

**Ministerstvo financií Slovenskej
republiky**

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

Identity and access management



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 56 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	3
2.1	Odporúčania	3
3	Popis aktuálneho stavu	8
3.1	Popis aktuálneho stavu a služieb	8
3.1.1	Analýza požiadaviek a potrieb	8
3.1.2	Architektúra	9
3.1.3	Procesná analýza	9
3.1.4	Legislatívna analýza	10
3.2	Hodnotenie aktuálneho stavu	12
3.3	Návrh zmeny	13
4	Navrhnuté riešenie	18
4.1	Popis navrhovaného riešenia	18
4.1.1	Koncepčný model riešenia	18
4.1.2	Model riadenia prístupových práv.	19
4.2	Zlepšenie	24
4.3	Definície služieb	25
4.4	Uskutočniteľnosť a náklady	26
4.4.1	Dopady na technické a softwarové vybavenie	26
4.4.2	Legislatívne dopady	27
4.4.3	Bezpečnostné dopady	29
4.4.4	Dopady na lokalitu a stavebnú činnosť	29
4.4.5	Ostatné dopady	29
4.4.6	Cena riešenia	30
4.5	Ekonomická analýza	31
4.5.1	Analýza rizík	31
4.6	Návrh projektového zámeru	34
4.6.1	Názov projektu	34
4.6.2	Obsahová náplň projektu	34
4.6.3	Ciele projektu	34
4.6.4	Výstupy projektu	35
4.6.5	Súvisiace projekty	35
4.6.6	Príprava projektu	35

4.6.7	Metodika riadenia	36
4.7	Zdôvodnenie doporučení	36
A	Definície elektronických služieb projektu	37
A.1	Podporné	38
A.1.1	Používateľské a aplikačné služby	38
A.1.1.1	Poskytnutie zoznamu rolí identity z IAM pre zadanú službu	38
A.1.1.2	Poskytnutie informácie o priradení roly identite	38
A.1.1.3	Poskytnutie zoznamu identít s prístupom ku službe	39
A.1.1.4	Poskytnutie zoznamu rolí informačného systému	40
A.1.1.5	Zápis identity do systému IAM	40
A.1.1.6	Zmena údajov identity v systéme IAM	41
A.1.1.7	Zneplatnenie identity v systéme IAM	41
A.1.1.8	Zápis roly do katalógu rolí systému IAM	42
A.1.1.9	Zmena údajov roly v katalógu rolí systému IAM	42
A.1.1.10	Zneplatnenie roly v katalógu rolí systému IAM	43
A.1.1.11	Pridanie roly identite v systéme IAM	43
A.1.1.12	Odobranie roly identite v systéme IAM	44
A.1.1.13	Pridanie autentifikačného prostriedku identite v systéme IAM	44
A.1.1.14	Odobranie autentifikačného prostriedku (AP) identite v systéme IAM	45
A.1.1.15	Poskytnutie autentifikačného rozhodnutia zo systému IAM	46
A.1.1.16	Generovanie nového hesla/reset hesla	46
A.1.1.17	Splnomocnenie inej osoby v systéme IAM	47
A.1.2	Používateľské služby	47
A.1.2.1	Zápis autentifikačného prostriedku do katalógu autentifikačných prostriedkov systému IAM	47
A.1.2.2	Zrušenie autentifikačného prostriedku z katalógu autentifikačných prostriedkov systému IAM	48
A.1.2.3	Poskytnutie profilu identity v systéme IAM	48
B	Výpočet odhadu prácnosti riešenia	50
B.1	Use-case riešenia IAM	50
B.2	Výpočet UCP	51
B.2.1	Faktor technickej komplexnosti (TCF)	52
B.2.2	Faktor komplexnosti prostredia (ECF)	52
B.2.3	Neupravená váha use-casov (UUCW)	53
B.2.4	Neupravená váha používateľských interakcií (UAW)	53

1 Základné informácie

1.1 Prehľad

Projekt je zameraný na vytvorenie základnej infraštruktúry systému Identity and Access management (ďalej len ako „IAM“) pre riadenie prístupu k službám eGovernment. IAM by mal byť základným centralizovaným riešením pre správu identít a prístupových práv v tomto prostredí. IAM je spoločným modulom Ústredného portálu verejnej správy, zároveň je jeho základným nástrojom správy užívateľov.

1.2 Dôvod

Dôvodom vykonania štúdie je vyhodnotenie uskutočniteľnosti zámeru vytvorenia základnej infraštruktúry systému IAM, ktorý má slúžiť ako podporný infraštruktúrny systém pre ostatné systémy a služby eGovernmentu a podľa Národnej koncepcie informatizácie verejnej správy (NKIVS) a má byť realizovaný ako národný projekt financovaný zo zdrojov OPIS.

Hlavným cieľom tejto čiastkovej štúdie je prispieť k:

- vytvoreniu systému IAM ako jednotného a dátovo konzistentného zdroja údajov o všetkých používateľoch (identitách) prístupujúcim k službám eGovernmentu a ich prístupových právach,
- sprístupneniu elektronických služieb IAM a zabezpečeniu ich použiteľnosti na riadenie prístupových práv publikovaných služieb eGovernmentu,
- efektívnej integrácii IAM do celkovej architektúry eGovernmentu, t.j. poskytovanie elektronických služieb IAM iným modulom a efektívne využívanie zdieľaných elektronických služieb poskytovaných inými modulmi eGovernmentu.

Vyššie uvedené ciele majú prispieť k dosiahnutiu globálneho cieľa OPIS, ktorým je vytvorenie inkluzívnej informačnej spoločnosti ako prostriedku pre rozvoj vysoko výkonnej vedomostnej ekonomiky.

1.3 Rozsah

Táto čiastková štúdia popisuje súčasný stav a rámcovo navrhuje budúce riešenie systému IAM, ktorý predstavuje jeden zo spoločných modulov architektúry eGovernmentu podľa Národnej koncepcie informatizácie verejnej správy (NKIVS).

Štúdia realizovateľnosti sa zaoberá posúdením možností nasadenia riešenia pre riadenie prístupu k službám poskytovaným prostredím eGovernmentu. Štúdia nerieši nasadenie riešenia IAM pre správu prístupových práv pre tie systémy používané na jednotlivých úradoch verejnej správy jej zamestnancami, ku ktorým sa neprístupuje prostredníctvom publikovaných služieb eGovernmentu.

1.4 Rámec projektu

Táto štúdia uskutočniteľnosti sa opiera o nasledujúce dokumenty:

- Operačný program informatizácia spoločnosti,
- Národná koncepcia informatizácie verejnej správy,
- Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy.

1.5 Použité skratky a značky

P. č.	Skratka / Značka	Vysvetlenie
1	APV	Aplikačno-programové vybavenie
2	ECF	Faktor komplexnosti prostredia (ECF)
3	FO	Fyzická osoba
4	G2G, G2E, G2A, G2B, G2C, G2P	Používateľ elektronickej služby: Government -> Government, Employee, Administration, Business, Citizen, Public
5	IFO	Identifikátor fyzickej osoby
6	IS	Informačný systém
7	ISVS	Informačný systém verejnej správy
8	KRIS	Koncepcia rozvoja informačných systémov
9	NASES	Národná agentúra sieťových a elektronických služieb
10	NFP	Nenávratný finančný príspevok
11	NKIVS	Národná koncepcia informatizácie verejnej správy
12	OPIS	Operačný program informatizácia spoločnosti
13	PO	Právnická osoba
14	Produkt/aplikácia IAM	Produkt konkrétneho dodávateľa, ktorý zabezpečuje jadro funkcionality IAM riešenia
15	RFO	Register fyzických osôb
16	Riešenie IAM	Komplexné riešenie zabezpečujúce služby modulu „Identity and Access Management“, ktoré sa skladá zo samotného produktu/aplikácie IAM a podpornej infraštruktúry (autentifikačný server, moduly web gate, a pod.)
17	SS	Súkromný sektor
18	TCF	Faktor technickej komplexnosti (TCF)
19	UAW	Neupravená váha používateľských interakcií (UAW)
20	UCP	Use-case body (UCP), prípad použitia
21	ÚPVS	Ústredný portál verejnej správy
22	UUCP	Neupravené use-case body (UUCP)
23	UUCW	Neupravená váha use-casov (UUCW)
24	VS	Verejná správa

Tabuľka 1: Prehľad použitých skratiek a značiek

2 Manažérske zhrnutie

Čiastková štúdia uskutočniteľnosti „Identity and Access Management“ (IAM) bola vypracovaná na základe požiadaviek Ministerstva financií SR s cieľom analyzovať realizovateľnosť nevyhnutnej a dostatočnej infraštruktúry, ktorá by umožnila riadiť práva identít prístupujúcich k službám eGovernmentu.

Základný rozsah požadovaných funkcionalít je uvedený v Národnej koncepcii informatizácie verejnej správy.

Aktuálny stav riadenia prístupových práv k službám poskytovaným prostredím eGovernment a informačným systémom verejnej správy všeobecne nie je v súlade s požiadavkami na bezpečnosť a efektívnosť súvisiacimi s cieľmi informatizácie verejnej správy.

V súčasnosti nie je možné zabezpečiť včasné, efektívne a bezpečné riadenie prístupu k informačným systémom poskytujúcim službu v rámci prostredia eGovernmentu.

2.1 Odporúčania

Navrhovaný systém riadenia identít a prístupových práv by mal implementovať v ďalších kapitolách podrobnejšie popísané základné princípy rozdelené do nasledovných oblastí:

- správa identít,
- správa autentifikačných údajov,
- správa prístupových práv,
- provisioning / poskytovanie informácií o oprávneniach,
- monitorovanie a audit,
- single-sign on pre webové služby / autentifikačný server.

Riešenie IAM by malo slúžiť ako centralizovaný konsolidovaný register všetkých identít využívajúcich publikované služby poskytované prostredím eGovernment a ich prístupové práva do spravovaných systémov.

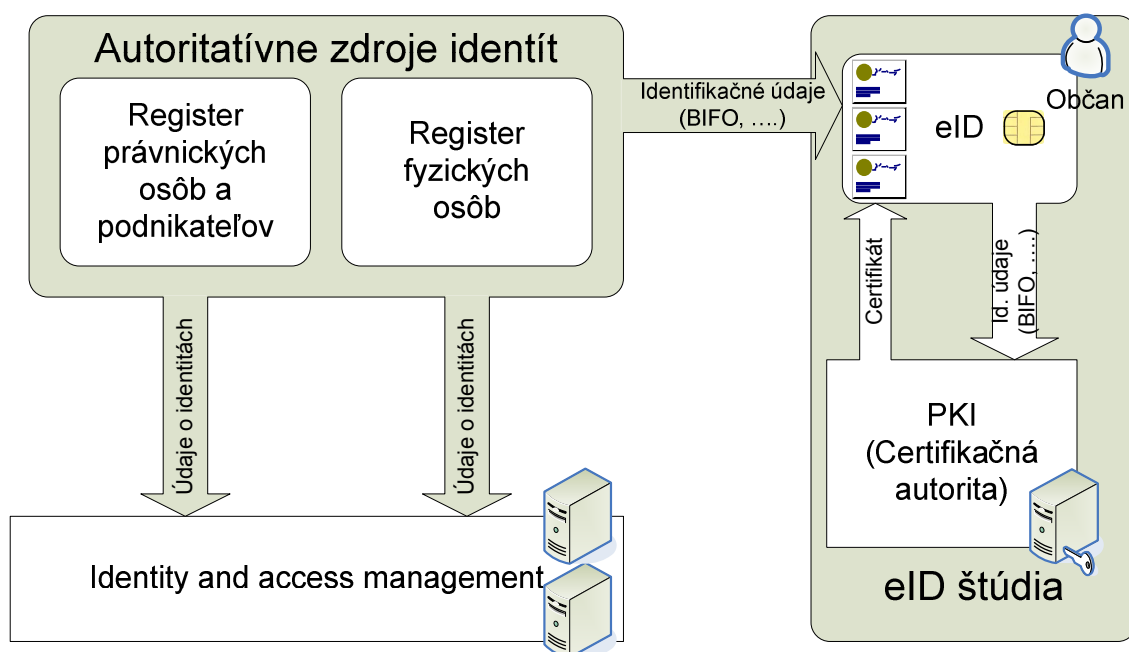
IAM je silne závislé na iných oblastiach spracovávaných ďalšími štúdiami uskutočniteľnosti:

- Registre (RFO, RPOaP, Portál zamestnancov verejnej správy), zoznamy medzi sebou komunikujúcich informačných systémov verejnej správy,
- eID karta spolu s príslušnou infraštruktúrou,
- interná architektúra portálov verejnej správy.

Poznámka: Pre zjednodušenie vychádzajú nasledujúce popisy z predpokladu, že používateľom elektronických služieb publikovaných prostredím eGovernmentu je najmä používateľ – občan.

Na to, aby identity (občania) mohli využívať služby prostredia eGovernment, resp. aby k nim mohli získať prístup, musia byť zaregistrovaní v systéme IAM. Túto registráciu však navrhujeme z pohľadu občanov vykonávať automaticky na základe premisy, že kto je občan SR má právo pristupovať k službám eGovernmentu (ak bude pre ne autorizovaný). Občan sa v našom návrhu nemusí registrovať na žiadnom z portálov verejnej správy, pre prístup postačuje to, že je ako občan vedený v RFO a má zriadené médium pre elektronickú identifikáciu (napr. eID kartu) s vydanými potrebnými certifikátmi.

Na Obr. 1.1 je schematicky zobrazený proces automatickej registrácie:



Obrázok 1.1: Registrácia identity do systému IAM

- Register fyzických osôb, Register právnických osôb a Portál zamestnancov verejnej správy vedú zoznamy „identít“, ktoré môžu mať potenciálne prístup k službám eGovernmentu.
- Register fyzických osôb priradí občanovi v rámci svojich procesov bezvýznamový identifikátor BIFO, ktorý bude súčasťou jeho identifikačného dokladu (eID karty).
- Informácie z RPOaP a RFO sú automaticky posielané do systému IAM, ktorý na ich základe vytvorí virtuálne identity v prostredí IAM.
- Na základe informácií z RPOaP a RFP, a definovaných pravidiel systém priradí vytvoreným identitám definované prístupové práva (napr. právo používať ÚPVS).

