha ostatních zdrojů.
- Projektový postup obsahuje na závěr jednotlivých kroků úkoly spočívající v posouzení zpracovaných výstupů, přičemž podle možností jsou k těmto úkolům přiřazeny zdroje, které nezpracovávaly posuzované výstupy.
- Vytvoření katalogu požadavků na systém a ověření, že splnění těchto požadavků je ověřitelné.
- Zapojení uživatelů do kontroly kvality (posuzování návrhů uživatelského rozhraní, akceptační testování).
- Provedená posouzení kvality produktů jsou dokumentována (kdo kontroloval, co kontroloval, s jakým výsledkem).
- Produkty, u kterých byly zjištěny nedostatky, jsou zadány k úpravě a odstranění a těchto nedostatků je kontrolováno.
- Určování příčin zjištěných chyb a zapracování preventivních činností do projektového postupu.
- Při zadání úkolu jen vždy specifikován požadovaný výstup a kriteria pro posouzení jeho kvality, specifikaci kriterií kvality stanovuje PM nebo jím pověřený zdroj (zejména o produktů výkonné části projektu).
- Před zahájením testování je zpracovávána specifikace testovacích případů pro jednotlivé úrovně testování.

Kontroly kvality

V rámci řízení kvality se uplatňují vedle sebe pravidelné (povinné) a nepravidelné (nepovinné) kontroly kvality.

Pravidelné kontroly

Pravidelné kontroly jsou prováděny v následujících termínech a rozsahu dle stanoveného schématu:

Dodržování projektového plánu	
Metoda:	Monitorování a sledování Plánu projektu. Informování o stavu projektu včetně hlášení výrazných projektových odchylek.
Odpovídá:	PM.
Četnost:	Kontinuálně, formálně minimálně jedenkrát týdně.
Cíl:	Dodržet všechny plánované milníky realizace.

Shoda výstupů se specifikací	
Metoda:	Ověření, zda výstup splňuje všechna kvalitativní a kvantitativní akceptační kritéria formou akceptace či dílčí kontroly.
Odpovídá:	PT a subjekty definované v Akceptačních kritériích.
Četnost:	Při akceptačním řízení.
Cíl:	Dodržet kritéria kvality realizace Projektu.

Projektová dokumentace	
Metoda:	Ověřit kompletnost projektové dokumentace dle požadavků Metodiky.
Odpovídá:	PT.
Četnost:	Průběžně minimálně jedenkrát týdně a při ukončení hlavních částí projektu.
Cíl:	Zajistit auditovatelnost realizace projektu.

Nepravidelné kontroly

Nepravidelné kontroly mohou být provedeny podle potřeby kdykoliv v průběhu projektu. Provedení kontroly iniciují PM nebo ŘK. Kontrolu kvality dokumentace, průběhu realizace a výstupů projektu provádí určený PM ve spolupráci s manažerem kvality projektu nebo manažer kvality sám a dle potřeby se účastní kterýkoliv účastník projektu. Pokud jsou při kontrole kvality shledány nedostatky, stanoví se přiměřené lhůty k jejich odstranění. Za odstranění těchto nedostatků odpovídá určení PM.

- **Kontrola vedení projektu**
  Formální kontrola, které se účastní zástupci liniového řízení MFČR, GFŘ, GŘC, SPCSS (včetně např. zástupců příslušných organizačních jednotek). Provedení kontroly je vedeno PM, výsledky kontroly jsou schváleny ŘK.
- **Kontrola Vedoucích řešitelských týmů**
  Kontrola kvality, prováděná manažerem kvality.
- **Kontrola člena týmu**
  Kontroly kvality na úrovni řešitelských týmů jsou prováděny formou pracovních jednání/workshopů či tzv. distribučním způsobem. Při těchto kontrolách, zpracovávají připomínky k předloženým výstupům ostatní členové PT, s odpovídajícími zkušenostmi a dovednostmi ve vztahu k revidovanému výstupu.
- **Kontrola sebe sama**
  Autor a/nebo vlastník výstupu sám provádí kontrolu výsledků své práce, v průběhu realizace i před předáním.

Ověřování požadavků a návrhu

Součástí procedur zajištění kvality je také prosazování řádného ověřování požadavků a návrhu, jehož cílem je omezení projektových rizik, která plynou z realizace částí projektu na základě chybných či neúplných vstupních požadavků nebo na základě návrhu, který by stanovené požadavky nerespektoval.

Veškeré požadavky musí vycházet z primárních požadavků definovaných v základním dokumentu projektu s tím, že je pouze vhodně upřesňují či doplňují, musí být specifikovány a odsouhlaseny kvalifikovanými subjekty a dále prověřeny. Tento cíl je zajištěn řízeným procesem konzultací / interview aplikací následujících kroků:

- PM stanoví požadavky a strukturu konzultací / interview, zvolí vhodné osoby pro jednotlivé konzultace / interview (respondenty) a naplánují konzultace / interview.
- Určení pracovníci provedou dle plánu jednotlivé konzultace / interview a zdokumentují je v podobě záznamů typu Zpráva / Zápis z jednání / Zápis interview, které jsou potvrzeny jednotlivými respondenty a prověřeny PM, případně dalšími jím určenými osobami.
- Je-li třeba, jsou po dohodě provedeny další doplňující konzultace / interview.

Veškeré návrhy částí díla musí vycházet z požadavků Smlouvy a z požadavků získaných v rámci konzultací / interview tak, aby splňovaly příslušné záměry projektu. Tohoto cíle je dosaženo řízeným procesem přípravy návrhu, v rámci kterého:

- Dodavatel musí písemně předkládat PT veškeré nové nebo zpřesňující návrhy řešení.
- PT musí zajistit řádné připomínkové řízení předložených návrhů a předat připomínky k zapracování.
- Po zapracování všech připomínek musí být návrh schválen na úrovni PT (případně na vyšší úrovni projektového týmu vyžaduje-li to jeho povaha).

