

TVORÍME VEDOMOSTNÚ SPOLOČNOSŤ
Európsky fond regionálneho rozvoja



Čiastková štúdia uskutočniteľnosti projektov prioritnej osi č.1
Operačného programu Informatizácia spoločnosti

Štúdia uskutočniteľnosti
Projektu budovania aplikačnej architektúry a
bezpečnostnej infraštruktúry rezortu Ministerstva
spravodlivosti SR

Obsah

Obsah 1

1	Základné informácie	5
1.1	Prehľad	5
Tabuľka 1 Identifikácia stakeholdera projektu		5
1.2	Dôvod	7
1.3	Rozsah a vízia projektu	8
1.4	Rámec projektu	9
1.5	Rozdielová analýza súčasného a cieľového stavu	9
Súčasný stav:		9
Cieľový stav:		10
1.6	Použité skratky a značky	10
2	Manažérske zhrnutie	14
3	Popis aktuálneho stavu	17
3.1	Legislatívna analýza	17
3.2	Aplikačná a dátová architektúra	19
3.2.1	Aplikácie	19
Základné informačné systémy sú obsiahnuté v tabuľke č.3.		19
3.2.2	Využívanie modulov plánovanej aplikačnej a bezpečnostnej architektúry existujúcimi systémami	25
3.2.3	Dátová architektúra	26
3.2.4	Integračná architektúra	27
Obr. 1 Aktuálny stav integrácii systémov		27
3.3	Vyhodnotenie súčasného stavu	28
4	Popis cieľového stavu	31
4.1	Legislatívna analýza	31
4.2	Analýza požiadaviek a potrieb aktérov/stakeholderov	31
Tabuľka 5 Analýza požiadaviek aktérov		31
4.3	Architektúra navrhovaného riešenia	32
4.3.1	Formulovanie cieľov	32
4.3.2	Očakávané prínosy	34
4.3.3	Popis služieb na biznis úrovni	35
4.3.4	Využitie cloudového riešenia MF SR	38
4.4	Popis architektúry	39
4.4.1	Prehľad integrácii v cieľovom stave	40

Obr. 2 Cieľový stav po zavedení centrálnej integračnej platformy	40
4.4.2 Integračná platforma	41
4.4.3 PKI infraštruktúra	47
4.4.4 Správa používateľov	49
4.4.5 Bezpečnostné a podporné mechanizmy	52
4.4.6 Mechanizmy pre podporu prevádzky infraštruktúry a informačných systémov	56
5 Uskutočniteľnosť a náklady	61
5.1 Dopady na technické a softwarové vybavenie	61
5.2 Organizačné dopady	62
5.3 Legislatívne dopady	62
5.4 Prevádzkové a bezpečnostné dopady	63
5.5 Bezpečnosť	63
5.5.1 Zabezpečenie prevádzky nasadeného riešenia	63
5.6 Nasadenie riešenia a marketingové požiadavky	65
5.7 Nefinančné prínosy a náklady	65
6 Plán implementácie – projektový zámer	66
6.1 Príprava projektu	66
6.2 Riadenie projektu a metodika riadenia	68
6.3 Harmonogram projektu	68
Návrh harmonogramu projektu	68
Aktivita 1: Analýza a návrh riešenia	68
Aktivita 2: Obstaranie SW licencií	69
Aktivita 3: Obstaranie a nasadenie HW	70
Aktivita 4: Implementácia	71
Aktivita 5: Testovanie	72
Aktivita 6: Nasadenie	72
Podporná aktivita: Riadenie projektu	73
Podporná aktivita: Publicita a informovanosť	73
Príloha č.1 - Rozpočet a nákladovo výnosová analýza	74
6.4 Strategický kontext	74
6.5 Ciele a obmedzenia	74
6.6 Rozpočet projektu	78

Tabuľka 7	78
Tabuľka 8 Odhadovaná výška rozpočtu	79
Tabuľka 9 Rozpočet projektu odhadovaný	80
6.7 Analýza nákladov	81
Tabuľka 10 Odhadované náklady projektu	81
6.8 Analýza prínosov	83
Tabuľka 11 Odhadované prínosy projektu	83
6.9 Čistá súčasná hodnota	86
Príloha č.2 – Popis elektronických služieb	87
6.10 Zoznam eGov služieb	87
6.10.1 Zabezpečenie prístupu k službe alebo informáciám pre oprávneného interného používateľa	87
6.10.2 Zabezpečenie prístupu k službe alebo informáciám pre oprávneného špecializovaného používateľa	88
6.10.3 Zabezpečenie prístupu k službe alebo informáciám pre oprávneného nešpecializovaného používateľa	90
6.10.4 Poskytnutie integrovanej elektronickej služby	91
6.11 Zoznam služieb informačného systému (IS)	94
6.11.1 Registrácia používateľa do systému centrálnej správy používateľov	95
6.11.2 Zabezpečenie centrálnej správy používateľov pre agendové systémy	95
6.11.3 Centrálna identifikácia a autorizácia používateľov pre agendové systémy	96
6.11.4 Riadenie prístupov k informačným zdrojom a funkciám informačných systémov pre agendové systémy	98
6.11.5 Monitorovanie a audit poskytovania správy používateľov a riadenia prístupu pre agendové systémy	98
6.11.6 Identifikácia a manažment služieb vystavených na integračnej platforme	99
6.11.7 Manažment životného cyklu služieb vystavených na integračnej platforme	100
6.11.8 Definovanie business procesu na integračnej platforme	101
6.11.9 Realizácia business procesu na integračnej platforme	102
6.11.10 Monitorovanie business procesov na integračnej platforme	102
6.11.11 Vydanie autorizačných údajov pre používateľa	103
6.11.12 Vykonanie autorizácie úkonu používateľom	104
Príloha č. 3 - Analýza rizík	106
6.11.13 Riziká spojené s celospoločenským prostredím	106
6.11.14 Riziká spojené s projektom a jeho cieľmi	106
6.11.15 Riziká spojené so spôsobom realizácie projektu	107
6.11.16 Iné riziká	108
Príloha č. 4 - Kalkulácie celkových nákladov na vlastníctvo softvéru (TCO)	1

Príloha č. 5 - Kalkulácie nákladov na vlastníctvo hardvéru (TCO)

8

1 Základné informácie

Časť podkladov a údajov použitých pri vypracovaní štúdie uskutočniteľnosti bola poskytnutá tretími stranami, pričom autor vychádza z predpokladu ich pravdivosti. Autor nezodpovedá za akúkoľvek škodu spôsobenú chybou, neúplnosťou, nepravdivosťou alebo čiastočnou nepravdivosťou poskytnutých údajov a podkladov ak takáto chyba, neúplnosť, nepravdivosť nebola zistiteľná s použitím bežnej starostlivosti a bez osobitného preverovania.

Štúdia je vypracovaná s využitím informácií vychádzajúcich zo známeho stavu skutočností ku dňu jej vypracovania. Autor nezodpovedá za akúkoľvek škodu spôsobenú využitím štúdie bez zohľadnenia prípadnej zmeny skutočností, z ktorých autor pri vypracovaní štúdie vychádza. V prípade takýchto zmien môže byť na základe požiadania adresáta štúdie táto po dohode zo strany autora modifikovaná tak, aby odzrkadľovala zmeny, ku ktorým došlo.

V prípade ak počas implementácie projektov na základe štúdie adresátom a/alebo treťou osobou bude štúdia alebo jej časti zmenené alebo pri realizácii opatrení v rámci prioritnej osi č. 1 Operačného programu Informatizácia spoločnosti sa nebude postupovať v súlade s informáciami obsiahnutými v štúdii, autor nebude zodpovedať za škodu, ktorá vznikne pri takejto implementácii alebo postupe s výnimkou prípadov, že zmeny alebo postup boli autorom vopred odsúhlasené písomnou formou.

Štúdia je autorským dielom, a ako adresát tak aj ďalšie osoby, ktoré budú štúdiu alebo jej jednotlivé časti využívať bez ohľadu na to, či s vedomím alebo bez vedomia autora sú povinné rešpektovať príslušné ustanovenia autorského zákona.

1.1 Prehľad

Štúdia uskutočniteľnosti pre budovanie aplikačnej architektúry a bezpečnostnej infraštruktúry vychádza z požiadaviek Záverečného informatívneho dokumentu – IT služby pre eJustice. Podrobnejšie rozpracováva problematiku budovania aplikačnej architektúry, ktorá je základom pre budovanie konceptu eJustice.

Táto štúdia realizovateľnosti je vytvorená Ministerstvom spravodlivosti Slovenskej republiky (ďalej „MS SR“) v spolupráci s externým dodávateľom.

Partnerom MS SR v tomto projekte je Národná agentúra pre sieťové a elektronické služby. V zmysle zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy je správcom Ústredného portálu verejnej správy Ministerstvo financií SR a prevádzkovateľom Úrad vlády SR prostredníctvom NASESu. Spoločné moduly ÚPVS sú na základe Národnej koncepcie informatizácie verejnej správy jednou zo základných súčastí integrovaného informačného systému verejnej správy.

Tabuľka 1 Identifikácia stakeholdera projektu

Ministerstvo spravodlivosti Slovenskej republiky	
IČO:	00166073

Právna forma:	321 Rozpočtová organizácia (13110 Ústredná štátna správa)
Adresa sídla:	Župné námestie 13, 813 11 Bratislava - Staré Mesto
Kód SK NACE	84110 Všeobecná verejná správa
Predmet prevažujúcej činnosti (OKEČ)	75110 Všeobecná verejná správa
Veľkosť organizácie	251-500 zamestnancov

Zdroj: Register organizácií ŠÚ SR

Prehľad relevantných životných situácií je nasledovný:

Zdroj: Číselník životných situácií a okruhov životných situácií, MF SR

Realizátorom navrhovaného projektu je Ministerstvo spravodlivosti Slovenskej republiky (MS SR) prostredníctvom svojich odborných útvarov. V tabuľke nižšie je uvedený zoznam úsekov verejnej správy a agend verejnej správy relevantných pre projekt.

Úseky a agendy verejnej správy:

Tabuľka 2 Súčasný stav kódov relevantných úsekov verejnej správy a agend verejnej správy v zodpovednosti MS SR

Kód úseku verejnej správy	Názov úseku verejnej správy	Kód agendy	Názov agendy verejnej správy
U00119	Súdy a väzenstvo	A0001644	Zjednocovanie výkladu a používania zákonov a iných všeobecne záväzných právnych predpisov
U00126	Plnenie úloh súvisiacich s členstvom Slovenskej republiky v Eurojuste		
U00208	Ochrana práv a zákonom chránených záujmov fyzických osôb, právnických osôb a štátu		
U00223	Vnútorná správa		
U00134	Koordinácia realizácie politík Európskej únie	A0003158	Slobodný prístup k informáciám
		A0003185	Sprístupňovanie informácií z informačných systémov verejnej správy

Zdroj: Výnos MF SR č. 478/2010 o základnom číselníku úsekov verejnej správy a agend verejnej správy

Projekt sa týka nasledovných životných situácií :

Životná situácia	• C01 Občan a štát – 051 Demokracia
------------------	-------------------------------------

	<ul style="list-style-type: none">• C01 Občan a štát – 055 Slobodný prístup k informáciám, utajované skutočnosti, archívy• C01 Občan a štát – 058 Účasť na veciach verejných• B05 Podnikanie – Služby 025;• C08 Zamestnanie - Práca vo verejnom záujme 131; Pracovnoprávne vzťahy 132; Štátny zamestnanec 137;
--	---

1.2 Dôvod

Informatizácia štátnej správy je vládou Slovenskej republiky vnímaná ako jedna z prioritných oblastí v rámci procesu informatizácie spoločnosti. Požiadavka elektronizácie služieb vyplýva z dokumentu Stratégia informatizácie verejnej správy (ďalej „SIVS“) schváleného uznesením vlády SR č. 131/2008. Vládnou víziou eGovernmentu je dosahovať neustály rast spokojnosti občanov s verejnou správou prostredníctvom poskytovania služieb atraktívnym a jednoduchým spôsobom za súčasného zvyšovania svojej efektívnosti, kompetentnosti a znižovania nákladov na verejnú správu.

Ciele plynúce zo Stratégie informatizácie verejnej správy majú prispieť k dosiahnutiu globálneho cieľa Operačného programu Informatizácia spoločnosti, ktorým je vytvorenie inkluzívnej informačnej spoločnosti ako prostriedku pre rozvoj vysoko výkonnej vedomostnej ekonomiky.

Dňa 2.2.2011 Vláda SR svojim uznesením č. 72/2011 schválila Revíziu budovania eGovernmentu (strednodobý plán implementácie priorít), ktorá definuje nové prístupy k budovaniu eGovernmentu a to najmä prostredníctvom budovania proaktívnych a transparentných elektronických služieb, ktoré vychádzajú zo životných situácií občanov a podnikateľov.

Táto stratégia budovania eGovernmentu v SR bola zakomponovaná do Zákona č. 305/2013 o eGovernmente, ktorý definuje základné princípy pre budovanie eGovernmentu v SR a elektronických služieb.

Štúdiá sa zameriava na vyhodnotenie možností efektívnej implementácie elektronických služieb a procesov rezortu Ministerstva spravodlivosti SR (ďalej „MS SR“) s využitím spoločných modulov jednotnej aplikačnej architektúry a bezpečnostnej infraštruktúry, v súlade s konceptom eJustice. Tento koncept, okrem iného, predpokladá implementáciu elektronických služieb a sprístupnenie týchto služieb a informačných zdrojov širokej verejnosti. Centralizáciou jednotlivých modulov je možné dosiahnuť zvýšenie efektívnosti implementácie jednotlivých systémov, ako aj zvýšenie celkového stavu bezpečnosti jej centralizovaným riadením.

Výsledkom riešenia projektu na báze predkladanej štúdie bude vytvorenie vybranej časti aplikačnej infraštruktúry, ktorá tvorí základ integrovanej aplikačnej architektúry MS SR, ako aj vybudovanie potrebnej bezpečnostnej infraštruktúry, ktorá je nevyhnutná pre dosahovanie základných cieľov konceptu eJustice.

Dôvodom vypracovania tejto štúdie je vyhodnotenie uskutočniteľnosti zámeru budovania aplikačnej architektúry a bezpečnostnej infraštruktúry, ktoré budú tvoriť základ pre budovanie a publikovanie elektronických služieb rezortu MS SR, v súlade s Národnou koncepciou informatizácie verejnej správy, Zákom č. 305/2013 o eGovernmente, ako aj v súlade s ostatnými programovými dokumentmi.

1.3 Rozsah a vízia projektu

Táto štúdia uskutočniteľnosti popisuje súčasný stav budovania informačných systémov v rezorte MS SR a navrhuje aplikačnú architektúru a bezpečnostnú infraštruktúru rezortu MS SR. V rámci tejto aplikačnej architektúry definuje aplikačnú infraštruktúru, t.j. zdieľané moduly, ktoré umožnia efektívnu implementáciu jednotlivých informačných systémov a poskytovanie elektronických služieb MS SR podľa NKIVS. Zdieľanými modulmi rozpracovanými v tejto štúdii realizovateľnosti sú:

- Modul Integrovaná platforma – prostriedok zabezpečujúci integráciu jednotlivých systémov nasadzovaných v rámci budovania konceptu eJustice,
- Modul PKI infraštruktúra – prostredie zabezpečujúce autorizáciu v rámci interných procesov,
- Modul Správa používateľov – modul zabezpečujúci jednotnú správu používateľov a ich oprávnení poskytujúci funkcie pre všetky nasadzované informačné systémy,
- Bezpečnostný modul – zabezpečujúci naplňovanie bezpečnostnej politiky a identifikáciu bezpečnostných incidentov
- Modul Bezpečného prehliadania elektronického súdneho spisu – zabezpečuje funkcionality prehliadania elektronického súdneho spisu internými používateľmi cez zabezpečený kanál z tabletov a osobných počítačov (PC)
- Modul podpory prevádzky – poskytujúci prostriedky pre podporu a zefektívnenie prevádzkových procesov.

Štúdia analyzuje súčasný stav budovania informačných systémov rezortu MS SR, s dôrazom na organizačné zabezpečenie, procesy, legislatívu a informačné a komunikačné technológie. Pred samotnou integráciou so spoločnými modulmi ÚPVS sa predpokladá prijatie vybraných opatrení na strane NASESu, ktoré boli zistené pri pravidelnej bezpečnostnej analýze rizík na strane ÚPVS. Riziká identifikované v rámci bezpečnostnej analýzy je nutné mitigovať pred začiatkom samotnej integrácie MS SR s ÚPVS.

Štúdia ďalej odporúča optimálny plán implementácie aplikačnej architektúry a aplikačnej infraštruktúry, zaoberá sa ekonomickým odôvodnením projektu a prostredníctvom analýzy nákladov a výnosov odôvodňuje výšku požadovaného nenávratného finančného príspevku. Súčasťou štúdie sú aj odporúčania na projektové riadenie implementačného projektu. V neposlednom rade sa zaoberá aj rizikami projektu a poskytuje odporúčania pre MS SR pre oblasti, ktoré sa týkajú elektronizácie, aj keď tieto sú mimo rozsahu tejto štúdie.

1.4 Rámec projektu

Táto čiastková štúdiá uskutočniteľnosti sa opiera najmä o nasledujúce dokumenty:

- Strategické dokumenty na úrovni EÚ:
 - Stratégia Európa 2020
 - súvisiace odporúčania a usmernenie EK, Rady a EP
- Strategické dokumenty na národnej úrovni:
 - Stratégia informatizácie verejnej správy
 - Národná koncepcia informatizácie verejnej správy SR
 - Stratégia informatizácie spoločnosti 2009 – 2013
 - Programové vyhlásenie Vlády Slovenskej republiky na roky 2012 - 2016
 - Národný program reforiem na roky 2011 – 2014
 - Digitálna agenda pre Európu v podmienkach SR
 - Stratégia informatizácie spoločnosti na roky 2009 – 2013
 - Revízia budovania eGovernmentu
 - Národná stratégia pre informačnú bezpečnosť SR
 - Národná stratégia SR pre digitálnu integráciu
 - Koncepcia využívania softvérových produktov vo verejnej správe
 - Revízia budovania eGovernmentu (strednodobý plán implementácie priorít)
- Programové dokumenty OPIS
 - Operačný program Informatizácia spoločnosti 2007-2013 (OPIS)
 - Programový manuál OPIS
- Strategické dokumenty na rezortnej úrovni:
 - KRIS MS SR,
 - Záverečný informatívny dokument – IT služby pre eJustice

Projekt podporuje rozvoj eGovernmentu, zefektívnenie fungovania verejnej správy prostredníctvom informatizácie a rozvoja elektronických služieb prostredníctvom špecializovaných komponentov G2G, G2C a v prípade ďalšieho rozvoja aj G2B. Projektom sa pokrýva 1. prioritná os OPIS Efektívna elektronizácia verejnej správy a rozvoj elektronických služieb, opatrenie 1.1 Elektronizácia verejnej správy a rozvoj elektronických služieb na centrálnej úrovni.

1.5 Rozdielová analýza súčasného a cieľového stavu

Realizáciou projektu sa zabezpečí zlepšenie súčasného stavu aplikačnej architektúry a dosiahnutie požadovaného cieľového stavu, ktorý uľahčí jednoduchosť prístupu k integrovaným službám systémov MS SR.

Súčasný stav:

- neexistencia jednotnej politiky prístupu k službám a informáciám, táto politika je implementovaná špecificky v jednotlivých agendových informačných systémoch samostatne,

- neexistencia centrálnej evidencie používateľov, každá aplikácia si evidenciu používateľov realizuje samostatne,
- neexistencia centralizovanej aplikačnej architektúry zdieľaných modulov, čo vedie k duplikácii modulov v jednotlivých systémoch,
- neexistencia integračnej platformy, ktorá umožní efektívnu integráciu existujúcich aplikácií – či na dátovej alebo procesnej. Integrácia sa realizuje (ak je nevyhnutná) priamym a špecifickým prepojením existujúcich aplikácií,
- neexistencia centrálnej bezpečnostnej politiky, ktorá je pravidelne monitorovaná a vyhodnocovaná.

Cieľový stav:

- jednotné rozhranie pre interných a externých používateľov implementujúce jednotnú politiku prístupu k službám a informáciám,
- centrálna evidencia interných a externých používateľov, centrálna riadenie prístupových práv, poskytovanie informácií o identitách a právach pre jednotlivé agendové systémy,
- centrálna bezpečnostná politika a nástroje na jej monitorovanie a vyhodnocovanie,
- jasne definovaná aplikačná architektúra s definovanými zdieľanými modulmi a s ich využitím pre budovanie jednotlivých systémov (zdieľanie spoločnej funkcionality),
- existencia centrálnej integračnej platformy pre implementáciu procesov a integráciu jednotlivých agendových systémov.

Podrobnejší popis súčasného stavu a cieľového stavu sa nachádza v ďalších častiach štúdie uskutočniteľnosti.

1.6 Použité skratky a značky

Tabuľka 3 Zoznam skratiek

Skratka / Značka	Vysvetlenie
APV	Aplikačné a programové vybavenie
Projekt BAA	Projekt budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu
IS EZZ	Informačný systém elektronická zbierka zákonov
IS PPI	Informačný systém Portál právnych informácií
IS ESS	Informačný systém elektronický súdny spis
IS RTIS	Informačný systém Rozvoj a technologická inovácia súdnotrestnej a súdnocivilnej agendy
CRL	Certificate revocation list – zoznam zrušených certifikátov
DB	Databáza
DMZ	Demilitarizovaná zóna
EK	Európska komisia
EP	Elektronický podpis
GUI	Grafical user interface - Grafické užívateľské rozhranie
G2C	Gouvernement to customer (verejná správa k občanovi)

G2G	Gouvernement to government (vzťahy vo verejnej správe)
G2E	Government to employees (zamestnanci verejnej správy)
IS VS	Informačný systém verejnej správy
ITMS	IT monitorovací systém pre štrukturálne a Kohézny fond
MV SR	Ministerstvo vnútra Slovenskej republiky
NKIVS	Národná koncepcia informatizácie verejnej správy
OPIS	Operačný program informatizácie spoločnosti
PKI	Public key infrastructure – infraštruktúra správy a distribúcie verejných kľúčov z asymetrickej kryptografie
REGOB	Register obyvateľov
REP	Rezortná elektronická podateľňa
RFO	Register fyzických osôb
RPO	Register právnických osôb
SAN	Storage Area Network
SLA	Service Level Agreement
SOA	Service oriented architecture – servisne orient. architektúra
SORO	Sprostredkovateľský orgán pod riadiacim orgánom
ZEP	Zaručený elektronický podpis
AS IS	Aktuálny stav bez realizácie projektu
BPM	Business process management
CBA	Nákladovo-výnosová analýza
CMS	Manažment správy obsahu (Content management system)
DB	Databáza
DMS	Systém správy a riadenia dokumentov (Document management system)
eGov	eGouvernement
ESB	Enterprise service bus
EÚ	Európska únia
GUI	Grafické používateľské rozhranie (Graphic User Interface)
G2B	Služby pre podnikateľov (Government to Business)
G2C	Služby pre občanov (Government to Citizens)
G2G	Služby pre verejnú správu, komunikácia systémov verejnej správy bez zásahu človeka (Government to Government)
HW	Hardvér (Hardware)
IAM	Identifikačný a autentifikačný modul (Identity and Access Management)
IKT	Info - komunikačné technológie

IS	Informačný systém
ITIL	Information Technology Infrastructure Library
ITU	Medzinárodná telekomunikačná únia
ISO	International Organization for Standardization
IS VS	IS verejnej správy
MF SR	Ministerstvo financií Slovenskej republiky
NPV	Čistá súčasná hodnota (Net Present Value)
OPIS	Operačný program Informatizácia spoločnosti
PMI	Project Management Institute
PRINCE	Projects in Controlled Environments
ROI	Návratnosť investícií (Return of Investment)
RUP	Rational Unified Process
SIEA	Slovenská inovačná a energetická agentúra
SLOV-LEX	Projekt Elektronická zbierka zákonov (IS SLOV-LEX)
SOA	Servisne orientovaná architektúra (Service Oriented Architecture)
SR	Slovenská republika
SW	Softvér (Software)
STN	Slovenská technická norma
TO BE	Cieľový stav po realizácii projektu
TOGAF	The Open Group Architecture Framework
TCO	Celkové náklady na vlastníctvo (Total Cost of Ownership)
CSRU	Centrálny systém referenčných údajov
ÚPVS	Ústredný portál verejnej správy
XML	Extensible Markup Language
ZEP	Zaručený elektronický podpis
LT	Legislatívny tok
Z. z.	Zbierka zákonov po roku 1993
Zb.	Zbierka zákonov v období 1945-1992
Zb. SNR	Zbierka zákonov Slovenskej Národnej rady v období 1944-1949
VS	Verejná správa
ÚOŠS	Ústredný orgán štátnej správy
WF	Workflow
WFe	Workflow engine
ZÚ	Zastupiteľský úrad
ŽoNFP	Žiadosť o nenávratný finančný príspevok
MPK	Medzirezortné pripomienkové konanie
PPI	Portál právnych informácií
eZbierka	elektronická podoba Zbierky zákonov Slovenskej republiky implementovaná v rámci projektu Elektronická zbierka zákonov

	informačný systém zabezpečujúci distribúciu vyhláseného práva rôznym cieľovým skupinám adresátov práva
eLegislatíva	informačný systém zabezpečujúci všetky procesy prípravy práva
EUR-LEX	právny systém EÚ na adrese http://new.eur-lex.europa.eu/homepage.html?locale=sk
JASPI	Jednotný automatizovaný systém právnych informácií; právny systém Ministerstva spravodlivosti SR na adrese http://jaspi.justice.gov.sk/jaspiw1/jaspiw_mini_fr0.htm
N-LEX	jednotné rozhranie pre prácu s úradnými zbierkami právnych predpisov štátov EÚ na adrese http://eur-lex.europa.eu/n-lex/index_sk.htm
JISS	Jednotný informačný systém na sledovanie legislatívneho procesu https://lt.justice.gov.sk/Default.aspx
RESS	Rozvoj elektronických služieb súdnictva
ESMO	Elektronické služby monitoringu obvinených a odsúdených osôb
NASES	Národná agentúra pre sieťové a elektronické služby

2 Manažérske zhrnutie

V súčasnosti je výkon agend v rezorte spravodlivosti podporovaný samostatnými informačnými systémami, z ktorých mnohé sú budované na zastaraných technológiách a je problematické ich efektívne prevádzkovať. Tieto informačné systémy nie sú dostatočne integrované a preto poskytujú služby výhradne pre určené agendy. Komplexnejšie procesy je problematické implementovať, čo výraznejšie limituje možnosti poskytovania služieb s vysokou pridanou hodnotou pre používateľov.

Rovnako využívanie mnohých systémov vyžaduje identifikáciu a autentifikáciu používateľov, ako aj selektívne riadenie ich prístupových práv v rámci údajov a služieb v týchto systémoch. V súčasnosti je správa používateľov a ich oprávnení realizovaná oddelene v jednotlivých systémoch. Procesy správy používateľov sú teda distribuované a málo efektívne a neumožňujú ich komplexné riadenia a zaistenie požadovanej úrovne bezpečnosti.

Z hľadiska bezpečnosti neexistuje prakticky implementovaná jednotná bezpečnostná politika a nie je vyhodnocovaná činnosť používateľov a súlad s touto bezpečnostnou politikou. Rovnako aj z hľadiska prevádzky nie je centrálné monitorovaná a sú minimálne automatizované jednotlivé rutinné činnosti. To na druhej strane zvyšuje zaťaženie prevádzkového personálu. Budovanie systémov v rámci konceptu eJustice z hľadiska prevádzky a riadenia bezpečnosti je preto nemysliteľné.

Budovania aplikačnej infraštruktúry a bezpečnostnej architektúry vytvorí podmienky pre efektívne naplňovanie cieľov konceptu eJustice.

Ciele projektu:

Cieľom projektu je vybudovať celorezortnú Integračnú platformu MS SR. Táto platforma vygeneruje v budúcnosti veľké úspory času pri implementácii zmenových požiadaviek všetkých aplikácií, ktoré sa v súčasnosti budujú a budú sa cez jednotnú Integračnú platformu integrovať s inými internými aj externými informačnými systémami. Bohužiaľ v súčasnosti nie je možné vygenerovať okamžitú úsporu nákladov v iných projektoch, nakoľko všetky aplikácie je potrebné prepojiť (zintegrovať) s touto Integračnou platformou.

Ďalším cieľom projektu je vybudovať jednotnú celorezortnú PKI infraštruktúru pre všetkých zamestnancov rezortu. PKI infraštruktúra zabezpečí požadovanú bezpečnosť vytvárania a overovania všetkých dokumentov v rámci celého rezortu MS SR.

Ďalším cieľom projektu je vytvoriť celorezortnú platformu pre Monitoring, Event Management, sledovanie a analýzu výkonnosti sietí, systémov a samozrejme aj aplikácií. Táto platforma v budúcnosti ušetrí veľké prostriedky a ľudské zdroje pri odstraňovaní väd a incidentov na celej infraštruktúre rezortu MS SR a aj aplikáciách.

V budúcnosti nebude nutné rozširovať tieto platformy, len pridávať funkcionality a nové prvky infraštruktúry.

Ďalším cieľom projektu je vybudovať celorezortnú IAM infraštruktúru, ktorá v budúcnosti bude generovať veľké úspory celej MS SR prevádzkovej IT organizácii pri riadení infraštruktúry (IM) všetkých základných prevádzkových komponentov, ako sú politiky, procesy, zariadenia,

dáta, ľudské zdroje aj externé integrácie a bude mať obrovský dosah na celkovú efektivitu IT organizácie rezortu MS SR.

Cieľom projektu z pohľadu NASES je aplikácia softvérového riešenia tretej strany, ktoré zabezpečí rozšírenie a zvýšenie bezpečnosti modulu IAM ÚPVS, kategorizáciu prístupových opatrení a rolí, konsolidáciu a šandardizáciu rozhraní pre integrované aplikácie, zavedenie jednotného štandardu bezpečnosti, kontrolných a auditovacích mechanizmov z pohľadu gestorov aplikácií a bezpečnostných audítorov.

Prínosy riešenia projektu pre vývoj a nasadzovanie systémov v rámci konceptu eJustice sú nasledovné:

- vytvorenie jednotnej platformy pre integráciu aplikácií. Integrácia aplikácií je vykonávaná centrálnie na integračnej platforme bez potreby priamej integrácie všetkých aplikácií a budovania množstva špecializovaných rozhraní,
- zefektívnenie procesy vývoja aplikácií využitím existujúcej funkčnosti integračnej platformy a jej služieb,
- možnosť budovania novej kvality služieb, ktorá umožní využívať procesnú integráciu funkčnosti viacerých aplikácií, čo vedie k poskytovaniu vyššej úžitkovej hodnoty pre používateľov ako interných, tak externých.

Prínosy riešenia projektu v oblasti správy používateľov a bezpečnosti sú nasledovné:

- naplňovanie zámerov konceptu eJustice riadením prístupu oprávnených používateľov k službám pre rôzne skupiny používateľov,
- centrálna správa používateľov a ich oprávnení pre všetky prevádzkované systémy,
- zabezpečenie autentifikácie a autorizácie používateľov (interných aj externých) pre prístup k službám a údajov v súlade s definovanou politikou,
- zabezpečenie prostriedkov pre autorizáciu všetkých dôležitých úkonov s následnou možnosťou definovania jednoznačnej a nespochybniteľnej zodpovednosti za vykonané úkony,
- monitorovanie a vyhodnocovanie bezpečnostnej situácie, ako podklad pre návrh a realizáciu opatrení.

Prínosy riešenia projektu v oblasti podpory prevádzky sú nasledovné:

- zmapovanie všetkých systémov a ich konfigurácií – podklad pre správu aktív a evidenciu využívania licencií pre nasadené systémy,
- monitorovanie stavu zariadení a dôležitých prevádzkových parametrov,
- spracovanie a korelovanie udalostí prichádzajúcich z monitorovaných zariadení,
- podpora pre Help-Desk – podpora používateľov vo využívaní služieb nasadených informačných systémov,
- podpora a čiastočná automatizácia základných prevádzkových operácií.

Vo vyššie uvedenom kontexte sú preto ciele projektu budovania aplikačnej architektúry a bezpečnostnej infraštruktúry nasledujúce:

- vytvoriť prostredie pre efektívnu integráciu aplikácií a budovanie komplexných procesov,

- vytvoriť prostredie pre manažment autorizačných prostriedkov pre pracovníkov rezortu používaných pri autorizácii rozhodnutí,
- vytvoriť prostredie pre správu používateľov a riadenie ich prístupových práv, ako aj manažment bezpečnosti informačných systémov v rezorte,
- vytvoriť podmienky pre podporu prevádzkových činností.

Štúdia sa podrobnejšie venuje rozpracovaniu týchto cieľov a návrhu spôsobu ich dosahovania. Úspešná realizácia projektu realizovaného na báze tejto štúdie prispeje k naplneniu cieľov budovania konceptu eJustice.

Projekt v súčasnej situácii môže byť plne financovaný z prostriedkov OPIS PO1, s minimálnym dopadom na rozpočet rezortu. Analýza nákladov a prínosov preukázala, že návratnosť investícií projektu je v 9. roku od začatia realizácie, pričom nepriame prínosy vysoko prekračujú cenu projektu, a tým významne urýchľujú materializáciu benefitov. Nepriame výnosy sú kalkulované na základe úspory času používateľov systému.