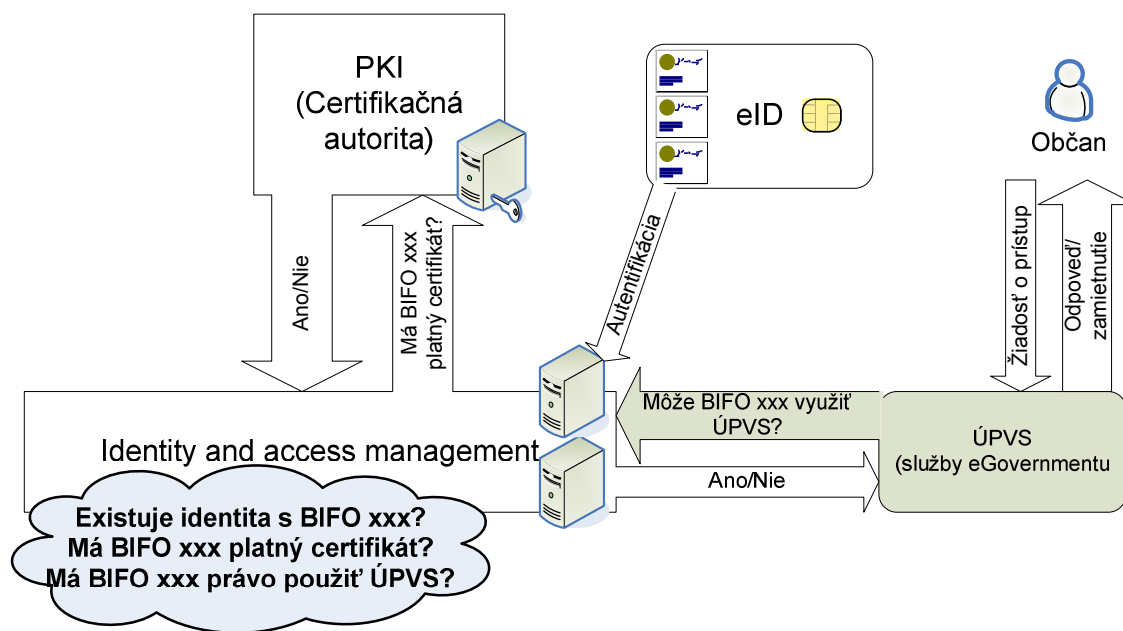
- Pre využívanie elektronických služieb musí občan získať eID kartu a získať autentifikačný certifikát (prípadne ďalšie certifikáty – ako kvalifikovaný certifikát pre ZEP) od akreditovanej certifikačnej autority, na základe identifikačných údajov občana. Súčasťou certifikátu bude aj BIFO, čo umožní spoľahlivú identifikáciu občana v systéme IAM a celom systéme elektronickej verejnej správy.

Na základe vyššie uvedených krokov získa občan elektronický autentifikačný prostriedok (autentifikačný certifikát na eID karte) a systém IAM dostatok informácií, aby na základe autentifikačného certifikátu poskytnutého občanom, ako aj informačným systémom verejnej správy, zamestnancom verejnej správy a iným spravovaným identitám vedel zabezpečiť:

- autentifikáciu – overenie spravovanej identity pri komunikácii so službami eGovernmentu,
- autorizáciu – stanovanie prístupových práv spravovanej identity, ku službám poskytovaným eGovernmentom, na ktoré má občan podľa definovaných pravidiel nárok.

Návrh riešenia karty eID a príslušnej infraštruktúry je popísaná v Štúdii uskutočniteľnosti eID.

Využívanie služieb identitou typu občan je zobrazené na Obr. 1.2.



Obrázok 1.2: Využívanie služieb eGovernmentu v spolupráci s IAM

V uvedenom príklade chce napríklad občan využiť služby portálu ÚPVS. Na úspešné poskytnutie služby prebehnú v istom zjednodušení tieto kroky:

- Občan pristúpi na portál ÚPVS, aby mohol začať využívať niektorú zo služieb (prihlásenie).
- Identifikuje/authentifikuje sa eID kartou, na ktorej je uložený autentifikačný certifikát s BIFOm.

- IAM si u vydavateľa certifikátu (príslušnej certifikačnej autority ako súčasti PKI) overí, či je certifikát platný, t.j. či je na jeho základe možné považovať poskytnuté informácie o identite za dôveryhodné. Ak certifikát nie je platný, prístup ku službe bude zamietnutý. Ak je certifikát platný, pokračuje sa ďalším krokom.
- IAM na základe informácií z RFO a definovaných prístupových pravidiel určí, či má občan právo využívať služby ÚPVS. Ak nie, prístup bude občanovi zo strany portálu ÚPVS zamietnutý.
- Ak sú splnené všetky podmienky pre poskytnutie prístupu občanovi na portál ÚPVS, systém IAM poskytne portálu ÚPVS definované údaje o občanovi spolu s informáciou, že občan môže využiť služby portálu ÚPVS.
- Portál ÚPVS využije informácie poskytnuté z IAM napr. na personalizáciu prostredia a občanovi umožní použiť služby portálu.

Pre efektívne využívanie služieb IAM bude potrebné organizačne a procesne zabezpečiť definovanie a naplnenie pravidiel pre prístup jednotlivých identít.

Jednotný mechanizmus správy identít a prístupových práv sa bude musieť premietnuť i do niektorých jestvujúcich právnych úprav. Bude potrebné ho premietnuť do zákona o informačných systémoch verejnej správy, bolo by užitočné, aby sa premietol i do zákona o slobodnom prístupe k informáciám, a bude potrebné vyriešiť i možnosť elektronickej komunikácie medzi žiadateľom a vybavujúcim pracovníkom v zákone o elektronickej podpise tak, aby sa legislatívne vytvoril priestor na kvalifikované autentifikačné certifikáty. Nové ustanovenia sa budú týkať aj jestvujúceho systému ochrany údajov, ktoré bude potrebné premietnuť i do zákona o ochrane utajovaných skutočností a zákone o ochrane osobných údajov.

Nasadenie Identity and Access Managementu sa bude musieť tiež zohľadniť v ďalších navrhovaných právnych úpravách, osobitne v zákone, ktorý vytvorí elektronickej ID kartu, v právnej úprave systému identifikácie občanov pri prístupe do základných registrov a v osobitných zákonoch o jednotlivých základných registroch (budúce novelizácie zákonov č. 224/2006 Z.z. a č. 301/1995 Z.) a ďalších databázach v správe verejnoprávných orgánov a organizácií.

Z technického hľadiska predstavuje riešenie IAM technologickú infraštruktúru, ktorá je čiastočne transparentná pre používateľa a ostatné služby eGovernmentu. Riešenie IAM samotné poskytuje aj niektoré publikované eGovernment služby, ale vo veľkej miere bude fungovať „na pozadí“ ostatných služieb, a preto bude potrebné zabezpečiť jeho integráciu do prostredia eGovernment a nevyhnutnú kompatibilitu so službami, ktoré ho budú využívať.

Odporúčame implementovať riešenie IAM, ktoré by zabezpečilo jednotnú a centralizovanú správu prístupu identít k službám publikovaných v prostredí eGovernment.

Riešenie IAM by okrem základnej funkcionality riadenia prístupových práv bodovo vymenovanej vyššie, by malo poskytovať aj nasledovné funkcie:

- vykonávať autentifikáciu užívateľov prístupujúcich k službám VS – technologicky môžu byť, najmä v prechodných obdobiach, použité bezpečnostne rôzne silné autentifikačné mechanizmy, avšak z koncového hľadiska odporúčame využitie výlučne certifikátov na účely autentifikácie,
- poskytovať autorizačné rozhrania pre prístup k službám VS,
- možnosť delegovania, resp. splnomocnenia inej osoby (úradníka) na vykonanie stanovených úkonov v mene identity, pričom delegovanie by malo umožňovať až 3-úrovňové zastupovanie (napr. občan – jeho zamestnávateľ – jeho zamestnanec v špecifickej funkcii – zástupca takéhoto zamestnanca) a vyhodnocovanie oprávnenosti pri takomto zastupovaní,
- možnosť implementácia tzv. Single Sign-On riešenia (pre občanov na úrovni webových stránok), ktoré umožní po prvom prihlásení používať v rámci danej relácie ostatné systémy a služby eGovernmentu bez potreby prihlasovať sa ku každému z nich,
- možnosť auditných funkcií a funkcií na prevenciu a detekciu potenciálnych podvodov vo vzťahu k prístupu k službám eGovernmentu.

3 Popis aktuálneho stavu

3.1 Popis aktuálneho stavu a služieb

3.1.1 Analýza požiadaviek a potrieb

V súčasnosti tvoria informačné systémy verejnej správy, resp. existujúce prvky eGovernmentu technologicky a architektonicky heterogénne prostredie, ktoré neumožňuje efektívne zdieľať zdroje jednotlivých systémov a centralizovane riadiť prístup k nim. Pre existujúce služby eGovernmentu sú prístupové práva riadené lokálne, pričom dochádza k duplicitným výskytom jednotlivých informácií o používateľov, nakoľko neexistuje jednotný centrálny register informácií o identitách, ktorý by slúžil na riadenie prístupu k jednotlivým službám eGovernmentu.

V dôsledku súčasnej nekoordinovanej praxe existujú viaceré problémy v oblasti riadenia prístupových práv vo verejnej správe:

- Rôzna úroveň bezpečnosti vyplývajúca z:
 - rôznych požiadaviek na bezpečnosť pre jednotlivé spracovávané údaje v procesoch eGovernment,
 - rôznej kvality procesu riadenia a kontroly prístupových práv,
 - rôznej kvality modelu prístupových práv a rolí,
- Komplikovaný a zväčša manuálny proces priradovania a odoberania prístupových práv pre jednotlivé služby, ktorý má za následok zdržania v procese žiadania a samotného priradenia prístupových práv. Táto doba sa môže pohybovať od niekoľkých hodín až po niekoľko dní, resp. týždňov.

Súčasný model riadenia prístupových práv neumožňuje v praxi:

- jasne definovať a zabezpečiť proces riadenia prístupových práv,
- jasne definovať jednotlivé roly pre prístup do koncových systémov a pravidlá pre ich priradovanie koncovým používateľom,
- efektívne a automatizovane riadiť (pridávať/odoberať) prístupové práva koncovým používateľom na základe informácií, ktoré už existujú v iných systémoch verejnej správy,
- sledovať a zaznamenávať potenciálne narušenia informačnej bezpečnosti vo vzťahu k logickému prístupu, resp. proaktívne im predchádzať.

3.1.2 Architektúra

V súčasnosti je architektúra informačných systémov pre riadenie prístupu interných zamestnancov tvorená prevažne doménovým radičom na jednotlivých úradoch, pričom riadenie prístupu do domény slúži ako prvá a niekedy aj jediná bariéra z hľadiska logického prístupu.

Vytvorením používateľského účtu v doméne a zaradenie do príslušných skupín (ak sú definované) umožní relevantnému používateľovi prístup do definovaných oblastí IS.

V prípade, ak sa na riadenie prístupu nepoužíva doména, je prístup riadený buď na úrovni Intranetu alebo až na úrovni jednotlivých aplikácií, ktoré sú na úrade využívané (ak poskytujú funkcionality riadenia prístupu). Toto riešenie sa využíva hlavne pre riadenie prístupu fyzických a právnických osôb do týchto systémov, nakoľko fyzické a právnické osoby zo strany verejnosti nemajú prístup do internej siete relevantných úradov.

Riadenie prístupu občanov ku službám eGovernmentu prebieha zväčša formou zaregistrovania sa na konkrétnom portáli, pričom v niektorých prípadoch je následne požadované potvrdenie identity používateľa, napr. preukázaním sa občianskym preukazom, čo vyžaduje minimálne jednu osobnú návštevu daného úradu. Občania sa musia registrovať do každej služby osobitne, pričom nie je zavedená unifikácia a centralizácia správy ich prístupových práv.

V súčasnosti je na ÚPVS využívaný registračný modul (RE). Registračný modul poskytuje služby identity manažmentu, manažmentu rolí a prístupov. Uchováva údaje registrovaných používateľov na portáli, zabezpečuje autentifikáciu používateľa na základe prihlasovacieho mena a hesla alebo pomocou zaručeného elektronického podpisu v prípade, že má používateľ zaregistrovaný a overený kvalifikovaný certifikát (KC).

3.1.3 Procesná analýza

Proces riadenia prístupu zamestnancom v súčasnej praxi pozostáva vyplnenia žiadosti o zriadenie/odobratie prístupu alebo zmeny prístupu (papierovej alebo elektronickej), ktorú vyplňa zväčša nadriadený zamestnanca, pre ktorého prístup sa žiada, resp. fyzická alebo právnická osoba ako používateľ služby.

Spôsob a rozsah schvaľovania žiadosti je individuálny a závisí na nastavení procesov a právomocí na danom úrade. Po schválení je žiadosť doručená administrátorovi/administrátorom jednotlivých systémov, ktorí zabezpečia príslušnú zmenu v prístupových právach koncového používateľa, resp. zriadenia prístupu môže sprostredkované zabezpečiť relevantný úradník prostredníctvom aplikácie na to vytvorenej.

V niektorých prípadoch sa pre zabezpečenie základného prístupu zamestnancov úradu (prístup do domény, zriadenie emailového účtu, prístup na spoločný Intranet) využívajú informácie z personálneho systému. Z personálneho systému sa urobí export relevantných informácií, ktoré sú potom buď automaticky alebo zväčša manuálne administrátormi využité pre z nich vyplývajúce zmeny prístupových práv koncových používateľov.

Preverky práv, ktoré sú vytvorené v koncových systémoch sa nevykonávajú pravidelne a kvalita prípadnej preverky veľmi závisí od jej vykonávateľa.

Pri zavádzaní elektronických služieb je potrebné riešiť nasledovné problémy:

- identifikovanie občana (užívateľa) a jeho autentifikácia v osobnom styku obvykle vizuálne alebo na základe vlastnoručného podpisu,
- overenie, či je prístupujúca identita oprávnená využiť služby.

Interaktívne služby verejnej správy slúžia na poskytovanie (okrem iného) nasledovnej funkcionality:

- poskytnutie informácie o stave vybavovania podaných žiadostí,
- informovania občana prostredníctvom „dátovej schránky“, do ktorej mu budú orgány verejnej správy zasielať poštu, ktorá bude ekvivalentom papierovej pošty
- umožnenie prístupu k elektronickým informáciám, ktoré môžu byť sprístupnené len danému občanovi
- umožnenie prístupu k verejným elektronickým informáciám, pri ktorých je potrebné prístupujúceho občana identifikovať, napr. z dôvodu spoplatnenia služby.

Pre zabezpečenie prístupu k interaktívnym (portálovým) službám je potrebné zabezpečiť bezpečnú identifikáciu a autentifikáciu občana, t.j. možnosť spoľahlivo určiť, ktorý občan k týmto službám prístupuje. Pre tieto účely nie je možné z legislatívnych a bezpečnostných dôvodov využiť zaručený elektronický podpis.

Na základe vyššie uvedeného bolo navrhnuté používanie autentifikačného certifikátu pre účely autentifikácie jeho držiteľa pri prístupe k službám verejnej správy a potenciálne aj k budúcim službám inštitúcií súkromného sektora. IAM riešenie musí podporovať autentifikáciu identít na základe verejných kľúčov a príslušných certifikátov.

