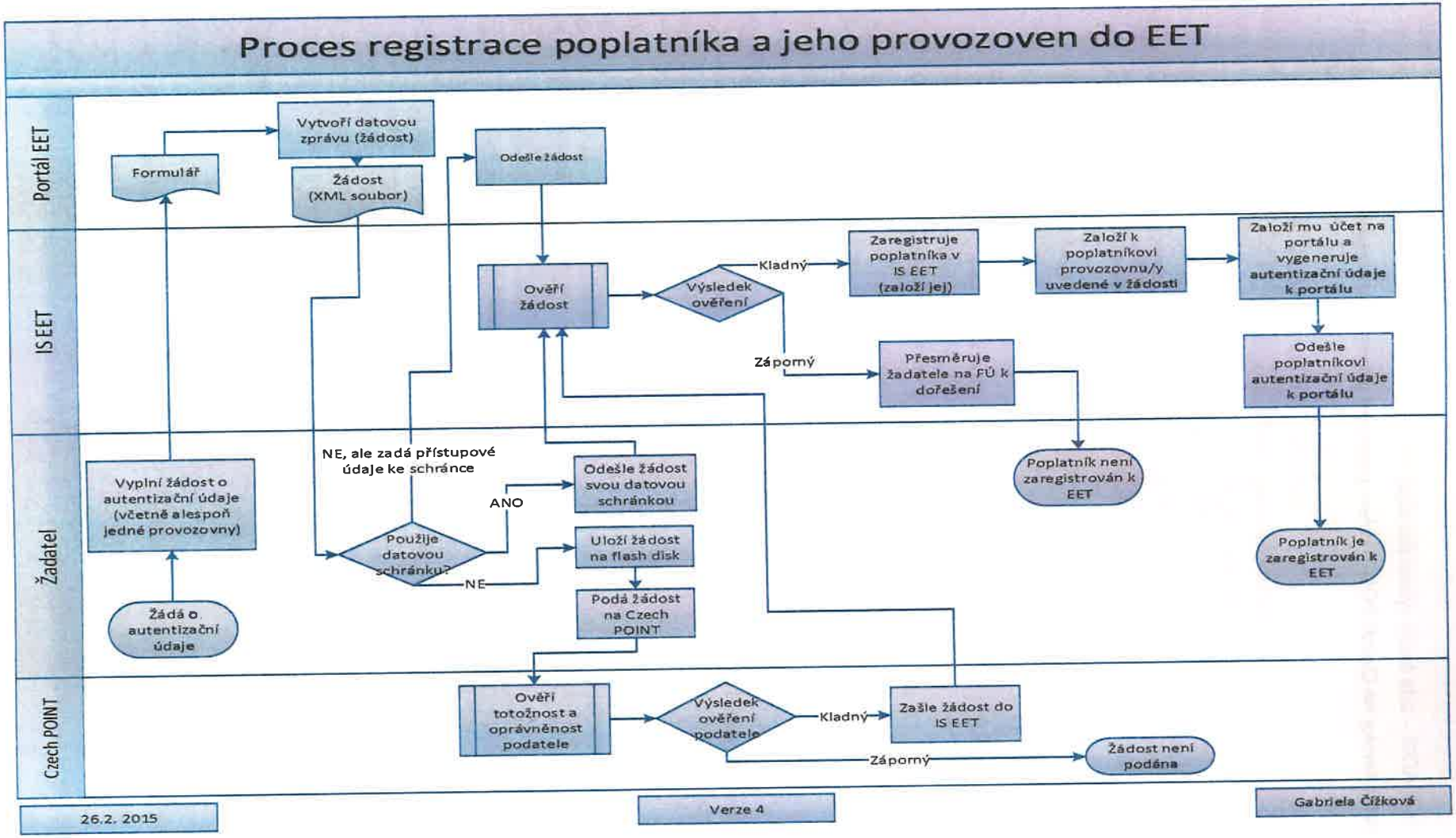
Nalezená rizika

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

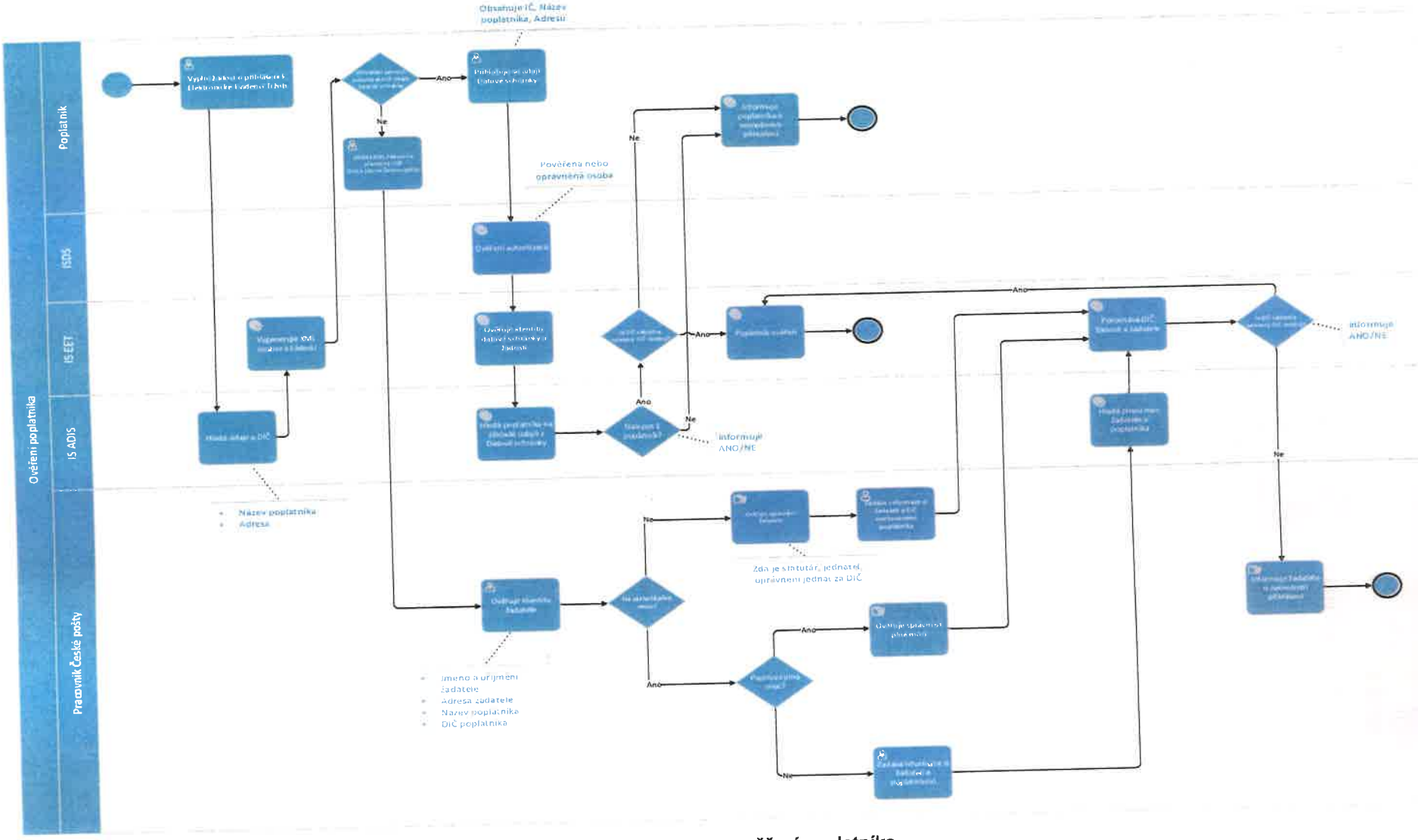


Obrázek 6: Proces registrace poplatníka a jeho provozoven do EET

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).