Ověřování výstupů projektu

Cílem ověřování výstupů projektu je zajistit předání díla jak v jednotlivých částech tak vcelku v podobě a kvalitě, která je plně v souladu s požadavky základního dokumentu projektu a s požadavky a návrhy specifikovanými a odsouhlasenými v průběhu projektu.

Správa a dokumentace projektu

V této části Metodiky řízení projektu stanoví základní pravidla nakládání a správy dokumentace projektu.

Kategorie dokumentace

Dokumentace projektu je členěna na následně vymezené kategorie:

- **Řízená dokumentace projektu:**
  Řízenou dokumentací projektu je veškerá dokumentace vyžadovaná smluvní dokumentací nebo metodikou řízení projektu, dokumentace sledovaná na úrovni vedoucích ŘT případně další dokumentace určená na úrovni PT. Jedná se nejen o výstupy projektu, ale také o důležitou podkladovou dokumentaci.
- **Pracovní dokumentace projektu:**
  Pracovní dokumentací projektu je veškerá dokumentace či materiály zpracovávané účastníky projektu v rámci jim přidělených úkolů či přímo sloužící k plnění těchto úkolů včetně dokumentace jako jsou podklady.
- **Specifická dokumentace projektu:**
  Specifickou dokumentací projektu je veškerá dokumentace či materiály zpracovávané v rámci projektu, se kterými, vzhledem k jejich charakteru, nelze nakládat výše uvedeným způsobem. Jedná se zejména o databáze, vytvářený programový kód a konfigurace.

Značení dokumentace

Pravidla značení dokumentace se vztahují na řízenou dokumentaci projektu s tím, že by měla být dodržována také pro zbývající typy dokumentace tam, kde je to možné. Značení (identifikace) jednotlivých dokumentů má základní strukturu **Identifikator_Verze.Pripona**, kde jednotlivé části identifikace mají následující význam:

- **Identifikátor**: identifikační řetězec dokumentu ve tvaru **NavestiUpresneniDoplnek** tvořený:
  - **návěštím a upřesněním**: specifické řetězce, které charakterizující typ dokumentu,
  - **doplňkem:** obecný text únosné délky dle uvážení autora dokumentu, který slouží ke zlepšení vypovídací hodnoty názvu souboru
- **Verze**: řetězec zajišťující přehled o verzování dokumentu na úrovni názvu dokumentu (pokud má verzování smysl). Verze je standardně uváděna ve tvaru vNN.NN (např. v01.02). V některých případech – např. pracovních meziverzí v rámci pracovní dokumentace lze užívat vhodná rozšíření (např. v01.02a).
- **Přípona**: řetězec dány typem souboru a vázány především na používané programové vybavení (např. doc, xls, txt).

V rámci identifikace dokumentů (návěští, upřesnění, doplňku) smí být užíváno výhradně:

- velkých a malých písmen bez diakritiky
- číslic 0 až 9
- speciálních znaků „_“ a „-“

Je-li předán podklad projektu s daným názvem (např. z externích zdrojů, pak je s ním nakládáno s jeho původní identifikací.

Podrobnější informace o značení jednotlivých hlavních typů dokumentů je uveden v následující tabulce:

Popis	Návěští	Upřesnění	Doplněk	Verze	Příklad
Obecný dokument na který nepatří do žádné z dále uvedených skupin			DleUvážení	_vNN.NN	Obecny_dokument_v01.02
Šablona dokumentu	Sab		_DleUvážení	_ vNN.NN	Sab_priklad_v00.01
Zpráva o stavu projektu	ZoS	-XX		_ vNN.NN	ZoS-03_v00.01
Zápis z jednání vedoucích projektu číslo NN ze dne dd.mm.rrrr	ZJ	-VP-XX_rrrrmmdd		_ vNN.NN	ZJ-VP-06_20090202_v01.00
Zápis z jednání Řídící rady číslo NN ze dne dd.mm.rrrr	ZJ	-RR-XX_ rrrrmmdd		_ vNN.NN	ZJ-RR-02_20090202_v01.00
Zápis z jednání - ostatní číslo NN ze dne dd.mm.rrrr	ZJ	-Os_ rrrrmmdd	_DleUvážení	_ vNN.NN	ZJ-Os_20090202_Pom_v01.00
Zápis interview ze dne dd.mm.rrrr	ZIn	_ rrrrmmdd	_DleUvážení	_ vNN.NN	ZIn_20090202_Modul_v00.12
Zpráva ze dne dd.mm.rrrr	Zpr	_ rrrrmmdd	_DleUvážení	_ vNN.NN	Zpr_20090202_Info_v01.00
Změnový požadavek číslo Z-XXXXX	Z	-XXXXX		_ vNN.NN	Z-00047_v01.02
Akceptační kritéria k akceptaci číslo XX	AK	-XX	_DleUvážení	_ vNN.NN	AK-05_Ucetnictvi_v00.25
Akceptační protokol k akceptaci číslo XX (dle akceptačních kritérií)	AP	-XX	_DleUvážení	_ vNN.NN	AP-05_Ucetnictvi_v01.00
Závěrečný akceptační protokol	AP-Z			_ vNN.NN	APZ_v01.00

Tabulka 3: Značení jednotlivých hlavních typů dokumentů

Nakládání s dokumentací

Pro nakládání s dokumentací jsou stanovena dle vymezených kategorií dokumentace následující zásady:

- **Řízená dokumentace projektu:**

Řízená dokumentace projektu podléhá řízenému zpracování, verzování, předávání, uložení na určeném řízeném zdroji, zálohování, evidenci a řízení přístupu.

