

Věcná část

zadávací dokumentace veřejné zakázky

„Implementátor AIS EO, AIS EOP a AIS ECD“

Obsah

1	Seznam zkratk	4
2	Předmět plnění veřejné zakázky:	5
2.1	Popis plnění:	6
2.1.1	Analýza a návrh AIS3 zahrnuje zpracování:.....	6
2.1.2	Dodávka, instalace a zprovoznění technické infrastruktury zahrnuje:.....	7
2.1.3	Vývoj a implementace AIS3 a školení zahrnuje:.....	7
2.1.4	Ověření AIS3 pilotním provozem s vybranou skupinou úřadů zahrnuje:.....	7
2.1.5	Předání AIS3 do rutinního provozu.....	7
2.1.6	Podpora provozu AIS3.....	8
3	Požadavky zadavatele na systém AIS EO, AIS EOP a AIS ECD	8
3.1	Legislativní rámec	8
3.1.1	Obecně.....	8
3.1.2	AIS EO.....	9
3.1.3	AIS EOP.....	9
3.1.4	AIS CD.....	9
3.2	Koncept řešení	9
3.3	Funkcionalita	11
3.3.1	Základní funkcionalita.....	11
3.3.2	Sledování dotazů - datový audit.....	11
3.3.3	Správa uživatelských oprávnění.....	11
3.4	Vazby s okolními systémy prostřednictvím ISZR a vazby na „výrobní“ systémy ePas a eOP 13	
3.5	Převod dat	24
3.5.1	Požadavky na převod dat ze stávajících systémů do AIS3.....	24
3.5.2	Bezpečnostní omezení.....	25
3.6	Technologické požadavky	25
3.6.1	Základní požadavky.....	25
3.6.2	Bezpečnostní požadavky.....	26
3.7	Provozní a kapacitní parametry systému	27
3.8	Postup předávání systému do provozu	28
3.8.1	Atestace způsobilosti k realizaci vazeb ISVS s jinými IS.....	28
3.8.2	Bezpečnostní audit.....	28
3.8.3	Testování systému.....	28
3.8.4	Požadavky na školení obsluhy.....	28
3.8.5	Požadavky na dokumentaci systému.....	29
	Součástí dodávky bude kompletní dokumentace AIS3, vyhotovenou v listinné (1 paré) a elektronické podobě (na datovém nosiči v editovatelné formě), obsahující kompletní popis AIS3, tj. především:.....	29
3.9	Požadavky na provoz	29
3.9.1	Dostupnost.....	30
3.9.2	Bezpečnost.....	30
3.9.3	Monitoring pro pracovníky Zadavatele.....	31
3.9.4	Obnova systému.....	31
3.9.5	Helpdesk pro koncového uživatele.....	32
3.9.6	Požadavky na servis zařízení a servis aplikace.....	32

3.9.7	Správa incidentů, problémů	32
3.9.8	Životní cyklus systému	33
4	<i>Harmonogram:</i>	33
4.1	Hlavní milníky projektu.....	33
5	<i>Charakteristika realizace</i>	34
5.1	I. Etapa – návrh AIS3	34
5.2	II. Etapa – implementace AIS3.....	35
Seznam obrázků		
Obrázek 1	Konceptuální schéma	10
Obrázek 2	Začlenění jednotlivých skupin editorů a externích systémů do celkové architektury AIS3 a ISZR	23
Obrázek 3	Orientační schéma migrace	25
Seznam Tabulek		
Tabulka 1	– Seznam zkratk	4

1 Seznam zkratek

Tabulka 1 – Seznam zkratek

Zkratka	Popis
AIS	Agendový informační systém
AIS EO	Agendový informační systém evidence obyvatel
AIS EOP	Agendový informační systém evidence občanských průkazů
AIS ECD	Agendový informační systém evidence cestovních dokladů
AIS3	Souhrnné označení pro AIS EO, AIS EOP, AIS ECD a podpůrné systémy
CBA	Analýza nákladů a přínosů (Cost-Benefit Analysis)
CDBP	Cestovní doklady s biometrickými prvky
CDBP-eOP	výrobní systém eOP
CEPP	Centrální evidence přístupových práv (stávající subsystem)
CIS	Cizinecký informační systém
CMS	Centrální místo služeb
CS	Centrální systém
CRŘ	Informační systém Centrální registr řidičů
CRV	Informační systém Centrální registr silničních vozidel
CVS	Centrální výpočetní středisko
eID	Systém ePasy, eOP a ePKP
eOP	Elektronický občanský průkaz
HW	Hardware
IOP	Integrovaný operační program
ISDS	Informační systém datových schránek
ISVS	Informační systémy veřejné správy
ISZR	Informační systém základních registrů
JIP OVM	Jednotný identitní prostor orgánů veřejné moci
KIVS	Komunikační infrastruktura veřejné správy
MV	Ministerstvo vnitra
MZV	Ministerstvo zahraničních věcí
ORG	Převodník identifikátorů základních registrů
PČR	Policie ČR
ROB	Registr obyvatel
ROS	Registr osob
RPP	Registr práv a povinností
RUIAN	Registr územní identifikace, adres a nemovitostí

SD	Modul evidence dotazů
SW	Software
ZR	Základní registry
ZVS	Záložní výpočetní středisko

2 Předmět plnění veřejné zakázky:

Předmětem Zakázky je služba „Implementátor AIS EO, AIS EOP a AIS ECD“ (dále jen „Plnění“), včetně změnového řízení.

Plnění se sestává z :

Realizace tří agendových informačních systémů vymezených příslušnými zákony:

- evidence obyvatel zahrnující i registr rodných čísel (dále jen „AIS EO“),
- evidence občanských průkazů (dále jen „AIS EOP“), včetně napojení na výrobní systém eOP (CDBP-eOP),
- evidence cestovních dokladů (dále jen „AIS ECD“), včetně napojení na výrobní systém CD (CDBP),

a zavedení centrálního dohledového a monitorovacího systému, centrální evidence dotazů a sledování změn dat, napojení na jednotný identitní prostor veřejné správy, napojení na IZSR a ROB, RUIAN, ROS, RPP, ORG a zřízení informačního serveru pro publikování informací o provozu AIS3, dokumentace, návodů apod.

(dále jen „AIS3“).

Realizace AIS3 představuje:

1. analýzu a návrh AIS3 včetně napojení na ISZR, ROB, RUIAN, ROS, RPP, ORG a na jednotný identitní prostor veřejné správy,
2. dodávku, instalaci a zprovoznění potřebné technologické infrastruktury (dále jen „Infrastruktura“) a její začlenění do stávající HW a síťové infrastruktury MV,
3. vývoj a implementace AIS3, školení vybraných uživatelů a obsluhy,
4. ověření dodaných AIS3 pilotním provozem s editory systému (s 3 vybranými krajskými úřady, 3 vybranými obcemi s rozšířenou působností, 3 vybranými matričními úřady, zvláštní matrikou Brno, 3 vybranými ohlašovnými trvalého pobytu, 3 vybranými soudy a bezpečnostními útvary), spolupráce s ISZR a jednotlivými základními registry, ověření spolupráce s 3 vybranými externími informačními systémy.
5. převedení provozu ze stávajících informačních systémů správních evidencí na dodané řešení včetně převedení dat ze stávajících systémů do AIS3,
6. předání AIS3 do rutinního provozu,

7. zajištění podpory rutinního provozu AIS3 po celou dobu záruční doby podle podmínek definovaných v příloze č. 1.4.

Zadavatel připouští implementaci AIS3 na fyzicky shodné, ale logicky oddělené technické infrastrukturu (izolace na úrovni virtuálních serverů a samostatných instancí AIS EO, AIS EOP a AIS ECD), všechny aplikace musí běžet a všechna data musí být uložena na technice vyhrazené pro AIS3, není přípustné jakékoliv ukládání dat do cloudu mimo AIS3.

Zadavatel požaduje po uchazeči, aby plnil roli systémového integrátora celé dodávky Plnění a byl zodpovědný za koordinaci všech dílčích plnění a subdodávek pro stránce smluvní, projektové i věcné.

Vítězný uchazeč je povinen při implementaci řešení AIS3 postupovat v součinnosti s hlavním architektem eGovernment, Architektem ROB a s vítězným uchazečem veřejné zakázky č. 60026098: „ROB“ (implementace informačního systému) a architektky ostatních základních registrů a architektem a řešitelem jednotného identitního prostoru veřejné správy.

2.1 Popis plnění:

2.1.1 Analýza a návrh AIS3 zahrnuje zpracování:

- analýzy současného stavu a požadavků Zadavatele s důrazem na rozdílovou analýzu mezi stavem uvedeným v ZD a aktuálními požadavky,
- globálního a detailního návrhu architektury AIS3 včetně návrhu technické infrastruktury a způsobu integrace do technologického prostředí Zadavatele se zahrnutím budoucích vazeb na ISZR,
- podrobného harmonogramu na celou oblast Plnění včetně vyznačení kontrolních bodů (např. bodů rozhodnutí), podrobný harmonogram musí akceptovat milníky stanovené v tomto zadání,
- analýzy rizik, seznam rizik a návrhu opatření k jejich eliminaci,
- detailních návrhů systémů (dále jen „DNS“), návrhu datových modelů, návrhu technické infrastruktury včetně specifikace požadavků na vytvoření stavebně provozních podmínek (umístění, datové sítě, elektroinstalace, příkon, chlazení apod.), návrhu postupu a způsobu implementace celé dodávky. Zadavatel požaduje návrh technické infrastruktury s ohledem na zajištění odpovídající dostupnosti a zajištění obnovy systémů po havárii (kapitola č. 3) Požadavky zadavatele na systém AIS EO, AIS EOP a AIS ECD),
- návrhu funkcionalit umožňujících obousměrně komunikovat AIS3 se základními registry příslušnou službou eGON, navázání na služby eGON definované v dokumentaci k informačním systémům základních registrů vztažených k AIS3 včetně vytvoření notifikačního systému AIS3,
- návrhu způsobu a postupu migrace dat ze stávajících informačních systémů správních evidencí včetně návrhu kontroly dat, který bude vycházet ze stávajícího datového modelu,
- bezpečnostního projektu a návrhu bezpečnostních opatření.

2.1.2 **Dodávka, instalace a zprovoznění technické infrastruktury zahrnuje:**

- dodávku HW a systémového SW, součástí dodávky musí být produkční prostředí pro systémy AIS3, prostředí testovací a prostředí školící pro koncové uživatele. Zadavatel požaduje návrh celého prostředí s ohledem na zajištění dostupnosti 0.999 a zajištění obnovy po havárii („disaster recovery“), tj. vytvoření dvou samostatných kompletů (jeden pro CVS a jeden pro ZVS). Pro CVS se vyžaduje zdvojení provozně kritických technologických prvků (servery, síťové aktivní prvky, zdvojené napájení všech serverů a aktivních prvků) a použití diskových polí se 100% vnitřní redundancí. Pro ZVS se vyžaduje zdvojení všech síťových prvků a použití serverů se zdvojeným napájením a použití polí se 100% vnitřní redundancí.
- instalaci technické infrastruktury,
- integraci technické infrastruktury do prostředí MV.

2.1.3 **Vývoj a implementace AIS3 a školení zahrnuje:**

- vývoj, dodávku a implementaci aplikačního programového vybavení pro AIS3 podle bodu 2.1.1,
- vytvoření a zprovoznění AIS3,
- vytvoření dokumentace v souladu se zákonem č. 365/2000 Sb., a s požadavky Zadavatele,
- školení administrátorů, technické obsluhy, hotline a školitelů uživatelů,
- součinnost při čištění a kontrole dat,
- vývoj a dodávku nástrojů pro migraci dat ze stávajících informačních systémů správních evidencí do AIS3,
- součinnost při migraci dat ze stávajících informačních systémů správních evidencí do AIS3,
- dodání testovacích scénářů na AIS3,
- testování AIS3 podle schválených testovacích scénářů.