Projekt bude realizovaný využitím moderných princípov riadenia (PRINCE2, ITIL) a návrhu architektúry (TOGAF). Uvedené overené metodiky a best-practices eliminujú niekoľko rizík projektu a umožnia vytvorenie kvalitného riešenia.

3 Popis aktuálneho stavu

Aktuálny stav predstavuje predovšetkým súhrn existujúcich systémov zabezpečujúcich jednotlivé agendy rezortu spravodlivosti. V nasledujúcej kapitole je uvedený prehľad aktuálnej legislatívy, nasleduje popis architektúry aktuálneho stavu rozčlenený v súlade s metodikou TOGAF na nasledovné pohľady:

- o Biznis architektúra,
- o Aplikačná a dátová architektúra,
- o Technologická architektúra.

Súčasný stav je rozpracovaný pre jednotlivé architektonické domény v podkapitolách nižšie. Pohľad na tento stav, definuje východiská a koncepcné návrhy pre ďalšie smerovanie rozvoja IT pre rezort spravodlivosti. Predstava ďalšieho rozvoja je postavená na IT požiadavkách vyplývajúcich z legislatívy a potrieb fungovania rezortu. Štúdiá identifikuje aj spoločné aplikačné a technologické moduly, ktoré je možné v rámci budovania budúcich systémov využiť viacerými systémami. Taktiež sú definované základné princípy pre budovanie infraštruktúry. Pri modernizácii alebo zavádzaní nových systémov by mali byť tieto princípy zohľadnené a akceptované, čoho dôsledkom by malo byť efektívnejšie využívanie prostriedkov rezortu.

3.1 Legislatívna analýza

Výkon činnosti rezortu Ministerstva spravodlivosti SR sa riadi všeobecne platnou legislatívou, ako aj legislatívou špecifickou pre konkrétne procesy zverené jednotlivých inštitúcií rezortu spravodlivosti.

Z hľadiska vecnej pôsobnosti rezortu spravodlivosti je dôležitý Zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy, ktorý vymedzuje pôsobnosť Ministerstva spravodlivosti SR:

- štátna správa súdov a väzenstva, legislatívu ústavného práva, trestného práva, občianskeho práva, obchodného práva, rodinného práva, konkurzného práva, medzinárodného práva súkromného,
- štátny dohľad nad exekútormi, notármi a ich komorami,
- kontrola dobrovoľných dražieb,
- zabezpečenie výkonu znaleckej, prekladateľskej a tlmočnickej činnosti,
- vydávanie Zbierky zákonov SR a Obchodného vestníka,
- zastupovanie SR na Európskom súde pre ľudské práva a pred Súdnyim dvorom EÚ
- zabezpečovanie plnenia úloh súvisiacich s členstvom SR v Eurojuste,

Pri analýze relevantnej legislatívy nemá zmysel z hľadiska predmetu tejto štúdie realizovateľnosti podrobnejšie analyzovať jednotlivé právne prepisy upravujúce špecifickú činnosť jednotlivých orgánov rezortu spravodlivosti. Z tohto dôvodu je legislatívna analýza zameraná prioritne na predpisy relevantné pre budovanie aplikačnej podpory pre realizáciu jednotlivých procesov, konkrétne budovaniu aplikačnej infraštruktúry a modulov spoločných pre jednotlivé agendy.

V rámci relevantnej legislatívy z hľadiska predmetu štúdie realizovateľnosti sú pre činnosť rezortu spravodlivosti dôležité predpisy podľa tabuľky č.2.

P.č.	Názov právneho predpisu
1	Zákon 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy;
2	Zákon č.71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov;
3	Zákon č. 145/1995 Z.z. o správnych poplatkoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;
4	Zákon č. 71/1992 Z.z. o súdnych poplatkoch v znení neskorších predpisov;
5	Zákon č. 305/2013 Z. z. o eGovernmente a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;
6	Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
7	Výnos MF SR č.55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy;
8	Zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov
9	Zákon 215/2002 Z. z. o elektronickom podpise v znení neskorších predpisov;
10	Vyhláška NBÚ č. 136/2009 Z. z. o spôsobe a postupe používania elektronického podpisu v obchodnom styku a administratívnom styku;
11	Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov;
12	Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov;
13	Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov;
14	Vyhláška NBÚ č. 338/2004 Z. z. o administratívnej bezpečnosti;
15	Zákon č.216/2007 Z. z. ktorým sa mení a dopĺňa zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.;
16	Výnos MV SR č. 525/2011 Z. z. o štandardoch pre elektronické informačné systémy na správu registratúry;

Tabuľka č.2 – legislatívny podklad

3.2 Aplikačná a dátová architektúra

3.2.1 Aplikácie

Rezort spravodlivosti disponuje rôznorodými informačnými systémami, z ktorých väčšina nie je z historických dôvodov centralizovaná a viazaná na zabezpečovanie výkonu konkrétnej agendy. Ich existencia je vo väčšine prípadov podmienená potrebou riešenia konkrétnej požiadavky. Sú postavené na technológiách, pre ktoré už viacerí výrobcovia v súčasnosti neposkytujú záruku ani podporu. Novšie informačné systémy sú síce prevádzkované centrálné, ale nespĺňajú kvalitatívne parametre, aká sa vyžadujú od riešení poskytovaných infraštruktúrou moderných dátových centier. V súčasnosti je realizovaných viacero projektov v rámci operačného programu Informatizácia spoločnosti, ktorých architektúra už zodpovedá súčasným požiadavkám, Ich vývoj a zdieľanie komponentov však taktiež nie sú dostatočným spôsobom koordinované z dôvodu zabezpečenia samostatnej funkčnosti týchto systémov.

Za rozvoj informačných systémov a ich prevádzku zodpovedá Sekcia informatiky a riadenia projektov Ministerstva spravodlivosti. Informačné systémy rezortu majú približne 6000 používateľov.

V minulosti bolo v rámci rezortu spravodlivosti realizovaných viacero projektov, ktorých stručný prehľad uvádzame v nasledujúcich častiach. V zásade je možné prevádzkované informačné systémy rozčleniť do nasledujúcich kategórií:

- systémy realizujúce prístupové body pre používateľov,
- systémy zabezpečujúce výkon špecializovaných agend rezortu spravodlivosti,
- systémy realizujúce výkon agend všeobecného charakteru.

Základné informačné systémy sú obsiahnuté v tabuľke č.3.

ID	Názov informačného systému	Kód z MetaIS	Počet používateľov	Stav
IS_01	Informačný systém súdov - Elektronická podateľňa	isvs_238	neobmedzene	prevádzkovaný a plánujeme rozvíjať
IS_02	Internetové služby rezortu spravodlivosti (IS RS)	isvs_239	neobmedzene	prevádzkovaný a plánujeme rozvíjať
IS_03	Informačný systém pre elektronický legislatívny proces	isvs_240	neobmedzene	prevádzkovaný a plánujeme rozvíjať
IS_04	Informačný systém súdov - Služby súdov	isvs_241	neobmedzene	prevádzkovaný a plánujeme rozvíjať
IS_05	Informačný systém súdov - Elektronický súdny spis	isvs_242	6000	prevádzkovaný a plánujeme rozvíjať

IS_06	Informačný systém súdov - Justičná pokladnica	isvs_243	100	prevádzkovaný a plánujeme rozvíjať
IS_07	Informačný systém súdov - Manažérske výstupy	isvs_244	6000	plánujeme vybudovať
IS_08	Informačný systém univerzálneho bezpečnostného úložiska súdnictva (UBÚS)	isvs_245	neobmedzene	plánujeme vybudovať
IS_09	Komplexný informačný systém na ekonomické a personálne agendy (KISEP)	isvs_246	6000	plánujeme vybudovať
IS_10	Administratívny informačný systém úradu ministerstva spravodlivosti (ADMIS-ÚMS)	isvs_247	250	plánujeme vybudovať
IS_11	Administratívny informačný systém Inštitútu vzdelávania (ADMIS-IV)	isvs_248	10	plánujeme vybudovať
IS_12	Administratívny informačný systém Justičnej akadémie (ADMIS-JA)	isvs_249	20	plánujeme vybudovať
IS_13	Výkazníctvo rezortu spravodlivosti a štatistické výstupy	isvs_250	neobmedzene	plánujeme vybudovať
IS_14	Informačný systém rezortného vzdelávania	isvs_251	3000	plánujeme vybudovať
IS_15	Register sudcov	isvs_252	neobmedzene	plánujeme vybudovať
IS_16	Register správcov konkurznej podstaty	isvs_253	20	prevádzkovaný a plánujeme rozvíjať
IS_17	Register úpadcov	isvs_254	neobmedzene	plánujeme vybudovať
IS_18	Informačný systém súdov - Súdny manažment	isvs_255	6000	prevádzkovaný a plánujeme rozvíjať
IS_19	Elektronická zbierka zákonov	isvs_258	10000	plánujeme vybudovať
IS_20	Register znalcov, tlmočníkov a prekladateľov	isvs_260	20	prevádzkovaný a plánujeme rozvíjať

IS_21	Register prekladateľov	isvs_261	20	prevádzkovaný a plánujeme rozvíjať
IS_22	Register tlmočníkov	isvs_262	neobmedzene	prevádzkovaný a plánujeme rozvíjať
IS_23	Portál právnych informácií JASPI	isvs_264	neobmedzene	prevádzkovaný a plánujeme rozvíjať
IS_24	Elektronické služby monitoringu obvinených a odsúdených osôb (ESMO)	isvs_5346	neobmedzene	plánujeme vybudovať
IS_25	Videokonferencie	isvs_5582	neobmedzene	plánujeme vybudovať
IS_26	Centrálna evidencia exekúcií	isvs_5583	20	plánujeme vybudovať
IS_27	Portál právnych informácií- Rozvoj projektu IS SLOV-LEX	isvs_5839	neobmedzene	plánujeme vybudovať
IS_28	Informačný systém registra úpadcov	isvs_5840	neobmedzene	plánujeme vybudovať

3.2.1.1 Systémy realizujúce prístupové body pre používateľov

Do tejto kategórie prevádzkovaných systémov patria:

- portál Ministerstva spravodlivosti,
- ÚPVS,
- Intranetový portál.

3.2.1.1.1 Portál Ministerstva spravodlivosti

Portál Ministerstva spravodlivosti (www.justice.gov.sk) poskytuje rozhranie pre poskytovanie informácií z rezortu spravodlivosti:

- organizácia a služby Ministerstva spravodlivosti,
- povinne zverejňované informácie,
- informácie o súdoch, pojednávaniach a súdnych rozhodnutiach,
- registre v pôsobnosti rezortu spravodlivosti, vrátane možnosti vyhľadávania v nich (Obchodný register, register znalcov, tlmočníkov a prekladateľov a pod.).

Z tohto portálu sú dostupné služby ďalších informačných systémov:

- JASPI - portál jednotného informačného systému právnych informácií,
- Obchodný register – www.orsr.sk. Tento portál umožňuje vyhľadávať vybrané údaje o zapísaných osobách v obchodnom registri. Jeho nevýhodou je iba informatívny charakter výpisov,

- Portál právnych predpisov – JISS. Umožňuje podrobné sledovanie prebiehajúceho legislatívneho procesu, vyhľadávanie materiálu a sprievodnej dokumentácie. Počas fázy pripomienkovacieho konania je možné cez portál zadávať pripomienky k legislatívnemu materiálu.

3.2.1.1.2 ÚPVS

ÚPVS predstavuje aj v súčasnosti prístupový bod pre využívanie vybraných elektronických služieb poskytovaných rezortom spravodlivosti:

- služby podaní pre služby Obchodného registra,
- služby podaní pre eŽaloby.

Tieto služby sprístupnené cez ÚPVS sú integrované na systém elektronickej podateľne, ktorá zabezpečuje ďalšie spracovanie takýchto podaní v súlade s príslušnou legislatívou.

3.2.1.1.3 Intranetový portál

Predstavuje vnútorné integrujúce informačné prostredie Ministerstva spravodlivosti, ktoré umožňuje spoluprácu prostredníctvom webového rozhrania, tvoriaceho informačný základ pre zverejňovanie údajov na internete pre interné účely rezortu.

3.2.1.2 Systémy zabezpečujúce výkon špecializovaných agend rezortu spravodlivosti

Do tejto kategórie prevádzkovaných systémov patria:

- obchodný register,
- súdny manažment,
- systém JASPI,
- systém JISS,
- interné registre a evidencie.

3.2.1.2.1 Obchodný register (Informačný systém súdov – služby súdov)

Obchodný register predstavuje zákonom definovanú evidenciu, do ktorej sa zapisujú zákonom stanovené údaje týkajúce sa podnikateľov, prípadne iných zákonom stanovených osôb. Je to prvý register, ktorý bol vedený a sprístupňovaný verejnosti v elektronickej forme.

V registri publikovanom na Internete je možné vyhľadávať podľa definovaných parametrov. Takto publikované informácie však nemajú právne záväzný charakter, je ich možné použiť iba na informatívne účely.

Systém Obchodného registra pozostáva z nasledujúcich súčastí:

- OR – CORWIN (obchodný register na súdoch) je prevádzkovaný centrálné na MS SR,

- OR – Dátová pumpa, prostredníctvom ktorej sa cez rozhranie webových služieb orgánom štátnej správy publikujú údaje z obchodného registra. Databáza pre dátovú pumpu je kópiou databázy OR-CORWIN,
- OR – eZBI je aplikácia, ktorá funguje na báze klient/server (hrubý klient) a zabezpečuje evidenciu a sprístupnenie dokumentov vedených v zbierke listín,
- OR – eSlužby – zabezpečuje rozhranie na ÚPVS, na ktorom sú elektronické služby publikované.

3.2.1.2.2 Súdny manažment (Informačný systém súdov – Elektronická podateľňa)

Tento projekt sa začal realizovať už v roku 1999 a adresoval nasledujúce oblasti v rezorte spravodlivosti:

- zaviesť protikorupčné opatrenia a zvýšiť transparentnosť súdnictva,
- odbremeniť sudcov od administratívnych úkonov a zrýchliť súdne konanie,
- zvýšiť dôveru občanov v súdnictva a zlepšiť vymożiteľnosť práva.

V rámci projektu bol nasadený systém "Podateľňa", ktorý zabezpečuje náhodné prideľovanie spisu. Tento systém umožňuje evidenciu súdneho spisu v elektronickej podobe a sledovanie obehu súdneho spisu počas jeho životného cyklu. Elektronický súdny spis však v slovenskom súdnictve absentuje.

Systém bol nasadený na všetky okresné a krajské sudy v Slovenskej republike. Od roku 2006 okresné a krajské sudy zverejňujú rozhodnutia v občianskoprávných a civilných veciach na Internete. Rovnako rozhodnutia na svojich stránkach zverejňuje aj Ústavný súd a Najvyšší súd.

3.2.1.2.3 Systém JASPI (Portál právnych informácií JASPI)

Systém JASPI (Jednotný automatizovaný systém právnych informácií) je nekomerčný zdroj právnych informácií v štáte. Pôvodne bol systém využívaný iba orgánmi verejnej moci, neskôr bol sprístupnený aj verejnosti.

Systém predstavuje databázu pre portál, prostredníctvom ktorého sa sprístupňujú informácie. Tieto informácie však nie sú právne záväzné, nakoľko oficiálnym publikačným médiom záväzných právnych informácií je Zbierka zákonov v listinnej podobe. Systém JASPI tiež umožňuje vyhľadávanie v registroch znalcov, tlmočníkov a prekladateľov a vyhľadávanie judikatúry a súdnych rozhodnutí.

3.2.1.2.4 Systém JISS (Informačný systém pre elektronický legislatívny proces)

Jednotný IS na sledovanie legislatívneho procesu (JISS) obsahuje portál právnych predpisov. Prácu s novelizovanými predpismi a tvorbu nových predpisov uľahčuje pracovníkom legislatívnych odborov editor právnych predpisov.

3.2.1.2.5 Interné evidencie

Interné registre a evidencie zabezpečujú evidenciu vybraného druhu údajov a ich sprístupňovanie oprávneným používateľom. Jedná sa najmä o register znalcov, tlmočníkov a prekladateľov.

3.2.1.3 Systémy realizujúce výkon agend všeobecného charakteru.

Do tejto kategórie prevádzkovaných systémov patria:

- interné registre a evidencie,
- registratúrna kniha,
- personálna agenda.

3.2.1.3.1 Interné registre a evidencie

Interné registre a evidencie zabezpečujú evidenciu vybraného druhu údajov a ich sprístupňovanie oprávneným používateľom. Jedná sa najmä o:

- Centrálna evidencia zmlúv - webová aplikácia, prostredníctvom ktorej sa vykonáva evidencia zmlúv,
- Evidencia objednávok - webová aplikácia, prostredníctvom ktorej sa vykonáva operatívna objednávok a umožňuje sa sledovanie ich stavov.

3.2.1.3.2 Registratúrna kniha

Predstavuje klient/server aplikáciu, ktorá umožňuje správu spisovej agendy Ministerstva spravodlivosti prostredníctvom vykonávanie elektronických registratúrnych zápisov. Aplikácia je riešená prostredníctvom architektúry tenkého klienta a centrálnej server aplikácie.

3.2.1.3.3 Personálna agenda

Personálna agenda je zabezpečovaná systémom Humanet. Predstavuje klient/server aplikáciu, ktorej centrálna databáza je umiestnená na Ministerstve spravodlivosti sa pristupuje k nej prostredníctvom webového rozhrania.

3.2.1.4 Novo budované systémy v rámci projektov OPIS

Tieto systémy implementujú prierezovo jednotlivé oblasti, nakoľko je požadovaná ich samostatná a nezávislá funkčnosť.

3.2.1.4.1 Elektronická zbierka zákonov

Tento systém podporuje proces tvorby a publikovania legislatívy, t.j. podporuje legislatívny tok ktorý sprístupňuje pre všetky zainteresované subjekty, ako aj pre verejnosť.

3.2.1.4.2 Elektronické služby monitoringu obvinených a odsúdených

Systém predstavuje agendový systém pre probáciu a mediáciu. Jeho hlavnú časť tvoria agendy monitorovania odsúdených, ako aj agendy zabezpečujúce administráciu tohto procesu.

3.2.1.4.3 Rozvoj elektronických služieb súdnictva

V rámci projektu Rozvoj elektronických služieb súdnictva sa buduje univerzálne bezpečné a dôveryhodné úložisko („archív súdnictva“), technická infraštruktúra videokonferencií pre informačné systémy rezortu, ktoré zabezpečujú elektronické služby pre občanov, podnikateľov a orgány verejnej moci.

3.2.2 Využívanie modulov plánovanej aplikačnej a bezpečnostnej architektúry existujúcimi systémami

Aplikačná a bezpečnostná platforma v zmysle tejto štúdie obsahuje nasledujúce základné súčasti:

- integračná platforma, vrátane integračných rozhraní na okolité systémy a registre
- systém správy používateľov a ich oprávnení (IAM),
- PKI infraštruktúra pre zabezpečenie procesov autorizácie úkonov a komunikácie
- bezpečnostná infraštruktúra zabezpečujúca implementáciu bezpečnostnej politiky a monitorovanie stavu bezpečnosti.

V nasledujúcej tabuľke je uvedené zhrnutie začlenenia jednotlivých modulov aplikačnej architektúry v jednotlivých prevádzkovaných a budovaných systémoch rezortu spravodlivosti.

	Integračná platforma	Integrácia na el. Schránky	Správa používateľov	PKI infraštruktúra	Bezpečnosť a monitorovací systém
Portál MS SR					
JASPI					
Obchodný register	Interná	X		Spracovanie podaní	

eŽaloby	Interná	X		Spracovanie podaní	
Súdny manažment			Interná		
IS Zboru väz. A just. stráže			Interná		
Interné registre a evidencie			Interná		
Registratúrna kniha			Interná		
Personálna agenda			Interná		
eZbierka	Interná		Interná	Autorizácia publikovanej legislatívy	
ESMO	Interná	X	Interná	Autorizácia interných úkonov	Vybrané atribúty
RES			Interná		

3.2.3 Dátová architektúra

Správy a ukladania dát v rezorte spravodlivosti je decentralizovaný a nie je vybudované žiadne dátové centrum štandardných parametrov. Nie sú ani využívané žiadne služby dátových centier iných rezortov verejnej správy alebo iných poskytovateľov. Využívajú sa priestory spĺňajúce iba minimálne bezpečnostné a prevádzkové požiadavky.

Novšie informačné systémy rezortu spravodlivosti sú síce prevádzkované centrálné, ale nie spôsobom zodpovedajúcim procesom dátového centra. Pri zálohovaní dát je riešené výhradne zálohovanie pre danú lokalitu, bez aktívnej výmeny dát medzi ostatnými lokalitami. Nie sú k dispozícii žiadne zariadenia na centralizovanú správu a ukladanie údajov, nakoľko tieto sa ukladajú na lokálne disky.

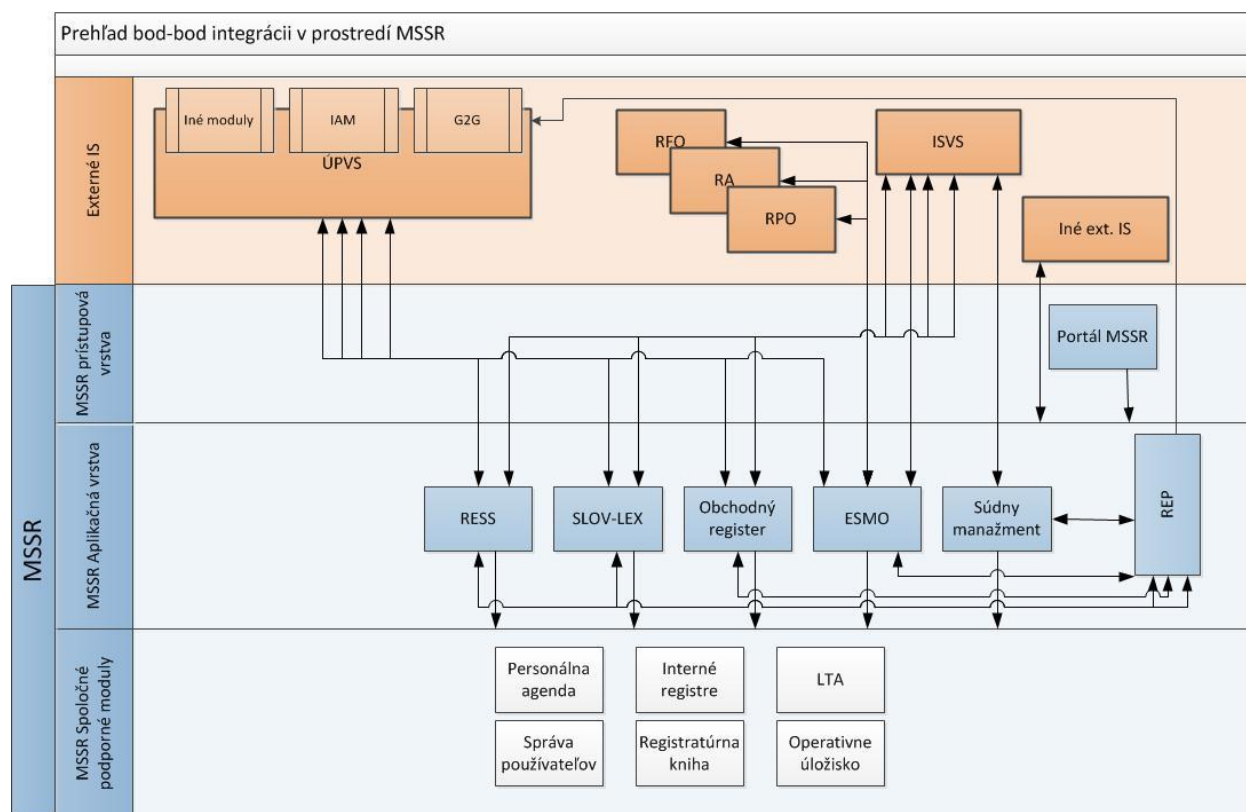
Na miestnej úrovni sa nachádza časť infraštruktúry týchto aplikácií spolu s lokálnou kópiou databázy. Z Okresných a Krajských súdov sa replikuje časť dát o konaniach na úložisko Ministerstva spravodlivosti. Na Krajských a Okresných súdoch je umiestnených 63 serverov pre aplikáciu Súdneho manažmentu a 63 serverov pre aplikáciu Súdno-trestnej agendy. Veľkosť databáz týchto aplikácií siaha rádovo do 10 GB údajov. Na centrálnej úrovni, v sídle Ministerstva spravodlivosti je umiestnený centrálny server databázy Obchodného registra. Veľkosť databáz obchodného registra dosahuje stovky GB, celkovo sa blíži k 1TB údajov.

V súčasnosti registrové súdy archivujú listiny v Zbierke listín v papierovej podobe. V prípade požiadavky je pre daný dokument realizovaný prevod do elektronickej formy.

Ministerstvo spravodlivosti výhradne spravuje a prevádzkuje databázy pre centrálné aplikácie a evidencie:

- JASPI
- obchodný register
- portál právnych predpisov
- registre správcov, znalcov, tlmočníkov a prekladateľov,
- centrálna evidencia zmlúv
- evidencia objednávok
- registratúrna kniha

3.2.4 Integračná architektúra



Obr. 1 Aktuálny stav integrácií systémov

V existujúcom stave sa vyskytujú opakované integrácie na interné ako aj externé IS, pričom tieto integrácie sú opakovane realizované v jednotlivých agendových systémoch rôznymi dodávateľmi na rôznych platformách. Okrem technickej realizácie sú rovnako duplikované procesy spojené s komunikáciou na IS uvedené na obrázku.

Táto forma integrácie bod-bod je neefektívna z pohľadu dodávky jednotlivých projektov, ďalšieho rozvoja a prevádzky ako aj z pohľadu governance integrácii v rezorte MSSR.

3.2.4.1 Integrácia interných systémov

V súčasnosti neexistuje jednotný koncept integrácie systémov v rezorte spravodlivosti. Integrácia systémov (ak taká existuje) je vykonávaná na báze asynchrónnej výmeny dát.

3.2.4.2 Integrácia na centrálné komponenty v rámci IS VS

V súčasnosti je realizovaná integrácia na ÚPVS pri spracovaní podaní do agendy Obchodného registra a ežaloby. Podania sú vytvárané na ÚPVS a následne sú zasielané na rozhranie elektronickej podateľne MS SR.

Integrácia s ďalšími komponentmi ÚPVS nie je realizovaná.

3.2.4.1 Integrácia na iné ISVS

Integrácia s inými ISVS je realizovaná na úrovni poskytovania dát (napr. dátová pumpa pri agende Obchodného registra).

3.3 Vyhodnotenie súčasného stavu

Na základe vyššie uvedenej analýzy skutočného stavu budovania jednotnej aplikačnej architektúry a integračnej platformy rezortu spravodlivosti je možné identifikovať nasledujúce problémy:

- veľký počet organizačných jednotiek v rezorte, z ktorých väčšina prevádzkuje vlastný informačný systém a zabezpečuje jeho vývoj a prevádzku viacerými prostriedkami,
- prevažne distribuované nasadenie systémov – systémy sú nasadzované vo väčšine distribuovane (samostatne na jednotlivých organizačných zložkách), iba niekoľko systémov bolo centralizovaných (napr. OR SR). To spôsobuje problémy so zabezpečením prevádzky týchto systémov a výrazné zaťaženie existujúcich ľudských zdrojov a súčasne aj neefektívne využitie technického vybavenia
- chýbajú formalizované IT procesy a rizikom je aj decentralizovaný spôsob ukladania dát,
- nízky stupeň integrácie systémov do interných procesov – jednotlivé systémy sú vyvíjané a nasadené samostatne, bez jasnej koncepcie ich efektívnej integrácie, ktorá môže zefektívniť interné komunikačné procesy a zdieľanie informácií,
- problémy so zabezpečením centralizovanej prevádzky existujúcich centrálnych systémov – absencia záložného výpočtového centra, bezpečnostných prvkov a pod.
- riziká spojené s existujúcim spôsobom prevádzky – distribuovaná prevádzka si vyžaduje väčšie ľudské zdroje na jej zabezpečenie a zvyšuje bezpečnostné riziko (napr. z dôvodu problematického vynucovania dodržiavania bezpečnostnej politiky),
- neexistencia centrálného systému správy používateľov s dôsledkom na zvýšenie náročnosti prevádzky takéhoto systému a súvisiacimi bezpečnostnými rizikami,

- neexistencia centrálnej bezpečnostnej politiky, prevádzky centralizovaných bezpečnostných prostriedkov a vyhodnocovania bezpečnostnej situácie v rezorte.
- neexistencia bezpečného spôsobu prehliadania elektronického súdneho spisu internými používateľmi zo vzdialených pracovísk znižuje efektivitu práce so súdnym spisom, ani v off-line režime

Z hľadiska posudzovania súčasného stavu je potrebné zohľadniť aj úlohy a výzvy, ktoré pred rezortom spravodlivosti stoja v celoslovenskom kontexte informatizácie verejnej správy a v kontexte pripravovanej legislatívy o elektronickom výkone verejnej moci:

- zabezpečenie výkonu verejnej moci elektronickým spôsobom a vytvorenie podmienok pre elektronickú komunikáciu – schválený Zákon o eGovernmente ukladá všetkým orgánom verejnej moci vykonávať verejnú moc aj elektronicky, t.j. elektronicky komunikovať s používateľmi služieb a s inými orgánmi verejnej moci, ako aj vykonávať všetky úkony elektronicky. Tomuto musí byť prispôbená aj architektúra informačného systému a napojenie na realizovanie výkonu verejnej moci.
- zefektívnenie výkonu verejnej moci – z hľadiska výkonu verejnej moci je dôraz kladený na efektívnosť verejnej správy. Z pohľadu procesov to znamená automatizáciu a integráciu jednotlivých procesov, t.j. vytváranie interných procesov integrujúcich služby a funkcie viacerých informačných systémov v rezorte spravodlivosti.
- zabezpečenie prístupu k referenčným registrom – z hľadiska zníženia administratívneho zaťaženia občanov a podnikateľských subjektov, aj z hľadiska zefektívnenia výkonu verejnej moci, je kľúčovým aspektom zdieľanie poskytovanie údajov spravovaných jednotlivými orgánmi verejnej moci – referenčných údajov v referenčných registroch. Z hľadiska úloh rezortu MS SR sa jedná najmä o sprístupňovanie údajov z Obchodného registra elektronickým a právne záväzným spôsobom, ako aj o využívanie údajov iných referenčných registrov v procesoch výkonu verejnej moci v rezorte MS SR.
- zabezpečenie prístupu k informáciám v rámci jednotlivých agend pre oprávnených používateľov, či je možné dosiahnuť „otvorenie“ systému justície verejnej kontrole, ako aj zefektívneniu procesov a zníženiu administratívy jednotlivých subjektov (napr. advokáti pri prístupe k obsahu elektronického súdneho spisu),
- zefektívnenie využitia finančných prostriedkov určených na informatizáciu rezortu – možnosť prevádzky informačnej podpory procesov vykonávaných v rezorte aj pri predpokladanom tlaku na znížovanie nákladov,
- zabezpečenie efektívnej prevádzky existujúcich systémov a bezpečnosti v kontexte zvýšených rizík vyplývajúcich s praktickou implementáciou konceptu eJustice.

Na základe pravidelnej bezpečnostnej analýzy, ktorú vykonal NASES na prevádzkovanom riešení – spoločné moduly ÚPVS (modul IAM), boli identifikované nasledujúce problémy:

- komunikačné rozhranie medzi referenčnou databázou identít a komponentmi modulu IAM – potreba zaistiť vyššiu úroveň bezpečnosti na úrovni komunikačných rozhraní,

- prístup k dátam uložených v referenčnej databáze identít - aktuálna štruktúra dát neumožňuje nastavenie požadovanej granularity oprávnení na jednotlivé typy uložených objektov (fyzické osoby, právnické osoby, inštitúcia, zamestnanec VS).

4 Popis cieľového stavu

4.1 Legislatívna analýza

Z hľadiska predmetu štúdie realizovateľnosti postačuje existujúca legislatívna báza, nie je potrebný žiadny návrh na zmenu legislatívy.

Predmet štúdie realizovateľnosti je plne v súlade s existujúcou legislatívou.

4.2 Analýza požiadaviek a potrieb aktérov/stakeholderov

Aktér/stakeholder – jednotlivec, tím alebo organizácia majúca kľúčovú rolu, resp. určité kľúčové záujmy v rámci vytvárania architektúry, ktoré sa môžu týkať všetkých aspektov v systéme fungovania, vývoja, alebo prevádzky, vrátane úvah, ako sú výkon, spoľahlivosť, bezpečnosť a pod. Aktér môže byť reprezentovaný napr. vedením organizácie, projektovými manažérmi, používateľmi, architektmi riešení a pod.).

Cieľový stav prináša do systému aj rozšírenie čo sa týka aktérov a cieľových skupín, pričom vytvorí nové skupiny používateľov z radov verejnej správy ako aj verejnosti. Analýzu ich požiadaviek ako východisko pre analýzu možností riešenia cieľového stavu uvádzame v nasledovnom prehľade.

