

**Ministerstvo financií Slovenskej
republiky**

Čiastková štúdia uskutočniteľnosti projektov
prioritnej osi 1 Elektronizácia verejnej správy
a rozvoj elektronických služieb OPIS

**Centrálna elektronická
podateľňa**



EURÓPSKA ÚNIA

TVORÍME VEDOMOSTNÚ SPOLOČNOSŤ
Európsky fond regionálneho rozvoja

Realizované s finančnou podporou Európskej únie v rámci programu Európsky
fond regionálneho rozvoja

Jún 2009

Tento dokument obsahuje 55 strán

Obsah

1	Základné informácie	1
1.1	Prehľad	1
1.2	Dôvod	1
1.3	Rozsah	1
1.4	Rámec projektu	2
1.5	Použité skratky a značky	2
2	Manažérske zhrnutie	4
2.1	Odporúčania	5
3	Popis aktuálneho stavu	7
3.1	Popis aktuálneho stavu a služieb	7
3.1.1	Analýza požiadaviek a potrieb	7
3.1.2	Architektúra	11
3.1.3	Procesná analýza	15
3.1.4	Legislatívna analýza	22
3.2	Hodnotenie aktuálneho stavu	25
3.3	Návrh zmeny	26
4	Navrhnuté riešenie	27
4.1	Popis navrhovaného riešenia	27
4.1.1	Popis služieb a funkcionality	27
4.1.2	Koncepcia riešenia elektronickej podateľne	27
4.1.3	Popis základných procesov	31
4.1.4	Elektronická podateľňa a ďalšie moduly NKIVS	33
4.1.5	Integrácia elektronickej podateľne na okolité prostredie	33
4.2	Zlepšenie	35
4.2.1	Vytvorenie podmienok pre budovanie elektronických služieb	36
4.2.2	Štandardizácia a zabezpečenie interoperability	36
4.2.3	Nasadenie overeného riešenia	36
4.2.4	Finančná efektívnosť – využitie overeného riešenia	36
4.3	Definície služieb	37
4.4	Uskutočniteľnosť a náklady	37
4.4.1	Dopady na technické a softwarové vybavenie	40
4.4.2	Organizačné dopady	40
4.4.3	Legislatívne dopady	40
4.4.4	Prevádzkové dopady	41
4.4.5	Dopady na lokalitu a stavebnú činnosť	41
4.4.6	Bezpečnostné dopady	41
4.4.7	Vývoj riešenia	41
4.4.8	Nasadenie riešenia	41

4.4.9	Cena riešenia	41
4.4.10	Marketingové požiadavky	42
4.4.11	Zhrnutie	42
4.5	Ekonomická analýza	42
4.6	Návrh projektového zámeru	42
4.6.1	Príprava projektu	42
4.6.2	Metodika riadenia	43
4.7	Zdôvodnenie doporučení	43
A	Definície elektronických služieb projektu	44
A.1	Podporné služby	45
A.1.1	Používateľské a aplikačné služby	45
A.1.1.1	Prijatie elektronického dokumentu alebo elektronického dokumentu podpísaného elektronickým podpisom	45
A.1.1.2	Vytvorenie elektronického podpisu odosielaného elektronického dokumentu	46
A.1.1.3	Informatívne overenie ZEP na poskytnutom elektronickom dokumente	46
A.1.1.4	Prevod ZEP na archívnu formu	47
A.1.1.5	Vytvorenie archívnej časovej pečiatky	47
A.1.1.6	Poskytnutie validačných údajov CRL pre kvalifikované certifikáty	48
B	Výpočet odhadu prácnosti riešenia	50
B.1	Use-case a používateľa riešenia	50
B.2	Výpočet UCP	50
B.2.1	Faktor technickej komplexnosti (TCF)	51
B.2.2	Faktor komplexnosti prostredia (ECF)	51
B.2.3	Neupravená váha use-casov (UUCW)	52
B.2.4	Neupravená váha používateľských interakcií (UAW)	52

1 Základné informácie

1.1 Prehľad

Centrálna elektronická podateľňa (CEP) tvorí jeden zo základných modulov architektúry integrovaného ISVS definovanej v rámci NKIVS. Použitie CEP je prierezové – je využívaná vo všetkých elektronických službách verejnej správy, ktoré sú viazané na použitie zarúčeného elektronického podpisu (ZEP), resp. vyžadujú spracovanie elektronického podania prostredníctvom CEP.

Podľa §2 písm. y) zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov elektronickou podateľňou je technické zariadenie slúžiace najmä na prijímanie, odosielanie a potvrdzovanie prijatia elektronických dokumentov, elektronických dokumentov podpísaných elektronickým podpisom a elektronických dokumentov podpísaných zarúčeným elektronickým podpisom.

V súlade s uvedenou definíciou elektronickej podateľne, CEP predstavuje centrálny modul, ktorý spracováva elektronické podania a elektronické podania podpísané elektronickým podpisom alebo zarúčeným elektronickým podpisom. Po prijatí, kontrole, spracovaní podania a overení elektronického podpisu alebo ZEP, ak ho podanie obsahuje, elektronická podateľňa generuje elektronické potvrdenie o prijatí alebo odmietnutí elektronického dokumentu vydaním vlastného elektronického dokumentu (elektronickej potvrdenky) s použitím časovej pečiatky. Okrem uvedenej základnej funkcionality môže modul CEP realizovať aj autorizovanie elektronických dokumentov odosielaných orgánmi verejnej správy cez modul elektronického doručovania, či už ako elektronické rozhodnutia, alebo odpisy z ISVS, resp. iné elektronické dokumenty. Tieto elektronické dokumenty môžu byť generované vlastnými modulmi ÚPVS, ako aj orgánom verejnej správy, ktorý CEP pre autorizáciu vlastných rozhodnutí využíva.

CEP je spoločným modulom ÚPVS a na základe NKIVS je jeho správcom a prevádzkovateľom MF SR a ÚV SR.

1.2 Dôvod

Cieľom predmetnej štúdie realizovateľnosti je definovanie princípov činnosti CEP, požiadaviek na funkcie poskytované ostatným modulom ÚPVS, definovanie koncepcie budovania rezortných elektronických podateľní prevádzkovaných ďalšími orgánmi verejnej správy (rezortné podateľne - REP), ako aj koexistencie CEP a REP v procesoch poskytovania elektronických služieb verejnej správy. Cieľom je vytvorenie integrovaného technologického a procesného prostredia, ktoré podporuje spracovanie elektronických podaní, využívanie ZEP a sprístupnenie PKI funkcionality pre používateľov ÚPVS.

1.3 Rozsah

Štúdia realizovateľnosti sa zameriava na nasledujúce oblasti:

- procesy spracovania v module CEP (resp. v rezortnej elektronickej podateľni prevádzkovej orgánom verejnej správy),
- integrácia modulu CEP na ostatné moduly ÚPVS,
- požadovaná technická infraštruktúra CEP,
- prevádzkové zabezpečenie činnosti CEP,
- funkcie sprístupnenia PKI modulov pre používateľov ÚPVS.

Štúdia realizovateľnosti analyzuje potreby spracovania elektronických podaní a elektronických rozhodnutí s dôrazom na využívanie ZEP, existujúce riešenia a definuje požadovaný cieľový stav. Súčasne definuje optimálny spôsob využitia existujúcich riešení CEP pri budovaní cieľového stavu.

1.4 Rámec projektu

Budovanie CEP je určené funkčnými požiadavkami definovanými v rámci dokumentu NKIVS. Tento dokument predstavuje základný funkčný rámec pre CEP.

Funkčnosť a prevádzka CEP je však limitovaná existujúcou legislatívou, najmä nasledujúcimi zákonmi:

- Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov.
- Vyhláška NBÚ č. 136/2009 Z. z. o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku.
- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy.

1.5 Použité skratky a značky

P.č.	Skratka / Značka	Vysvetlenie
1	BPM	Business Process Manager – modul ÚPVS implementujúci logiku spracovania podaní používateľa a správ určených pre používateľa
2	CEP	Centrálna elektronická podateľňa
3	CRL	Zoznam zrušených certifikátov (Certificate Revocation List)
4	EP	Elektronický podpis
5	HSM	Hardware Security Module – certifikovaný HW pre uchovávanie podpisovacieho kľúča (podpisovacích kľúčov) elektronickej podateľne
6	ISVS	Informačný systém verejnej správy
7	NKIVS	Národná koncepcia informatizácie verejnej správy
8	PKI	Public Key Infrastructure – infraštruktúra certifikátov a

P.č.	Skratka / Značka	Vysvetlenie
		certifikačných autorít, ktorá umožňuje dôveryhodné previazanie identity vlastníka certifikátu s jeho verejným kľúčom
9	QC	Kvalifikovaný certifikát (Qualified Certificate)
10	TS	Časová pečiatka (Time Stamp)
11	ÚOŠS	Ústredný orgán štátnej správy
12	ÚPVS	Ústredný portál verejnej správy
13	ZEP	Zaručený elektronický podpis
14	ZEP-A	Zaručený elektronický podpis v archívnej forme (t.j. všetky validačné údaje sú obsiahnuté v štruktúre ZEP)
15	ZEP-EPES	Zaručený elektronický podpis v základnej forme – s referenciou na podpisovú politiku, avšak bez časovej pečiatky
16	ZEP-T	Zaručený elektronický podpis s časovou pečiatkou

Tabuľka 1: Používané skratky a značky

2 Manažérske zhrnutie

Modul Centrálnej elektronickej podateľne je v zmysle NKIVS základným komponentom integrovaného ISVS a spoločným modulom ÚPVS. Na základe NKIVS je jeho správcom a prevádzkovateľom MF SR a ÚV SR.

Projekt bude realizovaný v rámci prioritnej osi č. 1 a opatrenia 1.1 Elektronizácia štátnej správy a zavádzanie služieb eGovernmentu na centrálnej úrovni.

CEP bude pre inštitúcie VS, ktoré nebudú mať zriadenú vlastnú rezortnú elektronickú podateľňu, poskytovať najmä službu prijatia a prvotného spracovania podaní od fyzických a právnických osôb. CEP bude vedieť prijať a spracovať elektronické dokumenty definovaných formátov a elektronické dokumenty podpísané elektronickým podpisom alebo ZEP, rovnako definovaných formátov. Základnou vlastnosťou modulu CEP bude overenie formálnych náležitostí prijatého elektronického dokumentu, t.j. formátu dokumentu a formátu elektronického podpisu a zároveň overenie platnosti elektronického podpisu, ak ho podanie bude obsahovať.

Výstupom z uvedeného procesu overenia bude vystavenie elektronickej potvrdenky s časovou pečiatkou o prijatí alebo odmietnutí prijatia podania a postúpenie elektronického podania na spracovanie príslušnej inštitúcii VS.

V prípade akceptovania podania, pokiaľ nepôjde o anonymné podanie, bude CEP zasielať kópiu podania spolu s elektronicou potvrdenkou do elektronickej schránky podávajúcej osoby v eDesk module.

Okrem uvedenej základnej funkcionality prijatia, spracovania a postúpenia podania na ďalšie spracovanie, bude CEP zabezpečovať dodatočné funkcie, ktorými sú:

- získavanie, archivovanie a poskytovanie CRL ku kvalifikovaným certifikátom,
- autorizácia odosielaného dokumentu (vytvorenie ZEP odosielaného dokumentu),
- informatívne overenie ZEP na poskytnutom elektronicom dokumente,
- prevod ZEP na archívnu formu,
- vytvorenie archívnej časovej pečiatky,
- poskytovanie aplikácie pre vyhotovenie ZEP pre PO/FO v rámci podaní realizovaných prostredníctvom ÚPVS.

Analogické funkcie ako modul CEP bude poskytovať aj modul rezortnej elektronickej podateľne (REP), ktorý bude budovaný a prevádzkovaný príslušným orgánom verejnej správy. Ten bude nasadzovaný v prípade, ak bude zmysluplné budovať podateľňu na úrovni príslušného orgánu verejnej správy – napr. pre inštitúcie VS zo značným množstvom agend, resp. značným množstvom podaní.

Vybudovanie systému modulov CEP a REP prispeje k efektívnemu využívaniu elektronických služieb. Modul CEP zároveň dáva možnosť pre malé inštitúcie a organizácie VS využiť jeho funkcionality bez nutnosti budovania vlastných finančne náročných riešení elektronickej podateľne. Zároveň bude nutné prevádzkovateľom CEP zadať kritéria na rozhodovanie kedy je efektívne a technicky zvládnutelné pripojenie konkrétnej inštitúcie VS na CEP, najmä vzhľadom na množstvo agend a priemerný počet podaní za definované obdobie.

Súčasťou riešenia modulu CEP však je aj vypracovanie systému metodických usmernení v nasledujúcich oblastiach:

- využívanie služieb modulu CEP a jeho integrácia do procesov poskytovania elektronických služieb,
- kritériá a doporučenia pre rozhodovanie o zriadení vlastného modulu REP,
- usmernenia pre nasadenie a prevádzku modulu REP a jeho integráciu do procesov poskytovania elektronických služieb.

2.1 Odporúčania

Implementovať navrhované riešenie systému elektronických podateľní do prostredia Integrovaného ISVS ako jedného zo základných predpokladov budovania elektronických služieb verejnej správy. Pri implementácii tohto riešenia maximálne využiť existujúce riešenie CEP prevádzkované v rámci ÚPVS a implementovať navrhované rozšírenia funkčnosti.

Súčasne navrhujeme v rámci ÚPVS realizovať spôsob voľného sprístupnenia certifikovaných prostriedkov pre ZEP pre používateľov elektronických služieb verejnej správy, čím bude masovo podporené využívanie týchto služieb a odstráni sa jedna z identifikovaných prekážok rozvoja plošného využitia týchto služieb. Je potrebné realizovať nasadenie prostriedkov pre vytváranie a overovanie ZEP minimálne pre nasledujúce formáty elektronických dokumentov, ktorých využitie sa predpokladá v rámci implementovaných elektronických služieb:

- XML – základný formát pre výmenu informácií v rámci štandardov pre ISVS,
- PDF – formát pre zabezpečenie neštruktúrovaných príloh (konkrétne formát PDF/A ktorý je potrebný pre vytvorenie ZEP k dokumentom typu PDF),
- 602-XML – formát pre elektronické formuláre v zmysle štandardov pre elektronické formuláre¹.

Súčasne je potrebné venovať pozornosť štandardizácii v oblasti použitia elektronických podateľní a formátov a profilov ZEP tak, aby sa zabezpečila vzájomná kompatibilita pri budovaní elektronickej komunikácie medzi jednotlivými súčasťami Integrovaného ISVS

¹ Tento formát je už v súčasnosti k dispozícii v rámci technológií implementovaných v rámci ÚPVS. Vzhľadom na technologickú neutrálnosť štandardu pre elektronické formuláre je možné v budúcnosti požadovať podporu aj pre ďalšie technológie, ktoré budú tento štandard podporovať.

a vytvorili sa základy pre budovanie konzistentného systému využívania ZEP v procesoch elektronických služieb verejnej správy.

3 Popis aktuálneho stavu

3.1 Popis aktuálneho stavu a služieb

3.1.1 Analýza požiadaviek a potrieb

Mnohé elektronické procesy poskytovania služieb verejnej správy sú viazané na použitie ZEP, ktorý predstavuje jediný elektronický ekvivalent pre vlastnoručný, resp. úradne osvedčený podpis. Platná legislatíva (Správny poriadok a ďalšie) v prípade podaní realizovaných elektronicky takmer bez výnimky explicitne vyžaduje použitie ZEP na to, aby išlo o relevantné podanie, resp. podanie ekvivalentné písomnému podaniu.

ZEP sa využíva jednak pre autorizáciu podaní, ako aj pre autorizáciu rozhodnutí a výstupov z ISVS. Použitie ZEP v procesoch verejnej správy upravuje existujúca legislatíva.

Pre spracovanie ZEP v procesoch orgánu verejnej správy je potrebné zabezpečiť funkcie overenia ZEP na podaní, ako aj autorizácie rozhodnutí a výstupov prostredníctvom ZEP, aby sa dosiahli požadované náležitosti takýchto úkonov. Pri hromadnom spracovaní podaní a rozhodnutí je potrebné nasadenie automatizovanej elektronickej podateľne. Funkčnosť a úlohy elektronickej podateľne v procesoch spracovania ZEP presne špecifikuje legislatíva. Nasadenie elektronickej podateľne je teda základným predpokladom pre budovanie elektronických služieb v rámci daného orgánu verejnej správy. Elektronická podateľňa zabezpečuje overenie elektronického podpisu prijatého podania a vystavenie potvrdenia o prijatí vo forme e-formulára, resp. elektronického dokumentu.