2.1.4 **Ověření AIS3 pilotním provozem s vybranou skupinou úřadů zahrnuje:**

- specifikaci požadavků na vybavení pilotních míst a zaškolení vybrané skupiny uživatelů,
- zpracování metodiky pro pilotní provoz na vybraných pracovištích (odpovídání dotazů, reporting chyb, atd.),
- realizaci pilotního provozu AIS3 a jeho podporu,
- vyhodnocení pilotního provozu AIS3 a promítnutí schválených změn do implementovaného řešení.

2.1.5 **Předání AIS3 do rutinního provozu**

Podmínkou pro převzetí a konečnou akceptaci AIS3 je, aby:

- byly akceptovány všechny samostatné části AIS3,

- byla převedena data ze stávajících informačních systémů správních evidencí do AIS3,
- byly AIS3 plně funkční pro všechny typy uživatelů,
- AIS3 plně spolupracoval s informačním systémem základních registrů (ISZR) a jednotlivými základními registry,
- byly plně funkční vazby na okolní systémy,
- byl akceptován návrh na zajištění provozu.

Převzetím AIS3 do rutinního provozu, který bude potvrzen protokolem, začíná běžet záruční doba pro samotné řešení AIS3 a platí dojednané záruční podmínky. Záruční lhůta pro hardware je řešena na základě záručních podmínek u dodané techniky.

2.1.6 Podpora provozu AIS3

Podpora provozu ze strany dodavatele zahrnuje především následující činnosti: zpracování návrhu na zajištění provozu, servis zařízení a aplikace, vedení požadavků na změny systému a poskytnutí součinnosti při obnově dat po havárii.

2.1.6.1 Zpracování návrhu na zajištění provozu

- Návrh na zajištění provozu obsahuje:
 - Plán vytváření záloh
 - Plán obnovy systému po havárii
 - Systém řízení bezpečnosti
 - Definici a řízení podpory
 - Návrh nastavení monitoringu
 - Definici a řízení životního cyklu systému

2.1.6.2 Podpora provozu

Okamžikem spuštění AIS3 do rutinního provozu, který bude potvrzen protokolem, začíná běžet rutinní podpora ze strany dodavatele podle specifikace v příloze č. 1.4 a to po celou dobu záruky.

3 Požadavky zadavatele na systém AIS EO, AIS EOP a AIS ECD

3.1 Legislativní rámec

3.1.1 Obecně

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů

Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů

Zákon č. 227/2009 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o základních registrech, ve znění pozdějších předpisů

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů

Zákon č. 13/1993 Sb., Celní zákon, ve znění pozdějších předpisů

Zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů

Zákon č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů

Zákon č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů

Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů

Nařízení vlády ČR č. 522/2005, kterým se stanoví seznam utajovaných informací

3.1.2 AIS EO

Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech ve znění pozdějších předpisů

Zákon č. 342/2006 Sb., kterým se mění některé zákony související s evidencí obyvatel a některé další zákony

Zákon č. 325/1999 Sb., o azylu ve znění pozdějších předpisů

Zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky ve znění pozdějších předpisů

Zákon č. 301/2000 Sb., o matrikách, jménu a příjmení ve znění pozdějších předpisů

3.1.3 AIS EOP

Zákon č. 328/1999 Sb., o občanských průkazech ve znění pozdějších předpisů

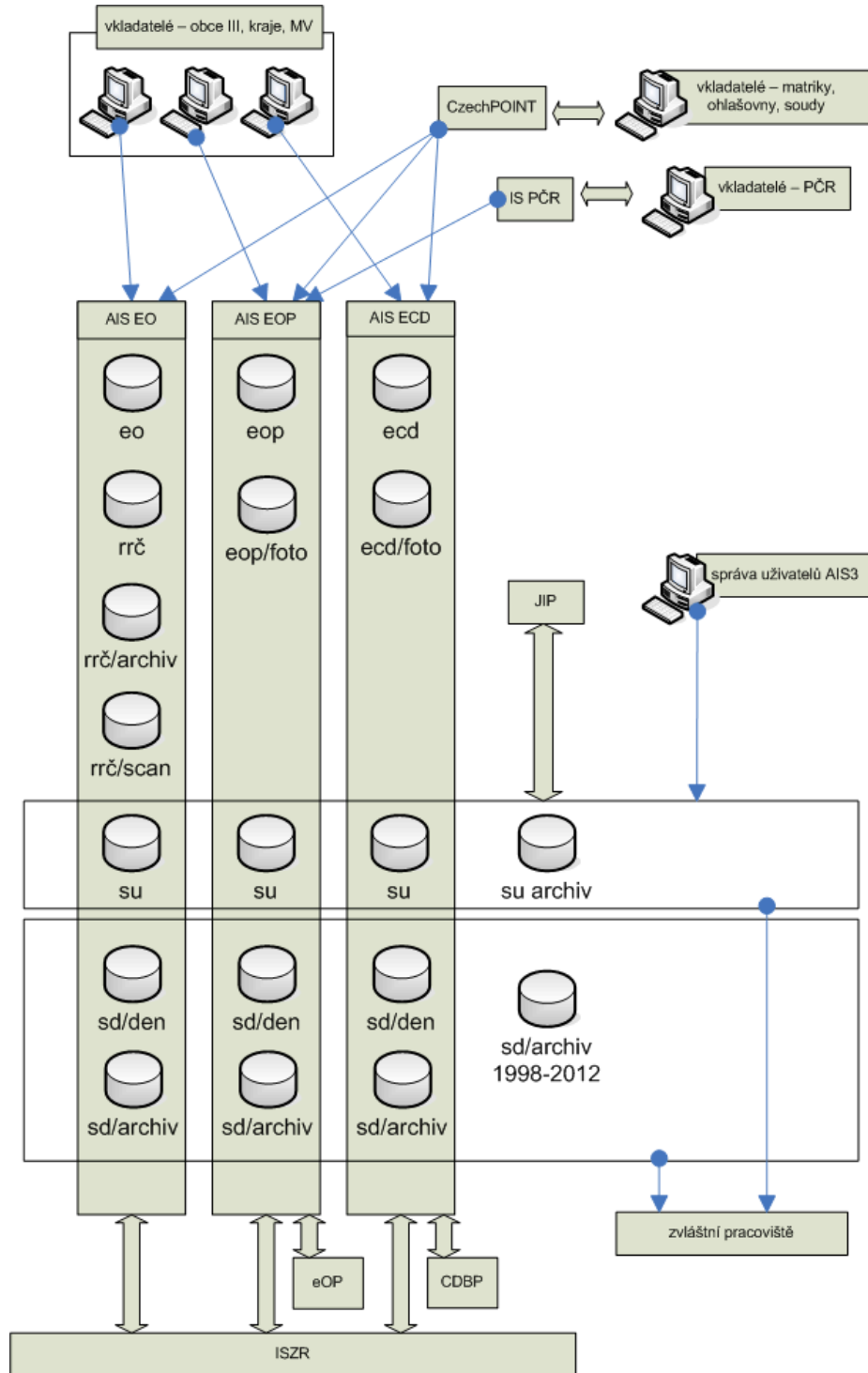
3.1.4 AIS CD

Zákon č. 329/1999 Sb., o cestovních dokladech, ve znění pozdějších předpisů

3.2 Koncept řešení

Základní konceptuální schéma agendových informačních systémů AIS3 je znázorněno na obrázku č.1. V tomto obrázku není znázorněna předpokládaná možnost využívat fotografie vzájemně mezi AIS EOP a AIS ECD od 1. 1. 2013.

V návrhu architektury AIS3 musí být zohledněna skutečnost, že jak datová základna AIS EOP, tak i datová základna AIS ECD musí být odděleny od datové základny AIS EO.



Obrázek č. 1 Konceptuální schéma

3.3 Funkcionalita

3.3.1 Základní funkcionality

Požadavky na funkcionality AIS3 jsou uvedeny Přílohách č. 1.2.1. až 1.2.4., soubory „ZD_AISEO_Priloha_1_2_*.pdf“. Obecně platí, že v řešení AIS3 je nutno zachovat veškerou stávající funkcionality pro výkon státní správy a samosprávy.

3.3.2 Sledování dotazů - datový audit

Součástí řešení musí být vytvoření společné evidence dotazů (dále jen „SD“) pro všechny aplikace AIS3. V rámci této evidence budou evidovány nově vznesené dotazy, zároveň do této evidence budou migrovány dotazy ze současných evidencí.

V případě potřeby musí být společná evidence dotazů pro AIS3 rozdělitelná do samostatných evidencí dotazů pro každou aplikaci AIS EO, AIS EOP a AIS ECD samostatně včetně přenesení dat o dotazech vztahujících se k příslušné aplikaci.

Každý dotaz do AIS a na něj navazující výdej dat (včetně výdejů pro aktualizace) musí být zaznamenán v SD. Musí být zaznamenány i dotazy, ke kterým nebyl nalezen žádný odpovídající záznam. V SD musí být zaznamenán i výdej údajů, vydávaných hromadnými výdeji.

Záznam musí obsahovat:

- popis dotazu v rozsahu minimálně:
 - o identifikace uživatele (login nebo interní id)
 - o datum a čas s přesností na vteřiny
 - o všechny údaje použité pro sestavení dotazu (položky v dotazu)
 - o identifikaci databáze (databází) použitých pro vyřízení dotazu
 - o důvod dotazu (vždy povinná položka u každého dotazu)
 - o prostředek (aplikace) použitý pro dotaz
- popis vydaných dat v rozsahu minimálně:
 - o identifikace druhu vydávaných dat (údaje k osobě, OP, CD, ...)
 - o identifikace konkrétního vydávaného subjektu (id osoby, OP, CD, ...)
 - o seznam vydaných údajů (bitová mapa apod.)

Zadavatel požaduje, aby uchazeč přihlédl k stávajícímu modelu SD. Vybranému uchazeči bude k dispozici datový model stávajícího SD. Podrobná specifikace bude Zadavatelem upřesněna ve fázi podrobné analýzy AIS3.

3.3.3 Správa uživatelských oprávnění

V souvislosti s budováním ISZR a základních registrů se předpokládá zavedení jednotné centrální správy uživatelů pro všechny orgány veřejné moci. Tento záměr bude realizován zavedením systému „Jednotný identitní prostor orgánů veřejné moci“ (JIP OVM).

V tomto materiálu jsou tedy vzhledem k uvedenému stavu uvedeny pouze základní požadavky na řešení správy uživatelů pro AIS3 s tím, že podrobnosti bude nutné projednat a rozhodnout v době analýzy AIS3 a řešení navrhnout v DNS AIS3 s přihlédnutím ke stavu, který bude platit po zprovoznění ISZR a JIP OVM.

V obecné rovině platí, že každý uživatel (fyzická osoba), který bude pracovat s AIS3 musí být plně identifikován, autentizován a musí být přesně známa jeho autorizace (nejen z hlediska oprávnění provádět jednotlivé operace, ale i z hlediska teritoriálního oprávnění). Žádná

z aplikací AIS3 nesmí používat login uživatele (jeho hodnotu nebo strukturu) k rozhodnutí o rozsahu oprávnění. Dále z hlediska požadavků vyplývajících ze zákonů a současné praxe není postačující znát při vyřizování jakéhokoliv požadavku pouze login pracovníka, musí být známo i jeho jméno, příjmení a instituce, kde je zaměstnán. Tyto údaje musí být uchovány po celou dobu, po kterou je v databázi AIS3 zapsána osoba, s kterou daný uživatel pracoval.