Tabuľka 5 Analýza požiadaviek aktérov

Požiadavky a potreby občanov a podnikateľov (nešpecializovaní používatelia)	<ul style="list-style-type: none"> (1) Poskytovanie komplexných elektronických služieb v súlade s potrebami používateľov, organizovaných na základe konceptu životných situácií (2) Sprístupnenie informácií a služieb v súlade s oprávneniami používateľa (3) Zníženie administratívnej záťaže a možnosť plnohodnotnej elektronickej komunikácie
Požiadavky a potreby špecializovaných používateľov (notári, advokáti, exekútori a pod.)	<ul style="list-style-type: none"> (4) Efektívne poskytovanie komplexných elektronických služieb v súlade s potrebami špecializovaných používateľov (5) Sprístupnenie informácií a služieb v súlade s oprávneniami používateľa (6) Zníženie administratívnej záťaže a možnosť plnohodnotnej elektronickej komunikácie (7) Zvýšenie komfortu práce (napr. odstránením viacnásobného prihlasovania, integráciou služieb a pod) (8) Zvýšenie bezpečnosti
Požiadavky a potreby MS SR a ostatných inštitúcií verejnej správy	<ul style="list-style-type: none"> (9) Každodenná použiteľnosť elektronických služieb a ich vysoká dostupnosť výstupov (10) Centralizovaná správa všetkých používateľov (interní, externí) a riadenie ich

	<p>oprávnení na základe role používateľa, resp. organizačného zaradenia</p> <p>(11) Vytvorenie jednotnej platformy zabezpečujúcej efektívnu integráciu systémov a agiend realizovaných v rámci konceptu eJustice</p> <p>(12) Zvýšenie bezpečnosti prevádzkovaných systémov</p> <p>(13) Zefektívnenie spôsobu prevádzky a podpory používateľov</p> <p>(14) Systémová podpora</p> <p>(15) Zlúčenie služieb</p> <p>(16) Zlepšenie prístupu k informáciám a toku informácií bez zníženia bezpečnosti</p> <p>(17) Umožnenie práce interným používateľom (najmä sudcom) zo vzdialených pracovísk (aj off-line režim) bez ohrozenia bezpečnosti citlivých informácií</p>
Požiadavky a potreby tretích zainteresovaných strán	<p>(18) Zvýšenie kvality a komplexnosti poskytovaných služieb</p> <p>(19) Vytvorenie integračných rozhraní pre integráciu systémov tretích strán</p>
Požiadavky zúčastnených strán (MS SR, NASES) na spoločné moduly ÚPVS (modul IAM)	<p>(20) Zvýšenie výkonnosti prostredia pre prácu s 5 mil. identitami.</p> <p>(21) Optimalizácia vnútorného fungovania služieb, podľa doporučených postupov a praktík vybranej technológie.</p> <p>(22) Optimalizácia štruktúry uložených dát, s dôrazom na ďalší rozvoj a udržateľnosť riešenia.</p> <p>(23) Zvýšenie bezpečnosti riešenia, povýšenie produktov na poslednú aktuálnu verziu, aplikácia posledných bezpečnostných záplat.</p>

4.3 Architektúra navrhovaného riešenia

4.3.1 Formulovanie cieľov

Rezort spravodlivosti v súčasnosti implementuje systém eJustice, ako jednu zo svojich základných priorít. Dosiahnutie tohto cieľa je však podmienené vybudovaním bezpečnostných a architekturných predpokladov, ktoré umožnia efektívnu implementáciu tohto zámeru a najmä zachovanie požadovanej úrovne bezpečnosti procesov a poskytovaných služieb.

Systém eJustice a takisto Projekt budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR využije v maximálnej možnej miere novovybudovanú budovu DataCentra na Kopčianskej ulici.

Z hľadiska naplňovania zámeru konceptu eJustice je možné formulovanie nasledujúcich základných východísk:

- **sprístupnenie elektronických služieb a informácií oprávneným používateľom** – za týmto účelom je nevyhnutné zabezpečovať evidenciu jednotlivých používateľov, realizovať procesy ich autentifikácie a autorizácie k jednotlivým funkciám a informáciám všetkých agendových informačných systémov. V súčasnosti každý z nasadených systémov zabezpečuje samostatne vlastnú evidenciu používateľov a informácie o oprávneniach využívaných pre riadenie prístupu k službám a informačným zdrojom danej aplikácie.
- **poskytovanie komplexných služieb oprávneným používateľom** – napriek tomu, že MS SR prevádzkuje jednotlivé agendové informačné systémy pre zabezpečenie jednotlivých agend, používatelia vyžadujú prierezový pohľad na uchovávané informácie a komplexné zabezpečovanie ich požiadaviek. Takýto prístup však presahuje možnosti jednotlivých samostatných agendových systémov a vyžaduje si procesnú a informačnú integráciu jednotlivých systémov do komplexných služieb.
- **zabezpečenie plnohodnotnej obojsmernej elektronickej komunikácie pri výkone agend** – koncept eJustice predpokladá plnohodnotnú elektronickejšiu realizáciu všetkých procesov rezortu spravodlivosti. To vyžaduje aj na strane riešení rezortu spravodlivosti vytvoriť podmienky nielen pre príjem podaní a žiadostí v elektronickej forme, ale taktiež vytvorenie podmienok na autorizáciu úkonov a komunikácie tak, aby tieto mohli byť plnohodnotne použité v elektronickej komunikačnej procesovej službe.
- **zabezpečenie efektívnej prevádzky informačných systémov** – vzhľadom na rozsah plánovaných informačných systémov a dostupné zdroje použiteľné pre ich prevádzku bude potrebné centralizovať a automatizovať jednotlivé prevádzkové procesy.
- **zabezpečenie plnenia bezpečnostnej politiky** – fungovanie konceptu eJustice je podmienené vytvorením bezpečnostných predpokladov, ktoré výrazným spôsobom znížia bezpečnostné riziká spojené s elektronizáciou procesov rezortu a ich sprístupnenia verejnosti. Toto vyžaduje nielen nasadenie prostriedkov na plnenie bezpečnostnej politiky, ale aj monitorovacích nástrojov umožňujúcich „ex-post“ identifikovať prieniky a prijímať opatrenia na ich zamedzenie.
- **vybudovanie infraštruktúry na bezpečné prehliadanie súdneho spisu** – pre zavedenie konceptu eJustice do prevádzky je potrebné, aby interní používatelia (najmä sudcovia) mohli pracovať s elektronickej súdny spisom kdekoľvek, vrátane vzdialených pracovísk. Na tento účel je potrebné vybudovať infraštruktúru, ktorá umožňuje týmto používateľom prehliadať elektronickej súdny spis cez zabezpečený kanál z tabletov alebo osobných počítačov. Tomu je potrebné prispôbiť aj infraštruktúrne vybavenie, najmä výmenou starých zariadení (PC) za nové zariadenia (PC), ktoré podporujú novšiu verziu operačného systému Windows. Existujúce zariadenia prevádzkované na operačnom systéme Windows XP už nie je už možné zabezpečiť, pretože Microsoft ako výrobca

ukončil bezpečnostnú podporu pre Windows XP a teda preň nevytvára bezpečnostné aktualizácie. Na prehliadanie elektronického súdneho spisu je potrebné obstaráť tablety, ktoré sudcom umožnia zefektívniť prácu s elektronickým súdnym spisom tak, že umožnia jeho bezpečné prehliadanie aj zo vzdialených pracovísk (aj off-line režim).

Na základe takto formulovaných východísk je možné z hľadiska budovania infraštruktúry pre koncept eJustice pre túto štúdiu realizovateľnosti vytýčiť nasledujúce ciele:

- **vybudovanie integračnej platformy** – táto integračná platforma sa stane základom pre integráciu jednotlivých informačných systémov do procesov poskytovania komplexnejších služieb, ako aj pre integráciu s ÚPVS a ostatnými ISVS. Integrácia informačných systémov zabezpečujúca výmenu dát a implementáciu komplexných procesov bude realizovaná prostredníctvom integračnej platformy a nie vzájomným prepájaním integráciou jednotlivých systémov navzájom.
- **vybudovanie systému správy používateľov** - evidencia používateľov a ich oprávnení bude budovaná ako centrálna, čím bude zabezpečená jednotná evidencia používateľov, ich autentifikácia a správa ich oprávnení pre všetky systémy konceptu eJustice. Tieto informácie budú využívané jednotlivými informačnými systémami priamo (t.j. poskytovanie údajov o autentifikovanom používateľovi a jeho oprávneniach jednotlivým systémom), alebo sprostredkované (identity provisioning, t.j. replikácia údajov o používateľoch a ich oprávneniach do evidencií týchto systémov).
- **vybudovanie PKI infraštruktúry** – PKI infraštruktúra je potrebná pre implementáciu procesov autorizácie úkonov vykonávaných v interných agendách v zmysle požiadaviek legislatívy, ako aj pre zvýšenie osobnej zodpovednosti používateľov v oblastiach, kde sa autorizácia jednotlivých krokov spracovania agendy legislatívne explicitne nevyžaduje.
- **nasadenie bezpečnostnej infraštruktúry** – nasadenie prostriedkov pre implementáciu bezpečnostných opatrení, ako aj pre monitorovanie bezpečnostnej situácie v celom prevádzkovom prostredí informačných systémov rezortu spravodlivosti.
- **nasadenie prostriedkov pre podporu prevádzkových činností** – zabezpečenie automatizácie a podpory jednotlivých prevádzkových činností z cieľom zefektívnenia celého prevádzkového prostredia a podpory používateľov.

Pri návrhu a budovaní integračnej a bezpečnostnej infraštruktúry je súčasne potrebné zohľadniť skutočnosť, že koncept eJustice nebude implementovaný ako jednorazové riešenie, ale že jeho budovanie bude predstavovať dlhodobý proces. Preto aj integrácia súčastí integračnej a bezpečnostnej infraštruktúry na jednotlivé agendové systémy bude postupná.

4.3.2 Očakávané prínosy

Vyššie uvedené princípy zavedú kvalitatívne nový stav v procese budovania a nasadzovania jednotlivých systémov podporujúcich koncept eJustice. Základné prínosy zavedenia navrhovanej aplikačnej a integračnej architektúry je možné zhrnúť nasledovne:

- **zníženie nákladov na budovanie elektronických služieb a procesov** – využívanie princípov integračnej platformy vytvára nové podmienky pre integráciu aplikácií a budovanie novej kategórie služieb, ktorá sa deje centrálna a riadene. Integračná platforma poskytuje flexibilitu z hľadiska budúceho rozširovania portfólia prevádzkovaných aplikácií a ich prepájania, ako aj definovania procesov nad aplikáciami. Súčasne prináša úspory z hľadiska integrácie, nakoľko nie je potrebné systémy integrovať navzájom (t.j. zabezpečiť integráciu všetkých so všetkými) ale postačuje systém integrovať na integračnú platformu.
- **zvýšenie bezpečnosti systémov a ich prevádzky** – nasadenie bezpečnostnej infraštruktúry vytvára aj predpoklady pre plné naplnenie zámerov v oblasti zabezpečenia jednotlivých systémov, ktoré sú základným predpokladom pre realizáciu konceptu eJustice. Tieto prostriedky zabezpečia:
 - centralizovaná správa používateľov a ich oprávnení,
 - centralizované vynucovanie bezpečnostnej politiky,
 - možnosť uplatnenia unifikovaných (centralizovaných) bezpečnostných mechanizmov pre všetky aplikácie
 - centralizované riadenie bezpečnosti (autentifikačné predmety, oprávnenia) so zamedzením vplyvu lokálnych vzťahov
 - centrálna monitorovanie bezpečnosti, vyhodnocovanie bezpečnostných incidentov a ich riešenie.
- **efektívnejšia prevádzka** – nasadenie podporných prostriedkov umožní zefektívniť a zautomatizovať procesy prevádzky jednotlivých systémov začleňovaných do konceptu eJustice.
- **zvýšenie transparentnosti** procesov v rezorte spravodlivosti s cieľom otvorenia justície verejnej kontrole.

4.3.3 Popis služieb na biznis úrovni

Informačné systémy rezortu spravodlivosti realizujú funkčnosť potrebnú pre zabezpečenie výkonu jednotlivých agend. Popri tejto funkčnosti je potrebné na úrovni biznis architektúry zabezpečiť nasledujúcimi eGov službami:

- zabezpečenie prístupu k službe alebo informáciám pre oprávneného interného používateľa
 - služba je určená pre interných používateľov, t.j. pracovníkov jednotlivých orgánov v rezorte spravodlivosti
 - predpokladá sa jednotný systém autentifikácie interných používateľov, ktorý nie je viazaný na používanie eID karty,
 - po autentifikácii je sprístupnená identita a jeho organizačné zaradenie, ktoré základom pre určenie jeho role a prístupových práv k funkciám jednotlivých agendových systémov,
 - bezpečný prístup k informáciám zo vzdialených pracovísk pomocou zabezpečeného kanála (prehliadanie elektronického súdneho spisu oprávnenými internými používateľmi z jednoúčelového tabletu)

- služba je typu G2E.
- zabezpečenie prístupu k službe alebo informáciám pre oprávnenému špecializovaného používateľa
 - služba je určená pre špecializovaných používateľov - notárov, exekútorov, advokátov, a pod.
 - služba vyžaduje spôsob autentifikácie prostredníctvom eID karty,
 - služba sprístupní identitu špecializovaného používateľa a v prípade potreby aj organizáciu, za ktorú používateľ koná,
 - pre špecializovaných používateľov služba určuje ich oprávnenia pre prístup k „neverejným“ službám agendových informačných systémov, t.j. k funkciám ktoré nie sú určené pre verejnosť
 - služba je typu G2C resp. G2B.
- zabezpečenie prístupu k službe alebo informáciám pre oprávnenému nešpecializovaného používateľa
 - služba je určená pre nešpecializovaných používateľov, t.j. pre občanov a komerčné subjekty využívajúce nešpecializované služby rezortu spravodlivosti
 - služba vyžaduje spôsob autentifikácie prostredníctvom eID karty,
 - služba je typu G2C, resp. G2B
- poskytnutie integrovanej elektronickej služby
 - integrovaná elektronická služba je služba, ktorá nie je priamo poskytovaná agendovými systémami, ale je „vyskladaná“ zo služieb jednotlivých agendových systémov. Integrovaná služba v súlade s princípom živostných situácií reaguje na požiadavku používateľa a snaží sa ju naplniť integráciou dielčích služieb, t.j. virtualizuje prostredie jednotlivých agend (agendových systémov) od pohľadu používateľa na jeho funkcie

Vyššie eGov služby sú následne viazané na IT služby uvedené v nasledujúcej tabuľke:

eGov služba (Biznis úroveň)	IS služba (Úroveň informačných systémov)
zabezpečenie prístupu k službe alebo informáciám pre oprávneného <ul style="list-style-type: none"> • interného používateľa • špecializovaného používateľa • nešpecializovaného používateľa 	Registrácia používateľa do systému centrálnej správy používateľov
	Zabezpečenie centrálnej správy používateľov pre agendové systémy
	Centrálna identifikácia a autorizácia používateľov pre agendové systémy
	Riadenie prístupov k informačným zdrojom a funkciám informačných systémov pre agendové systémy

eGov služba (Biznis úroveň)	IS služba (Úroveň informačných systémov)
Poskytnutie integrovanej elektronickej služby	Monitorovanie a audit poskytovania správy používateľov a riadenia prístupu pre agendové systémy
	Vydanie autorizačných údajov pre používateľa
	Vykonanie autorizácie úkonu používateľom
	Identifikácia a manažment služieb vystavených na integračnej platforme
	Manažment životného cyklu služieb vystavených na integračnej platforme
	Definovanie business procesu na integračnej platforme
	Realizácia business procesu na integračnej platforme
	Monitorovanie business procesov na integračnej platforme

4.3.4 Využitie cloudového riešenia MF SR

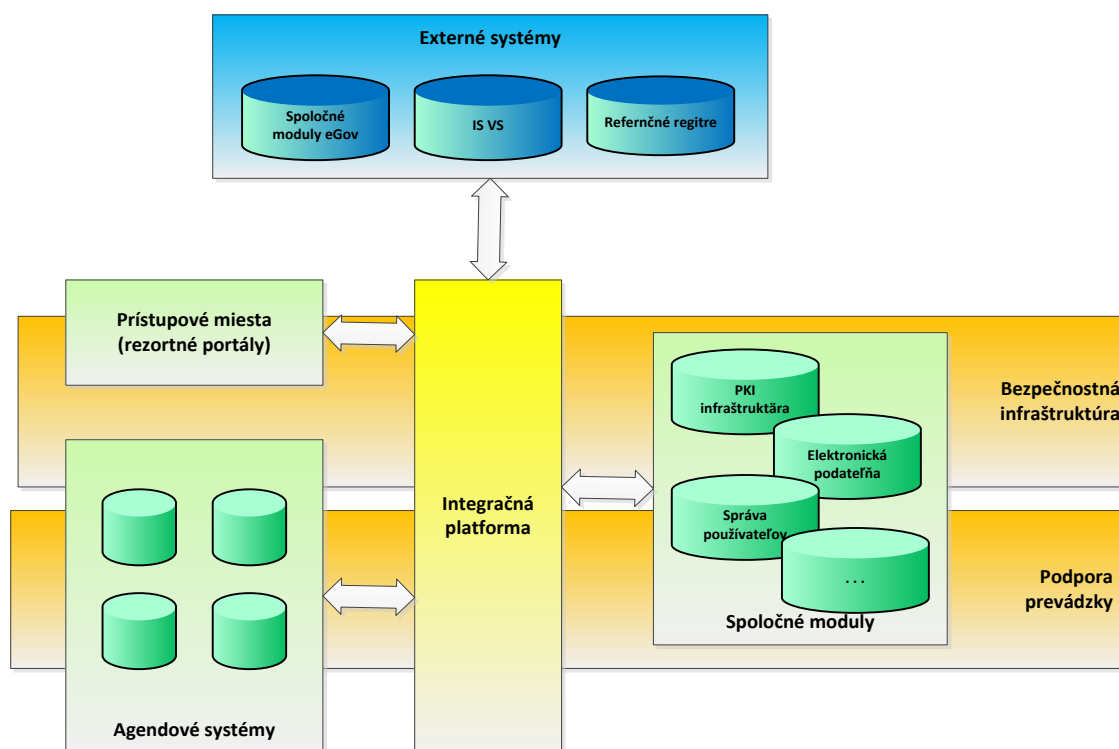
Technické riešenie projektu BAA je cloud ready a v maximálnej miere využije možnosti cloudového riešenia MF SR.

Od MF SR bude project MS SR žiadať nasledovné HW konfigurácie:

Požadovaná výpočtová kapacita					
Účel	Typ	Ks	Počet CPU x jadier	Veľkosť pamäte [v GB]	Veľkosť HDD [v GB]
Podpora prevádzky - server	virtuálny	4	2x15	48	1 000
Spolu		4	2	48	1000
Požadovaná úložná kapacita					
Účel	Typ	Kapacita v TB ročne	Počet rokov	Kapacita celkom v TB	
Audio nahrávanie					
kapacita na 1 rok pri 514 PM, bitrate 192 MBps, počet hodín v roku 1875	disk	77,5	3	232,5	
Skenovanie					
Počet naskenovaných strán za rok x priemer. veľkosť strany v MB	disk	14,5	3	43,5	
Metadáta v RDBMS					
Počet spisov okres/rok					
Počet spisov kraj/rok					
Spolu					
Počet spisov x priemerná veľkosť spisu v MB	disk	3,5	3	10,5	
Počet doručeníek x priemerná veľkosť doručienky	disk	0,5	3	1,5	
Video					
250 dní x 2 hod. nahrávania x dátový tok x počet súdov	disk	44	3	132	
Spolu		140		420	

4.4 Popis architektúry

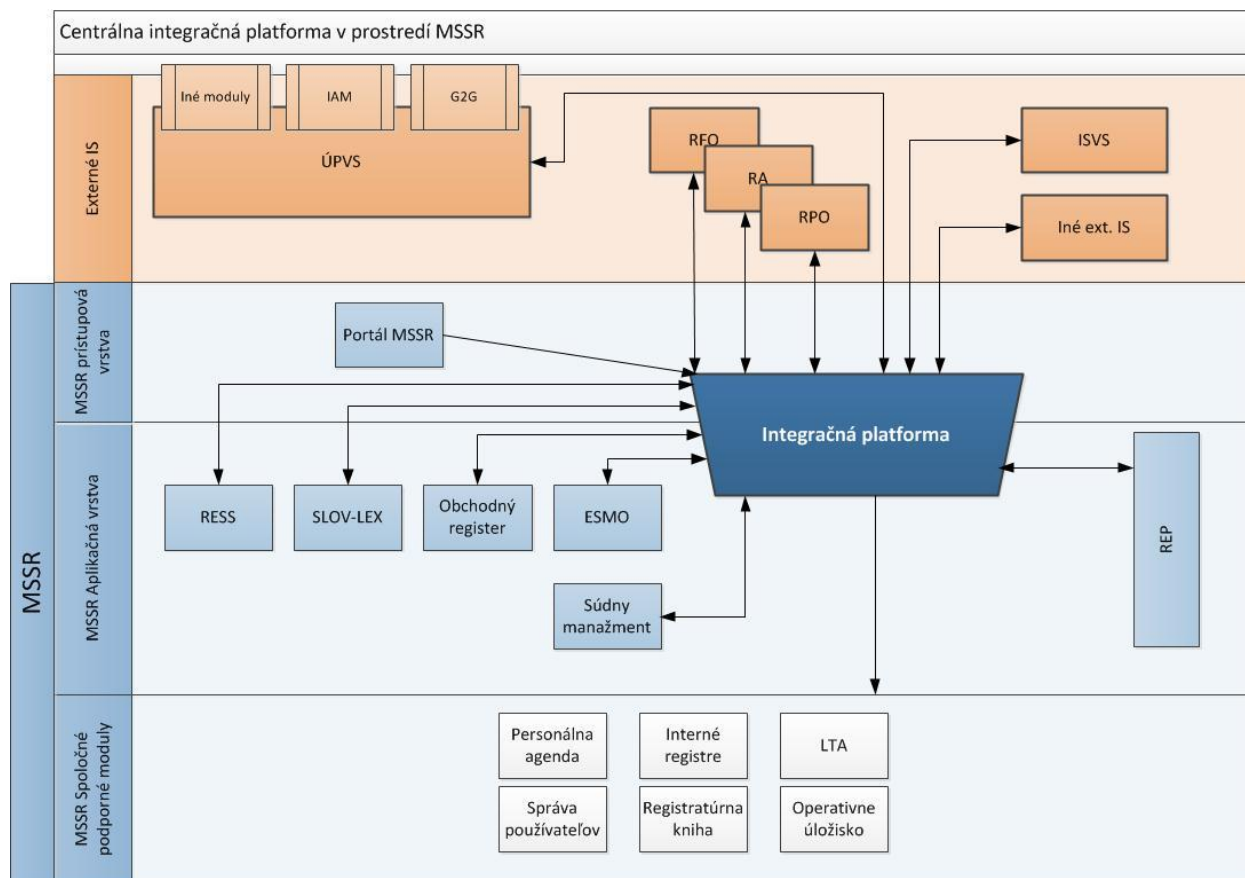
Architektúra pre budovanie konceptu eJustice je ilustrovaná na nasledujúcom obrázku¹:



V ďalších častiach sú podrobnejšie popísané jednotlivé súčasti architektúry, ktoré sú predmetom tejto štúdie.

¹ Uvedený obrázok je iba koncepčnou ilustráciou architektúry eJustice, jej realizácia môže viesť k zónovaniu jednotlivých systémov

4.4.1 Prehľad integrácie v cieľovom stave



Obr. 2 Cieľový stav po zavedení centrálnej integračnej platformy

V cieľovom stave zavedenie centrálnej integračnej platformy v rezorte MSSR umožní zjednotiť realizované opakované integrácie na:

1. Externé informačné systémy
 - ÚPVS
 - G2G
 - IAM
 - eForm
 - MEP
 - ďalšie podľa potreby
 - Referenčné registre
 - RPO
 - RFO
 - RA
 - Iné ISVS a ďalšie IS
2. Interné podporné informačné systémy a rezortné moduly
 - Rezortná elektronická podateľňa (REP)

- Dlhodobý elektronický archív (LTA)
- Interné registre
- Správa používateľov
- Registratúrna kniha
- Operatívne úložisko

Vytvorenie integračných bodov na úrovni centrálnej elektronickej podateľne umožní jednotnú správu (SOA governance) všetkých uvedených integrácií a umožní realizovať spoločné úpravy na jednom mieste bez potreby zásahu do všetkých agendových IS ak sa ich zmena priamo nedotýka.

Komplexnosť integrácií pri spôsobe bod-bod má exponenciálny charakter $O(n^2)$ pričom využitím integračnej platformy ako spoločného miesta – Hub služieb sa charakteristika mení na lineárnu $O(n)$, čo pri početnosti systémov v rezorte a stratégii ďalšieho rozvoja je nevyhnutným predpokladom na efektívne využívanie ďalších prostriedkov.

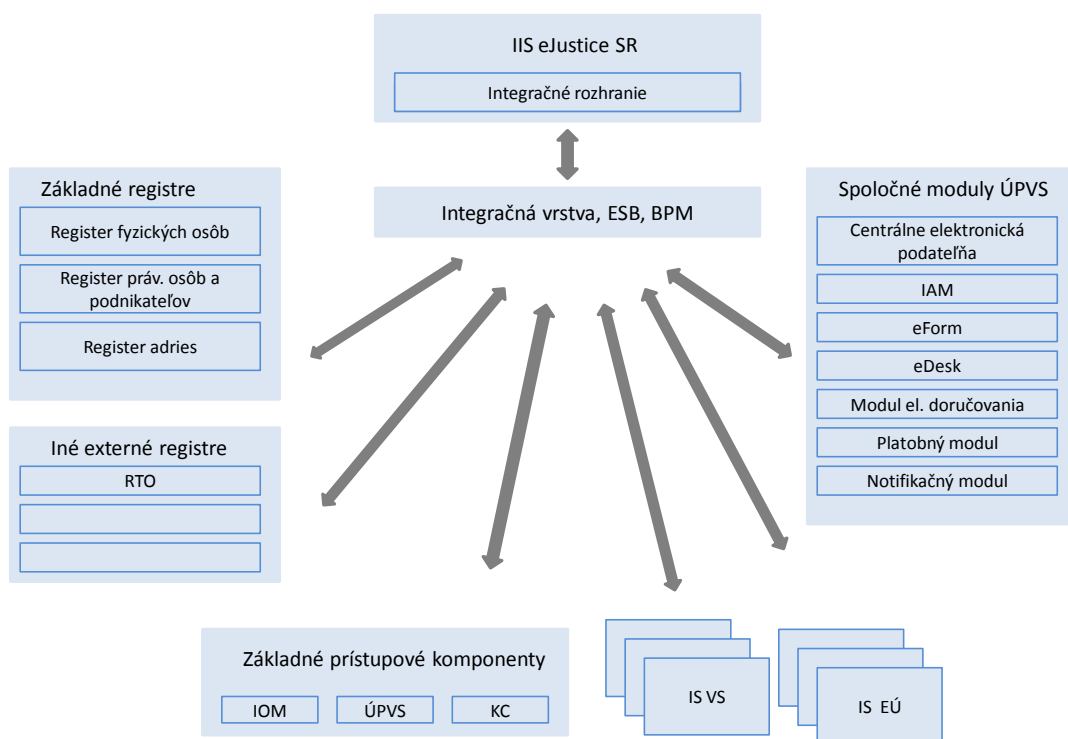
4.4.2 Integračná platforma

Integračná platforma je nástrojom na prepájanie jednotlivých systémov a nimi poskytovaných funkcií a služieb centralizovaným a riadeným spôsobom. V kontexte aplikačnej a integračnej architektúry je integračná platforma základným nástrojom, prostredníctvom ktorého je realizované začlenenie jednotlivých agendových informačných systémov do aplikačnej architektúry realizujúcej koncept eJustice.

Koncept použitia integračnej platformy pre účely budovania konceptu eJustice je založený na nasledujúcich princípoch:

- všetky systémy (agendové aj podporné) publikujú svoje funkcie a služby ako Webové služby, ktoré sú prístupné integračnej platforme. Predpokladá sa použitie princípu SOA (Service Oriented Architecture).
- vzájomná komunikácia jednotlivých všetkých systémov rezortu bude prebiehať prostredníctvom integračnej platformy. Komunikačné procesy a integračná logika je implementovaná prostriedkami integračnej platformy.
- prepojenie systémov rezortu na externé systémy bude taktiež realizované prostredníctvom integračnej platformy a špeciálne vytvorenými integračnými rozhraniami.

Ilustrácia dôležitosti integračnej platformy (integračnej vrstvy) z hľadiska prepojenia všetkých systémov rezortu a okolitých systémov je znázornená na nasledujúcom obrázku (prevzatého z dokumentu „Záverečný informatívny dokument - Výsledný opis predmetu zákazky, Príloha č. 1“).



Použitie SOA k integrácii jednotlivých systémov umožní:

- jasná definícia rozhraní a procesov vedúca k nižšej chybovosti a prehľadnosti vzájomnej interakcie jednotlivých systémov a umožňujúca realizovať integráciu jednotlivých systémov jednotným spôsobom,
- zjednodušenie integrácie jednotlivých systémov do aplikačnej architektúry s využitím integračných prostriedkov integračnej platformy, možnosť opakovaného použitia implementovaných rozhraní a procesov s následkom zníženia nákladov na zmenu a elimináciu duplicit vo vývoji integračných rozhraní,
- zachovanie investícií do existujúcich systémov – v praxi môže byť lákavá predstava „prestavania“ celého spektra technologicky odlišných aplikácií do jednej vzorovej architektúry, ale tento prístup je v praxi zväčša z finančných dôvodov nerealizovateľný a vedie k znehodnoteniu minulých investícií. Práve koncept integračnej architektúry umožní využitie existujúcich systémov s malými zmenami aj v novom prostredí..
- minimalizovať dopad zmien v rozhraniach jedného systému – zmena rozhrania vedie k zmene na integračnej platforme, pričom využívanie služby ostatnými systémami ostáva nezmenené,
- vykonávať procesné zmeny v logike spracovania na integračnej platforme, s minimalizáciou zásahu do jednotlivých agendových systémov, pružnejšie reagovanie na zmeny, nakoľko zmena

integračného rozhrania alebo procesu sa vykonáva centralizovane, bez potreby zásahu do jednotlivých systémov. Takýto prístup výrazne znižuje ľudské a finančné náklady na realizáciu zmien a umožňuje oveľa pružnejšiu reakciu na zmeny v okolitom prostredí.

- centralizácia vybraných bezpečnostných mechanizmov, ako napr. autorizácia prístupu k jednotlivým službám,
- možnosť merania procesov a ich optimalizácie na základe objektívnych kritérií,
- sledovanie plnenia SLA požiadaviek.

4.4.2.1 Integrácia systémov rezortu spravodlivosti

Interné systémy rezortu spravodlivosti budú integrované prostredníctvom služieb integračnej platformy. V praxi to znamená, že služba informačného systému bude sprístupnená prostredníctvom služby integračnej platformy. Z tohto pohľadu je pri vývoji agendových systémov potrebné zohľadniť nasledujúce princípy:

- služby poskytované okolitému prostrediu budovať ako Webové služby, ktoré budú sprístupnené pre integračnú platformu (t.j. ostatné systémy k nim budú pristupovať prostredníctvom integračnej platformy)
- využívanie služieb iných systémov bude volaním služby integračnej platformy (ktorá následne zabezpečí aktiváciu zodpovedajúcej služby príslušného systému)
- agendové systémy budú implementovať výlučne vlastnú funkčnosť, procesná integrácia funkčnosti jednotlivých systémov navzájom bude realizovaná na úrovni integračnej platformy, v jej procesnej vrstve. Táto bude realizovaná na základe analýzy business procesov nad jednotlivými agendovými systémami.

4.4.2.2 Integračná platforma a integrácia so spoločnými modulmi a externými systémami

Poskytovanie elektronických služieb v rezorte spravodlivosti je nemysliteľné bez využitia funkcionality spoločných modulov a informačných systémov iných orgánov verejnej moci.

Integrácia na spoločné moduly bude vykonaná prostredníctvom funkcionality integračnej platformy, kde budú implementované taktiež komunikačné procesy zabezpečujúce využitie funkcionality jednotlivých spoločných modulov². Predpokladá sa využívanie nasledujúcich spoločných modulov a ich funkcionality sprístupnenej prostredníctvom integračnej platformy:

- modul elektronických schránok – zabezpečenie prístupu k elektronickej schránke ministerstva spravodlivosti (do ktorej sa realizuje doručovanie zasielaných elektronických správ/podaní) a ostatných orgánov rezortu – zabezpečenie sprístupnenia doručovaných správ a zasielanie potvrdenia o doručení vytváraných elektronicou podateľňou rezortu.
- modul elektronického doručovania – doručovanie zasielaných správ (informácie, rozhodnutia a pod) elektronickým spôsobom,

² Predpokladá sa, že služby týchto modulov budú vystavené a služby prístupné prostredníctvom integračnej platformy.