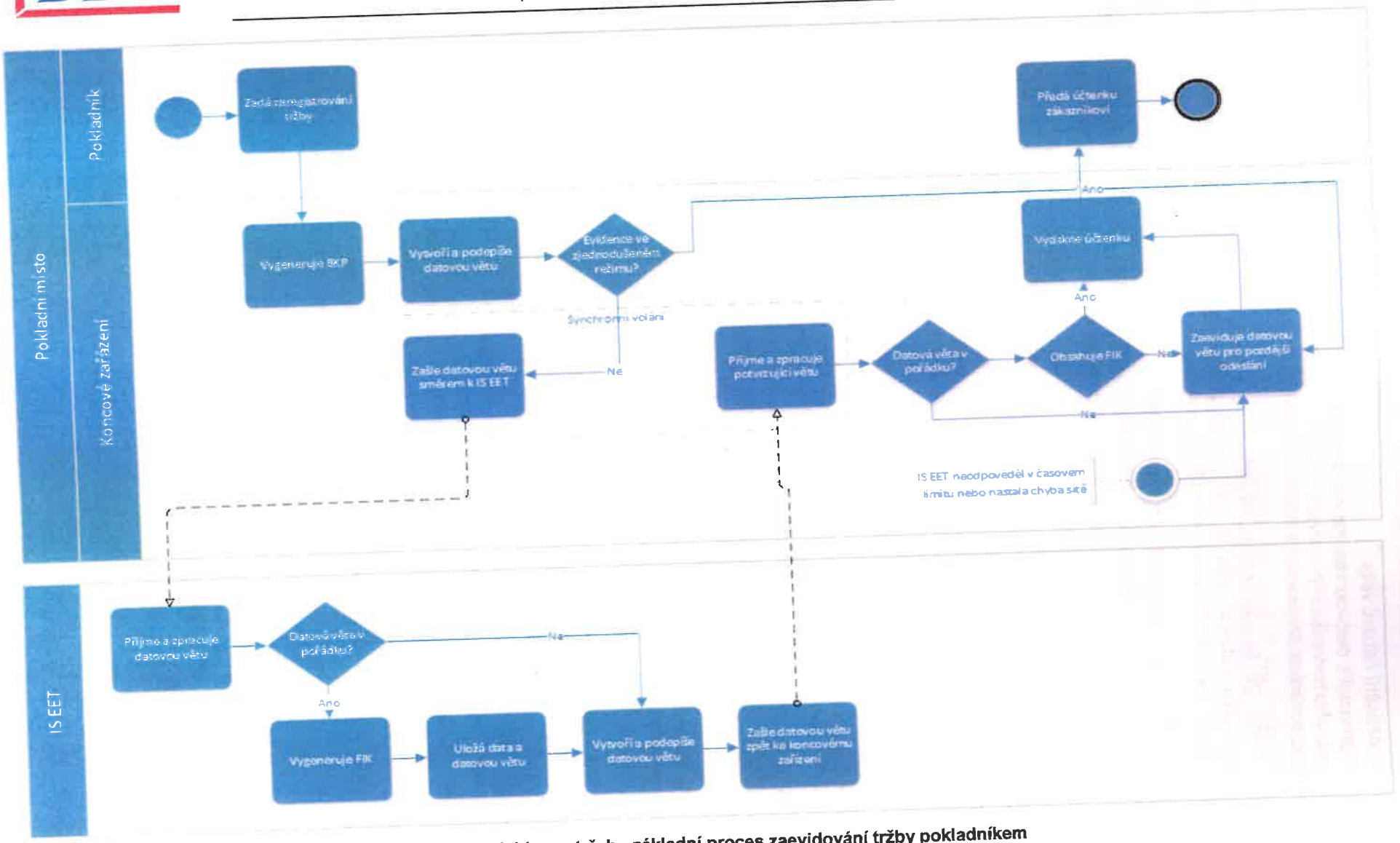
V případě, že koncové zařízení pracuje ve zjednodušeném režimu evidence tržeb, může k tomuto kroku přistoupit, aniž by provedlo zaevidování v IS EET. Tuto povinnost má do 120 hodin.

Uložení přijatých dat

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

Vytištění a předání účtenky

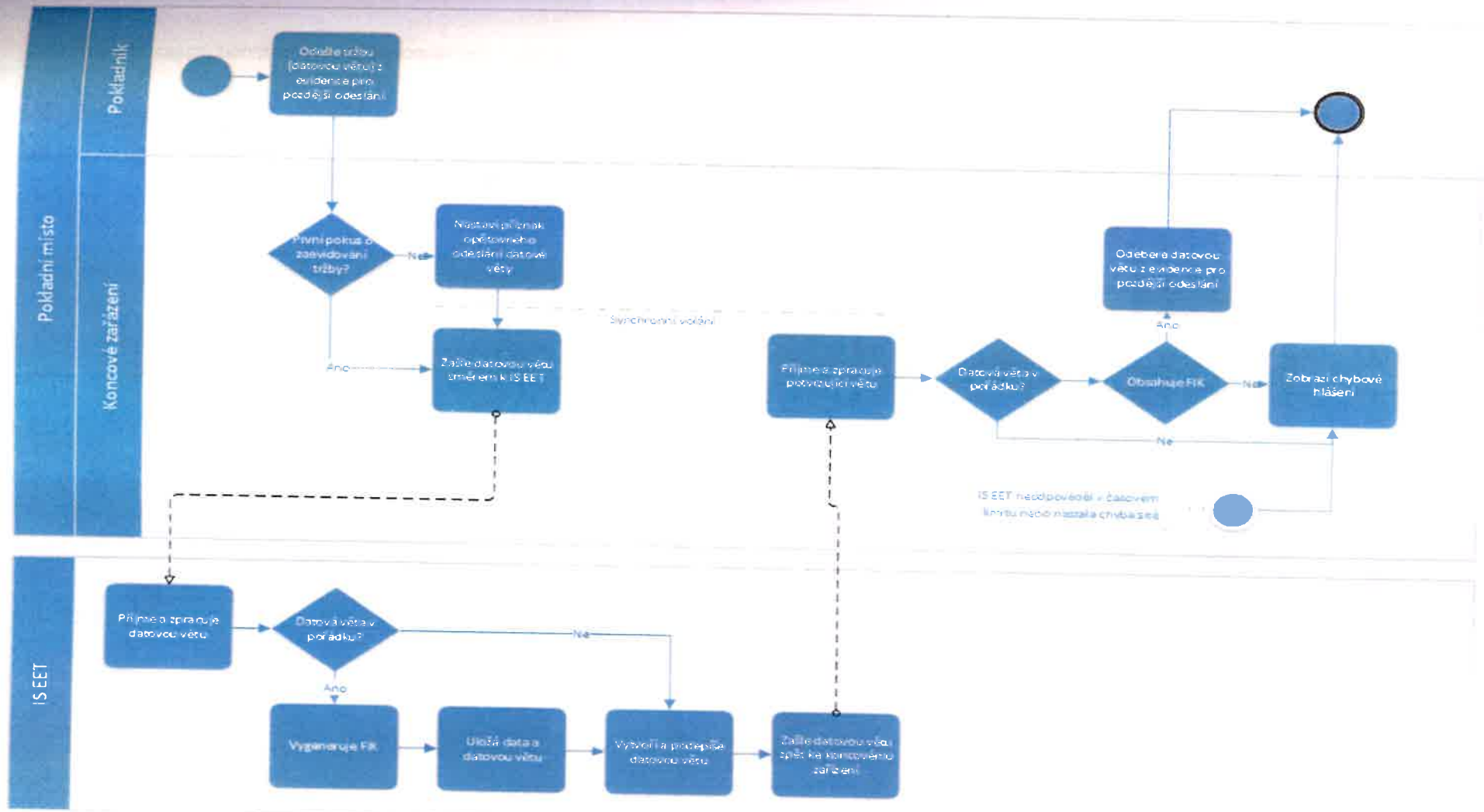
K vytištění a předání účtenky zákazníkovi musí dojít vždy. V případě, že dojde k přijetí FIK, je na účtenku vytištěn společně s BKP kódem. V opačném případě je místo FIK na účtenku vytištěn podpis dané účtenky.