3.1.4 Legislatívna analýza

Pod názvom Identity and Access Management má Národná koncepcia informatizácie verejnej správy na mysli problematiku vstupovania do jednotlivých portálov verejnej správy: registráciu používateľov, správu ich používateľských účtov, ich autentifikáciu a autorizáciu. V koncepcia uvádza, že problematiku si každý z portálov verejnej správy v súčasnosti zabezpečuje samostatne.

Treba ešte upresniť, že prístup k informáciám, ktoré sa nachádzajú v rozličných databázach verejnej správy, aj ak sú už v elektronickej podobe, je veľmi rôznorodý:

- Sú databázy, ktoré sú už na internete verejne dostupné. K najdôležitejším patria údaje z katastra nehnuteľností a obchodný register. Občan sa tu môže dostať k akýmkoľvek údajom, t.j. nielen k údajom o sebe. Ide vlastne o verejné databázy. Na druhej strane, tieto databázy majú iba informatívny charakter: ak si občan vytlačí výpis z týchto databáz, nemôže ich použiť v úradnom styku.

- Ďalej to sú databázy, ktoré sú už v elektronickej podobe, mohli by byť dostupné cez internet, ale občan sa do týchto databáz nedostane. Dostanú sa k nim len úradníci, ktorí ich majú oprávnenie využívať. Najtypickejšou z takýchto databáz je register trestov. Oprávnenie na prístup do registra trestov vyplýva z pracovného zaradenia pracovníkov, ktorí k údajom z nich majú prístup. Títo pracovníci v súčasnosti majú prístup k celým registrom, môžu sa dostať k údajom aj za občanov, ktorí o to nežiadajú. Občan môže získať informácie len o sebe, ak o ne požiada príslušného pracovníka, a ten mu vydá úradnú listinu (napr. výpis z registra trestov).
- Treťou kategóriou sú informácie a databázy, ktoré cez internet nie sú dostupné. A to aj ak už jestvujú v elektronickej podobe. K týmto údajom majú prístup jedine pracovníci, ktorí na to majú oprávnenie a sú zaradení do príslušných funkcií v inštitúcii, ktorá databázu takýchto informácií spravuje. Súčasná právna úprava však ani týmto pracovníkom nebráni vyberať z databázy aj údaje, o ktoré nikto nežiada. Pred takýmto možným zneužitím údajov nejestvuje zatiaľ žiadna ochrana. Občan, alebo iná inštitúcia môže o údaje z takýchto databáz požiadať, a ak mu to príslušné právne normy dovoľujú, tak mu oprávnený pracovník poskytne príslušnú informáciu, prípadne mu poskytne úradný výpis. Väčšina databáz, ktoré sa podľa navrhovaného systému majú stať základnými registrami majú tento charakter.
- Štvrtou kategóriou sú databázy, ktoré majú čisto interný charakter. Kým tie vyššie uvedené sú, alebo by mali byť chránené, predovšetkým preto, lebo zhromažďujú rozličné, aj citlivé osobné údaje, alebo obchodné údaje, v tejto kategórii sa nachádzajú údaje, ktoré chráni pre zneužitím štát. Z týchto databáz sa údaje poskytujú len používateľom podľa predpisov o ochrane utajovaných skutočností a pre internú potrebu inštitúcií, ktoré ich vedú.

Právna úprava súčasného stavu prístupového procesu do registrov a ostatných informačných systémov verejnej správy sa týka predovšetkým tradičnej formy, keď sa občan, (žiadateľ) musí osobne dostaviť do úradovne každej príslušnej inštitúcie, ktorá poskytuje z konkrétnej databázy výpis. Svoju totožnosť preukazuje predovšetkým občianskym preukazom (zákon č. 224/2006 Z.z. o občianskych preukazoch v znení neskorších predpisov), prípadne iným dokladom, ktoré uvádza napríklad zákon o Policajnom zbore Slovenskej republiky č. 171/1993 Z.z. v znení neskorších predpisov v § 18 ods. 2 (preukaz poslanca Národnej rady Slovenskej republiky, preukaz člena vlády, služobný preukaz sudcu, služobný preukaz prokurátora, služobný preukaz príslušníka ozbrojeného zboru, potvrdenie o odovzdaní, strate alebo odcudzení občianskeho preukazu). Obdobne možno na preukázanie totožnosti použiť aj cestovný pas. Občan takýto úradný výpis z niektorej databázy verejnej správy potrebuje ako doklad na vybavenie svojej žiadosti na inom orgáne verejnej moci.

Systém teda funguje tak, že na vybavenie svojej žiadosti musí občan zhromaždiť potrebné údaje z databáz, ktoré vedú iné inštitúcie verejnej moci, než tá, ktorá o jeho veci rozhoduje. Do najdôležitejších databáz (registrov), obsahujúcich predovšetkým osobné údaje, občan priamy prístup nemá, dostane len úradný výpis, obsahujúci tie údaje, ktoré sú potrebné na vybavenie jeho veci. Za ochranu pred zneužitím zodpovedajú príslušní pracovníci inštitúcie, ktorá databázu spravuje, ktorí do nej majú prístup a výpisy poskytujú. Na identifikáciu občana sa v týchto databázach používa najčastejšie všeobecný identifikátor: rodné číslo (zákon Národnej rady Slovenskej republiky č. 301/1995 Z.z. o rodnom čísle v znení neskorších predpisov). Len niektoré špeciálne databázy využívajú osobitné identifikačné čísla (napríklad daňové úrady používajú daňové identifikačné čísla) alebo ich kombináciu s rodným číslom.

Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy v znení neskorších predpisov v § 8 umožňuje vydávanie elektronických odpisov, alebo výpisov z informačných systémov verejnej správy. Takýto odpis alebo výpis môže, ak to technické podmienky umožňujú, príslušný úradník, ktorý má prístup do potrebnej databázy, odoslať v elektronickej podobe, a podpísať ho zaručeným elektronickým podpisom s časovou pečiatkou. Zákon výslovne požaduje, aby úradník zistil totožnosť osoby žiadajúcej o výpis, alebo odpis, neustanovuje však ako. Do úvahy teda prichádza buď tradičné zistenie totožnosti (fyzicky predložením občianskeho preukazu), alebo elektronicky, ak žiadateľ využije zaručený elektronický podpis. Pravdepodobne by sa dal použiť aj obyčajný elektronický podpis, ale súčasná právna úprava využívanie jednoduchého elektronického podpisu v styku s orgánmi verejnej moci síce pripúšťa, ale okruh jeho použitia značne obmedzuje.

Osobitným okruhom poskytovania údajov, ktoré sú aj v databázach, ktoré vedú orgány verejnej moci, sú údaje poskytované podľa zákona č. 211/2000 Z.z. o slobodnom prístupe k informáciám. Orgány verejnej moci sú povinné poskytnúť akékoľvek informácie, ktoré nepodliehajú nejakej z foriem utajovania, alebo ochrany ustanovenými príslušnými právnymi normami. Poskytujú ich v dvoch režimoch: vymedzený okruh informácií sú povinné sprístupniť (zverejniť) a ostatné poskytujú na žiadosť. Na zverejnenie sa dnes využívajú portály, ktoré tieto inštitúcie už väčšinou majú, a to aj bez akejkoľvek právnej úpravy. Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy zriadil Ústredný portál verejnej správy, ktorý sčasti už slúži a v budúcnosti bude oveľa precíznejšie slúžiť i na tieto účely.

Pokiaľ ide o poskytovanie informácií na žiadosť, okrem tradičnej písomnej (papierovej) formy, asi nič nebráni používať i elektronickú komunikáciu. Ide napokon o informácie, ktoré nepodliehajú žiadnej ochrane, takže ani otázka identifikácie žiadateľa nie je významná. Dôležité je však, aby bolo možné preukázať, že žiadosť o informáciu bola podaná, kedy bola podaná, a ak bola vybavená, tiež kedy bola vybavená. Z týchto procesných skutočností totiž môžu vyplývať právne následky. Preto tu v elektronickej forme asi tiež asi prichádza do úvahy využívanie elektronického podpisu, ktorý pre tieto účely poskytuje už dostatočnú základňu pre identifikáciu tak žiadateľa, ako aj úradníka, čo žiadosť vybavuje. Využitím časovej pečiatky sa zabezpečí aj údaj o čase podania žiadosti a o čase jej vybavenia.

Z uvedeného vyplýva, že otázka identifikácie a otázka prístupových práv pri vstupe do informačných systémov verejnej správy sa v súčasnosti rieši ad hoc, podľa agendy, o ktorú ide. Každý register, resp. informačný systém, spravujú konkrétni úradníci, ktorí majú právo prístupu len do tohto registra. Občan, ktorý potrebuje údaje z viacerých registrov, musí požiadať o výpis každého z nich osobitne. Všade bude musieť preukázať svoju totožnosť. A to aj vtedy, ak údaje využije pre rozhodovanie iného orgánu verejnej moci.

3.2 Hodnotenie aktuálneho stavu

Aktuálny stav riadenia prístupových práv k službám poskytovaným prostredím eGovernment a informačným systémom verejnej správy všeobecne nie je v súlade s požiadavkami na bezpečnosť a efektívnosť súvisiacimi s cieľmi informatizácie verejnej správy.

V súčasnosti nie je možné zabezpečiť včasné, efektívne a bezpečné riadenie prístupu k informačným systémom poskytujúcim službu v rámci prostredia eGovernmentu.

3.3 Návrh zmeny

Systém riadenia identít a prístupových práv by malo implementovať nižšie popísané základné princípy rozdelené do nasledovných oblastí:

- správa identít,
- správa autentifikačných údajov,
- správa prístupových práv,
- provisioning/poskytovanie informácií o oprávneniach,
- monitorovanie a audit,
- Single-Sign On pre webové (portálové) služby VS/authentifikačný server.

Nižšie uvedené základné princípy definujú základne vlastnosti IAM systému ako technického riešenia, obsahujú však aj procesné a organizačné aspekty, ktorých naplnenie je potrebné pre fungovania celého riešenia IAM. Systém IAM je centrálnym zdrojom poskytovania uvedených služieb.

Správa identít

- Existuje centralizované riešenie IAM ako konsolidovaný register všetkých identít využívajúcich publikované služby poskytované prostredím eGovernment. Identity sú spravované v rámci jedného globálneho riešenia IAM, ktoré však umožňuje správu identít pre jednotlivé orgány VS tam, kde to má zmysel samostatne – napr. prístupové práva svojich zamestnancov.
- Nasledovné typy identít sú registrované v IAM systéme:
 - fyzické osoby,
 - právnické osoby,
 - neosobné identity – typicky informačné systémy.
- Nasledovné typy fyzických osôb sú reprezentované ako identity:
 - používateľov služieb (fyzické a právnické osoby, široká verejnosť, cudzinci – osoby ktoré môžu byť fyzicky hendikepované),
 - zamestnancov úradov, ktorí spravujú a zabezpečujú dohľad na poskytovanými službami (ďalej len ako „zamestnanci“), avšak len ak je táto správa a dohľad vykonávaná prostredníctvom existujúcich publikovaných služieb eGovernmentu. T.j. cieľom tejto štúdie nie je posudzovať riadenie prístupu k tzv. „back-endu“ informačných systémov

verejnej správy, bez ohľadu na to, či poskytujú alebo neposkytujú publikované služby eGovernmentu.

- IAM systém obsahuje informácie o všetkých používateľských účtoch využívajúcich služby eGovernmentu a ich priradenie jednotlivým identitám.
- Všetky názvy používateľských účtov vo všetkých informačných systémoch/službách sú konzistentné a v súlade s definovanou konvenciou pre pomenovanie účtov, vrátane identifikátorov pre občanov.
- IAM systém registruje v obmedzenej miere informácie o organizačnom kontexte, vrátane časovej informácie (účinnosť od – do), ktorý umožňuje riadenie prístupu na základe organizačných pravidiel.
- Informácie sú do IAM systému dodávané iba z autoritatívnych zdrojov s cieľom zaručiť konzistenciu týchto údajov, pričom pre jednotlivé typy identít sú definované nasledovné autoritatívne zdroje informácií:
 - fyzické osoby – Register fyzických osôb,
 - právnické osoby – Register právnických osôb a podnikateľov,
 - register inštitúcií verejnej správy,
 - portál zamestnancov verejnej správy – identity zamestnancov budú riadené individuálne na jednotlivých úradoch,
 - identity informačných systémov – budú riadené manuálne.
- Akékoľvek zmeny v rámci autoritatívnych zdrojov smú byť vykonávané iba oprávneným personálom.
- Zmeny v autoritatívnych zdrojoch vedú automaticky k príslušným zmenám stavu identít, organizačnej štruktúry a prístupových práv v IAM systéme a následne koncových spravovaných systémoch/službách.

Správa autentifikačných údajov

- Všetky entity musia byť autentifikované pred prístupom k systémom/službám, ktoré nie sú len všeobecného/verejného/informačného charakteru.
- Zoznam všetkých podporovaných autentifikačných prostriedkov je vedený v systéme IAM, napr. certifikáty, one-time password tokeny, heslá. Bez definovania bezpečnostných požiadaviek na úroveň bezpečnosti pri využívaní jednotlivých služieb eGovernmentu je potrebné využívať najsilnejší spôsob autentifikácie – autentifikácia protokolmi verejnej kryptografie využitím certifikátov.

- Spôsob autentifikácie pre jednotlivé služby a systémy bude určený bezpečnostnými požiadavkami vyplývajúcimi z analýzy rizík. Je možné definovať viacero klasifikačných stupňov, pre každý stupeň môže byť vyžadovaný iný autentifikačný prostriedok.
- Pre každého používateľa vedie systém IAM zoznam pridelených prostriedkov autentifikácie.
- Ak sú povolené heslá, sú definované politiky kvality hesiel, vrátane minimálnej dĺžky hesla, doby platnosti hesla, požiadaviek na komplexnosť, histórie použitých hesiel, atď.
- Zmenu a resetovanie hesla môžu iniciovať používatelia (identity) sami v systéme IAM, pre všetky informačné systémy, v ktorých má daná identita vytvorený používateľský účet. Autentifikácia heslom môže byť využívaná napríklad pre autentifikovanie informačných systémov medzi sebou v prechodnom období, v tomto prípade správcovia systémov budú nastavovať heslá. Z pohľadu bezpečnosti komunikácie medzi systémami a obmedzenia možného úniku údajov je jednoznačne preferovaným konečným spôsobom autentifikácie pre informačné systémy použitie certifikátov a vzájomná autentifikácia pomocou nich.
- V prípade zistenia potenciálne fraudulentného správania môže byť vyžadovaná dodatočná reautentifikácia s využitím definovaných autentifikačných prostriedkov.