Z hľadiska spracovania elektronických podaní bez ZEP existujúca legislatíva síce pripúšťa možnosť spracovávať elektronické dokumenty bez EP a elektronické dokumenty s EP elektronickou podateľňou, avšak nedefinuje konkrétne podmienky narábania s uvedenými elektronickými dokumentmi a spôsob ich overovania. Z hľadiska procesov spracovania týchto podaní je potrebné realizovať minimálne nasledujúce úkony:

- Zabezpečiť integritu elektronického podania, t.j. preukázateľne zabezpečiť nemennosť obsahu podania po jeho prijatí. Toto je možné dosiahnuť pripojením časovej pečiatky k elektronickému podaniu a vystavením potvrdenia o doručení, ktoré by taktiež malo referovať obsah pôvodného podania.
- Zabezpečiť potvrdenie o doručení podania (podobne ako je tomu pri podaniach so ZEP, kde takýto krok predpisuje legislatíva).
- V rámci jednotlivých inštitúcií VS stanoviť zoznam možných agend (podaní alebo žiadostí, napr. vo forme elektronických formulárov), kde je akceptované aj podanie bez EP alebo bez ZEP.

Z vyššie uvedených požiadaviek je možné konštatovať, že elektronická podateľňa, resp. jej jednotlivé funkcie, môžu byť využívané aj pri spracovaní elektronických podaní, ktoré nie sú autorizované prostredníctvom ZEP. Elektronická podateľňa teda bude zapojená do procesov spracovania všetkých podaní, ktoré sú zasielané elektronickou formou.

Existujúca legislatíva definuje nasledovné základné požiadavky na funkčnosť elektronickej podateľne a ňou realizované procesy:

- kontrolu prijímaných elektronických dokumentov predovšetkým z hľadiska schopnosti ich bezproblémového čítania technickými prostriedkami elektronickej podateľne, dodržanie ustanoveného formátu a obsahu a neprítomnosť škodlivých kódov a bitových sekvencií (napríklad makrá, vírusy, trójske kone, červy a pod.),
- overenie platnosti ZEP na prijatom podaní a platnosti kvalifikovaného certifikátu viazaného na ZEP prijatého podania,
- vystavenie potvrdenia o prijatí podania, ktoré je autorizované ZEP (osoby poverenej prevádzkou elektronickej podateľne),
- odoslanie podania na ďalšie vybavenie v orgáne verejnej moci,
- autorizácia dokumentu odosielaného od inštitúcie VS prostredníctvom elektronickej podateľne.

Súčasne je logikou procesov spracovania elektronických podaní požadované zabezpečenie nasledujúcich funkcií:

- vystavenie potvrdenia o doručení podania, ktoré nie je autorizované ZEP (osoby poverenej prevádzkou elektronickej podateľne),
- zabezpečenie integrity elektronického podania, ktoré nie je autorizované ZEP² pridaním časovej pečiatky.

Existujúca legislatíva bližšie nešpecifikuje spôsob zabezpečovania vyššie uvedených funkcií a procesov – tieto môžu byť zabezpečované manuálne (poverenou osobou), alebo automatizovane systémom elektronickej podateľne. Je zrejmé, že pri hromadnom spracovávaní, či už elektronických podaní, alebo autorizácii dokumentov, musí elektronická podateľňa pracovať v automatizovanom režime, bez zásahu do realizácie jednotlivých úkonov manuálnym spôsobom operátorom elektronickej podateľne. Táto štúdia sa ďalej bude zaoberať práve takýmito podateľňami, nakoľko centrálna spracovanie elektronických podaní modulom CEP predpokladá automatické spracovanie veľkého množstva elektronických podaní. Nie je vylúčené nasadenie elektronických podateľní pracujúcich v manuálnom režime pre organizácie, ktoré nezabezpečujú hromadné spracovanie vstupov alebo výstupov, kde bude vzhľadom na množstvo podaní denne výhodnejšie a efektívnejšie použiť elektronickú podateľňu pracujúcu práve v manuálnom režime.

Legislatíva stanovuje požiadavku zabezpečenia funkčnosti elektronickej podateľne pre všetky organizácie. Podľa §29 ods. 1) zákona o elektronickom podpise sú orgány verejnej moci povinné oznámiť Národnému bezpečnostnému úradu elektronickú adresu elektronickej podateľne, na ktorej prijímajú podania vo forme elektronických dokumentov podpísané

² V prípade podania autorizovaného prostredníctvom ZEP integritu podania zabezpečuje práve ZEP.

elektronickým podpisom alebo elektronických dokumentov podpísaných zaručeným elektronickým podpisom do 1.6.2009.

Z dôvodu zefektívnenia vynakladania prostriedkov na budovanie elektronických podateľní v rámci jednotlivých inštitúcií verejnej správy bol v rámci budovania ÚPVS zavedený modul CEP (centrálnej elektronickej podateľne). Tento modul má za cieľ centrálne zabezpečiť požadovanú funkčnosť elektronickej podateľne a poskytnúť ju pre potreby implementácie elektronických služieb poskytovaných prostredníctvom ÚPVS. Takéto poslanie centrálnej elektronickej podateľne bolo definované aj v rámci základného dokumentu – NKIVS.

Modul centrálnej elektronickej podateľne zabezpečuje požadovanú funkcionálnosť elektronickej podateľne a súčasne poskytuje aplikácie/prostriedky pre používateľov ÚPVS³ na vytváranie elektronických, resp. zaručených elektronických podpisov a na informatívne overenie platnosti elektronických podpisov.

Nasadzovanie CEP a ďalších elektronických podateľní podmieňuje využívanie zaručeného elektronického podpisu a s ním spojených technológií a štandardov, ako aj schopnosť prijímania a spracovania elektronických podaní v elektronickej forme. Z hľadiska súčasného stavu rozvoja elektronických podateľní sú prakticky nasadené nasledujúce známe riešenia:

- ÚPVS - implementovaná CEP pre spracovanie prijatých podaní a autorizáciu odosielaných, resp. komunikovaných dokumentov. Elektronická podateľňa sa využíva pri komunikácii medzi živnostenským registrom a daňovou správou a ročne bolo spracovaných a autorizovaných viac ako 150 000 elektronických podaní.
- Ministerstvo spravodlivosti SR – implementácia elektronickej podateľne pre spracovanie prijatých podaní do obchodného registra. Mesačne sú spracovávané rádovo stovky návrhov do Obchodného registra a je vydávaných niekoľko tisíc výpisov z Obchodného registra.
- Daňová správa – implementácia elektronickej podateľne pre spracovanie prijatých daňových priznaní a registračných formulárov pre daňový subjekt (väzba na Živnostenský register). Podateľňa Daňovej správy ročne spracováva niekoľko tisícov podaní daňových priznaní a viac ako 100 000 podaní pre elektronickú registráciu daňového subjektu.
- Colná správa – implementácia elektronickej podateľne pre zabezpečovanie obojsmernej elektronickej komunikácie v procesoch tranzitu a dovozu/vývozu (t.j. spracovanie podaní, ako aj odosielanie a autorizácia elektronických rozhodnutí). Mesačne je spracovávaných skoro 150 000 elektronických dokumentov prechádzajúcich systémom elektronickej podateľne.

Z vyššie uvedených referencií je zrejmé, že už v súčasnosti sú nasadené a prevádzkované viaceré riešenia elektronickej podateľne. Je teda možné hodnotiť súčasný stav a získané skúsenosti. Súčasný stav je možné charakterizovať ako stav, keď nie je zabezpečená vzájomná kompatibilita riešení, ako aj filozofie nasadzovania elektronických podateľní a využívania

³ Pod pojmom používateľia ÚPVS sa v tomto prípade rozumejú používateľia elektronických služieb verejnej správy, t.j. občania (pre procesy G2C) a právnické subjekty (pre služby G2B)

prostriedkov pre ZEP. Táto skutočnosť je významným faktorom brzdiacim plošné rozširovanie využívania ZEP. Z hľadiska existujúcich problémov sú najdôležitejšie nasledujúce skutočnosti:

- Nekompatibilita štandardizovaných formátov pre ZEP - v súčasnosti je používaných viacero štandardizovaných formátov ZEP – CAdES a XAdES. Tieto sú síce oba medzinárodnými štandardami a podporované aj zo strany NBÚ, ale sú vzájomne nekompatibilné. Preto používateľ môže pri komunikácii s konkrétnym orgánom verejnej správy využívať iba ten formát ZEP, ktorý podporuje príslušná elektronická podateľňa (t.j. musí mať k dispozícii certifikovaný prostriedok, ktorý vie vyhotoviť daný formát ZEP). V súčasnosti z existujúcich nasadení elektronickej podateľne riešenie MS SR podporuje formát CAdES a všetky ostatné vyššie uvedené riešenia formát XAdES.
- Vzájomná nekompatibilita prostriedkov pre ZEP – v súčasnosti nie sú certifikované prostriedky pre ZEP vzájomne plne kompatibilné. Dôvodom je šírka, rozsiahlosť a najmä voľnosť definície existujúcich štandardov a z nej vyplývajúca potreba vytvárania špecifických profilov pre ZEP podporovaných konkrétnym certifikovaným prostriedkom. Nakoľko nebol v rámci SR definovaný jednotný záväzný profil pre oba formáty ZEP, nie je možné garantovať plnú kompatibilitu prostriedkov (t.j. ZEP vytvorený jedným certifikovaným prostriedkom nemusí byť overiteľný iným certifikovaným prostriedkom).
- Príkladom ilustrujúcim problém rôznorodosti profilov môžu byť profily formátu XAdES, ktorý primárne vznikol za účelom podpisovania dokumentov formátu XML (vlastná štruktúra XAdES je vo formáte XML, CAdES používa binárne ASN.1 kódovanie). Nakoľko formát XML zo svojej podstaty nemá implicitne priradenú vizualizáciu definujúcu sémantiku údajov danej štruktúry, je vizualizácia kľúčovým prvkom pri podpisovaní tejto štruktúry, nakoľko interpretuje sémantiku podpisovaných údajov. Niektoré XAdES profily preto definujú medzi podpisovanými dátami v štruktúre podpisu aj vizualizáciu podpisovanej schémy (napr. XSL transformácia), ktorá zabezpečí jednotné zobrazenie údajov pre podpisovateľa ako aj overovateľa ZEP. Platnosť ZEP je v tomto prípade viazaná na platnosť použitej vizualizácie (platnosť vizualizácie určí subjekt definovaním XSD pre podpisované údaje)⁴. Ak dva certifikované prostriedky teda nepodporujú rovnaký profil definujúci požadované údaje v štruktúre podpisu, nemusí byť vytvorený podpis správne overený.
- Neexistencia štandardu pre spojenie ZEP s podpisovaným elektronickým dokumentom. Spojenie medzi dokumentom a ZEP napr. pre XAdES môže byť nasledovné:
 - EMBEDDED – štruktúra elektronického podpisu je súčasťou štruktúry podpisovaného elektronického dokumentu. Toto je špecifické pre každý formát elektronického dokumentu, nakoľko jeho definícia musí takýto spôsob podporovať (napr. pre dokumenty typu XML je toto možné⁵). Táto forma síce umožňuje viacnásobný podpis dokumentu (viacerými používateľmi), ale neumožňuje podpisovať súčasne viacero dokumentov. Rovnako spracovanie takéhoto elektronického podpisu nebude nezávislé

⁴ Zodpovedný subjekt teda definuje platné typy dokumentov zverejnením zodpovedajúcej XML schémy dokumentu (definovaná syntax dokumentu) a XSL transformácie do príslušného formátu pre zobrazenie (definovaný vizualizačný predpis ako základ sémantiky dokumentu)

⁵ Rovnako aj definícia formátu PDF definuje možnosť umiestnenia elektronického podpisu v štruktúre dokumentu

od štruktúry dokumentu – pri spracovaní bude potrebné poznať na určitej úrovni štruktúru dokumentu, čo môže limitovať univerzálnosť spracovania.

- EMBEDDING – podpisovaný elektronický dokument je súčasťou štruktúry elektronického podpisu. Táto forma síce umožňuje podpísať viacero dokumentov súčasne, ale nepodporuje viacnásobný podpis jedného dokumentu.
- DETACHED – elektronický podpis a podpisovaný dokument sú samostatné objekty, ktoré spolu spája vlastná aplikačná logika implementovaného procesu. Táto forma podporuje súčasne viacnásobný podpis, ako aj súčasný podpis viacerých dokumentov, ale je potrebné špecifikovať štruktúru, ktorou budú tieto spojené. V súčasnosti takýto štandard neexistuje, aj keď sa ho NBÚ pokúsilo čiastočne zdefinovať v dokumentoch zverejňovaných na svojej webovej stránke, a preto môžu byť jednotlivé realizované proprietárne riešenia vzájomne nekompatibilné.
- Obmedzenie použitia ZEP v rámci jednotlivých štátov EÚ – v rámci EÚ síce existuje Direktíva 1999/93/EC o elektronickom podpise, ktorá je však veľmi všeobecná. Jednotlivé krajiny EÚ definovali vlastnú, a často odlišnú legislatívu pre využívanie elektronického podpisu (v procesoch verejnej správy). Preto je použitie elektronického podpisu, a najmä ZEP, limitované na konkrétny štát a zatiaľ neexistuje spôsob využívania ZEP v celom priestore EÚ.
- Otvorený problém archivácie elektronických dokumentov so ZEP – zabezpečenie dlhodobej overiteľnosti ZEP je problém, ktorý nie je centrálné riešený. V súčasnosti sú používané dva spôsoby – prevod ZEP na archívnu formu (ZEP-A) a samostatné uchovávanie validačných údajov a ich archivácia. Problém sa stáva už v súčasnosti aktuálny, nakoľko nasadené riešenia sa presúvajú zo stavu pilotného overovania do stavu rutinej prevádzky a vzniká veľké množstvo elektronických dokumentov so ZEP, pre ktoré je potrebné zabezpečiť dlhodobú overiteľnosť ZEP.

Obmedzená podpora povolených formátov elektronických dokumentov pre vyhotovenie ZEP sa môže javiť podobne, ako predchádzajúce skutočnosti, problémom z hľadiska plošného rozšírenia používania ZEP. Je však potrebné si uvedomiť bezpečnostné požiadavky kladené na ZEP, najmä z pohľadu jednoznačnej vizualizácie podpisovaného a následne overovaného elektronického dokumentu. Legislatívou definované a povolené formáty elektronických dokumentov, ktoré je možné podpisovať ZEP však môžu na druhej strane byť výhodou, nakoľko v rámci riešenia elektronických podateľní bude postačujúce ošetriť túto existujúcu minimálnu množinu a nebude potrebné realizovať zložité implementácie ani podporu akýchkoľvek formátov. V súčasnosti je možné podpisovať iba nasledujúce formáty elektronických dokumentov – TXT (ASCII), RTF, PDF, HTML, XML, TIFF, PNG a ODF.

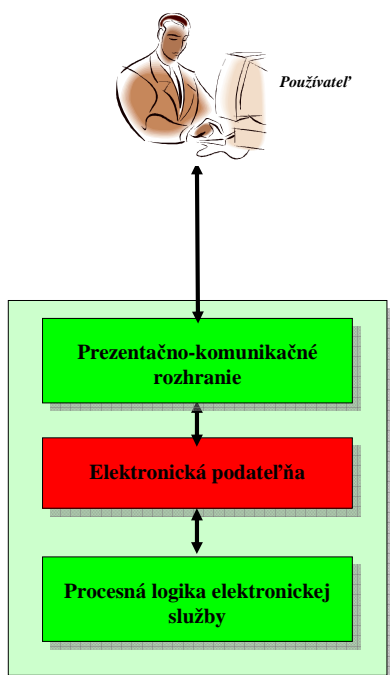
3.1.2 Architektúra

3.1.2.1 Architektúra začlenenia elektronickej podateľne do procesov elektronických služieb

Architektúra začlenenia elektronickej podateľne do procesov poskytovania elektronických služieb verejnej správy závisí od implementácie danej elektronickej služby, resp. konkrétneho

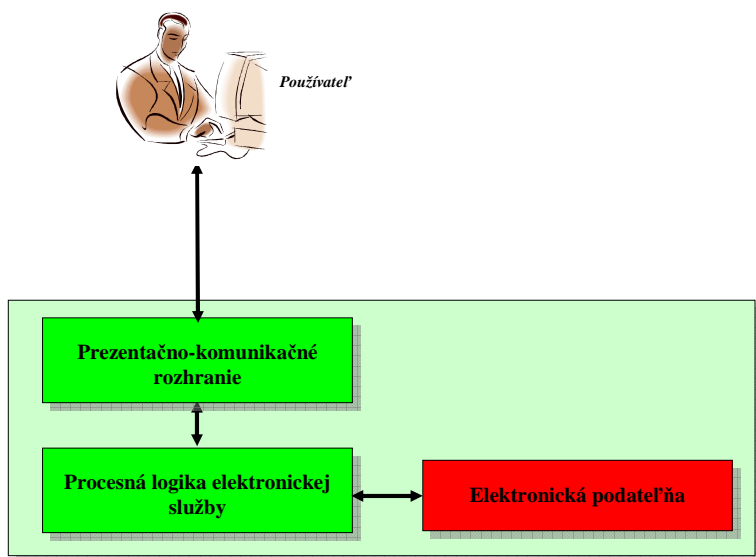
rozhrania pre zabezpečenie elektronickej komunikácie. V existujúcich implementáciách je možné identifikovať nasledujúce dva spôsoby integrácie elektronickej podateľne do architektúry poskytovania elektronických služieb:

- „Aktívna elektronická podateľňa“ – využitie vlastnej logiky spracovania elektronických dokumentov, ktorá je implementovaná elektronickou podateľňou. Elektronické podania sú spracovávané najskôr elektronickou podateľňou, a až následne sú odovzdané na spracovanie vlastnej logiky implementácie elektronickej služby. Takýto spôsob začlenenia elektronickej podateľne do procesov elektronických služieb je ilustrovaný na nasledujúcom obrázku.