- **Pracovní dokumentace projektu:**
  Pracovní dokumentace projektu podléhá pravidelnému ukládání na určeném zdroji pracovní dokumentace, zálohování a řízení přístupu.

  Účastníci projektu odpovídají za údržbu své pracovní dokumentace na zdroji pracovní dokumentace v souladu s pokyny příslušného vedoucího projektového týmu v takovém stavu, aby tato dokumentace mohla být dále použita v případě nepřítomnosti účastníka nebo při poškození či ztrátě dokumentace na jiných zdrojích (např. lokální pracovní stanice).

- **Specifická dokumentace projektu:**
  Specifická dokumentace projektu podléhá minimálně pravidelnému zálohování a řízení přístupu. Dále může být žádoucí verzování a další opatření. Veškerá opatření jsou určována a zajišťována specificky dle charakteru dokumentace určenými účastníky projektu.

Účtenková loterie

Jedním z podpůrných nástrojů může být účtenková loterie. Základním účelem loterie je zvýšení známosti systému EET mezi spotřebiteli a podpora občanů – spotřebitelů při implementaci projektu (zavedení elektronické evidence tržeb) a identifikace poplatníků.

Účtenková loterie nebyla v žádné zemi organizována na obdobné podmínky, zejména způsob fiskalizace. Východiska z jiných zemí však mohou posloužit jako ilustrační a pomoci identifikovat klíčové vlastnosti možné loterie v České republice.

V případě loterie na Tchaj-wan šlo de facto o číselnou loterii, kde byla losována výherní čísla (koncovky) čísel účtenek. Účtenky bylo potřebné zaregistrovat jenom v případě výhry. Výhry byly odstupňovány podle počtu čísel (čtyřčíslí bylo nejmenší a šestičíslí nejvyšší z hlediska výhry). Nevýhodou byla náhodnost a možnost obchodníků generovat čísla účtenek z falešných pokladnic s nepravděpodobnými koncovkami, např. všechny stejné číslo 9999 apod.

Loterie v Slovenské republice byla postavena na principu registrované účtenky, kde podstatným registračním a odlišovacím znakem byli čísla registračních pokladen. Registrované účtenky, resp. čísla pokladen, byly porovnávány vůči databázi registračních pokladen a v případě chybného / neexistujícího čísla nebylo možné účtenku zaregistrovat. Bylo možné nahlásit špatně vystavenou účtenku, to však už nebylo odměněno šancí získat nějakou výhru. Z těchto důvodů byly registrovány zejména účtenky z obchodních řetězců, které však nebyly cílovou skupinou pro odhalování podvodných pokladen.

Z výše uvedených zkušeností vyplývá, že je vhodné orientovat účtenkovou loterii na oblast odhalování špatně vystavených účtenek..

Je možné předpokládat následující základní scénáře pro eventuální okruhy slosovatelných účtenek v rámci specifických „sub loterií“:

1. Účtenka je validní – obsahuje číslo účtenky poplatníka a i správný fiskální identifikační kód.
2. Účtenka může být validní, ale neobsahuje fiskální identifikační kód
3. Účtenka obsahuje nesprávný (falešný) fiskální identifikační kód
4. Účtenka obsahuje jiné nesprávné údaje (např. název poplatníka, datum, ičo nebo hodnotu DPH apod.)

Pozn.: Scénář nevydání účtenky vůbec není vzat v úvahu.

Ověření účtenky i její registrace by měla být co nejjednodušší. V naprosté většině případů bude postačovat jako první krok validace fiskálního identifikačního kódu. Po jeho validaci by měli být poskytnuty ověřovateli i doplňkové údaje jako jsou název poplatníka, nebo provozovny, datum a čas.

V případě negativního ověření, by měla být možnost registrace i této účtenky, minimálně pro kontrolní účely.

Právě účtenky, které nejsou validní, by mohly být zařazeny do slosování samostatně (čímž se dramaticky zvýší pravděpodobnost výhry) nebo uplatnit na ně nějaký bonus – žolíka.

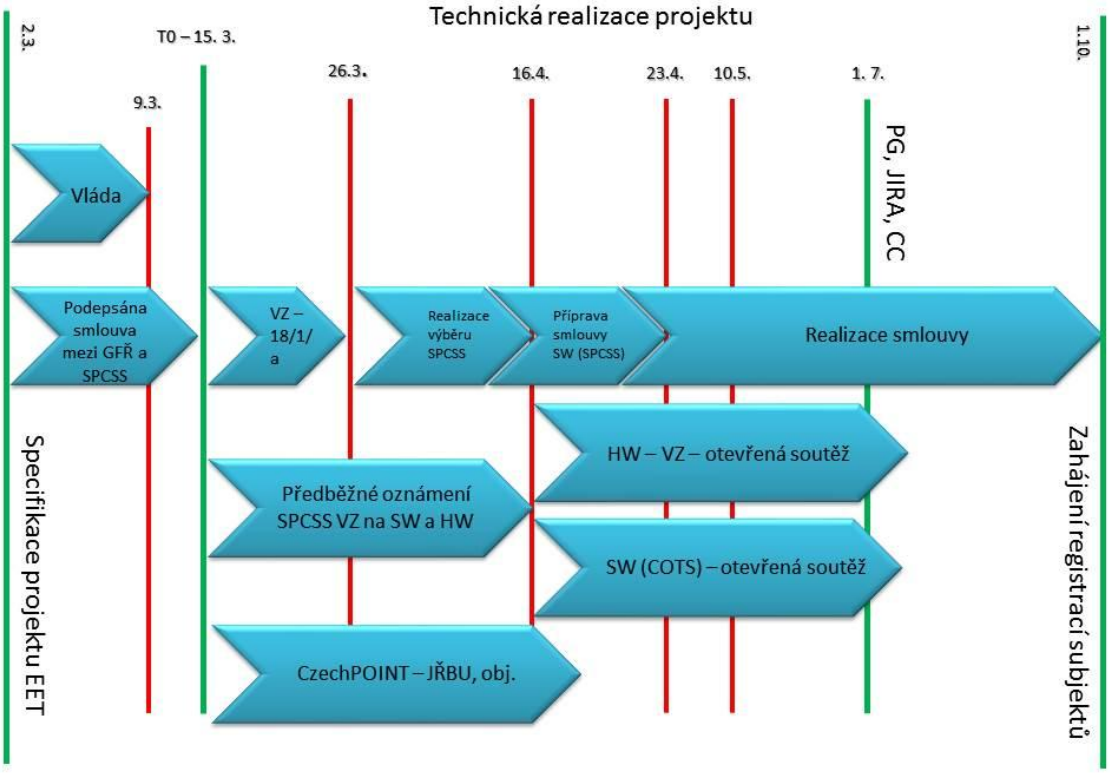
Např. účtenky, které nemají fiskální identifikační kód a budou slosovány, mohou mít několikanásobnou výhru. Nebo účtenky, které mají fiskální identifikační kód, ale není validní, tj. je falešný, by mohli být zařazeny do samostatného slosování.