Správa prístupových práv

- Prístupové práva k jednotlivým službám eGovernmentu sú občanom poskytované automaticky na základe ich práva využívať služby eGovernmentu. Občanom nie sú na úrovni IAM pridelené priamo práva pre koncové informačné systémy (pozri časť Provisioning).
- Prístupové práva k službám sú poskytované identitám na základe ich príslušnosti k organizačnej štruktúre, resp. v prípade zamestnancov ich profesie. Informácie o roliach, ktoré existujú v riadených informačných systémoch, povolených možnostiach priradenia rolí v týchto systémoch jednotlivým pozíciám organizačnej štruktúry, profesiám a identitám, sú uchovávané a aktualizované centrálné v systéme IAM, pričom správa, resp. aktualizácia týchto prístupových práv môže byť decentralizovaná – niektoré typy prístupových práv môžu spravovať určené pracovníci orgánov, ktorým tieto prístupové práva zodpovedajú. Zároveň sú v systéme IAM uchovávané a aktualizované informácie o skutočnom priradení určitých rolí jednotlivým užívateľom (entitám) prostredníctvom používateľských účtov.
- Prístup k systémom je priradený v súlade so zásadou “najnižšieho privilégia”, t.j. identite sú pridelené iba tie privilégia, ktoré potrebuje na vykonanie svojich pridelených úloh.
- Pre priradenie roly je možné zadať, že toto priradenie nadobúda účinnosť od určitého termínu a vyprší po uplynutí stanovenej doby.
- Oprávnení aktéri sú definovaní pre všetky procesné činnosti. Všetky úlohy správy prístupových práv sú vykonávané podľa definovaných a zdokumentovaných procesov.

- Prístupové práva sú riadené podľa Role Based Access Control modelu. Priradenie rolí môže byť manuálne alebo automatické. Je možné definovať pravidlá pre automatické priradzovanie rolí pri splnení konkrétnych kritérií.
- Roly pre prístup k službám definuje subjekt verejnej správy, pre potreby ktorého sa daná rola vytvára. Požiadavku na vytvorenie (zmenu, zrušenie) roly schvaľuje príslušný zodpovedný pracovník; zároveň určí, pre ktoré organizačné zložky, profesie, pracovné pozície alebo jednotlivých používateľov je rola určená.
- Roly do systému IAM a ich zmeny zadáva príslušný zodpovedný pracovník za daný subjekt VS.
- Definícia rolí zahŕňa aj definíciu segregácie právomocí. Systém IAM monitoruje a vynucuje dodržiavanie segregácie právomocí. Pridelenie rolí v rozpore s definovanými pravidlami segregácie je okamžite eskalované IAM systémom podľa definovaných pravidiel, pričom pridelené role nesmú byť aktivované skôr ako je uzavretý eskalačný proces.

Nastavovanie prístupových práv v riadených systémoch (Provisioning)

- Provisioning práv (autorizácií) v koncových informačných systémoch (vrátane databáz a operačných systémov) vykonáva systém IAM podľa definovaných mapovaní rolí pre eGovernment služby a prístupových práv v koncových systémoch.
- Pre systémy, ktoré nie sú technicky integrované so systémom IAM prebieha provisioning vo forme dohodnutých správ (napr. email) smerovaných na dohodnuté subjekty (napr. administrátorov, ktorí podľa príslušného emailu nastavujú práva v koncových systémoch).
- Pre informačné systémy integrované s IAM, ktoré si udržiavajú vlastné autorizačné informácie prebieha provisioning zmien najneskôr do nasledujúceho pracovného dňa.

Monitorovanie a audit

- Monitorovací systém umožňuje online detekciu podvodných aktivít, stanovovanie miery rizika že ide o podvodnú aktivitu a iniciáciu automatickej reakcie.
- Kedykoľvek je možné zobrazit' všetky práva aktuálne alebo v čase v minulosti priradené špecifickej identite.
- Kedykoľvek je možné zobrazit' všetky identity, ktorým je pridelené aktuálne alebo v čase v minulosti špecifické právo.
- Je možné generovať pravidelné štatistické správy o rôznych typoch udalostí v IAM (napr. zlyhanie autentizácie, počet zmien hesla za každú entitu, atď.)
- Monitorovací systém musí byť autonómny/nezávislý od cieľových systémov, t.j. musí vedieť poskytnúť vyššie uvedené výstupy bez nutnosti komunikácie s cieľovými systémami.

Single Sign-On/Autentifikačný server

- Umožňuje autentifikáciu na základe certifikátov (podľa implementovaného PKI)
- Je podporované web Single Sign-On riešenie (automatické prihlásenie k IS na základe predchádzajúceho prihlásenia k inému systému) pre systémy, ktoré to technicky umožňujú.
- Všetky koncové systémy musia byť budované tak, aby podporovali Web Single Sign-On (**Web SSO**), čiže ak sa identita autentifikuje voči jednej webovej stránke, je autentifikovaná voči všetkým ostatným stránkam integrovaným na IAM riešenie.
- Web SSO využíva ako zdroj identít zdroj využívaný riešením IAM.

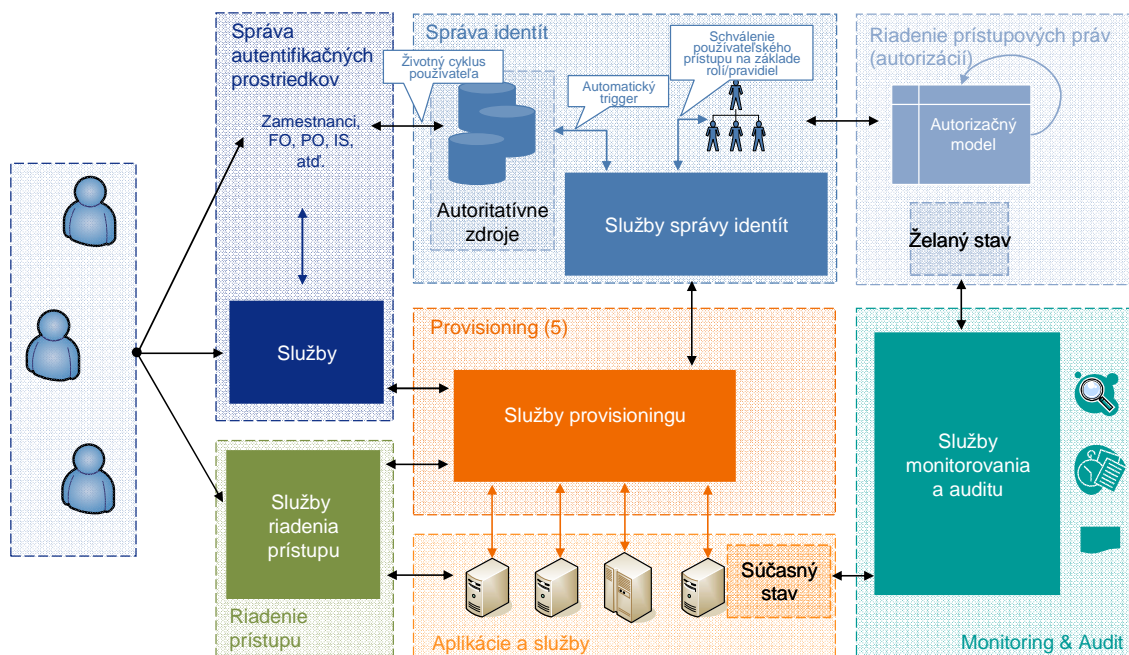
4 Navrhnuté riešenie

4.1 Popis navrhovaného riešenia

4.1.1 Konceptný model riešenia

Model riešenia IAM sa skladá z nasledovných logických modulov:

- **Správa identít** – modul zabezpečuje riadenie identít a ich základných údajov. Medzi hlavné funkcie patrí načítavanie nových identít, resp. zmena stavu existujúcich identít na základe informácií z autoritatívneho zdroja (informácií o identitách), spolu s informáciami o organizačnom, prípadne inom kontexte, ak sa využíva.
- **Správa autentifikačných prostriedkov** – modul zabezpečuje riadenie autentifikačných prostriedkov, ktoré slúžia na preukázanie deklarovanej identity. Medzi základne autentifikačné prostriedky patria heslá, certifikáty, tokeny generujúce jednorazové heslá, a pod. Pre potreby identifikácie identít občanov bude slúžiť primárne eID karta. Modul umožňuje riadiť priradenie, resp. vygenerovanie autentifikačných prostriedkov (napr. eID karta) pre identity. Tento modul spravuje informácie o tom, ktoré autentifikačné prostriedky sú vyžadované pre prihlásenie do toho-ktorého systému/služby na základe autentifikačnej politiky, a zoznam a konfigurácie autentifikačných prostriedkov priradených jednotlivým používateľom.
- **Správa prístupových práv (správa autorizácií)** – modul zabezpečuje určenie množiny povolených operácií, ktoré môže identita vykonať na základe katalógu roli/právomocí, typu, resp. jednotlivých atribútov identity (napr. zaradenie v organizačnej štruktúre) a pravidiel, ktoré tieto informácie vyhodnotia a stanovia, ku ktorým službám môže identita pristupovať. Sem spadajú aj riadenie delegovania právomocí.
- **Riadenie prístupu** – modul, resp. jeho agenti logicky inštalovaní pred vstupom k požadovanej službe vynucujú definované pravidlá prístupu v závislosti na oprávneniach identity a priamo zabezpečujú povolenie alebo odopretie prístupu ku službe, ku ktorej sú viazaní. Tento modul vyhodnocuje prístup aj na základe delegovaných právomocí.
- **Provisioning** – modul zabezpečuje prenos autorizačných informácií do koncových systémov, ktoré samé riadia prístup používateľov. Na základe zoznamu používateľov a ich rolí v koncovom systéme, sa tento vie rozhodnúť, ktoré služby jednotlivým používateľom poskytne, a ku ktorým prístup zamietne.
- **Monitoring a audit** – modul slúži na monitoring funkcie celého IAM riešenia, vrátane všetkých relevantných aktivít používateľov, správcov a pod. Dôležitou časťou tohto modulu je možnosť detekcie podvodných aktivít v reálnom čase (nie len dodatočnou analýzou žurnálov) na základe prispôsobiteľných pravidiel. Modul umožňuje v spolupráci s modulom na riadenie prístupu reakciu na podvodné aktivity (doplnková autentifikácia, zablokovanie session,...)



Obrázok 4.1: Logický model riešenia IAM

Princípy fungovania jednotlivých logických modulov sú popísané v časti 3.3 Návrh zmeny.

4.1.2 Model riadenia prístupových práv.

V navrhovanom modeli riadenia prístupových práv je potrebné rozdeliť spravované identity podľa toho, kam budú mať štandardne prístup:

- Fyzické osoby – fyzickej osobe je pridelená rola „Občan“, prípadne viac rolí („Občan pod 18 rokov“, „Občan nad 18 rokov“ a pod.), nakoľko každá fyzická osoba je zároveň občanom. Rola Občan poskytuje prístup ku každej verejne prístupnej službe, ktorú môže fyzická osoba potenciálne využiť. Prístup je priradovaný na základe práva občana využívať služby eGovernmentu. Týmto sa maximálne zjednoduší model riadenia práv pre fyzické osoby - občanov.
- Právnické osoby – podobne ako pre fyzické osoby, aj pre právnické osoby má zmysel povoliť prístup ku všetkým službám, ktoré môžu potenciálne využiť. Je potrebné zvážiť, či obmedzovať prístup ku službám na základe typov (obchodná organizácia, orgán štátnej správy, atď.), ktoré môžu jednotlivé právnické osoby nadobúdať. Môžu nastať dve situácie:
 - Prístup pre právnické osoby bude povolený pre všetky typy právnických osôb na všetky typy služieb, ktoré môžu právnické osoby použiť. V tomto prípade sa môže stať, že právnická osoba daného typu bude chcieť využiť služby, na ktorej využitie nie je oprávnená, resp. služby, ktoré v jej prípade nemajú zmysel. V takomto prípade bude potrebné kontrolovať oprávnenosť a zmysluplnosť požiadavky priamo v rámci procesu poskytovania služby a odmietnuť poskytnutie služby, ak je to na to dôvod – táto aktivita bude vykonaná priamo eGovernment službou, mimo IAM.

- Prístup pre právnické osoby bude riadený priamo na úrovni IAM na základe typu (formy) právnickej osoby. Tento prístup vyžaduje zadefinovanie zoznamu prístupných služieb pre jednotlivé typy právnických osôb do systému IAM a zavádzanie „biznis“ logiky meniacej sa s legislatívou priamo do prostredia IAM.
- Informačné systémy – riadenie prístupu informačných systémov bude vykonávané na základe definovaných dátových tokov v rámci procesov/služieb verejnej správy, z ktorých vyplynú požiadavky na spoločnú komunikáciu relevantných informačných systémov alebo služieb. Forma riadenia prístupu informačných systémov (automaticky, manuálne) bude určená na základe budúcich potrieb, avšak principiálne sa nelíši od riadenia prístupu „bežných“ identít. Očakáva sa, že nastavenie prístupových práv bude relatívne stabilné a po prvotnom nastavení nebude dochádzať k častej potrebe toto nastavenie meniť. Informačné systémy budú pristupovať k jednotlivým službám eGovernmentu prostredníctvom webových služieb.
- Zamestnanci verejnej správy – riadenie prístupu zamestnancov je jednotlivých typov identít najzložitejšie. Je možné použiť viac koncepcií:
 - Vytvorenie katalógu rolí a ich individuálne automatické priradovanie zamestnancom na základe ich pracovnej pozície, organizačnej jednotky, resp. iného kontextu. Pre efektívne fungovanie tohto riešenie by bolo potrebné zmapovať jednotlivé typy pracovných pozícií, zabezpečiť jednoznačné definovanie pracovných pozícií a ich pracovných náplní, na základe ktorých by boli vytvorené samotné roly a pravidlá pre ich priradenie. Tento variant zároveň pre efektívne fungovania predpokladá, že nedochádza k častej zmene pracovnej náplne jednotlivých pracovných pozícií, ale že sa len menia ľudia, ktorí sú na relevantnú pracovnú pozíciu priradení.
 - Priebežné definovanie katalógu rolí a ich „manuálne“ priradovania na základe oprávnenej potreby alebo žiadosti. Toto riešenie je vhodnejšie do častejšie sa meniaceho prostredia (ktorým verejná správa bez pochyby je), avšak s postupom času a pribúdajúcim množstvom rolí je riadenie prístupu stále zložitejšie a komplikovanejšie. Pri takomto prístupe vnika množstvo duplicitných, resp. veľmi podobných rolí, ktoré robí správu týchto rolí neudržateľnou. Tento aspekt je ešte viac viditeľný pri projektoch, kde musí spolupracovať viac organizácií, pričom každá môže riadiť len časť z používateľov (svojich zamestnancov).
 - Riadenie prístupov zamestnancov len na úrovni „vlastných“ informačných systémov, resp. jednotlivých úradov. Pri tomto prístupe sa predpokladá, že jednotlivé organizácie verejnej správy riadia prístup k informačným systémom využívajúcim služby eGovernmentu spoľahlivo a teda jednotlivé informačné systémy je možné pokladať za dôveryhodné. Na základe tohto predpokladu je potom možné globálne povoliť presne definované interakcie medzi jednotlivými informačnými systémami verejnej správy využívajúcimi služby eGovernmentu.