Obrázek 8: Evidence tržeb - základní proces zaevidování tržby pokladníkem

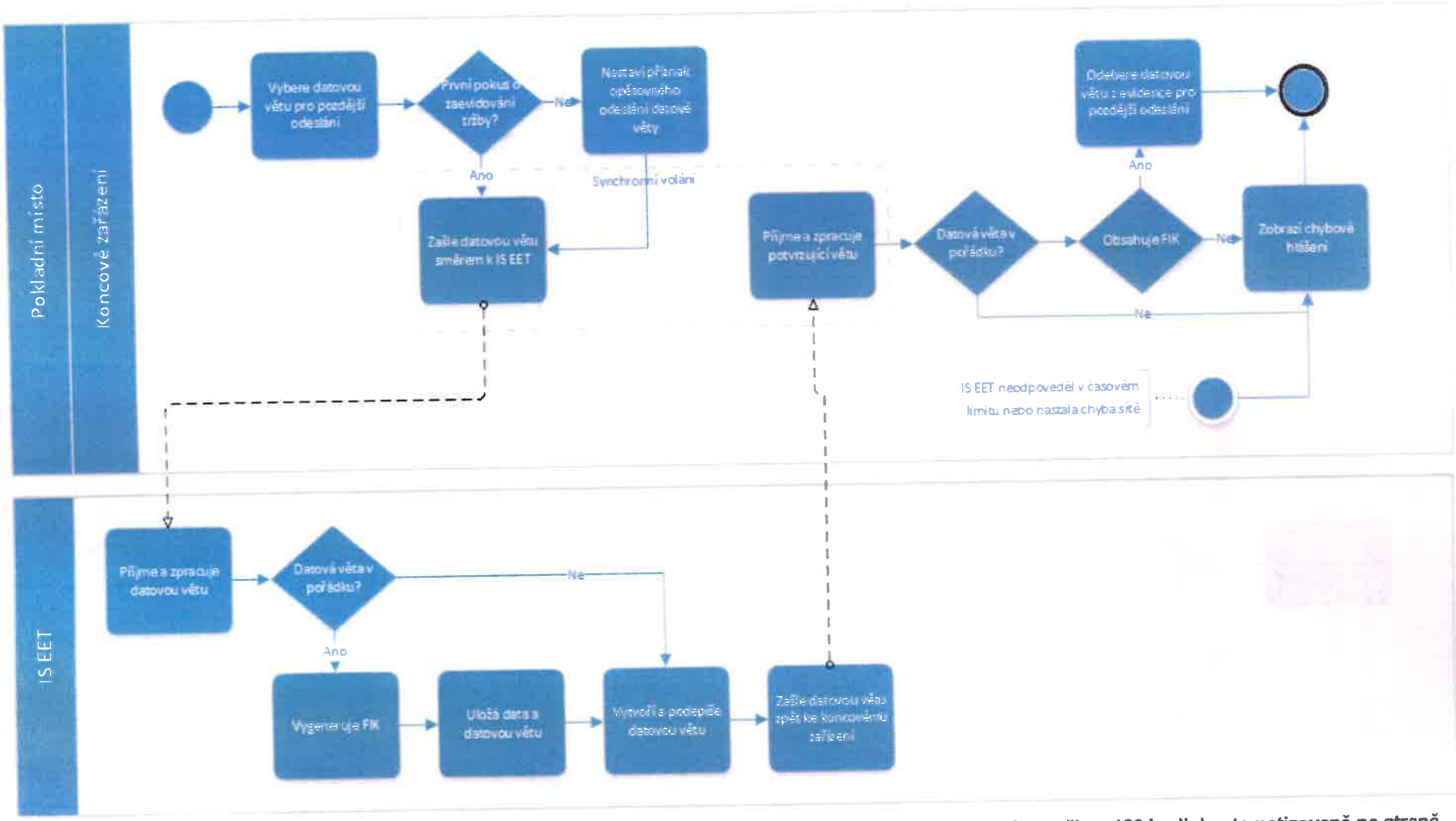
Evidence proběhne současně s vytištěním účtenky. Ve zjednodušeném režimu může dojít k zaevidování tržby pro pozdější odeslání.

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



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

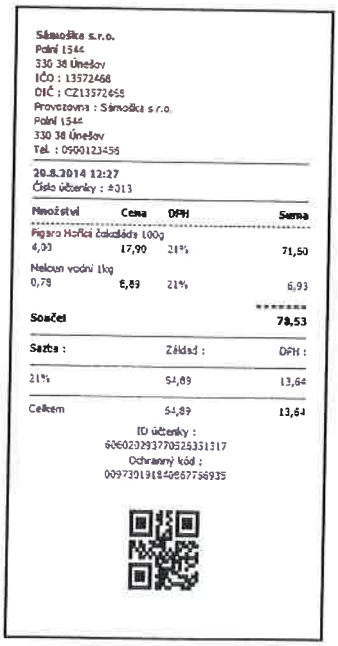
V rámci uvedených procesů je zapotřebí zohlednit následující případy užití.

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

20.8.2014 12:27
Číslo účtenky : 4013

Množství	Cena	DPH	Suma
Pigaro Hořící čokoláda 100g			
4,00	17,90	21%	71,60
Nelcun 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 :
606020293770525351317
Ochranný kód :
009730191840667756935

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

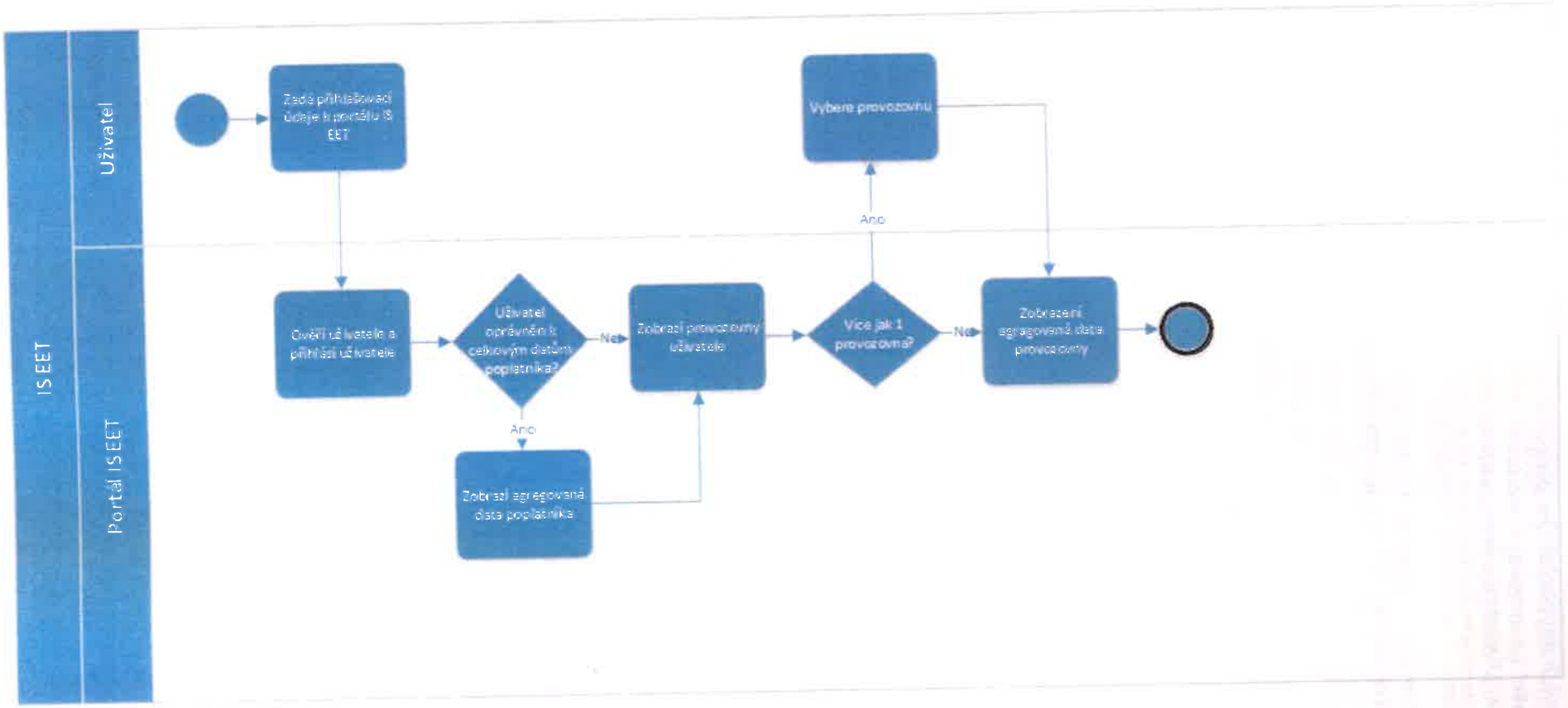
Má-li uživatel oprávnění (autorizace) k zobrazení veškerých agregovaných dat poplatníka, jsou mu zobrazeny. V opačném případě jsou mu zobrazena agregovaná data skrze jednotlivé provozovny.