Z hlediska AIS3 přichází v úvahu použití správ uživatelů v následující hierarchii:

- a) interní správa uživatelů AIS3 (správa uživatelů jako součást řešení AIS3), samostatná pro každý jednotlivý AIS,
- b) JIP OVM,
- c) externí správa uživatelů používaná externí aplikací.

Pro uživatele v roli „editor“ (včetně pracovníků MV nebo PČR v této roli) musí být identifikace, autentizace a autorizace zajištěna buď interně v rámci AIS3 (vlastní správa uživatelů) nebo s využitím JIP OVM. V případě, že by v JIP OVM nebyly trvale uchovávány všechny identifikační údaje o uživateli, musí být přepsány do interní správy uživatelů.

Pro uživatele v roli „tazatel“, který zasílá dotaz prostřednictvím externí aplikace, která byla autentizována v ISZR je možné převzít identifikaci uživatele od této externí aplikace. Vždy je však požadováno převzetí minimálně následujících údajů: login uživatele, jméno a příjmení uživatele, v které instituci (případně v které organizační jednotce) je zaměstnán, lokalita, kde je zaměstnán (obec). Všechny identifikační údaje musí být v tomto případě uloženy v interní správě uživatelů spolu s označením aplikace a organizace, která údaje předala.

Pro identifikaci a autentizaci pracovníků provozu AIS3 (správa uživatelů, hotline) může být použita buď interní správa uživatelů AIS3 nebo JIP OVM, pro identifikaci a autentizaci administrátorů a operátorů AIS3 pak systémové prostředky nebo interní správa uživatelů AIS3.

V případě, že pro správu uživatelů v roli „editor“ bude použita interní správa uživatelů AIS3, musí být o každém takovém uživateli vedeny minimálně následující údaje:

- základní identifikační údaje tak, aby byl jednoznačně dohledatelný (jméno, příjmení, instituce, organizační jednotka, přidělený login),
- kontaktní údaje (telefon, email),
- role a teritorium (oprávnění k provádění jednotlivých operací v příslušném AIS, na jakém teritoriu může dané operace provádět),
- autentizační údaje,
- elektronická podoba schvalovacího dokumentu, kterým bylo schválilo zařazení uživatele do příslušné role,
- identifikační a kontaktní údaje osoby, která schválila zařazení uživatele do příslušné role.

Obdobný rozsah údajů pak musí být veden o pracovnících provozu AIS3.

V případě změny musí být původní hodnoty archivovány s uvedením platnosti od - do.

Pro zjednodušení práce pracovníků správy uživatelů je požadováno vytvořit nad správami uživatelů jednotlivých AIS společné uživatelské rozhraní.

3.4 Vazby s okolními systémy prostřednictvím ISZR a vazby na „výrobní“ systémy ePas a eOP

Funkcionality AIS3 musí zajistit náhradu stávajících rozhraní, tiskových výstupů a hromadných výdejů. Podrobnosti budou upřesněny v rámci analýzy a návrhu AIS3 podle reálného stavu řešení ISZR a ZR.

Pro výdeje dat, tiskové výstupy nebo hromadné výdeje dat, které nebude možno zajistit prostřednictvím ISZR a budou nadále vyžadovány, musí být v rámci analýzy navržen alternativní způsob řešení.

Přehled stávajících tiskových výstupů a hromadných výdejů bude upřesněn při analýze.

Orientační seznam stávajících základních rozhraní a výdejů dat je uveden Příloze č. 1.3 soubor „ZD_AISEO_Priloha_1_3_Rozhrani.xls“. V následujících části je uveden popis nejvýznamnějších rozhraní k jednotlivým AIS.

Uchazeč musí zajistit realizaci všech stávajících výdejů (základní i změnové) a programových rozhraní nebo navrhnout a vyřešit alternativní způsob zpracování nebo poskytování dat tak, aby nedošlo k omezení funkčnosti navazujících systémů externích subjektů, obcí atd..

Pro potřebu dalšího popisu jsou rozlišeny tři skupiny editorů AIS3:

- 1. skupina: editoři na obcích s rozšířenou působností, krajích, MV. Připojení těchto editorů je realizováno prostřednictvím sítí MV přímo k AIS3. Předpokládá se použití „tenkého klienta“ na straně editora (web prohlížeč). V této části popisu není dále rozváděno.
- 2. skupina: editoři na ohlašovnicích, matrikách, soudech. Připojení těchto editorů je zprostředkováno IS CzechPOINT. Editoři používají k dotazování a editování údajů v AIS formuláře IS CzechPOINT. Propojení IS EO/EOP/ECD je zajišťováno programovým rozhraním na bázi web services.
- 3. skupina: editoři Policie ČR. Připojení této skupiny editorů není v současném systému (v době vzniku tohoto dokumentu) realizováno. Zadavatel předpokládá, že připojení těchto editorů bude zprostředkovávat IS PČR. Propojení s AIS3 bude realizováno prostřednictvím web services, zajištěna musí být plná autentizace koncového uživatele (editora).

Návrh začlenění jednotlivých skupin editorů a externích systémů do celkové architektury AIS3 a ISZR je znázorněn na obrázku č. 2.

3.4.1 AIS EO

Rozhraní na základní registry

Komunikace AIS EO ze základními registry se realizuje příslušnou službou eGON, definovanou v dokumentaci k informačním systémům základních registrů vztažených k AIS3. Prostřednictvím tohoto rozhraní provádí AIS EO:

- aktualizaci údajů osob v ROB pro občany České republiky (zakládání nových osob, modifikace údajů vedených v ROB o osobách, výmaz osob z ROB, prvotní aktualizace dat v ROB),
- získávání údajů o právnických osobách z ROS (prvotní inicializace dat v EO z ROS pro vedené právnícké osoby, využití notifikačních služeb),
- získávání údajů o aktuálních adresách z RUIAN (prvotní inicializace dat v EO z RUIAN pro vedené platné adresy, využití notifikačních služeb).

Rozsah dat, která se zasílají/modifikují do/v ROB je dán výčtem vedených položek v ROB podle zákona.

ISZR pomocí rozhraní zasílá na AIS EO žádosti o reklamace údajů osob vedených v ROB a požadavky jiných AIS na data z EO, která nejsou vedena v ROB.

AIS EO připravuje notifikace změn k údajům vedených v AIS EO.

Rozhraní technologií Web Services. Zabezpečení, způsob a obsah komunikace specifikují projekty základních registrů.

Univerzální dotazovací rozhraní pro externí subjekty

Pro orgány veřejné moci (OVM) s právem získávání údajů z evidence obyvatel a registru rodných čísel (dále „externí subjekty“) je ve stávajícím IS EO vytvořeno programové rozhraní, které umožňuje externímu subjektu získávat údaje v rozsahu zákonného oprávnění tohoto subjektu (vydávají se pouze údaje, explicitně uvedené v příslušném zákoně). Rozhraní poskytuje přístup pomocí web services nebo pomocí XML dotazu a odpovědi, použit je přenosový protokol https. Provádí se basic autentizace volající aplikace. Nad tímto programovým rozhraním je dále vytvořen tzv. web klient, který umožňuje přístup uživatelů externího subjektu přímo z www prohlížeče (v tomto případě se provádí plná autentizace uživatele).

Zadavatel požaduje nahradit toto rozhraní obdobnou funkčností, zajišťovanou prostřednictvím eGON funkcí, které bude externí subjekt volat prostřednictvím ISZR. Přitom se předpokládá, že ISZR „rozloží“ dotaz externího subjektu na čtení údajů z ROB a čtení údajů z AIS EO a odpovědi obou systémů „složí“ do jedné odpovědi. Rozsah vydávaných údajů musí odpovídat oprávnění v příslušném zákonu (úplný přehled připojených externích subjektů a aplikovaných zákonů bude k dispozici v době analýzy AIS3).

Přímé dotazování uživatelů externích subjektů z www prohlížeče do AIS EO se v době vzniku tohoto dokumentu nepředpokládá, má být nahrazeno přístupem prostřednictvím portálu veřejné správy. Součástí řešení musí tedy být spolupráce s portálem veřejné správy nebo návrh jiného řešení, které externím uživatelům z institucí bez vlastního informačního systému umožní získávání údajů z AIS EO.

Rozhraní pro IS Policie ČR

Pro IS Policie ČR je v současnosti vytvořeno programové rozhraní IS EO uloženými procedurami databázového systému Informix.

Zadavatel předpokládá, že přístup IS Policie ČR bude realizován standardním voláním eGON funkcí prostřednictvím ISZR. Toto řešení je však nutné v rámci analýzy upřesnit a projednat s Policí ČR za účasti hlavního architekta ZR a správce AIS EO v době analytických prací vzhledem k rozsáhlým a nestandardním požadavkům Policie ČR a požadavku Policie ČR na přímé připojení k AIS. Pokud bude dohodnuto řešení odlišné od standardního, realizovat dohodnuté řešení při zachování standardních bezpečnostních požadavků (výdej v souladu s příslušnými zákony, autentizace/autorizace aplikace, přebírání identifikace uživatele, zápis výdeje dat atd.).

Hromadné výdeje dat pro externí subjekty

V rámci stávajícího systému je realizováno 25 samostatných programů pro výdej dat externím subjektům (VZP, MO, MF, ..), které jsou spouštěny pravidelně nebo na žádost externího subjektu. Programy zpracovávají vstupní soubory dodané externími subjekty nebo se vstupní údaje zadávají interaktivně. Výstupem jsou textové a .unl soubory. Výstupy jsou předávány na médium (CD/DVD) nebo „vystavením“ na web stránce.

Zadavatel požaduje posoudit v rámci analýzy každý jednotlivý existující výdej a po projednání s příslušným externím subjektem navrhnout odpovídající nové řešení (zachovat stávající výdej včetně struktury údajů, nahradit výdejem prostřednictvím ISZR) a zajistit jeho realizaci nebo navrhnout zánik daného výstupu.

Hromadné výdeje dat do informačních systémů pro obce, obce III a Prahu

V rámci stávajícího systému jsou realizovány programy pro výdej dat z IS EO ve formě textových souborů a definovaných .unl souborů určené pro jednotlivé obce, obce III a Prahu. Soubory .unl slouží pro zpracování informací o osobách příslušných obcím v jejich obecních systémech. Spouštění programů provádějí obce podle svých potřeb (zpracování se provádí na tzv. „okresních serverech“). Programy respektují rozsah působnosti subjektů a podle toho vydávají pouze osoby dle působnosti daného subjektu.

Zadavatel požaduje navrhnout v rámci analýzy nový způsob výdeje dat pro obce, obce III a Prahu a zajistit jeho realizaci. Strukturu výstupních souborů je nutné zachovat, aby externí subjekty nebyly nuceny upravovat svoje díla. Subjekt musí mít možnost on-line stáhnout výsledky zpracování na svoji výpočetní techniku pro další zpracování (prostřednictvím ISZR a KIVS).

Rozhraní pro e-Pasy (projekt CDBP MV, výroba cestovních dokladů) a e-Pasy na MZV (část pro přístup do EO)

Ve stávajícím systému je vytvořeno specializované programové rozhraní, které pomocí technologie web services poskytuje údaje z IS EO pro potřeby projektu CDBP (e-pasy). Toto programové rozhraní používá i informační systém MZV pro projekt CDBP v rámci MZV.

Zadavatel předpokládá, že vzhledem k rozdělení IS EO a IS ECD na zcela samostatné AIS s vlastními AIFO, bude pro systém CDBP zajišťovat podporu AIS ECD a data z AIS EO budou získávána standardním voláním eGON funkcí ISZR (viz popis v části ECD).

