GLOBÁLNÍ ARCHITEKTURA ZÁKLADNÍCH REGISTRŮ

Datum vzniku:	7.4.2014
Počet stran:	46
Verze	1.0
Zodpovídá:	MV ČR, útvar hlavního architekta eGovernment

OBSAH

Seznam změn			
Datum	**Verze**	**Popis změny**	**Změněno kým**
20.6.2009	1.0	Založení dokumentu	Petr Tiller
24.6.2009	1.0	Uvolnění dokumentu	Ondřej Hůrka

1. Funkční dekompozice na úroveň jednotlivých systémů

1.1. Základní východiska

Informační systém základních registrů (ISZR) je definován zadavatelem jako referenční rozhraní pro přístup k základním registrům. ISZR poskytuje komplexní eGON služby oprávněným subjektům nad základními registry s ohledem na jejich aktuální oprávnění v registru práv a povinností.

1.2. Cíle

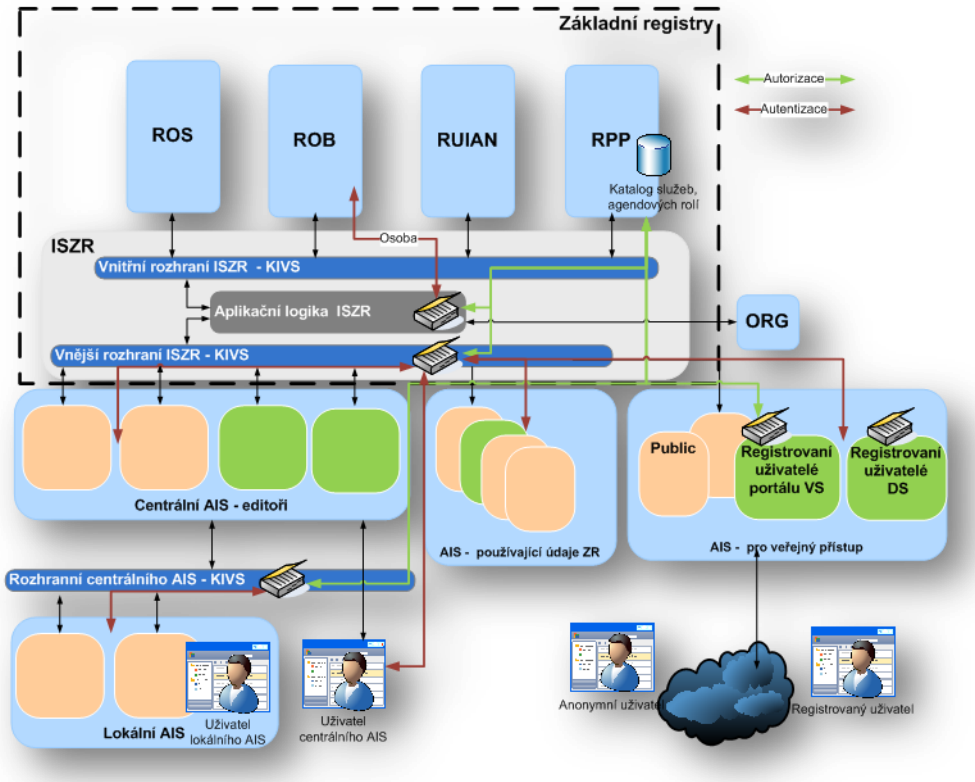
Cílem návrhu funkční dekompozice je popis funkcí informačního systému ZR a jejich návaznosti. Popisované funkce jsou obrazem business procesů systému Základních registrů, které vymezuje:

- Zákon č. 111/2009 sb. o základních registrech
- Koncepce stanovená Operační strategií Základních registrů.

1.3. Souhrnný popis

1.3.1. Globální funkcionalita systému Základních registrů

Globální funkcionalita komponent systému základních registrů je uvedena na následujícím obrázku



Systém základních registrů se skládá z:

- **Jednotlivé základní registry –** obsahují infrastrukturu pro uchovávání dat a komunikují s vnitřním rozhranním ISZR. Infrastruktura pro jednotlivé základní registry bude umístěna v různých fyzických lokalitách.