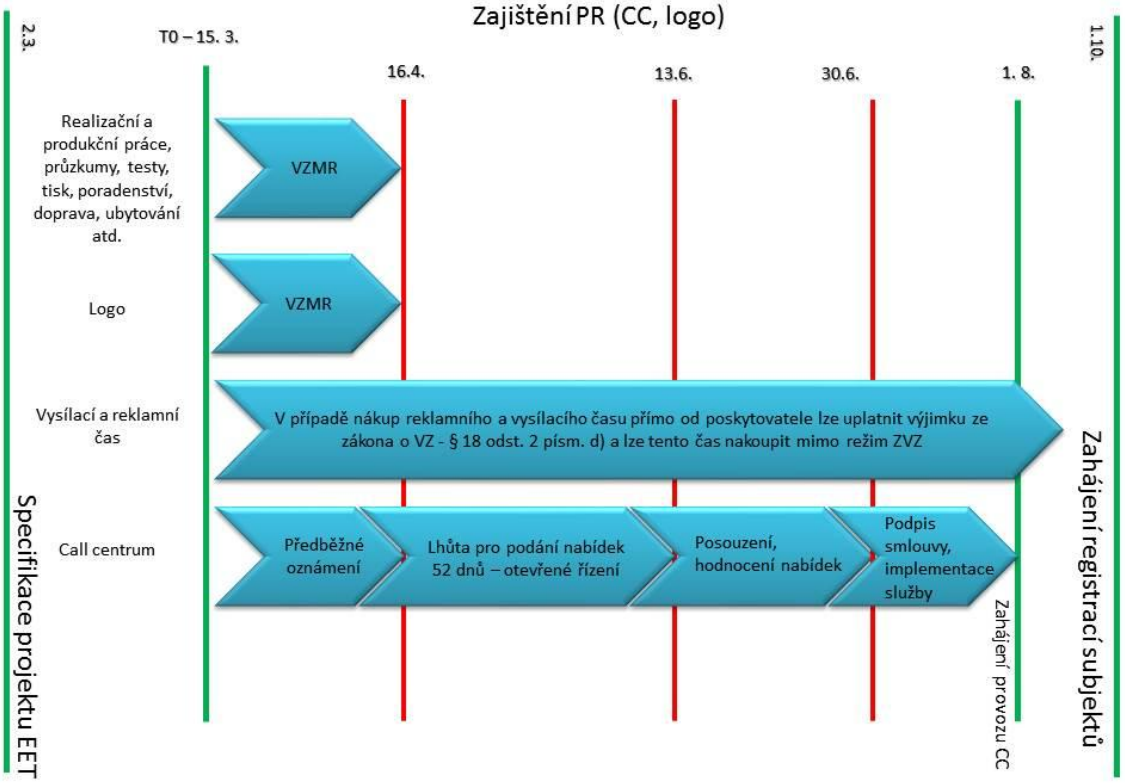
Preferováním neúplných nebo nevalidních účtenek je možno dosáhnout zvýšeného zájmu na získání právě těchto účtenek a tím vyhledávaní provozoven, které jsou více rizikové.

Je potřeba zvážit riziko falšování účtenek soutěžícími? Jde vlastně o jakýsi los, který ovšem nemá žádné ochranné prvky. Falšovat účtenky, kde je něco špatně nebo údaje chybí, je asi to nejjednodušší. Natisknu si libovolný počet účtenek, které nepůjdou žádným způsobem zkontrolovat (budou obsahovat falešné údaje, případně bude chybět údaj o obchodníkovi). Z pohledu výše uvedeného je ovšem taková účtenka vlastně nejcennější a mám šanci získat žolíka.

Účtenky, které nepůjdou ztotožnit s konkrétním dohledatelným obchodníkem, by neměly být do slosování zařazeny. Otázka je, zda a za jakých podmínek jsme schopni všechny účtenky kontrolovat.

Harmonogram projektu





Analýza přínosů a nákladů

Analýza přínosů a nákladů je strukturována jako jednoduchá projekce nákladů a přínosů v čase. Některé obvyklé aspekty jako hodnota projektu nebo projekce rizik v čase nebyly do analýzy zahrnuty.