Dále zadavatel předpokládá, že MZV bude muset upravit svůj systém na standardní volání eGON funkcí prostřednictvím ISZR.

Za těchto předpokladů nebude nutné realizovat uvedené specializované rozhraní. Upřesnění a projednání uvedených předpokladů bude nutné provést v rámci analýzy AIS3.

Rozhraní pro e-OP (projekt e-OP/CDBP MV, výroba občanských průkazů) (část pro přístup do EO)

Ve stávajícím systému je vytvořeno specializované programové rozhraní, které pomocí technologie web services poskytuje údaje z IS EO pro potřeby projektu e-OP/CDBP (e-OP).

Zadavatel předpokládá, že vzhledem k rozdělení IS EO a IS EOP na zcela samostatné AIS s vlastními AIFO, bude pro systém e-OP/CDBP zajišťovat podporu AIS EOP a data z AIS EO budou získávána standardním voláním eGON funkcí ISZR (viz popis v části EOP).

Za těchto předpokladů nebude nutné realizovat uvedené specializované rozhraní. Upřesnění a projednání uvedených předpokladů bude nutné provést v rámci analýzy AIS3.

Rozhraní pro centrální registr řidičů (CRŘ) Ministerstva dopravy

Ve stávajícím systému je vytvořeno specializované programové rozhraní, které pomocí technologie web services poskytuje údaje z IS EO pro potřeby centrálního registru řidičů.

Zadavatel předpokládá, že od okamžiku spuštění ISZR začne centrální registr řidičů používat standardních volání funkcí v rámci ISZR a nadále nebude nutné provozovat specializované rozhraní pro tento případ.

Rozhraní na informační systém CzechPOINT pro editory 2. skupiny

Pro editory 2. skupiny je ve stávajícím systému vytvořeno specializované programové rozhraní (technologie web services, protokol https, basic autentizace volající aplikace), které umožňuje provádění vybraných změn (aktualizací) prostřednictvím formulářů CzechPOINTu (změny lze provádět v IS EO, IS EOP, IS ECD).

Editoři této skupiny se internetem připojují přímo k systému CzechPOINT, jsou autentizováni systémem CzechPOINT a pracují s formuláři systému CzechPOINT. Systém CzechPOINT pak změny předává voláním web services tohoto programového rozhraní. Výběr dat z IS EO je zajišťován univerzálním programovým rozhraním, identickým s programovým rozhraním pro externí subjekty a rozsahem údajů podle oprávnění jednotlivých editorů.

Jedná se o následující editory:

- ohlašovny obcí (změna trvalého pobytu)
- matriční úřady (matriční změny)
- soudy (rozhodnutí o změně svéprávnosti, svěření do opatrovnictví, ...).

Zadavatel požaduje realizovat v rámci AIS EO obdobnou funkcionalitu, aby programové vybavení systému CzechPOINT nemuselo být upravováno. Podle potřeby lze ve spolupráci s řešiteli systému CzechPOINT realizovat úpravy formulářů.

Rozhraní na web MV

V rámci stávajícího systému je zpracovávána řada výstupů (seznamy, statistiky), které jsou publikovány na webu MV.

Zadavatel požaduje provést se správcem webu MV a správcem AIS EO v rámci analýzy posouzení jednotlivých výstupů, určených pro publikování na webu MV a navrhnout odpovídající způsob zpracování a předávání údajů pro web MV a zajistit jeho realizaci. Podrobný seznam výstupů, publikovaných na webu MV bude k dispozici při analýze AIS3.

Publikování „adresy“

V rámci stávajícího systému je pro řadu navazujících systémů a pro WEB MV „publikován“ obsah subsystému „adresa“ (ve formátu .unl souborů s předem dohodnutou strukturou, soubory jsou nahrávány na ftp servery odběratelů, dále vystavovány na web serverech CVS ke stažení a některým odběratelům předávány na CD).

Zadavatel požaduje provést se správcem webu MV, správcem AIS EO a správcem základního registru RUIAN posouzení účelnosti toho výstupu, a navrhnout odpovídající způsob řešení a zajistit jeho realizaci, nebo navrhnout jiný způsob zajištění tohoto výstupu pro navazující systémy. Podrobný seznam odběratelů bude k dispozici při analýze AIS3.

3.4.2 AIS EOP

Rozhraní na základní registry

AIS EOP je v roli sekundárního editora ROB.

Komunikace AIS EOP ze základními registry se realizuje příslušnou službou eGON, definovanou v dokumentaci k informačním systémům základních registrů vztažených k AIS3. Prostřednictvím tohoto rozhraní provádí EOP:

- aktualizaci údajů osob v ROB pro občany České republiky
- získávání údajů o aktuálních adresách z RUIAN (prvotní inicializace dat v EO z RUIAN pro vedené platné adresy, využití notifikačních služeb).

Rozsah dat, která se zasílají/modifikují do/v ROB je dán výčtem vedených položek v ROB podle zákona.

ISZR pomocí rozhraní zasílá na AIS EOP žádosti o reklamace údajů osob vedených v ROB a požadavky jiných AIS na výdej dat z EOP, která nejsou vedena v ROB.

AIS EOP připravuje notifikace změn k údajům vedených v AIS EOP.

Rozhraní technologií Web Services. Zabezpečení, způsob a obsah komunikace specifikují projekty základních registrů.

Univerzální dotazovací rozhraní pro externí subjekty

Pro OVM s právem získávání údajů z evidence občanských průkazů (dále „externí subjekty“) je ve stávajícím IS EOP vytvořeno programové rozhraní, které umožňuje

externímu subjektu získávat údaje v rozsahu zákonného oprávnění tohoto subjektu (vydávají se pouze údaje, explicitně uvedené v příslušném zákoně). Rozhraní poskytuje přístup pomocí web services nebo pomocí XML dotazu a odpovědi, použit je přenosový protokol https. Provádí se basic autentizace volající aplikace. Nad tímto programovým rozhraním je dále vytvořen tzv. web klient, který umožňuje přístup uživatelům externího subjektu přímo z www prohlížeče (v tomto případě se provádí plná autentizace uživatele).

Zadavatel požaduje nahradit toto rozhraní obdobnou funkcí, zajišťovanou prostřednictvím eGON funkcí, které bude externí subjekt volat prostřednictvím ISZR. Přitom se předpokládá, že ISZR „rozloží“ dotaz externího subjektu na čtení údajů z ROB a čtení údajů z AIS EOP a odpovědi obou systémů „složí“ do jedné odpovědi. Rozsah vydávaných údajů musí odpovídat oprávnění v příslušném zákonu (úplný přehled připojených externích subjektů a aplikovaných zákonů bude k dispozici v době analýzy AIS3).

Přímé dotazování uživatelů externích subjektů z www prohlížeče do AIS EOP se v době vzniku tohoto dokumentu nepředpokládá, má být nahrazeno přístupem prostřednictvím portálu veřejné správy. Součástí řešení musí tedy být spolupráce s portálem veřejné správy nebo návrh jiného řešení, které externím uživatelům z institucí bez vlastního informačního systému umožní získávání údajů z AIS EOP.

Rozhraní pro IS Policie ČR

Pro IS Policie ČR je v současnosti vytvořeno programové rozhraní IS EOP uloženými procedurami databázového systému Informix. Dále používá IS Policie ČR pro čtení fotografií volání univerzálního programového rozhraní, založeného na web services a XML dotazu a odpovědi.

Zadavatel předpokládá, že přístup IS Policie ČR bude realizován standardním voláním funkcí prostřednictvím ISZR. Toto řešení je však nutné v rámci analýzy upřesnit a projednat s Policí ČR za účasti hlavního architekta ZR a správce AIS EOP v době analytických prací vzhledem k rozsáhlým a nestandardním požadavkům Policie ČR a požadavku Policie ČR na přímé připojení k AIS. Pokud bude dohodnuto řešení odlišné od standardního, realizovat dohodnuté řešení při zachování standardních bezpečnostních požadavků (výdej v souladu s příslušnými zákony, autentizace/autorizace aplikace, přebírání identifikace uživatele, zápis výdeje dat atd.).

Rozhraní na informační systém CzechPOINT pro editory 2. skupiny

Pro editory 2. skupiny je ve stávajícím systému vytvořeno specializované programové rozhraní (technologie web services, protokol https, basic autentizace volající aplikace), které umožňuje provádění vybraných změn (aktualizací) prostřednictvím formulářů CzechPOINTu (změny lze provádět v IS EO, IS EOP, IS ECD).

Editoři této skupiny se internetem připojují přímo k systému CzechPOINT, jsou autentizováni systémem CzechPOINT a pracují s formuláři systému CzechPOINT. Systém CzechPOINT pak změny předává voláním web services tohoto programového rozhraní. Součástí rozhraní je i výběr údajů o OP osob, které vstupují do matričních změn z IS EOP, zajišťovaný univerzálním programovým rozhraním, identickým s programovým rozhraním pro externí subjekty a rozsahem údajů podle oprávnění jednotlivých editorů.

Jedná se o následující editory:

- ohlašovny obcí (změna trvalého pobytu)

- matriční úřady (matriční změny)
- soudy (rozhodnutí o změně svéprávnosti, svěření do opatrovnictví, ...).

Zadavatel požaduje realizovat v rámci AIS EOP obdobnou funkcionalitu, aby programové vybavení systému CzechPOINT nemuselo být upravováno. Podle potřeby lze ve spolupráci s řešiteli systému CzechPOINT realizovat úpravy formulářů.

Seznam změn, prováděných prostřednictvím systému CzechPOINT je uveden v příloze č. 1.1. Věcná část zadávací dokumentace veřejné zakázky „Implementátor AIS EO, AIS EOP a AIS ECD“.

Rozhraní na informační systém Policie ČR pro editory 3. skupiny

Policie ČR je editorem údajů o OP (ztráta, odcizení OP). Pro tuto skupinu editorů je nezbytné vytvořit programové rozhraní k informačnímu systému Policie ČR tak, aby příslušníci Policie ČR mohli provádět požadované změny v AIS EOP.

Způsob realizace je nezbytné projednat s Policí ČR, správcem AIS EOP a hlavním architektem ZR za MV.

Rozhraní pro e-OP (projekt e-OP/CDBP MV, výroba občanských průkazů) (část pro přístup do EOP)

Ve stávajícím systému je vytvořeno specializované programové rozhraní, které pomocí technologie web services poskytuje údaje z IS EOP pro potřeby projektu e-OP/CDBP (e-OP). Zároveň poskytuje přístup do IS EO (viz popis v části IS EO) a IS ECD (výběr fotografie). Dále přebírá od e-OP/CDBP údaje o vyrobených občanských průkazech a zapisuje je do IS EOP.

Zadavatel požaduje provedení plné integrace stávajícího systému e-OP (e-OP/CDBP) do AIS EOP tak, aby nebylo nutné provádět v rámci systému e-OP/CDBP změny nebo úpravy programového řešení. Zadavatel tedy předpokládá, že AIS ECD bude pro e-OP/CDBP poskytovat přístup k údajům o občanských průkazech, přebírat a ukládat údaje o vyrobených občanských průkazech a dále zajistí (zprostředkováním volání eGON funkcí ISZR) přístup e-OP/CDBP k údajům z AIS EO (emulátor stávajícího programového rozhraní IS EO pro e-OP/CDBP) a k fotografiím v AIS ECD (emulátor stávajícího programového rozhraní IS ECD pro e-OP/CDBP).

Zadavatel předpokládá upřesnění této problematiky v rámci analytických prací AIS3.