Obrázok 1: Aktívna elektronická podateľňa

- „Pasívna“ elektronická podateľňa – využitie logiky spracovania elektronických dokumentov implementovaných v samostatnom module riadenia spracovania procesov (BPM – Business Process Manager), ktorý podľa potreby aktivuje jednotlivé funkcie elektronickej podateľne. Takýto spôsob začlenenia elektronickej podateľne do procesov elektronických služieb je ilustrovaný na nasledujúcom obrázku:

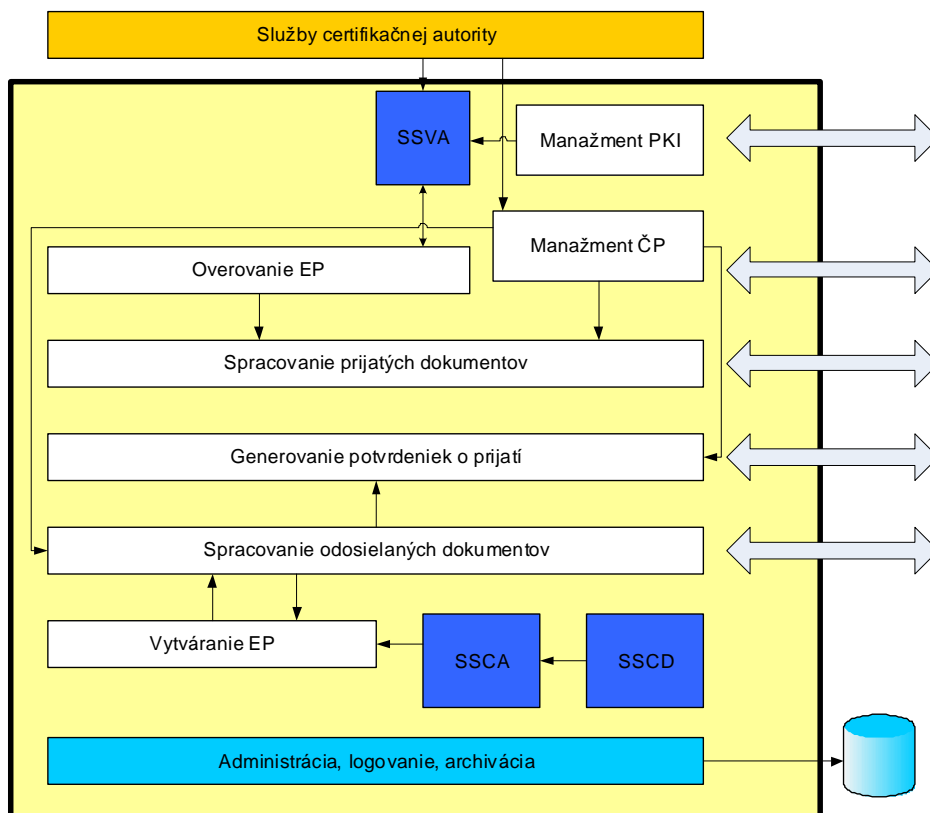


Obrázok 2: Pasívna elektronická podateľňa

Z hľadiska celkovej koncepcie začlenenia elektronickej podateľne do procesov spracovania elektronických služieb verejnej správy sa preferuje nasadenie elektronickej podateľne pracujúcej v „pasívnom“ režime.

3.1.2.2 *Koncepčná architektúra elektronickej podateľne*

Vnútrotná architektúra elektronickej podateľne (t.j. jej členenie na vnútorné moduly a ich vzájomné funkčné prepojenie) je závislá od jej konkrétnej implementácie. Každá architektúra však musí vytvárať podmienky pre zabezpečenie minimálnej zákonom požadovanej funkčnosti. Jeden z možných pohľadov na vnútornú architektúru elektronickej podateľne je ilustrovaný na nasledujúcom obrázku:



Obrázok 3: Architektúra elektronickej podateľne

3.1.2.3 Architektúra prevádzkového prostredia

Nasadenie elektronickej podateľne musí spĺňať prevádzkové a bezpečnostné požiadavky.

V zmysle vyhlášky NBÚ č. 136/2009 Z.z. je elektronická podateľňa prevádzkovaná podľa schváleného bezpečnostného projektu a bezpečnostnej smernice, na ktorých obsah a štruktúru sa primerane vzťahuje technická norma⁶. Z hľadiska prevádzkových požiadaviek je potrebné splniť nasledujúce požiadavky:

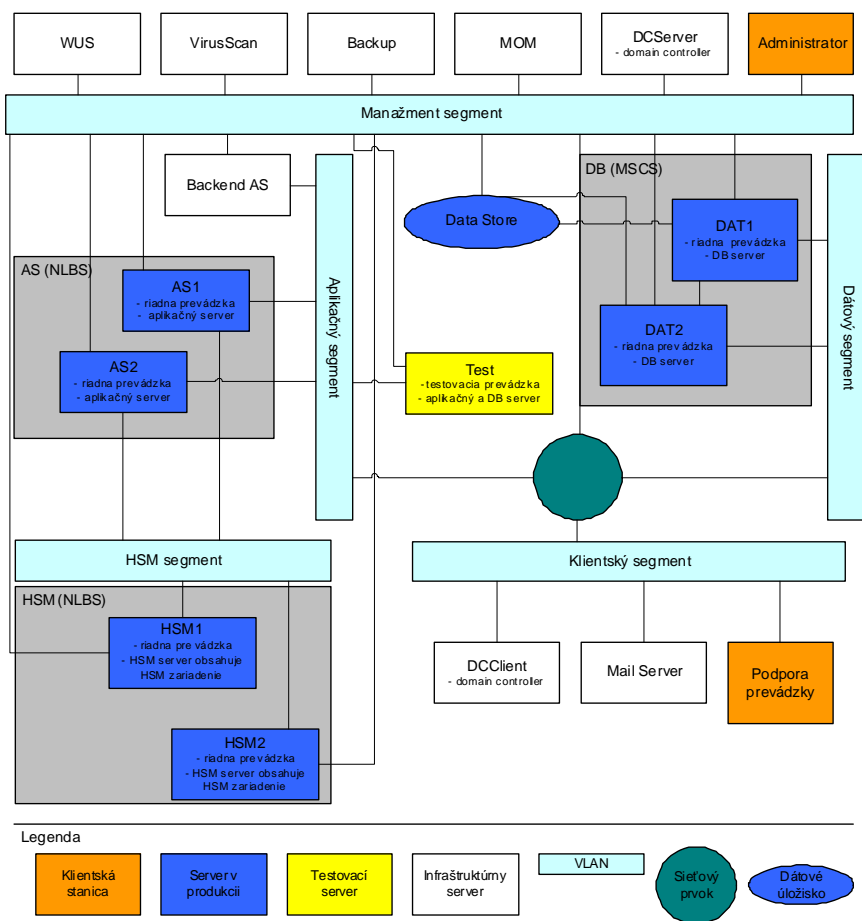
- **Odolnosť voči výpadkom** – infraštruktúra elektronickej podateľne musí zabezpečovať funkčnosť celého riešenia aj v prípade výpadku jedného z HW komponentov. Preto musí celá architektúra byť budovaná na princípoch fail-over.
- **Škálovateľnosť** – vzhľadom na predpokladaný nárast zaťaženia elektronickej podateľne, ako aj so zohľadnením efektívnosti vynakladania finančných prostriedkov na budovanie infraštruktúry, musí byť zabezpečená škálovateľnosť riešenia tak, aby bolo možné

⁶ STN ISO/IEC 27002. Informačné technológie. Zabezpečovacie techniky. Pravidlá dobrej praxe manažérstva informačnej bezpečnosti.

infraštruktúru plynule rozširovať podľa aktuálnych požiadaviek na jej výkonnosť a priepustnosť.

- Bezpečnosť (v zmysle dostupnosti) – prevádzková architektúra musí zabezpečovať ochranu kritických modulov pred útokmi potenciálnych narušiteľov. To sa týka najmä jednotlivých procesov, ale najmä hardvérových modulov (HSM) pre prácu so ZEP a ochrany privátnych kľúčov používaných pri vytváraní ZEP.

Príklad plánovanej architektúry prevádzkového prostredia ÚPVS je ilustrovaný na Obrázok 4. Vzhľadom k obmedzeným zdrojom však plánovaná prevádzková architektúra nie je dobudovaná, čím je nemožné splniť všetky vyššie uvedené prevádzkové požiadavky.



Obrázok 4: Príklad architektúry prevádzkového prostredia ÚPVS

3.1.3 Procesná analýza

Procesná analýza uvedená v nasledujúcich častiach sa týka najmä elektronických služieb poskytovaných prostredníctvom ÚPVS s využitím CEP. Nie sú pokryté špecifické procesy,

ktoré môžu byť určené napr. manuálnym spracovaním podaní v elektronickej podateľni, resp. špecifické procesy komunikácie s konkrétnym orgánom verejnej správy.

3.1.3.1 Vytváranie ZEP na podaní

ZEP sa používa v procesoch elektronických služieb na autorizáciu podaní. ZEP zabezpečuje dosiahnutie zákonom požadovaných formálnych náležitostí elektronických dokumentov potrebných pre ich použiteľnosť v elektronických procesoch verejnej správy. Vlastný proces vytvárania elektronického dokumentu môže byť od jeho podpísania ZEP oddelený. Elektronický dokument môže byť vytváraný manuálne (príslušným „editorom“ alebo na to určenou aplikáciou), alebo môže byť automaticky generovaný samostatnou aplikáciou.

Vytvorenie ZEP a jeho pripojenie k podpisovanému dokumentu môže byť rovnako manuálne alebo automatické.

Manuálne vytváranie ZEP

Manuálne vytváranie ZEP je realizované certifikovanou aplikáciou, kedy používateľ musí mať k dispozícii komerčne zakúpený kvalifikovaný certifikát verejného kľúča, ktorý je spolu s príslušajúcim tajným kľúčom uložený na bezpečnom HW zariadení. Po aktivácii aplikácie je analyzovaný vlastný podpisovaný dokument a používateľovi je zobrazený obsah elektronického dokumentu, ktorý bude podpisovaný. Následne používateľ vyberie podpisový certifikát a aplikácia pomocou HW zariadenia vytvorí ZEP, ktorý predpísaným spôsobom pripojí k podpisovanému dokumentu. Z hľadiska používateľa teda vytváranie ZEP predstavuje pomerne jednoduchý proces.

Odlíšnosti existujúcich riešení pre manuálne vytváranie ZEP sú jednak vo formáte vytváraného ZEP, ako aj v typoch podporovaných formátov elektronických dokumentov. Najvýznamnejším rozdielom však je spôsob, akým používateľ získa certifikovanú aplikáciu pre vytváranie ZEP. V súčasnosti sú k dispozícii nasledujúce prístupy:

- Komerčne dostupné prostriedky – používateľ si musí vopred zakúpiť certifikovaný prostriedok, prostredníctvom ktorého bude vytvárať ZEP. Prostriedok na overenie ZEP má voľne, bezplatne k dispozícii. Takýto prístup je použitý pre procesy Ministerstva spravodlivosti SR.
- Voľne dostupné prostriedky – pre používateľa sú k dispozícii prostriedky pre vytváranie a overovanie ZEP bezplatne v rámci poskytovanej služby (certifikovaný prostriedok je integrovaný do elektronických procesov poskytovania služby). Takýto prístup je využívaný na ÚPVS, Colnom a Daňovom riaditeľstve.

Automatické vytváranie ZEP

V prípade automatizovaného vytvárania ZEP na strane tvorcu podania je potrebné nasadenie elektronickej podateľne a v rámci nej certifikovaného prostriedku pre automatizované

vytváranie ZEP (takýto prostriedok je možné prevádzkovať iba v rámci elektronickej podateľne).

3.1.3.2 Zaslanie elektronického dokumentu so ZEP

Podanie, t.j. elektronický dokument autorizovaný ZEP, je zasielaný do elektronickej podateľne príslušného orgánu. Spôsob zasielania elektronického dokumentu môže byť špecifický pre konkrétny spôsob poskytovania elektronickej služby.

Vo väčšine implementovaných elektronických služieb je zaslanie elektronického podania realizované prostredníctvom portálového riešenia (zaslanie prostredníctvom elektronickej pošty nie je využívané). Portálové riešenie teda implicitne definuje zákonom požadovanú adresu elektronickej podateľne, ktorá je integrovaná do procesov poskytovania elektronických služieb a nie je používateľom dostupná samostatne.

Portálové riešenie (napr. ÚPVS) používateľovi poskytuje komunikačnú schránku, ktorá uchováva elektronickú komunikáciu medzi používateľom a daným orgánom verejnej správy. Portálové riešenie môže taktiež sprístupniť Webovú službu (Web Service), prostredníctvom ktorej je možné podanie zaslať automatizovaným spôsobom, bez potreby využitia používateľského rozhrania pre „manuálne“ zaslanie elektronického podania. Vo väčšine prípadov je podanie realizované ako XML dokument, ktorý zabezpečuje možnosť následného automatického spracovania údajov obsiahnutých v podaní.

Identický spôsob zaslania elektronického podania je aplikovateľný aj pre elektronické podania, ktoré nie sú autorizované prostredníctvom ZEP.

3.1.3.3 Prijatie elektronického dokumentu

Spôsob spracovania elektronického dokumentu v elektronickej podateľni je nezávislý od spôsobu jeho zaslania. Preto nasledujúce princípy sú platné pre činnosť elektronickej podateľne všeobecne.

Po prijatí elektronického dokumentu (podania) je logikou spracovania aktivovaný systém elektronickej podateľne. Ten preverí minimálne nasledovné formálne náležitosti elektronického dokumentu:

- kontrolu prijímaných elektronických dokumentov predovšetkým z hľadiska schopnosti ich bezproblémového čítania technickými prostriedkami elektronickej podateľne, dodržanie ustanoveného formátu a obsahu a neprítomnosť škodlivých kódov a bitových sekvencií (napríklad makrá, vírusy, trójske kone, červy a pod.),
- typ a formát elektronického dokumentu, vrátane verzie formátu dokumentu,
- požadované náležitosti elektronického dokumentu (napr. súlad s požadovanými schémami v prípade použitia XML dokumentov).

V prípade identifikácie nezrovnalostí prijatého elektronického dokumentu elektronická podateľňa zasiela odosielateľovi informáciu o odmietnutí dokumentu s uvedením dôvodu (kód chyby), ktorý autorizuje (potvrdenie o doručení). Takéto spracovanie elektronického dokumentu (podania) bude realizované aj pre elektronické podania bez ZEP.

V prípade pozitívneho overenia elektronického dokumentu je potrebné zabezpečiť podmienky pre jeho prípadné opätovné overenie v budúcnosti. Nakoľko vo väčšine prípadov používateľ (odosielateľ) vytvára ZEP bez časovej pečiatky (vydávanie časovej pečiatky je komerčnou službou), pripojí elektronická podateľňa k ZEP aj časovú pečiatku, t.j. transformuje ZEP z formy ZEP-EPES do formy ZEP-T (v prípade podania bez ZEP len doplní časovú pečiatku). Týmto je zároveň zabezpečená aj integrita takéhoto elektronického podania, najmä pokiaľ ide o podanie bez ZEP.

3.1.3.4 Overenie ZEP

Overovanie ZEP na zaslanom elektronickom dokumente je zabezpečované certifikovaným prostriedkom. V elektronickej podateľni pracujúcej v automatizovanom režime musí aj tento certifikovaný prostriedok pracovať v automatizovanom režime.

Overenie ZEP, v súlade s legislatívne definovanými požiadavkami, znamená získanie informácií potrebných na vlastné overenie platnosti ZEP (validačné dáta), s následným vlastným overením ZEP. Validačné dáta slúžia v hrubom priblížení na overenie platnosti kvalifikovaného certifikátu podpisovateľa v čase overovania (tento čas je spravidla daný časom obsiahnutým v časovej pečiatke viazanej na overovaný ZEP). Validačné dáta v zásade tvoria certifikáty v certifikačnej ceste (t.j. v ceste dôvery od vydavateľa kvalifikovaného certifikátu – ACA až po koreň certifikačnej cesty – certifikát NBÚ) a k nim viazané informácie o platnosti týchto certifikátov. Tieto môžu v súčasnosti byť poskytované nasledujúcim spôsobom:

- Zoznamy zrušených certifikátov (CRL), ktoré bývajú vydávané v pravidelných intervaloch, s maximálnou periodicitou 24 hodín. Pre overenie platnosti certifikátu v čase podpisovania je potrebné získať CRL vydaný bezprostredne po tomto čase.
 - Nakoľko potrebné validačné údaje nemusia byť v čase overovania k dispozícii (overovanie prebieha pred vydaním CRL nasledujúceho po čase vytvorenia ZEP), vo všeobecnosti nie je možné realizovať on-line overenie platnosti ZEP na báze využívania CRL. Elektronická podateľňa preto spravidla využíva stav „častočného overenia ZEP“, v ktorom boli vykonané všetky kontroly s dostupnými validačnými dátami a je potrebné vykonať záverečnú kontrolu po získaní potrebných validačných údajov. Po získaní potrebných validačných údajov je potom stav transformovaný na „overený“, resp. „neoverený“.
- On-line informácia o stave platnosti certifikátu – vo všeobecnosti realizovaná prostredníctvom OCSP protokolu, resp. iným spôsobom špecifikovaným v štandardoch vydávaných NBÚ. Možnosť využívania tohto prístupu bola síce dodatočne zavedená zákonom č. 214/2008 Z. z. (ktorý je novelou zákona o EP), v súčasnosti však tento protokol nepodporujú všetky ACA a preto ho nie je možné univerzálne využívať (ak čo len jedna ACA tento protokol nepodporuje, nie je vo všeobecnosti možné garantovať on-line overenie ZEP).