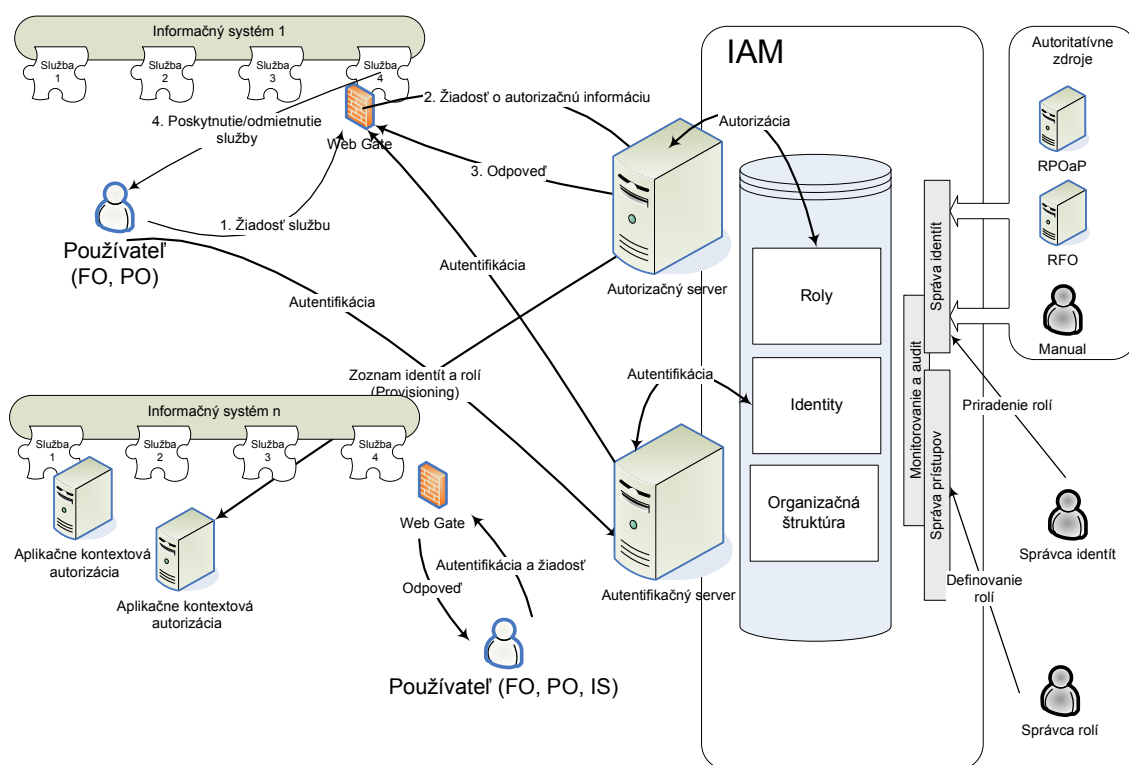
4.1.2.1 Technická architektúra riešenia

V rámci riešenia IAM bude priamo samotnou IAM aplikáciou/produktom zabezpečovaná funkcionálna nasledovných IAM modulov:

- správa identít,
- správa autentifikačných prostriedkov,
- správa prístupových práv (autorizácií),
- provisioning,
- monitoring a audit.

Funkcionalita modulu „Riadenie prístupu“ bude zabezpečovaná spoločne tzv. prístupovými bránami a ďalšou infraštruktúrou riešenia. Jednotlivé prístupové brány budú kontrolovať prístup na úrovni prístupu k webovým stránkam a k webovým službám.

Funkcionalita modulov web gate zabezpečuje výkon riadenia prístupu pre služby/servisy, na ktoré sa vzťahuje. Jedná sa o typ prvku webovej infraštruktúry. Umožňuje poskytnúť alebo odoprieť prístupu používateľovi na základe jeho prístupových práv.



Obrázok 4.2: Technický model riešenia IAM

4.1.2.2 Získavanie informácií o identitách a správa identít

Vytváranie identít sa bude vykonávať na požiadanie a bude riadené automaticky. V rámci riešenia IAM sa predpokladá spojenie s registrom fyzických osôb. Z tohto registra budú pravidelne prenášané informácie o fyzických osobách, ktorým budú následne priradené

prístupové práva role „Občan“ alebo „Cudziniec“ pre občanov inej štátnej príslušnosti s povolením na pobyt. Identity v roli občana sa budú autentifikovať eID kartou, na ktorej budú relevantné autentifikačné certifikáty.

Riadenie identít v roli zamestnancov bude vykonávané manuálne, resp. na základe definovaných pravidiel v relevantnej organizácii, pričom tieto organizácie budú mať možnosť spravovať si práva identít, ktoré pod ne kompetenčne spadajú (zamestnanci), resp. identít, ktoré majú mať do IS týchto organizácií prístup.

Riadenie identít reprezentujúcich informačné systémy VS, ktoré navzájom komunikujú a využívajú služby eGovernmentu bude vykonávané manuálne poverenými administrátormi.

V rámci riešenia IAM bude existovať jednotný repozitár relevantných údajov o identitách, t.j. meno a priezvisko, adresa, telefónne číslo a ďalšie voliteľné údaje, ktoré bude užitočné z hľadiska využívania služieb eGovernmentu registrovať. Tieto údaje budú prístupné definovaným službám a umožnia spravovať ich pre tieto definované služby na jednom mieste. T.j. zmenu napr. telefónneho čísla nebude potrebné vykonať v rámci všetkých používaných služieb, ale bude stačiť zmena v tomto centrálnom repozitári. Taktiež, informácie o napr. adrese občana zo systému IAM bude možné využiť na nasmerovania občana na jemu miestne príslušný orgán pri komunikácii s VS. Informácie o občanovi môžu obsahovať aj ďalšie atribúty, ktoré umožnia napr. personalizáciu informačných portálov, napr. pre zrakovo postihnutých občanov zvýraznením farieb a využitím ďalších prostriedkov, ktoré zvyšujú prístupnosť a použiteľnosť takýchto riešení.

Informácie z repozitára identít bude možné potenciálne využiť na publikovanie zoznamu pracovníkov subjektov verejnej správy, ich organizačnej štruktúry a pod.

Bude definovaná konvencia na pomenovanie a identifikáciu identít v prostredí IAM a eGovernmentu. Táto konvencia umožní jednoznačne identifikovať a autentifikovať identitu či už pri prístupe pomocou certifikátu, mena/hesla a pod. Pre fyzické osoby je navrhované použitie bezvýznamového identifikátora BIFO, ktorý by mal byť aj súčasťou eID karty.

4.1.2.3 *Single Sign-On*

V rámci riešenia IAM sa predpokladá využitie funkcionality Single Sign-On. Táto funkcionality umožňuje identite pristupovať k viacerým službám eGovernmentu poskytovaným cez webové rozhrania, prípadne zverejnené služby, pričom autentifikácia identity je požadovaná len raz – pri využívaní ďalších služieb zabezpečuje prenos autentifikačných informácií infraštruktúra IAM.

Z pohľadu identít pristupujúcich na webové služby (t.j. typicky občania, cudzí štátni príslušníci, niektorí zamestnanci verejnej správy) je potrebné tzv. webové Single Sign-On. Používateľ sa teda v prípade úspešnej autentifikácie voči jednej webovej stránke už nemusí autentifikovať voči ďalším webovým stránkam.

Systémy prevádzkujúce služby eGovernmentu, pre ktoré sa požaduje autentifikácia webového Single Sign-On musia byť integrovateľné so zvoleným autentifikačným riešením. Do úvahy prichádzajú dva spôsoby integrácie:

- **Tesná integrácia** – v tomto prípade eGovernment služba neimplementuje žiadny autentifikačný mechanizmus a autentifikáciu kompletne deleguje na IAM systém. To znamená, že pri prístupe neautentifikovaného používateľa ho služba automaticky presmeruje na autentifikačný server. Informáciu o identite prístupujúceho používateľa služba obdrží prostredníctvom tokenu (napr. HTTP header premenná) vo forme jednoznačného identifikátora (napr. BIFO).
- **Voľná integrácia** – niektoré služby už majú vlastný autentifikačný mechanizmus (napr. niektoré portály verejnej správy). Na dosiahnutie Single Sign-on s takýmto typom služieb je vhodné využiť niektorý zo štandardov na výmenu autentifikačných dát medzi doménami – SAML, WS-Federation, Liberty Alliance ID-FF. Používateľ sa potom môže prihlásiť prostredníctvom centrálného autentifikačného servera a využívať aj služby, ktoré implementujú vlastný autentifikačný mechanizmus, bez ďalšieho prihlasovania.
- Pri použití viacerých autentifikačných mechanizmov je potrebné zabezpečiť dodatočnú silnejšiu autentifikáciu pri prístupe k systémom, ktoré ju vyžadujú, aj keď bol už používateľ autentifikovaný slabšími autentifikačnými mechanizmami.

4.1.2.4 Provisioning a poskytovanie informácií o prístupových právach (roliach)

Pre riadené služby/aplikácie/systémy sú k dispozícii nasledovné spôsoby zisťovania informácií o autorizáciách a ich vynucovania:

- **Provisioning do koncových systémov** – IAM systém ako jediný systém automaticky udržiava zoznam identít aj s ich prístupovými právami v koncovom systéme (aplikácia, služba, databáza). Na základe tohto zoznamu potom aplikácia/služba môže autonómne riadiť prístup k svojim komponentom. Výhodou tohto riešenia je relatívna nezávislosť od aplikácie IAM. Odpadá potreba riadenia prístupov v IAM manažovaných systémoch inými subjektami alebo systémami, čím sa znižujú napr. požiadavky na množstvo potrebných licencií.
- **Riadenie prístupu na úrovni komponentu Web gate** – v tomto prípade je pred samotnú službu nainštalovaný komponent Web gate, ktorý je súčasťou IAM aplikácie a riadi prístup k samotnej službe na základe identity a jej privilégii. Komponent Web gate sa pre každý prístup identity dotazuje na autorizačný server systému IAM, ktorý komponentu Web gate poskytuje informácie o tom, či má alebo nemá poskytnúť prístup k danej službe.
- **Riadenie prístupu na úrovni služby eGovernmentu** – pri tomto riešení pri volaní služby eGovernmentu daná služba prostredníctvom webových služieb a služieb aplikácie IAM o relevantné autorizačné informácie (napr. zoznam rolí danej identity pre volanú službu, a pod.), na základe ktorých služba eGovernmentu určí, či prístup umožní alebo zamietne. V tomto prípade je pre fungovanie služby potrebné funkčné spojenie na autorizačný server IAM – bez tohto spojenia nie je možné overiť prístupové práva pre volanú službu, t.j. nie je možné službu poskytnúť. V tomto prípade je potrebná úprava relevantných služieb tak, aby umožňovali vyžiadať si potrebné informácie z IAM aplikácie a vedeli ich spracovať.

4.1.2.5 Splnomocnenie iného používateľa

Riešenie IAM bude podporovať aj funkcionality splnomocnenia tretej osoby na vykonanie špecifických úkonov v mene splnomocňujúcej osoby. Toto prenesenie identity umožní nasledujúce scenáre:

- pracovníkovi kontaktného centra alebo integrovaného obslužného miesta používať e-služby portálu verejnej správy v mene klienta, ktorému sprostredkováva poskytnutie danej e-služby
- občanovi splnomocniť iného občana na vykonanie špecifického úkonu alebo množiny úkonov
- občanovi splnomocniť informačný systém alebo právnickú osobu na vykonanie špecifického úkonu alebo množiny úkonov.

Parametre splnomocnenia môžu byť:

- splnomocnenie na určitý okruh služieb,
- splnomocnenie na obmedzený čas, po ktorom splnomocnenie je automaticky zrušené.

Vyhodnocovanie autorizácie na prístup k službe eGovernmentu musí byť schopné vyhodnotiť vyššie uvedené scenáre delegovania a ich kombinácie až do 3 úrovne:

- splnomocnenie identity inou identitou,
- splnomocnenie fyzickej osoby právnickou osobou (potenciálne vyhodnotenie kombinované pomocou mechanizmov dostupných v certifikátoch a zaručenom elektronickom podpise),
- splnomocnenie právnickej osoby fyzickou osobou (napr. poverenie, že systém môže vykonávať za fyzickú osobu špecifikované úkony v rámci služieb),
- 3- úrovňové splnomocnenie - splnomocnenie fyzickej osoby pre právnickú osobu (napr. zamestnávateľa), ktorý splnomocní na výkon špecifikovanej služby (alebo množiny služieb) fyzickú osobu a tá môže splnomocniť (napríklad z dôvodu zastupovania) ešte ďalšiu fyzickú osobu.

Zároveň je možné splnomocniť zamestnanca na správu špecifickej časti systému. Táto funkcionality je vo veľkej miere dostupná v existujúcich IAM produktoch, známa skôr pod názvom delegovanie. V závislosti od finálnej architektúry riešenia IAM a od zvoleného dodávateľa a jeho riešenia sa bude líšiť miera úprav potrebných pre dosiahnutie špecifikovanej funkcionality splnomocňovania a ich vyhodnocovania pri autorizácii.

4.2 Zlepšenie

Nasadenie centralizovaného IAM riešenie prinesie tieto podstatné výhody:

- Jednotné a centralizované riadenie prístupu ku všetkým podporovaným publikovaným službám eGovernmentu.
- Zníženie nákladov a potrebného času na vytvorenie/modifikáciu/zablokovanie prístupu používateľa vďaka využitiu automatizovaného riešenia.
- Zaistenie konzistentnej úrovne bezpečnosti na základe systematického vynucovania definovaných bezpečnostných politík pre všetky integrované koncové systémy a skupiny používateľov.
- Zlepšenie, resp. zavedenie možností pokročilého monitorovania a auditovania činnosti samotného IAM riešenia a jeho používateľov, zlepšenie možnosti online detekcie prípadných podvodných aktivít a ich eliminácie pod.