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.

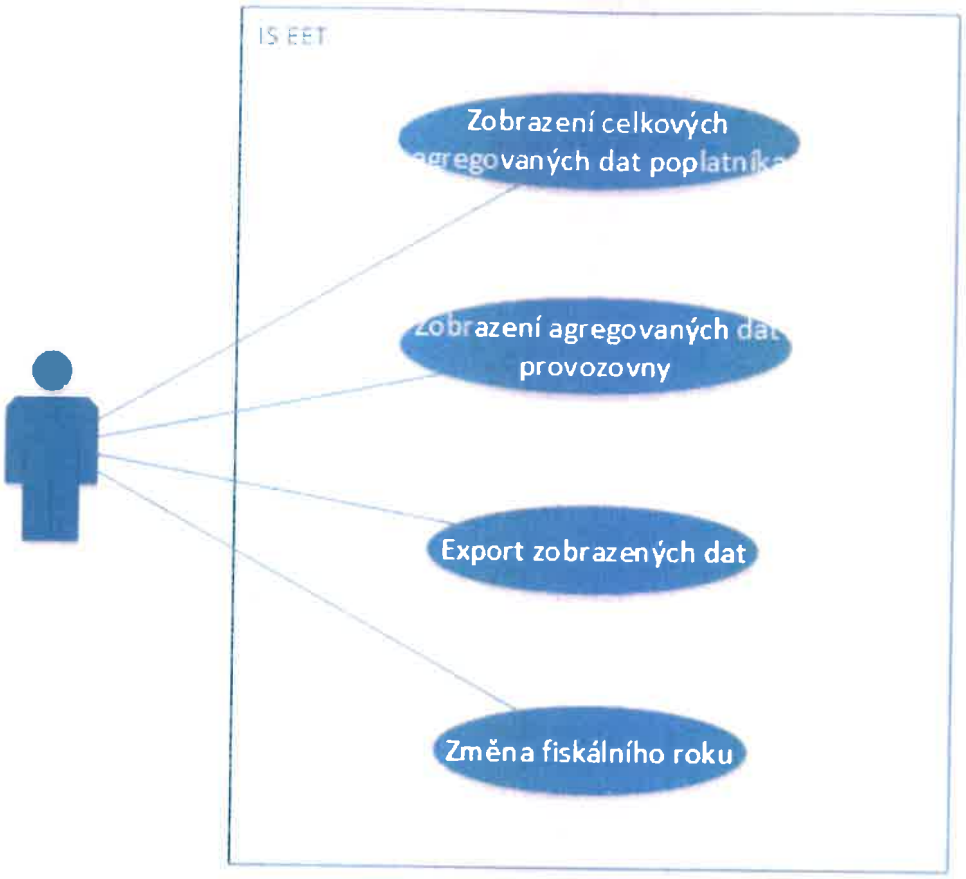


Obrázek 11 Zobrazení agregovaných dat

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.