Väzba elektronickej podateľne a certifikovaného prostriedku pre overovanie ZEP významným spôsobom ovplyvňuje architektúru a procesy overovania vo vzťahu k získavaniu validačných údajov. V súčasnosti sú prakticky využívané nasledujúce prístupy:

- Validačné údaje získava a uchováva certifikovaný prostriedok pre overovanie ZEP. Získanie validačných údajov je iniciované vždy pri overovaní platnosti ZEP. Dôsledkom tohto prístupu sú nasledujúce faktory:
 - Nakoľko validačné údaje sú získavané iba pri overovaní konkrétneho ZEP, v sekvencii získavaných validačných údajov môžu vzniknúť „medzery“. Dôsledkom môže byť, že pri získavaní chýbajúcich validačných údajov k certifikátu, ktorému skončila platnosť (uplynula expiračná doba) je potrebná manuálna interakcia operátora certifikovaného prostriedku pre overovanie ZEP, čo je v rozpore s pôvodným zámerom automatizovaného spracovania podaní a overovania ZEP.
 - Takýto spôsob získavania a spracovávania validačných údajov komplikuje spôsob archivácie dokumentov so ZEP, resp. prevod ZEP na archívnu formu ZEP-A.
- Validačné údaje získava a uchováva elektronická podateľňa, ktorá pri overovaní ZEP poskytne certifikovanému prostriedku potrebné validačné dáta. Dôsledky takéhoto prístupu sú:
 - Elektronická podateľňa pravidelne v rámci vlastných procesov získava validačné dáta (napr. získava potrebné CRL) nezávisle od procesov overovania ZEP. Tým je zabezpečená úplnosť validačných údajov nezávisle od procesov overovania platnosti ZEP.
 - Vzhľadom na centrálny spôsob spracovania a uchovávania CRL údajov nie je problémová integrácia viacerých certifikovaných produktov pre overovanie ZEP.
 - Centrálna evidencia validačných údajov otvára širšie možnosti pre zabezpečenie dlhodobej archivácie dokumentov so ZEP.

Z vyššie uvedenej analýzy možností vzájomnej interakcie elektronickej podateľne a certifikovaného prostriedku pre overenie ZEP je zrejmé, že nie je možná (resp. je veľmi komplikovaná) vzájomná integrácia odlišných prostriedkov pracujúcich s odlišnou filozofiou.

3.1.3.5 Vystavenie potvrdenia o prijatí

Po prijatí a spracovaní elektronického dokumentu so ZEP, alebo aj bez ZEP, elektronická podateľňa vystavuje potvrdenie o prijatí elektronického dokumentu s použitím časovej pečiatky. V tomto potvrdení elektronická podateľňa buď potvrdí prijatie (t.j. úspešné doručenie do elektronickej podateľne a splnenie základných technických podmienok na prijatie) elektronického dokumentu, alebo jeho odmietnutie. V tomto prípade uvedie príčinu odmietnutia elektronického dokumentu (napr. prostredníctvom chybového kódu).

V praxi nie je zadefinovaný žiaden štandard na formu a obsah takéhoto potvrdenia o prijatí, preto existujúce riešenia implementujú vlastné proprietárne formy potvrdenia o prijatí. V zmysle platnej legislatívy možno konštatovať, že potvrdenie o prijatí elektronického dokumentu musí obsahovať minimálne identifikáciu prijatého dokumentu (ktorá ak má byť jednoznačná, tak by mala byť realizovaná prostredníctvom hash elektronického dokumentu) a zároveň musí obsahovať čas vystavenia potvrdenia realizovaný prostredníctvom časovej pečiatky.

3.1.3.6 Vytvorenie ZEP pre výstupy a rozhodnutia

V prípade automatického vytvárania ZEP systémom elektronickej podateľne je využívaná certifikovaná aplikácia určená špecificky na tento účel (NBÚ pre tento typ certifikovaných prostriedkov zaviedol samostatnú kategóriu). V tomto prípade po aktivácii činnosti elektronickej podateľne za účelom autorizácie dokumentu ZEP je aktivovaný proces vytvorenia ZEP, t.j. je certifikovanou aplikáciou analyzovaný obsah podpisovaného dokumentu a v automatickom režime je bez explicitného zobrazenia dokumentu vytvorený ZEP, ktorý je pripojený k podpisovanému elektronickému dokumentu.

Z dôvodov vytvorenia podmienok pre následné overenie platnosti ZEP elektronická podateľňa zabezpečí pridanie časovej pečiatky do vytvorenej štruktúry ZEP, čiže vytvára formát ZEP-T (CADES-T, či XAdES-T).

3.1.3.7 Odosielanie výstupov elektronickou podateľňou

Spôsob odosielania elektronických výstupov elektronickou podateľňou v rámci elektronických služieb verejnej správy závisí na konkrétnej implementácii elektronickej služby. Vo väčšine existujúcich prípadov sa používa portálové riešenie, kde odoslaná správa je uložená v komunikačnej schránke používateľa a takýmto spôsobom je mu sprístupnená. Existujúce riešenia v súčasnosti nezabezpečujú preukázateľné doručenie výstupu, nakoľko elektronický spôsob doručovania nie je legislatívne všeobecne ukotvený. Táto problematika je súčasťou štúdie uskutočniteľnosti pre modul elektronického doručovania.

3.1.3.8 Overenie ZEP používateľom

Po prijatí elektronického výstupu elektronickej služby verejnej správy autorizovanej prostredníctvom ZEP je potrebné overiť platnosť ZEP, a tým aj platnosť takéhoto elektronického dokumentu. Tu je potrebné vykonať nasledujúce úkony:

- Vlastné overenie platnosti ZEP.
- Overenie oprávnenia podpisovateľa k autorizácii daného typu dokumentu (rozhodnutia, odpisu a pod.). Za týmto účelom je možné využiť tzv. „mandátne certifikáty“ zavedené Zákom č. 214/2008 Z. z., v ktorých je oprávnenie držiteľa uvedené priamo v certifikáte, alebo je možné odkazovať na zoznam oprávnených certifikátov publikovaným poskytovateľom danej služby. Túto operáciu však musí vykonať používateľ a nie je súčasťou certifikovaných prostriedkov pre overovanie platnosti ZEP.

Pre overovanie platnosti ZEP používateľom, podobne ako v prípade automatického overovania v prostredí elektronickej podateľne, je potrebné sprístupniť validačné údaje a použiť certifikovaný prostriedok pre overovanie ZEP. V praxi sa používajú nasledujúce prístupy:

- Použitie certifikovaného prostriedku pre overovanie ZEP – v súčasnosti sú voľne k dispozícii certifikované prostriedky pre overovanie platnosti ZEP. Tieto zabezpečia pre dané overovanie platnosti ZEP získanie validačných údajov a následné overenie platnosti ZEP. Nakoľko však validačné údaje nie sú získavané pravidelne, môže nastať situácia, kedy v prípade, že certifikátu skončila platnosť, nie je možné validačné údaje získať automaticky a používateľ musí manuálne sprístupniť potrebné validačné údaje – napr. CRL vydané v konkrétnom časovom intervale.
- Použitie vystavenej služby ako možnosti overiť ZEP. V súčasnosti ÚPVS poskytuje bezplatnú službu informatívneho overenia platnosti ZEP pre používateľov. Služba využíva certifikované prostriedky elektronickej podateľne ÚPVS a po zaslaní dokumentu so ZEP používateľovi oznámi informatívny výsledok overovacieho procesu. Vzhľadom na skutočnosť, že komunikačný kanál, ktorým sa pre používateľov tejto služby zobrazuje výsledok overenia nie je súčasťou certifikovanej aplikácie pre overenie ZEP, je spolaľnosť sa na správnosť takto získanej informácie o stave podpisu v plnej zodpovednosti používateľa tejto služby.

3.1.3.9 Overenie ZEP z dlhodobého hľadiska

Z hľadiska používania elektronických dokumentov podpísaných ZEP je dôležité zabezpečiť možnosť overenia ZEP aj po uplynutí platnosti pôvodného certifikátu, ktorý prislúcha ku tajnému kľúču prostredníctvom, ktorého bol ZEP vyhotovený. To spočíva v zabezpečení integrity elektronického dokumentu, elektronického podpisu a validačných údajov potrebných na jeho overovanie. V súčasnosti je v praxi využívaný princíp transformácie štruktúry ZEP na štandardmi odporúčanú archívnu formu (t.j. CAdES-A, resp. XAdES-A). Táto transformácia znamená doplnenie všetkých validačných údajov do štruktúry podpisu a zabezpečenie ich integrity archívnu časovou pečiatkou.

Tento spôsob je vhodný v prípade archivácie malého množstva elektronických dokumentov so ZEP – pre koncových používateľov elektronických služieb. V prípade poskytovateľov elektronických služieb, u ktorých sa predpokladá spracovávanie a uchovávanie veľkého množstva dokumentov so ZEP, takýto spôsob uchovávania spôsobuje nasledujúce prevádzkové problémy:

- V každej archívnej štruktúre ZEP sa uchováávajú kompletne validačné dáta, t.j. existuje výrazná duplicita údajov. Toto zvyšuje nároky na pamäťové kapacity.
- Každá archívna časová pečiatka po čase expiruje a je ju potrebné pred expiráciou obnoviť. V prípade archívneho ZEP je potrebné vkladať novú archívnu pečiatku do každej štruktúry ZEP. V prípade veľkého množstva dokumentov a jednotlivých podpisov toto predstavuje nemalé prevádzkové náklady, nakoľko služba časovej pečiatky je poskytovaná na komerčnej báze.

V prípade archivácie väčšieho množstva elektronických dokumentov so ZEP bude potrebné zaviesť iný, efektívnejší spôsob vyhotovovania archívnej formy ZEP, napr. formou oddeleného uchovávanía elektronických dokumentov so ZEP a samostatného uchovávanía validačných údajov, čím sa zabezpečí ich unikátne uchovávanie. Integrita týchto údajov môže byť hromadne chránená archívnu časovou pečiatkou, čím sa výrazne znížia požiadavky na počet potrebných časových pečiatok (tzv. balíčkovanie údajov). Podobné riešenia sú prevádzkované niekoľko rokov a v praxi sa osvedčili (napr. CRSR, DRSR).

3.1.4 Legislatívna analýza

Podľa zákona č. 215/2002 Z. z. o elektronickom podpise je elektronickou podateľňou technické zariadenie slúžiace najmä na prijímanie, odosielanie a potvrdzovanie prijatia elektronických dokumentov, elektronických dokumentov podpísaných elektronickým podpisom a elektronických dokumentov podpísaných zaručeným elektronickým podpisom. Podľa § 24 ods. 8 tohto zákona súlad elektronickej podateľne s požiadavkami podľa tohto zákona overuje a potvrdzuje Národný bezpečnostný úrad na základe žiadosti a vydáva osvedčenie o zhode s požiadavkami podľa tohto zákona. Ak úrad rozhodne o súlade elektronickej podateľne s požiadavkami tohto zákona, vydá osvedčenie o zhode s požiadavkami tohto zákona, ktorého platnosť je najviac päť rokov.

Podľa vyhlášky Národného bezpečnostného úradu č. 136/2009 Z. z. elektronická podateľňa, ktorej elektronickú adresu oznámil orgán verejnej moci úradu podľa § 29 ods. 1 zákona, zabezpečuje administratívny styk. Administratívnym stykom sa podľa §2 citovanej vyhlášky NBÚ rozumie odoslanie, prijatie alebo potvrdenie odoslania, alebo potvrdenie prijatia elektronického dokumentu podpísaného platným elektronickým podpisom alebo zaručeným elektronickým podpisom medzi orgánmi verejnej moci alebo medzi orgánom verejnej moci a fyzickou osobou, alebo medzi orgánom verejnej moci a právnickou osobou. Pri manipulácii s elektronickým dokumentom, najmä pri potvrdzovaní jeho prijatia alebo postúpení na ďalšiu manipuláciu využíva elektronická podateľňa službu časovej pečiatky. Bezpečnosť prevádzky elektronickej podateľne musí zodpovedať bezpečnostným dokumentom prijatým orgánom verejnej moci a vychádza z jeho bezpečnostnej politiky.

Ustanovenia § 6 ods. 2 predmetnej vyhlášky ustanovujú aj požiadavky na funkcionálnu elektronickej podateľne. Podľa týchto požiadaviek elektronická podateľňa zabezpečuje:

- prijímanie, odosielanie, overovanie, potvrdzovanie a spracovanie elektronických dokumentov prostredníctvom (i) siete na prenos údajov, (ii) elektronickej pošty a (iii) štandardných nosičov údajov,
- kontrolu prijímaných elektronických dokumentov najmä na schopnosť ich bezproblémového čítania technickými prostriedkami elektronickej podateľne, dodržanie ustanoveného formátu a obsahu a neprítomnosť škodlivých kódov a bitových sekvencií (makrá, vírusy, trójske kone, červy a pod.),
- overenie platnosti kvalifikovaného certifikátu viazaného na zaručený elektronický podpis elektronického dokumentu,

- potvrdenie o prijatí alebo odmietnutí elektronického dokumentu vydaním vlastného elektronického dokumentu s použitím časovej pečiatky,
- odoslanie elektronického dokumentu na ďalšie vybavenie v orgáne verejnej moci alebo v orgáne verejnej správy,
- prijatie elektronického dokumentu vybaveného alebo vytvoreného úradom na jeho odoslanie mimo orgánu verejnej moci alebo orgánu verejnej správy.

Príloha č. 1 predmetnej vyhlášky ustanovuje podrobné zásady pre prijímanie a potvrdzovanie prijatia elektronických podaní.

Orgán verejnej moci má po zriadení elektronickej podateľne povinnosť zverejniť⁷:

- zoznam úplných elektronických adries umožňujúcich styk s elektronickou podateľňou,
- adresu umiestnenia elektronickej podateľne a adresu, na ktorej možno s orgánom verejnej moci alebo s orgánom verejnej správy komunikovať o otázkach využívania a činnosti elektronickej podateľne,
- zoznam kvalifikovaných certifikátov alebo úplnú elektronickú adresu, na ktorej sa nachádza zoznam kvalifikovaných certifikátov všetkých zamestnancov orgánu verejnej moci alebo orgánu verejnej správy, ktorí zabezpečujú prevádzku elektronickej podateľne,
- formáty elektronických dokumentov z množiny prípustných formátov, ktoré elektronická podateľňa prijíma,
- typy a charakteristiky nosičov údajov, na ktorých elektronická podateľňa elektronické dokumenty prijíma,
- pravidiel zasielania elektronických dokumentov a potvrdzovania ich prijatia vrátane možného časového obmedzenia styku s elektronickou podateľňou,
- zoznam typov prijímaných elektronických dokumentov a spôsob získania elektronických predlôh podaní.

Podľa § 2 písm. h) zákona č. 275/2006 Z. z. o ISVS je funkciou ÚPVS o. i. aj elektronická podateľňa. Zo štúdií k MED, eDesk a eForm vyplýva, že modul centrálnej elektronickej podateľne ako aj modul elektronického doručovania budú súčasťou ÚPVS. V častiach týchto štúdií, týkajúcich sa legislatívnych dopadov sa navrhuje, aby sa generálnym zákonom ustanovilo (zjednodušene), že (i) ak sa v danom konaní umožňuje elektronické podanie podaní, potom sa toto realizuje cez ÚPVS a (ii) ak sa v konaní umožňuje elektronické doručovanie rozhodnutí, potom sa toto realizuje cez MED a eDesk. Z technického hľadiska je CEP

⁷ Podľa novej vyhlášky NBÚ č. 136/2009 Z. z. sa už orgánu verejnej moci neukladá povinnosť zriadiť elektronickú podateľňu, ak orgán využíva ZEP. Zo znenia platnej legislatívy teda vyplýva, že orgán verejnej moci môže zriadiť vlastnú elektronickú podateľňu, rovnako ako môže zabezpečiť funkcie podateľne prostredníctvom CEP v rámci ÚPVS či zdieľaním elektronickej podateľne s inými orgánmi.

osobitným modulom, avšak z právneho hľadiska len prostriedkom na zabezpečenie najmä podávania a prijímania podaní, resp. odosielania rozhodnutí a potvrdzovania samotného podania/odoslania, resp. fixácie času, v ktorom k nim došlo. Ak sa teda elektronické podávanie a elektronické doručovanie realizuje cez ÚPVS a súčasťou ÚPVS je aj CEP, ako nástroj na realizáciu týchto činností, potom legislatíva nekladie žiadne zásadné prekážky na využívanie CEP ako nástroja na realizáciu týchto procesných inštitútov.