4.3 Definície služieb

Súčasťou rozvojového zámeru vybudovania infraštruktúry pre riešenie IAM bude aj zavedenie minimálne nasledovných skupín elektronických služieb poskytovaných riešením IAM:

- Podporné služby – Používateľské a aplikačné služby:
 - Poskytnutie zoznamu rolí identity z IAM pre zadanú službu – Príloha A.1.1.1,
 - Poskytnutie informácie o priradení roly identite – Príloha A.1.1.2,
 - Poskytnutie zoznamu identít s prístupom ku službe – Príloha A.1.1.3,
 - Poskytnutie zoznamu rolí informačného systému – Príloha A.1.1.4,
 - Zápis identity do systému IAM – Príloha A.1.1.5,
 - Zmena údajov identity v systéme IAM – Príloha A.1.1.6,
 - Zneplatnenie identity v systéme IAM – Príloha A.1.1.7,
 - Zápis roly do katalógu rolí systému IAM – Príloha A.1.1.8
 - Zmena údajov roly v katalógu rolí systému IAM – Príloha A.1.1.9,
 - Zneplatnenie roly v katalógu rolí systému IAM – Príloha A.1.1.10,
 - Pridanie roly identite v systéme IAM – Príloha A.1.1.11,
 - Odobranie roly identite v systéme IAM – Príloha A.1.1.12,
 - Pridanie autentifikačného prostriedku identite v systéme IAM – Príloha A.1.1.13,

- Odobranie autentifikačného prostriedku (AP) identity v systéme IAM – Príloha A.1.1.14,
- Poskytnutie autentifikačného rozhodnutia zo systému IAM – Príloha A.1.1.15,
- Generovanie nového hesla/reset hesla – Príloha A.1.1.16,
- Splnomocnenie inej osoby v systéme IAM – Príloha A.1.1.17.
- Podporné služby – Používateľské služby:
 - Zápis autentifikačného prostriedku do katalógu autentifikačných prostriedkov systému IAM – Príloha A.1.2.1,
 - Zrušenie autentifikačného prostriedku z katalógu autentifikačných prostriedkov systému IAM – Príloha A.1.2.2,
 - Poskytnutie profilu identity v systéme IAM – Príloha A.1.2.3.

Podrobná špecifikácia predpokladaných elektronických služieb IAM je uvedená v Prílohe A tejto štúdie. Za účelom vytvorenia a koordinovania komplexného modelu eGovernmentu budú tieto služby ďalej namodelované v prostredí nástroja pre katalogizáciu a hierarchizáciu elektronických služieb.

4.4 Uskutočniteľnosť a náklady

4.4.1 Dopady na technické a softwarové vybavenie

V rámci implementácie riešenia IAM bude potrebné zabezpečiť nasledovné zmeny:

- Inštalácia a konfigurácia hardvéru a aplikačného programového vybavenia samotného IAM systému,
- Prispôsobenie koncových spravovaných systémov na komunikáciu s IAM systémom,
- Prispôsobenie systémov, z ktorých IAM získava informácie (napr. RFO, RPO),
- Prispôsobenie a vývoj systémov na podporu SSO a vytvorenie autentifikačného SSO servera v rámci IAM,
- Implementácia Access servera a prispôsobenie a vývoj systémov v súlade s autorizačnou architektúrou Access servera.

4.4.2 Legislatívne dopady

To, čo pod pojmom Identity and Access Management uvádza Národná koncepcia informatizácie verejnej správy, má dve strany mince: jednoduchší a operatívnejší prístup používateľov do portálov verejnej správy, ale zároveň zvýšenie úrovne ochrany údajov. Ak chceme vytvoriť nový mechanizmus ochrany údajov v databázach, ktoré spravujú verejnoprávne orgány a organizácie, tak je treba najskôr vymedziť, čo chceme chrániť.

Súčasná úroveň ochrany údajov v databázach verejnoprávných inštitúcií je už nepostačujúca. Je vymedzená predovšetkým zákonom o ochrane utajovaných skutočností (č. 215/2004 Z.z. v znení neskorších predpisov), zákonom o ochrane osobných údajov (č. 428/2002 Z.z. v znení neskorších predpisov) a Obchodným zákonníkom (č. 513/1991 Zb. v znení neskorších predpisov), ako i dlhoročnou administratívnou tradíciou. Podľa tejto administratívnej tradície do citlivých registrov a databáz môžu vstupovať len príslušní pracovníci inštitúcií, ktoré konkrétny register alebo databázu spravujú. Osobitne zákon o slobodnom prístupe k informáciám, ktorý založil režim „čo nie je osobitným zákonom utajené, musí sa zverejniť, alebo poskytnúť žiadateľovi“, vytvoril zásadne novú situáciu.

Kvalitatívne nový prvok pri manažmente registrov a databáz v správe orgánov verejnej moci a ďalších verejnoprávných inštitúcií vytvára informatizácia spoločnosti, osobitne možnosť hromadného prístupu cez internet a prepojenie týchto databáz. Vzniká tak reálna možnosť oveľa rýchlejšieho vybavovania žiadostí a podaní občanov, oveľa kvalitnejší výkon štátnej správy, ale aj oveľa väčšie riziko zneužitia uchovávaných údajov.

I keby sa základné zásady administrovania nemenili, nové prvky, ktoré do týchto činností už v súčasnosti vnáša proces informatizácie spoločnosti, je treba reflektovať i v existujúcom právnom poriadku. Osobitne sa to týka zákona o slobodnom prístupe k informáciám, ktorý by mal podrobnejšie upraviť základné zásady pre elektronickú komunikáciu žiadateľa s úradnou inštitúciou.

Nový systém označený pojmom Identity and Access Management však nepochybne predpokladá i určitý zásah do spôsobu administrácie verejnej správy. Národná koncepcia ale bližšie nehovorí o tom, ako tým navrhuje súčasný spôsob výkonu verejnej správy zmeniť.

Ako príklad analogickej kvalitatívnej zmeny vyvolanej elektronizáciou verejnej správy možno uviesť navrhovaný systém manažmentu identifikácie a prístupových oprávnení pri vstupovaní do základných registrov v Českej republike. Tento príklad je pre nás zaujímavý aj preto, lebo vychádza zo spoločného právneho základu a spoločnej administratívnej tradície. V Českej republike sa navrhuje, aby zákon o základných registroch zriadil osobitný základný register práv a povinností, ktorý bude okrem iného zabezpečovať manažment prístupových oprávnení pre pracovníkov verejnej správy, vstupujúcich do základných registrov. Okrem toho vytvára sústavu identifikátorov fyzických osôb, ktorá zabezpečí, aby sa pracovník verejnej správy, vybavujúci ich žiadosť, dostal len k tým údajom, ktoré sú nevyhnutné. Správu týchto identifikátorov a ich transformáciu a generovanie bude zabezpečovať osobitný úrad. Navrhuje sa, aby to bol Úrad na ochranu osobných údajov. Tento systém manažmentu prístupových práv a identifikácie zachováva tradíciu, podľa ktorej sa k citlivým údajom v základných registroch dostanú len pracovníci verejnej správy, teda nie priamo žiadatelia, avšak len ak budú mať prístupové práva, a len k tým údajom, ktoré bude žiadateľ na vybavenie svojej žiadosti potrebovať. Systém teda zvyšuje úroveň ochrany údajov pred zneužitím zo strany úradníkov, ale zároveň zvyšuje

operatívnosť vybavovania žiadostí: bude možné na jednom mieste vybaviť žiadosť bez toho, aby občan musel chodiť po úradoch, ktoré mu na vybavenie jeho žiadosti musia dnes poskytovať potrebné podklady.

Národná koncepcia sa pri používaní pojmu Identity and Access Management nevyjadřila podrobnejšie. Výslovne sa v nej uvádza, že jej ide o vstup do portálov verejnej správy, kam občan vstupuje priamo. Pri týchto vstupoch platí všeobecný režim ochrany údajov a aj povinností orgánov verejnej správy. Vytvorenie jednotnej sústavy správy identít a prístupových oprávnení by len pre vstup do portálov verejnoprávných inštitúcií by zrejme nebol potrebný. Osobitne ak sa bude zvyšovať význam Ústredného portálu verejnej správy.

Súčasťou NKIVS je aj vstupovanie do základných registrov a ďalších informačných systémov verejnej správy. A tu je nesmierne dôležité, či v prípade vstupu do týchto databáz, počítame so sprostredkovateľskou úlohou pracovníkov verejnej správy, alebo azda máme na mysli, že do týchto databáz budú občania cez internet vstupovať priamo. Ak by mali vstupovať priamo, tak to by bola dramatická zmena tradície výkonu verejnej správy a obrovské bezpečnostné riziko. Ale samozrejme, pre vybavovanie agendy, by to bolo najoperatívnejšie. V prípade priameho vstupovania občanov do základných registrov, by bolo potrebné riešiť otázku manažmentu prístupových práv pre každého občana, vstupujúceho do týchto databáz, ale vystačili by sme si s jedným zabezpečeným identifikátorom pre všetky registre a databázy. Je potrebné upozorniť, že nie je známy štát, v ktorom by sa prístup do základných databáz spravovaných orgánmi verejnej moci takto otvoril.

Z toho, ako Národná koncepcia hovorí o sústave identifikátorov, sa však dá vyvodiť, že pre vstup do základných registrov a ďalších databáz v správe verejnoprávných inštitúcií bude naďalej platiť zásada sprostredkovania cez príslušných pracovníkov. V takomto prípade má zmysel hovoriť o manažmente prístupových oprávnení týchto pracovníkov (nie žiadateľov) a zároveň o manažmente systému identifikátorov fyzických osôb (teda žiadateľov). Išlo by o obdobný systém, ako sa vytvára v Českej republike.

Podľa toho, aký model si zvolíme, bude potrebné upraviť náš právny poriadok. V každom prípade to bude vyžadovať základnú úpravu, buď v zákone o základných registroch, alebo v osobitnom zákone o správe identít a prístupových práv. Táto základná úprava bude obsahovať ustanovenia o prístupových právach k údajom vedených v základných registroch a ďalších databázach, otvorený katalóg agend, ktoré sa budú dať touto formou vybavovať, ako i základné ustanovenia o správe systému identifikácie fyzických osôb, vrátane inštitucionálneho zabezpečenia týchto činností.

Jednotný mechanizmus správy identít a prístupových práv sa bude musieť premietnuť i do niektorých jestvujúcich právnych úprav. Bude potrebné ho premietnuť do zákona o informačných systémoch verejnej správy, bolo by užitočné, aby sa premietol i do zákona o slobodnom prístupe k informáciám, a bude potrebné vyriešiť i možnosť elektronickej komunikácie medzi žiadateľom a vybavujúcim pracovníkom v zákone o elektronickej podpise. Nové ustanovenia sa budú dotýkať aj jestvujúceho systému ochrany údajov, ktoré bude potrebné premietnuť i do zákona o ochrane utajovaných skutočností a zákona o ochrane osobných údajov.

Úprava Identity and Access Managementu sa bude musieť tiež zohľadniť v ďalších navrhovaných právnych úpravách, osobitne v zákone, ktorý vytvorí elektronickú ID kartu, v právnej úprave systému identifikácie občanov pri prístupe do základných registrov a v osobitných zákonoch o jednotlivých základných registroch a ďalších databázach v správe verejnoprávných orgánov a organizácií.

Takto vytvorený mechanizmus správy identít a prístupových práv by sa dal využiť i pre vstupovanie do ústredného portálu verejnej správy, a prípadne do osobitných portálov verejnoprávných inštitúcií priamo z domu, cez internet. V zákone o elektronickom podpise by však bolo potrebné vyriešiť otázku transformácie identifikácie prostredníctvom elektronického podpisu na systém identifikácie v registroch a databázach verejnej správy.

4.4.3 Bezpečnostné dopady

V rámci projektu je potrebné implementovať kontrolné mechanizmy informačnej bezpečnosti.

Táto problematika bude riešená v rámci prípravy projektu ako súčasť prípravy žiadosti o nenávratný finančný príspevok.

4.4.4 Dopady na lokalitu a stavebnú činnosť

V rámci projektu sa nepredpokladajú významnejšie stavebné úpravy súvisiace s osadením technológií, alebo prístupnením služieb na mieste prevádzky systému IAM.

4.4.5 Ostatné dopady

Analýza ostatných dopadov projektového zámeru nasadenia IS IAM je popísaná v nasledujúcich častiach.

4.4.5.1 Organizačné dopady

- Potreba zavedenia funkcií správcov na riadenie prístupových práv pre identity za jednotlivé organizácie verejnej a štátnej správy a riadenie rolí pre informačné systémy v kompetencii jednotlivých orgánov.
- V prípade riadenia práv na úrovni jednotlivých zamestnancov odporúčame zladenie architektúry personálnych systémov jednotlivých organizácií tak, aby poskytovali jednotné rozhranie o organizačnej štruktúre a zamestnancoch pre IAM.

4.4.5.2 Prevádzkové dopady

- Náklady na výkon riadenia identít a prístupových práv na jednotlivých orgánoch.
- Náklady na zabezpečenie komunikačnej premávky medzi:

- zdrojovými systémami a IAM,
- IAM a koncovými systémami,
- Online komunikácia medzi systémami IAM a PKI vrátane používania kariet eID.
- V prípade zlyhania IAM ako centrálnej infraštruktúry nebudú dostupné služby závisiace na IAM. Tieto služby nebudú môcť vykonávať svoje ďalšie funkcie.

4.4.5.3 Dopady na vývoj riešenia

- Všetky ostatné ISVS musia byť vyvíjané tak, aby podporovali autentifikačný server (na úrovni WebSSO) implementovaný v rámci IAM, či už prostredníctvom delegovania autentifikácie (tesná väzba), alebo prostredníctvom federácie (voľná väzba).
- Zvolené ISVS musia byť vyvíjané tak, aby mali rozhrania podporované access serverom implementovaným v rámci IAM.

4.4.5.4 Dopady na nasadenia riešenia

- Je potrebné zabezpečiť z dlhodobého pohľadu schopnosť implementátora IAM riešenia aktualizovania a údržby IAM systému.

4.4.5.5 Dopady na marketingové požiadavky

Dopady na marketingové požiadavky nie sú špecificky pre IAM predpokladané, všeobecné marketingové požiadavky budú celkovo špecifikované v Štúdii uskutočniteľnosti základný prístupový bod – ÚPVS.

4.4.6 Cena riešenia

Pre odhad minimálnych nákladov na vytvorenie základného komponentu Identity and access management sme použili metodiku UCP (Use-Case Points).

Na základe odhadu náročnosti vývoja aplikácie predstavuje predpokladaný časový náklad na implementáciu 19 883 človekohodín. Tento údaj je potrebné považovať za spodnú hranicu investičných nákladov do vývoja softvérového riešenia. Odvodenie vstupných parametrov odhadu prácnosti je uvedené v Prílohe A.1.2.

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 7,1 mil. Eur s DPH.

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

4.5 Ekonomická analýza

Systém IAM predstavuje back-endový infraštruktúrny systém poskytujúci služby ostatným systémom. Poskytované služby IAM nebudú prístupné priamo občanom SR. Z tohto pohľadu nie sú očakávané priame finančné príjmy plynúce z nasadenia IAM.

Nefinančné prínosy IAM sú:

- Zjednodušenie a zprehľadnenie riadenia práv v prostredí všetkých ISVS – jediný entita, ktorá bude riadiť prístupy v spravovaných systémoch bude IAM,
- zjednodušenie architektúry všetkých ISVS vzhľadom k výkonu potrebných autentifikácie a autorizácie.

Táto čiastková štúdia ďalej predpokladá, že ostatné aspekty ekonomickej analýzy budú riešené v rámci prípravy projektu.