Důvodem použití jednoduchého modelu byl zřejmý převis přínosů na d náklady, kde jsou přínosy řádově vyšší než náklady. Nejedná se tudíž o standardní projekt, u kterého by rozhodování o projektu záviselo na výsledku analýzy nákladů a přínosů.

Uvedení výčtu přínosů a také nákladů však považujeme za důležité z hlediska získání přehledu o přínosech a nákladech a jejich struktuře.

Přínosy

Identifikace přínosů

Identifikace přínosů počítá jenom s jedním přínosem a to zlepšením výběru daní. Ostatní efekty, jako např. kultivace podnikatelského prostředí, snižování negativních efektů šedé ekonomiky apod. nejsou kvantifikovány.

U hlavního přínosu, vyšších příjmů z daní, byla realizována kvantifikace přínosu dvěma metodami. S ohledem na charakter kvantifikace (kvantum jsou samotné peněžní prostředky), se jedná de facto o přímou monetarizaci přínosů.

Kvantifikace byla prostřednictvím metod:

- Kvantifikací přínosu prostřednictvím snížení podílu šedé ekonomiky, a
- Kvantifikací přínosu prostřednictvím snížení odchylky ve výběru daní, tzv. VAT Gap.

Kvantifikace přes šedou ekonomiku

Friedrich Schneider: „Size and Development of the Shadow Economy of 31 European and 5 other OECD Countries from 2003 to 2013“

15,5% HDP[11] za rok 2013, což představuje 596 mld. Kč. Pokles šedé ekonomiky byl v letech 2003 – 2013 cca 6% ročně.

Rozsah šedé ekonomiky není rovnoměrný, ale v jednotlivých odvětvích se liší. Největší podíl (až 25 – 35% z celé produkce) je v sektoru stavebnictví a téměř žádný v hornictví, bankovních službách a distribuci elektřiny. Ostatní sektory jsou nad 10% z celkové produkci v sektorech.

Podle statistického úřadu čtyři sektory, u kterých je podíl šedé ekonomiky nadprůměrný, mají podíl více než 31% na celkovém HDP.

Stavebnictví	7,4%
Obchod, opravy motorových vozidel a spotřební zboží	11,8%
Pohostinství a ubytování	1,9%
Doprava, skladování, pošty a telekomunikace	10,5%

Dá se předpokládat, že **šedá ekonomika u těchto sektorů je více než 200 mld**.

Samozřejmě, potřeba vzít v úvahu i jiné odvětví, jako jsou služby, zemědělství, výroba - zejména spotřebního zboží atd. Z tohoto důvodu byla jako základ pro výpočet odhadnuta hodnota 400 mld. šedé ekonomiky zasažené projektem EET.

[11] 3 845,93 mld. Kč za rok 2013

Propočet předpokládaných příjmů prostřednictvím potlačení šedé ekonomiky je vztaženo na % snížení celkové šedé ekonomiky následovně:

Scénář	**pesimistický**	**konzervativní**	**optimistický**
% transferu šedé ekonomiky	1 %	3 %	5 %
přínos (navýšené daně)	4 mld. Kč	12 mld. Kč	20 mld. Kč

Kvantifikace VAT GAP

Byl použit propočet podle studie Evropské komise „Study to quantify and analyse the VAT Gap in the EU-27 Member States“ [12]; konkrétně poměr („Household consumption VAT Liability“ k „Total VTTL“) a k „VAT Revenues“.

Jedná se tedy o předpokládaný podíl domácností na celkové daňové mezeře vypočtený jako podíl spotřeby domácností (61,7%) na daňové mezeře DPH (3,267 mld. Euro – 84,9 mld. Kč).

Samozřejmě, projekce dokonalého potlačení mezery je nereálná a v nejlepším státě EU (Holansko, Finsko) představuje 5%. Dosažení mediánu zemí EÚ (15%) je pro účely odhadu přiměřené jako maximální dosažitelná hodnota. Za rok 2012 byla hodnota daňové mezery DPH 22%. To zmanená, že v celkovém vyjádření by byla maximální dosažitelná hodnota 27 mld. Kč.

Dosažení této hodnoty jsme odhadli rozloženě v čase na následujících hodnotách v jednotlivých letech:

	2016	2017	2018	2019 - 2021	2022 - 2024
% z předpokládané maximální dosažené hodnoty	10%	25%	40%	50%	60%
suma	2,7 mld.	6,75 mld.	10,8 mld.	13,5 mld.	16,2 mld.

Z obou metod vychází střednědobě objem dosažitelných přínosů 10 – 15 mld. Kč. Pro účely projekce přínosů v čase a srovnání s náklady byla použita hodnota **12 mld. Kč**.

[12] http://ec.europa.eu/taxation_customs/resources/documents/common/publications/studies/vat-gap.pdf

Náklady

Iniciační náklady:

Rozpočet investiční fáze projektu ELEKTRONICKÁ EVIDENCE TRŽEB

Náklady investiční fáze projektu 390 907 355 Kč

Termín realizace investiční fáze 1.1.2015 - 31.12.2015

Název položky	Odhadovaný náklad v Kč*	Organizace	Projektový tým	Způsob objednávky	Datum dodávky
Poradenství, konzultace	241 879	MF	Projektový	Přímá objednávka	1. 2. 2015
Poradenství PR a komunikace	1 500 000	MF	Projektový	Veřejná soutěž	2/15 -4/16
Externí právní poradenství, právní zastoupení	1 500 000	FS	Právní a admin. podpora	Veřejná soutěž	Trvale
Znalecké posudky	300 000	FS	Právní a admin. podpora	Veřejná soutěž	Trvale
Implementace pilot	7 086 776	SPCSS	Technický		7-12/2015
Správní poplatky, soudní poplatky	100 000	FS	Právní a admin. podpora	Rozpočet	Trvale
Kreativní agentura	2 000 000	FS	PR a komunikace	Veřejná soutěž	3/15 -9/16
Realizační a produkční práce	2 000 000	FS	PR a komunikace	VS a objednávka	4/15 - 9/16
Nákup medií přes agenturu	12 000 000	FS	PR a komunikace	Veřejná soutěž	8/15 - 9/16
Nákup medií napřímo	1 000 000	FS	PR a komunikace	Objednávka	8/15 - 9/16
Průzkumy a testy	500 000	FS	PR a komunikace	Objednávka	2/15 -12/16
Tisky a výroba 3D	1 000 000	FS	PR a komunikace	VS a objednávka	5/15 - 10/16
Ostatní náklady	500 000	FS	PR a komunikace	Objednávka	2/15 - 10/16
Osobní vozidla	3 500 000	FS	Odborný	VS, smlouvy	1. 1. 2016
Vzdělávání, vstupní příprava	175 000	FS	Odborný	VS, objednávka v limitu	1. 1. 2016
Ostatní věcné výdaje mimo programy	4 825 000	FS	Odborný	Objednávky, smlouvy	1. 1. 2016
Jednorázové výdaje ICT (vybavení nových zaměstnanců)	16 500 000	FS	Odborný	Objednávky, smlouvy	1. 1. 2016
Osobní vozidla	2 800 000	CS	Odborný	Veřejná soutěž	1. 1. 2016
Mobilní kanceláře	8 000 000	CS	Odborný	Veřejná soutěž	1. 1. 2016
Vystrojení	3 044 200	CS	Odborný	Pokryto rámcovými smlouvami	1. 1. 2016
Technické prostředky	818 500	CS	Odborný	Veřejná soutěž	1. 1. 2016
Informační technologie:	2 845 000	CS	Odborný	Veřejná soutěž	1. 1. 2016
				Rámcová smlouva CS	1. 1. 2016
					1. 1. 2016

Z toho: 80 chytrých telefonů 40 notebooků 40 přenosných tiskáren + 8x multifunkční tiskárna do mobilní kanceláře				VS - centrální zadávání MF VS - centrální zadávání MF	1. 1. 2016
Vybavení pracoviště	960 000	CS	Odborný	VS - centrální zadávání MF	1. 1. 2016
Vybavení pracoviště	720 000	CS	Odborný	VS - centrální zadávání MF	1. 1. 2016
Vzdělávání, vstupní příprava	2 365 000	CS	Odborný	Bez VS	1. 1. 2016
Výzbroj	1 050 000	CS	Odborný	Veřejná soutěž	1. 1. 2016
Call centrum	2 000 000	FS	Front office		15. 10 .2015
Nastavení systémů ČP, procesní ICT	10 000 000	FS	Front office	Objednávka ČP	1. 6. 2015
Nastavení Call centra ČP Brno	1 500 000	FS	Front office	Objednávka ČP	1. 6. 2015
Personální náklady na 2FTE	2 400 000	FS	Front office	Objednávka ČP	1. 3. 2015
Mzdové náklady na 1 FTE	1 800 000	SPCSS	Front office	Existující smlouva	1. 3. 2015
Realizace komunikace (NIX)	24 200 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
Certifikační autorita EET	14 520 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
Frontend vrstva	63 283 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
Aplikační a DB vrstva	8 228 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
Storage a zálohování	145 200 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
ESB	4 235 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
Service desk	1 210 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
Aplikace EET (SW)	27 000 000	FS	Technický	Veřejná soutěž	1. 11. 2015
Úpravy ADIS	8 000 000	FS	Technický	JŘBÚ	1. 11. 2015
CELKEM	**390 907 355**				

*včetně DPH

Provozní náklady:

Rozpočet provozní fáze projektu ELEKTRONICKÁ EVIDENCE TRŽEB

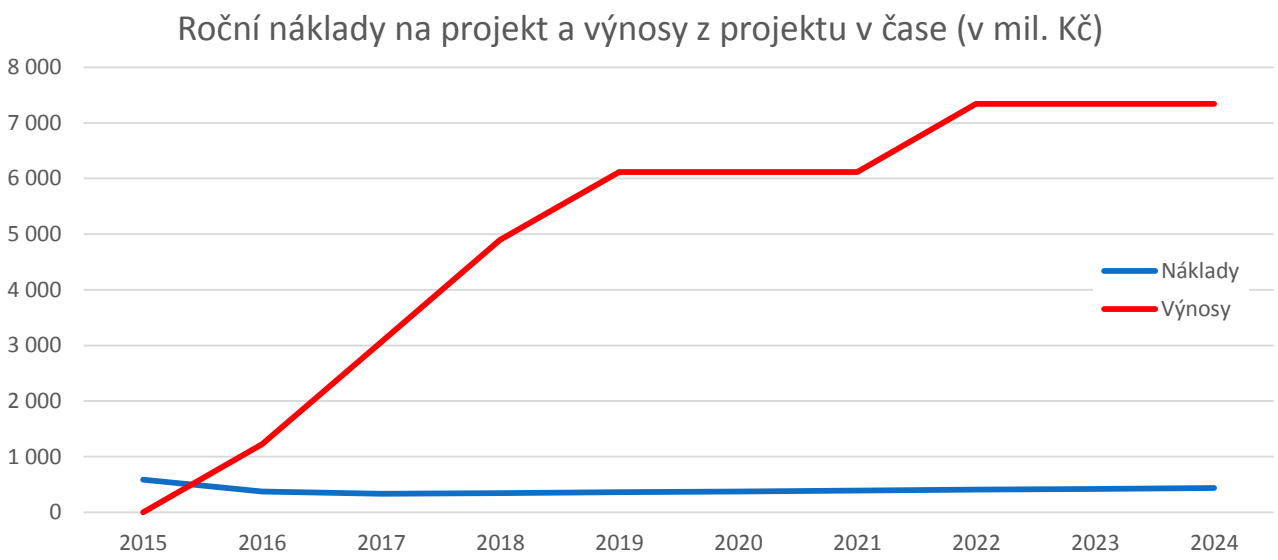
Náklady provozní fáze projektu 417 479 245 Kč