Vyššie uvedené platí aj pri súčasne platnej legislatíve a explicitne bude ustanovené, resp. navrhuje sa ustanoviť aj v novele zákona o ISVS, kde sa § 5 (obsahujúci ustanovenia o ÚPVS), dopĺňa novými odsekmi, podľa ktorých:

- podanie uskutočnené prostredníctvom elektronickej podateľne ústredného portálu má rovnaké právne účinky ako podanie uskutočnené prostredníctvom elektronickej podateľne príslušnej povinnej osoby, ak povinná osoba uvedie ústredný portál ako elektronickú adresu umiestnenia svojej elektronickej podateľne,
- prevádzkovateľ ústredného portálu zodpovedá za riadne a nepretržité fungovanie ústredného portálu, za nepretržitú dostupnosť jeho služieb a technické zabezpečenie doručenia podaní príslušnému orgánu verejnej moci alebo orgánu verejnej správy cez ústredný portál.

Predmetná novela teda „zrovnoprávňuje“ elektronickú podateľňu ÚPVS s elektronickými podateľňami jednotlivých orgánov verejnej moci vtedy, ak orgán verejnej moci uvedie ÚPVS ako adresu umiestnenia svojej elektronickej podateľne.

Predpokladom na využitie CEP v jednotlivých konaniach je možnosť realizovať elektronické podanie, resp. vydávanie rozhodnutí v elektronickej podobe. Týmto otázkam sa venujeme podrobne v štúdiu k MED, eDesk, resp. eForm – preto na účel tejto štúdie budeme tieto podmienky považovať za splnené.

Z hľadiska práva je presné určenie podateľne, resp. miesta, kde ten ktorý orgán prijíma podania, dôležité najmä z hľadiska ustanovení o vecnej a miestnej príslušnosti orgánu verejnej moci. Na relevantnú inicializáciu konania, resp. dodržanie procesných lehôt je dôležité podať podanie na tom orgáne, ktorý je príslušný vecne (teda je oprávnený v danej veci „kompetenčne“ konať) a tiež miestne (teda v skupine „kompetenčne“, vecne príslušných orgánov je tým z týchto orgánov, ktorý v danom prípade je oprávnený konať). Zjednodušene povedané, kým vecná príslušnosť je závislá od povahy veci, o ktorú v konaní ide (napr. pri ochrane osobnosti je príslušný súd) tak miestna príslušnosť určuje, ktorý zo súdov je oprávnený konať v konkrétnom stupni konania (napr. súd, v obvode ktorého má bydlisko navrhovateľ).

V „papierovom svete“ realizuje správne určenie vecnej a miestnej príslušnosti v zásade ten, kto podanie podáva a následne orgán, ktorému bolo podané, svoju príslušnosť skúma. Na tomto mieste nemá význam podrobná analýza postupu orgánu, ak zistí, že nie je príslušný, resp. dopad podania na nepríslušný orgán na postavenie podávajúceho v konaní. Preto sa obmedzíme len na základné pravidlá, ktoré v zásade platia vždy. V prvom rade platí zásada, že ak sa podanie realizuje na nepríslušný orgán, tento má povinnosť postúpiť ho orgánu príslušnému a to tak, aby pokiaľ možno bolo minimalizované nebezpečenstvo škody, vzniknutej z omeškania. Nie bez výnimky, ale v mnohých konaniach platí, že ak sa podanie realizuje na nepríslušný orgán, lehoty zostávajú zachované. Doručenie podania príslušnému orgánu je v zásade momentom,

kedy sa konanie začína – teda ak sa podá na nepríslušný orgán, začína vtedy, kedy vec po postúpení dôjde orgánu príslušnému.

Uvedené platí aj vo svete elektronickom, pretože, zjednodušene povedané, ak sa umožňuje elektronické podanie, potom elektronická podateľňa orgánu je len iný komunikačný kanál a iná adresa na doručenie podania. Moment, kedy orgán podaním disponuje (kedy mu dôjde) je momentom začatia konania rovnako, ako v „papierovom svete“. Z hľadiska implementácie CEP je teda z právneho hľadiska dôležité, či elektronická podateľňa ÚPVS je alebo nie je adresou na doručovanie orgánom verejnej moci – inými slovami, či prijatie podania CEP je alebo nie je prijatím podanie konkrétnym orgánom verejnej moci. Ak je, tak vo zvyšku sú procesné predpisy použiteľné bez úpravy. Bližšie k tomu v časti 4.4.3.

3.2 Hodnotenie aktuálneho stavu

Aktuálny stav v oblasti nasadzovania elektronických podateľní je možné charakterizovať ako stav, v ktorom sú k dispozícii funkčné riešenia nasadenia elektronických podateľní a ich integrácia do reálne poskytovaných elektronických služieb verejnej správy. Z prevádzky týchto riešení je možné identifikovať nasledujúce problémy, ktoré je potrebné pri ďalšom rozvoji tejto oblasti riešiť:

- Neexistencia jasnej koncepcie budovania systému elektronických podateľní. V súčasnosti je síce v rámci ÚPVS vybudovaná centrálna podateľňa, jej využívanie však nie je legislatívne ukotvené. Nie je spracovaná analýza, kedy je vhodné pre daný orgán verejnej správy vybudovať vlastnú elektronickú podateľňu, alebo využiť funkčnosť centrálnej elektronickej podateľne. Budovaním samostatných podateľní môže dochádzať k neefektívnemu využívaniu aj tak obmedzených finančných prostriedkov. Naopak, pri využití centrálnej elektronickej podateľne na príliš veľké množstvo agend so značným množstvom podaní denne môže viesť k tomu, že CeP nebude technicky zvládať uvedený nápor, resp. by riešenie CeP bolo značne finančne nákladné ako keby sa pre vybranú agendu(y) realizovali rezortné elektronické podateľne.
- Nedostatočná úroveň štandardizácie. Tá sa týka najmä nasledujúcich oblastí:
 - Štandardizácia formátov ZEP (používanie viacerých profilov).
 - Štandardizácia spôsobu väzby ZEP na podpisovaný dokument.
 - Štandardizácia formy a obsahu elektronického potvrdenia o prijatí elektronického dokumentu vystavovaného elektronickou podateľňou.
 - Štandardizácia metodiky a procesov dlhodobej archivácie elektronických dokumentov so ZEP. Štandardizácia musí byť vykonávaná spôsobom, aby sa v maximálnej miere zohľadnili existujúce riešenia. Znamená to, že štandardizácia nemôže vyústiť k nahrádzaniu všetkých existujúcich riešení novými, ale snaha musí smerovať k zachovaniu čo najväčšieho množstva existujúcich riešení v súlade s pripravovanými štandardami.

- Neexistencia centrálnej evidencie povolených schém dokumentov (definovaných dátových štruktúr XML schém) a k nim pripojených vizualizačných schém. V súčasnosti sú tieto evidované proprietárnym spôsobom subjektom zabezpečujúcim poskytovanie danej elektronickej služby. V budúcnosti je táto funkčnosť plánovaná pre eForm modul.
- Nemožnosť on-line overovania platnosti ZEP, čo má vplyv na procesy poskytovania elektronických služieb. Pre služby s požadovanou dobou odozvy (nižšou ako stredná doba úplného overenia ZEP) je potrebné definovať nové procesy, prípadne vykonať analýzu rizík umožňujúcu ďalšie spracovanie na báze iba čiastočne overeného ZEP. Použitie protokolu OCSP, ktoré by uvedený problém riešilo, nie je štandardizované, a zatiaľ nie je v SR podporované zo strany všetkých ACA. Rozhranie na OCSP bude potrebné implementovať v rozhraní elektronickej podateľne, ako aj zdefinovať spôsob dlhodobej archivácie dokumentov so ZEP, kde platnosť certifikátov nebude overovaná na báze CRL, ale OCSP.
- Poddimenzovanie prevádzkového prostredia – v súčasnosti je nasadenie CEP na ÚPVS funkčné, no nie je pripravené na masívny nárast počtu spracovávaných podaní vzhľadom na HW infraštruktúru, ktorá je pre prevádzku CEP dostupná. Súčasne nie je dostatočne zabezpečené prevádzkové prostredie proti výpadkom jednotlivých komponentov.

3.3 Návrh zmeny

Návrh zmeny vyplýva zo spôsobu riešenia problémov identifikovaných v predchádzajúcej časti. Ciele navrhovaných zmien je možné sumarizovať nasledovne:

- Vypracovanie jasne definovaného systému a metodiky nasadzovania elektronických podateľní pri implementácii elektronických služieb verejnej správy s jasnou prioritizáciou využívania centrálnej elektronickej podateľne (CEP) prevádzkovej v rámci ÚPVS.
- Zabezpečenie efektívneho využitia funkčnosti ďalších centralizovaných modulov definovaných v NKIVS za účelom efektívneho nasadzovania a integrácie elektronickej podateľne do procesov elektronických služieb.
- Zabezpečenie vzájomnej kompatibility prostriedkov ZEP pri komunikácii používateľov s verejnou správou, ako aj medzi orgánmi verejnej správy navzájom. Táto kompatibilita bude dosahovaná cielenou štandardizáciou všetkých aspektov používania ZEP v elektronických procesoch služieb verejnej správy, ako aj nasadzovania elektronických podateľní.
- Sprístupnenie infraštruktúry PKI pre čo najširšie spektrum používateľov. Toto bude dosahované orientáciou na bezplatné poskytovanie prostriedkov pre vyhotovenie a overovanie ZEP. Okrem samostatných prostriedkov budú pre používateľov poskytované služby spojené s PKI (napr. informatívne overovanie platnosti ZEP alebo prevod ZEP do archívnej formy a pod.).

4 Navrhnuté riešenie

Návrh riešenia CEP, resp. metodiky nasadzovania elektronických podateľní na vybraných orgánoch verejnej správy, vyplýva z naplnenia cieľov definovaných v predchádzajúcej časti tohto dokumentu.

4.1 Popis navrhovaného riešenia

4.1.1 Popis služieb a funkcionality

Základné služby, ktoré bude CEP poskytovať sú:

- pre oblasť spracovania podaní:
 - prijatie elektronického dokumentu alebo elektronického dokumentu podpísaného elektronickým podpisom.
- pre oblasť spracovania požiadaviek na PKI služby elektronickej podateľne:
 - autorizácia odosielaného dokumentu (vytvorenie ZEP odosielaného dokumentu),
 - informatívne overenie ZEP na poskytnutom elektronickom dokumente,
 - prevod ZEP na archívnu formu,
 - vytvorenie archívnej časovej pečiatky,
 - poskytnutie validačných údajov (CRL) pre kvalifikované certifikáty.

Ďalšie základné interné funkcie CEP sú nasledovné:

- overenie formálnych náležitostí prijatého elektronického dokumentu,
- overenie ZEP prijatého dokumentu,
- doplnenie časovej pečiatky k prijatému elektronickému dokumentu (so ZEP aj bez ZEP),
- vystavenie potvrdenia o prijatí so ZEP s časovou pečiatkou (pokiaľ nejde o anonymné podanie),
- získavanie a archivovanie CRL ku kvalifikovaným certifikátom.

4.1.2 Konceptia riešenia elektronickej podateľne

Koncept navrhovaného riešenia spočíva vo vybudovaní CEP a systému rezortných elektronických podateľní prevádzkovaných vybranými orgánmi verejnej správy. Tieto

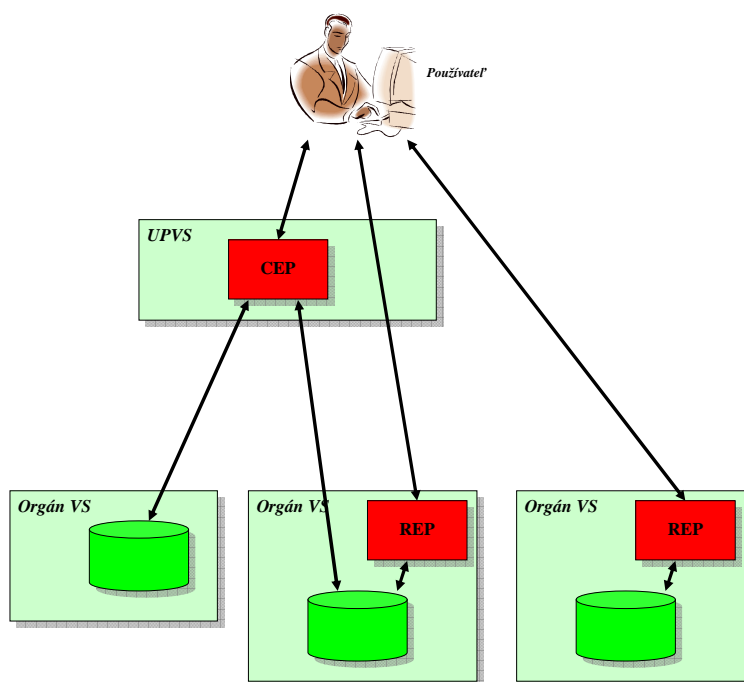
elektronické podateľne budú okolitému prostrediu, v ktorom sú nasadené, poskytovať zákonom a procesmi požadované funkcie a služby. Táto koncepcia nasadzovania elektronických podateľní je založená na nasledujúcich princípoch:

- Preferované využívanie modulu **centrálnej elektronickej podateľne (CEP)**⁸, ktorá bude prevádzkovaná v rámci ÚPVS. Modul CEP bude primárne využívaný pre spracovanie podaní zasielaných prostredníctvom ÚPVS ako prístupového bodu elektronických služieb verejnej správy. Súčasne bude využívaný pre autorizáciu centrálne distribuovaných výstupných dokumentov (t.j. elektronických rozhodnutí, resp. elektronických výstupov z ISVS) pre orgány verejnej správy, ktoré sa rozhodnú takúto službu CEP využívať.
- Modul CEP bude okrem štandardných služieb elektronickej podateľne prostredníctvom ÚPVS poskytovať aj základné služby práce s elektronickým podpisom – službu informatívneho overovania platnosti ZEP a službu prevodu ZEP do nasledovných foriem:
 - ZEP-T,
 - ZEP-A.
- Súčasne bude modul CEP zhromažďovať a predpísaným spôsobom uchovávať validačné dáta, potrebné pre zabezpečenie dlhodobého overovania platnosti ZEP na elektronických dokumentoch. Tieto dáta bude pre overenie konkrétneho ZEP poskytovať prostredníctvom elektronickej služby ďalším modulom, ktoré budú túto funkcionality požadovať.
- Nasadzovanie **rezortnej elektronickej podateľne (REP)**⁹ je primárne určené pre autorizáciu elektronických výstupov z ISVS a rozhodnutí daného orgánu automatickým spôsobom (v prípade že daný orgán verejnej správy nevyužíva takúto službu v rámci CEP), najmä vzhľadom na potrebu plnej kontroly nad procesom autorizácie zo strany príslušného orgánu verejnej správy alebo vzhľadom na značné množstvo prijímaných podaní.
- Rezortná elektronická podateľňa by mala byť určená na spracovanie elektronických podaní, ak je predpokladaná vysoká početnosť podaní (a tým neúmerne vysoká záťaž CEP) alebo príslušný rezort prijíma podania prostredníctvom vlastného portálového rozhrania mimo ÚPVS (t.j. podania na REP sú zadávané prostredníctvom informačného portálu príslušného rezortu, alebo portálu príslušného orgánu verejnej správy).
- Dôvodom na nasadenie REP môžu byť aj iné režimové opatrenia a bezpečnostné požiadavky jednotlivých rezortov, resp. orgánov verejnej správy.

Možnosti nasadzovania modulov CEP a REP a ich použitie v elektronickej komunikácii s používateľmi elektronických služieb verejnej správy je ilustrovaný na nasledujúcom obrázku:

⁸ Modul CEP je v dokumente NKIVS definovaný ako jeden zo spoločných modulov UPVS.

⁹ Modul REP je v dokumente NKIVS definovaný ako jeden z administratívnych systémov v aplikačnej vrstve informačného systému úseku.



Obrázok 5: Nasadenie modulov CEP a REP

Dôležitým aspektom popisovanej koncepcie nasadzovania elektronických podateľní je ich interoperabilita a podpora dosahovania cieľov NKIVS. Z tohto pohľadu sú dôležité nasledujúce princípy:

- Podpora jednoznačne definovaných profilov formátov pre ZEP – všetky nasadzované elektronické podateľne budú podporovať štandardizované formáty ZEP. Súčasne bude podporovaný jeden profil ZEP, ktorý zabezpečí interoperabilitu medzi rôznymi certifikovanými prostriedkami pre vytváranie a overovanie ZEP. Výber používaného certifikovaného prostriedku bude na používateľovi.
- V rámci implementovaných elektronických služieb bude používateľom bezplatne poskytovaná základná infraštruktúra pre používanie ZEP. Jedná sa o certifikované prostriedky a služby, prostredníctvom ktorých bude môcť používateľ vykonávať základné funkcie vytvárania a overovania ZEP s dôrazom na jednoduchosť ich používania. Takýto prístup nevylučuje používanie komerčne dostupných produktov, ktoré používateľovi poskytujú vyššiu funkčnosť a používateľský komfort vzhľadom k bezplatne poskytovaným prostriedkom a službám.
- Štandardizácia štruktúry elektronického podania, t.j. elektronického formulára podania k službe a k nemu viazaných možných elektronických príloh, ktoré môžu byť súčasťou podpísaného podania, resp. môžu byť samostatne autorizované treťou stranou (napr. vydávané potvrdenia alebo výpisy).
- Podpora spracovania viacnásobných podpisov, ako aj podpisov viacerých objektov, resp. kombinácie oboch týchto spôsobov.