Neplatné, ztracené a odcizené občanské průkazy

V současném IS EOP jsou vytvářeny seznamy neplatných, ztracených a odcizených občanských průkazů. Seznamy jsou vytvářeny jako .unl soubory v předem dohodnuté struktuře a pomocí ftp jsou nahrávány na určený server „odběratele“.

Unl soubory jsou vytvářeny pro:

- Schengenský informační systém
- Interpol
- WEB MV (publikování seznamu na webu MV).

Pro každého „odběratele“ je stanoven odlišný formát souboru (pro WEB MV se předává každý den kompletní seznam dokladů, pro Schengenský informační systém a Interpol je předáván seznam „přírůstků“ a „úbytků“).

Zadavatel požaduje, vytvořit pro uvedené odběratele výstupy ve stejném formátu a zajistit jejich předávání prostřednictvím ISZR („publikování“ souboru ke stažení). Předávané seznamy musí obsahovat minimálně následující údaje: čísla, popřípadě série ztracených, odcizených, zničených nebo neplatných občanských průkazů a datum ohlášení ztráty, odcizení nebo zničení občanského průkazu. Minimální četnost vystavení je jedenkrát denně a v rámci analýzy musí být upřesněna s jednotlivými „odběrateli“.

3.4.3 AIS ECD

Rozhraní na základní registry

AIS ECD je v roli sekundárního editora ROB.

Komunikace AIS ECD ze základními registry se realizuje příslušnou službou eGON, definovanou v dokumentaci k informačním systémům základních registrů vztažených k AIS3. Prostřednictvím tohoto rozhraní provádí AIS ECD:

- aktualizaci údajů osob v ROB pro občany České republiky
- získávání údajů o aktuálních adresách z RUIAN (prvotní inicializace dat v EO z RUIAN pro vedené platné adresy, využití notifikačních služeb).

Rozsah dat, která se zasílají/modifikují do/v ROB je dán výčtem vedených položek v ROB podle zákona.

ISZR pomocí rozhraní zasílá na AIS ECD žádosti o reklamace údajů osob vedených v ROB a požadavky jiných AIS na výdej dat z ECD, která nejsou vedena v ROB.

AIS ECD připravuje notifikace změn k údajům vedených v AIS ECD.

Rozhraní technologií Web Services. Zabezpečení, způsob a obsah komunikace specifikují projekty základních registrů.

Univerzální dotazovací rozhraní pro externí subjekty

Pro OVM s právem získávání údajů z evidence cestovních dokladů (dále „externí subjekty“) je ve stávajícím IS ECD vytvořeno programové rozhraní, které umožňuje externímu subjektu získávat údaje v rozsahu zákonného oprávnění tohoto subjektu (vydávají se pouze údaje, explicitně uvedené v příslušném zákoně). Rozhraní poskytuje přístup pomocí web services nebo pomocí XML dotazu a odpovědi, použit je přenosový protokol https. Provádí se basic autentizace volající aplikace. Nad tímto programovým rozhraním je dále vytvořen tzv. web klient, který umožňuje přístup uživatelů externího subjektu přímo z www prohlížeče (v tomto případě se provádí plná autentizace uživatele).

Zadavatel požaduje nahradit toto rozhraní obdobnou funkčností, zajišťovanou prostřednictvím eGON funkcí, které bude externí subjekt volat prostřednictvím ISZR. Přitom se předpokládá, že ISZR „rozloží“ dotaz externího subjektu na čtení údajů z ROB a čtení údajů z AIS ECD a odpovědi obou systémů „složí“ do jedné odpovědi. Rozsah vydávaných údajů musí odpovídat oprávnění v příslušném zákonu (úplný přehled

připojených externích subjektů a aplikovaných zákonů bude k dispozici v době analýzy AIS3).

Přímé dotazování uživatelů externích subjektů z www prohlížeče do AIS ECD se v době vzniku tohoto dokumentu nepředpokládá, má být nahrazeno přístupem prostřednictvím portálu veřejné správy. Součástí řešení musí tedy být spolupráce s portálem veřejné správy nebo návrh jiného řešení, které externím uživatelům z institucí bez vlastního informačního systému umožní získávání údajů z AIS ECD.

Rozhraní pro IS Policie ČR

Pro IS Policie ČR je v současnosti vytvořeno programové rozhraní IS ECD uloženými procedurami databázového systému Informix. Dále používá IS Policie ČR pro čtení fotografií volání univerzálního programového rozhraní, založeného na web services a XML dotazu a odpovědi.

Zadavatel předpokládá, že přístup IS Policie ČR bude realizován standardním voláním eGON funkcí prostřednictvím ISZR. Toto řešení je však nutné v rámci analýzy upřesnit a projednat s Policí ČR za účasti hlavního architekta ZR a správce AIS ECD v době analytických prací vzhledem k rozsáhlým a nestandardním požadavkům Policie ČR a požadavku Policie ČR na přímé připojení k AIS. Pokud bude dohodnuto řešení odlišné od standardního, realizovat dohodnuté řešení při zachování standardních bezpečnostních požadavků (výdej v souladu s příslušnými zákony, autentizace/autorizace aplikace, přebírání identifikace uživatele, zápis výdeje dat atd.).

Rozhraní pro e-Pasy (projekt CDBP MV) a ePasy na MZV (část pro přístup do ECD)

Ve stávajícím systému je vytvořeno specializované programové rozhraní, které pomocí technologie web services poskytuje údaje z IS ECD pro potřeby projektu CDBP (e-pasy). Zároveň poskytuje přístup do IS EO (viz popis v části IS EO). Dále přebírá od CDBP údaje o vyrobených cestovních dokladech a zapisuje je do IS ECD.

Zadavatel požaduje provedení plné integrace stávajícího systému e-Pasy (CDBP) do AIS ECD tak, aby nebylo nutné provádět v rámci systému CDBP změny nebo úpravy programového řešení. Zadavatel tedy předpokládá, že AIS ECD bude pro CDBP poskytovat přístup k údajům o cestovních dokladech, přebírat a ukládat údaje o vyrobených cestovních dokladech a dále zajistí (zprostředkováním volání eGON funkcí ISZR) přístup CDBP k údajům z AIS EO (emulátor stávajícího programového rozhraní IS EO pro CDBP).

Zadavatel předpokládá upřesnění této problematiky v rámci analytických prací AIS3.

Rozhraní pro e-OP (projekt e-OP/CDBP MV, výroba občanských průkazů) (část pro přístup do ECD)

Ve stávajícím systému je vytvořeno specializované programové rozhraní, které pomocí technologie web services poskytuje údaje z IS ECD pro potřeby projektu e-OP/CDBP (e-OP), jde o poskytnutí fotografie z cestovního dokladu pro výrobu občanského průkazu.

Zadavatel předpokládá, že vzhledem k rozdělení IS ECD a IS EOP na zcela samostatné AIS s vlastními AIFO, bude pro systém e-OP/CDBP zajišťovat podporu AIS EOP a data z AIS ECD budou získávána standardním voláním eGON funkcí ISZR (viz popis v části EOP).

Za těchto předpokladů nebude nutné realizovat uvedené specializované rozhraní. Upřesnění a projednání uvedených předpokladů bude nutné provést v rámci analýzy AIS3.

Rozhraní na informační systém CzechPOINT pro editory 2. skupiny

Pro editory 2. skupiny je ve stávajícím systému vytvořeno specializované programové rozhraní (technologie web services, protokol https, basic autentizace volající aplikace), které umožňuje provádění vybraných změn (aktualizací) prostřednictvím formulářů CzechPOINTu (změny lze provádět v IS EO, IS EOP, IS ECD).

Editoři této skupiny se internetem připojují přímo k systému CzechPOINT, jsou autentizováni systémem CzechPOINT a pracují s formuláři systému CzechPOINT. Systém CzechPOINT pak změny předává voláním web services tohoto programového rozhraní. Součástí rozhraní je i výběr údajů o CD osob, které vstupují do matričních změn z IS ECD, zajišťovaný univerzálním programovým rozhraním, identickým s programovým rozhraním pro externí subjekty a rozsahem údajů podle oprávnění jednotlivých editorů.

Jedná se o následující editory:

- ohlašovny obcí (změna trvalého pobytu)
- matriční úřady (matriční změny)
- soudy (rozhodnutí o změně svéprávnosti, svěření do opatrovnictví, ...).

Zadavatel požaduje realizovat v rámci AIS ECD obdobnou funkcionalitu, aby programové vybavení systému CzechPOINT nemuselo být upravováno. Podle potřeby lze ve spolupráci s řešiteli systému CzechPOINT realizovat úpravy formulářů.

Neplatné, ztracené a odcizené cestovní doklady

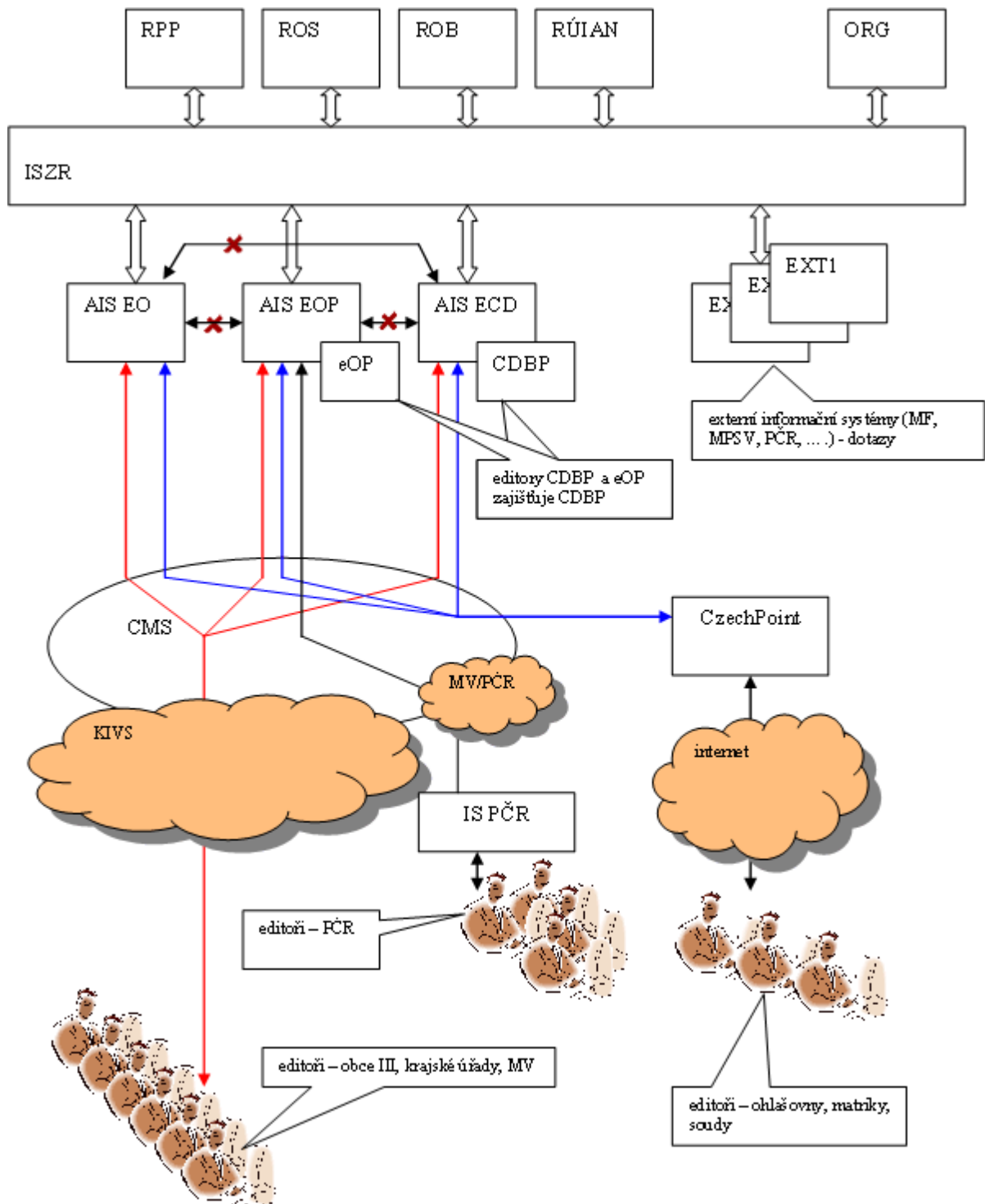
V současném IS ECD jsou vytvářeny seznamy neplatných, ztracených a odcizených cestovních dokladů. Seznamy jsou vytvářeny jako .unl soubory v předem dohodnuté struktuře a pomocí ftp jsou nahrávány na určený server „odběratele“.