- **Vnitřní rozhranní ISZR –** slouží k interní bezpečné komunikaci mezi jednotlivými komponentami systému základních registrů. Předpokladem je, že toto komunikační rozhraní je nedostupné mimo systém základních registrů. Poskytuje základní služby pro komunikaci logiky zpracování ISZR s jednotlivými základními registry a ORG.
- **Aplikační logika ISZR –** tato komponenta zajišťuje výkonnou část ISZR. Z registru práv a povinností přebírá matice oprávnění, udržuje sadu povolených služeb a složených funkcí. Zajišťuje správu front zpráv. Zprostředkuje přepočet AIFO pro jednotlivé agendy prostřednictvím ORG.
- **Vnější rozhranní ISZR –** slouží k publikaci služeb základních registrů. Provádí primárně řízení vstupních a výstupních front, publikaci katalogu služeb základních registrů a předávání požadavků aplikační logice ISZR. Představuje základní bezpečnostní perimetr a jedinou spojnici mezi systémem základních registrů a vnějším světem.
- **Centrální AIS (editoři) –** provádějí editační služby referenčních údajů. Zajišťují proces validace a přípravy referenčních údajů. Do systému základních registrů zasílají **pouze** platné údaje. Používají služby systému základních registrů pro čtení referenčních údajů. Mohou nabízet své služby, které poskytují údaje neuchovávané v základních registrech (historická data, atributy subjektů a objektů mimo rozsah udržovaný v základních registrech).
- **Lokální AIS –** poskytují uživatelské prostředí pro uživatele editorů základních registrů pro přípravu referenčních údajů. Se systémem základních registrů komunikují prostřednictvím centrálních AIS, kterým předávají údaje pro zápis do základních registrů nebo od nich přebírají údaje ze systému základních registrů.
- **Ostatní AIS –** používají služby systému základních registrů pro čtení referenčních údajů. Mohou nabízet své služby, které poskytují údaje neuchovávané v základních registrech (historická data, atributy subjektů a objektů mimo rozsah udržovaný v základních registrech).
- **AIS pro veřejný přístup –** používají omezenou množinu služeb systému základních registrů. Využívají pouze čtení referenčních údajů i nereferenčních kopií dat ze základních registrů.

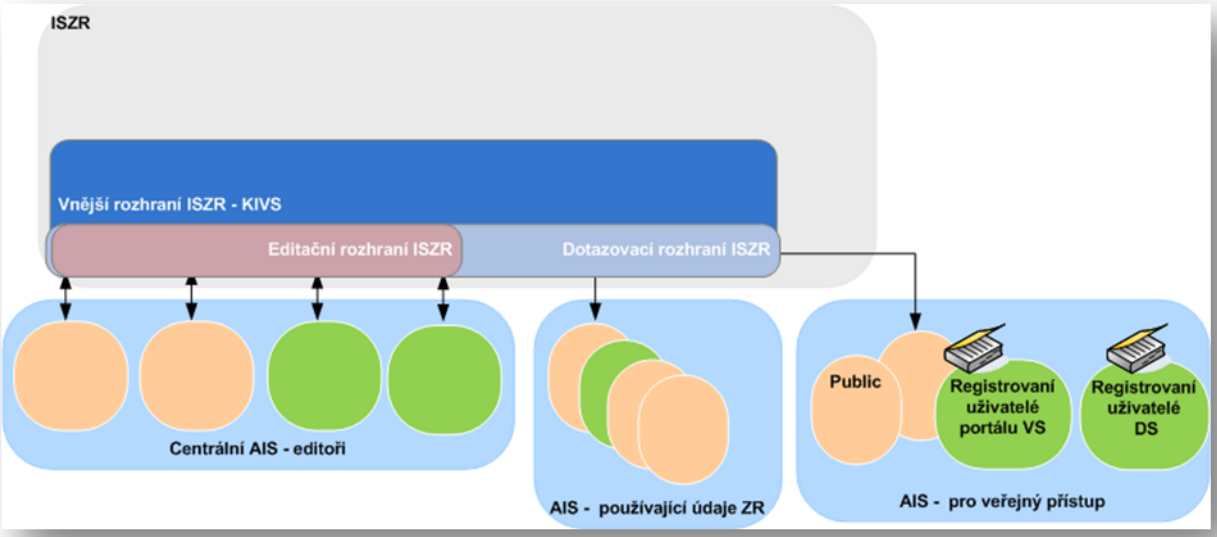
1.3.2. Služby vnějšího komunikačního rozhraní

Vnější komunikační rozhraní je jediným přístupovým bodem pro externí subjekty pro přístup ke službám základních registrů. Toto rozhraní je realizováno na technologii Komunikační infrastruktury veřejné správy (KIVS).