Termín realizace provozní fáze 1.1.2016 - 31.12.2016

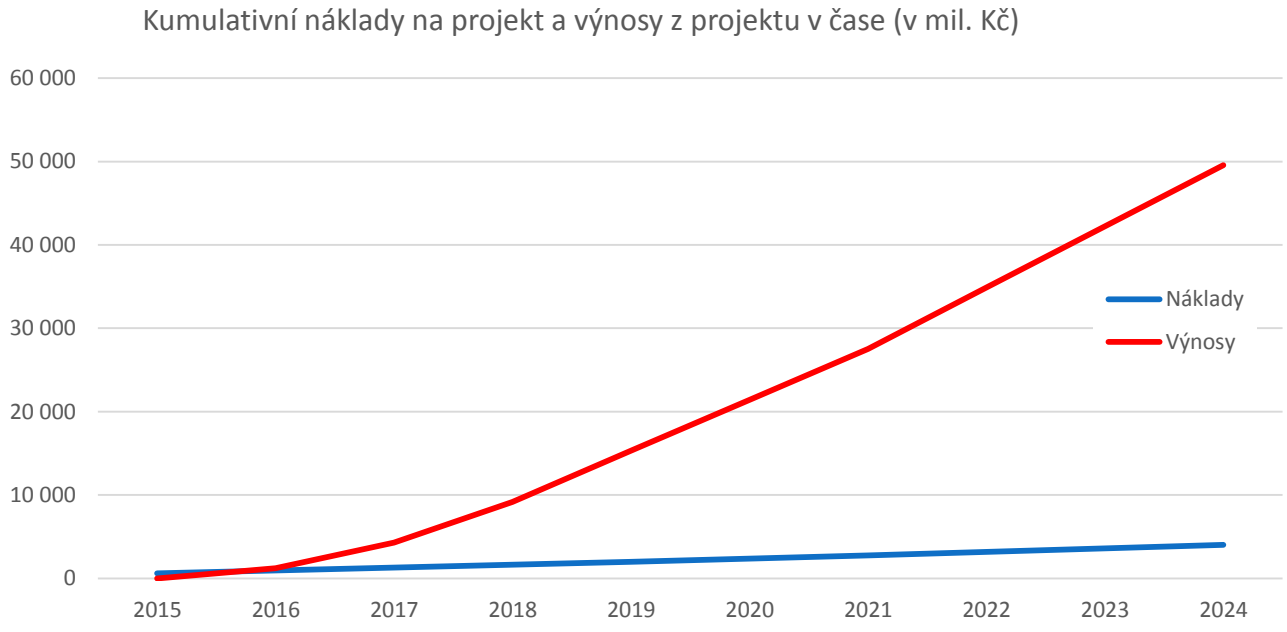
Název položky	Odhadovaný náklad v Kč*	Organizace	Projektový tým	Způsob objednávky	Datum dodávky
Poradenství PR a komunikace	500 000	MF	PR a komunikace	Veřejná soutěž	2/15 -4/16
Obnova vozidel	2 700 000	CS	Odborný	VS 1x za 4 roky	Trvale
Provoz vozidel	1 800 000	CS	Odborný	Navýšení rozpočtu	Trvale
Vystrojení obnova	806 235	CS	Odborný	Navýšení rozpočtu	Trvale
Obnova technických prostředků	163 700	CS	Odborný	Navýšení rozpočtu	Trvale
Ostatní provozní náklady	2 080 000	CS	Odborný	Navýšení rozpočtu	Trvale
Ostatní provozní náklady	800 000	CS	Odborný	Navýšení rozpočtu	Trvale
Mzdové náklady	64 779 276	CS	Odborný	Navýšení rozpočtu	kalendářní rok
Provoz systému souvisejících s EET v systémech ČP	1 000 000	FS	Front office	Navýšení rozpočtu	od 1. 1. 2016
Provoz technického callcentra ČP	600 000	FS	Front office	Objednávka ČP	od 1. 1. 2016
Provoz zákaznického callcentra ČP	2 400 000	FS	Front office	Objednávka ČP	od 1. 1. 2016
Kontrolní nákupy	10 000 000	CS	Odborný	Navýšení rozpočtu	trvale, kalendářní rok
Výdaje na platy včetně příslušenství	133 979 147	FS	Odborný	Navýšení rozpočtové položky	1. 1. 2016
Ostatní IT náklady	4 500 000	FS	Odborný	Objednávky, smlouvy	1. 1. 2016
Kontrolní nákupy	20 000 000	FS	Odborný	Navýšení rozpočtu	trvale, kalendářní rok
Údržba/Obnova hardware	117 425 290	SPCSS	Technický	Veřejná soutěž	1. 1. 2016
Housing	6 845 251	SPCSS	Technický	Veřejná soutěž	1. 1. 2016
Service Desk	30 700 346	SPCSS	Technický	Veřejná soutěž	1. 1. 2016
Aplikace EET (SW)	5 400 000	FS	Technický	Veřejná soutěž	1. 11. 2015
PR	2 000 000	FS	PR a komunikace		Kalendářní rok
Ostatní provozní náklady	9 000 000	FS	Odborný	Objednávky, smlouvy	1. 1. 2016
CELKEM	**417 479 245**				