Unl soubory jsou vytvářeny pro:

- Schengenský informační systém
- Interpol
- WEB MV (publikování seznamu na webu MV).

Pro každého „odběratele“ je stanoven odlišný formát souboru (pro WEB MV se předává každý den kompletní seznam dokladů, pro Schengenský informační systém a Interpol je předáván seznam „přírůstků“ a „úbytků“).

Zadavatel požaduje, vytvořit pro uvedené odběratele výstupy ve stejném formátu a zajistit jejich předávání prostřednictvím ISZR („publikování“ souboru ke stažení). Předávané seznamy musí obsahovat minimálně následující údaje: o ztracených, odcizených nebo neplatných cestovních dokladech: číslo, druh, datum vydání a datum skončení platnosti ztraceného, odcizeného nebo neplatného cestovního dokladu a datum a místo ohlášení jeho ztráty nebo odcizení. Minimální četnost vystavení je jedenkrát denně a v rámci analýzy musí být upřesněna s jednotlivými „odběrateli“.



Obrázek č. 2 Začlenění jednotlivých skupin editorů a externích systémů do celkové architektury AIS3 a ISZR

3.5 Převod dat

3.5.1 Požadavky na převod dat ze stávajících systémů do AIS3

Součástí řešení AIS3 je i převod dat ze stávajících informačních systémů správních evidencí do AIS3. Převod dat do AIS3 bude proveden z centrálních databází stávajících systémů. Před vlastní migrací provedou odborné útvary Ministerstva vnitra konsolidaci dat mezi 77 okresními servery a centrálními databázemi. Orientační schéma migrace je uvedeno na obrázku 3.

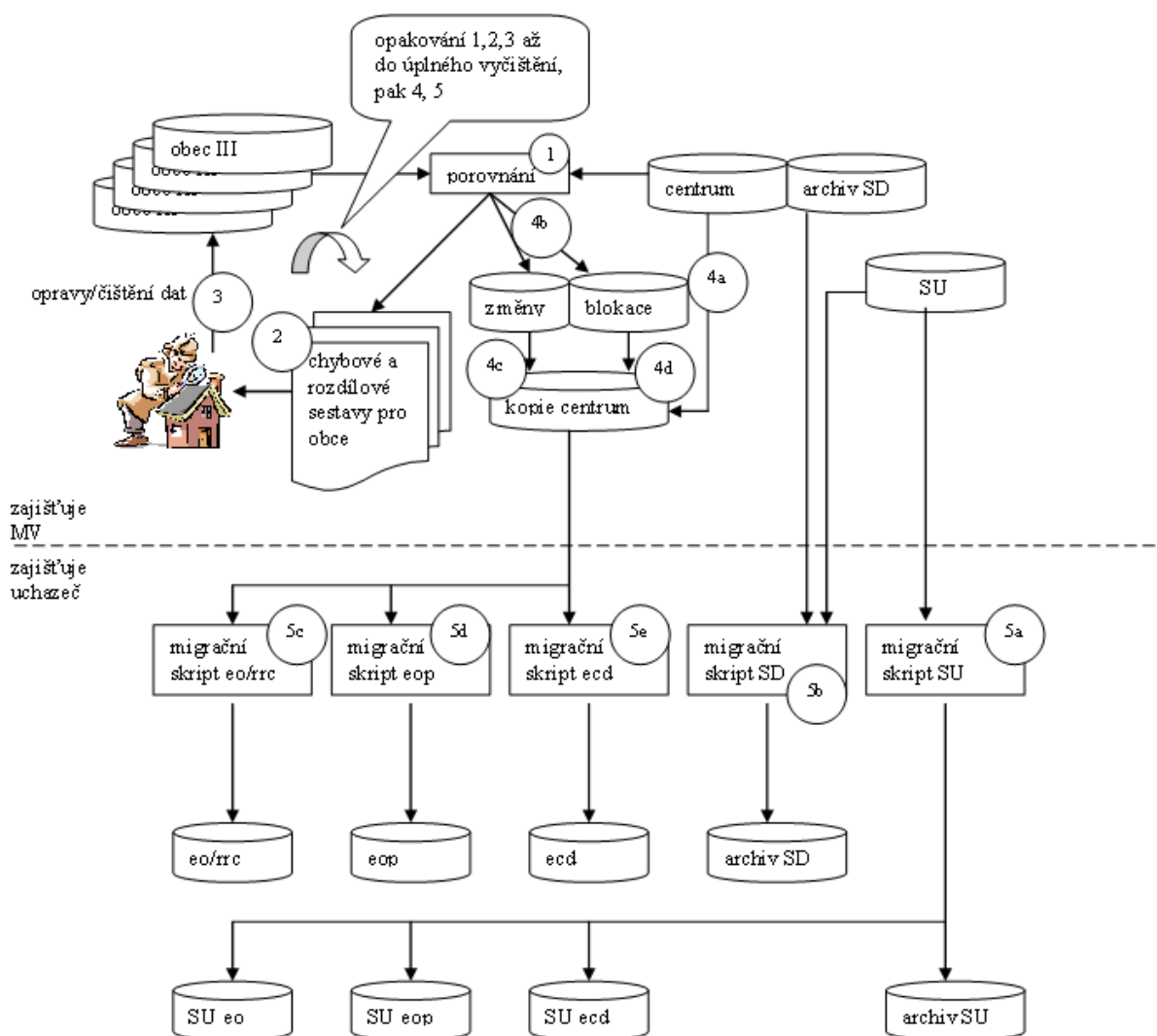
Převod dat bude zahrnovat činnosti zajišťované Zadavatelem:

1. Porovnání dat okresních databází s databází v centru.
2. Generování rozdílových sestav pro obce.
3. Čištění a opravy dat na obcích.

Zaznamenání změn, blokace chybných dat a dat, kde jsou rozdíly mezi okresem a centrem.

Od uchazeče je v oblasti čištění a migrace dat požadováno následující:

1. Navrhnout a vytvořit programy pro migraci jednotlivých centrálních databází stávající evidence obyvatel (včetně evidence rodných čísel), stávající evidence občanských průkazů a stávající evidence cestovních dokladů do AIS3.
2. Navrhnout a vytvořit programy pro migraci stávající evidence uživatelů a sledování dotazů a vytvořit z nich „archivní“ datové fondy dostupné v pro vyhledávání.
3. Navrhnout a vytvořit programy pro kontrolu dat převedených do AIS3.
4. Navrhnout datové modely a migrační skripty tak, aby nedošlo ke ztrátě dat v AIS3 oproti stávajícímu stavu (jak aktuálních, tak archivních).



Obrázek č. 3 Orientační schéma migrace

3.5.2 Bezpečnostní omezení

Veškeré aktivity související s datovým obsahem agend lze provádět pouze v prostorách Zadavatele a za asistence pověřených pracovníků Zadavatele. O každé manipulaci s daty je nutno vypracovat protokol.

3.6 Technologické požadavky

3.6.1 Základní požadavky

3.6.1.1 Instance AIS

Zadavatel požaduje vytvořit technickou infrastrukturu AIS EO, AIS EOP, AIE ECD v následujících instancích:

- Provozní (CVS 1+1, ZVS 1+0)
- Testovací (měla by v potřebné míře kopírovat provozní infrastrukturu, aby bylo možné otestovat všechny mechanismy včetně reakce na selhání, disaster recovery atd., musí umožnit testování změn/oprav/patchů před nasazením na provozní prostředí)
- Školící

3.6.1.2 Připojení do komunikační infrastruktury

AIS EO, AIS EOP a AIS ECD budou připojeny do komunikační infrastruktury státní správy připojením na centrální komunikační uzel státní správy ČR. Centrální komunikační uzel státní správy ČR tvoří dva redundantní bloky IC (InterConnect) – IC1 a IC2 a dva redundantní bloky CMS (Centrální místo služeb) označované dnes jako CMS1. Jednotlivé AIS budou redundantně připojeny k IC1 a IC2 na L2 vrstvě optickými spoji GE s možností agregace linek Nx1GE technologií EtherChannel (LACP).

V době vzniku tohoto dokumentu je v provozu CMS1 a připravuje se další etapa výstavby CMS označovaná jako CMS2.

Zadavatel předpokládá, že podrobnosti připojení k IC1 a IC2 budou upřesněny v době analytických prací a přípravy globálního návrhu systému. V rámci návrhu musí být upřesněny a s Českou poštou projednány požadavky na další parametry komunikačního propojení, tj. VPN, VLAN, směrovací protokoly, adresace IPv4 a IPv6, VSS, NTP, DNS atd. v závislosti na technologiích, použitých při návrhu AIS3.

Vnitřní propojení jednotlivých zařízení (serverů) v rámci jednotlivých AIS je záležitostí uchazeče.

3.6.1.3 Komunikace s ISZR a externími systémy

Komunikace s ISZR bude probíhat podle specifikací ISZR protokolem https a technologií „web services“. Komunikace s externími systémy bude probíhat výhradně prostřednictvím ISZR.

3.6.1.4 Komunikace s uživateli systému (editory)

Komunikace s uživateli systému (editory) bude probíhat výhradně prostřednictvím interconnectu (IC1/IC2). Při návrhu systému je nezbytné vzít v úvahu, že obce jsou do komunikační infrastruktury připojeny většinou linkou o rychlosti 1Mb/s, sdílenou s jinými agendami.

3.6.1.5 Prostředky na straně uživatele

K systému musí být ze strany koncového uživatele připojitelné PC s operačním systémem Microsoft Windows XP a vyšší a prohlížeči MS Internet Explorer 8 a vyšší nebo Mozilla FireFox 4 a vyšší nebo Google Chrome 12 a vyšší. Tento požadavek se týká uživatelů (editorů), kteří budou používat web rozhraní ASI3.

3.6.2 Bezpečnostní požadavky

3.6.2.1 Organizační

Návrh systému musí obsahovat komponenty a oblasti, které umožní správci a provozovateli informačního systému zavedení, provozování, monitorování a kontrolu bezpečnosti zpracovávaných, přenášených a ukládaných informací. Odtud vyplývá rámcové vymezení oblasti informačních rizika a stanovení směrů a postupů řešení nápravných opatření.

3.6.2.2 Technologické

V návrhu musí být zmíněny požadavky na bezpečnost informačních technologií. Zejména se jedná o eliminaci hrozeb, které se týkají neoprávněného přístupu, kompromitace, modifikace nebo zneužití zpracovávaných informací apod.

Technologická zařízení (zejména se jedná o komponenty obsahující paměťová média) musí být chráněna proti rizikům i při používání mimo prostory organizace.