- platobný modul – podpora pre vytváranie pokynov na úhradu a zabezpečenie získavania informácie o úhrade súdnych a správnych poplatkov pre služby poskytované orgánmi rezortu,
- autentifikačný modul – autentifikácia externých používateľov poskytované informácií o ich identite (bude podporovaná aj „štandardná“ autentifikácia prostredníctvom eID karty, resp. iným podporovaným autentifikačným mechanizmom podporovaným autentifikačným modulom)
- modul elektronických formulárov – zabezpečuje publikovanie elektronických formulárov používaných v rámci služieb rezortu spravodlivosti. Integrácia zabezpečí aktualizáciu (sťahovanie) formulárov, ktorá sa využívanú v službách napr. ako prílohy
- notifikačný modul – zasielanie notifikácií používateľom o stave poskytovania vyžiadaných služieb,
- modul úradnej komunikácie – zabezpečenie výmeny informáciami s ISVS iných orgánov mimo rezort spravodlivosti. Toto sa týka najmä získavania údajov z referenčných registrov. Tu bude zabezpečená integrácia na tieto služby, ktorá je realizovaná priamym prepojením systémov, nie prostredníctvom komunikácie cez elektronické schránky.
- modul centrálnej elektronickej podateľne – vzhľadom na zámer budovania vlastnej „rezortnej“ elektronickej podateľne sa v budúcnosti nepredpokladá využívanie funkcionality tohto modulu.

Integračná platforma bude slúžiť v budúcnosti na rýchlejšiu a lacnejšiu integráciu z externými IS VS, ktoré sa dnes nedajú definovať konečnou množinou IS VS, resp. registrov.

Integrácia na tieto systémy bude vykonaná prostredníctvom komunikácie prostredníctvom elektronických schránok, resp. prostredníctvom modulu úradnej komunikácie. V rámci tejto integrácie bude realizovaná integrácia na služby referenčných registrov (dostupné v čase realizácie projektu), resp. na služby CSRU.

V tomto projekte sa budú realizovať nasledovné integrácie :

- IS RESS
- Elektronická podateľňa MSSR
- Elektronické služby doručovania ÚPVS (ako generická integrácia na iné IS VS)
- IS RTIS
- IS EZZ
- IS PPI
- IS ESMO
- IS RÚ

4.4.2.3 Požiadavky na funkčnosť integračnej platformy

Integračná platforma bude budovaná na SOA princípoch. V prvom pohľade na SOA architektúru je možné identifikovať jej nasledujúce súčasti:

- **Enterprise Servis Bus (ESB)** - ESB predstavuje jeden zo základných stavebných prvkov servisne orientovanej integrácie, ktorý umožňuje vzájomne prepájať prístupné služby.
- **databáza služieb a register služieb (SOA Governance)** – slúži ako evidencia služieb prístupných prostredníctvom integračnej platformy a ich vzájomných väzieb.

- **orchestrácia procesov (BPM – Business Process Management)** – predstavuje základný nástroj pre vytváranie zložitejších procesov, integrujúcich viaceré publikované služby.
- **rozhrania pre sprístupnenie SOA služieb** – slúži primárne na publikovanie služieb z existujúcich aplikácií.

4.4.2.3.1 Enterprise Service Bus (ESB)

ESB zabezpečuje spojovacu, integračnú vrstvu v SOA riešeniach. Umožňuje prepájať jednotlivé sprístupnené služby do komplexnejších procesov a rozhraní a udržať si v prehľad nad týmito rozhraniami.

Koncept ESB poskytuje nasledujúce možnosti pre prepájanie služieb:

- zabezpečuje riadenú komunikáciu medzi službami (systémami pripojenými k integračnej platforme) prostredníctvom správ,
- zabezpečuje prenos vymieňaných správ, spoľahlivé doručenie správ, transformáciu správ (pokiaľ komunikácia medzi službami vyžaduje transformáciu formátu dát) a ich smerovanie,
- podporuje komunikáciu synchronným spôsobom (request – reply) alebo asynchronným spôsobom (publish – subscribe).

ESB zabezpečuje nasledovné funkcie:

- virtualizácia služby sprostredkovaním volania služby – ESB predstavuje prostredníka medzi poskytovateľom služby a jej klientmi. Pre žiadateľa o službu je transparentné ktorý systém službu poskytuje a aké je reálne rozhranie systému pre túto službu (transformácia správ v prípade potreby). Toto umožňuje zvýšiť flexibilitu v prípade zmeny poskytovateľa, parametrov volania služby, ako aj fyzického umiestnenia poskytovateľa služby bez potreby zmeny rozhrania na ESB poskytovaného klientom.
- spoľahlivé doručovanie správ. Aj v prípade nedostupnosti cieľového systému je správa doručená pri jeho opätovnej dostupnosti,
- transformácia schémy - služby poskytované prostredníctvom ESB môžu využívať iný formát správy (schému) ako poskytuje v publikovanej službe poskytovateľ. Táto vlastnosť je zásadnou najmä pri orchestrácii a agregácii služieb na integračnej platforme.
- voľnosť prepojenia služieb – ESB vystupuje ako sprostredkovateľ medzi poskytovateľom služby a jej používateľmi. Takáto vrstva poskytuje možnosť premostenia komunikačných protokolov, formátov správ a zabezpečovacích technológií.
- skladanie služieb – ESB môže zabezpečovať sekvenčné volanie viacerých služieb, ktoré sa klientovi môže javiť ako volanie jedinej služby sprístupnenej na ESB. Klientovi sa vracia výsledok volania postupnosti služieb. V takejto orchestrácii sa môže definovať aj vetvenie na základe vyhodnotenia definovaných podmienok.
- možnosť konfigurovania parametrov – ESB umožňuje konfiguráciu parametrov (t.j. bez potreby kompilovania a nasadzovania). Konfiguráciou sa menia parametre, ktoré sú okamžite v ESB aplikované.
- centralizované presadzovanie bezpečnostnej politiky – na ESB je možné implementovať bezpečnostné princípy, ktorých aplikácia je centralizovaným a riadeným spôsobom vynucovaná.

- monitorovanie - ESB umožňuje sledovať stav prevádzky a využívania jednotlivých služieb. Schopnosť zachytenia výkonnostných ukazovateľov na ESB môže pomôcť vyladiť výkon ESB. Monitorovanie výkonnosti môže ďalej pomôcť plánovaniu zvýšenia kapacity.

4.4.2.3.2 Databáza služieb a register služieb

Databáza služieb a register služieb (SOA Governance) slúži ako evidencia služieb sprístupnených prostredníctvom integračnej platformy a ich vzájomných väzieb. Na základe údajov tohto registra je služba sprístupnená a vykonáva sa prípadná transformácia dát, resp. implementácia zložitejšieho procesu.

Databáza služieb (Service repository) predstavuje katalóg informácií o jednotlivých službách od ich návrhu, vývoja, testovania až po ich nasadenie. Obsahuje popisy služieb:

- WSDL (Web Service Definition Language)
- XSD (XML Schema Definition) – popisy schém pre vstupy a výstupy služby
- požiadavky, procesné modely, pravidlá a štandardy,
- SLA (Service Level Agreement)
- politiky.

Register služieb (Service registry) slúži na publikovanie a vyhľadávanie služieb, obsahuje definície služieb, popis ich rozhrania, operácií a parametrov.

Jednotlivé implementácie databázy služieb a registra služieb môžu byť v jednotlivých implementáciách riešené ako:

- ako dva samostatné systémy,
- postavené na Service Registry, ktorý je rozšírený o ďalšie objekty,
- ako Service repository systém, ktorý v sebe obsahuje Service Registry.

4.4.2.3.3 Business Process Management

Business Process Management (BPM) predstavuje základný nástroj pre vytváranie zložitejších procesov, integrujúcich viaceré publikované služby. Podporuje aj procesy s dlhším trvaním s možnosťou hybernácie pri čakaní výstupu kroku spracovania realizovaného pripojenou službou. Toto je realizované definíciou toku spracovania (Workflow), kde v jednotlivých krokoch môžu byť volané publikované služby. Workflow môže využívať aj príkazy riadenia spracovania ako rozhodovanie a sekvencia. Proces je kontrolovaný centrálnou, prostredníctvom Procesného manažéra a nie je súčasťou programovej logiky v jednotlivých aplikáciách.

BPM produkty často podporujú simuláciu a ladenie priepustnosti procesov už vo fáze návrhu. Návrh samotného procesu je robený v grafickom prostredí.

BPM je možné vidieť vo viacerých vrstvách:

- Business Process vrstva – v tejto vrstve sa realizujú všetky procesy. Tieto sú implementované cez BPEL a podporuje audit a nástroje workflowu.
- Web Services vrstva - vystavuje existujúcu aplikačnú funkcionálnu ako službu. Web služby implementujú funkcionálnu a doménovú logiku.

- Rules vrstva – definuje závislosti medzi entitami. Pravidlá sú deklaratívne a moderné prostredia poskytujú grafické rozhrania pre vytváranie a editáciu pravidiel. Pravidlá bývajú vystavené ako Web služby, takže môžu byť využívané rôznymi aplikáciami a vytvárať priestor pre jednoduchšiu integráciu.

BPM je možné prevádzkovať samostatne, ale predstavuje prirodzený doplnok k SOA architektúre. Z pohľadu SOA predstavuje BPM samostatný systém, ktorý poskytuje služby (spustenie procesu, zistenie aktuálneho stavu procesu, a pod.) a súčasne aj používa služby iných systémov (t.j. vyvoláva konkrétne služby, z ktorých sa daný proces skladá). Z tohto pohľadu je možné ho napojiť na ESB zbernicu podobne ako iné systémy.

4.4.2.3.4 Rozhrania pre sprístupnenie SOA služieb

Všetky systémy začlenené do SOA poskytujú svoju funkčnosť prostredníctvom publikovaných služieb. Komerčné prostredia poskytujú štandardizované rozhrania (konektory), prostredníctvom ktorých sú sprístupnené služby z existujúcich systémov alebo technológií:

- adaptéry na štandardné technológie (RDBMS, file systém, e-mail, protokoly pre výmenu správ),
- adaptéry na komerčné balíkové riešenia (SAP, Siebel, ..)

4.4.3 PKI infraštruktúra

V procesoch realizovaných konceptom eJustice je potrebná autorizácia komunikácie a úkonov. V súčasnosti legislatíva definuje jediný spôsob autorizácie úkonov, ktorý má právne účinky vlastnoručného podpisu, resp. úradne osvedčeného podpisu – a to je zaručený elektronický podpis (ZEP) alebo zaručená elektronická pečať (ZEPe). ZEP alebo ZEPe ako prostriedok autorizácie úkonov zabezpečí jednoznačnú preukaznú silu v prípade prípadného sporu. Práve PKI infraštruktúra vytvára podmienky pre využitie tohoto spôsobu autorizácie v procesoch rezortu spravodlivosti.

Pre využitie ZEP a ZEPe je potrebné vytvoriť prostredie (PKI infraštruktúru), ktoré zabezpečí:

- podmienky pre vytváranie zaručeného elektronického podpisu (zaručenej elektronickej pečate) a jeho overovanie,
- integráciu prostriedkov pre vytváranie a overovanie zaručeného elektronického podpisu (zaručenej elektronickej pečate) do jednotlivých aplikácií/systémov, v ktorý je autorizácia zaručeným elektronickým podpisom využívaná,
- právne prostredie, ktoré použitie zaručeného elektronického podpisu v interných procesoch bude umožňovať a kodifikovať.

Vytvorenie týchto podmienok sa nazýva aj vybudovanie PKI infraštruktúry. V rámci budovania PKI infraštruktúry je potrebné:

- **zabezpečiť dostupnosť a integráciu aplikácie pre vytváranie ZEP a ZEPe** – nakoľko elektronizácia interných procesov rezortu spravodlivosti je založená na využívaní zaručeného elektronického podpisu, je nevyhnutné zabezpečiť možnosť vytvárania ZEP pre všetkých pracovníkov rezortu spravodlivosti v rámci existujúcich agendových informačných systémov, resp. prostriedky pre vytváranie ZEPe. Autorizácia dokumentov a rozhodnutí ZEP a ZEPe musí byť prirodzene

integrovaná do elektronických procesov. Súčasne je potrebné tieto prostriedky integrovať taktiež do elektronickej podateľne, ako aj procesy overovania ZEP a ZEPe.

Na tieto účely je vhodné z finančných dôvodov využiť multilicenciu certifikovaného prostriedku pre vytváranie a overovanie ZEP a ZEPe poskytovanej v rámci riešenia projektu ÚPVS. Táto aplikácia je plne integrovateľná do prostredia prístupových bodov (Web rozhranie) a bude takýmto spôsobom sprístupnená funkcionality vytvárania ZEP pre všetkých pracovníkov rezortu, ktorý budú s jednotlivými informačnými systémami pracovať. Súčasne je táto licencia použiteľná aj pre systém elektronickej podateľne.

- **vytvorenie legislatívnych a organizačných podmienok pre používanie ZEP a ZEPe** – pre využívanie ZEP je potrebné vytvoriť podmienky umožňujúce jeho plošné využívanie. Nakoľko sa predpokladá využívanie tzv. mandátnych certifikátov alebo systémových certifikátov (ich definovanie je obsiahnuté v Zákone o eGovernmente, ktorým bol novelizovaný Zákon o elektronickom podpise), nie je vhodné využívanie služieb komerčných registračných autorít pre vydávanie kvalifikovaných certifikátov s uvedením mandátu pre pracovníkov rezortu spravodlivosti alebo systémových certifikátov pre jednotlivé organizačné zložky rezortu spravodlivosti. Toto rozhodnutie vyplýva taktiež z predpokladaného počtu vydávaných kvalifikovaných certifikátov (niekoľko tisíc).

Je vhodné, aby proces vydávania kvalifikovaných certifikátov interným pracovníkom a systémových certifikátov pre jednotlivé organizácie rezortu bol pod plnou kontrolou MS SR, a teda nebol vykonávaný prostredníctvom verejných registračných autorít. Je navrhované vybudovanie systému interných registračných autorít, využívaných výhradne pre potreby rezortu spravodlivosti. Vzhľadom na rozmiestnenie používateľov a ich počet bude dostatočné zriadenie registračnej autority vo všetkých krajských mestách (napr. v priestoroch krajských súdov). Zriadenie registračnej autority však predpokladá výber akreditovanej certifikačnej autority, ktorá bude služby rezortu spravodlivosti poskytovať (rozsah požadovaných služieb je uvedený v samostatnom bode).

Použitím špecializovanej registračnej autority určenej výhradne pre potreby MS SR je možné definovať dodatočné kontroly identity a oprávnení a zabezpečiť využívanie aj interných identifikátorov. Z tohto dôvodu je vhodné, aby v rámci rezortu MS SR bol vytvorený systém interných registračných autorít prepojených na systém akreditovanej certifikačnej autority.

- **vytvorenie podmienok pre on-line overovanie ZEP v interných procesoch** – pre plynulosť interných procesov je potrebné zabezpečiť on-line overenie platnosti zaručených elektronických procesov, nakoľko „štandardné“ overovanie platnosti prostredníctvom CRL (zoznamu zrušených certifikátov) spôsobuje neakceptovateľné prestoje. Na tieto účely sa využíva OCSP protokol (protokol pre on-line overovanie stavu certifikátu), ktorý musí akreditovaná certifikačná autorita poskytujúca služby rezortu spravodlivosti podporovať.

Je potrebné funkčnosť elektronickej podateľne, ktorá sa bude využívať pre overovanie platnosti zaručeného elektronického podpisu, rozšíriť o podporu protokolu OCSP a

zabezpečiť prepojenie na poskytovanie tejto služby u vybranej akreditovanej certifikačnej autority.

- **vytvorenie legislatívneho prostredia pre využívanie ZEP** – používanie ZEP v interných procesoch rezortu spravodlivosti je viazané na vytvorenie zodpovedajúceho legislatívneho prostredia, t.j. prostredia interných predpisov a riadiacich aktov, ktoré upravujú použitie zaručeného elektronického podpisu v internom prostredí. V rámci projektu bude vytvorená sada interných predpisov, ktoré budú upravovať použitie zaručeného elektronického podpisu v interných procesoch rezortu a ktoré budú stanovovať postupy pri jeho používaní a povinnosti a zodpovednosti držiteľov kvalifikovaných certifikátov.
- **výber poskytovateľa akreditovaných certifikačných služieb** – pre vybudovanie prostredia pre využívanie zaručeného elektronického podpisu sa predpokladá využitie služieb certifikačnej autority Ministerstva vnútra SR, čo bude upresnené počas analýzy. V rámci projektu budú vypracované požiadavky na takéhoto poskytovateľa služieb.

Akreditovaný poskytovateľ certifikačných služieb by mal v pre potreby rezortu spravodlivosti poskytovať nasledujúce služby:

- vydávanie kvalifikovaných certifikátov pre potreby rezortu spravodlivosti s uvedením mandátu pre držiteľa certifikátu,
- dodanie certifikovaných prostriedkov pre uchovávanie privátneho kľúča (predpokladá sa využitie čipovej karty, ktorá bude využívaná aj pre procesy autentifikácie používateľov, prípadne aj ako interný identifikačný preukaz).
- dodanie a nasadenie registračných autorít pre vydávanie certifikátov pre potreby rezortu spravodlivosti. V rámci budovania systému registračných autorít musí byť vykonané zaškolenie používateľov a dodanie prevádzkovej dokumentácie (podklad pre vypracovanie interných riadiacich aktov upravujúcich procesy vydávania kvalifikovaných certifikátov).
- poskytovanie služby OCSP – pre on-line overovanie platnosti kvalifikovaných certifikátov vydávaných vybraným poskytovateľom akreditovaných certifikačných služieb musí poskytovateľ týchto služieb poskytovať aj službu OCSP.
- poskytovanie služby časovej pečiatky – pre fungovanie elektronickej podateľne a zabezpečenia dlhodobého uchovávanie elektronických dokumentov so zaručeným elektronickým podpisom je potrebné zabezpečiť službu časovej pečiatky.

4.4.4 Správa používateľov

Komplexná správa používateľov je obsiahnutá vo funkčnosti modulu identifikácie, autentifikácie a riadenia prístupov (IAM – Identity and Access Management), ktorý zabezpečuje centralizovanú implementáciu autentifikačných mechanizmov, ktorými používateľ preukazuje svoju identitu. V rámci modulu je možné identifikovať nasledujúce typy používateľov:

- interní používatelia (používatelia interných systémov),
- externí používatelia (občan, právnický subjekt v zastúpení oprávneného používateľa a externé systémy).

Modul IAM jednotne a centrálné poskytuje služby správy používateľov, autentifikácie používateľov, riadenia prístupu k funkciám a objektom informačných systémov a autorizácie používateľov. V rámci funkčnosti modulu bude implementovaný aj zber žiadostí o zriadenie prístupu (registračný formulár), a následne v rámci rozhrania modulu IAM funkčnosť pre spracovanie podaných žiadostí vo väzbe na funkcie správy používateľov a riadenie prístupov. Uvedené služby budú realizované vo väzbe na evidenciu internej organizačnej štruktúry a evidenciu externých subjektov (zahŕňajúcu aj ich vnútornú štruktúru na úrovni organizačných zložiek a oprávnených osôb).

Overená identita používateľa/systému môže byť následne využívaná v agendových systémoch pre stanovenie oprávnení pre prístup k funkciám a údajom jednotlivých agendových systémov (ak oprávnenia pre daný agendový systém nie sú obsahom modulu IAM, ale sú manažované priamo k konkrétnom agendovom systéme). V opačnom prípade poskytuje IAM okrem overenej identity aj rolu používateľa, resp. jeho oprávnenia.

Podľa úrovne autentifikácie (t.j. dôveryhodnosť použitého autentifikačného mechanizmu) môže byť takáto identita aj so úrovňou autentifikácie využívaná pre riadenie prístupov k informačným zdrojom a funkciám informačných systémov.

Ostatné systémy rezortu spravodlivosti mechanizmy správy používateľov, autentifikácie a správy oprávnení preto nemusia mať implementované, využívajú služby centrálného IAM rezortu. Z hľadiska správy prístupov modul môže mať implementované centralizované oprávnenia pre vybrané systémy, lokálne systémy však môžu využívať role pre používateľa evidované v centrálnom systéme na riadenie konkrétnych oprávnení v jednotlivých systémoch (t.j. oprávnenia sú viazané na používateľské role).

Modul IAM v rámci konceptu eJustice pozostáva z infraštruktúry systému IAM pre riadenie prístupu k službám a funkciám jednotlivých informačných systémov začlenených do aplikačnej architektúry. IAM bude základným centralizovaným riešením pre správu identít a prístupových práv v prostredí eJustice. Hlavným cieľom vytvorenia IAM je:

- vytvorenie systému IAM ako jednotného a dátovo konzistentného zdroja údajov o všetkých používateľoch (identitách) prístupujúcim k službám jednotlivých informačných systémov aplikačnej architektúry a ich prístupových právach, resp. iných informáciách o používateľoch,
- sprístupnenie elektronických služieb IAM a zabezpečenie ich použiteľnosti na riadenie prístupových práv v jednotlivých moduloch a informačných systémoch,
- efektívna integrácia IAM do celkovej aplikačnej architektúry, t.j. poskytovanie elektronických služieb IAM iným modulom a efektívne využívanie zdieľaných elektronických služieb poskytovaných inými modulmi.

Systém riadenia identít a prístupových práv bude implementovať nasledovné oblasti:

- **správa identít** – správa interných, tak aj externých používateľov. V praxi to znamená vedenie a administrácia registra používateľov, ktorý bude prepájať ich identitu s identifikátorom používateľa, autentifikačnými nástrojmi a oprávneniami, ktoré sú používateľovi pridelené. Správa identít je prepojená na systém konektorov zabezpečujúcich konektivitu na najpoužívanejšie operačné systémy, databázy, adresárové služby a aplikácie na prístup k údajom o používateľoch a službách registra, napr. X.500 directory services, ktoré vystavuje svoje rozhranie cez LDAP protocol.

Používateľské rozhranie pre správu používateľských účtov bude pre zvoleného používateľa poskytovať možnosti pre vytvorenie (zápisom alebo importom), modifikáciu, zneplatnenie a zneplatnenie používateľského účtu.

Evidencia používateľov je rozdelená podľa spôsobu prístupu:

- verejná zóna - externí používatelia (fyzická osoba, právnická osoba, resp. externé systémy prístupujúce v ich mene)
- privátna zóna - interní používatelia (úradník, prokurátor/sudca, atď.) a interné agendové systémy.

Rozlíšenie jednotlivých typov používateľov bude využívané aj v súvislosti s vyhodnocovaním oprávnení na základe typu používateľa a/alebo príslušnosti používateľa v rámci daného typu štruktúry (oprávnenia vyplývajúce s príslušnosti alebo pozície zamestnanca, príslušnosť a oprávnenie osoby v rámci subjektu).

- **autentifikácia používateľov** – v praxi znamená preverenie deklarovanej identity používateľa prostredníctvom použitia autentifikačného predmetu (meno/heslo, token, prihlasovací certifikát a pod.). Pre autentifikáciu používateľa bude k dispozícii viacero autentifikačných mechanizmov viazaných na jeho identitu.

IAM zabezpečí autentifikáciu a overenie identity používateľa autentifikačným mechanizmom podľa aktuálneho nastavenia a na základe overenej identity bude IAM následne poskytovať ďalšie funkcie ako detailné identifikačné údaje a autorizačné údaje používateľa. Budú podporované minimálne nasledujúce autentifikačné mechanizmy

- pre overovanie interných používateľov a systémov môže byť použitý:
 - intranetový X.500 adresár (napr. MS Active Directory) prístupný cez LDAP protokol,
 - PKI (X.509 certifikát),
 - meno/heslo založený na technológii Digest Autentification (RCF 2617).
- pre overovanie externých používateľov môže byť použitý:
 - IAM ÚPVS (podpora autentifikácie prostredníctvom eID karty),
 - intranetový X.500 adresár (napr. MS Active Directory) prístupný cez LDAP protokol,
 - PKI (X.509 certifikát),
 - meno/heslo založený na technológii Digest Autentification (RCF 2617).
- **správa prístupových práv a riadenie prístupov** - zabezpečí riadenie oprávnení k prístupu k informáciám a službám informačných systémov. Základným prvkom hierarchie riadenia prístupov je oprávnenie, ktoré bude autorizovať daného používateľa pre využitie operácie alebo funkcie systému. Oprávnenie je viazané na rolu, ku ktorej je konkrétny používateľ po autorizácii priradený. Táto hierarchia umožňuje detailne skladať role z oprávnení na operácie zodpovedajúce niektorej z komplexnejších činností. Skupiny budú zodpovedať vyšším celkom zoskupujúcim viaceré činnosti do typových zaradení používateľov reprezentované skladaním skupín z jednotlivých rolí. V rámci riadenia prístupov budú používatelia zaraďovaní do skupín – potom pri autorizácii používateľov bude overovaná dostupnosť požadovaných oprávnení na základe ich zaradenia do skupín a v nich obsiahnutých roliach.

- **single sign-on** – znamená jednotné prihlasovanie používateľov raz a do všetkých systémov, t.j. po úspešnej autentifikácii používateľa je jeho identita prenášaná (napr. SAML, WS-Security a pod.) do všetkých systémov a použitá pre riadenie jeho oprávnení. Používateľ sa teda nemusí autentifikovať (prihlasovať) do každého systému samostatne.
- **monitorovanie a audit** – základnou funkčnosťou budú prehľady správy používateľov a riadenia prístupov – okrem štandardným prehľadov objektov a ich hierarchie, aj informácie o vykonaných operáciách. Podporovaným cieľom analýzy auditných informácií a reportovania bude najmä kontrola správy používateľov a riadenia prístupov a vyhľadávanie podozrivých aktivít naznačujúcich pokusy o narušenie integrity a obmedzení prístupu.

4.4.5 Bezpečnostné a podporné mechanizmy

Bezpečnostné a podporné mechanizmy tvoria samostatnú oblasť zabezpečujúcu jednotné a koordinované dosahovanie bezpečnostných cieľov. Sem patria nasledujúce oblasti:

- autentifikácia používateľov
- riadenie prístupov,
- ochrana proti infiltráciám
- selektívny prístup k aplikáciám
- logovanie a analýza logov
- riadenie bezpečnostnej politiky

Nakoľko problematika bezpečnosti je komplexná, taktiež riešenia v oblasti bezpečnosti musia pokrývať maximum bezpečnostných aspektov. Veľmi dôležitým parametrom je komplexnosť riešení, nakoľko separátny manažment jednotlivých bezpečnostných atribútov neposkytuje komplexný pohľad o stave bezpečnosti.

4.4.5.1 Autentifikácia používateľov

Autentifikácia používateľov je základným predpokladom pre ich identifikáciu a následné povolenie práv. Správu používateľov zabezpečuje modul IAM, ktorý používateľov člení na interných a externých. Rovnako sa predpokladá riadenie prístupových práv na úrovni informačných systémov, preto IAM bude spravovať aj „technické identity“ pre informačné systémy.

Autentifikácia predstavuje základný prostriedok pre dôveryhodné preverenie identity používateľa. Z hľadiska jednotlivých kategórií používateľov sú predpokladané nasledujúce typy autentifikácie (ktoré musí podporovať aj IAM modul):

- externý používateľ – predpokladá sa podpora všetkých autentifikačných prostriedkov v súlade s ustanovenia Zákona o eGovernmente:
 - eID karta
 - alternatívny autentifikátor (v prípade že MV vyhláškou taký určí)
 - pre portály rezortu sa nepredpokladá vydávanie vlastných autentifikátorov
- interný používateľ – predpokladá sa autentifikácia na základe PKI, kde používateľ má na karte uložený autentifikačný certifikát (vydávaný v rámci budovanej PKI infraštruktúry). Takáto

autentifikácia viazaná na bezpečné zariadenie pre uchovávanie autentifikačných údajov (príslušného súkromného kľúča) zabezpečuje dostatočnú úroveň autentifikácie používateľov pri prístupe k informačným systémom.

Z pohľadu dlhodobých cieľov je v projekte uvažované o biometrickej autentifikácii, ktorá z hľadiska používateľa autentifikačný proces zjednodušuje a súčasne poskytuje požadovanú úroveň bezpečnosti. Je možné uvažovať o autentifikácii odtlačku prstu na pracovných staniciach, alebo odtlačku ruky na myši.

- informačný systém – pre autentifikáciu informačného systému pri prístupe k službám integračnej platformy (iných informačných systémov) bude používaný autentifikačný certifikát.

4.4.5.2 Riadenie prístupov

Riadenie prístupov umožňuje priradenie zodpovedajúcich prístupových práv pre oprávnených autentifikovaných používateľov (to však neznamená, že niektoré služby nevyžadujú autentifikáciu, t.j. sú poskytované všetkým, aj anonymným používateľom). Riadenie prístupov je možné realizovať na viacerých úrovniach:

- prístupy k funkciám informačných systémov – sú zabezpečené jednotlivými informačnými systémami. Po autentifikácii používateľa je informačnému systému poskytnutá identita používateľa a prípadne aj jeho rola pre daný informačný systém. Ten na základe týchto informácií vyhodnotí oprávnenia používateľa pri prístupe k jednotlivým funkciám a službám.
- prístupy k službám integračnej platformy – na úrovni integračnej platformy sú na úrovni informačných systémov definované práva komunikácie s inými informačnými systémami.
- prístupy z Internetu – zabezpečenie ochrany interných systémov pred útokmi z Internetu (firewall, resp. aplikačný firewall). V súčasnosti je firewall a vytvorenie DMZ štandardným spôsobom ochrany pred útokmi z Internetu. Vývoj však vyžaduje nasadenie moderných prostriedkov ako aplikačný firewall.

4.4.5.2.1 Aplikačný firewall

Architektúra konceptu eJustice je postavená na princípoch SOA. Takýto prístup predpokladá použitie moderných technológií budovania informačných systémov a sprístupňovania ich služieb (napr. AJAX, JSON), ktoré na druhej strane umožňujú nové typy útokov, najmä z prostredia Internetu na baze nekvalitne napísaného kódu, alebo známych chýb prevádzkovaných prostredí. Podľa správy 2012 Verizon Data Breach Investigations Report boli v 54 percentách prípadov úniku údajov vo veľkých organizáciách použité webové aplikácie ako vstupná brána pre realizáciu útoku.

Z uvedených dôvodov na úrovni prístupu z Internetu je potrebné zabezpečiť vynucovanie politiky a identifikáciu útokov špecializovaným prostriedkom zabezpečujúcim ochranu na vrstve 7 (aplikačná vrstva). Ochrana tejto vrstvy umožňuje napr. čeliť útokom typu DoS, databázovým SQL injection útokom, cross-site scripting, útokmi brute force a day-zero útokmi.

Aplikačný firewall rieši prístup k jednotlivým službám a umožňuje zabrániť ich zneužitiu nepovoleným spôsobom. Chráni teda publikované webové služby a webové stránky pred útokmi z externého prostredia, ktoré využívajú chyby nasadených technológií.

Aplikačný firewall umožňuje centralizované riešenie ochrany pred útokmi z externého prostredia pred nasledujúcimi typmi útokov:

- chyby aplikácií – ochrana pre webové aplikácie a webové služby pred útokmi na známe chyby v implementácii technológií,
- dostupnosť publikovaných aplikácií a služieb – rozšírená ochrana pred distribuovanými útokmi zahŕňajúcimi služby (DDoS),
- útoky na vytypované aplikácie a ich vystavené služby (napr. ako Web servis) – vlastné filtrovanie útokov na jednotlivé aplikácie, ktoré majú špecifické vlastnosti.

Aplikačný firewall musí taktiež obsahovať vzorky najvýznamnejších útokov, schopnosť ich identifikovať a pokiaľ možno automatizovaným spôsobom eliminovať pokusy o narušenie bezpečnosti. Aplikačný firewall eliminuje všetky odchýlky od bežných komunikačných scenárov. Mal by zabezpečovať nasledujúce základné funkcie:

- identifikácia relácie a vynucovanie bezpečnostných politík v kontexte ochrany proti útokmi z vonkajšieho prostredia,
- integrovaný XML firewall,
- aktualizácia signatúr útokov,
- geolokačné blokovanie,
- zabezpečenie pre SMTP a FTP,
- audit a reporting.

4.4.5.3 Ochrana proti infiltráciám

Infiltrácie (vírusy, trójske kone a pod.) predstavujú pomerne rozšírený spôsob narušenia bezpečnosti. Prostriedky v tejto kategórii musia zabezpečiť identifikáciu týchto infiltrácií a ochranu všetkých vstupných bodov informačného systému pred prienikom týchto infiltrácií.

V praxi sa používajú prostriedky pre nasledujúce vstupné body:

- súborový systém a kontrola uchovávaných ako aj všetkých vstupujúcich súborov do interného prostredia,
- elektronická pošta – kontrola všetkých prichádzajúcich aj odchádzajúcich správ v mailovom serveri, redukcia spamu,
- ochrana prenosov dát prostredníctvom webových protokolov (HTTP, HTTPS, FTP),
- kontrola prehliadaných webových stránok na prítomnosť škodlivého kódu, prípadne prístupu k „podozrivým“ stránkam ako súčasť riešenia zabezpečujúceho ochranu proti infiltráciám (prístupové gateway)

Pri výbere prostriedku treba mať na zreteli najmä nasledujúce vlastnosti:

- podpora kontroly vstupných bodov, t.j. koncové zariadenia (počítače, mobilné zariadenia), mailové servery a gateway na prístup do Internetu,

- pravidelná aktualizácia databázy infiltrácií,
- efektívna distribúcia aktualizácií produktu a databázy infiltrácií na všetky kontrolné body na ktorých sú prevádzkované detekčné prostriedky,
- podpora všetkých platforiem prevádzkovaných v rezorte spravodlivosti,
- riešenie procesov spracovania identifikovaných infiltrácií (ukladanie do karantény, uvoľňovanie z karantény),
- centralizovaný manažment celého systému a reporting (kompaktnosť systému).