4.5.1 Analýza rizík

V ďalšom texte sú popísané riziká, ktoré sa vzťahujú k samotnému projektu t.j. vývoju riešenia, a jeho implementácii.

Ohodnotenie rizík je vykonané v stupnici ECHO, ktorá je popísaná v nasledujúcej tabuľke.

Skratka	Názov stupne	Význam
E	Exposure	Vysoké riziko – potreba okamžitého riešenia
C	Concern	Stredné riziko (nepriama hrozba) – protiopatrenie by malo byť založené na aktuálnom hodnotení konkrétneho rizika
H	House Keeping	Nízke riziko
O	OK	Minimálne (akceptovateľné) riziko

Tabuľka 2: Stupnica hodnotenia ECHO

4.5.1.1 Predpoklady

V čase vypracúvania tejto štúdie neboli definované bezpečnostné opatrenia pre celú infraštruktúru, v ktorej budú prvky IAM operovať.

Predpoklad 1: Efektívne riadenie bezpečnosti

Pre účely tejto štúdie predpokladáme, že systém riadenia informačnej bezpečnosti v rámci celej infraštruktúry pre podporu IAM, bude adekvátny (napríklad v zmysle certifikácie voči ISO/IEC 27001).

Predpoklad 2: Použitie bezpečných kryptografických algoritmov pre autentifikáciu a šifrovanie

Pre implementáciu sú zvolené algoritmy, postupy a kontrolné opatrenia podľa usmernení platných pre oblasť zaručeného elektronického podpisu podľa NBU SR a rozšírené aj na autentifikačné aspekty potrebné pre účely autentifikácie v tejto štúdii.

4.5.1.2 Legislatívne riziko

Legislatívne riziko spočíva v časovom nesúlade priebehu nutných legislatívnych zmien a faktického priebehu projektu. Môže tak vzniknúť situácia, keď bude riešenie implementované, no pre jeho spustenie nebude právna opora. Dopadom je oddiaľovanie možnosti využívania benefitov eGovernmentu pre jeho prijímateľov.

Súvisiace riziká: finančné, politické

Hodnotenie

E – bez potrebnej legislatívy nie je možné nasadenie riešenia. Časovo neskoordinované riešenie legislatívnych otázok spôsobí oddialenie možnosti nasadenia a možné nesplnenie časových cieľov.

Odporúčané kroky

- a) Na základe tejto štúdie iniciovať zmenu na popisovaných legislatívnych normách
- b) Zahájiť práce na zmenách príslušných zákonov

4.5.1.3 Dodávateľské riziko

Riziko nesplnenia záväzku dodávateľa dodať dielo v súlade s požiadavkami zadávateľa a zmluvou.

Súvisiace riziká: finančné a organizačné

Hodnotenie

H – nízky stupeň odráža predpoklad, že MF SR je skúseným a vyspelým odberateľom a má skúsenosti s projektmi obdobného rozsahu

Odporúčané kroky

Zmluvná požiadavka aplikácie preverenej projektovej metodiky na strane dodávateľa

4.5.1.4 Technické riziko

Riziko technického nesúladu riešenia a súčasnej infraštruktúry a/alebo zlyhaní niektorého informačného aktíva.

Súvisiace riziká: bezpečnostné a funkčné – prerušenie poskytovania služby, strata lebo nedostupnosť dát

Hodnotenie

E – bez definovania celkovej architektúry služieb eGovernmentu, modelu jeho financovania vo vzťahu k občanom nie je možné vytvoriť z tejto štúdie presný design a vybrať vhodnú technológiu.

Odporúčané kroky

Definovať celkovú architektúru služieb eGovernmentu, model toku financií od občanov smerom k službám eGovernmentu, ktorú sú spoločné pre všetky prvky eGovernmentu.

4.5.1.5 Časové riziko

Riziko časovej synchronizácie súvisiacich projektov v rôznych rezortoch.

Hodnotenie

H – proces informatizácie verejnej správy je koordinovaným procesom.

Odporúčané kroky

Dôsledne plánovať časový harmonogram vzájomne závislých projektov.

4.5.1.6 Bezpečnostné riziko

Riziko neoprávneného prístupu, zneužitia alebo poškodenia dát.

Hodnotenie

H – nízky stupeň vychádza zo znalosti autentizačných mechanizmov aplikovaných pre systémy štátnej správy. Nezohľadňuje riziko primárnych dátových zdrojov ani riziká bezpečnosti komunikácie.

Odporúčané kroky

Návrh riešenia bezpečnosti informačného systému v kontexte preneseného výkonu štátnej správy na samosprávu.

Záver

Navrhnuté riešenie neobsahuje silné interné rizikové vplyvy. Jediným podstatným rizikovým faktorom je legislatívne riziko. Toto riziko je však externou hrozbou a prípadný dodávateľ nemá možnosť ho priamo znížiť. Vlastníkom rizika je tak v plnej miere MV.

4.6 Návrh projektového zámeru

4.6.1 Názov projektu

Národný projekt IAM.

4.6.2 Obsahová náplň projektu

Riešenie IAM pre publikované služby bude budované ako základný nástroj pre riadenie prístupu k jednotlivým publikovaným službám eGovernmentu. Riešenie bude pokrývať riadenie prístupov fyzických osôb – občanov a zamestnancov SS a VS, právnických osôb a informačných systémov ku službám vytváraným v prostredí eGovernmentu.

Nevyhnutnou súčasťou projektu riešenia IAM je zabezpečenie komunikačného rozhrania pre jednotlivé služby eGovernmentu, ktoré budú s riešením IAM integrované. Je potrebné zabezpečiť, aby dané služby vedeli využívať špecifikované služby, ktoré poskytuje IAM riešenie pre riadenie prístupu k integrovaným službám.

V rámci projektu implementácie riešenia IAM bude potrebné zabezpečiť nasledovné:

- Implementovať a nasadiť zvolený IAM produkt vybraného dodávateľa,
- Implementovať a nasadiť ostatné potrebné prvky infraštruktúry v závislosti od finálneho konceptu a vybraného produktu, napr. autentifikačný server, PKI a pod.
- Integrovať koncové systémy (služby) do systému IAM, teda zabezpečiť ich bezproblémovú komunikáciu so službami riešenia IAM,
- Definovať roly reprezentujúce jednotlivé prístupové práva pre jednotlivé služby,
- Definovať pravidlá, na základe ktorých budú vytvorené roly pridelované jednotlivých používateľom.

4.6.3 Ciele projektu

Ciele projektu sú nasledovné:

- Vybudovanie hardvérovej infraštruktúry pre IAM, vývoj a nasadenie softvérových prvkov IAM na zabezpečenie požadovanej funkčnosti,
- Centralizovať správu identít a prístupových práv v jednom systéme poskytujúcom službu ostatným ISVS,
- Implementovať prepojenie IAM so zdrojovými systémami,

- Implementovať prepojenie IAM s riadenými systémami (implementácia rozhrania na poskytovanie údajov pre riadené systémy) a aktualizovať riadené systémy,
- Definovať požiadavky na zmenu organizačných procesov zabezpečujúcich kontinuálny chod IAM.

4.6.4 Výstupy projektu

Kľúčové výstupy projektu nasadenia riešenia sú zhrnuté v nasledujúcich bodoch:

- nasadenie riešenia IAM,
- sprístupnenie služieb IAM ostatným službám eGovernmentu,
- nastavenie technologického riešenia a sprievodných procesov s cieľom umožniť prechod z manuálneho riadenia identít a práv na ich automatickú správu v prostredí IAM.

4.6.5 Súvisiace projekty

Nasadzovanie IS IAM je potrebné koordinovať najmä s nasledujúcimi plánovanými alebo predpokladanými projektami:

- eID karta a PKI,
- zabezpečenie sieťovej komunikácie IAM s ostatnými systémami,
- všetky ostatné služby eGovernmentu, ktoré budú využívať služby IAM,
- ÚPVS (všeobecnejšie celý eGovernment) a všetky spoločné moduly,
- register fyzických osôb,
- register právnických osôb,
- Register inštitúcií verejnej správy,
- Portál zamestnancov verejnej správy.

4.6.6 Príprava projektu

- Definovanie presných požiadaviek na IAM riešenie.
- Zverejnenie výzvy.
- Výber implementátora riešenia – odporúčaný postup je:

- príprava detailného designu riešenia podľa architektúry a organizácie súvisiacich systémov,
- pilotné verifikovanie konceptu,
- postupná integrácia systémov VS a identít do IAM riešenia.

4.6.7 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 všetkých elektronických služieb riešenia IAM:

- Služba je implementovaná základným komponentom architektúry eGovernmentu podľa dokumentu NKIVS.
- Povinné osoby garantujúce službu:
 - správca: Ministerstvo financií Slovenskej republiky,
 - prevádzkovateľ: Národná agentúra pre sieťové a elektronické služby.
- Zdrojové elektronické služby modulov ISVS, na ktorých je popisovaná služba závislá (t.j. bez volania ktorých nie je možné dodať spoľahlivý výsledok volania tejto služby) sú služby modulov:
 - základné identifikátory / identifikátor fyzických osôb (IFO),
 - základné registre / register fyzických osôb a register právnických osôb.
 - spoločné moduly ÚPVS / eForm modul pre odovzdávanie vstupov a výstupov služieb IAM,
 - Poznámka: IAM bude ďalej komunikovať v rámci identifikácie a autentifikácie FO komunikovať s eID kartou.
- Klasifikácia služby/Zaradenie služby/Názov agendy: Všetky
- Klasifikácia služby/Zaradenie služby/Názov úseku správy: Všetky
- 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.),
 - miera spokojnosti používateľov (napr. kvantifikácia na stupnici diskretných hodnôt),
 - 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).

A.1 Podporné

A.1.1 Používateľské a aplikačné služby

A.1.1.1 Poskytnutie zoznamu rolí identity z IAM pre zadanú službu

Položka	Hodnota
Základné údaje	
Názov služby	Poskytnutie zoznamu rolí identity z IAM pre zadanú službu
Popis služby	<ul style="list-style-type: none"> • Poskytnutie zoznamu rolí, ktoré má špecifikovaná identita pridelené v rámci špecifikovaného cieľového systému - autorizácia identity. • Služba si prostredníctvom tejto IAM služby overí, či používateľ služby má právo použiť volanú službu. Používateľom volaná služba získa zoznam rolí, ktoré sú pridelené používateľovi. Na základe tohto zoznamu a internej logiky volanej služby, volaná služba rozhodne o úrovni prístupu používateľa.
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> • ISVS organizácie VS (G2G) – primárny používateľ, • organizácia VS (G2G),
Komunikačné kanály	<ul style="list-style-type: none"> • webové služby, • www.
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, • identifikácia identity, pre ktorú je požadovaný zoznam • špecifikácia IS, pre ktorý má byť poskytnutý zoznam rolí identity
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> • zoznam rolí pridelených identite v špecifikovanom systéme • odmietnutie poskytnutia zoznamu

A.1.1.2 Poskytnutie informácie o priradení roly identite

Položka	Hodnota
Základné údaje	
Názov služby	Poskytnutie informácie o priradení roly identite
Popis služby	<p>Poskytnutie o informácie (ano/ nie) o tom, či špecifikovaná identita má alebo nemá priradenú špecifikovanú rolu - autorizácia identity.</p> <p>Služba si prostredníctvom tejto IAM služby overí, či používateľ služby má právo použiť volanú službu. Služba IAM poskytne jednoznačnú odpoveď, na základe ktorej volaná služba povolí alebo zamietne prístup k svojej funkcionalite.</p>

Položka	Hodnota
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G), občan (G2C), podnikateľ (G2B).
Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
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, identifikácia identity, o ktorej je požadovaná informácia, špecifikácia role, ktorá sa má overiť.
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> odpoveď ano/nie, odmietnutie poskytnutia informácie.

A.1.1.3 Poskytnutie zoznamu identít s prístupom ku službe

Položka	Hodnota
Základné údaje	
Názov služby	Poskytnutie zoznamu identít s prístupom ku službe
Popis služby	Poskytnutie zoznamu identít, ktoré majú prístup (t.j. priradenú minimálne jednu rolu) do špecifikovaného systému. Táto IAM služba vygeneruje zoznam zoznam identít a rolí, ktoré majú prístup k špecifikovanej službe. Služba bude využívaná prevažne pre auditné účely a správu rolí.
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G).
Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
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, identifikácia informačného systému, pre ktorý je požadovaný zoznam identít
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> zoznam identít s prístupom do špecifikovaného IS odmietnutie poskytnutia zoznamu

A.1.1.4 Poskytnutie zoznamu rolí informačného systému

Položka	Hodnota
Základné údaje	
Názov služby	Poskytnutie zoznamu rolí informačného systému
Popis služby	Poskytnutie zoznamu rolí, ktoré obsahuje/poskytuje na priradenie špecifikovaný IS. Klient služby na základe volania tejto IAM služby má možnosť zistiť, ktoré roly súvisia so špecifikovanou službou.
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G).
Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
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, identifikácia IS, pre ktorý je požadovaný zoznam rolí
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> zoznam rolí, ktoré IS obsahuje odmietnutie poskytnutia zoznamu

A.1.1.5 Zápis identity do systému IAM

Položka	Hodnota
Základné údaje	
Názov služby	Zápis identity do systému IAM
Popis služby	Vytvorenie identity v systéme IAM - jednotné vytvorenie používateľského účtu - registrácia. Služba zabezpečí vytvorenie "identity" používateľa v systéme IAM na základe vstupných údajov. Tejto identite budú neskôr priradené relevantné role v závislosti od jej právomocí.
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G).
Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
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, zoznam údajov potrebných pre vytvorenie novej identity (BIFO, meno, priezvisko...)