Z důvodu přehlednosti lze rozhraní rozčlenit a jeho jednotlivé části označit jako Editační rozhraní ISZR a Dotazovací rozhraní ISZR. Toto členění je pouze logické a technologické. Centrální AIS v roli editora budou připojeny současně k editačnímu i dotazovacímu rozhraní.

1.3.2.1. Komunikace Centrálních AIS – editoři s ISZR

Tato kapitola popisuje výhradně komunikaci a komunikační rozhraní mezi Centrálními AIS v roli editora směrem k editačnímu rozhraní ISZR. Lze tedy říci, že tato kapitola popisuje podmnožinu funkcí implementovaných v rámci celého rozhraní ISZR, speciálně určenou pro komunikaci vyvolanou za účelem editace údajů v ZR. Pokud se dále v této kapitole mluví o komunikačním rozhraní ISZR, je tím míněno právě toto Editační rozhraní ISZR.



Z aplikačního hlediska je žádoucí, aby komunikační rozhraní mezi Centrálními AIS zabezpečilo pro roli editora údajů několik základních vlastností, které jsou klíčové pro správné fungování systému. Tyto vlastnosti lze charakterizovat následovně:

- transakčnost,
- perzistence dat,
- perzistence spojení.

Transakčnost požadavků na změny v ZR, které jsou odesílány z AIS, je požadována na úrovni vnějšího komunikačního rozhranní. V tomto smyslu je ukončením transakce potvrzení příjmu celé zprávy v ISZR.

Následné zpracování (provedení vlastního zápisu do základních registrů) je oddělená transakce, o jejímž výsledku je spolu s ID požadavku informován AIS, který požadavek zadal. AIS je povinen zajistit spárování této informace na původní požadavek k editaci.

Dále je třeba zajistit perzistenci dat odeslaných v rámci požadavků na změny, které jsou z AIS odeslány na komunikační sběrnici ISZR a následně je potvrzeno jejich odeslání a jejich přijetí na straně komunikačního rozhraní ISZR.

Pod pojmem perzistence dat je v tomto kontextu míněna definice životnosti těchto dat na komunikační sběrnici ISZR. Tato definice vychází ze základní koncepce ZR, která zjednodušeně formulováno, předpokládá jedinečnost provedené editace a její provedení.

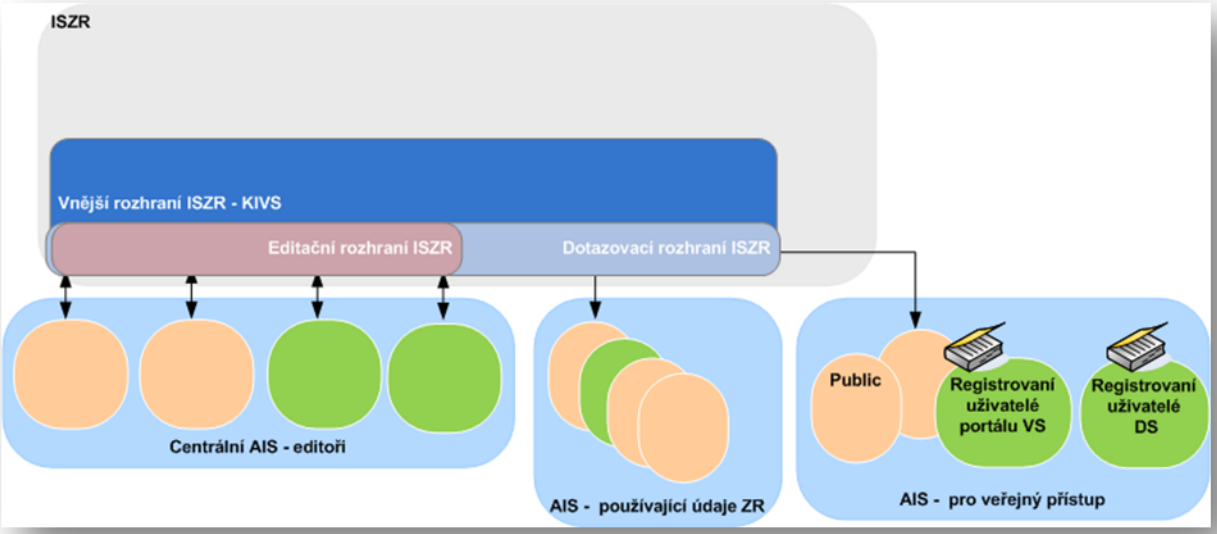
U požadavků na editaci, které byly doručeny na komunikační sběrnici, je třeba zajistit, aby jejich životnost byla ukončena pouze zpracováním přijatých dat, tedy aby nemohlo dojít k jejich destrukci na základě výpadku kteréhokoliv spolupracujícího systému, včetně výpadku systému komunikační sběrnice ISZR v okamžiku, kdy jsou data na této sběrnici zpracovávána.