4.4.5.4 Logovanie a analýza logov

Používaním systémov vznikajú „digitálne odtlačky“ činnosti jednotlivých používateľov a systémov – záznamy (logy). Na ich základe je možné podrobnejšie vyhodnocovať činnosť jednotlivých používateľov a analyzovať súlad z celkovou korporátnou politikou (t.j. či používateľ nevykonáva „podozrivú“ alebo nepovolenú aktivitu).

Bezpečnosť konceptu eJustice nie je potrebné iba definovať, ale zabezpečiť realizáciu bezpečnostnej politiky a sledovanie jej dodržiavania, čiže sledovať a pravidelne vyhodnocovať bezpečnostnú situáciu. Na tomto základe sú potom realizované kroky, ktorými prevádzkovateľ systémov reaguje na konkrétnu bezpečnostnú situáciu.

Analýzou logov z jednotlivých systémov je možné dosiahnuť:

- analyzovať činnosti jednotlivých systémov a identifikovať stavy, ktoré sú odlišné od nastavených „štandardných“ hodnôt,
- podporovať vývoj aplikácií analýzou chybových hlásení a logov popisujúcich činnosť systému vedúceho k chybovému stavu,
- identifikovať nepovolenú činnosť používateľov,
- preukázanie súladu s korporátnymi politikami.

Z hľadiska manažmentu bezpečnosti v oblasti logovania a monitorovania bude implementovaná nasledujúca funkcionálna:

- centralizovaný zber logov – centralizovaný a automatizovaný zber logovacích záznamov z bezpečnostných mechanizmov a z jednotlivých prevádzkovaných aplikácií. Centralizovaný zber umožňuje centrálnu implementáciu bezpečnostných mechanizmov zabráňujúcich neautorizovanej modifikácii týchto záznamov, ako aj ich následnú archiváciu podľa bezpečnostnej politiky.
- vyhodnocovanie logov a bezpečnostných incidentov – centralizované vyhodnocovanie logovacích záznamov a ich vzájomná korelácia za účelom identifikácie podozrivého správania používateľov a bezpečnostných incidentov (prichádzajúcich či z interného či z externého prostredia).
- archivácia záznamov tak, aby bolo možné identifikovať následne použiť tieto záznamy aj neskôr pri analýzach bezpečnostných incidentov, ako aj pri zhromažďovaní dôkazového materiálu pri nelegálnych aktivitách interných a externých používateľov.

Základné požiadavky pre riešenie pre správu a analýzu logov:

- zber logov v rôznych formátoch, nakoľko jednotlivé systémy môžu vytvárať logy v špecifických formátoch. Metódy zberu musia podporovať agentové aj „agent-less“ metódy,
- keďže formát logov nie je štandardizovaný, je potrebné konvertovať jednotlivé záznamy do unifikovaného formátu, ktorý je možné následne centralizovane uchovať a spracovať,
- podpora rýchlej analýzy logov za súčasného efektívneho využitia dostupných pamäťových zdrojov. Efektívna analýza logov vedie k rýchlej identifikácii hľadaných vzorov a možnosti reakcie na nežiadúci stav.
- podpora inteligentných pamäťových médií ako SAN/NAS/DAS pre zabezpečenie dostatočnej kapacity pre uchovávanie všetkých kolektovaných záznamov a ich uchovania pre potrebnú dobu pre ich prípadné využitie pre dokumentovanie vzniknutých udalostí a stavov, resp. správania používateľov.
- bezpečné uchovávanie logov takým spôsobom, aby ich bolo možné použiť ako dôkazový materiál v prípade indikovania nežiadúceho stavu a vyvodenia zodpovednosti za tento stav alebo správanie používateľa. Dôležité je zachovanie integrity a autenticity.
- správa logov býva často vyžívaná s koreláciou udalostí pre detekciu narušení bezpečnosti aj z interného prostredia. Preto prostriedky bývajú prepojené so správou udalostí, kde indikácia vzoru v logoch znamená zaslanie udalosti, ktorá je ďalej vyhodnocovaná a korelovaná s inými.

4.4.6 Mechanizmy pre podporu prevádzky infraštruktúry a informačných systémov

Účelom nasadenia týchto mechanizmov je vytvorenie podmienok pre efektívnejšiu prevádzku nasadenej infraštruktúry a informačných systémov. Tieto riešenia budú orientované do nasledujúcich oblastí:

- monitoring zariadení,
- event manažment,
- manažment koncových zariadení,
- správa licencií a ich využitia,
- sledovanie a analýza výkonnosti aplikácií,
- podpora procesov zálohovania
- podpora používateľov,
- procesy a riešenie incidentov.

4.4.6.1 Monitoring zariadení

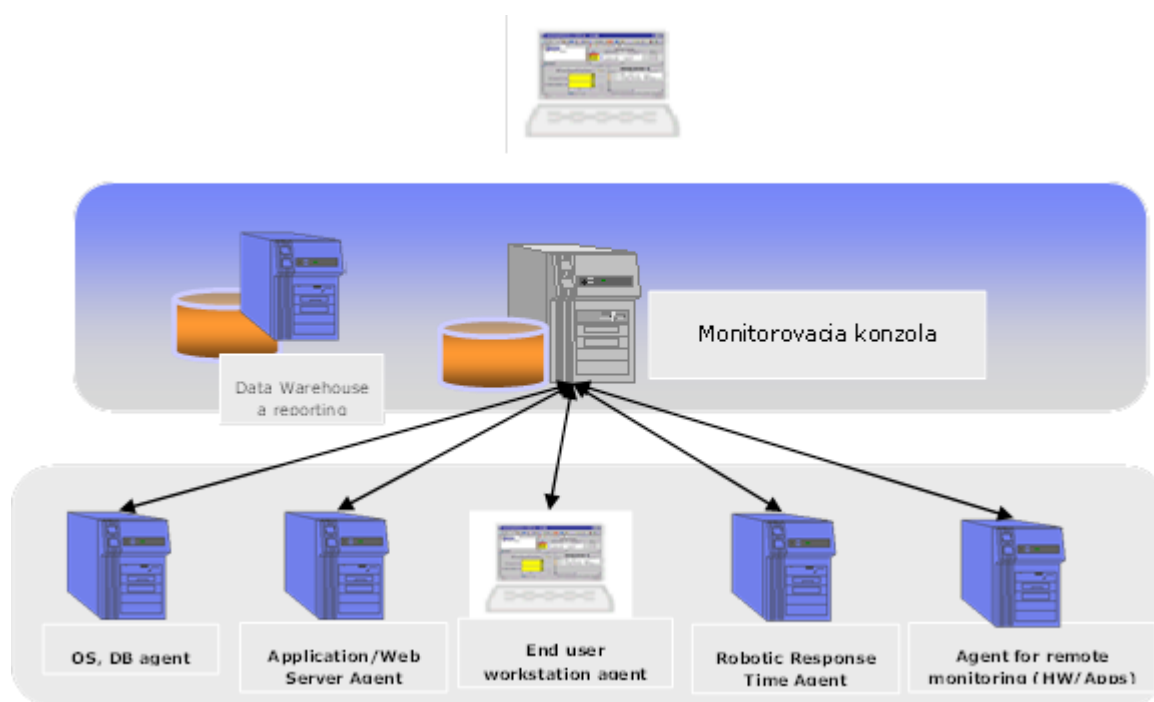
Monitoring vo všeobecnosti znamená sledovanie prevádzkového stavu monitorovaných zariadení. V rámci monitorovania je sledovaných viacero prevádzkových parametrov, ako napr. celková dostupnosť, využitie zdrojov, celkové prevádzkové podmienky (napr. teplota, vlhkosť) a pod. Základom je manažment aktív (HW zariadenia, SW systémy, sieťové prvky a pod), ktorý zabezpečí evidenciu všetkých týchto zariadení – základ pre všetky následné aktivity.

Stav jednotlivých parametrov je vyhodnocovaný vzhľadom na preddefinované úrovne a je reportovaný do centrálného monitorovacieho uzla vo forme udalostí. Tu je možné sledovať prevádzkový stav (napr. výpadok) alebo dosiahnutie definovaných kritických hodnôt monitorovaných parametrov (napr. vyťaženosť procesora, zaplnenie pamäťového média, dosiahnutie kritickej teploty).

Z hľadiska monitorovania je dôležité nielen sledovanie prevádzkového stavu jednotlivých zariadení, ale najmä väzba stavu zariadenia na konkrétne business procesy. To následne umožňuje vyhodnocovanie dopadov výpadkov na činnosť organizácie a tým aj definovanie priorit riešenia týchto stavov.

Významnou súčasťou monitorovacích nástrojov sú analytické a reportovacie schopnosti. Tie umožňujú sledovanie trendov a proaktívne predchádzanie kritických stavov a výpadkov, napr. sledovať trend vyťaženia procesora a proaktívne zabezpečenie vyššej výkonovej kapacity pred reálnym vznikom problému.

Koncepcná schéma monitorovacieho systému je ilustrovaná na nasledujúcom obrázku:



4.4.6.2 Event manažment

Monitorovanie širokého spektra prevádzkových a bezpečnostných parametrov vedie k vzniku veľkého počtu udalostí. Spracovanie udalostí z prevádzkového prostredia riešenia systémy pre Event Management.

Systém ku každej reportovanej udalosti doplní zodpovedajúce parametre (napr. údaje o zariadení, alebo aj o SLA ktoré určuje prioritu riešenia udalosti). Operátor teda má komplexnejší pohľad na udalosť a dokáže udalosť efektívnejšie vyhodnotiť v celkovom kontexte prevádzky organizácie.

Vzhľadom na v praxi vznikajúci veľký počet reportovaných udalostí (stavov), je hlavnou úlohou Event managementu znížiť počet zobrazovaných udalostí:

- filtráciou udalostí reportujúcich bezporuchový („štandardný“) stav,

- filtráciou duplicit (opätovné reportovanie chybového stavu) – zabezpečí sa, že opakované hlásenie sa nezobrazuje.
- koreláciou udalostí – niekoľko udalostí spojí podľa korelačných pravidiel a tak umožní lepšie pochopiť súvislosti medzi udalosťami (napr. výpadok siete môže spôsobiť nedostupnosť viacerých koncových zariadení)

Následná podpora vyhodnocovania udalostí, rozpoznanie príčin a následkov (root cause analýza) zabezpečí, že je možné riešiť príčinu problému a nevenovať pozornosť následkom tohto problému.

4.4.6.3 Manažment koncových zariadení

Prostriedky zaradené v tejto kategórii (Endpoint Management) zabezpečujú podporu základných prevádzkových aktivít na koncových staniciach. Práve koncové stanice (server, pracovné stanice, notebooky, tablety a mobily) sa vyznačujú vysokým počtom a ich prevádzková podpora vyžaduje značné nasadenie podporného personálu. Práve automatizácia základných prevádzkových aktivít vedie k výraznému zefektívneniu prevádzkových činností.

Prostriedky tejto kategórie poskytujú nasledujúcu funkcionálnosť:

- automatizácia zmien - distribúcia inštalácií (image) operačných systémov a ich opráv a servisných balíčkov na koncové zariadenia, ktoré umožnia štandardizovať nasadené prevádzkové prostredia. Týmto je možné zredukovať riziká spojené s nekvalifikovanou inštaláciou a konfiguráciou parametrov prostredia koncového zariadenia, vrátane jeho bezpečnostných a prevádzkových nastavení.
- zabezpečenie súladu s korporátnou politikou – možnosť definovania konfigurácie koncových zariadení a zabezpečenia zhody s touto politikou, udržiavanie auditných správ pre zmeny politiky,
- distribúcia softvéru na základe definovanej politiky. Funkcionalita musí zohľadňovať jednak zaťaženie sietí (t.j. minimalizovať zaťaženie nepresúvaním inštalačného balíka z centra na koncovú stanicu, ale zabezpečením hierarchickej distribúcie), ako aj špecifiká prostredí pri inštalácii softvérových produktov.
- možnosť odinštalovania softvérových produktov v súlade s korporátnou licenčnou politikou,
- reporting – podpora funkcií na zber a prezentáciu údajov z koncových zariadení, ich obsahu a stavu.

4.4.6.4 Správa licencií a ich využitia

V rámci rezortu spravodlivosti sa využíva mnoho produktov, ktoré sú nasadzované a využívané v súlade s licenčnými zmluvami. Práve porušenie licenčnej zmluvy môže mať pre organizáciu následky v pokutách. Je dôležité poznať, kde a akým spôsobom sa inštalované softvérové produkty používajú.

Prostriedky tejto kategórie zabezpečujú nasledujúce základné funkcie:

- inventarizácia stavu prostredí - analýza koncových zariadení a identifikácia nasadených systémov a aplikácií (licencovaných a aj nelicencovaných) - zbieranie údajov o nasadených zariadeniach a systémoch, ako aj využívania licencovaných produktoch.

- identifikácia inštalovaných systémov - prostriedky tejto kategórie majú databázy veľkého počtu balíkových riešení, ktoré umožňujú identifikovať pri analýze koncových zariadení. V prípade operačných systémov identifikácia aplikovaných záplat na danom koncovom zariadení a identifikácia prípadného nesúladu s korporátnou politikou aplikácie záplat.
- sledovanie oprávnení na využívanie príslušného licencovaného produktu, v súlade s rolou daného používateľa a na ňu viazanými prostriedkami definovanými korporátnou politikou.
- sledovanie reálneho využívania nasadených licencovaných produktov na úrovni koncových zariadení a zabezpečovanie súladu s licenčnou politikou. Sledovanie reálneho využitia a vyhodnocovanie využívania licencií na koncových zariadeniach môže viesť k optimalizácii využívania dostupných licencií,

4.4.6.5 Sledovanie a analýza výkonnosti aplikácií

V praxi sú výkonnostné problémy prevádzkovaných aplikácií častokrát riešené zvýšením výkonu infraštruktúry. Analýzou výkonnostných problémov je možné presnejšie určiť zdroj problémov a adresnejšie smerovať nápravné opatrenia.

Prostriedky tejto kategórie umožňujú monitorovať výkonnosť jednotlivých systémov a aplikácií a sledovať súlad s požadovanými parametrami, napr. odozva, SLA a pod.

4.4.6.6 Podpora procesov zálohovania

Strata údajov predstavuje najvýznamnejší rizikový faktor pre mnohé organizácie. Systémy pre podporu zálohovania zabezpečujú komplexný proces zálohovania a obnovy systémov v prípade výpadku. Podporujú vytváranie inkrementálnych, ako aj úplných záloh ako údajov tak aj celých systémov.

Systém pre podporu zálohovania musí umožňovať definovať zálohovacie procedúry selektívne pre jednotlivé systémy a musí informovať o výsledku procesov zálohovania (prepojenie na Event Management). Zálohovacie procesy musia podporovať zálohovacie centrálnych systémov, ako aj vybraných koncových zariadení.

4.4.6.7 Podpora používateľov (Help Desk)

Efektívnosť využívania informačných systémov závisí od schopnosti používateľov používať tieto systémy. V prípade potreby používateľa majú k dispozícii podporný tím a systém, ktorý zabezpečuje ich podporu.

Predpokladá sa existencia jednotného kontaktného miesta na riešenie všetkých používateľských požiadaviek a incidentov (Help Desk), pričom správa incidentov a problémov je v súlade s postupmi procesov ITIL. Táto oblasť zahŕňa aj efektívne riadenie tretích strán pre hardvérovú a softvérovú podporu. Pre všetky poskytované služby sa v rámci oblasti podpory v praxi zabezpečuje pravidelný reporting dosiahnutých úrovní pre riadiace zložky projektu.

Systém Help-desku by mal zabezpečovať minimálne nasledujúce funkcie:

- reportovanie problémov a zabezpečenie sledovanie procesu ich riešenia,

- prístup k báze znalostí obsahujúcej riešenia najčastejšie sa vyskytujúcich problémov (samoobslužný systém riešenia problémov),
- podpora-on-line komunikácie pracovníka Help-Desku s používateľom, s možnosťou sledovania a „prevzatia“ obrazovky pracovnej stanice používateľa – „remote control“ (sledovanie stavu prostredia obrazovky, praktická ukážka postupu pre riešenie problému používateľa).

4.4.6.8 Procesy a riešenie incidentov

V prevádzke je potrebné riešiť problémy a incidenty, a preto je vhodné mať k tomuto podporné prostriedky. Prostriedky v tejto kategórii umožňujú jednak spravovať základné procesy:

- manažment konfigurácií (evidencia spolu súvisiacich prvkov a nastavení)
- riadenie zmien (evidencia vykonaných zmien v systéme),
- SLA manažment – riadenie SLA procesov a požiadaviek na služby.

Popri týchto podporných prostriedkoch sa využívajú prostriedky pre podporu jednotlivých činností pri riešení problémov:

- manažment incidentov
- manažment problémov
- manažment znalostí

Produkty v tejto oblasti zabezpečujú identifikáciu incidentov na báze vyhodnotenia reportovaných udalostí a manažment celého procesu riešenia incidentu, t.j. jeho pridelenie na riešenie, sledovanie stavu riešenia a sledovanie požadovaných dôb odozvy v súlade so SLA. Súčasne prostriedky poskytujú databázu znalostí, z ktorej môže podporný personál vychádzať pri riešení problémov. Často sa pre určité udalosti definuje automatizovaný proces ich riešenia, ktorý zefektívni činnosť podporného tímu.

5 Uskutočniteľnosť a náklady

Vybudovanie cieľového riešenia aplikačnej architektúry a bezpečnostnej infraštruktúry MS SR je zložitý proces, ktorý okrem technológií zahŕňa tiež zmeny najmä v organizácii budovania informačných systémov a prevádzky informačných systémov. V tejto časti štúdie je preto uvedená analýza podmienok, ktoré je potrebné vytvoriť pre úspešné zrealizovanie a nasadenie cieľového riešenia do prevádzky.

Nasadenie novej aplikačnej architektúry a bezpečnostnej infraštruktúry vyžaduje vytvorenie širokého spektra predpokladov.

Plánované zmeny sa týkajú najmä nasledujúcich oblastí:

- technológia – nasadenie nových technológií potrebných pre prevádzku novej infraštruktúry,
- organizácia a procesy – organizačné a procesné zmeny zamerané na ukotvenie nových procesov v oblasti integrácie aplikácií, bezpečnosti a prevádzky,
- personálna oblasť – zvyšovanie kvalifikácie zamestnancov pre prácu s novými technológiami a procesmi.

5.1 Dopady na technické a softwarové vybavenie

MS SR ako povinná osoba postupuje podľa princípov pre stanovenie celkových nákladov na vlastníctvo SW (TCO). Stanoveniu celkových nákladov na vlastníctvo SW (TCO) je uvedené v Prílohe č.1 spoločne s kalkuláciou nákladov na vlastníctvo hardvéru.

Zohľadnené princípy sú stanovené v:

- Metodickom pokyne pre štandardné náležitosti opisu predmetu zákazky, štandardné podmienky účasti vo verejnom obstarávaní a optimálne zmluvné podmienky v súvislosti s projektmi v oblasti informačnokomunikačných technológií (verzia 1.51 – máj 2013) a prílohy 1-5³
 - návrh štruktúry požiadaviek a vzory pre jednotlivé kategórie opisu predmetu zákazky s príslušnými náležitosťami zmluvných podmienok.
- Metodickom usmernení pre obstarávanie softvérových produktov vo verejnej správe;
- Príručke k Metodickému usmerneniu pre obstarávanie softvérových produktov vo verejnej správe

Vzhľadom na charakter riešenia je potrebné zohľadniť dopady na technické a softvérové vybavenie v nasledujúcich oblastiach:

- diskový priestor pre ukladanie potrebných dát,
- integrácia rezortných systémov s inými systémami

³ http://www.informatizacia.sk/ext_dok-metodicky_pokyn_std_obstaravanie_1-5/15304c

- výmena zastaralých osobných počítačov sudcov a ich nahradenie novými osobnými počítačmi a zariadeniami (jednouúčelové tablety)

Nasadenie a prevádzka aplikačnej architektúry a bezpečnostnej infraštruktúry vyžaduje zavedenie nových technológií. To sa týka najmä technológií zabezpečujúcich integráciu – integračnej platformy, autentifikačného modulu, PKI ako aj produktov pre podporu prevádzky a riadenie bezpečnosti.

Z hľadiska využitia vlastností nového riešenia je prioritne potrebné nasadiť základné infraštruktúrne komponenty – integračnú platformu a IAM tak, aby mohli byť využívané pri riešení existujúcich projektov a budovaní nových systémov. Až následne môžu byť nasadzované PKI komponenty a integrované do systémov. Nasadenie prostriedkov pre riadenie bezpečnosti a podporu prevádzky je možné paralelne a viac-menej nezávisle od riešenia existujúcich projektov.

5.2 Organizačné dopady

Cieľové riešenie aplikačnej architektúry a bezpečnostnej infraštruktúry predpokladá nový spôsob organizácie vývoja a integrácie aplikácií, ako aj novú organizáciu prevádzky a plnenia bezpečnostnej politiky. Je potrebné vykonať ako organizačné zmeny, tak aj procesné zmeny.

Organizačné zmeny sa budú týkať najmä:

- zabezpečenia procesov vývoja jednotlivých informačných systémov v rámci konceptu eJustice tak, aby boli v maximálnej miere využité možnosti riešeného projektu,
- zmeny náplne jednotlivých útvarov súvisiacich so zmenou procesov podpory prevádzky.

Procesné zmeny sa týkajú najmä zmeny procesov poskytovania služieb, procesov riešenia prevádzky a riadenia bezpečnosti. Bude potrebné vytvoriť interné smernice záväzné pre zamestnancov, ktoré budú nové procesy kodifikovať.

Nasadenie nových technológií nasadených v rámci riešenia projektu bude vyžadovať zvýšenie kvalifikácie určených zamestnancov potrebnej pre efektívne využívanie systému a zabezpečenia jeho prevádzky. Nasadené riešenia sa stanú súčasťou všetkých systémov a schopnosť využívania ich funkcionality sa stane základným kvalifikačným predpokladom pre väčšinu pracovných pozícií v oblasti zabezpečovania vývoja a prevádzky informačných systémov v rezorte.

5.3 Legislatívne dopady

Pre nasadenie technológií a systémov nasadzovaných v rámci riešenia projektu nie je predpokladaná žiadna zmena v existujúcej legislatíve.

Bude však potrebná zmena internej legislatívy, t.j. interných predpisov upravujúcich používanie PKI pre autorizáciu úkonov, ako aj prevádzky a riadenia bezpečnosti v oblasti informačných systémov.

5.4 Prevádzkové a bezpečnostné dopady

Nasadenie a prevádzka navrhovaného systému vyžaduje zabezpečenie podmienok, ktoré umožnia prevádzkovanie infraštruktúry a vytvárania podmienok pre vývoj nových systémov v požadovanom rozsahu a kvalite. Toto sa týka najmä riešenia bezpečnostných otázok, ako aj problematiky vlastného zabezpečenia prevádzky systému a sprístupňovania jeho funkcionality.

5.5 Bezpečnosť

Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy ukladá povinným osobám zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy ako aj zabezpečovať, aby informačný systém verejnej správy vyhovoval štandardom.

Pri dodávke a nasadzovaní riešenia aplikačnej architektúry a bezpečnostnej infraštruktúry byť zohľadnená existujúca bezpečnostná politika a prevádzkové predpisy, ktoré budú upravené vzhľadom k požiadavkám a novým možnostiam nasadeného riešenia. Požiadavky Výnosu MF SR určujú v § 28 písm. a) obsah bezpečnostnej politiky, ktorú má mať povinná osoba vypracovanú a schválenú. V zmysle požiadavky Výnosu stanovenej v § 28 písm. b) bude bezpečnostná politika organizácie dodržaná a realizovaná najmä prostredníctvom bezpečnostného projektu a z neho vyplývajúcich opatrení. Bezpečnostný projekt bude stanovovať realizované bezpečnostné opatrenia na technickej systémovej a organizačnej úrovni a stanovovať požiadavky na ich implementáciu v rámci jednotlivých systémových modulov vyvíjaného informačného systému, pričom bude zohľadňovať možnosti nových nasadených technológií.

5.5.1 Zabezpečenie prevádzky nasadeného riešenia

Nasadzované riešenie musí byť osadené do prevádzkového prostredia, ktoré bude zabezpečovať všetky súčasti životného cyklu, najmä manažmentu návrhu a implementácie informačných systémov v prostredí rezortu spravodlivosti. Preto sú navrhované prevádzkové prostredia nasledovné.

5.5.1.1 Prevádzkové prostredie

Prevádzkové prostredie bude slúžiť na prevádzku dodaného riešenia v primárnom prevádzkovom centre. Budú v ňom prevádzkované všetky systémy a primárne bude funkčnosť systémov začlenených v koncepte eJustice poskytovaná z tohoto centra, okrem prípadu, keď dôjde k výpadku tohto prostredia.

Prevádzkové prostredie musí zabezpečovať trvalú dostupnosť funkcií všetkých informačných systémov (a tým aj aplikačnej architektúry a bezpečnostnej infraštruktúry). Preto sa predpokladá využívanie technológií clusteringu, load-balancingu a ďalších, ktoré zabezpečia dostupnosť funkcií systémových modulov a systému aj v prípade výpadku jedného z komponentov.

Samostatnou požiadavkou je škálovateľnosť systému, t.j. prispôsobenie systému meniacim sa požiadavkám na výkonnosť. Vzhľadom na možnú finančnú úsporu je vhodné zvážiť využívanie technológií virtualizácie.

5.5.1.2 Záložné prevádzkové prostredie

Záložné prevádzkové prostredie bude slúžiť ako záloha k prevádzkovému prostrediu, bude mať totožné aplikačné vybavenie ako produkčné prostredie. Záložné prevádzkové prostredie bude prevádzkované v záložnom prevádzkovom centre a bude mať parametre umožňujúce aspoň základnú kontinuitu prevádzky a poskytovania služieb informačných systémov – preto nemusí byť výkonovo dimenzované identicky ako prevádzkové prostredie.

5.5.1.3 Stabilizačné prostredie

Stabilizačné prostredie bude podobné prevádzkovému prostrediu a bude slúžiť na finálne schválenie (predprodukčné testovanie) novej verzie pred nasadením do produkčného prostredia a zároveň bude slúžiť na overovanie prípadných problémov produkčného prostredia (identifikáciu príčiny). Stabilizačné prostredie môže byť vybudované v rámci záložného prevádzkového prostredia.

5.5.1.4 Školiace prostredie

Školiace prostredie bude slúžiť pre prípravu administrátorov a používateľov systému, ako aj vývojárov jednotlivých informačných systémov pre zvládnutie technológií potrebných pre implementáciu integračného konceptu a bezpečnostných technológií. Školiace prostredie bude minimálnym variantom prostredia, dostatočným na demonštráciu a overenie funkcionality systému.

5.5.1.5 Testovacie prostredie

Testovacie prostredie bude slúžiť na prezentovanie a testovanie zmien a novej funkčnosti v rámci iteratívneho nasadzovania, na integračné, systémové a akceptačné testy, ako aj na testovanie parciálnych verzií systému počas jednotlivých vývojových iterácií. Testovacie prostredie bude v správe Prevádzkovateľa systému.

5.6 Nasadenie riešenia a marketingové požiadavky

Okrem technologických krokov implementácie, ktoré vykoná vybraný dodávateľ v spolupráci s odbornými útvarmi v oblasti informatiky v rezorte sprístupnenie informácií potrebných pre efektívne využívanie výsledkov riešenia projektu. Informácia o novom riešení bude zverejnená na webových stránkach MS SR, na stránkach www.informatizacia.sk, portal.gov.sk/Portal/sk/default.aspx, a prostredníctvom tlačovej správy. Pri zavádzaní elektronických služieb v rámci projektu predpokladáme štandardnú a preverenú komunikáciu zo strany rezortu a ďalších zaangażovaných inštitúcií. Cieľom komunikácie bude informovať a motivovať potenciálnych užívateľov služieb s novými možnosťami služieb, propagovať tieto verejné služby, ich zefektívnenie a poukázať na vyšší komfort pre užívateľa. Pri komunikácii voči verejnosti a užívateľom e-služieb navrhujeme využiť marketingový mix (oznámenia v masmédiách rôzneho druhu – elektronické, printové, vlastné web služby, oznámenia úradoch verejnej správy; rozhovory s predstaviteľmi rezortu v masmédiách a ďalšie).

Rozpočet projektu reflektuje náklady na publicitu. Predbežne boli náklady na publicitu a informovanosť odhadnuté na 105 600,00 €. Ďalšie náklady na publicitu budú vykrývané z komunikačného rozpočtu ministerstva so zapojením príslušných pracovníkov.

Popis navrhovanej metodiky projektového riadenia celého životného cyklu.

Metodológia projektu „Projektu budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR“ je navrhovaná v zmysle požiadaviek IT projektov a projektov OPIS. Aktivita, ich dekompozícia, metodológia a špecifické výstupy budú popísané v návrhu projektu (Opis projektu). Ako štandardné a medzinárodne uznávané pre účely riadenia komplexných projektov sú odporúčané metodiky ako napr. PMI, v prípade projektov OPIS sa predpokladá PRINCE2. Vývoj softvérového diela bude realizovaný podľa metodiky RUP. Pre riadenie prevádzky IT sa aplikuje napr. ITIL.

5.7 Nefinančné prínosy a náklady

Kľúčovým nefinančným prínosom je bezpečnosť prístupu k právnym informáciám z jedného prístupového bodu. Z tohto bodu bude môcť verejnosť, podnikatelia, odborná verejnosť aj zamestnanci rezortu justície pristupovať k službám a dátam rezortu MS SR bezpečne a rýchlo, podľa vopred stanovených oprávnení.

Participujúci účastníci (stakeholderi) ocenia väčšiu transparentnosť a bezpečnosť celého procesu a zlepši sa prístup k právnym informáciám.

Ďalším nefinančným prínosom bude skvalitnenie práce, ktoré súvisí s výmenou zastaralých osobných počítačov. Táto výmena musí prebehnúť z dôvodu eliminácie bezpečnostných rizík (nepodporované Windows XP).

6 Plán implementácie – projektový zámer

6.1 Príprava projektu

Spôsob realizácie

Projekt bude realizovaný dodávateľským spôsobom, bude využívať zdroje externých dodávateľov (outsourcing) počas celého životného cyklu systémov, ako v etape predprojektovej prípravy, návrhu a implementácie, do istej miery aj prevádzky navrhovaných systémov. Metodicky a analyticky, ako projektoví manažéri a členovia všetkých projektových tímov sa budú zúčastňovať pracovníci MS SR.

V organizačnom zabezpečení projektu bude zabezpečená účasť interných zamestnancov MS SR na všetkých úrovniach riadenia projektu (Projektový výbor, resp. Projektová rada, projektoví manažéri, členovia projektových tímov).

Obsahová náplň projektu

Obsahová náplň projektu je vytvorenie podmienok pre zefektívnenie vývoja a integrácie aplikácií, riadenie bezpečnosti a zefektívnenie prevádzky informačných systémov. Dôraz sa kladie na organizačné zabezpečenie, procesy a informačné a komunikačné technológie.

Projekt na úrovni technologického riešenia bude realizovať:

- vytvorenie integračnej platformy pre integráciu informačných systémov a implementáciu komplexných procesov,
- vytvorenie prostredia pre centrálnu správu používateľov a ich prístupových práv,
- prostredie pre využívanie PKI pre autorizáciu úkonov realizovaných v rámci agend rezortu,
- prostredie pre monitorovanie systémov a zefektívnenie prevádzkových procesov a riadenia bezpečnosti informačných systémov,
- technologickú infraštruktúru systému pre realizáciu vyššie uvedených oblastí.

Ciele projektu

Základné ciele navrhovaného projektu sú:

- vytvoriť prostredie pre efektívnejší vývoj informačných systémov, využívajúcich centrálnu poskytovanú funkcionality integračnej platformy, prostredia PKI a centralizovanej správy používateľov,
- vytvoriť prostredie pre efektívnejšiu integráciu informačných systémov a ich služieb s cieľom implementácie komplexných procesov s vyššou pridanou hodnotou pre používateľov,
- vytvoriť prostredie pre efektívnejšie riadenie a výkon prevádzkových procesov,

- vytvoriť prostredie pre manažment bezpečnosti v informačných systémoch rezortu.

Výstupy projektu

- systém integračnej platformy,
- systém správy používateľov a riadenia prístupových práv,
- prostredie pre využívanie PKI pre autorizáciu úkonov,
- prostredie pre monitorovanie systémov a spracovanie prevádzkových a bezpečnostných udalostí,
- prostredie pre podporu prevádzkových aktivít,
- interná legislatíva upravujúca požiadavky na používateľov a ich povinnosti v súvislosti s využívaním novo nasadzovaných systémov a technológií.

Spôsob financovania

Program OPIS predstavuje prostriedok umožňujúci zabezpečiť finančné prostriedky potrebné pre realizáciu navrhovaného projektu ako súčasť plnenia cieľov prioritnej osi 1 opatrenia 1.1 Elektronizácia verejnej správy a rozvoj elektronických služieb na centrálnej úrovni organizácie štátnej správy a organizácie v ich zriaďovateľskej pôsobnosti. Je možné realizovať všetky etapy projektu, t.j. finančne zabezpečiť vybudovanie cieľového riešenia projektu. Podmienky poskytnutia pomoci budú uvedené v písomnom vyzvaní, keďže v tomto prípade by sa malo jednať o národný projekt.