Položka	Hodnota
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> potvrdenie zápisu identity odmietnutie zápisu identity a zdôvodnenie

A.1.1.6 Zmena údajov identity v systéme IAM

Položka	Hodnota
Základné údaje	
Názov služby	Zmena údajov identity v systéme IAM
Popis služby	Zmena údajov/parametrov identity v systéme IAM - Jednotná správa údajov používateľského účtu – personalizácia.
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G), občan (G2C), podnikateľ (G2B).
Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
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, zoznam údajov potrebných pre vytvorenie novej identity (BIFO, meno, priezvisko...)
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> potvrdenie zápisu identity odmietnutie zápisu identity a zdôvodnenie

A.1.1.7 Zneplatnenie identity v systéme IAM

Položka	Hodnota
Základné údaje	
Názov služby	Zneplatnenie identity v systéme IAM
Popis služby	Zneplatnenie/zrušenie identity v systéme IAM. Táto služba zabezpečí zablokovanie identity v systéme IAM - daná identita nebude môcť využívať elektronické služby, ktoré závisia na IAM.
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G).
Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
Stav implementácie	<ul style="list-style-type: none"> špecifikácia

Položka	Hodnota
Atribúty služby	
Vstup (parametre služby – špecifikácia požiadaviek používateľa na službu)	<ul style="list-style-type: none"> identifikácia používateľa služby, identifikátor identity na zrušenie
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> potvrdenie zrušenia identity odmietnutie zrušenia identity a zdôvodnenie

A.1.1.8 Zápis roly do katalógu rolí systému IAM

Položka	Hodnota
Základné údaje	
Názov služby	Zápis roly do katalógu rolí systému IAM
Popis služby	Vytvorenie/pridanie roly do katalógu rolí v systéme IAM. Služba zabezpečí vytvorenie roly v katalógu rolí. Rola zodpovedá definovaným prístupovým práva k špecifikovaným službám. Aby bolo možné rolu neskôr pridelit' inej identite, musí byť najprv vytvorená v katalógu rolí.
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G).
Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
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, zoznam údajov potrebných pre vytvorenie novej roly (ID, názov, popis, identifikátor koncového systému, zoznam oprávnení na koncovom systéme, ktoré patria do roly)
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> potvrdenie zápisu roly odmietnutie zápisu roly a zdôvodnenie

A.1.1.9 Zmena údajov roly v katalógu rolí systému IAM

Položka	Hodnota
Základné údaje	
Názov služby	Zmena údajov roly v katalógu rolí systému IAM
Popis služby	Služba zabezpečí zmenu údajov existujúcej roly v katalógu rolí systému IAM.
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G).
Komunikačné kanály	<ul style="list-style-type: none"> webové služby,

Položka	Hodnota
	<ul style="list-style-type: none"> • www.
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, • zoznam údajov potrebných pre aktualizáciu údajov existujúcej roly (ID, názov, popis, identifikátor koncového systému, zoznam oprávnení na koncovom systéme, ktoré patria do roly).
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> • potvrdenie zápisu roly, • odmietnutie zápisu roly a zdôvodnenie.

A.1.1.10 Zneplatnenie roly v katalógu rolí systému IAM

Položka	Hodnota
Základné údaje	
Názov služby	Zneplatnenie roly v katalógu rolí systému IAM
Popis služby	Služba zabezpečí zneplatnenie roly v katalógu rolí v systéme IAM. Interná logika služby musí zabezpečiť konzistenciu relácií role <-> identity, t.j. zneplatniť len rolu ktorá nie je v žiadnej relácii s niektorou identitou alebo zneplatniť aj identity naviazané na zneplatňovanú rolu.
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> • ISVS organizácie VS (G2G), • organizácia VS (G2G).
Komunikačné kanály	<ul style="list-style-type: none"> • webové služby, • www.
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, • ID existujúcej roly, ktorá má byť zneplatnená.
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> • potvrdenie zápisu roly, • odmietnutie zápisu roly a zdôvodnenie.

A.1.1.11 Pridanie roly identity v systéme IAM

Položka	Hodnota
Základné údaje	
Názov služby	Pridanie roly identity v systéme IAM
Popis služby	Vytvorenie/pridanie roly špecifikovanej identity v systéme IAM. Služba pridelí špecifikovanú rolu z katalógu rolí špecifikovanej identity.
Klasifikácia služby	

Položka	Hodnota
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G).
Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
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, identifikácia identity, identifikácia roly,
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> potvrdenie vykonania akcie odmietnutie vykonania akcie a zdôvodnenie

A.1.1.12 Odoberanie roly identity v systéme IAM

Položka	Hodnota
Základné údaje	
Názov služby	Odoberanie roly identity v systéme IAM
Popis služby	Zrušenie/odobratie roly špecifikovanej identity v systéme IAM. Služba zabezpečí odobratie špecifikovanej roly špecifikovanej identity. Daná identita nebude môcť využívať služby, ktoré vyžadujú danú rolu.
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G).
Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
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, identifikácia identity, identifikácia roly,
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> potvrdenie vykonania akcie odmietnutie vykonania akcie a zdôvodnenie

A.1.1.13 Pridanie autentifikačného prostriedku identity v systéme IAM

Položka	Hodnota
Základné údaje	
Názov služby	Pridanie autentifikačného prostriedku identity v systéme IAM

Položka	Hodnota
Popis služby	Vytvorenie/pridanie autentifikačného prostriedku (napr. autentifikačný certifikát na eID karte) špecifikovanej identity v systéme IAM pre podporu jednotnej autentifikácie používateľov pri používaní portálov verejnej správy (SSO).
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G).
Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
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, identifikácia identity, identifikácia AP,
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> potvrdenie vykonania akcie odmietnutie vykonania akcie a zdôvodnenie

A.1.1.14 Odobranie autentifikačného prostriedku (AP) identity v systéme IAM

Položka	Hodnota
Základné údaje	
Názov služby	Odobranie autentifikačného prostriedku (AP) identity v systéme IAM
Popis služby	Zrušenie/odobratie autentifikačného prostriedku špecifikovanej identity v systéme IAM
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G).
Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
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, identifikácia identity, identifikácia AP,
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> potvrdenie vykonania akcie odmietnutie vykonania akcie a zdôvodnenie

A.1.1.15 Poskytnutie autentifikačného rozhodnutia zo systému IAM

Položka		Hodnota
Základné údaje		
	Názov služby	Poskytnutie autentifikačného rozhodnutia zo systému IAM
	Popis služby	Poskytnutie informácie (ano/ nie) o tom, či je špecifikovaná identita autentifikovaná zadanými autentifikačnými údajmi. Prostredníctvom tejto IAM služby je možné overiť autentifikačné údaje danej identity. V prípade aktívnej autentifikácie (napr. eID karta) sa volaním tejto služby iniciuje v IAM proces autentifikácie a až po jeho ukončení služba poskytne výstupné rozhodnutie.
Klasifikácia služby		
	Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G),
	Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
	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 identity, autentifikačné údaje (credentials).
	Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> odpoveď ano/nie, odmietnutie poskytnutia informácie.

A.1.1.16 Generovanie nového hesla/reset hesla

Položka		Hodnota
Základné údaje		
	Názov služby	Generovanie nového hesla/reset hesla
	Popis služby	Služba vygeneruje nové heslo, resp. vykoná reset existujúceho hesla podľa požiadavky na vstupe pre danú identitu.
Klasifikácia služby		
	Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), organizácia VS (G2G), občan (G2C), podnikateľ (G2B).
	Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
	Stav implementácie	<ul style="list-style-type: none"> špecifikácia
Atribúty služby		
	Vstup (parametre služby – špecifikácia)	<ul style="list-style-type: none"> identifikácia používateľa služby,

Položka	Hodnota
požiadaviek používateľa na službu)	<ul style="list-style-type: none"> identifikácia identity, požiadavka na vytvorenie nového hesla alebo na reset existujúceho.
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> potvrdenie vykonania akcie, odmietnutie vykonania akcie a zdôvodnenie.

A.1.1.17 Splnomocnenie inej osoby v systéme IAM

Položka	Hodnota
Základné údaje	
Názov služby	Splnomocnenie inej osoby v systéme IAM
Popis služby	Zápis záznamu o splnomocnení do systému IAM, na základe ktorého bude môcť splnomocnený konať v mene splnomocniteľa pre špecifikovanú množinu služieb.
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> ISVS organizácie VS (G2G), občan (G2C), podnikateľ (G2B).
Komunikačné kanály	<ul style="list-style-type: none"> webové služby, www.
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, identifikácia identity - splnomocniteľa, identifikácia identity - splnomocnenca, identifikácia služieb, na ktoré sa vzťahuje plnomocnenstvo
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> potvrdenie vykonania akcie odmietnutie vykonania akcie a zdôvodnenie

A.1.2 Používateľské služby

A.1.2.1 Zápis autentifikačného prostriedku do katalógu autentifikačných prostriedkov systému IAM

Položka	Hodnota
Základné údaje	
Názov služby	Zápis autentifikačného prostriedku do katalógu autentifikačných prostriedkov systému IAM
Popis služby	Služba zabezpečí pridanie autentifikačného prostriedku do katalógu autentifikačných prostriedkov (napr.. typ "heslo", typ "certifikát", typ "generátor jednorazových hesiel" a pod.)

Položka	Hodnota
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> organizácia VS (G2G).
Komunikačné kanály	<ul style="list-style-type: none"> www.
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, zoznam údajov potrebných pre vytvorenie nového autentifikačného prostriedku (ID, názov, popis,
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> potvrdenie zápisu autentifikačného prostriedku odmietnutie zápisu autentifikačného prostriedku a zdôvodnenie

A.1.2.2 *Zrušenie autentifikačného prostriedku z katalógu autentifikačných prostriedkov systému IAM*

Položka	Hodnota
Základné údaje	
Názov služby	Zrušenie autentifikačného prostriedku z katalógu autentifikačných prostriedkov systému IAM
Popis služby	Zrušenie/odobratie autentifikačného prostriedku z katalógu autentifikačných prostriedkov v systéme IAM. Služba zabezpečí odobratie autentifikačného prostriedku z katalógu autentifikačných prostriedkov (napr. typ "heslo", typ "certifikát", typ "generátor jednorazových hesiel" a pod.)
Klasifikácia služby	
Používatelia služby	<ul style="list-style-type: none"> organizácia VS (G2G).
Komunikačné kanály	<ul style="list-style-type: none"> www.
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, identifikátor autentifikačného prostriedku na odobratie
Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> potvrdenie zrušenia autentifikačného prostriedku odmietnutie zrušenia autentifikačného prostriedku a zdôvodnenie

A.1.2.3 *Poskytnutie profilu identity v systéme IAM*

Položka	Hodnota
Základné údaje	
Názov služby	Poskytnutie profilu identity v systéme IAM
Popis služby	Poskytnutie atribútov profilu identity uložených v systéme IAM.

Položka		Hodnota
		V atribútoch profilu sa uchovávali napríklad osobné nastavenia pre personalizáciu.
Klasifikácia služby		
	Používatelia služby	<ul style="list-style-type: none"> • ISVS organizácie VS (G2G), • organizácia VS (G2G), • občan (G2C), • podnikateľ (G2B).
	Komunikačné kanály	<ul style="list-style-type: none"> • webové služby, • www.
	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, • požia.
	Výstup (výsledok služby poskytnutý používateľovi služby)	<ul style="list-style-type: none"> • atribúty profilu identity, • odmietnutie poskytnutia profilu a zdôvodnenie.

B Výpočet odhadu prácnosti riešenia

Pre odhad pracnosti 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 riešenia IAM

V rámci riešenia IAM je možné väčšinu aktivít zredukovať na základné operácie:

- zapísanie položky do systému IAM,
- zmena položky v systéme IAM,
- zneplatnenie (odstránenie) položky zo systému IAM,
- poskytnutie informácie zo systému IAM,

Predpokladá sa, že každá položka bude obsahovať minimálne 4 údaje.

Operácia „Zapísanie položky“ pracuje s nasledovnými objektami:

- zapísanie identity do systému IAM,
- zapísanie roly do katalógu rolí systému IAM,
- zapísanie autentifikačného prostriedku do katalógu autentifikačných prostriedkov,
- zapísanie (pridanie) roly identity,
- zapísanie (pridanie) autentifikačného prostriedku identity,
- zápis splnomocnenia inej osoby v systéme IAM.

Operácia „Zmena položky“ pracuje s nasledovnými objektami:

- zmena údajov identity v systéme IAM

Operácia „Zneplatnenie (odobratie) položky“ pracuje s nasledovnými objektami:

- odobratie identity zo systéme IAM,
- odobratie roly z katalógu rolí systému IAM,
- odobratie autentifikačného prostriedku z katalógu autentifikačných prostriedkov,
- odobratie roly identity,

- odobratie autentifikačného prostriedku identite.

Operácia „Poskytnutie informácií zo systému IAM“ pracuje s nasledovnými objektami:

- poskytnutie zoznamu rolí identity pre zadanú službu,
- poskytnutie informácie o priradení roly identite,
- poskytnutie zoznamu identít s prístupom ku službe,
- poskytnutie zoznamu rolí informačného systému

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

P. č.	Use-case	Zložitosť	Počet
1	Zapísanie položky do IAM repository	15	24
2	Zmena položky v IAM repository	15	4
3	Odobratie položky z IAM repository	15	5
4	Poskytnutie informácie z IAM repository	15	4
Spolu			37

Tabuľka 3: Zoznam a ohodnotenie use-casov riešenia

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

P. č.	Používateľ	Zložitosť	Počet
1	ISVS organizácie VS (G2G)	3	120
2	organizácia VS (G2G)	3	200
3	interný subjekt VS (G2E)		
4	občan (G2C)	3	1
Spolu			321

Tabuľka 4: Zoznam a ohodnotenie používateľov riešenia

B.2 Výpočet UCP

Výpočet Use-case bodov (UCP) je uvedené 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	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)	750	B.2.3 + B.2.4
3	Faktor technickej komplexnosti (TCF)	1,205	B.2.1
4	Faktor komplexnosti prostredia	1,1	B.2.2

P. č.	Parameter	Hodnota	Odvozenie hodnoty
	(ECF)		
5	Use-case body (UCP)	994	$2 * 3 * 4$
6	Prácnosť v človekohodinách	19 883	$1 * 5$

Tabuľka 5: Výpočet 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	Distribúovaný systém	2	5	10
T2	Výkon	1	5	5
T3	Efektívnosť pre používateľa	1	5	5
T4	Komplexnosť vnútorných procesov	1	5	5
T5	Znovapoužiteľnosť	1	5	5
T6	Jednoduchosť inštalácie	0,5	5	2,5
T7	Jednoduchosť používania	0,5	5	2,5
T8	Prenosnosť	2	5	10
T9	Jednoduchosť zmeny	1	4	4
T10	Súbežnosť	1	3	3
T11	Osobitné bezpečnostné prvky	1	5	5
T12	Poskytuje priamy prístup k tretím systémom	1	5	5
T13	Špeciálne znalosti a zručnosti používateľov	1	3	3
Spolu				65
TCF ($0,6 + (0,01 * \text{Spolu})$)				1,25

Tabuľka 6: 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	1	1,5
E2	Skúsenosti s implementáciou	0,5	2	1
E3	Skúsenosti s objektovo orientovaným prístupom	1	1	1
E4	Schopnosť vedúcich analytikov	0,5	3	1,5
E5	Motivácia	1	0	0

ID	Faktor	Váha	Komplexnosť	Výsledok
E6	Stabilita požiadaviek	2	4	8
E7	Zamestnanci na čiastočný úväzok	-1	0	0
E8	Zložitý programovací jazyk	-1	5	-5
Spolu				8
ECF (1,4 + (-0,03 * Spolu))				1,16

Tabuľka 7: 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	0	0
Komplexné	Zahŕňa zložitú užívateľské rozhranie, dotýka sa 3 alebo viac databáz, viac ako 7 krokov, jej implementácia sa týka viac ako 10 tried.	15	37	555
Spolu				555

Tabuľka 8: 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	0	0
Komplexné	Používateľ je človek komunikujúci prostredníctvom používateľského rozhrania.	3	321	963
Spolu				963

Tabuľka 9: Výpočet neupravenej váhy používateľských interakcií (UUCW)