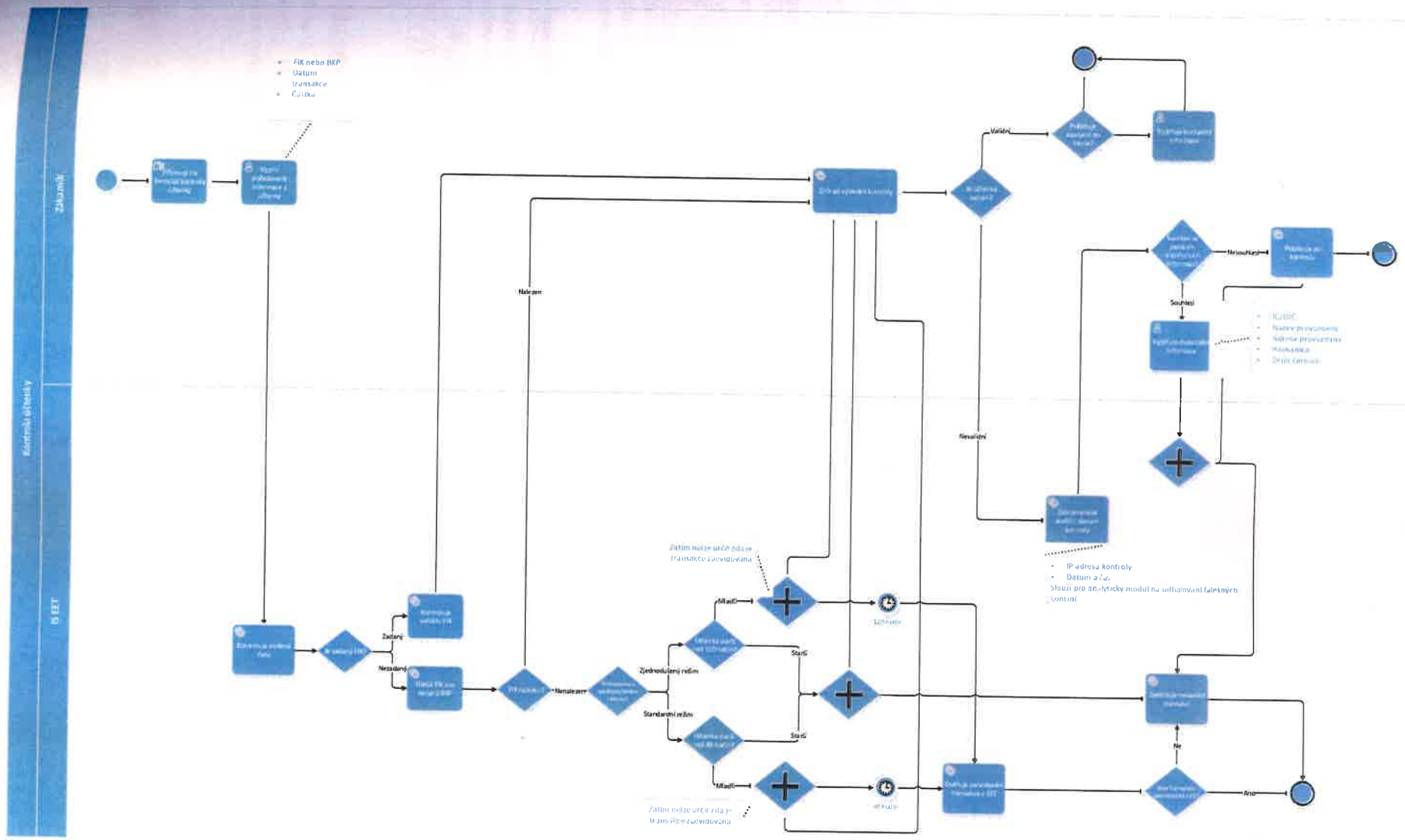
Logování událostí

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

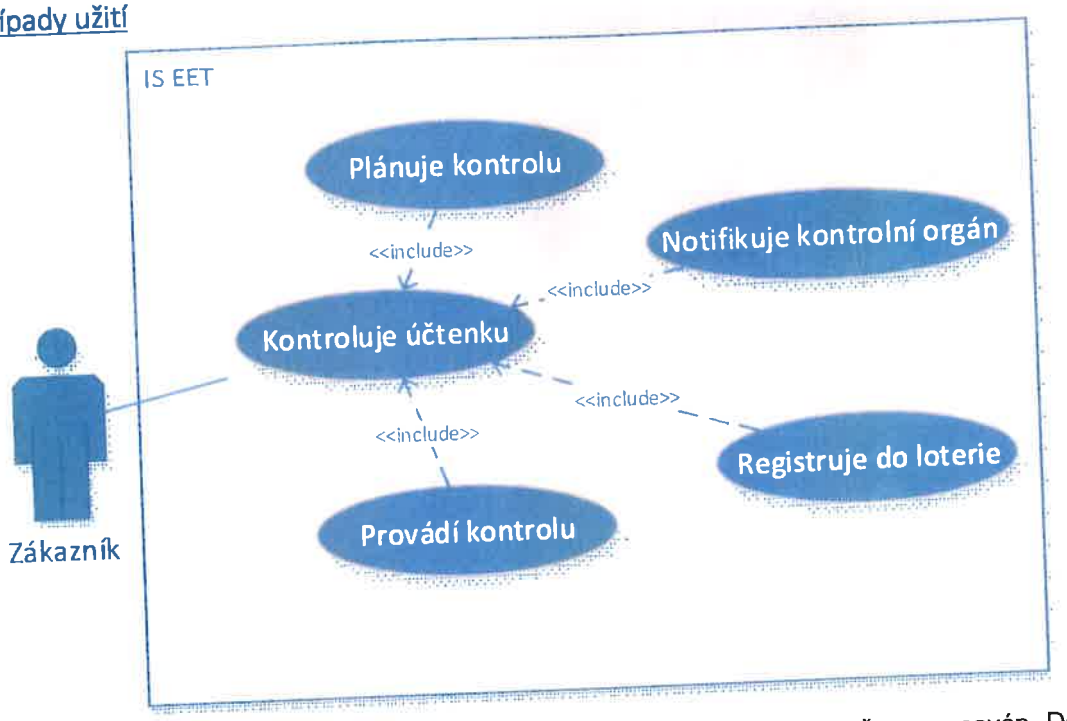
Popis kroků procesu

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 určen na přesnou identifikaci poplatníka a provozovny. Proces dále neobsahuje další chybové stavy.

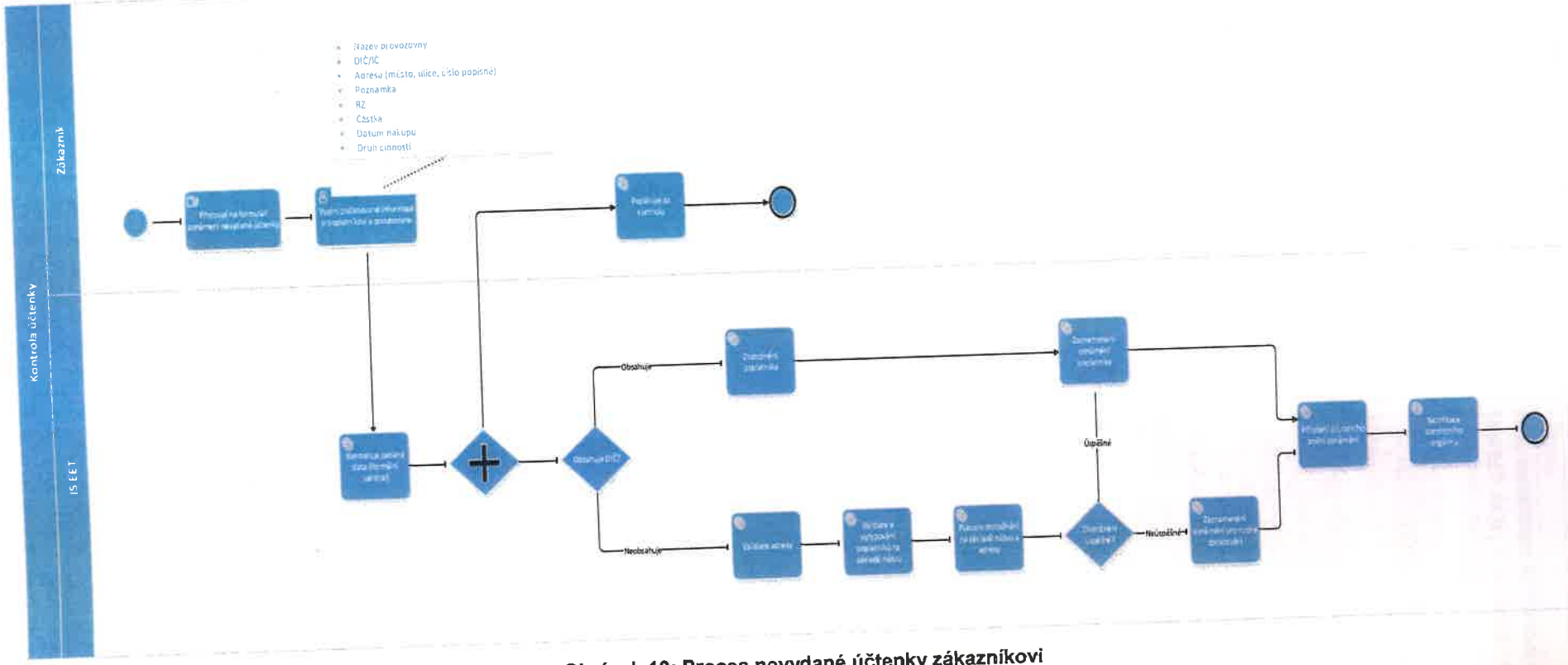
Logování událostí

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

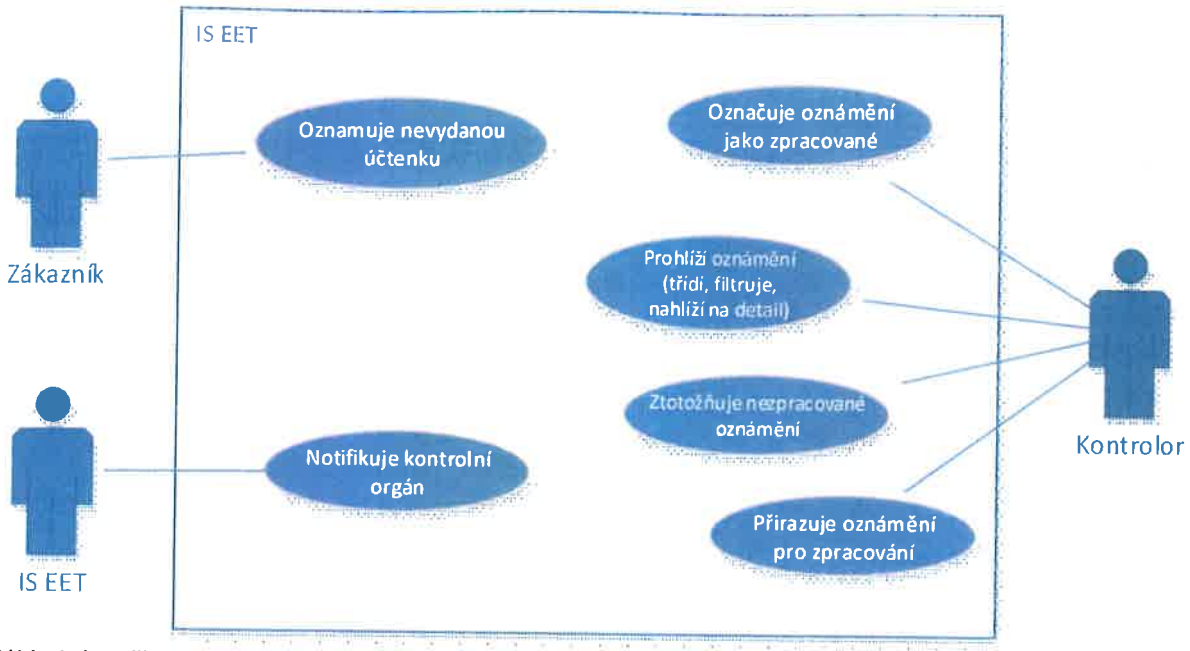
Popis kroků procesu

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.