OPIS umožňuje financovanie projektov nasledovnými spôsobmi:

- systémom zálohových platieb – ŠRO,
- systémom predfinancovania,
- systémom refundácie.

Prijímatelia - štátne rozpočtové organizácie sú oprávnení využívať systém zálohových platieb alebo systém refundácie v súlade s rozhodnutím SORO v spolupráci s prijímateľom. Pri úhradách faktúr zo zálohovej platby sú prijímatelia povinní zachovať pomer zdrojov (EU:ŠR).

Systém refundácie sa uplatňuje v prípade rozhodnutia riadiaceho orgánu po dohode s prijímateľom a v prípade záverečných platieb pri uplatnených systémoch predfinancovania. Prijímateľ môže kombinovať uvedené spôsoby v závislosti od rozhodnutia SORO stanoveného v zmluve o poskytnutí nenávratného finančného príspevku, avšak nemožno kombinovať oba spôsoby v rámci jednej žiadosti o platbu.

Systém refundácie predpokladá, že prijímateľ realizuje projekt z vlastných zdrojov a následne si náklady refunduje z OPIS. Pre potreby realizácie navrhovaného projektu sa preto javí ako výhodnejšie využiť spôsob zálohových platieb, pri ktorom v prípade 100% krytia nákladov na projekt z OPIS nie je potrebné v implementačnej fáze jeho realizácie zabezpečiť krytie zo ŠR.

6.2 Riadenie projektu a metodika riadenia

Ministerstvo financií SR vydalo Metodický pokyn MF SR č. 55/2014 v znení novely č. 276/2014 Z.z. pre riadenie IT projektov, ktorý popisuje základné požiadavky pre projektové riadenie v oblasti informačno-komunikačných technológií a je zdrojovo založený na medzinárodnej metodike PRINCE II (PProjects IN Controlled Environment – Projekty v riadenom prostredí).

Táto metodika riadenia projektov je zameraná na zadefinovanie a dodanie produktov s dôrazom na ich kvalitu; úspešný projekt je orientovaný na výsledok a nie na jednotlivé činnosti. Procesy PRINCE2 sa zameriavajú na chronologický vývoj projektu; projekt je riadený po etapách: Predprojektová príprava, Iniciácia projektu, Strategické riadenie projektu, Riadenie etapy, Riadenie dodávky produktu, Riadenie hraníc etapy, Ukončenie projektu (životný cyklus projektu).

6.3 Harmonogram projektu

Nižšie uvedený harmonogram rámcovo popisuje odhad trvania hlavných aktivít projektu. Úlohou štúdie uskutočniteľnosti bude okrem iného aj analýza možnosti realizácie jednotlivých častí projektu tak aby služby mohli byť postupne poskytované ešte pre finálnym ukončením projektu.

Návrh harmonogramu projektu

Názov aktivity	Začiatok realizácie aktivity	Ukončenie realizácie aktivity
Hlavné aktivity	(MM/RRRR)	(MM/RRRR)
Analýza a návrh riešenia	04/2015	08/2015
Obstaranie SW licencií	04/2015	06/2015
Obstaranie a nasadenie HW	04/2015	06/2015
Implementácia	04/2015	08/2015
Testovanie	05/2015	08/2015
Nasadenie	05/2015	09/2015

Podporné aktivity	(MM/RRRR)	(MM/RRRR)
Riadenie projektu	04/2015	09/2015
Publicita a informovanosť	04/2015	09/2015

Uvedené procesy a činnosti budú realizované v rámci hlavných a podporných aktivít projektu:

Aktivita 1: Analýza a návrh riešenia

Aktivita bude realizovaná od začiatku technickej časti projektu, prevažne v úvodnej fáze, pričom sa vzhľadom na prepojenie aktivít a možnú potrebu priebežných úprav ukončí predbežne 1 mesiac pred ukončením implementácie technického riešenia.

Má nasledujúce hlavné aktivity:

- Detailná definícia požiadaviek, pričom dôjde k podrobnej analýze potrieb budúcich používateľov;
- Definovanie podrobných požiadaviek na funkcie systému;
- Validácia navrhnutej architektúry;
- Rozvoj prostredia projektu, ktoré zastrešuje jednotlivé vrstvy architektúry;
- Vytvorenie projektového tímu.

Hlavné míľniky tejto fázy označené ako Míľniky architektúry sú:

- Stabilná vízia;
- Dohodnutá množina požiadaviek;
- Validovaný návrh architektúry;
- Akceptácia rizík;
- Akceptácia nákladov;
- Reálna šanca na úspech;
- Detailne špecifikovaný projektový plán.

Počas fázy Analýzy a návrhu budú podrobnejšie špecifikované požiadavky, čím sa overí navrhnutá architektúra systému. Tieto požiadavky sú podrobne uvedené do tej miery, aby bolo možné pochopiť riziká architektúry a zabezpečiť pochopenie rozsahu každej požiadavky pre následné plánovanie. Na overenie architektúry sa implementuje a otestuje „end-to-end“ kostra pracovného kódu, ktorý podporuje vysoko rizikové prípady použitia systému. Na konci tejto fázy je nutné preveriť míľniky architektúry.

V rámci tejto etapy bude vypracovaný

- Procesný model
- Analýza a Funkčná špecifikácia
- Technická architektúra systému

V rámci tejto Aktivity budú detailne analyzované a navrhnuté nasledovné moduly:

- Integrovaná platforma
- PKI infraštruktúra
- Správa používateľov

Aktivita 2: Obstaranie SW licencií

- V rámci tejto etapy bude realizovaná dodávka potrebných SW licencií. Tieto prostriedky budú nasadené do produkčného prostredia tak, aby mohli byť nasadené a implementované moduly IS BAA.

V rámci tejto aktivity sa zabezpečí nasledovný SW pre primárne dátové centrum:

Integračná platforma	Softvér a licencie pre Integračné platformy
Správa používateľov (IAM)	Softvér a licencie pre Aplikačnú podporu
Správa používateľov (IAM)	Softvér a licencie pre Aplikačnú podporu - mobilné zariadenia
PKI	PKI SW infraštruktúra
Bezpečnosť	Licencia pre Aplikačný firewall a load balancing
Bezpečnosť	Licencia nástroja pre logovanie a analýzu logov
Bezpečnosť	Licencia systému ochrany proti sieťovej infiltrácii
Bezpečnosť	Licencia systému ochrany proti aplikačnej infiltrácii
Bezpečnosť	Licencia pre biometrickú autentifikáciu
Bezpečnosť	Softvér a licencie pre inteligentný editor
Bezpečnosť	Softvér a licencie pre Komunikačné systémy a zabezpečenie
Podpora prevádzky	Softvér a licencie pre Databázy
Podpora prevádzky	Licencia pre Monitoring a Event management (network)
Podpora prevádzky	Licencia pre Monitoring a Event management (systémy a aplikácie)
Podpora prevádzky	Licencie pre Sledovanie a analýzu výkonnosti aplikácií
Podpora prevádzky	Licencia pre Správu licencií a využitia
Podpora prevádzky	Licencia pre podporu používateľov a procesy riešenia incidentov
Softvér	Softvér a licencie pre operačný systém Microsoft Windows Server Datacenter edition
Softvér	Licencie pre operačný systém RedHat Linux Enterprise Standard
Softvér	Softvér a licencie pre Databázy (licencia na procesor - skóre 10000)
Softvér	Softvér a licencie pre operačný systém Microsoft Windows Server Standard edition

Aktivita 3: Obstaranie a nasadenie HW

- V rámci tejto etapy bude realizovaná dodávka HW infraštruktúry. Tieto prostriedky budú nasadené do produkčného prostredia tak, aby mohli byť nasadené a implementované moduly IS BAA.
- Rozdelenie HW:
 - HW - servery (OS, AS, WS, RDBMS)
 - HW - sieťové komponenty (LAN)
 - HW – PC a tablety

V rámci tejto aktivity sa zabezpečí nasledovný HW pre primárne dátové centrum:

Integračná platforma	Server pre IP - 2 CPU, 48GB RAM, 1TB SAS 10k HDD, 2x1 Gbit/s
Správa používateľov (IAM)	Server pre IAM - 2 CPU, 48GB RAM, 1TB SAS 10k HDD, 2x1 Gbit/s
PKI	Počítač operátora RA
PKI	Monitor LCD Operátora RA
PKI	Multifunkčná tlačiareň operátora RA
PKI	Čítačka čipových kariet
PKI	Čipová karta
Bezpečnosť	Počítač sudcu a vyššieho súdneho úradníka
Bezpečnosť	Tlačiareň súdu
Bezpečnosť	Tablet sudcu
Bezpečnosť	Prenosný počítač sudcu
Bezpečnosť	Server pre aplikačný firewall a load balancing
Bezpečnosť	Server pre Logovanie a analýzu logov (SIEM) - 2 CPU, 128GB RAM, 14TB HDD
Bezpečnosť	Server pre Logovanie a analýzu logov (SIEM) - 2 CPU, 48GB RAM, 1TB SAS 10k HDD, 2x1 Gbit/s
Bezpečnosť	Server pre systém ochrany proti sieťovej infiltrácii
Bezpečnosť	L2/L3 Switch pre systém ochrany proti sieťovej infiltrácii
Bezpečnosť	Server pre systém ochrany proti aplikačnej infiltrácii 2 CPU, 48GB RAM, 1TB SAS 10k HDD, 2x1 Gbit/s
Bezpečnosť	Samostatný sieťový firewall
Bezpečnosť	Prístupový prepínač pre DC
Bezpečnosť	Server pre biometrickú autentifikáciu
Bezpečnosť	Server pre Logovanie a monitoring - 2 CPU, 48GB RAM, 1TB SAS 10k HDD, 2x1 Gbit/s
Bezpečnosť	HSM modul umiestniteľný do štandardného PCIe rozhrania s 2000 transakciami za sekundu

Aktivita 4: Implementácia

V rámci aktivity Implementácia budú zabezpečené činnosti súvisiace s postupnou implementáciou modulov technického riešenia a ich integráciou medzi sebaÚPVSou a IS BAA s ostatnými ISVS. Cieľom tejto aktivity je implementácia a integrácia nasledovných modulov IS:

- Integračná platforma
- PKI infraštruktúra
- Správa používateľov

Má nasledujúce hlavné aktivity:

- Vývoj a programovanie;
- Implementácia a testovanie systémov;
- Vytvorenie dokumentácie riešenia.

Hlavné míľniky tejto fázy označené na predchádzajúcom obrázku ako Míľniky počiatkovej funkcionality sú:

- Stabilné riešenie;

- Aktualizovaná množina požiadaviek;
- Pripravení a oboznámení stakeholderi;
- Akceptácia rizík;
- Akceptácia nákladov;
- Projektový plán.

Fáza Implementácie sa zameriava na vytvorenie systému, ktorý je pripravený na nasadenie. Dôraz sa kladie na prioritizovanie požiadaviek a dokončenie ich špecifikácie, na ich analýzu, návrh riešenia, ktoré ich spĺňa, a programovanie a testovanie softvéru a testovanie komunikačnej infraštruktúry. Na konci tejto fázy musia byť splnené Míľniky počiatočnej funkcionality.

Aktivita 5: Testovanie

Aktivita testovania začne postupne po ukončení analyticko-vývojových činností jednotlivých funkcionalít v 2. mesiaci implementácie. Predpokladané ukončenie aktivity je 1 mesiac pred ukončením projektu, v nadväznosti na posledné implementačné práce. Cieľom aktivity je preveriť interakciu medzi modulmi, správnosť integrácie komponentov softvéru, či všetky požiadavky boli správne implementované a identifikovať chyby a zaistiť ich riešenie pred nasadením IS BAA do ostrej prevádzky.

V rámci tejto aktivity prebehne testovanie nasledovných modulov IS a ich integračné testovanie:

- Integračná platforma
- PKI infraštruktúra
- Správa používateľov

Aktivita 6: Nasadenie

Cieľom predmetnej aktivity je postupné nasadzovanie základnej infraštruktúry, prvá iterácia úprav, sada integračných služieb a portálov so službami. Prvé nasadzovania sa uvažujú v polovici časového harmonogramu technického riešenia ak neuvažujeme obstarávanie, zazmluvnenie a spúšťanie projektu. Úlohou aktivity je úspešné vytvorenie produkčných verzií a sprístupnenie aplikácií koncovým používateľom. Bude tiež zahŕňať činnosti ako plánovanie a riadenie beta testovania, migrácia existujúcich údajov, formálnu akceptáciu. Nasadzovanie bude trvať do konca trvania projektu. V rámci aktivity prebehne nasadenie nasledovných modulov IS BAA:

- Integračná platforma
- PKI infraštruktúra
- Správa používateľov

Aktivita takisto predpokladá činnosti v oblasti školenia kľúčových používateľov/školiteľov na strane MS SR, ktoré bude poskytovať dodávateľ technického riešenia a jeho plán bude súčasťou sprievodnej projektovej dokumentácie z implementácie projektu. Okrem modulu „Školenie školiteľov“ žiadateľ vypracuje bezpečnostný projekt.

Počet školení:	11
Minimálny počet účastníkov na školení:	7
Dĺžka trvania jedného školenia:	24 osobohodín
Predmet školení:	školenia školiťel'ov, školenia administrátorov, technické školenia

Súčasťou školení bude aj školiaca dokumentácia a v cene sú zahrnuté aj náklady na prípravu školení (napr. príprava priestorov, príprava školiacej dokumentácie a pod.).

Podporná aktivita: Riadenie projektu

Aktivita bude trvať počas celej doby spúšťania, realizácie a ukončovania projektu. Pokrýva činnosti verejného obstarávania, celostného projektového riadenia, finančného riadenia a monitorovania realizácie projektu v zmysle systému riadenia ŠF a KF a systému finančného riadenia ŠF a KF.

Grant projektu bude zabezpečovať strategickú koordináciu projektových činností na strane prijímateľa. Projektový manažér bude riadiť administratívne a organizačné zabezpečenie implementácie projektu, komunikovať a spolupracovať s vybraným dodávateľom, komunikovať s RO a SORO, sledovať plnenie harmonogram projektu a zabezpečovať dokumenty požadované RO a SORO. Asistent projektového manažéra bude zabezpečovať administratívnu podporu projektu, písomnú komunikáciu, administratívne vedenie projektovej dokumentácie a prípravu podkladov pre členov projektového tímu. Finančné riadenie projektu (žiadosti o platbu), kontrolu rozpočtu projektu a jeho súladu s účtovnými dokladmi, kontrolu podpornej účtovnej dokumentácie a poradenstvo pri definovaní oprávnených výdavkov bude zabezpečovať finančný manažér. Činnosť manažéra monitorovania bude zahŕňať monitorovanie projektu (monitorovacie správy), kontrolu jeho priebehu a súladu s cieľmi, monitorovanie naplňovania indikátorov projektu a vyhodnocovanie plnenia jednotlivých aktivít projektu. Interné kapacity pre riadenie projektu budú v prípade potreby doplnené externými kapacitami.

Riadenie projektu pokrýva aj aktivity podľa aktuálnej metodiky riadenia IT projektov vo verejnej správe a príslušné výstupy projektového cyklu v zmysle výnosu k štandardom pre ISVS č. 55/2014, ktoré bude zabezpečovať prijímateľ a to svojimi zdrojmi, v spolupráci s dodávateľom technického riešenia. V neposlednom rade bude aktivita riadenia projektu pokrývať tzv. zaistenie kvality (quality assurance).

Výstupmi aktivity budú žiadosť o NFP a jej prílohy, dokumentácia k verejnému obstarávaniu, dokumentácia k riadeniu projektu, žiadosti o platbu, monitorovacie správy projektu a pod.

Táto aktivita bude realizovaná len vnútornými zamestnancami podľa pravidiel odmeňovania MS SR.

Podporná aktivita: Publicita a informovanosť

Aktivita pokrýva oblasť výdavkov na zabezpečenie aktivít informovania a publicity v súlade s Manuálom pre informovanie a publicitu. MS SR umiestni na mieste realizácie projektu reklamnú tabuľu o projekte (1 x) a najneskôr do 6 mesiacov po ukončení realizácie projektu trvalo vysvetľujúcu tabuľu (1 x). Na miestach realizácie (zainteresované sekcie, pracoviská) bude zabezpečená informovanosť plagátmi. MS SR vydá

tlačovú správu, ktorá bude obsahovať informácie o projekte, jeho prínosoch, o výške NFP, OPIS a ERDF, vydá a roz distribuuje tlačенý informačný materiál k aktivitám projektu, zabezpečí reklamné a propagačné predmety, informačné a komunikačné materiály o projekte a zrealizuje aj informovanie širokej verejnosti prostredníctvom médií a tlačových konferencií.

Príloha č.1 - Rozpočet a nákladovo výnosová analýza

6.4 Strategický kontext

Štúdiá je vypracovaná súlade so záväznými strategickými dokumentmi:

- Záverečný informatívny dokument – IT služby pre eJustice
- Operačný program informatizácia spoločnosti,
- Stratégia informatizácie verejnej správy,
- Národná koncepcia informatizácie verejnej správy,
- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov (v znení č. 678/2006 Z. z., č. 385/2008 Z. z., č. 553/2008 Z. z., č. 570/2009 Z. z., č. 69/2012 Z. z.) /Účinný od 1.1.2011/
- Výnos Ministerstva financií Slovenskej republiky č. 55/2014 o štandardoch pre informačné systémy verejnej správy v znení,
- Zákon č. 305/2014 o eGovernmente.

Pri zavádzaní každého nového systému, je potrebné zohľadniť náklady na jeho vybudovanie, ako aj možné úspory vznikajúce zavedením systému a zmenou existujúcich procesov.

6.5 Ciele a obmedzenia

Obsahom analýzy nákladov a prínosov je vyčíslenie budúcich nákladov a prínosov projektu, ktorého výsledkom má byť elektronizácia vybraných služieb. Výstupom CBA je súhrnný ukazovateľ čistej súčasnej hodnoty (NPV) uvádzaný v EUR a návratnosť investície (ROI) uvádzaná v rokoch. Oba ukazovatele vyjadrujú porovnanie celkových nákladov a prínosov dvoch alternatív:

Alternatíva 1 – kvantifikácia nákladov a prínosov východiskového stavu služieb, tzn. že poskytovanie služieb bude prebiehať bez realizácie projektu OPIS, tak ako doposiaľ, prevažne v papierovej, resp. v kombinovanej podobe.

Alternatíva 2 – kvantifikácia cieľového stavu po realizácii projektu elektronizácie služieb, tzn. že poskytovanie služieb bude prebiehať v elektronizovanej podobe na vyššej úrovni sofistikovanosti v rôznom nábehu do produkčnej prevádzky.

Predpoklady, z ktorých výpočet analýzy výnosov a nákladov vychádzal:

- Pri nahrádzaní v súčasnosti poskytovaných služieb elektronickými sa pre účely analýzy predpokladá ich 100%-ná substitúcia.
- Početnosť použitia elektronických služieb sa vzhľadom na analyzovaný charakter služieb a činnosti v oboch alternatívach počas uvažovaných rokov rovnaká, avšak elektronizácia viacerých agend má vplyv na zmenu počtu ich volaní.
- Trvanie vybavenia agendy bude trvať po realizácii projektu kratšie na strane poskytovateľa aj používateľa.
- Priemerný počet zamestnancov na strane poskytovateľa služby, ktorí sú priamo zapojení do spracovania agendy je 20. Títo zamestnanci však nevenujú 100% svojho pracovného času vybavovaniu agendy.
- Pre výpočet nákladov a prínosov a vzájomnej porovnateľnosti budú pre obe alternatívy platiť rovnaké faktory.

Parametre boli stanovené osobitne pre každú alternatívu. Boli odhadnuté na základe empirických údajov o počte podaní, trvaní služby a pod. za posledné 3 roky a po realizácii projektu.

Nákladovo-výnosová analýza zohľadňuje oprávnené aj neoprávnené priame výdavky, neobsahuje výdavky na nepriame náklady (podporné aktivity projektu) a nezohľadňuje infláciu.

Pri hodnotení prínosu elektronických služieb je v dôsledku času potrebného na vývoj a nasadenie IS do reálnej prevádzky zohľadnené v Alternatíve 2, že oneskorenie nevzniká.

Tento prístup prispieva k zaisteniu udržateľného rozvoja. Použitá metodika Analýzy nákladov a prínosov je v súlade s „Metodickým rámcom MF SR pre analýzu nákladov a prínosov (Metodický rámec pre projekty prioritnej osi 1 Elektronizácia verejnej správy a rozvoj elektronických služieb OPIS, zameranej na celkovú architektúru eGovernmentu, Analýza nákladov a prínosov Ministerstva financií SR). Cieľom CBA analýzy je vyhodnotenie komplexných sociálno-ekonomických dopadov na obyvateľstvo.

Ekonomická návratnosť riešenia je závislá od vzťahu medzi nákladmi potrebnými na vytvorenie a prevádzkovanie riešenia a prínosmi, ktoré poskytuje. Nákladová časť je ovplyvnená cenou vybudovania riešenia, ktorej odhad je uvedený v kapitole 7. tejto Prílohy. Presná hodnota nákladov bude však určená až spôsobom zabezpečenia služieb a výsledkom verejného obstarávania. Cena prevádzkovania riešenia bude vychádzať z výsledného návrhu riešenia a spôsobu zabezpečenia prevádzky.

Prínosy riešenia sa prejavujú na strane verejnej správy ako aj podnikateľov a verejnosti.

Pre výpočet CBA boli použité nasledovné predpoklady:

Na základe simulácie funkčnosti riešenia, odhadu účastníkov volaných služieb a ďalších parametrov bola vykonaná kvantifikácia prínosov a nákladov projektu.

1. odhad priamych finančných nákladov subjektu na realizáciu projektu

2. stanovenie a kvantifikácia prínosov implementácie projektu pre jeho užívateľov

Pre odhad jednotlivých parametrov boli využité nasledujúce podporné vstupné údaje, ktoré vychádzajú z oficiálnych dát Štatistického úradu SR a iných verejných zdrojov. Jednotlivé údaje a ich prepočty sú uvedené v nasledujúcej tabuľke č.6:

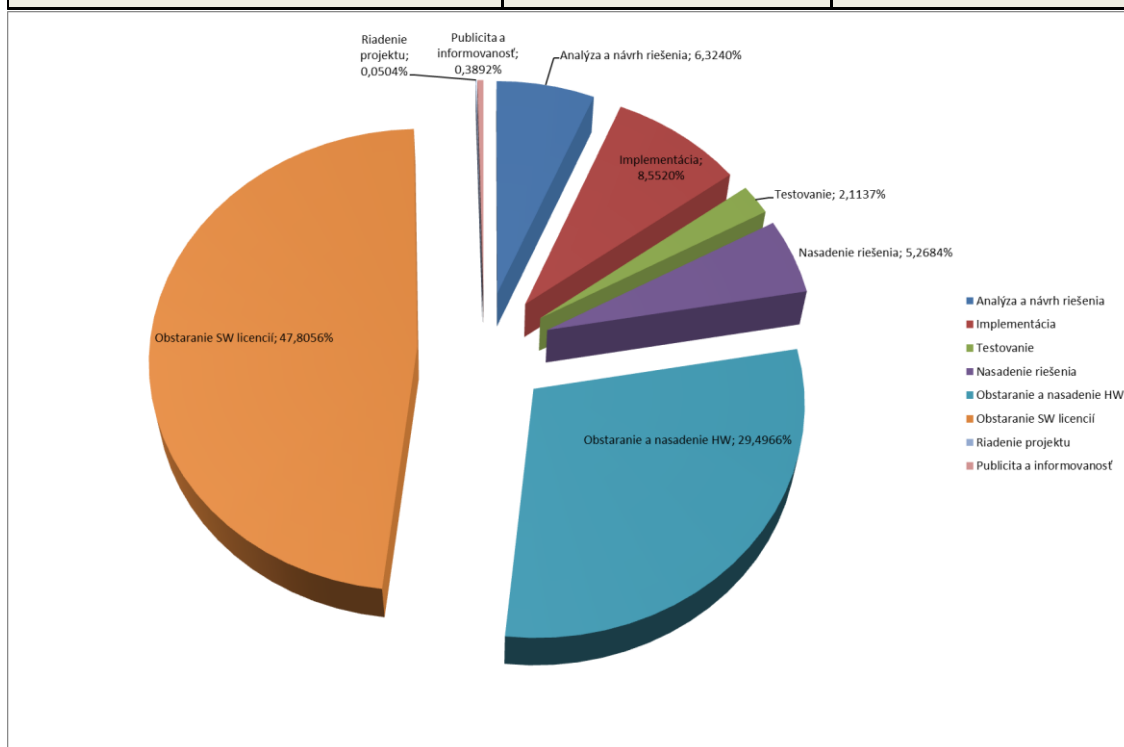
Názov faktora	Popis	Referenčná hodnota
Životnosť projektu (t)	Referenčné obdobie je počet rokov, na ktorý sa v analýze nákladov a výnosov uvádzajú predpovede.	15 rokov
Diskontná sadzba (r)	Systém riadenia ŠF a KF v prípade verejných investičných projektov spolufinancovaných z fondov stanovuje 5,5 % finančnú diskontnú sadzbu pre výpočet čistej súčasnej hodnoty investície v stálych cenách roku predloženia žiadosti o NFP.	5,5 %
Osobné náklady (Cper)	<p>Cper (poskytovateľ) = Cper (VS) = $980 \cdot 1,358 / 160 = 8,32$ EUR/hod, pričom 980 EUR je priemerná hrubá mzda vo verejnej správe za rok 2014 (zdroj: http://portal.statistics.sk/showdoc.do?docid=35594). Odvody (SP, ZP, SF) sú 35,8%. Fond pracovnej doby na 1 mesiac je 160 hodín (čas na prestávku nie je započítaný).</p> <p>Cper (SS) = $786 \cdot 1,358 / 160 = 6,67$ EUR/hod, pričom 786 EUR je priemerná hrubá mzda v národnom hospodárstve za rok 2014 (zdroj: http://portal.statistics.sk/showdoc.do?docid=35594). Odvody (SP, ZP, SF) sú 35,8%. Fond pracovnej doby na 1 mesiac je 1920 hodín/rok (čas na prestávku nie je započítaný).</p>	<p>8,12 EUR/hod (poskytovateľ)</p> <p>6,67 EUR/hod (používateľ)</p>

	Osobné náklady sú faktorom prevádzkových variabilných nákladov.	
Materiálové náklady podania (Cpap)	(Cpap) = Poštovné (0,83 EUR) + Tlač (0,02 EUR) + Papier (0,01 EUR) + Obálka (0,03 EUR). Predpokladom CBA je 1 podanie = 1 papierová zásielka. Materiálové náklady podania sú faktorom prevádzkových variabilných nákladov.	0,89 EUR
Názov faktora	Popis	Referenčná hodnota

6.6 Rozpočet projektu

Tabuľka 7

Priemerná cena človekodňa objednávateľa v eur s DPH		660
Priemerná cena človekodňa zamestnanca MS SR v eur s DPH		108
Aktivita	Odhadovaná prácnosť v človekohodinách	Odhadovaná prácnosť v človekodňoch
Analýza a návrh riešenia	12 000,00	1 500,00
Implementácia	30 528,00	3 816,00
Testovanie	8 152,00	1 019,00
Nasadenie riešenia	22 528,00	2 816,00
Obstaranie HW		
Obstaranie SW licencií		
Riadenie projektu		
Publicita a informovanosť		
SPOLU	73 208,00	9 151,00



Tabuľka 8 Odhadovaná výška rozpočtu

Typ výdavku	Položka	Suma v € vrátane DPH
Služby	Analýza a návrh riešenia	1 716 000,00 €
	Implementácia	2 320 560,00 €
	Testovanie	573 540,00 €
	Nasadenie riešenia	1 429 560,00 €
	Riadenie projektu	32 760,00 €
	Publicita a informovanosť	86 520,00 €
Služby spolu		6 158 940,00 €
HW	Obstaranie a nasadenie HW	8 003 784,00 €
SW licencie	Obstaranie SW licencií	12 971 856,00 €
SPOLU		27 134 580,00 €

Náklady na realizáciu „Projektu budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR“ budú ovplyvnené výsledkom verejného obstarávania jednotlivých položiek potrebných pre vybudovanie riešenia. Vzhľadom na funkčnosť a zameranie riešenia bude potrebné vybudovať bezpečný a stabilný systém.

Pre odhad náročnosti vývoja aplikácie bola použitá metóda Use Case Points. Vybudovanie a sprevádzkovanie riešenia si vyžaduje aj ďalšie projektové činnosti, ktorých náročnosť je odvodená na základe skúseností a benchmarkov.

Prácnosť týchto činností vzhľadom na celkové náklady vybudovania a sprevádzkovania riešenia je odhadovaná vo výške:

Aktivita	Rozdelenie %	Rozdelenie ks MD
Analýza a návrh riešenia	6,3240%	2 600,00
Implementácia	8,5520%	3 516,00
Testovanie	2,1137%	869,00
Nasadenie riešenia	5,2684%	2 166,00
Obstaranie a nasadenie HW	29,4966%	
Obstaranie SW licencií	47,8056%	
Riadenie projektu	0,0504%	
Publicita a informovanosť	0,3892%	
SPOLU	100,00%	9 151,00

Náklady na implementáciu aplikačného programového vybavenia obsahujú činnosti spojené s analytickou a vývojovou časťou projektu. Jedná sa o identifikovanie požiadaviek, návrh riešenia, prípravu legislatívnych úprav ako aj vývoj aplikačného vybavenia.

Testovanie obsahuje prípravné činnosti potrebné pre vykonanie dôkladného overenia funkčnosti riešenia. Obsahuje to prípravu testovacích scenárov, testovanie programových blokov, integračné a záťažové testy. Súčasťou týchto činností je aj akceptačné testovanie vzhľadom na špecifikované požiadavky.

V rámci školení je obsiahnutá ako príprava tak aj samotná realizácia školení. Školenie bude rozdelené na školenie používateľov a školenie administrátorov riešenia. Harmonogram školení bude navrhnutý tak, aby používatelia boli schopní adekvátne otestovať dodané riešenie.

Činnosti v rámci roll out-u sú zamerané na uvedenie riešenia do produkčného prostredia. Budú obsahovať spustenie funkčnosti vytvorených elektronických služieb, prípadnú konverziu údajov pre živé agendy a zabezpečenie produkčnej spolupráce s externými systémami.

Na základe uvedeného výpočtu a predpokladanej priemernej ceny 550 Eur bez DPH za človeko/deň poskytovania služieb je predpokladaná cena vytvorenia riešenia (nákupu SW) a jeho uvedenia do prevádzky 19,011 mil. Eur s DPH.

Vybudovanie riešenia si vyžaduje okrem uvedených činností aj náklady na zabezpečenie HW a jeho nasadenie v sume 8,003 mil. Eur s DPH.

Náklady na podporné aktivity, ktoré obsahujú riadenie projektu, riadenie, ako aj zabezpečenie publicity je možné predpokladať v sume viac ako 119 280 Eur s DPH.

Na základe vyššie uvedených položiek je možné očakávať celkové náklady na realizáciu „Projektu budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR“ v sume 27,134 mil. Eur s DPH.

Tabuľka 9 Rozpočet projektu odhadovaný

Priame výdavky - Hlavné aktivity	v EUR s DPH	v EUR bez DPH	celkových výdavkov
610620 Osobné náklady	0,00 €	0,00 €	0,00%
637001 Školenia, kurzy, semináre, porady, konferencie, sympóziá	0,00 €	0,00 €	0,00%
637003 Propagácia, reklama a inzercia	86 520,00 €	72 100,00 €	0,32%
637004 Všeobecné služby - Riadenie projektu	32 760,00 €	13 680,00 €	0,12%
711003 Nákup softvéru	19 011 516,00 €	15 842 930,00 €	70,06%
713002 Nákup výpočtovej techniky	8 003 784,00 €	6 669 820,00 €	29,50%
Celkový súčet	27 134 580,00 €	22 598 530,00 €	100,00%

6.7 Analýza nákladov

Tabuľka 10 Odhadované náklady projektu

Obdobie	NÁKLADY								
	HW			Fixné náklady SW			Služby		
	Alternat. 1	Alternat. 2	rozdiel	Alternat. 1	Alternat. 2	rozdiel	Alternat. 1	Alternat. 2	rozdiel
t1	23 000,00	8 026 784,00	8 003 784,00	61 000,00	13 032 856,00	12 971 856,00	185 000,00	6 224 660,00	6 039 660,00
t2	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
t3	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
t4	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
t5	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
t6	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
t7	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
t8	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
t9	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
t10	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
t11	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
t12	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
t13	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
t14	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
t15	23 000,00	212 631,00	189 631,00	61 000,00	783 280,80	722 280,80	185 000,00	433 220,00	248 220,00
Alternat. 1	Variabilné náklady						Náklady spolu		
	Všeobecný materiál			Osobné náklady			Alternat. 1	Alternat. 2	rozdiel
	Alternat. 1	Alternat. 2	rozdiel	Alternat. 1	Alternat. 2	rozdiel			
58 000,00	58 000,00		0,00	480 000,00	480 000,00	0,00	807 000,00	27 822 300,00	27 015 300,00
58 000,00	57 420,00		-580,00	528 000,00	470 400,00	-57 600,00	855 000,00	1 956 951,80	1 101 951,80
58 000,00	56 846,00		-1 154,00	580 800,00	460 992,00	-119 808,00	907 800,00	1 946 969,80	1 039 169,80
58 000,00	56 278,00		-1 722,00	638 880,00	451 772,00	-187 108,00	965 880,00	1 937 181,80	971 301,80
58 000,00	55 715,00		-2 285,00	702 768,00	442 737,00	-260 031,00	1 029 768,00	1 927 583,80	897 815,80
58 000,00	55 158,00		-2 842,00	773 045,00	433 882,00	-339 163,00	1 100 045,00	1 918 171,80	818 126,80
58 000,00	54 606,00		-3 394,00	850 350,00	425 204,00	-425 146,00	1 177 350,00	1 908 941,80	731 591,80
58 000,00	54 060,00		-3 940,00	935 385,00	416 700,00	-518 685,00	1 262 385,00	1 899 891,80	637 506,80
58 000,00	53 519,00		-4 481,00	1 028 924,00	408 366,00	-620 558,00	1 355 924,00	1 891 016,80	535 092,80
58 000,00	52 984,00		-5 016,00	1 131 816,00	400 199,00	-731 617,00	1 458 816,00	1 882 314,80	423 498,80
58 000,00	52 454,00		-5 546,00	1 244 998,00	392 195,00	-852 803,00	1 571 998,00	1 873 780,80	301 782,80
58 000,00	51 929,00		-6 071,00	1 369 498,00	384 351,00	-985 147,00	1 696 498,00	1 865 411,80	168 913,80
58 000,00	51 410,00		-6 590,00	1 506 448,00	376 664,00	-1 129 784,00	1 833 448,00	1 857 205,80	23 757,80
58 000,00	50 896,00		-7 104,00	1 657 093,00	369 131,00	-1 287 962,00	1 984 093,00	1 849 158,80	-134 934,20
58 000,00	50 387,00		-7 613,00	1 822 802,00	361 748,00	-1 461 054,00	2 149 802,00	1 841 266,80	-308 535,20
						SPOLU	20 155 807,00	54 378 148,20	34 222 341,20

Tabuľka 10 poskytuje rámcový prehľad nákladov potrebných na implementáciu projektu Budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR.