3.6.2.3 Provozní

- V návrhu musí být uvedeny požadavky na provozní zajištění výpočetní techniky a dalších komponent (např. síťové prvky) – požadované napájení + požadavek na výkon UPS, požadavek na chlazení dodané techniky, váha dodané techniky.

3.7 Provozní a kapacitní parametry stávajících systémů

Počty záznamů a počty operací jsou uvedeny v následujících tabulkách:

AIS		EO	EOP	ECD
Počet evidovaných subjektů	primární tabulka	16 800 000	24 300 000	14 800 000
	Archiv	82 200 000	40 300 000	25 300 000
	Foto	-	13 400 000	6 200 000
Počet změn za měsíc	okres – centrum *)	30 000	330 000	45 000
	centrum – okres *)	120 000		
	via CzechPOINT **)	40 000		
Počet dotazů za měsíc	Interaktivní	cca 5-10 mil		
Počet uživatelů	obce+resort	cca 4 000		
	externí subjekty	cca 20 000		
	PČR	více než 40 000		

*) údaj znamená počet řádek transakcí, přenesených mezi okresním serverem a centrem

**) údaj znamená počet osob aktualizovaných z matrik, ohlašoven a soudů prostřednictvím formulářů CzechPOINT

„Sledování dotazů“ (datový audit)	SD
denní tabulka (počet záznamů – denní přírůstek)	cca 600 000
počet archivních tabulek (měsíční tabulky)	156 (13 let x 12 měsíců)
počet záznamů v archivních tabulkách	cca 1 220 000 000

„Správa uživatelů“	SU
počet lokálně evidovaných účtů	Cca 30 000
přístupy na externí servery	MPSV, MZe, MSp, CUZK, MF, MPO a postupně další

3.8 Postup předávání systému do provozu

3.8.1 Atestace způsobilosti k realizaci vazeb ISVS s jinými IS

Zadavatel požaduje spolupráci při přípravě na atestaci způsobilosti k realizaci vazeb ISVS s jinými IS prostřednictvím referenčního rozhraní podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

3.8.2 Bezpečnostní audit

Návrh systému musí obsahovat takovou koncepci, která umožní realizovat pravidelné interní bezpečnostní kontroly. Cílem těchto kontrol bude určení míry shody s bezpečnostními požadavky stanovenými v právních předpisech ČR, jakož i posouzení souladu s požadavky bezpečnostních norem ISO/IEC.

S tím souvisí respektování požadavků souvisejících s řešením bezpečnosti ve vztahu k potenciálním bezpečnostním rizikům a návrh základních bezpečnostních procesů tak, aby byly v souladu s příslušnými normami resp. zákony.

3.8.3 Testování systému

Součástí plnění bude provedení následujících typů testů:

- **Testy funkcionality** – sestavené pro kontrolu funkčnosti jednotlivých komponent řešení s požadavky Zadavatele na zpracování procesů, které má řešení podporovat.
- **Integrační testy** – určené pro kontrolu funkčnosti systému jako celku. Jsou zaměřeny na operace, které jsou považovány za hlavní body funkčnosti při integraci dílčích komponent celého systému včetně všech rozhraní.
- **Bezpečnostní testy** – ukazující na míru bezpečnosti systému a jeho shodu s bezpečnostními požadavky (bezpečnostním projektem) např. na možnosti neautorizovaného přístupu, efektivnost bezpečnostních opatření, ochranu proti nežádoucímu kódu, bezpečnostním chybám apod. Součástí bezpečnostních testů musí být i provedení penetračních testů.
- **Zátěžové testy** – ověření reálného výkonu a odolnosti systému při velké zátěži. Testy jsou soustředěny na nalezení výkonnostních limitů a úzká hrdla architektury systému, limity aplikací, web služeb apod.
- **Performance test** - sleduje jaká je jeho odezva systému, výkonnost, propustnost apod.
- **Recovery testy** – testující reakci testovaného produktu na black-out systému, HW chybu, výpadky SW atd.

3.8.4 Požadavky na školení obsluhy

Zaškolení následujících skupin obsluhy:

- **administrátoři** – školení bude zaměřeno na zajištění provozu jednotlivých systémů, odstraňování problémů, předcházení problémům, řešení havarijních situací apod. – školení musí minimálně zahrnovat obsluhu techniky, architektonický návrh systému, popis jednotlivých komponent a jejich funkcionality, obsluhu jednotlivých komponent a jejich konfigurování, metody monitorování stavu systému, používání monitorovacího

systému, řešení základních havarijních situací, předcházení havarijním situacím, řešení zálohování a případných obnov dat na discích serverů a databázích, vazby na jiné systémy, základní informace o použitém OS, databázovém serveru a dalším systémovém SW.

- **operátoři (nepřetržitý dohled)** – školení bude zaměřeno na popis základního architektonického návrhu, obsluhu techniky, použití monitorovacích nástrojů, vyhodnocování hlášení monitorovacího systému, zálohování.
- **HelpDesk** – školení bude zaměřeno na architekturu systému, návaznost na jiné systémy, práci se všemi uživatelskými aplikacemi (podrobné školení), řešení problémových situací, řešení problémů v datech (popř. použití specializovaných nástrojů na opravu dat).
- **škoolitelé** – školení bude zaměřeno na architekturu systému, práci s jednotlivými uživatelskými aplikacemi (podrobné školení), řešení základních chyb.

3.8.5 Požadavky na dokumentaci systému

Součástí dodávky bude kompletní dokumentace AIS3, vyhotovenou v listinné (1 paré) a elektronické podobě (na datovém nosiči v editovatelné formě), obsahující kompletní popis AIS3, tj. především:

- provozní dokumentace podle § 10 a 11 vyhlášky č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy). Požadovaný formát dokumentace je DOC nebo XLS.
- popis souhrnu určených činností a potřebných oprávnění pro provádění těchto činností pro správce systému a bezpečnostního správce systému v předmětných informačních systémech (§ 12 výše uvedené vyhlášky). Požadovaný formát dokumentace je DOC nebo XLS.
- předávání údajů do informačního systému o informačních systémech veřejné správy
- dokumentaci podrobné analýzy a návrhu AIS3. Požadovaný formát dokumentace je UML (Unified Modelling Language). Uchazeč ve své nabídce povinně navrhne způsob dokumentace (konkrétní diagramy nebo jiný způsob strukturovaného popisu) procesů AIS3, architektury, logického a fyzického schématu datového modelu databáze a objektového modelu AIS3. Uchazeč dále povinně v nabídce nabídne v rámci Celkové nabídkové ceny licenci na software, ve kterém jsou podrobná analýza a podrobný návrh AIS3 vytvořeny, a to pro 3 uživatele (minimálně 1 licence musí být vývojová licence, umožňující úpravu dodané dokumentace)
- všechny technické, odborné, uživatelské a záruční informace potřebné pro Zadavatele k zajištění trvalého provozu AIS3 dle sledovaného účelu a cílů Projektu definovaného v „zadávací dokumentaci veřejné zakázky“.

(dále jen „Dokumentace“).

Z pohledu bezpečnosti informací musí Dokumentace obsahovat záznamy v takovém stavu a rozsahu, aby bylo zajištěno, že (veškeré) činnosti související s bezpečnostními aspekty jsou zpětně dohledatelné. Dokumentace musí být chráněna a strukturována, musí být zajištěna její integrita, dostupnost i v rámci dlouhodobého ukládání.

3.9 Požadavky na provoz

Rutinní provoz dodaných systémů AIS3 bude zabezpečován Zadavatelem.

3.9.1 Dostupnost a požadavky na výkonnostní charakteristiky

Systém jako celek musí být v provozu 7x24x365, povolené jsou pouze plánované odstávky (viz dále).

Aktualizační funkce systémů (výkon státní a veřejné správy) musí být v provozu v pracovní dny od 6:00 do 21:00 nepřetržitě. Odstávky v pracovní době nejsou přípustné. Výpadky budou řešeny formou penalizací, přičemž je požadováno uvedení systému zpět do provozu v souladu s požadavky v příloze č. 1.4 .

Poskytování dat na interaktivních rozhraních musí být v provozu 7x24x365. Výpadky budou penalizovány. Při nutnosti odstavení primárního systému musí být možné přepnutí dotazovacích funkcí do záložního systému nebo zrcadla systému bez výpadku funkčnosti.

Požadované výkonnostní charakteristiky:

- Dostupnost AIS na eGON rozhraních pro dotazy (měsíční hodnocení, režim 7x24, nezahrnují se plánované odstávky) - 99.9%
- Dostupnost AIS na interaktivních rozhraních (měsíční hodnocení, zahrnuje pouze pracovní dny 6:00 - 21:00, nezahrnují se plánované odstávky) - 99.9%
- Maximální přípustná doba odezvy na interaktivním rozhraní editorů v době provozní špičky **) - 3s *)
- Maximální přípustná doba odezvy na interaktivním rozhraní editorů mimo dobu provozní špičky **) - 1s *)
- Maximální přípustná doba odezvy na eGON rozhraních pro 90% dotazů ***) - 1s *)
- Maximální přípustná doba odezvy na eGON rozhraních pro hromadné výdeje - 20s

*) do tohoto času se nezapočítává reakční doba JIPu a ISZR

***) špička je časové období 9:00-11:00 a 13:00-15:00 v pondělí a středu

***) nezahrnuje hromadné dotazy podle AIFO a výdeje připravených výstupů (sestavy apod.)

Počty operací na jednotlivých eGON rozhraních a na interaktivních rozhraních pro editory bude stanoven v době analýzy.

V současnosti jsou v době špičky připojeny cca 3000 editorů a jejich počet vzroste v souvislosti s rolí PČR jako třetího editora.

Na eGON rozhraní pro dotazy z externích systémů je nezbytné počítat se stovkami dotazů za sekundu, přesnější údaj bude stanoven v době analýzy.

3.9.2 Bezpečnost

Systém nezpracovává utajované údaje. Systém zpracovává citlivá osobní data a musí splňovat všechny požadavky zákona č.101/2000 Sb., o ochraně osobních údajů ve znění pozdějších předpisů.

Veškeré přenosy dat po datových linkách vně CVS a ZVS (a mezi CVS a ZVS) musí být chráněny šifrováním.

Musí být proveden bezpečnostní audit systému s ohledem na splnění požadavků zákona č. 365/2000 Sb.

Všechny přístupy uživatelů musí být autentizovány. Všechny externí aplikace přistupující k IS musí být autentizovány (minimálně na úrovni basic autentizace).

Externí aplikace musí předávat identifikaci uživatele, jehož požadavek vyřizují a plně zodpovídají za jeho úplnou a správnou autentizaci.

Všechny servery systému musí být synchronizovány na časový normál Zadavatele umístěný v CMS (aby bylo zajištěno správné datování logů systému a zejména dat v databázích).

Zadavatel požaduje zavedení centrálního „logu“ (syslog), do kterého budou soustředěna všechna chybová, bezpečnostní a havarijní hlášení jednotlivých prvků a komponent (bezpečnostní hlášení jen pokud bezpečnostní projekt nestanoví jinak).

3.9.3 Monitoring pro pracovníky Zadavatele

Monitoring musí být koncipován tak, aby se stal součástí správy incidentů, problémů. Systém musí být navržen tak, aby bylo zajištěno, že:

- Jsou monitorovány všechny důležité parametry IT komponent (zatížení CPU, využití paměti RAM, počet procesů, swap prostory, diskové prostory, databázové prostory, dynamika přírůstků dat a odhad lhůty zaplnění, logy ...).
- Je sledována a kontrolována dostupnost aplikací/služeb a stav jejich zpracování.
- Je monitorován a zobrazován počet provedených dotazů/operací na jednotlivých rozhraních (kontrola, zda je rozhraní ze strany uživatele využíváno).
- Je navržen proces ke zpracování výsledků monitoringu a hlášení výjimek, havarijních stavů a možného vzniku havarijních stavů
- Je navržen proces ke zpracování nestandardních stavů (chyby, vzniklé v aplikacích a programových rozhraních, pokusy o neoprávněný přístup k aplikacím apod.).