Z pohledu AIS je vhodné, pokud bude komunikační rozhraní ISZR řešeno takovým způsobem, aby jednou vytvořené spojení s komunikačním rozhraním ISZR, mohlo po provedeném ověření setrvat otevřené po dobu, po kterou bude komunikující AIS toto spojení potřebovat.

V rámci globální architektury je tedy třeba pro implementaci logiky rozhraní ISZR, realizující Editační rozhraní ISZR, zvolit takovou technologii, která výše uvedené podmínky splňuje. V praxi to znamená nasazení middleware technologií typu MOM (Message Oriented Middleware).

1.3.2.2. Komunikace AIS používajících údaje ZR se systémem ISZR

Tato kapitola popisuje výhradně komunikaci a komunikační rozhraní mezi AIS v roli konzumenta informací uložených v ZR s využitím systému ISZR. Lze tedy říci, že tato kapitola popisuje podmnožinu funkcí implementovaných v rámci celého rozhraní ISZR, speciálně určenou pro komunikaci vyvolanou za účelem dotazování údajů uložených v ZR. Pokud se dále v této kapitole mluví o komunikačním rozhraní ISZR, je tím míněno právě toto Dotazovací rozhraní ISZR.



Z aplikačního hlediska je žádoucí, aby komunikační rozhraní pro dotazující se AIS zabezpečilo několik základních vlastností, které jsou klíčové pro správné fungování systému. Tyto vlastnosti lze charakterizovat následovně:

- interoperabilita,
- dostupnost,
- rychlost.

Dotazovací rozhraní ISZR bude využíváno rozsáhlou množinou různých AIS. Z technologického pohledu půjde o existující aplikace postavené na různých platformách, tak i o aplikace budoucí, u kterých nelze implementační platformu předem definovat.

Z výše uvedené technologické nejednoznačnosti přistupujících AIS je třeba dotazovací rozhraní navrhnout způsobem, který bude z pohledu přistupujícího systému v maximální míře postaven na obecných technologických standardech pro výměnu dat, tak, aby byla zajištěna maximální interoperabilita různých technologických platforem.

Jak již bylo uvedeno výše, bude dotazovací rozhraní ISZR využíváno rozsáhlou množinou různých AIS. Z provozního pohledu budou jednotlivé AIS umístěny v mnoha různých lokalitách a využívány v prakticky neomezeném časovém režimu. Z toho důvodu je třeba klást důraz na zajištění dostatečné dostupnosti rozhraní.

Účelem rozboru dostupnosti rozhraní v této kapitole není způsob zabezpečení fyzického spojení a komunikace mezi AIS a rozhraním ISZR, ale pouze dostupnost rozhraní jako takového.

Z pohledu fungování infrastruktury státu hraje dostupnost dotazovacího rozhraní klíčovou roli. Funkčnost, resp. dostupnost tohoto rozhraní při přístupu k obecným údajům uloženým v ZR je jednou ze základních myšlenek celého projektu ZR. Bez zaručené dostupnosti rozhraní ISZR nelze realizovat myšlenku sdílení údajů v ZR.

Při podrobnějším pohledu na pojem dostupnosti lze rozlišit jednak dostupnost z pohledu spolehlivosti rozhraní a jednak dostupnost z pohledu kapacity rozhraní. Přestože tyto dva pohledy spolu úzce souvisí, je vhodné je při návrhu globální architektury definovat jednotlivě, aby bylo zřejmé, jaké požadavky musí splnit následný konkrétní návrh jak po stránce fyzického tak i logického návrhu.

Při návrhu architektury řešení je tedy třeba pro zajištění:

- **spolehlivosti rozhraní** – poskytnout transparentní vstupní logický komunikační bod, který bude ošetřovat a překlenovat situace provozních a technických výpadků;
- **kapacita rozhraní** – poskytnout transparentní vstupní logický komunikační bod, který bude schopen ošetřovat jak současný předpokládaný, tak v budoucnu rostoucí počet požadavků na rozhraní s dostatečnou rezervou.