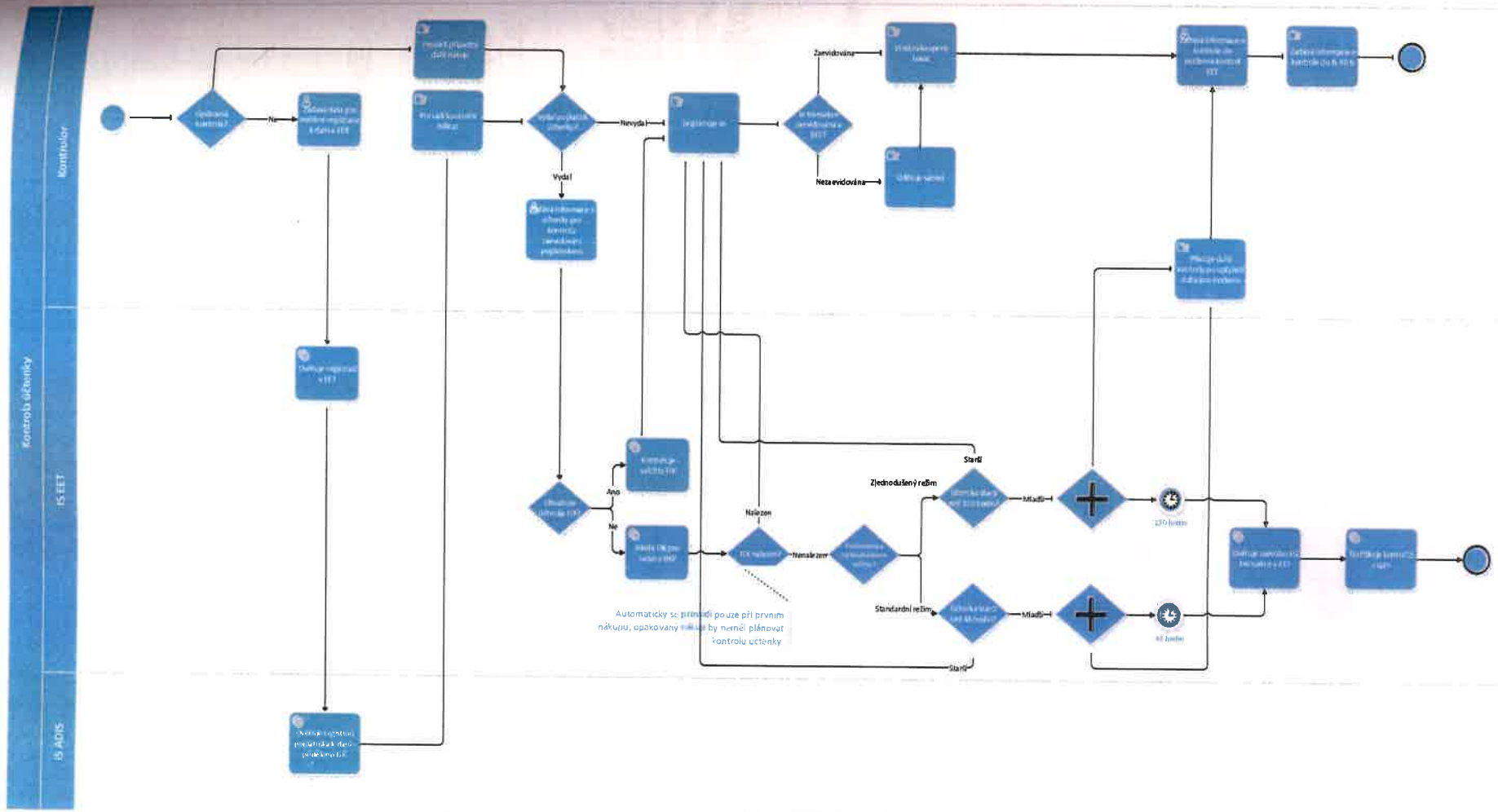
Proces Kontrolní nákup

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.

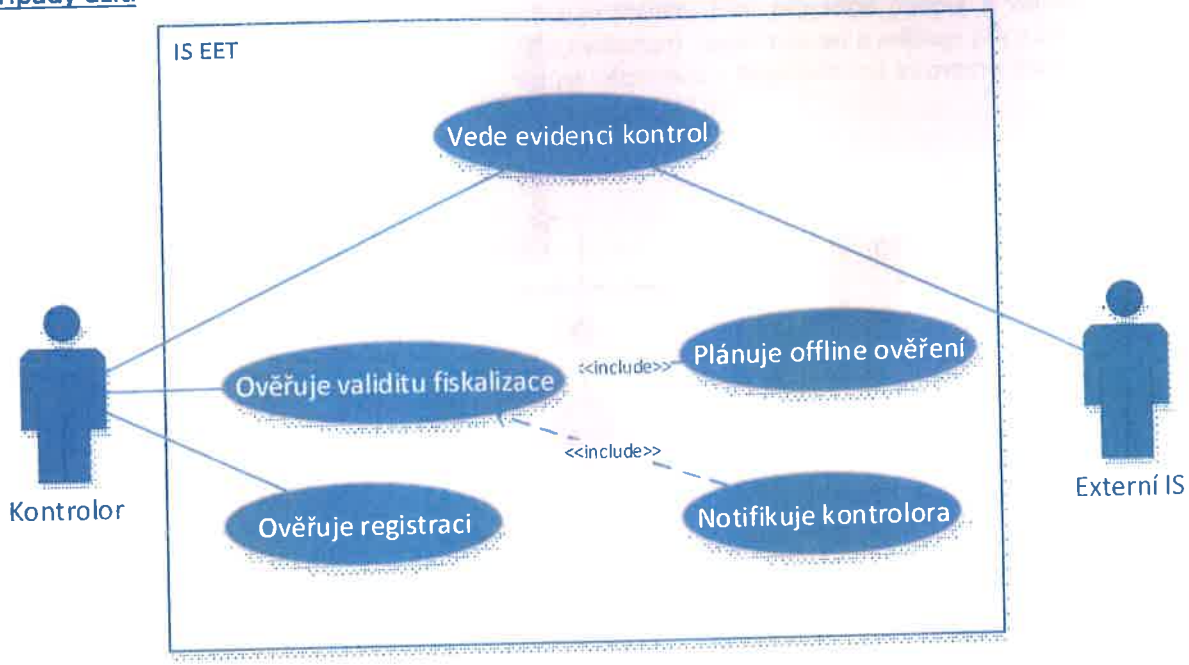
c. Účtenka byla vydána v off-line režime – kontrolor zaznamenává průběh kontroly a plánuje další kontrolu. Systém paralelně naplánuje kontrolu pozdní evidence. Kontrolor je informován o výsledku, vrací se do provozovny, kde může zrealizovat další nákup (systém v tomto případě zkontroluje validitu FIK, 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)

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

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)
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)

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

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

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)
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).

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.

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

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.

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

[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.

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 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	X0Z217LsLJcBUPhUGW2tWc6CTmM	
OKP	BASE64	hiTtrr/D5uv1GxhXhoSrfwvfY96XpZy1HNQeE88i3y4jD0Xyj2zkGKWVY/tGKJJWb6QTRbdAV2vGT01gxcM0CFy5bSMfh6jP1W7qGCiD9RAKzXS0T8cd5DpjuqeQHfZFdNz8DaA/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:

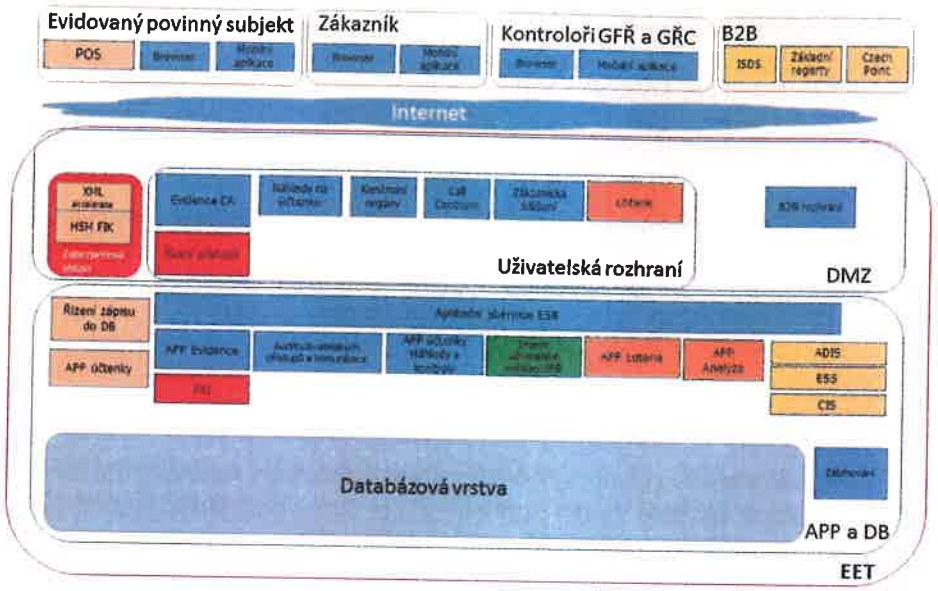
1. Registrace a evidence údajů a certifikátů o povinném subjektu
2. Evidence tržeb
3. Přístup poplatníka k vlastním statistickým údajům
4. Kontrola účtenky zákazníkem
5. Nahlášení neobdržené účtenky zákazníkem
6. Kontroly ze strany FS a CS
7. Následná analýza a vyhodnocování dat
8. Loterie

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 podaní
  - 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 dostj je :

dostj = [1 - Tnedost / (počet hodin v měsíci)] * 100 %

kde

Tnedost	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 Tnedost	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 Tnedost	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:

$$DOST = \sum dost_j / n$$

Kde

dostj	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:

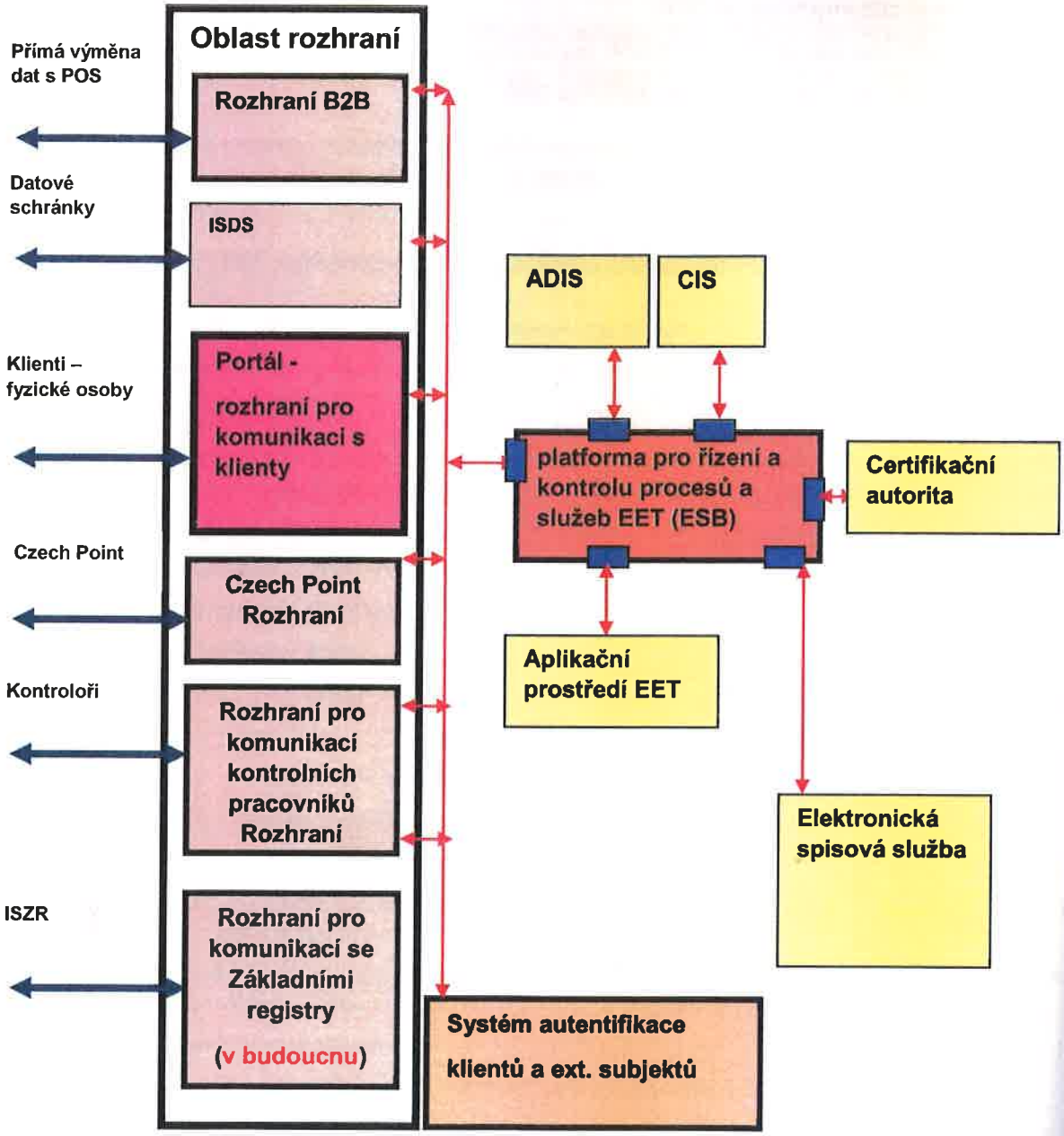
- komunikační infrastruktury,
- jednotné registrace, identifikace a autorizace pro pracovníky GFŘ a GŘC.

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.

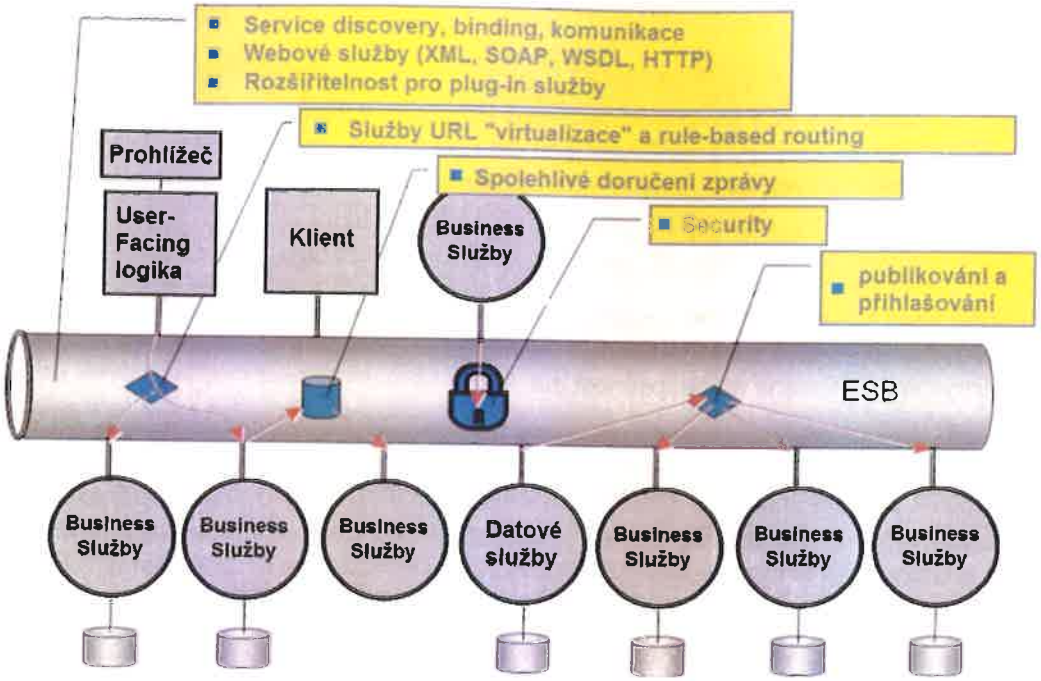
Access Manager musí umožňovat tyto základní typy autentizace:

- 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

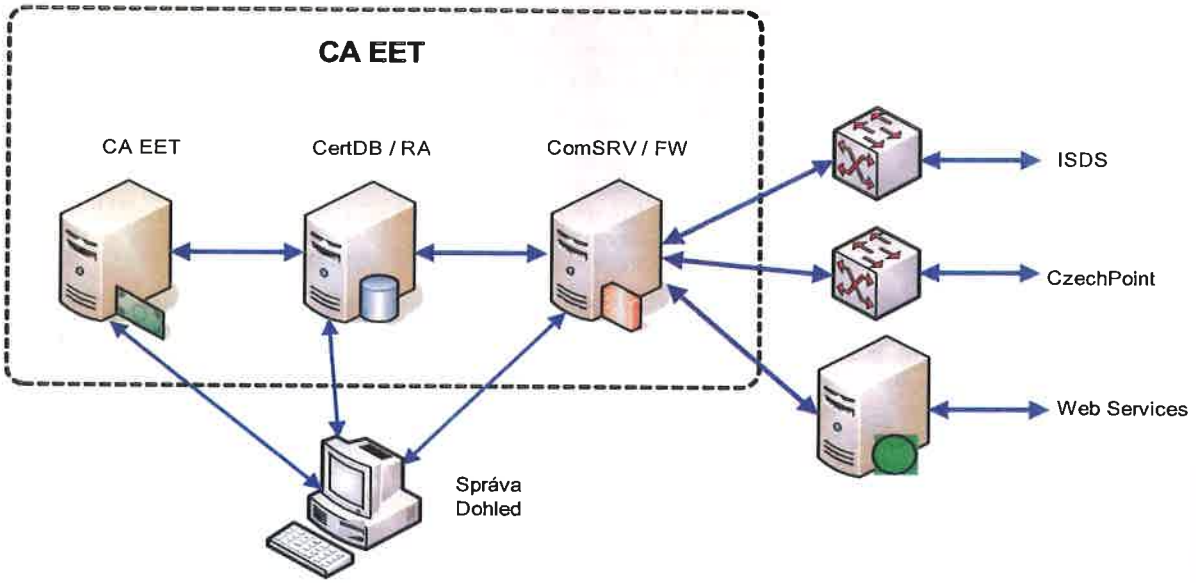
Certifikační autorita

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.

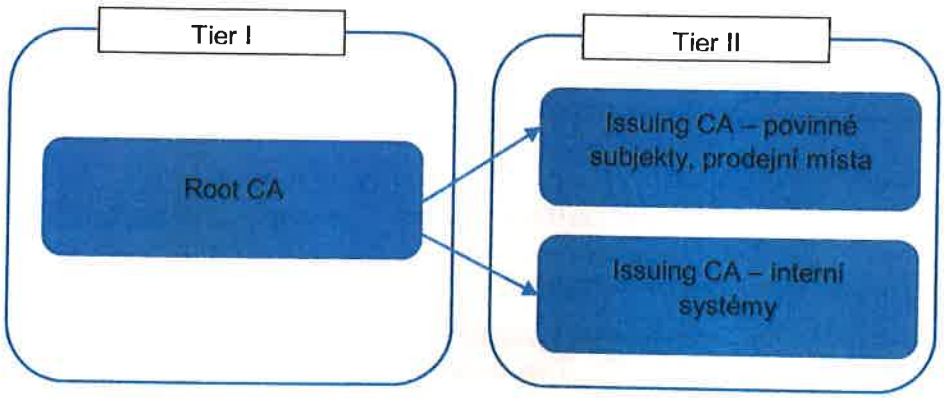
Předpokládá se, že každá CA EET bude řešena jako sada serverů a jiných zařízení, umístěných ve společné 19" přístrojové skříni. Tato skříň bude umístěna v technologických prostorách s fyzickým a režimovým zabezpečením. Obsluha a dohled budou prováděny vzdáleně, pomocí pracovních stanic a napojením na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

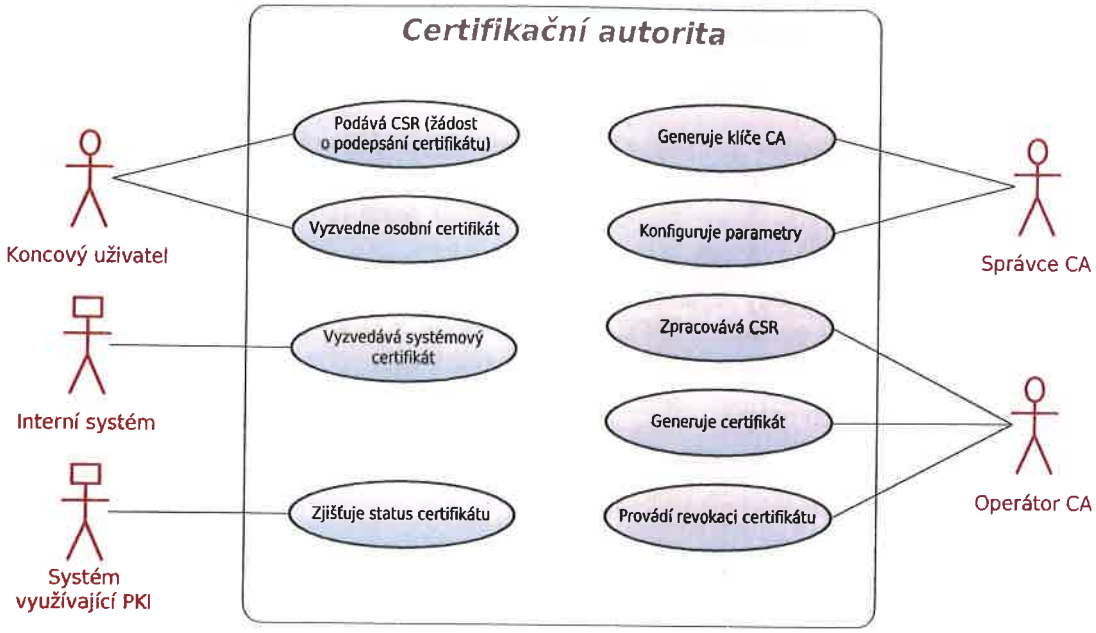
Požadavky na nastavení a kontrolu času

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).

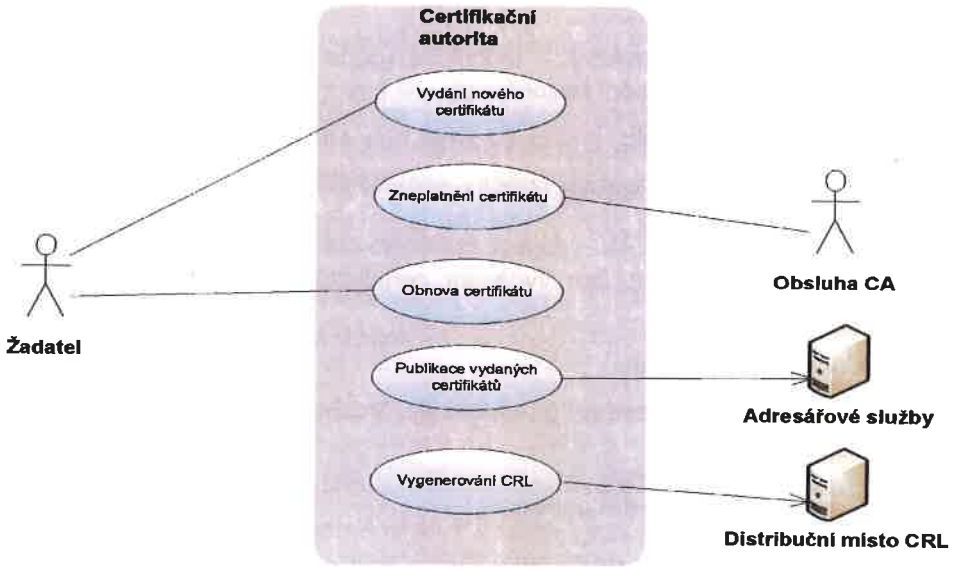
Požadovaná užití rozhraní CA



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