Metodika CBA rozlišuje náklady na fixné a variabilné.

Alternatíva 1 predstavuje súčasný stav a teda situáciu bez implementácie projektu. Údaje pre fixné náklady tejto alternatívy vychádzajú z priemerných výdavkov na IKT za posledné tri roky v členení na hardvér, softvér a služby. Keďže ide o situáciu bez implementácie projektu, pre účely CBA modelujeme rovnakú výšku fixných nákladov až do konca projektového cyklu (15 rokov). Variabilné náklady sa delia na všeobecný materiál a osobné náklady. Ich výšku určuje metodika CBA (viď predpoklady).

Alternatíva 2 predstavuje stav nákladov v prípade implementácie projektu. Pre fixné náklady platí, že rozdiel medzi alternatívou 2 a alternatívou 1 v prvom roku, počas ktorých je plánovaná implementácia projektu, predstavuje výšku investícií alebo hodnotu NFP.

Predpoklady - Pokles variabilných nákladov v alternatíve 2 súvisí s poklesom nákladov na všeobecný materiál a so znižovaním osobných nákladov.

Pri modelovaní výšky nákladov na všeobecný materiál vychádzame z predpokladu, že náklady na jedno podanie sú vo výške 0,89 EUR. Metodika CBA uvažuje s touto hodnotou ako minimálnou, a je možné v prípade potreby odôvodniť jej nárast. Pri výpočte CBA projektu Budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR však vo všeobecnosti vychádzame z konzervatívnych predpokladov. To znamená, že v prípade odhadovaných údajov podhodnocujeme prínosy a nadhodnocujeme náklady alternatívy 2. Z rovnakého dôvodu modelujeme medziročný pokles nákladov na všeobecný materiál po realizácii projektu len vo výške 1%.

Elektronizácia procesov povedie v alternatíve 2 po sprevádzkovaní riešenia k skráteniu času vybavovania na strane rezortu spravodlivosti. V CBA sa to prejaví poklesom osobných nákladov na vybavovanie konkrétnych agend. Ušetrený časový fond je možné riešiť presunmi zamestnancov na iné pracovné pozície (napr. tvorba metodík, rezortných analýz, presun na prioritné oblasti záujmu rezortu a pod.), prípadne môže nastať situácia, že služby, ktoré boli doteraz poddimenzované a kapacity rezortu spravodlivosti nestihli vybaviť celý dopyt po žiadaných službách, budú môcť byť poskytované v požadovanej frekvencii a kvalite aj nad rámec doterajších kapacitných možností.

Odchod mimo pracovný pomer je rovnako jednou s alternatív, pričom takéto rozhodnutie bude plne v kompetencii vedenia MS SR.

Po implementácii projektu očakávame, že MS SR vzniknú dodatočné náklady na správu a prevádzku vybudovaných IS. Tieto náklady sú odhadované ročne vo výške 8% alebo 10% z celkovej výšky fixných nákladov na služby. V CBA sa prejavujú nárastom fixných nákladov v alternatíve 2 v rokoch 2 až 15 pri položke Služby.

Tieto náklady nie sú oprávneným výdavkom v zmysle OPIS a ministerstvo bude musieť nájsť na ich financovanie zdroje z vlastného rozpočtu, čím zároveň zabezpečí trvalú udržateľnosť projektu Budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR.

ČISTÉ PRÍNOSY		Čisté prínosy					
		Finančné prínosy			Ekonomické prínosy		
Obdobie		Alternat. 1	Alternat. 2	rozdiel	Alternat. 1	Alternat. 2	rozdiel
t1		-807 000,00	-27 822 300,00	-27 015 300,00	-807 000,00	-27 822 300,00	-27 015 300,00
t2		-855 000,00	-1 956 951,80	-1 101 951,80	-855 000,00	3 221 916,53	4 076 916,53
t3		-907 800,00	-1 946 969,80	-1 039 169,80	-907 800,00	3 231 898,53	4 139 698,53
t4		-965 880,00	-1 937 181,80	-971 301,80	-965 880,00	3 241 686,53	4 207 566,53
t5		-1 029 768,00	-1 927 583,80	-897 815,80	-1 029 768,00	3 251 284,53	4 281 052,53
t6		-1 100 045,00	-1 918 171,80	-818 126,80	-1 100 045,00	3 260 696,53	4 360 741,53
t7		-1 177 350,00	-1 908 941,80	-731 591,80	-1 177 350,00	3 269 926,53	4 447 276,53
t8		-1 262 385,00	-1 899 891,80	-637 506,80	-1 262 385,00	3 278 976,53	4 541 361,53
t9		-1 355 924,00	-1 891 016,80	-535 092,80	-1 355 924,00	3 287 851,53	4 643 775,53
t10		-1 458 816,00	-1 882 314,80	-423 498,80	-1 458 816,00	3 296 553,53	4 755 369,53
t11		-1 571 998,00	-1 873 780,80	-301 782,80	-1 571 998,00	3 305 087,53	4 877 085,53
t12		-1 696 498,00	-1 865 411,80	-168 913,80	-1 696 498,00	3 313 456,53	5 009 954,53
t13		-1 833 448,00	-1 857 205,80	-23 757,80	-1 833 448,00	3 321 662,53	5 155 110,53
t14		-1 984 093,00	-1 849 158,80	134 934,20	-1 984 093,00	3 329 709,53	5 313 802,53
t15		-2 149 802,00	-1 841 266,80	308 535,20	-2 149 802,00	3 337 601,53	5 487 403,53
SPOLU		-20 155 807,00	-54 378 148,20	-34 222 341,20	-20 155 807,00	18 126 008,47	38 281 815,47

Prínosy sú v CBA metodológii vyjadrené ako suma priamych a nepriamych prínosov. Pri výpočte prínosov vchádzajú do kalkulácie viaceré premenné. Pre účely nášho modelu sme vychádzali z nasledovných predpokladov a zistení:

- V súčasnom stave dosahuje početnosť definovaných elektronických služieb 3,55 mil.,
- Údaje o početnosti poskytovaných služieb vychádzajú z osobných pohovorov so zástupcami jednotlivých organizačných zložiek rezortu spravodlivosti,
- Predpokladáme, že elektronizácia neprinesie ročné zníženie frekvencie využívania služieb, zvolili sme veľmi konzervatívny prístup,

Predpoklady:

- Interní zamestnanci - 600 zamestnancov sa prihlasujú v súčasnosti 3 x denne autentifikáciou do 3 rôznych systémov, predpokladáme, že ročne strávia v práci 250 dní
- špecializovaní používatelia – 8000 používateľov, využívajú dnes autentifikáciu/podanie 1x denne, ročne 250 dní, v súčasnosti je možné využívať služby len listinne/na papieri
- nešpecializovaní používatelia využívajú služby v odhadovanej výške 100.000 dožiadaní ročne
- integrovaná služba – predpokladáme, že sa využíva 100.000krát ročne samostatne, po integrácii sa zníži početnosť prihlasovaní do systémov na tretinu
- Pre výpočet úspory času sme vychádzali z predpokladu, že elektronické služby na konci uvažovaného obdobia bude využívať :

Čo sa týka priamych prínosov, pri ich analýze neuvažujeme s výberom správnych poplatkov, pričom pre alternatívu 2 po realizácii projektu uvažujeme s nulovými správnymi poplatkami. Do priamych prínosov zarátavame len predpokladané zníženie osobných nákladov po zavedení projektu.

Základným zistením tohto modelového príkladu je fakt, že kľúčovým prínosom z projektu sú nepriame prínosy, t.j. výrazné zníženie záťaže prihlasovania do jednotlivých systémov občanov, podnikateľov aj interných zamestnancov. V terminológii CBA ide o nepriamy prínos meraný cenou ušetreného času používateľa, ktorý tvorí za určené obdobie 15 rokov sumu presahujúcu 72 mil. EUR. To súvisí najmä so skrátením priemernej dĺžky vybavenia služby na strane používateľa služby.

Predpoklady:

- Pre službu Zabezpečenie prístupu k službe alebo informáciám pre oprávneného interného používateľa - existujúca autentifikácia trvá 17 sekúnd, cez kartu sa skráti na 2 sekundy pre interných používateľov
- Pre službu Zabezpečenie prístupu k službe alebo informáciám pre oprávneného špecializovaného používateľa - externý používateľ - špecializovaný - autentifikácia/podanie dnes trvá 17 minút, elektronicky potrvá 2 minúty, priemerne sa dnes prihlasuje do 3 systémov, úspora je 2 autentifikácie do systémov
- Pre službu Zabezpečenie prístupu k službe alebo informáciám pre oprávneného nešpecializovaného používateľa - externý používateľ - nešpecializovaný - autentifikácia/podanie dnes trvá 17 minút, elektronicky potrvá 2 minúty
- Pre službu Poskytnutie integrovanej elektronickej služby - priemerná dĺžka podania 17 min, priemerne 3 podania, úspora 2 podania a elektronicky 3 min
- Poskytnutie integrovanej elektronickej služby - priemenná doba spracovania výstupu 5 min, úspora 2 výstupy

Ekonomické prínosy sú súčtom finančných prínosov a úspory času používateľa. Čistý finančný prínos a čistý ekonomický prínos je vyjadrený rozdielom finančných respektíve ekonomických prínosov a im prislúchajúcich nákladov bez vplyvu časového faktora.

Okrem uvedených finančne kvantifikovaných prínosov existujú ešte jedna kategória prínosov, ktorá nevchádza do modelu CBA. Ide o nepriame prínosy súvisiace so zvýšením bezpečnosti prístupu k systémom MS SR, chybovosti vkladáných údajov, zlepšením relevantnosti respektíve vo všeobecnosti zvýšením kvality poskytovaných služieb. CBA pri kvantifikácii prínosov uvažuje najmä so skrátením času vybavovania, či už na strane ministerstva alebo podnikateľa, občanov alebo interných zamestnancov.

6.9 Čistá súčasná hodnota

Čistá súčasná hodnota z projektu					
koeficient obdobia	Finančná (FNPV)	Ekonomická (ENPV)	Kumulovaná diskont. návratnosť ENPV		
0	-27 015 300,00	-27 015 300,00	-27 015 300,00	<	
1	-1 044 504,08	3 864 375,86	-23 150 924,14	<	
2	-933 644,62	3 719 322,15	-19 431 601,99	<	
3	-827 173,88	3 583 221,15	-15 848 380,84	<	
4	-724 731,95	3 455 737,28	-12 392 643,55	<	
5	-625 976,92	3 336 553,16	-9 056 090,40	<	
6	-530 583,90	3 225 368,77	-5 830 721,63	<	
7	-438 245,64	3 121 899,08	-2 708 822,55	<	
8	-348 665,86	3 025 878,89	317 056,35	Rok návratu investície	
9	-261 565,25	2 937 055,37	3 254 111,72	>	
10	-176 672,88	2 855 195,01	6 109 306,73	>	
11	-93 732,04	2 780 076,38	8 889 383,11	>	
12	-12 496,16	2 711 492,87	11 600 875,98	>	
13	67 272,89	2 649 253,01	14 250 128,99	>	
14	145 804,28	2 593 178,81	16 843 307,79	>	
SPOLU	-32 820 216,02	16 843 307,79			

Obsahom CBA analýzy je vyčíslenie budúcich nákladov a prínosov projektu, ktorého výsledkom je elektronizácia služieb MS SR podľa Prílohy č.2. Základným výstupom CBA je súhrnný ukazovateľ čistej súčasnej hodnoty (NPV – net present value) uvádzaný v EUR a návratnosť investície (PBP - Payback period) uvádzaná v rokoch.

Z hľadiska širších súvislostí elektronizácia prinesie významné ekonomické prínosy, spočívajúce predovšetkým v úspore času občanov a ministerstva. Po zohľadnení všetkých nákladov bude prínos projektu v uvažovanom časovom období 15 rokov vyjadrený ako čistá súčasná ekonomická hodnota dosahovať viac ako 16,843 mil. EUR. Z toho vyplýva, že projekt má ekonomické opodstatnenie v zmysle podmienok OPIS a investícia sa vráti v deviatom roku od začiatku projektu.

Príloha č.2 – Popis elektronických služieb

6.10 Zoznam eGov služieb

Z pohľadu e-Government môžeme plánované služby rozdeliť nasledovne:

P.č.	Názov eGov služby	Úroveň elektronizácie
1.	Zabezpečenie prístupu k službe alebo informáciám pre oprávneného interného používateľa	4
2.	Zabezpečenie prístupu k službe alebo informáciám pre oprávneného špecializovaného používateľa	4
3.	Zabezpečenie prístupu k službe alebo informáciám pre oprávneného nešpecializovaného používateľa	4
4.	Poskytnutie integrovanej elektronickej služby	4

6.10.1 Zabezpečenie prístupu k službe alebo informáciám pre oprávneného interného používateľa

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby eGov	Zabezpečenie prístupu k službe alebo informáciám pre oprávneného interného používateľa
Kód	
Popis	<p>eGovernment služba „Zabezpečenie prístupu k službe alebo informáciám pre oprávneného interného používateľa“ je určená na zabezpečenie prístupu k službám alebo informáciám uchovávaných v jednotlivých informačných systémov integrovaných v koncepte eJustice interným používateľom, t.j. pracovníkom jednotlivých orgánov v rezorte spravodlivosti.</p> <p>Autentifikácia interných používateľov je realizovaná prostredníctvom dedikovaného autentifikačného mechanizmu MS SR (t.j. nepredpokladá sa používanie eID kariet pre služobné účely). Na základe autentifikácie používateľa sú sprístupnené na základe jeho organizačného zaradenia jeho oprávnenia/role, na základe ktorých konkrétny informačný systém určí funkcie a rozsah informácií, ku ktorým má autentifikovaný interný používateľ oprávnenie</p>
Úroveň elektronizácie služby	4 ⁴

⁴ Predpokladá sa sprístupnenie informácií a služieb, ktoré sú výstupmi ďalších elektronických služieb

Základné údaje	
Názov atribútu	Popis a typ atribútu
Vyžadovaná úroveň autentifikácie	3
Notifikácia o priebehu konania	0
Vyžadovanie platby	Nie
Gestor	MS SR
Vstupné dokumenty (parametre)	Zadanie
Typ vstupu	Elektronicky
Výstupné dokumenty (parametre)	Poskytnutie požadovanej informácie alebo služby v súlade s požiadavkou
Typ výstupu	Elektronicky

Výkony	
Názov atribútu	Popis a typ atribútu
Parameter, dátum, hodnota, zdroj hodnoty	<p>Súčasná hodnota:</p> <ul style="list-style-type: none"> počet poskytnutí prístupu za rok : 1 350.000⁵ <p>Cieľová hodnota:</p> <ul style="list-style-type: none"> počet poskytnutí prístupu za rok : 450.000

Vzťahy	
Služby IS volané touto službou eGov (služba eGov závisí na týchto službách IS)	Poskytovanie informácií pre oprávnených používateľov z jednotlivých agendových systémov
Prístupové komponenty	Špecializovaný portál
Používateľ služby eGov	G2E.
Životná situácia	Legislatíva, súdy, väzenstvo
Agenda verejnej správy	A 0001641, A 0001642

6.10.2 Zabezpečenie prístupu k službe alebo informáciám pre oprávneného špecializovaného používateľa

⁵ Predpokladá sa pre 600 zamestnancov rezortu 3x denne autentifikácia do 3 rôznych systémov, po nasadení služby centrálnej autentifikácie bude potrebná iba jedna autentifikácia 3x denne

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby eGov	Zabezpečenie prístupu k službe alebo informáciám pre oprávneného špecializovaného interného používateľa
Kód	
Popis	<p>eGovernment služba „Zabezpečenie prístupu k službe alebo informáciám pre oprávneného špecializovaného používateľa“ je určená na zabezpečenie prístupu k špecializovaným (neverejným) službám alebo informáciám uchovávaných v jednotlivých informačných systémov integrovaných v koncepte eJustice pre špecializovaných používateľov, ktorými sú napr. notári, exekútori, advokáti, a pod. Pre týchto sú určené špecializované funkcie, ktoré nie sú voľne prístupné verejnosti.</p> <p>Autentifikácia interných používateľov je realizovaná prostredníctvom všeobecného autentifikačného prostriedku – eID karty. Na základe autentifikácie je pre systémy rezortu spravodlivosti poskytnutá identita špecializovaného používateľa a v prípade potreby aj organizácia, za ktorú používateľ koná. Pre špecializovaných používateľov služba určuje ich oprávnenia pre prístup k „neverejným“ službám agendových informačných systémov, t.j. k funkciám ktoré nie sú určené pre verejnosť.</p>
Úroveň elektronizácie služby	4 ⁶
Vyžadovaná úroveň autentifikácie	3
Notifikácia o priebehu konania	0
Vyžadovanie platby	Nie
Gestor	MS SR
Vstupné dokumenty (parametre)	Zadanie
Typ vstupu	Elektronicky
Výstupné dokumenty (parametre)	Poskytnutie požadovanej informácie alebo služby v súlade s požiadavkou
Typ výstupu	Elektronicky

⁶ Predpokladá sa sprístupnenie informácií a služieb, ktoré sú výstupmi ďalších elektronických služieb

Výkony	
Názov atribútu	Popis a typ atribútu
Parameter, dátum, hodnota, zdroj hodnoty	<p>Súčasná hodnota:</p> <ul style="list-style-type: none"> počet poskytnutí prístupu za rok : 2 000.000⁷ <p>Cieľová hodnota:</p> <ul style="list-style-type: none"> počet poskytnutí prístupu za rok : 2 000.000

Vzťahy	
Služby IS volané touto službou eGov (služba eGov závisí na týchto službách IS)	Poskytovanie informácií pre oprávnených používateľov z jednotlivých agendových systémov
Prístupové komponenty	Špecializovaný portál
Používateľ služby eGov	G2B resp. G2C (podľa typu špecializovaného používateľa).
Životná situácia	Legislatíva, súdy, väzenstvo
Agenda verejnej správy	A 0001641, A 0001642

6.10.3 Zabezpečenie prístupu k službe alebo informáciám pre oprávneného nešpecializovaného používateľa

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby eGov	Zabezpečenie prístupu k službe alebo informáciám pre oprávneného nešpecializovaného interného používateľa
Kód	
Popis	<p>eGovernment služba „Zabezpečenie prístupu k službe alebo informáciám pre oprávneného nešpecializovaného používateľa“ je určená na zabezpečenie prístupu k službám alebo informáciám uchovávaných v jednotlivých informačných systémov integrovaných v koncepte eJustice pre verejnosť.</p> <p>Autentifikácia interných používateľov je realizovaná prostredníctvom všeobecného autentifikačného prostriedku – eID karty. Na základe autentifikácie je pre systémy rezortu spravodlivosti poskytnutá identita nešpecializovaného používateľa a v prípade potreby aj organizácia, za ktorú používateľ koná,</p>
Úroveň elektronizácie služby	4 ⁸

⁷ Predpoklad 8.000 externých používateľov (advokáti, notári, exekútori), predpoklad minimálne 1 prístup denne, v súčasnosti realizovaný vo väčšine prípadov, v cieľovom riešení elektronický prístuplistinne

⁸ Predpokladá sa sprístupnenie informácií a služieb, ktoré sú výstupmi ďalších elektronických služieb

Základné údaje	
Názov atribútu	Popis a typ atribútu
Vyžadovaná úroveň autentifikácie	3
Notifikácia o priebehu konania	0
Vyžadovanie platby	Nie
Gestor	MS SR
Vstupné dokumenty (parametre)	Zadanie
Typ vstupu	Elektronicky
Výstupné dokumenty (parametre)	Poskytnutie požadovanej informácie alebo služby v súlade s požiadavkou
Typ výstupu	Elektronicky

Výkony	
Názov atribútu	Popis a typ atribútu
Parameter, dátum, hodnota, zdroj hodnoty	<p>Súčasná hodnota:</p> <ul style="list-style-type: none"> počet poskytnutí prístupu za rok : 100.000⁹ <p>Cieľová hodnota:</p> <ul style="list-style-type: none"> počet poskytnutí prístupu za rok : 100.000

Vzťahy	
Služby IS volané touto službou eGov (služba eGov závisí na týchto službách IS)	Poskytovanie informácií pre oprávnených používateľov z jednotlivých agendových systémov
Prístupové komponenty	Špecializovaný portál
Používateľ služby eGov	G2B resp. G2C (podľa typu používateľa).
Životná situácia	Legislatíva, súdy, väzenstvo
Agenda verejnej správy	A 0001641, A 0001642

6.10.4 Poskytnutie integrovanej elektronickej služby

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby eGov	Poskytnutie integrovanej elektronickej služby

⁹ Predpokladá sa ročne 100.000 prístupov verejnosti, ktoré sú v súčasnosti realizované listinne, v cieľovom riešení sa predpokladá realizácia elektronickým spôsobom

Základné údaje	
Názov atribútu	Popis a typ atribútu
Kód	
Popis	<p>eGovernment služba „Poskytnutie integrovanej elektronickej služby“ je určená na poskytovanie komplexných služieb, pri ktorých je potrebná integrácia služieb viacerých špecializovaných informačných systémov.</p> <p>Integrovaná elektronická služba je služba, ktorá nie je priamo poskytovaná agendovými systémami, ale je „vyskladaná“ zo služieb jednotlivých agendových systémov. Integrovaná služba v súlade s princípom životných situácií reaguje na požiadavku používateľa a snaží sa ju naplniť integráciou dielčích služieb, t.j. virtualizuje prostredie jednotlivých agend (agendových systémov) od pohľadu používateľa na jeho funkcie.</p> <p>Služba zabezpečuje vykonanie príslušného procesného toku a aktivácie funkcií a služieb jednotlivých informačných systémov tak, aby bola požiadavka používateľa komplexne spracovaná.</p>
Úroveň elektronizácie služby	4 ¹⁰
Vyžadovaná úroveň autentifikácie	3
Notifikácia o priebehu konania	Podľa špecifik implementovaného procesu spracovania
Vyžadovanie platby	Podľa špecifik implementovaného procesu spracovania
Gestor	MS SR
Vstupné dokumenty (parametre)	Parametre volanej integrovanej služby
Typ vstupu	Elektronicky
Výstupné dokumenty (parametre)	Poskytnutie výstupov integrovanej elektronickej služby
Typ výstupu	Elektronicky

Výkony	
Názov atribútu	Popis a typ atribútu
Parameter, dátum, hodnota, zdroj hodnoty	<p>Súčasná hodnota:</p> <ul style="list-style-type: none"> počet poskytnutí služby za rok : 100.000¹¹ <p>Cieľová hodnota:</p> <ul style="list-style-type: none"> počet poskytnutí služby za rok : 33.333

¹⁰ Predpokladá sa poskytovanie elektronického výstupu v rámci sprístupnenia integrovanej elektronickej služby

¹¹ V súčasnosti realizovaných cca 100.000 samostatných podaní, po zavedení integrovanej služby sa predpokladá realizácia elektronickým spôsobom a zníženie počtu samostatných podaní o 1/3 z dôvodu poskytovania integrovanej služby, ktorá rieši viacero samostatných podaní

Vzťahy	
Služby IS volané touto službou eGov (služba eGov závisí na týchto službách IS)	Sprístupnenie služieb a získavania informácií z jednotlivých agendových systémov
Prístupové komponenty	Špecializovaný portál
Používateľ služby eGov	G2C, G2B
Životná situácia	Legislatíva, súdy, väzenstvo
Agenda verejnej správy	A 0001641, A 0001642

6.11 Zoznam služieb informačného systému (IS)

Z pohľadu informačného systému môžeme plánované nové služby rozdeliť nasledovne:

P.č.	Názov služby IS	Typ služby
1.	Registrácia používateľa do systému centrálnej správy používateľov	Vstupná
2.	Zabezpečenie centrálnej správy používateľov pre agendové systémy	Vstupná
3.	Centrálna identifikácia a autorizácia používateľov pre agendové systémy	Vstupno/Výstupná
4.	Riadenie prístupov k informačným zdrojom a funkciám informačných systémov pre agendové systémy	Výstupná
5.	Monitorovanie a audit poskytovania správy používateľov a riadenia prístupu pre agendové	Výstupná
6.	Identifikácia a manažment služieb vystavených na integračnej platforme	Vstupná
7.	Manažment životného cyklu služieb vystavených na integračnej platforme	Vstupná
8.	Definovanie business procesu na integračnej platforme	Vstupná
9.	Realizácia business procesu na integračnej platforme	Výstupná
10.	Monitorovanie business procesov na integračnej platforme	Vstupná
11.	Vydanie autorizačných údajov pre používateľa	Vstupno/Výstupná
12.	Vykonanie autorizácie úkonu používateľom	Výstupná

6.11.1 Registrácia používateľa do systému centrálnej správy používateľov

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby	Registrácia používateľa do systému centrálnej správy používateľov
Verzia	1.0
Popis	Služba „Registrácia používateľa do systému centrálnej správy používateľov“ rieši prvotný zber identifikačných a autorizačných údajov o používateľoch. Služba ponúka centrálnu grafické rozhranie pre zadanie registračných údajov a riadi proces registrácie používateľa s účelom vytvorenia používateľského účtu v centrálnej správe používateľov. Tento proces môže byť automatický alebo plnoautomatický – vyžadujúci súčinnosť pracovníka Ministerstva spravodlivosti Slovenskej republiky.
Charakter služby	Vstupná
Informačný systém	IAM
Správca	Ministerstvo spravodlivosti SR
Prevádzkovateľ	Ministerstvo spravodlivosti SR

Vzťahy	
Používateľ služby IS	G2C G2B G2G G2E
Komunikačný kanál	webové sídlo, Intranet
Agenda verejnej správy	A 0001641, A 0001642, A0001644, A0003158, A0003185

6.11.2 Zabezpečenie centrálnej správy používateľov pre agendové systémy

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby	Zabezpečenie centrálnej správy používateľov pre agendové systémy
Verzia	1.0
Popis	Služba „Zabezpečenie centrálnej správy používateľov pre agendové systémy“ je určená pre zber a manažment identifikačných, autentifikačných a autorizačných údajov používateľov jednotlivých agendových systémov.

Základné údaje	
Názov atribútu	Popis a typ atribútu
	<p>Služba podporuje správu používateľov ako pre verejnú zónu (externí používatelia) tak aj pre privátnu zónu (interní používatelia).</p> <p>Služba zbiera informácie nasledujúcich typov používateľov:</p> <ul style="list-style-type: none"> • fyzická osoba (napr. občan) • úradníka (napr. probačný a mediačný úradník, prokurátor/sudca, atď.) • systém (napr. interný agendový systém alebo externý systém). <p>Zber a manažment informácií o používateľoch sa týka nasledujúcich okruhov informácií:</p> <ul style="list-style-type: none"> • identita používateľa • autentifikačné údaje používateľa • prístupové práva používateľa <p>Autorizačné údaje minimálne obsahujú nasledujúce dátové objekty:</p> <ul style="list-style-type: none"> • Používateľ, Používateľský účet, Skupina, Rola, Oprávnenie • Organizácia, Organizačná zložka, Osoba • Osoby subjektov, Splnomocnenia <p>Služba ponúka rozhranie (grafické rozhranie pre administrátora a Webové servery pre informačné systémy) na zadanie a zmenu hore uvedených údajov.</p> <p>Služba vystavuje grafické rozhranie pre koncového používateľa s účelom prihlásenie, odhlásenia a nahlásenia zmeny osobných údajov.</p>
Charakter služby	Vstupná
Informačný systém	IAM
Správca	Ministerstvo spravodlivosti SR
Prevádzkovateľ	Ministerstvo spravodlivosti SR

Vzťahy	
Používateľ služby IS	G2C G2B G2G G2E
Komunikačný kanál	webové sídlo, Intranet
Agenda verejnej správy	A 0001641, A 0001642, A0001644, A0003158, A0003185

6.11.3 Centrálna identifikácia a autorizácia používateľov pre agendové systémy

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby	Centrálna identifikácia a autorizácia používateľov pre agendové systémy
Verzia	1.0
Popis	<p>Služba „Centrálna identifikácia a autorizácia používateľov pre agendové systémy“ poskytuje identifikačné a autorizačné mechanizmy pre jednotlivé agendové systémy tak, aby ich používatelia mohli prihlásiť (t.j. identifikovať a autentifikovať) jednotným spôsobom v rámci jednotlivých agendových systémov. Systémy používajúce túto službu budú môcť spĺňať požiadavku na single sign-on (jednotné prihlasovanie používateľov raz a do všetkých systémov).</p> <p>Služba podporuje minimálne nasledujúce autentifikačné mechanizmy:</p> <ul style="list-style-type: none"> • Meno/Heslo • X.500 directory services (napr. Microsoft Active Directory) • X.509 certifikáty (resp. PKI infraštruktúra) • Prihlásenie cez ÚPVS <p>Služba zabezpečí aj dodržanie kvality podporovaných autentifikačných mechanizmov - napr. pri Meno/Heslo aké sú minimálne požiadavky na kvalitu hesla a obnovu hesla; pri PKI či sú akceptované self-signed certifikáty alebo na prihlásenie môže byť použitý aj kvalifikovaný certifikát, ktorý primárne je určený účely elektronického podpisu. Parametre kvality autentifikačných mechanizmov sú konfigurovateľné.</p> <p>Autorizačné údaje sú poskytované z centrálnej správy používateľov s nasledujúcimi spôsobmi:</p> <ul style="list-style-type: none"> • na požiadanie (poskytnutie známych autentifikačných údajov alebo len informácie či používateľ disponuje s určitým autentifikačným údajom) • pomocou notifikácie zmien
Charakter služby	Vstupno/výstupná
Informačný systém	IAM
Správca	Ministerstvo spravodlivosti SR
Prevádzkovateľ	Ministerstvo spravodlivosti SR

Vzťahy	
Používateľ služby IS	G2C G2B G2G G2E
Komunikačný kanál	webové sídlo, Intranet
Agenda verejnej správy	A 0001641, A 0001642, A0001644, A0003158, A0003185

6.11.4 Riadenie prístupov k informačným zdrojom a funkciám informačných systémov pre agendové systémy

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby	Riadenie prístupov k informačným zdrojom a funkciám informačných systémov pre agendové systémy
Verzia	1.0
Popis	<p>Služba „Riadenie prístupov k informačným zdrojom a funkciám informačných systémov pre agendové systémy“ poskytuje potrebné autorizačné údaje používateľa pre jednotlivé agendové systémy tak, aby mohli efektívne rozhodovať o prístupe k svojim informačným zdrojom a funkciám.</p> <p>Autorizačné údaje sú poskytované z centrálnej správy používateľov s nasledujúcimi spôsobmi:</p> <ul style="list-style-type: none"> • na požiadanie (poskytnutie známych autentifikačných údajov alebo len informácie či používateľ disponuje s určitým autentifikačným údajom) • pomocou notifikácie zmien
Charakter služby	Výstupná
Informačný systém	IAM
Správca	Ministerstvo spravodlivosti SR
Prevádzkovateľ	Ministerstvo spravodlivosti SR

Vzťahy	
Používateľ služby IS	G2C G2B G2G
Komunikačný kanál	webové sídlo, Intranet
Agenda verejnej správy	A 0001641, A 0001642, A0001644, A0003158, A0003185