- Štandardizácia väzby ZEP na podpisované dokumenty (objekty) – CEP aj všetky REP budú podporovať jeden štandard, ktorý bude implementovaný taktiež v aplikáciách implementujúcich elektronické služby verejnej správy.
- Štandardizácia obsahu a formy potvrdenia o doručení – CEP a všetky REP budú vydávať jednotné potvrdenky o doručení. Centrálne bude publikovaný zoznam možných chybových kódov odmietnutia podania, ktorý bude oznamovaný používateľovi.
- Zabezpečenie podpory najpoužívanejších formátov elektronických dokumentov. Tieto budú zabezpečené dostupnosťou certifikovaných prostriedkov pre vytváranie a overovanie ZEP pre tieto formáty elektronických dokumentov. Z hľadiska podporovaných formátov dokumentov je potrebné zabezpečiť najmä nasledujúce formáty:
 - XML - používaný pre prenos štruktúrovaných údajov. Pre XML dokumenty bude zabezpečené vytváranie ZEP pre všeobecné XML schémy, ako aj pre špecifické schémy určené pre elektronické formuláre – napr. 602XML),
 - PDF – pre prenos neštruktúrovaných údajov a dokumentov.
- Zber a uchovávanie validačných údajov – CEP a REP budú zabezpečovať zber validačných údajov a ich uchovávanie so zabezpečením preukázateľnosti integrity týchto dlhodobo uchovávaných údajov. Tieto údaje budú poskytované ďalším aplikáciám pre potreby overovania dlhodobo uchovávaných dokumentov so ZEP.

Koncepcia dlhodobého uchovávania elektronických dokumentov so ZEP je založená na nasledujúcich princípoch:

- Produkčný systém je zodpovedný za uchovávanie elektronického dokumentu so ZEP (vo formáte ZEP-T). produkčný systém zodpovedá za preukázateľné zabezpečenie integrity týchto dokumentov, napr. archívnu časovú pečiatkou.
- Modul CEP a REP zodpovedá za získanie a uchovávanie všetkých validačných údajov (CRL a certifikátov) a preukázateľné zabezpečenie ich integrity, napr. archívnu časovú pečiatkou.
- Pri overení ZEP na konkrétnom dokumente sa pre verifikačný proces poskytne dokument so ZEP, ako aj validačné dáta zodpovedajúce podpisovanému certifikátu (certifikačná cesta) k danému času vytvorenia podpisu (obsiahnutého v časovej pečiatke v ZEP-T).

Modul elektronickej podateľne bude viesť vlastnú evidenciu oprávnených používateľov (administrátorov systému elektronickej podateľne) a ich oprávnení pre administráciu elektronickej podateľne. CEP bude pre služby identifikácie a autentifikácie využívať spoločný modul NKIVS, ktorým je IAM modul.

Riešenie CEP a REP bude vychádzať z existujúceho riešenia elektronickej podateľne ÚPVS, ktoré už v súčasnosti preukázalo svoju funkčnosť a vhodnosť zvolenej koncepcie budovania. Nakoľko je to otvorené a modulárne riešenie, je možné ho postupne rozširovať o novú funkčnosť podľa potrieb.

Návrh riešenia vychádza z koncepcie rozšírenia funkčnosti existujúceho riešenia elektronickej podateľne a rozšírenia tohto riešenia na všetky požadované nasadenia REP.

4.1.3 Popis základných procesov

Základnými procesmi CEP a REP viazanými na procesy elektronických služieb verejnej správy sú nasledujúce procesy:

- spracovanie podania,
- autorizácia odosielaného dokumentu,
- spracovanie požiadavky na PKI službu elektronickej podateľne.

Súčasne s vyššie uvedenými procesmi sú v rámci CEP poskytované používateľom nasledujúce funkcie:

- prostriedky pre vytváranie ZEP na podaní (elektronickom dokumente),
- informatívne overenie platnosti ZEP na prijatom rozhodnutí, resp. výstupe z IS VS.

4.1.3.1 Podanie

Podanie je na systém elektronickej podateľne doručené nasledujúcim spôsobom:

- Elektronické podanie zaslané prostredníctvom ÚPVS. Toto podanie je spracovávané CEP, alebo v prípade existencie REP je zaslané na spracovanie príslušnej REP.
- Elektronické podanie zaslané prostredníctvom portálu príslušného orgánu verejnej správy. Toto podanie je spracovávané REP príslušného orgánu verejnej správy.

Bez ohľadu na spôsob zaslania podania je ďalšie spracovanie podania v oboch vyššie uvedených prípadoch identické. Funkčnosť CEP a REP je v oboch prípadoch identická a je nasledovná:

- spracovanie podania a overenie formálnych náležitostí (formát dokumentu, platnosť elektronickej predlohy - elektronického formulára a pod.),
- kontrola platnosti ZEP na elektronickom podaní/dokumente v prípade, že tento je autorizovaný prostredníctvom ZEP (pod podaním je chápaná aj možná štruktúra viacerých elektronických dokumentov a k nim viazaných viacerých podpisov),
- doplnenie časovej pečiatky do ZEP, v prípade, že podanie/elektronický dokument nie je autorizovaný prostredníctvom ZEP s časovou pečiatkou a taktiež doplnenie časovej pečiatky v prípade, že podanie/elektronický dokument nie je autorizovaný prostredníctvom ZEP,

- vystavenie elektronického potvrdenia o prijatí s prípadným uvedením príčiny odmietnutia podania, ktoré je autorizované ZEP¹⁰ elektronickej podateľne s časovou pečiatkou.

4.1.3.2 *Autorizácia odosielaného dokumentu*

V prípade potreby automatizovaného spôsobu autorizácie elektronického dokumentu (resp. aj rozhodnutia alebo výstupu ISVS obsahujúceho viacero elektronických dokumentov) je dokument zaslaný elektronickej podateľni (CEP alebo REP). Elektronická podateľňa automaticky vytvorí ZEP¹¹, ktorý je následne pripojený k podpisovanému dokumentu. Vytváraný ZEP je vo formáte ZEP-T.

Dôležitou funkčnosťou elektronickej podateľne je možnosť výberu podpisového kľúča, ktorým je ZEP podpisovaného dokumentu vytváraný. Týmto je umožnené používať rôzne podpisové kľúče pre vytváranie ZEP používaného pre autorizáciu rôznych typov rozhodnutí alebo výstupov z ISVS. Takúto funkčnosť musí však podporovať certifikovaný prostriedok pre automatické vytváranie ZEP určený pre použitie v elektronickej podateľni. Takáto funkčnosť umožní autorizovať v CEP dokumenty aj „v mene“ iného orgánu, ak tento orgán bude súhlasiť s uložením vlastného privátneho kľúča v HSM zariadení CEP, resp. REP v prípade autorizácie odosielaného dokumentu v mene určitej organizačnej jednotky.

Podmienkou na využitie uvedených služieb pre iné orgány verejnej správy je legislatívna podpora a existencia bezpečnostných mechanizmov zabezpečujúcich jednoznačnú identifikáciu, autentifikáciu a následnú autorizáciu oprávnených osôb alebo systémov príslušných orgánov verejnej správy na využitie uvedenej služby, t.j. na oprávnenie zaslať vzdialenému HSM zariadeniu elektronický dokument na vyhotovenie ZEP.

4.1.3.3 *Spracovanie požiadavky na PKI službu elektronickej podateľne*

CEP, resp. REP poskytuje okolitým modulom a používateľom služby spojené s využívaním PKI. Tieto služby sú aktivované prostredníctvom prístupových komponentov. Poskytovateľom týchto služieb je systém elektronickej podateľne (CEP). Pre používateľov sa jedná o nasledujúce služby:

- Vytvorenie ZEP – používateľ vytvorí ZEP na podaní prostredníctvom PKI prostriedkov (certifikovanej aplikácie) poskytovaných používateľom (tieto prostriedky síce neposkytuje priamo modul CEP a REP, ale sú poskytované prostredníctvom prístupových komponentov). Podmienkou je aby používateľ disponoval certifikovaným bezpečným zariadením na vyhotovenie ZEP (SSCD, napr. elektronická čipová karta alebo USB token).
- Informatívne overenie platnosti ZEP – používateľ zašle elektronický dokument so ZEP na službu publikovanú v rámci ÚPVS. Publikovaná služba používateľa informuje o platnosti ZEP na zaslanom dokumente. Informácia o platnosti ZEP má však len informatívny charakter nakoľko prenosový kanál, ktorým sa zasiela informácia o overení nie je súčasťou certifikovanej aplikácie pre overenie ZEP v zmysle zákona o elektronickom podpise.

¹⁰ Pri vytváraní ZEP použije elektronická podateľňa certifikát, resp. privátny podpisový kľúč poverenej osoby.

¹¹ Pri vytváraní ZEP použije elektronická podateľňa certifikát, resp. privátny podpisový kľúč poverenej osoby.

- Prevod ZEP do archívnej formy – používateľ vytvorí požiadavku na prevod ZEP do archívnej formy prostredníctvom služby publikovanej na ÚPVS. Archívny podpis (ZEP-A) vytvára podmienky pre dlhodobé uchovanie elektronického dokumentu so ZEP. Služba po zaslaní dokumentu so ZEP prevedie štruktúru ZEP do archívnej formy (ZEP-A), resp. v prípade potreby do štruktúry ZEP doplní ďalšiu archívnu časovú pečiatku.
- Poskytnutie validačných údajov – validačné údaje pre overovanie ZEP môžu byť poskytnuté priamo pre daný čas overovania, resp. pre určitý časový interval.

4.1.3.4 Synchronizácia interných údajov

CEP, resp. REP synchronizuje interne používané údaje s externými modulmi. Jedná sa najmä o získavanie povolených schém pre elektronické formuláre používané v procesoch formálneho overovania prijatého elektronického podania.

4.1.4 Elektronická podateľňa a ďalšie moduly NKIVS

NKIVS definuje modul CEP ako jeden zo spoločných modulov ÚPVS a REP ako jeden z administratívnych systémov v aplikačnej vrstve informačného systému úseku. Vzťahy s inými modulmi architektúry integrovaného informačného systému verejnej správy sú dané procesmi zabezpečovanými modulom elektronickej podateľne. Tieto vzťahy sú určované nasledujúcimi faktormi:

- elektronická podateľňa je budovaná ako „pasívny“ modul, t.j. jej činnosť je riadená externou logikou spracovania elektronického dokumentu,
- potreba validácie formálnych náležitostí – podaní, t.j. platnosti elektronickej predlohy (formuláru) a použitej vizualizačnej schémy formulára.

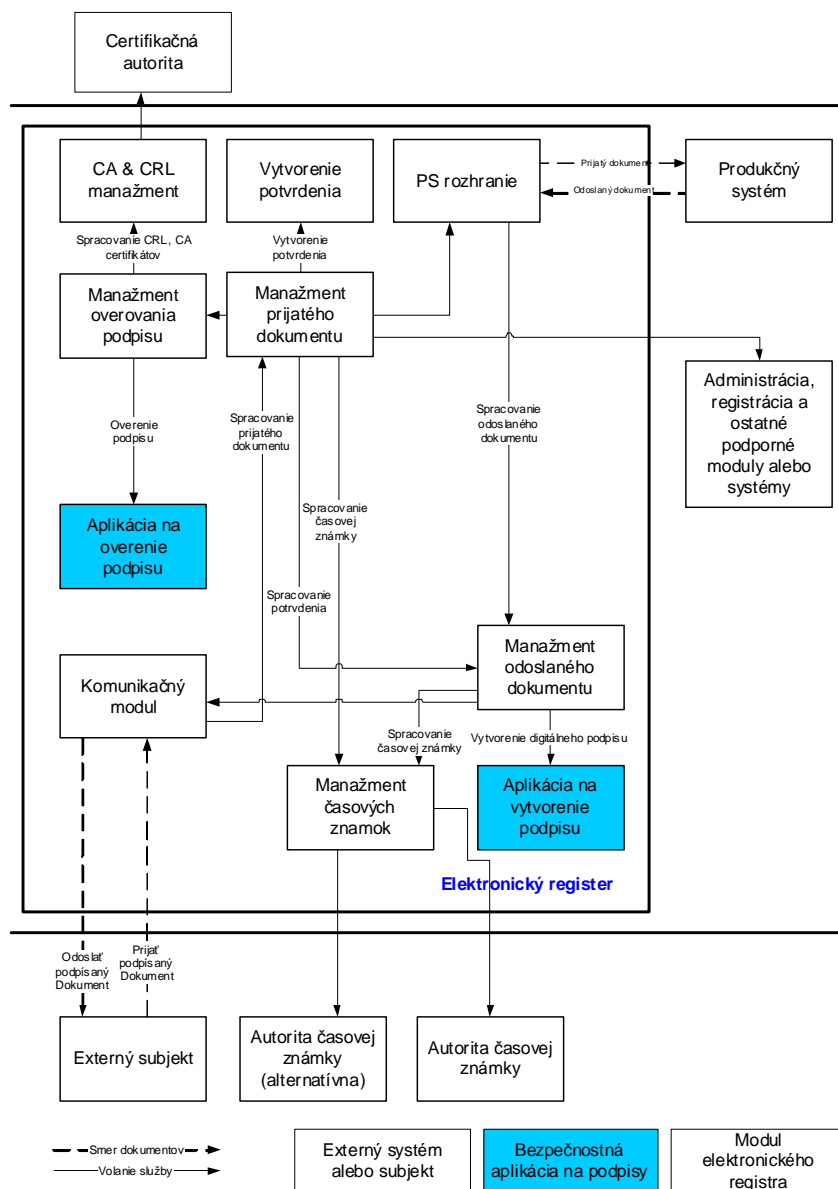
Z vyššie uvedených väzieb je zrejmé, že modul CEP ÚPVS je úzko viazaný na eForm modul, resp. na submodul BPM, ktorý predstavuje súčasť eForm modulu. Nakoľko aj REP vyžaduje identické väzby, je potrebné ho priamo napojiť na eForm modul ÚPVS, resp. na podriadený eForm modul prevádzkovaný v rámci daného orgánu verejnej správy.

REP bude podriadená BPM modulu v IS úseku správy, ktorý riadi logiku spracovania podania/požiadavky. Ide o Transakčné jadro, ktoré bude zabezpečovať riadenie logiky spracovania v rámci ÚPVS.

4.1.5 Integrácia elektronickej podateľne na okolité prostredie

Integrácia elektronickej podateľne na okolité systémy musí spĺňať požiadavky kladené NKIVS a súčasne musí zabezpečovať plnenie základných funkcií elektronickej podateľne. Z hľadiska integrácie na okolité systémy je možné túto integráciu členiť na spôsob poskytovania služieb a spôsob integrácie na ďalšie systémy potrebné pre zabezpečenie funkčnosti.

Integrácia jednotlivých modulov elektronickej podateľne s okolitým prostredím je ilustrovaná na nasledujúcom obrázku:



Obrázok 6: Integrácia elektronickej podateľne

Integračné rozhranie pre sprístupnenie služieb elektronickej podateľne je možné charakterizovať nasledovne:

- Rozhranie elektronickej podateľne (CEP aj REP) je implementované ako Webová služba (Web Service), ktorá je volaná z okolitých modulov (t.j. eForm modul v ÚPVS a BPM modul v IS úseku). Toto rozhranie poskytuje nasledujúcu funkcionality:

- overenie formálnych náležitostí prijatého elektronického dokumentu,
- overenie elektronického podpisu prijatého dokumentu,
- doplnenie časovej pečiatky k prijatému elektronickému dokumentu (so ZEP bez časovej pečiatky alebo bez ZEP),
- vystavenie potvrdenia o prijatí,
- vytvorenie elektronického podpisu odosielaného dokumentu,
- prevod ZEP na archívnu formu,
- poskytnutie validačných údajov,
- synchronizácia povolených schém elektronických formulárov s eForm modulom.

Vytvorenie potvrdení o prijatí podania bude realizované mimo modulu elektronickej podateľne (t.j. v eForm, resp. v BPM). Podpísanie ZEP-om a doplnenie časovej pečiatky bude zabezpečené funkciami elektronickej podateľne. Zasielané bude používateľovi ako ostatné odosielané dokumenty do modulu elektronickej schránky v eDesk module. Takáto implementácia vyplýva z požiadavky oznámenia prípadného dôvodu odmietnutia podania v potvrdenke o prijatí.

Elektronická podateľňa kontroluje iba vybrané aspekty podania, vecný obsah podania sa kontroluje v logike spracovania podania (napr. oprávnenia podávajúceho). V tomto prípade pri vystavovaní potvrdenia o doručení by takýto chybový kód nebolo možné zahrnúť do potvrdenia o doručení.