Výsledky monitoringu a hlášení výjimek, havarijních stavů a možného vzniku havarijních stavů musí být v reálném čase zobrazováno pracovníkům nepřetržitého dohledu (operátoři) a administrátorům systému. Vznik havarijních stavů musí být dále ohlášen SMS zprávou určeným pracovníkům.

3.9.4 Obnova systému

3.9.4.1 Obnova systému po havárii

V případě havárie primárního systému musí být veškerý provoz převeden do ZVS. Uchazeč zpracuje plán obnovy systému po havárii (DRP).

3.9.4.2 Zálohování

Návrh systému musí zajišťovat minimální pravděpodobnost poškození/zničení dat v důsledku havárie disků.

Data mohou být ukládána pouze na externí disková pole se zajištěním RAID 1, RAID 5 nebo RAID 6 a se zápisem dat do RAM cache. Veškerá data musí být v reálném čase replikována do záložního výpočetního střediska.

Je požadováno vytvoření referenční kopie všech serverů po jejich instalaci a dále v případě podstatných změn v konfiguraci nebo dodaném aplikačním programovém vybavení (cílem je zajištění rychlé a bezproblémové obnovy serveru v případě jeho totální havárie). Veškeré disky v serverech musí být zajištěny zdvojením (RAID 1). Disky musí být vyměnitelné za provozu (hotswappable) aby nemusel být přerušen provoz serveru při havárii disku.

Vytvářejí se denní, týdenní a roční zálohy dat z diskových prostorů serverů. Přednostně se vytvářejí zálohy L0 pokud to rozsah zálohovaných dat umožňuje. Vytvořené zálohy nebo jejich klony se ukládají mimo prostory CVS. U všech záloh databází se musí ověřit jejich čitelnost provedením zpětné obnovy na vyhrazený stroj.

Zálohovací systém musí poskytovat informace o průběhu a výsledku zálohování pracovníkům nepřetržitého dohledu (operátoři) a administrátorům systému.

Musí být možné vytvářet adhoc zálohy podle potřeby („ruční“ záloha).

3.9.4.3 Obnova dat

Systém musí být navržen s dostatečnou redundancí tak, aby obnova dat nebyla za běžné situace potřebná (zajištění disků technologií RAID, spolehlivá disková pole, repliky databází, databázový log, atd.). Pro případ totálního selhání ukládacího systému nebo poškození dat chybou funkcí aplikace zpracuje uchazeč postupy obnovy dat ze zálohy. Požadováno je obnovení „co nejlíže“ k poslednímu funkčnímu stavu (např. obnova databáze z denní zálohy a přihraní dat z logů).

3.9.5 Helpdesk pro koncového uživatele

Funkce Helpdesk pro uživatele systémů bude primárně zajišťovat Zadavatel vlastním týmem pracovníků. Uchazeč musí v dostatečné míře zaškolit pracovníky Helpdesku v řešení základních problémů s aplikací. Uchazeč musí zajistit Helpdesk druhé úrovně a to v pracovní dny od 7:00 do 17:00 hodin.

V době ověřování s uživateli a v prvním období jednoho měsíce po spuštění AIS3 bude nutné zajistit zvýšenou podporu jak koncových uživatelů, tak pracovníků Helpdesku ze strany uchazeče. V tomto období se předpokládá přímá účast pracovníků uchazeče na pracovišti Helpdesku MV.

3.9.6 Požadavky na servis zařízení a servis aplikace

V záruční době zajišťuje Uchazeč servis veškerého HW, systémového SW a aplikačního programového vybavení.

Požadavky na rozsah technické podpory dodaného HW a dodaného systémového SW a aplikačního SW jsou uvedeny v Příloze č. 1.4.,soubor:

„ZD_AISEO_Priloha_1_4_Specifikace_podpory.doc“.

3.9.7 Správa incidentů, problémů

Pro zajištění řešení havarijních a mimořádných stavů zpracuje uchazeč postupy (metodiku) jejich řešení.

Bezprostřední dohled nad chodem AIS3 zajišťují pracovní týmy Zadavatele (administrátoři a služba nepřetržitého dohledu). Uchazeč zajišťuje podporu L2. Metodika musí stanovit úkoly a

povinnosti jednotlivých týmů, pravidla jejich spolupráce a součinnosti a pravidla eskalace incidentů a problémů.

3.9.8 Životní cyklus systému

Pro zajištění životního cyklu systému zapracuje uchazeč návrh na správu změn a správu verzí, jejich nasazení a hodnocení kvality.

4 Harmonogram:

4.1 Hlavní milníky projektu

I. Etapa – návrh AIS3

T_0	Podpis smlouvy,
$T_1 = T_0 + 60$	Analýza požadavků na AIS3, analýza datových struktur a vazeb, vazby na ex. systémy, komunikace mezi systémy, globální návrh AIS3, včetně akceptace
$T_2 = T_0 + 90$	Detailní návrh AIS3, návrhy datových modelů, návrh eGon funkcí,
$T_{2A} = T_2 + 10$	Akceptace DNS AIS3
$T_3 = T_0 + 120$	Drátěný model AIS3 („wireframe“), analýza dat, návrh kontrolních mechanismů a postupů převodu dat do AIS3,
$T_{3A} = T_3 + 10$	Akceptace drátěného modelu AIS3, analýzy dat, návrhu kontrolních mechanismů a postupů převodu dat do AIS3,
$T_4 = T_0 + 150$	Podpůrné procedury pro kontrolu a převod dat,
$T_{4A} = T_4 + 10$	Akceptace podpůrných procedur pro kontrolu a převod dat,

II. Etapa – implementace AIS3

$T_5 = T_2 + 150$	Implementace technické infrastruktury, napojení do komunikační infrastruktury provozní, testovací, školící)
$T_6 = T_3 + 120$	Instalace APV, školení uživatelů
$T_7 = T_6 + 30$	Ověření funkčnosti AIS3 s vybranou skupinou uživatelů a ISZR,
$T_8 = T_7 + 30$	Předání díla AIS3, předání finální dokumentace
$T_9 = T_8 + 30$	Akceptace AIS3,
$T_{10} = T_9 + 30$	Finální naplnění dat AIS3 a uvedení AIS3 do rutinního provozu

5 Charakteristika realizace

5.1 I. Etapa – návrh AIS3

V rámci realizace budou zpracovány analytické dokumenty a vytvořen návrh jednotlivých agendových informačních systémů.

Zhotovitel provede analýzu požadavků zadavatele, právního rámce, technologického prostředí zadavatele a stávajícího systému se zaměřením na datové struktury a vazbu na okolní systémy. Na základě provedené analýzy bude zpracován globální návrh agendového informačního systému evidence obyvatel AIS EO, agendového informačního systému evidence občanských průkazů AIS EOP a agendového informačního systému evidence cestovních dokladů AIS ECD včetně podpůrných systémů. Globální návrh bude obsahovat rozčlenění na základní komponenty systému, dále procesní, funkční a datový model, charakteristiky uživatelských rolí, základní grafický koncept, návrh technické infrastruktury, bezpečnostní projekt, vše se zřetelem na vazby na ISZR, ROB a další základní registry a JIP a návrh eGon funkcí a spolupráce s ISZR. Globální návrh bude podléhat akceptaci ze strany Zadavatele.

Na základě schválených globálních návrhů budou zpracovány Detailní návrhy jednotlivých agendových systémů zahrnující datový model, návrh obrazovek, reportů, návrh přístupových práv ve vazbě na organizaci agendy, detailní návrh architektury agendových systémů včetně podpůrných systémů.

Detailní návrh musí rovněž obsahovat všechny požadavky na vytvoření stavebně provozních podmínek pro zařízení navrhované Zadavatelem (jako je např. energetika, klimatizace, požadavky na síť, stavební připravenost). Dále je součástí návrhu způsob získání testovacích dat, návrh testovacích postupů, návrh bezpečnostních opatření a rozpracované GUI. Detailní návrh bude podléhat akceptaci ze strany Zadavatele.

Na základě schváleného Detailního návrhu AIS3 bude zpracován drátěný model umožňující přechody mezi jednotlivými obrazovkami. Návrh Drátěného modelu bude podléhat akceptaci ze strany Zadavatele.

Součástí I. Etapy je provedení analýzy stávajícího datového modelu, návrh kontrol dat a způsobu a postupu migrace dat. Návrh podléhá akceptaci ze strany Zadavatele.

Na základě schválených postupů budou připraveny kontrolní procedury a procedury podporující čištění dat.

Výstupy:

Dokumenty:

Analýza požadavků zadavatele, právního rámce a stávajícího stavu

Globální návrh AIS3

Analýza rizik a návrhu opatření k jejich eliminaci

Bezpečnostní projekt

Detailní návrh AIS3

Návrh bezpečnostních opatření

Analýza stávajícího datového modelu, návrh kontrol dat, způsobu a postupu migrace dat

Návrh postupu testování AIS3

Návrh obrazovek a grafického rozhraní

Drátěný model AIS3

Procedury

Procedury umožňující kontrolu dat a migraci dat

5.2 II. Etapa – implementace AIS3

II. Etapa část I zahrnuje dodávku a instalaci serverů a systémového software v souladu s detailním návrhem technické infrastruktury v prostředí Zadavatele.

Výstupy:

Stroje a zařízení:

Dodávka technické infrastruktury

Software:

Dodávka systémového SW

Dokumentace

Technická dokumentace k dodanému systémovému SW a HW

Protokol o instalaci technické infrastruktury (HW a systémový SW)

Protokol o školení administrátorů systému

Protokol o provedeném zaškolení obsluhy

II. Etapa část II zahrnuje dodávku aplikačního programového vybavení pro AIS3, jeho instalaci, spolupráci při čištění a kontrole dat a migraci dat ze stávajících zdrojů do AIS3. Dále zahrnuje integraci AIS3 s informačním systémem základních registrů, ověření funkčnosti rozhraní vůči systémům základních registrů, spuštění eGON služeb.

Součástí etapy je pilotní ověření provozu AIS3 s vybranými úřady a základními registry a základní zaškolení administrátorů systému a dalšího technického personálu.

Součástí předávaných výstupů je i návrh na zajištění rutinního provozu AIS3, který mimo jiné bude obsahovat metodiky testování a nasazování nových verzí, postupy řešení havarijních a mimořádných stavů. Návrh musí stanovit organizační zajištění provozu, úkoly a povinnosti jednotlivých týmů, pravidla jejich spolupráce a součinnosti, pravidla eskalace incidentů a problémů.

Výstupy:

Software:

Aplikační programové vybavení AIS3

Dokumentace

Detailní návrh rozhraní AIS3, detailní návrh služeb eGon služeb

Protokol o testování AIS3

Zpráva o průběhu pilotního provozu AIS3

Zpráva o průběhu čištění dat

Návrh na zajištění provozu AIS3

Dokumentace AIS3 (systémová, bezpečnostní a uživatelská) a provozní dokumentace AIS3

Protokol o zaškolení administrátorů, ostatního technického personálu, školitelů uživatelů

Popis technické podpory AIS3 v období záruční doby

Programové aplikační vybavení AIS3

Protokol o zahájení rutinního provozu AIS3

Protokol o instalaci aplikačního programového vybavení

Protokol o migraci dat

Protokol o zahájení provozu AIS3