6.11.5 Monitorovanie a audit poskytovania správy používateľov a riadenia prístupu pre agendové systémy

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby	Monitorovanie a audit poskytovania správy používateľov a riadenia prístupu pre agendové
Verzia	1.0
Popis	<p>Služba „Monitorovanie a audit poskytovania správy používateľov a riadenia prístupu pre agendové systémy“ umožňuje centrálnu analýzu auditných informácií týkajúce:</p> <ul style="list-style-type: none"> • Identifikácie a autorizácie používateľov • Poskytnutých autorizačných údajov • Zmien v správe používateľov <p>Služba ďalej umožňuje vyhľadávanie podozrivých aktivít naznačujúcich pokusy o narušenie integrity a obmedzení prístupu.</p>
Charakter služby	Výstupná
Informačný systém	IAM
Správca	Ministerstvo spravodlivosti SR
Prevádzkovateľ	Ministerstvo spravodlivosti SR

Vzťahy	
Používateľ služby IS	G2G
Komunikačný kanál	webové sídlo, Intranet
Agenda verejnej správy	A 0001641, A 0001642, A0001644, A0003158, A0003185

6.11.6 Identifikácia a manažment služieb vystavených na integračnej platforme

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby	Identifikácia a manažment služieb vystavených na integračnej platforme
Verzia	1.0
Popis	<p>Služba „Identifikácia a manažment služieb vystavených na integračnej platforme“ rieši identifikáciu služieb, ktoré by mali byť vystavené na integračnej platforme pre použitie jednotlivými agendovými systémami alebo externými systémami. Hlavným artefaktom je katalóg služieb, ktorý spravuje minimálne nasledujúce informácie o jednotlivých službách:</p> <ul style="list-style-type: none"> • business opis služby

Základné údaje	
Názov atribútu	Popis a typ atribútu
	<ul style="list-style-type: none"> • technický opis služby • poskytovateľ služby • konzumenti služby
Charakter služby	Vstupná
Informačný systém	Integračná platforma
Správca	Ministerstvo spravodlivosti SR
Prevádzkovateľ	Ministerstvo spravodlivosti SR

Vzťahy	
Používateľ služby IS	G2G
Komunikačný kanál	webové sídlo, Intranet
Agenda verejnej správy	A 0001641, A 0001642, A0001644, A0003158, A0003185

6.11.7 Manažment životného cyklu služieb vystavených na integračnej platforme

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby	Manažment životného cyklu služieb vystavených na integračnej platforme
Verzia	1.0
Popis	<p>Služba „Manažment životného cyklu služieb vystavených na integračnej platforme“ rieši celý životný cyklus vystavenej služby na integračnej platforme a to hlavne:</p> <ul style="list-style-type: none"> • zaevidovanie služby • nastavenie technických parametrov služby - konfigurácia komunikačných kanálov, zabezpečenie služby, atď. • aktualizácia služby (aj s verzovaním) • ukončenie poskytovania služby <p>Vystavené služby sú buď pre Interné systémy a moduly alebo pre externé systémy. Poskytovateľom služieb môžu byť buď agendové systémy (interné systémy) alebo externé systémy, ktoré poskytujú služby potrebné pre interné systémy.</p> <p>Služby na integračnej platforme môžu byť zložitejšie – vyskladané z existujúcich služieb.</p>

Základné údaje	
Názov atribútu	Popis a typ atribútu
Charakter služby	Vstupná
Informačný systém	Integračná platforma
Správca	Ministerstvo spravodlivosti SR
Prevádzkovateľ	Ministerstvo spravodlivosti SR

Vzťahy	
Používateľ služby IS	G2G
Komunikačný kanál	webové sídlo, Intranet
Agenda verejnej správy	A 0001641, A 0001642, A0001644, A0003158, A0003185

6.11.8 Definovanie business procesu na integračnej platforme

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby	Definovanie business procesu na integračnej platforme
Verzia	1.0
Popis	<p>Služba „Definovanie business procesu na integračnej platforme“ rieši tvorbu business procesov z existujúcich služieb.</p> <p>Vytvorené business procesy sú vystavené na integračnej platforme ako služby.</p> <p>V prípade potreby parametre business procesu môže byť konfigurovateľné bez potreby zásahu programátora pomocou konfigurovateľných pravidiel (Rules).</p> <p>Vytvorené business procesy umožnia zaznamenávať dôležité udalosti obchodného alebo technického rázu.</p>
Charakter služby	Vstupná
Informačný systém	Integračná platforma
Správca	Ministerstvo spravodlivosti SR
Prevádzkovateľ	Ministerstvo spravodlivosti SR

Vzťahy

Používateľ služby IS	G2G
Komunikačný kanál	webové sídlo, Intranet
Agenda verejnej správy	A 0001641, A 0001642, A0001644, A0003158, A0003185

6.11.9 Realizácia business procesu na integračnej platforme

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby	Realizácia business procesu na integračnej platforme
Verzia	1.0
Popis	Služba „Realizácia business procesov na integračnej platforme“ riadi vykonávanie business procesov. Business procesy môžu byť synchrónneho alebo asynchrónneho rázu. Asynchrónne procesy sú často dlho trvajúce. V tomto prípade riadenie procesov rieši aj hybernáciu príslušného procesu a následné zobudenie procesu pri výskyte očakávanej udalosti. Pri vykonávaní business procesov sú zaznamenávané dôležité udalosti obchodného alebo technického rázu.
Charakter služby	Výstupná
Informačný systém	Integračná platforma
Správca	Ministerstvo spravodlivosti SR
Prevádzkovateľ	Ministerstvo spravodlivosti SR

Vzťahy	
Používateľ služby IS	G2C G2B G2G
Komunikačný kanál	webové sídlo, Intranet
Agenda verejnej správy	A 0001641, A 0001642, A0001644, A0003158, A0003185

6.11.10 Monitorovanie business procesov na integračnej platforme

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby	Monitorovanie business procesov na integračnej platforme
Verzia	1.0
Popis	<p>Služba „Monitorovanie business procesov na integračnej platforme“ sleduje a vyhodnocuje vykonávanie business procesov. Služba ďalej poskytuje výstupy vo forme reportov vykonávaní business procesov ako:</p> <ul style="list-style-type: none"> • Úspešne vykonané business procesy • Neúspešne vykonané business procesy • Procesy čakajúce na určitú udalosť • a iné. <p>V prípade vyskytnutia technickej chyby v procese alebo nesplnení business parametrov služba notifikuje obsluhu.</p>
Charakter služby	Vstupná
Informačný systém	Integračná platforma
Správca	Ministerstvo spravodlivosti SR
Prevádzkovateľ	Ministerstvo spravodlivosti SR

Vzťahy	
Používateľ služby IS	G2G
Komunikačný kanál	webové sídlo, Intranet
Agenda verejnej správy	A 0001641, A 0001642, A0001644, A0003158, A0003185

6.11.11 Vydanie autorizačných údajov pre používateľa

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby	Vydanie autorizačných údajov pre používateľa
Verzia	1.0
Popis	<p>Služba „Vydanie autorizačných údajov pre používateľa“ zabezpečí zber identifikačných údajov a oprávnení, ktoré sú potrebné pre vydanie kvalifikovaného certifikátu používateľa, v ktorom je definované jeho oprávnenie na vykonávanie úkonov v rámci plnenia pracovných úloh.</p> <p>Prostredníctvom kvalifikovaného certifikátu s uvedenými oprávneniami môže používateľ autorizovať vykonávané úkony prostredníctvom</p>

Základné údaje	
Názov atribútu	Popis a typ atribútu
	zaručeného elektronického podpisu, čím bude zabezpečená integrita a nepopierateľnosť týchto úkonov pri ich následnom hodnotení.
Charakter služby	Vstupno/výstupná
Informačný systém	PKI infraštruktúra
Správca	Ministerstvo spravodlivosti SR
Prevádzkovateľ	Ministerstvo spravodlivosti SR

Vzťahy	
Používateľ služby IS	G2C G2B G2G
Komunikačný kanál	webové sídlo, Intranet
Agenda verejnej správy	A 0001641, A 0001642, A0001644, A0003158, A0003185

6.11.12 Vykonanie autorizácie úkonu používateľom

Základné údaje	
Názov atribútu	Popis a typ atribútu
Názov služby	Vykonanie autorizácie úkonu používateľom
Verzia	1.0
Popis	Služba „Vykonanie autorizácie úkonu používateľom“ zabezpečí vytvorenie zaručeného elektronického podpisu, ktorým používateľ autorizuje úkon realizovaný v konkrétnom agendovom informačnom systéme.
Charakter služby	Výstupná
Informačný systém	PKI infraštruktúra
Správca	Ministerstvo spravodlivosti SR
Prevádzkovateľ	Ministerstvo spravodlivosti SR

Vzťahy	
Používateľ služby IS	G2C G2B G2G

Komunikačný kanál	webové sídlo, Intranet
Agenda verejnej správy	A 0001641, A 0001642, A0001644, A0003158, A0003185

Príloha č. 3 - Analýza rizík

V tejto časti je uvedená analýza projektových rizík. Tieto sú členené na samostatné skupiny rizík, ktoré sú následne rozpracované samostatne:

- Riziká spojené v celospoločenskom prostredí,
- Riziká spojené s projektom a jeho cieľmi,
- Riziká spojené so spôsobom realizácie projektu,
- Iné riziká.

Popis rizík obsahuje vlastný názov rizika, ako aj nasledujúce atribúty:

- Pravdepodobnosť rizika – pravdepodobnosť udalosti, ktorá spôsobí vznik rizikového faktoru,
- Dopady rizika – dôsledky výskytu rizika na projekt a dosahovanie jeho cieľov,
- Miera rizika pre projekt – miera významu rizika (kombinácia pravdepodobnosti výskytu a jeho dopadov na projekt) určujúca prioritu rozsah opatrení, ktoré na elimináciu rizika je potrebné prijímať.

Popis rizík na viac obsahuje návrh opatrení, ktoré je potrebné v rámci projektu vykonať na zamedzenie rizika a jeho dopadov na projekt.

6.11.13 Riziká spojené s celospoločenským prostredím

Riziká spojené s celospoločenským prostredím zahŕňujú riziká, ktoré existujú mimo vlastného projektu a na ktoré MS SR nemá priamy dosah. Riziká v tejto oblasti sú podrobnejšie popísané v nasledujúcej tabuľke.

Riziko	Pravdep.	Dopady	Miera Riz.
Časové obmedzenia na realizáciu projektu	vysoká	vysoká	Vysoká
<i>Vzhľadom na financovanie projektu z programu OPIS je potrebné ukončenie všetkých aktivít projektu a aj formálne ukončenie realizácie do konca roku 2015. V praxi to znamená požiadavku na ukončenie realizácie projektu v horizonte 7/8 2015. Akýkoľvek posun vo formálnych krokoch vedúci k naštartovaniu riešenia môže mať následok nestihnúť termínu na ukončenie a tým ohrozenie využitia finančných prostriedkov z programu OPIS. V takom prípade by riešenie projektu muselo byť financované z rozpočtovej kapitoly MS SR v rámci rozpočtových prostriedkov.</i>			

6.11.14 Riziká spojené s projektom a jeho cieľmi

Riziká spojené s projektom a jeho cieľmi zahŕňujú riziká mimo vlastného projektu a dosahovania jeho cieľov. Tieto riziká MS SR dokáže ovplyvniť. Riziká v tejto oblasti sú podrobnejšie popísané v nasledujúcej tabuľke.

- Vývoj duplicitnej funkcionality v rámci systémov
- Nezvládnutie technológií vývojármi aplikácií
- Nezvládnutie technológií prevádzkovateľmi

Riziko	Pravdep.	Dopady	Miera Riz.
Nenaplnenie očakávaných prínosov projektu – nedostatočné využívanie funkcionality v iných systémoch	nízka	vysoké	stredná
<p><i>Aplikačná architektúra a bezpečnostná infraštruktúra je budovaná najmä z dôvodu ich centralizácie a sprístupnenia funkcií pre ďalšie systémy nasadzované v rámci konceptu eJustice. V prípade že ostatné systémy nebudú v očakávanej miere integrované na poskytované funkcie, nemožno ciele projektu považovať za naplnené. Preto je potrebné pri návrhu a implementácii ďalších systémov trvať na ich integrácii s cieľmi tohto projektu.</i></p> <p><i>Je potrebné zohľadniť stav rozpracovania niektorých projektov, ktoré sú v štádiu realizácie a s použitím výstupov tohto projektu nepočítajú.</i></p>			
Nezvládnutie poskytovaných technológií vývojármi aplikácií	nízka	stredné	stredná
<p><i>Využitie aplikačnej architektúry a bezpečnostnej infraštruktúry vyžaduje od vývojárov ďalších informačných systémov. V prípade nezvládnutia potrebných technológií nemusí využitie výsledkov priniesť očakávaný efekt.</i></p>			
Nezvládnutie poskytovaných technológií prevádzkovým personálom	nízka	stredné	stredná
<p><i>Nasadené prostriedky poskytujú veľké možnosti v oblasti podpory prevádzky. Ak však tento personál nedokáže využiť všetky funkcionality týchto prostriedkov, nebude možné dosiahnuť očakávané prínosy.</i></p>			

6.11.15 Riziká spojené so spôsobom realizácie projektu

Riziká spojené so spôsobom realizácie projektu zahrňujú riziká, ktoré priamo spojené so spôsobom riešenia projektu. MS SR ich môže ovplyvniť spôsobom riadenia projektu. Riziká v tejto oblasti sú podrobnejšie popísané v nasledujúcej tabuľke.

Riziko	Pravdep.	Dopady	Miera Riz.
Nedostatočnosť súčinnosti pri riešení zo strany zadávateľa	stredná	významná	vysoká
<p><i>eGovernment projekt je významný transformačný projekt, ktorý bude mať vplyv na spôsob výkonu správ v celom rezorte. Je prirodzené očakávať rezistenciu zamestnancov rezortu. Z toho dôvodu je potrebné zaviesť program riadenia zmien (change management). Postupné nasadzovanie (roll-out) respektíve pilotovanie vybudovaných zmien a ich komunikácia dovnútra rezortu výrazne prispieje k akceptácii zmien.</i></p>			

6.11.16 Iné riziká

Riziká v tejto časti zahŕňujú iné riziká, na ktoré má MS SR čiastočný dosah. Riziká v tejto oblasti sú podrobnejšie popísané v nasledujúcej tabuľke.

Riziko	Pravdep.	Dopady	Miera Riz.
Nepokrytie potrebných prevádzkových nákladov v rozpočte MS SR	Stredná	vysoké	vysoké
<i>Nedostatok prostriedkov na prevádzku systému bude ohrozovať trvalú udržateľnosť vybudovaného riešenia. Nedodržanie podmienok udržateľnosti OPIS by viedlo k vráteniu poskytnutého NFP. Prevádzkové náklady je potrebné projektovať do prípravy rozpočtov MSSR v nasledujúcich obdobiach.</i>			
Nedostatok finančných prostriedkov pre neprojektové aktivity	Stredná	vysoké	stredná
<i>V rámci riešenia projektu a dosahovania jeho cieľov je potrebné vykonať zásahy v okolitých systémoch tak aby boli začlenené do aplikačnej architektúry a bezpečnostnej infraštruktúry. Tieto odchýlky je potrebné analyzovať a dostatočne vopred zabezpečiť finančné prostriedky potrebné pre úpravu týchto systémov.</i>			

Príloha č. 4 - Kalkulácie celkových nákladov na vlastníctvo softvéru (TCO)

1. Náklady na zakúpenie SW Licencie**													
číslo riadku	názov skupiny	popis položky	Počet ks licencií	jednot ková cena v EUR bez DPH	CEL KOM cena licencií v EUR bez DPH	CEL KOM DPH v %	CELKOM cena licencií v EUR s DPH	1. rok	2. rok	3. rok	4. rok	5.rok	Spolu za 5 rokov
1.1	Nutný SW - aplikačný												
1	Integračná platforma	Softvér a licencie pre Integračné platformy	1	480 000,00	480 000,00	20%	576 000,00	0,00	0,00	0,00	0,00	0,00	0,00
2	Správa používateľov (IAM)	Softvér a licencie pre Aplikačnú podporu	1	907 965,00	907 965,00	20%	1 089 558,00	0,00	0,00	0,00	0,00	0,00	0,00
3	Správa používateľov (IAM)	Softvér a licencie pre Aplikačnú podporu - mobilné zariadenia	2 600	260,00	676 000,00	20%	811 200,00	0,00	0,00	0,00	0,00	0,00	0,00
4	PKI	PKI SW infraštruktúra	1	270 000,00	270 000,00	20%	324 000,00	0,00	0,00	0,00	0,00	0,00	0,00
5	Bezpečnosť	Licencia pre Aplikačný firewall a load balancing	1	220 000,00	220 000,00	20%	264 000,00	0,00	0,00	0,00	0,00	0,00	0,00
6	Bezpečnosť	Licencia nástroja pre logovanie a analýzu logov	1	435 000,00	435 000,00	20%	522 000,00	0,00	0,00	0,00	0,00	0,00	0,00
7	Bezpečnosť	Licencia systému ochrany proti sieťovej infiltrácii	1	60 000,00	60 000,00	20%	72 000,00	0,00	0,00	0,00	0,00	0,00	0,00

Čiastková štúdia uskutočniteľnosti projektov prioritnej osi 1 Elektronizácia verejnej správy a rozvoj elektronických služieb OPIS Projekt budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR

8	Bezpečnosť	Licencia systému ochrany proti aplikačnej infiltrácii	1	1 250 000,00	1 250 000,00	20%	1 500 000,00	0,00	0,00	0,00	0,00	0,00	0,00
9	Bezpečnosť	Licencia pre biometrickú autentifikáciu	1	235 000,00	235 000,00	20%	282 000,00	0,00	0,00	0,00	0,00	0,00	0,00
10	Bezpečnosť	Softvér a licencie pre inteligentný editor	1 300	600,00	780 000,00	20%	936 000,00	0,00	0,00	0,00	0,00	0,00	0,00
11	Bezpečnosť	Softvér a licencie pre Komunikačné systémy a zabezpečenie	1 300	631,00	820 300,00	20%	984 360,00	0,00	0,00	0,00	0,00	0,00	0,00
12	Podpora prevádzky	Softvér a licencie pre Databázy	68	46 915,00	3 190 220,00	20%	3 828 264,00	0,00	0,00	0,00	0,00	0,00	0,00
13	Podpora prevádzky	Licencia pre Monitoring a Event management (network)	1	57 000,00	57 000,00	20%	68 400,00	0,00	0,00	0,00	0,00	0,00	0,00
14	Podpora prevádzky	Licencia pre Monitoring a Event management (systémy a aplikácie)	1	850 355,00	850 355,00	20%	1 020 426,00	0,00	0,00	0,00	0,00	0,00	0,00
15	Podpora prevádzky	Licencie pre Sledovanie a analýzu výkonnosti aplikácií	1	240 000,00	240 000,00	20%	288 000,00	0,00	0,00	0,00	0,00	0,00	0,00
16	Podpora prevádzky	Licencia pre Správu licencií a využitia	1	75 000,00	75 000,00	20%	90 000,00	0,00	0,00	0,00	0,00	0,00	0,00
17	Podpora prevádzky	Licencia pre podporu používateľov a procesy riešenia incidentov	1	60 000,00	60 000,00	20%	72 000,00	0,00	0,00	0,00	0,00	0,00	0,00
1.2 Nutný SW - systémový													
1.	Softvér	Softvér a licencie pre operačný systém Microsoft Windows Server Datacenter edition	12	4 000,00	48 000,00	20%	57 600,00	0,00	0,00	0,00	0,00	0,00	0,00
2.	Softvér	Licencie pre operačný systém RedHat Linux Enterprise Standard	2	800,00	1 600,00	20%	1 920,00	0,00	0,00	0,00	0,00	0,00	0,00

Čiastková štúdia uskutočniteľnosti projektov prioritnej osi 1 Elektronizácia verejnej správy a rozvoj elektronických služieb OPIS Projekt budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR

3	Softvér	Softvér a licencie pre Databázy (licencia na procesor - skóre 10000)	4	38 000,00	152 000,00	20%	182 400,00	0,00	0,00	0,00	0,00	0,00	0,00
4	Softvér	Softvér a licencie pre operačný systém Microsoft Windows Server Standard edition	2	720,00	1 440,00	20%	1 728,00	0,00	0,00	0,00	0,00	0,00	0,00

Licencie Celkom							12 971 856,00	0 €	0 €	0 €	0 €	0 €	0 €
------------------------	--	--	--	--	--	--	----------------------	------------	------------	------------	------------	------------	------------

2. Náklady na inštaláciu SW													
číslo riadku	názov skupiny	popis položky	počet hodín /ks		CEL KOM cena v EUR bez DPH	CEL KOM DPH v %	CELKOM cena v EUR s DPH	1. rok	2. rok	3. rok	4. rok	5.rok	Spolu za 5 rokov
1		Analýza a návrh riešenia	1,00		1 430 000,00	20%	1 716 000,00	171 600,00	171 600,00	171 600,00	171 600,00	171 600,00	858 000,00
2		Implementácia	1,00		1 823 800,00	20%	2 188 560,00	218 856,00	218 856,00	218 856,00	218 856,00	218 856,00	1 094 280,00
3		Testovanie	1,00		532 950,00	20%	639 540,00	63 954,00	63 954,00	63 954,00	63 954,00	63 954,00	319 770,00
4		Nasadenie riešenia	1,00		1 246 300,00	20%	1 495 560,00	149 556,00	149 556,00	149 556,00	149 556,00	149 556,00	747 780,00

Náklady na inštaláciu SW Celkom	6 039 660 €	603 966 €	603 966 €	603 966 €	603 966 €	603 966 €	3 019 830 €
--	--------------------	------------------	------------------	------------------	------------------	------------------	--------------------

3. Náklady na podporu a údržbu softvéru (ročný poplatok výrobcovi softvéru)													
číslo riadku	názov skupiny	popis položky	počet		CEL KOM cena licen cií v EUR bez DPH	CEL KOM DPH v %	CELKOM cena licencií v EUR s DPH	1. rok	2. rok	3. rok	4. rok	5.rok	Spolu za 5 rokov
3.1	Nutný SW - aplikačný												
1	Integrač ná platfor ma		1,00		72 000,0 0	20%	0,00		86 400,00	86 400,00	86 400,00	86 400,00	259 200,00
2	IAM		1,00		90 796,50	20%	0,00		108 955,80	108 955,80	108 955,80	108 955,80	326 867,40
3	PKI		1,00		6 000,0 0	20%	0,00		7 200,00	7 200,00	7 200,00	7 200,00	21 600,00
4	Aplikačn ý firewall		1,00		187 500,0 0	20%	0,00		225 000,00	225 000,00	225 000,00	225 000,00	675 000,00
5	Manage ment podpory prevádzk y		1,00		35 250,0 0	20%	0,00		42 300,00	42 300,00	42 300,00	42 300,00	126 900,00
6	Security informat ion and event manage ment (SIEM)		1,00		0,00	20%	0,00		0,00	0,00	0,00	0,00	0,00

Čiastková štúdiá uskutočniteľnosti projektov prioritnej osi 1 Elektronizácia verejnej správy a rozvoj elektronických služieb OPIS Projekt budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR

7	Intrusion prevention systems (IPS)		1,00		0,00	20%	0,00		0,00	0,00	0,00	0,00	0,00
8	Ochrana proti infiltrácii		1,00		0,00	20%	0,00		0,00	0,00	0,00	0,00	0,00
3.2	Nutný SW - systémový												
9	Softvér a operačný systém Microsoft Windows Server Datacenter Edition		12,00		10560,00	20%	0,00		152064,00	152064,00	152064,00	152064,00	456192,00
10	Licencie pre operačný systém RedHat		2,00		352,00	20%	0,00		844,80	844,80	844,80	844,80	2 534,40
11	Softvér a licencie pre Databázy (licencia na procesor - skóre 10000)		4,00		33440,00	20%	0,00		160512,00	160512,00	160512,00	160512,00	481536,00

Náklady na podporu a údržbu softvéru (ročný poplatok výrobcovi softvéru) Celkom	0 €	0 €	783 277 €	783 277 €	783 277 €	783 277 €	2 349 830 €
--	------------	------------	----------------------	----------------------	----------------------	----------------------	------------------------

4. Náklady na (nevyhnutný) upgrade softvéru													
číslo riadku	názov skupiny	popis položky	počet		CEL KOM cena licen cií v EUR bez DPH	CEL KOM DPH v %	CELKOM cena licencií v EUR s DPH	1. rok	2. rok	3. rok	4. rok	5.rok	Spolu za 5 rokov
4.1	Nutný SW - aplikačný												
4.2	Nutný SW - systémový												

Náklady na (nevyhnutný) upgrade softvéru Celkom	0 €	0 €	0 €	0 €	0 €	0 €
--	------------	------------	------------	------------	------------	------------

5. Náklady na školenia													
číslo riadku	názov skupiny	popis položky	jednot ková cena v EUR bez DPH		CEL KOM cena licen cií v EUR bez DPH	CEL KOM DPH v %	CELKOM cena licencií v EUR s DPH	1. rok	2. rok	3. rok	4. rok	5.rok	Spolu za 5 rokov
1.	Všeobec né podmien ky	Školenie administrátora	0,00	1,00	0,00	20%	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Čiastková štúdia uskutočniteľnosti projektov prioritnej osi 1 Elektronizácia verejnej správy a rozvoj elektronických služieb OPIS Projekt budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR

2.	Všeobecné podmienky	Školenie užívateľské	0,00	1,00	0,00	20%	0,00	0,00	0,00	0,00	0,00	0,00	0,00
3.	Podporný servis	Zaškolenie technických pracovníkov	0,00	1,00	0,00	20%	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Náklady na školenia Celkom	0 €	0 €	0 €	0 €	0 €	0 €	0 €
-----------------------------------	------------	------------	------------	------------	------------	------------	------------

6. Náklady na záruky spojené s prevádzkou softvéru													
číslo riadku	názov skupiny	popis položky	počet		CEL KOM cena licen cií v EUR bez DPH	CEL KOM DPH v %	CELKOM cena licencií v EUR s DPH	1. rok	2. rok	3. rok	4. rok	5.rok	Spolu za 5 rokov

Náklady na záruky spojené s prevádzkou softvéru Celkom	0 €	0 €	0 €	0 €	0 €	0 €
---	------------	------------	------------	------------	------------	------------

TCO Celkom	19 011 516 €	603 966 €	1 387 243 €	1 387 243 €	1 387 243 €	1 387 243 €	5 369 660 €
-------------------	---------------------	------------------	--------------------	--------------------	--------------------	--------------------	--------------------

Príloha č. 5 - Kalkulácie nákladov na vlastníctvo hardvéru (TCO)

1. Náklady na zakúpenie HW*													
číslo riadku	názov skupiny	popis položky	merná jednotka ks alebo človekohodina	jednotková cena technických zariadení v EUR bez DPH	CELKOM cena technických zariadení v EUR bez DPH	CELKOM DPH v %	CELKOM cena technických zariadení v EUR s DPH	1. rok	2. rok	3. rok	4. rok	5.rok	Spolu za 5 rokov
1.1	Nutný HW - servery (OS) - názov												
1.	Integračná platforma	Server pre IP - 2 CPU, 48GB RAM, 1TB SAS 10k HDD, 2x1 Gbit/s	3	21 000,00	63 000,00	20%	75 600,00	0,00	6 048,00	0,00	6 048,00	0,00	12 096,00
2.	Správa používateľov (IAM)	Server pre IAM - 2 CPU, 48GB RAM, 1TB SAS 10k HDD, 2x1 Gbit/s	3	21 000,00	63 000,00	20%	75 600,00	0,00	6 048,00	0,00	6 048,00	0,00	12 096,00
3.	PKI	Počítač operátora RA	80	800,00	64 000,00	20%	76 800,00	0,00	3 840,00	0,00	3 840,00	0,00	7 680,00
4.	PKI	Monitor LCD Operátora RA	80	500,00	40 000,00	20%	48 000,00	0,00	2 400,00	0,00	2 400,00	0,00	4 800,00
5.	PKI	Multifunkčná tlačiareň	80	1 700,00	136 000,00	20%	163 200,00	0,00	8 160,00	0,00	8 160,00	0,00	16 320,00

Čiastková štúdia uskutočniteľnosti projektov prioritnej osi 1 Elektronizácia verejnej správy a rozvoj elektronických služieb OPIS Projekt budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR

		operátora RA											
6.	PKI	Čítačka čipových kariet	6080	32,00	194 560,00	20%	233 472,00	0,00	11 673,60	0,00	11 673,60	0,00	23 347,20
7.	PKI	Čipová karta	6160	23,00	141 680,00	20%	170 016,00	0,00	8 500,80	0,00	8 500,80	0,00	17 001,60
8.	Bezpečnosť	Počítač sudcu a vyššieho súdneho úradníka	2500	900,00	2 250 000,00	20%	2 700 000,00	0,00	135 000,00	0,00	135 000,00	0,00	270 000,00
9.	Bezpečnosť	Tlačiareň súdu	43	10 250,00	440 750,00	20%	528 900,00	0,00	26 445,00	0,00	26 445,00	0,00	52 890,00
10.	Bezpečnosť	Tablet sudcu	1300	450,00	585 000,00	20%	702 000,00	0,00	35 100,00	0,00	35 100,00	0,00	70 200,00
11.	Bezpečnosť	Prenosný počítač sudcu	1300	840,00	1 092 000,00	20%	1 310 400,00	0,00	65 520,00	0,00	65 520,00	0,00	131 040,00
12.	Bezpečnosť	Server pre aplikačný firewall a load balancing	2	115 000,00	230 000,00	20%	276 000,00	0,00	13 800,00	0,00	13 800,00	0,00	27 600,00
13.	Bezpečnosť	Server pre Logovanie a analýzu logov (SIEM) - 2 CPU, 128GB RAM, 14TB HDD	2	20 000,00	40 000,00	20%	48 000,00	0,00	2 400,00	0,00	2 400,00	0,00	4 800,00
14.	Bezpečnosť	Server pre Logovanie a analýzu logov (SIEM) - 2 CPU, 48GB RAM, 1TB SAS 10k	1	21 000,00	21 000,00	20%	25 200,00	0,00	2 016,00	0,00	2 016,00	0,00	4 032,00

Čiastková štúdia uskutočniteľnosti projektov prioritnej osi 1 Elektronizácia verejnej správy a rozvoj elektronických služieb OPIS Projekt budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR

		HDD, 2x1 Gbit/s											
15.	Bezpečnosť	Server pre systém ochrany proti sieťovej infiltrácii	1	250 000,00	250 000,00	20%	300 000,00	0,00	15 000,00	0,00	15 000,00	0,00	30 000,00
16.	Bezpečnosť	L2/L3 Switch pre systém ochrany proti sieťovej infiltrácii	2	20 010,00	40 020,00		40 020,00	0,00	2 001,00	0,00	2 001,00	0,00	4 002,00
17.	Bezpečnosť	Server pre systém ochrany proti aplikačnej infiltrácii 2 CPU, 48GB RAM, 1TB SAS 10k HDD, 2x1 Gbit/s	2	21 000,00	42 000,00	20%	50 400,00	0,00	4 032,00	0,00	4 032,00	0,00	8 064,00
18.	Bezpečnosť	Samostatný sieťový firewall	2	75 000,00	150 000,00	20%	180 000,00	0,00	14 400,00	0,00	14 400,00	0,00	28 800,00
19.	Bezpečnosť	Prístupový prepínač pre DC	4	80 000,00	320 000,00	20%	384 000,00	0,00	30 720,00	0,00	30 720,00	0,00	61 440,00
20.	Bezpečnosť	Server pre biometrickú autentifikáciu	1	230 000,00	230 000,00	20%	276 000,00	0,00	22 080,00	0,00	22 080,00	0,00	44 160,00
21.	Bezpečnosť	Server pre Logovanie a monitorin	3	21 000,00	63 000,00	20%	75 600,00	0,00	0,00	0,00	0,00	0,00	0,00

Čiastková štúdia uskutočniteľnosti projektov prioritnej osi 1 Elektronizácia verejnej správy a rozvoj elektronických služieb OPIS Projekt budovania aplikačnej architektúry a bezpečnostnej infraštruktúry rezortu Ministerstva spravodlivosti SR

		g - 2 CPU, 48GB RAM, 1TB SAS 10k HDD, 2x1 Gbit/s											
22.	Bezpečnosť	HSM modul umiestniť eľný do štandardn ého PCIe rozhrania s 2000 transakcia mi za sekundu	2	30 000,00	60 000,00	20%	72 000,00	0,0 0	0,00	0,00	0,00	0,00	0,00
1.2 Nutný HW - ostatné zariadenia													
1.	Podpora prevádzk y	Rozšíreni e úložnej kapacity - 36TB 7k2 HDD, 3TB SAS 10k HDD, 8 FC ports	1	140 000,00	140 000,00	20%	168 000,00	0,0 0	18 000,00	18 000,00	18 000,00	18 000,00	18 000,00
2.					0,00	20%	0,00	0,0 0	0,00	0,00	0,00	0,00	0,00
2. Náklady na súvisiace stavebné práce a iné práce***													
2.1 Iné práce													
1.		Inštalácia serverov	1	20 480,00	20 480,00	20%	24 576,00	0,0 0	1 966,08	0,00	1 966,08	0,00	3 932,16
2.			0		0,00	20%	0,00	0,0 0	0,00	0,00	0,00	0,00	0,00
HW Celkom							8 003 784,00 €	0 €	435 150 €	18 000 €	435 150 €	18 000 €	852 301 €