Integračné rozhranie na eForm modul bude zabezpečovať minimálne funkciu aktualizácie zoznamu a schém prípustných elektronických dokumentov a k nim viazaných povolených vizualizácií (URL, hash) tak, aby bolo možné vyhodnotiť správnosť ZEP vo väzbe na povolený formulár a jeho schválenú vizualizáciu.

Integračné rozhranie na služby PKI bude zabezpečovať nasledujúce funkcie:

- získavanie CRL zo všetkých ACA (zoznam ACA a ich služieb a prístupových adries je súčasťou interných evidencií elektronickej podateľne),
- rozhranie na službu časovej pečiatky – služba časovej pečiatky bude poskytovaná od vybranej ACA. Zároveň bude vhodné mať integrovanú službu časovej pečiatky od záložného poskytovateľa.

4.2 Zlepšenie

Navrhované riešenie CEP a REP z hľadiska súčasného stavu predstavuje nasledujúce pozitívne zmeny:

- vytvorenie podmienok pre budovanie elektronických služieb,
- štandardizácia a zabezpečenie interoperability,
- nasadenie overeného riešenia,
- finančná efektívnosť – využitie overeného spoločného riešenia.

4.2.1 Vytvorenie podmienok pre budovanie elektronických služieb

Vytvorením a nasadením systémov elektronickej podateľne (CEP alebo REP) sa vytvoria komplexné infraštruktúrne podmienky pre budovanie elektronických služieb verejnej správy, ktoré sú bez nasadenia modulu elektronickej podateľne nerealizovateľné (či už sa jedná o podania so ZEP, resp. aj bez ZEP).

Služby elektronickej podateľne sú prostredníctvom rozhrania Webových služieb k dispozícii ostatným modulom ÚPVS, resp. modulom IS úseku správy. Súčasne sú prostredníctvom elektronickej podateľne sprístupnené základné PKI služby aj pre používateľov elektronických služieb, ktoré podporujú ich plošné využívanie.

4.2.2 Štandardizácia a zabezpečenie interoperability

Vytvorenie jednotného systému elektronických podateľní postavených na všeobecne platných štandardoch vytvára priestor pre ich vzájomné prepojenie v procesoch elektronických služieb. Štandardizácia používaných formátov ZEP vytvára priestor pre znižovanie nákladov ako u používateľov elektronických služieb, tak ako aj pre ich používateľov.

Navrhnutá koncepcia hierarchického budovania elektronických podateľní výrazne znižuje náklady na ich implementáciu a prevádzku, nakoľko je možné efektívne využívať štandardizované postupy nasadzovania a integrácie do procesov elektronických služieb.

4.2.3 Nasadenie overeného riešenia

Pre implementáciu jednotlivých typov elektronických podateľní je navrhnuté nasadenie overených riešení. Tieto významným spôsobom redukovujú riziká projektov budovania a nasadzovania týchto riešení a umožňujú využitie doposiaľ získaných skúseností a osvedčených postupov a riešení. Súčasne sa výrazným spôsobom znižujú náklady spojené s budovaním, resp. zaobstaraním licencie osvedčeného riešenia elektronickej podateľne, ktorá musí mať osvedčenie súladu s požiadavkami legislatívy.

4.2.4 Finančná efektívnosť – využitie overeného riešenia

Využitie overeného riešenia vytvára podmienky pre efektívnejší proces obstarávania, kde centralizovaným obstaraním riešenia elektronickej podateľne je možné dosiahnuť výrazne

výhodnejšie podmienky, ako keby obstarávanie zabezpečovali jednotlivé orgány verejnej správy samostatne.

4.3 Definície služieb

Súčasťou rozvojového zámeru vybudovania systému elektronickej podateľne (CEP alebo REP) je zavedenie nasledovných skupín elektronických služieb:

- spracovanie podaní:
 - Prijatie elektronického dokumentu alebo elektronického dokumentu podpísaného elektronickým podpisom – A.1.1.1,
- spracovanie požiadaviek na PKI službu elektronickej podateľne:
 - Vytvorenie elektronického podpisu odosielaného elektronického dokumentu – A.1.1.2,
 - Informatívne overenie ZEP na poskytnutom elektronickom dokumente – A.1.1.3,
 - Prevod ZEP na archívnu formu – A.1.1.4,
 - Vytvorenie archívnej časovej pečiatky – A.1.1.5,
 - Poskytnutie validačných údajov CRL pre kvalifikované certifikáty – A.1.1.6.

Všetky elektronické služby CEP sú v súlade s klasifikáciou elektronických služieb podľa dokumentu „Katalóg služieb - Štruktúra a základné princípy“ klasifikované ako:

- podporné služby a
- používateľské a aplikačné služby.

Podrobne definície týchto služieb sú uvedené v Prílohe A.

4.4 Uskutočniteľnosť a náklady

Budovanie riešenia pre systém elektronických podateľní (t.j. CEP a REP) vychádza z existencie funkčného riešenia elektronickej podateľne prevádzkovaného v rámci ÚPVS a z filozofie jeho ďalšieho rozšírenia v súlade s požiadavkami tejto štúdie. Súčasne toto implementované riešenie môže byť rozšírené v rámci jednotlivých orgánov verejnej správy, ktoré elektronickú podateľňu v rámci nimi prevádzkovaných ISVS budú budovať.

Implementácia riešenia CEP a REP definovaného v tejto štúdii vytvorí predpoklady pre budovanie infraštruktúry pre poskytovanie elektronických služieb verejnej správy, v súlade s cieľmi a prístupom definovaných v rámci dokumentu NKIVS.

Dobudovanie riešenia CEP bude orientované do nasledujúcich projektov:

- Rozšírenie funkčnosti elektronickej podateľne:
 - **Rozšírenie množiny podporovaných spracovávaných formátov elektronických dokumentov** – bude implementovaná podpora nasledujúcich formátov elektronických dokumentov, ktorých využitie je plánovaná v rámci elektronických služieb verejnej správy – formát PDF¹² a 602-XML pre elektronické formuláre. Toto sa týka nielen rozšírenia funkcionality elektronickej podateľne, ale taktiež získania certifikovaných prostriedkov pre elektronickú podateľňu pre automatizované vytváranie a overovanie ZEP pre tieto formáty v elektronickej podateľni, ako aj pre používateľov ÚPVS.
 - **Podpora spracovania zložených štruktúr** – funkcionality CEP je potrebné rozšíriť o podporu spracovania zložených elektronických dokumentov (napr. podanie s prílohami), ktoré môžu byť tvorené elektronickými dokumentmi rôzneho typu. Toto rozšírenie umožní spracovanie v podstate akéhokoľvek podania, alebo rozhodnutia alebo výstupu z ISVS.
 - **Synchronizácia údajov s modulom eForm** – funkcionality bude zabezpečovať rozšírenie existujúcich evidencií a elektronických formulárov a s nimi viazaných vizualizačných schém potrebných pre zabezpečenie funkcie elektronickej podateľne a ich aktualizáciu s centrálnymi evidenciami eForm modulu.
 - **Poskytovanie validačných údajov** – budú implementované funkcie sprístupňovania a poskytovania validačných údajov do externého prostredia. Tieto validačné údaje budú využiteľné v systéme dlhodobého uchovávaní elektronických dokumentov so ZEP.
 - **Sprístupnenie funkcie časovej pečiatky** – pre ochranu integrity bude medzi službami elektronickej podateľne sprístupnená aj služba vytvorenia časovej pečiatky.
 - **Podpora oboch typov formátov ZEP** – budú implementované PKI prostriedky, ktoré dokážu vyhotoviť a overiť formát CAdES aj XAdES.
- Rozšírenie funkcií poskytovaných používateľom:
 - **Poskytnutie prostriedkov pre podporu nových formátov** – pre používateľov budú v rámci poskytovaných elektronických služieb verejnej správy poskytované prostriedky pre podporu vytvárania (a aj overovania) ZEP pre nové formáty elektronických dokumentov (PDF a 602-XML). Vzhľadom na potrebu prevodu PDF dokumentov do PDF/A formy bude súčasťou týchto prostriedkov aj takýto konvertor.¹³
 - **Prevod ZEP na archívnu formu** – pre používateľov bude sprístupnená funkcia zabezpečujúca prevod ZEP na elektronickom dokumente na archívnu formu (ZEP-A)

¹² Z hľadiska podpory ZEP pre dokumentu PDF bude podporovaný štandard PDF/A z dôvodu zabezpečenia požadovaných vlastností podpisovaných dokumentov vo formáte PDF.

¹³ Konvertor do PDF/A bude súčasťou procesu elektronickej služby, nebude však súčasťou certifikovaných prostriedkov pre vytváranie a overovanie ZEP.

zabezpečujúcu jednak možnosť jeho dlhodobejšieho uchovania, ako aj jednoduchšieho overovania z hľadiska používateľov.

- **Vytvorenie a poskytnutie prostriedku pre overovanie ZEP pre používateľov** – nakoľko je overovanie ZEP vo všeobecnosti zložitý proces vyžadujúci získavanie validačných údajov používateľom, sprístupnený prostriedok bude určený pre overovanie platnosti ZEP vo formáte ZEP-A.
- **Dobudovanie služby overovania ZEP pre používateľov** – v rámci služieb poskytovaných používateľom bude rozšírená implementácia overenia ZEP na ÚPVS. Súčasne táto služba bude používateľom sprístupnená ako Webová služba nevyžadujúca použitie používateľského rozhrania (možnosť jej integrácie do automatizovaných procesov používateľa).
- Dobudovanie prevádzkového prostredia CEP
 - dosiahnutie plánovanej konfigurácie základného HW a SW vybavenia tak, aby bolo možné zabezpečiť plánované prevádzkové a bezpečnostné parametre pre systém CEP,
 - definovanie prevádzkových postupov zabezpečujúcich dosiahnutie požadovaných bezpečnostných a prevádzkových parametrov modulu CEP,
 - dopracovanie prevádzkovej dokumentácie pre modul CEP,
 - vypracovanie metodických doporučení pre orgány verejnej správy, ktoré sa rozhodnú CEP využívať ako svoju elektronickú podateľňu. V rámci metodických usmernení budú zakomponované návody a doporučenia zabezpečujúce efektívnu integráciu modulu CEP do procesov budovaných elektronických služieb.
- Vytvorenie podmienok pre budovanie a prevádzku REP:
 - **Získanie časovo neobmedzenej multilicencie** na nasadenie modulu elektronickej podateľne a certifikovaných prostriedkov pre vytváranie a overovanie ZEP, ktoré sú potrebné pre budovanie REP. Takáto multilicencia zjednoduší proces budovania elektronických podateľní v rámci jednotlivých orgánov verejnej správy v prípadoch, keď je nasadenie takejto elektronickej podateľne nevyhnutné. Tým bude jednak zabezpečené efektívnejšie vynakladanie finančných prostriedkov na takéto centralizované riadenie nasadzovania elektronických podateľní, a bude zabezpečená ich kompatibilita v prípade potreby vzájomnej komunikácie medzi jednotlivými orgánmi verejnej správy pri poskytovaní elektronických služieb verejnej správy.
 - Vypracovanie metodických doporučení pre orgány verejnej správy, ktoré sa rozhodnú budovať a prevádzkovať REP. Budú definované postupy implementácie systému REP, ako aj integrácie do prostredia orgánu verejnej správy. Rovnako budú dokumentované aj potrebné prevádzkové postupy. V rámci metodických usmernení budú zakomponované taktiež návody a doporučenia zabezpečujúce efektívnu integráciu modulu CEP do procesov budovaných elektronických služieb.

4.4.1 Dopady na technické a softwarové vybavenie

Cieľová architektúra riešenia je definovaná v časti 4.1. Je potrebné dobudovať existujúce riešenie do stavu definovanom v tejto časti.

4.4.2 Organizačné dopady

Rozšírením funkcionality existujúceho riešenia CEP sa nepredpokladajú dodatočné organizačné zmeny pri zabezpečovaní jej prevádzky. Existujúce organizačné zabezpečenie bude možné využiť aj pri implementácii a nasadzovaní elektronických podateľní na jednotlivých orgánoch verejnej správy.

4.4.3 Legislatívne dopady

Z hľadiska práva je elektronická podateľňa, resp. jej adresa „len“ adresou príslušného orgánu verejnej moci. Inými slovami, je to miesto, ktoré je miestom prijímania podaní adresovaných tomuto orgánu. Podľa platnej právnej úpravy, ak má orgán verejnej moci zriadenú elektronickú podateľňu, je povinný zverejniť jej adresu. Touto adresou však nie je povinne ÚPVS. Vzhľadom na to, že sa uvažuje o implementácii modulu CEP a súčasne aj o existencii REP pre niektoré orgány verejnej moci a ÚPVS by mal byť spoločným prístupovým bodom na účely komunikácie s orgánmi verejnej moci (využívajúc aj eDesk a eForm), je možné navrhnúť, aby (i) CEP bola elektronickou podateľňou pre každý orgán verejnej moci, ktorý poskytuje svoje služby elektronicky a nemá zriadenú vlastnú elektronickú podateľňu a zároveň (ii) ak má orgán verejnej moci zriadenú vlastnú elektronickú podateľňu, aby adresou jej umiestnenia bol vždy aj ÚPVS – inými slovami, aby bola vždy prístupná aj cez ÚPVS. Táto úprava je plne súladná s úpravou § 5 ods. 3 písm. b) zákona o ISVS, podľa ktorého sú povinné osoby povinné sprístupniť svoje e-služby aj cez ÚPVS. Predmetná úprava by mohla byť vykonaná v generálnom zákone, ktorý bude upravovať aj elektronické podávanie podaní, či elektronické doručovanie, alebo v zákone o ISVS. Takouto úpravou by sa dosiahlo, že adresou na elektronické doručovanie by bol vždy ÚPVS, či už cez CEP alebo REP.

Nasadenie CEP a rezortných elektronických podateľní však bude vyžadovať ustanovenie nových štandardov, ktoré je možné ustanoviť vyhláškou Národného bezpečnostného úradu, a to

- Definovanie národného profilu ZEP.
- Definovanie štandardu pre väzbu ZEP na podpisovaný dokument (dokumenty). Takýto štandard je v súčasnosti predložený na posúdenie NBÚ, nebol však zo strany NBÚ publikovaný.
- Definovanie štandardu pre väzbu časovej pečiatky na objekt (objekty), ktorých integrita má byť časovou pečiatkou chránená.
- Pokiaľ ide o moment doručenia, tento nie je potrebné osobitne legislatívne upravovať, pretože doručenie orgánu verejnej moci sa bude preukazovať potvrdením času prijatia na doručenke, týmto orgánom vystavenej. Inými slovami, časom doručenia budú čas, uvedený na tejto potvrdenke. Je následne technickou otázkou definovať moment, kedy je podanie

akceptované orgánom verejnej moci v zmysle, že sa dostane do jeho dispozície a elektronická podateľňa po overení náležitostí toto podanie prijme.

4.4.4 Prevádzkové dopady

Rozšírením funkcionality existujúceho riešenia CEP sa nepredpokladajú dodatočné zmeny v spôsobe prevádzky CEP. Existujúce prevádzkové postupy bude možné využiť aj pri implementácii a nasadzovaní elektronických podateľní na jednotlivých orgánoch verejnej správy.

4.4.5 Dopady na lokalitu a stavebnú činnosť

Nasadzovanie a prevádzka systému CEP nemá priame dopady na lokalitu (zmenu existujúcej lokality), ani na dodatočnú stavebnú činnosť.

4.4.6 Bezpečnostné dopady

Z hľadiska nasadzovania a prevádzky modulu CEP pravdepodobne nebude potrebné nasadzovanie dodatočných bezpečnostných opatrení. Požiadavky na zabezpečenie systému CEP, ako aj jeho prevádzky sú pokryté existujúcimi riešeniami a postupmi. Mieru bezpečnosti, resp. mieru rizika by bolo vhodné preskúmať vykonaním bezpečnostného auditu celého systému CEP.

4.4.7 Vývoj riešenia

Vývoj riešenia je možné plne realizovať externými zdrojmi a pomerne nezávisle. Je však potrebná koordinácia s vývojom modulu eForm, s ktorým bude zabezpečená komunikácia. Z hľadiska vývoja nie je potrebná žiadna nadštandardná súčinnosť správcu a prevádzkovateľa.

4.4.8 Nasadenie riešenia

Nasadenie riešenia je možné vykonať nezávisle a pomocou štandardných postupov používaných v rámci ÚPVS.

4.4.9 Cena riešenia

Na základe odhadu náročnosti vývoja aplikácie predstavuje predpokladaný časový náklad na implementáciu 31 990 človekohodín. Tento údaj je potrebné považovať za spodnú hranicu investičných nákladov do vývoja softvérového riešenia, resp. jeho rozšírenia.

Vzhľadom na rozsah systému a požiadavky naň kladené bude potrebné vybudovať robustné riešenie. Predpokladané náklady na obstaranie HW, SW a činností spojených s implementáciou sú 7 598 000 Eur s DPH.

Detailný rozpočet projektu bude riešený v rámci prípravy projektu ako súčasti prípravy žiadosti o nenávratný finančný príspevok.