*včetně DPH

Návratnost projektu v čase



Obrázek 46: Roční náklady na projekt a výnosy z projektu v čase



Obrázek 47: Kumulativní náklady na projekt a výnosy z projektu v čase

Přílohy

Příloha č. 1 – Návrh obsahu datové věty účtenky

DATOVÁ ZPRÁVA

číslo pole	*pole datové věty*	*typ pole*	*poznámka*	*ověření na vstupu*	*poznámka k ověřování*
			hlavička		
1	UUID	VARCHAR(32)	"Hlavička" datové zprávy, každá zpráva zaslaná na centrální systém EET musí obsahovat identifikátor té zprávy. Toto samé je aplikováno i v případě, že se jedná o opakované zaslání této zprávy z důvodu chyby při realizaci při doručení zprávy. Jedná se o standardní údaj. Generování UUID podléhá patřičnému standardu.	ANO	Při příchodu datové zprávy se kontroluje pouze přítomnost této položky.
2	Datum a čas odeslání zprávy	datum rozšířené	DD.MM.RRRR HH.MM.SS.	ANO	Při příchodu datové zprávy se kontroluje pouze přítomnost této položky.
3	Identifikace, zda se jedná o případ opětovného zaslání tržby	BOOL	A/N		
			obsah datové věty		
4	DIČ	alfanumerické	AAxxxxxxxx, kde AA je písmeno a xxxxxxxx jsou číslice.	ANO	Ověření při příchodu datové zprávy provádí pouze kontrolu syntaxe DIČ, nevaliduje jeho existenci. DIČ se musí také shodovat s identifikátorem certifikátu.
5	Identifikace provozovny	VARCHAR(64)	Přidělováno provozovně v rámci její registraci v IS EET.	ANO	Při příchodu datové zprávy se kontroluje pouze přítomnost této položky.
6	Identifikace koncového zařízení	VARCHAR(64)	Definuje poplatník.	ANO	Při příchodu datové zprávy se kontroluje pouze přítomnost této položky.
7	Pořadové číslo účtenky	číselné	Číslo účtenky v rámci daného koncového zařízení nebo v rámci provozovny. Určováno položkou č. 8. Restart vždy k 1. 1.	ANO	Při příchodu datové zprávy se kontroluje pouze přítomnost této položky.
8	Datum a čas přijetí tržby	datum rozšířené	DD.MM.RRRR HH.MM.SS. Případně datum vystavení účtenky, pokud byla vystavena dříve viz datová položka č. 27. V případě, že se jedná o vystavení účtenky, neměl by se tento čas lišit s datem odeslání zprávy o více jak 48 hodin (resp. 120 dle režimu evidence tržeb)	ANO	Při příchodu datové zprávy se kontroluje pouze přítomnost této položky.
9	Způsob přidělování pořadového čísla účtenky	CHAR (1)	zobrazuje způsob přidělování pořadového čísla účtenky centrálně na úrovni provozovny nebo individuálně z pokladního místa. Očekáváme P - provozovna, M - pokladní místo)		
10	Celková částka tržby	číselné		ANO	Při příchodu datové zprávy se kontroluje pouze přítomnost této položky.
11	Celková částka nepodléhající DPH	číselné	vyplňují jen plátci DPH		
12	Celkový základ daně s první sníženou sazbou DPH	číselné	vyplňují jen plátci DPH		
13	Celková DPH s první sníženou sazbou	číselné	vyplňují jen plátci DPH		
14	Celkový základ daně s druhou sníženou sazbou DPH	číselné	vyplňují jen plátci DPH		
15	Celková DPH s druhou sníženou sazbou	číselné	vyplňují jen plátci DPH		
16	Celkový základ daně se základní sazbou DPH	číselné	vyplňují jen plátci DPH		
17	Celková DPH se základní sazbou	číselné	vyplňují jen plátci DPH		
18	Částka v DPH režimu pro cestovní službu	číselné	vyplňují jen plátci DPH		

19	Částka v DPH režimu pro prodej použitého zboží	číselné	vyplňují jen plátci DPH		
20	Částka v DPH režimu pro investiční zlato	číselné	vyplňují jen plátci DPH		
21	Celkem za vydané vratné obaly (speciální DPH režim)	číselné			
22	Celkem za přijaté vratné obaly (speciální DPH režim)	číselné			
23	Celkem za prodej multi-purpose voucherů, nabití elektronické peněženky	číselné			
24	Celkem za užití multi-purpose voucherů nebo elektronické peněženky	číselné			
25	BKP	VARCHAR (64)	nesmí být již použit dříve, bezpečnostní kód poplatníka	ANO	Při příchodu datové zprávy se kontroluje pouze přítomnost této položky.
26	Způsob platby	CHAR (1)	(hotovost, karta, poukázka,…)		
27	Idenfikace subjektu (DIČ) v případě vydání účtenky, nebo části tržby z účtenky jménem tohoto subjektu	alfanumerické	Příkladem je tržba provedena na e-shop s platbou typu dobírka, kdy účtenka je vystavena na České poště, identifikace v tomto poli bude DIČ obchodu.		
28	Celková částka tržby inkasována jménem jiného subjektu	číselné			
29	Typ zaslání účtenky	číselník	Běžný/zjednodušený režim evidence		
30	rezerva	XML Element	Položka, která se může opakovat v libovolném počtu podle počtu rezervních položek. Každá rezervní položka bude obsahovat element pro ID (číselný unikátní identifikátor rezervní položky), Typ (datový typ dle číselníku), Hodnota.		

legenda: položky obdobné Chorvatskému modelu