4.4.10 Marketingové požiadavky

V rámci realizácie projektu budú vykonané aktivity ohľadne vytvorenia povedomia o existencii a funkčnosti riešenia.

4.4.11 Zhrnutie

Dopady na navrhované riešenie sú uvedené v predchádzajúcich kapitolách.

4.5 Ekonomická analýza

Táto čiastková štúdia predpokladá, že aspekty ekonomickej analýzy budú riešené v rámci prípravy projektu ako súčasti prípravy žiadosti o nenávratný finančný príspevok. .

4.6 Návrh projektového zámeru

4.6.1 Príprava projektu

Názov projektu

Národný projekt: Centrálna elektronická podateľňa

Ciele projektu

Dobudovanie Centrálny elektronickej podateľne ako spoločného modulu ÚPVS, tak aby predstavoval riešenie využiteľné rôznymi organizáciami VS pre prijímanie elektronických podaní a autorizáciu elektronických dokumentov odosielaných orgánmi verejnej správy.

Výstupy projektu

Bezprostrednými výsledkami projektu bude zavedenie funkčného modulu centrálny elektronickej podateľne a sprístupnenie elektronických služieb modulu.

Súvisiace projekty

Nasadzovanie CEP je potrebné koordinovať s projektmi zameranými na spoločné moduly ÚPVS.

4.6.2 Metodika riadenia

Metodika riadenia projektu bude vychádzať zo samostatného dokumentu popisujúceho metodický rámec pre riadenie projektov OPIS.

4.7 Zdôvodnenie doporučení

Zdôvodnenie doporučení je implicitne uvedené v častiach 4.1 až 4.6 tejto štúdie.

A Definície elektronických služieb projektu

V nasledujúcom zozname sú uvedené spoločné vlastnosti a doplňujúce informácie o elektronických službách CEP, ktoré sú popísané v tabuľkách nižšie.

- Služby sú implementované základným komponentom architektúry eGovernmentu podľa dokumentu NKIVS.
- Povinné osoby garantujúce službu:

správca: Úrad vlády Slovenskej republiky,

prevádzkovateľ: Úrad vlády Slovenskej republiky.
- Predpokladá sa, že špecifikáciu minimálne nasledovných výkonových parametrov doplní oprávnený žiadateľ vo fáze prípravy žiadosti o NFP:
 - frekvencia použitia služby (počet / obdobie),
 - doba odozvy (napríklad on-line, 24h a pod.),
 - frekvencia incidentov (počet / obdobie),
 - náklady za poskytnutie služby (náklady poskytovateľa),
 - náklady za použitie služby (náklady používateľa),
 - prínosy – finančné (napr. ušetrenie nákladov a poplatky z poskytnutia služby),
 - prínosy – monetarizované nefinančné (napr. kvantifikácia ušetreného času a pozitívnych dopadov na prostredie).
- Zaradenie služieb k agendám a úsekom správy vyplynie nepriamo zo zaradenia príslušných eGov služieb, ktoré sú na tejto službe závislé.

A.1 Podporné služby

A.1.1 Používateľské a aplikačné služby

A.1.1.1 *Prijatie elektronického dokumentu alebo elektronického dokumentu podpísaného elektronickým podpisom*

Položka		Hodnota
Základné údaje		
	Názov služby	Prijatie elektronického dokumentu alebo elektronického dokumentu podpísaného elektronickým podpisom
	Popis služby	<p>Služba realizuje prijatie elektronického dokumentu (podania) a v rámci spracovania vykoná nasledovné funkcie v závislosti od toho, či je podanie podpísané elektronickým podpisom alebo nie:</p> <ul style="list-style-type: none"> • overenie formálnych náležitostí prijatého elektronického dokumentu, • overenie elektronického podpisu prijatého dokumentu, • doplnenie časovej pečiatky k prijatému elektronickému dokumentu (so ZEP aj bez ZEP), • vystavenie potvrdenia o prijatí.
Klasifikácia služby		
	Používatelia služby	<ul style="list-style-type: none"> • občan (G2C) • podnikateľ (G2B) • IS podnikateľa (G2C)
	Komunikačné kanály	<ul style="list-style-type: none"> • webové služby • e-mail • www
	Stav implementácie	<ul style="list-style-type: none"> • špecifikácia - implementácia funkčnosti v rámci existujúceho riešenia CEP
Atribúty služby		
	Vstup (parametre služby – špecifikácia požiadaviek používateľa na službu)	<ul style="list-style-type: none"> • identifikácia používateľa služby • elektronický dokument (autorizovaný ZEP, resp. aj dokument bez ZEP)
	Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> • elektronická potvrdenka (okrem anonymných podaní) • postúpenie alebo nepostúpenie podania na spracovanie v ISVS

A.1.1.2 Vytvorenie elektronického podpisu odosielaného elektronického dokumentu

Položka	Hodnota
Základné údaje	
Názov služby	Vytvorenie elektronického podpisu odosielaného elektronického dokumentu
Popis služby	Služba realizuje vytvorenie elektronického podpisu odosielaného elektronického dokumentu, resp. viacerých elektronických dokumentov podpísaných jedným elektronickým podpisom (napr. elektronické rozhodnutie s prílohami, ktoré môžu byť aj vo viacerých formátoch podporovaných systémom elektronickej podateľne). Elektronická podateľňa môže pre vytvorenie elektronického podpisu využiť privátne kľúče viacerých poverených osôb (t.j. podpisovať za viaceré orgány verejnej správy alebo organizačné jednotky).
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G) interný subjekt VS (G2E)
Komunikačné kanály	<ul style="list-style-type: none"> www webové služby
Stav implementácie	<ul style="list-style-type: none"> špecifikácia - implementácia funkčnosti v rámci existujúceho riešenia CEP
Atribúty služby	
Vstup (parametre služby – špecifikácia požiadaviek používateľa na službu)	<ul style="list-style-type: none"> identifikácia používateľa služby elektronický dokument, resp. viaceré elektronické dokumenty určenie povinnej osoby, ktorej privátny kľúč má byť pri vytváraní ZEP použitý (podpisový certifikát) identifikácia a autentifikácia oprávnenej osoby na využitie služby
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> vytvorený ZEP (ZEP vytváraný vo formáte ZEP-T)

A.1.1.3 Informatívne overenie ZEP na poskytnutom elektronickom dokumente

Položka	Hodnota
Základné údaje	
Názov služby	Informatívne overenie ZEP na poskytnutom elektronickom dokumente
Popis služby	Služba poskytuje používateľom elektronických služieb možnosť overenia platnosti elektronického podpisu na zaslanom elektronickom dokumente, resp. viacerých elektronických dokumentov podpísaných jedným elektronickým podpisom. Používateľ je v rámci poskytovanej služby informovaný o stave overenia.
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G) interný subjekt VS (G2E) občan (G2C) podnikateľ (G2B) IS podnikateľa (G2C)

Položka	Hodnota
Komunikačné kanály	<ul style="list-style-type: none"> • www • webové služby
Stav implementácie	<ul style="list-style-type: none"> • špecifikácia – implementácia funkčnosti v rámci existujúceho riešenia ÚPVS
Atribúty služby	
Vstup (parametre služby – špecifikácia požiadaviek používateľa na službu)	<ul style="list-style-type: none"> • identifikácia používateľa služby • elektronický dokument, resp. viaceré elektronické dokumenty podpísané ZEP
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> • informácia o výsledku overenia ZEP elektronického dokumentu

A.1.1.4 Prevod ZEP na archívnu formu

Položka	Hodnota
Základné údaje	
Názov služby	Prevod ZEP na archívnu formu
Popis služby	Služba poskytuje používateľom elektronických služieb možnosť prevodu elektronického dokumentu so ZEP na jeho archívnu formu, ktorá zabezpečuje možnosť jeho dlhodobého overenia.
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> • ISVS organizácie VS (G2G) • interný subjekt VS (G2E) • občan (G2C) • podnikateľ (G2B) • IS podnikateľa (G2C)
Komunikačné kanály	<ul style="list-style-type: none"> • www • webové služby
Stav implementácie	<ul style="list-style-type: none"> • špecifikácia – implementácia funkčnosti v rámci existujúceho riešenia ÚPVS
Atribúty služby	
Vstup (parametre služby – špecifikácia požiadaviek používateľa na službu)	<ul style="list-style-type: none"> • identifikácia používateľa služby • elektronický dokument podpísaný platným ZEP
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> • ZEP vo formáte ZEP-A

A.1.1.5 Vytvorenie archívnej časovej pečiatky

Položka	Hodnota
Základné údaje	
Názov služby	Vytvorenie archívnej časovej pečiatky

Položka		Hodnota
	Popis služby	Služba realizuje zabezpečenie integrity pre zadané údaje pripojením časovej pečiatky k údajom (resp. balíku údajov). V prípade existencie archívnej časovej pečiatky vytvorí ďalšiu (následnú) archívnu pečiatku.
Klasifikácia služby		
	Používatelia služby	<ul style="list-style-type: none"> • ISVS organizácie VS (G2G) • interný subjekt VS (G2E) • občan (G2C) • podnikateľ (G2B) • IS podnikateľa (G2C)
	Komunikačné kanály	<ul style="list-style-type: none"> • www • webové služby
	Stav implementácie	<ul style="list-style-type: none"> • špecifikácia
Atribúty služby		
	Vstup (parametre služby – špecifikácia požiadaviek používateľa na službu)	<ul style="list-style-type: none"> • identifikácia používateľa služby • údaje nad ktorými sa požaduje vytvorenie archívnej časovej pečiatky (balík údajov)
	Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> • archívna časová pečiatka

A.1.1.6 Poskytnutie validačných údajov CRL pre kvalifikované certifikáty

Položka		Hodnota
Základné údaje		
	Názov služby	Poskytnutie validačných údajov CRL pre kvalifikované certifikáty
	Popis služby	Služba realizuje poskytnutie zoznamov všetkých CRL ku kvalifikovaným certifikátom vydávaných všetkými ACA za dané časové obdobie.
Klasifikácia služby		
	Používatelia služby	<ul style="list-style-type: none"> • ISVS organizácie VS (G2G) • interný subjekt VS (G2E) • občan (G2C) • podnikateľ (G2B) • IS podnikateľa (G2C)
	Komunikačné kanály	<ul style="list-style-type: none"> • www • webové služby
	Stav implementácie	<ul style="list-style-type: none"> • špecifikácia
Atribúty služby		
	Vstup (parametre služby – špecifikácia požiadaviek používateľa)	<ul style="list-style-type: none"> • identifikácia používateľa služby • časový interval

Položka		Hodnota
	na službu)	
	Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> zoznam relevantných CRL pre zadaný časový interval

B Výpočet odhadu prácnosti riešenia

Pre odhad náročnosti a ceny riešenia je použitá metodológia Use-Case-Points (UCP). Podrobný popis metodológie je uvedený na <http://www.codeproject.com/gen/design/usecasep.asp>.

B.1 Use-case a používatelia riešenia

Zoznam use-caseov a ohodnotenie ich zložitosti je uvedené v tabuľke nižšie.

Zoznam e-služieb (resp. usecase-ov)			
P.č.	Názov	Zložitosť	Počet
1	Prijatie elektronického dokumentu alebo elektronického dokumentu podpísaného elektronickým podpisom	15	20
2	Vytvorenie EP odosielaného elektronického dokumentu	15	20
3	Informatívne overenie ZEP na poskytnutom elektronickom dokumente	15	20
4	Prevod ZEP na archívnu formu	10	5
5	Vytvorenie archívnej časovej pečiatky	15	10
6	Poskytnutie validačných údajov (CRL) pre kvalifikované certifikáty	10	5

Tabuľka 2: Zoznam a ohodnotenie use-caseov

Zoznam používateľov a ohodnotenie ich zložitosti je uvedené v tabuľke nižšie.

Zoznam používateľov / Actors				
P.č.	Typ používateľa	Rola používateľa	Zložitosť	Počet
1	občan (G2C)	-	3	5
2	ISVS organizácie VS (G2G)	-	3	20
3	interný subjekt VS (G2E)	-	2	5
4	IS podnikateľa (G2C)	-	3	20
5	podnikateľ (G2B)	-	3	5

Tabuľka 3: Zoznam a ohodnotenie používateľov riešenia

B.2 Výpočet UCP

Výpočet Use-case bodov (UCP) je uvedený v nasledujúcej tabuľke. Detailné odvodenie východiskových parametrov tohto výpočtu je spracované v ďalších častiach tejto prílohy.

P. č.	Parameter	Hodnota	Odvodenie hodnoty
1	Faktor produktivity	20,00	Pomer človekohodín na vývoj jedného use-casu vychádzajúci zo skúsenosti predošlých projektov. Typicky v intervale 15-30, resp. 20.
2	Neupravené use-case body (UUCP)	1 310	B.2.3 + B.2.4
3	Faktor technickej komplexnosti	1,11	B.2.1

P. č.	Parameter	Hodnota	Odvozenie hodnoty
	(TCF)		
4	Faktor komplexnosti prostredia (ECF)	1,1	B.2.2
5	Use-case body (UCP)	1 599,51	$2 * 3 * 4$
6	Pracnosť v človekohodinách	31 990	$1 * 5$

Tabuľka 4: Use-case bodov (UCP)

B.2.1 Faktor technickej komplexnosti (TCF)

13 štandardných technických faktorov vyplývajúcich z požiadaviek na IS. Váha 0 označuje irelevantnosť požiadavky na IS a hodnota 5 znamená, že faktor má najväčší vplyv (požiadavka má najväčšiu váhu).

ID	Faktor	Váha	Komplexnosť	Výsledok
T1	Distribučný systém	2	3	6
T2	Výkon	1	4	4
T3	Efektívnosť pre používateľa	1	5	5
T4	Komplexnosť vnútorných procesov	1	4	4
T5	Znovapoužiteľnosť	1	5	5
T6	Jednoduchosť inštalácie	0,5	1	0,5
T7	Jednoduchosť používania	0,5	5	2,5
T8	Prenosnosť	2	4	8
T9	Jednoduchosť zmeny	1	3	3
T10	Súbežnosť	1	4	4
T11	Osobitné bezpečnostné prvky	1	5	5
T12	Poskytuje priamy prístup k tretím systémom	1	2	2
T13	Špeciálne znalosti a zručnosti používateľov	1	2	2
Spolu				51
TCF ($0,6 + (0,01 * \text{Spolu})$)				1,11

Tabuľka 5: Výpočet faktora technickej komplexnosti (TCF)

B.2.2 Faktor komplexnosti prostredia (ECF)

6 faktorov vplyvu externého prostredia na IS. Hodnota 0 znamená, že faktor prostredia je irelevantný pre tento projekt; 3 je priemerný, 5, znamená to, že má silný vplyv.

ID	Faktor	Váha	Komplexnosť	Výsledok
E1	Znalosť UML	1,5	2	3
E2	Skúsenosti s implementáciou	0,5	3	1,5
E3	Skúsenosti s objektovo orientovaným prístupom	1	1	1

ID	Faktor	Váha	Komplexnosť	Výsledok
E4	Schopnosť vedúcich analytikov	0,5	3	1,5
E5	Motivácia	1	1	1
E6	Stabilita požiadaviek	2	1	2
E7	Zamestnanci na čiastočný úväzok	-1	0	0
E8	Zložitý programovací jazyk	-1	0	0
Spolu				10
ECF ($1,4 + (-0,03 * \text{Spolu})$)				1,1

Tabuľka 6: Výpočet faktora komplexnosti prostredia (ECF)

B.2.3 Neupravená váha use-casov (UUCW)

Jednotlivé prípady použitia sú klasifikované na jednoduché, priemerné alebo komplexné, a vážené v závislosti od počtu krokov, ktoré obsahujú, vrátane alternatívnych prúdov.

Typ use-case	Popis	Váha	Počet	Výsledok
Jednoduché	Jednoduché užívateľské rozhranie, dotýka iba jediného subjektu, databázy, scenár použitia má 3 kroky, alebo menej, implementuje menej ako 5 tried.	5	0	0
Priemerné	Viac použitých rozhraní, dotýka 2 alebo viac databáz subjektov, 4 až 7 krokov, implementuje medzi 5 až 10 tried.	10	10	100
Komplexné	Zahŕňa zložité užívateľské rozhranie, dotýka sa 3 alebo viac databáz, viac ako 7 krokov, jej implementácia sa týka viac ako 10 tried.	15	70	1 050
Spolu				1 150

Tabuľka 7: Výpočet neupravenej váhy use-casov (UUCW)

B.2.4 Neupravená váha používateľských interakcií (UAW)

Podobne ako UUCW, sú podľa zložitosti interakcií klasifikované aj používatelia riešenia.

Typ use-case	Popis	Váha	Počet	Výsledok
Jednoduché	Používateľ je reprezentovaný iným IS s definovaným API.	1	0	0
Priemerné	Používateľ je reprezentovaný iným IS, ktorý komunikuje prostredníctvom protokolu, napr. TCP/IP.	2	5	10
Komplexné	Používateľ je človek komunikujúci prostredníctvom používateľského rozhrania.	3	50	150
Spolu				160

Tabuľka 8: Výpočet neupravenej váhy používateľských interakcií (UAW)