Dotazovací rozhraní systému ISZR bude velkou měrou využíváno na procesy v režimu „online“. Pakliže má systém ZR přinést v tomto směru maximální přínos, je třeba zajistit, aby celý systém dokázal zajistit definovanou, v praxi co nejkratší, dobu odezvy. Z tohoto globálního požadavku tedy plynou i požadavky na jednotlivé subsystémy systému ZR na zajištění definované, co nejkratší, doby odezvy, tedy tento požadavek je kladen i na systém ISZR.

Výchozím předpokladem dále uváděných technologií je komunikace mezi externími systémy a agendovými systémy prostřednictvím webových služeb. Webové služby (WS) jsou definovány skupinou W3C (World Wide Web Consotium) – mezinárodní standardizační organizací pro World Wide Web.

Webové služby jako takové jsou definovány jako „softwarový systém navržený pro podporu vzájemné sítové spolupráce počítačů“. Síťová spolupráce je realizována prostřednictvím HTTP protokolu.

Ke standardům webových služeb jsou doplněny další standardy rozšiřující možnosti webových služeb. Tyto specifikace jsou označovány jako WS-*. V souvislosti s návrhem komunikace s agentovými systémy lze uvést následující specifikace:

Kategorie	Protokol
Výměna zpráv (Messaging)	SOAP, WS-Addressing, MTOM
Metadata	WSDL, WS-MetadataExchange, WS-Policy
Bezpečnost (Security)	WS-Security, WS-SecureConversation, WS-Trust
Důvěryhodnoct (Reliability)	WS-ReliableMessaging
Transakce	WS-Coordination, WS-AtomicTransaction

1.3.2.3. Komunikace AIS používajících údaje jiného AIS

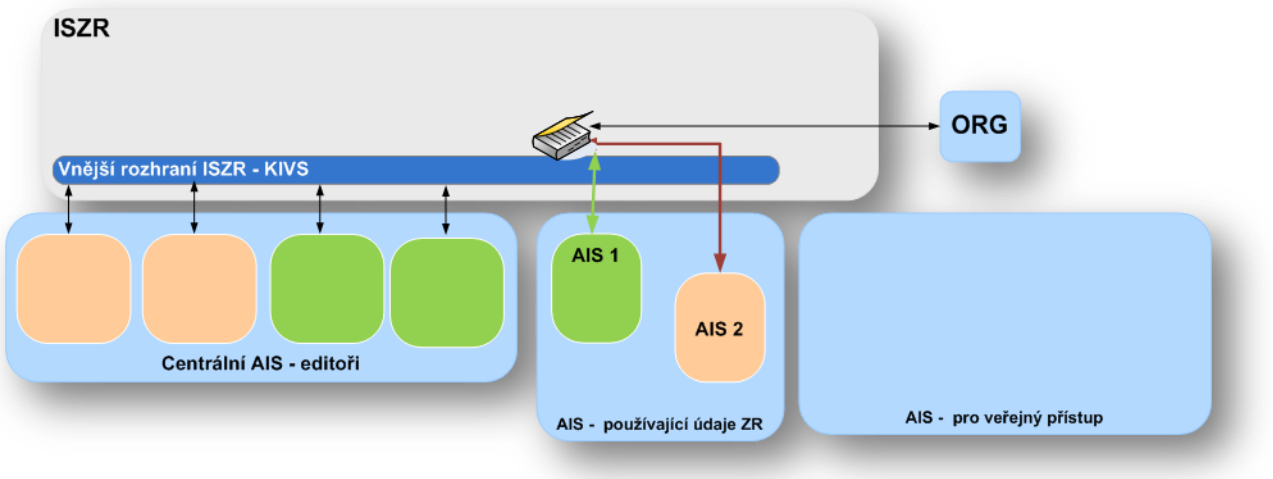
Komunikace AIS-AIS je speciálním případem komunikace s ISZR. Jedná se o případ, kdy údaj, který AIS1 potřebuje ke své činnosti, není uložen přímo v základních registrech (není tedy referenční), ale v jiném informačním systému AIS2 orgánu veřejné moci. ISZR zde mimo ověření oprávnění pro využití služby, která poskytuje přístup k dané informaci, zprostředkovává zabezpečenou komunikaci mezi AIS1 a AIS2.

Z povahy procesu zde ISZR nemůže garantovat odezvu na dotaz, protože dostupnost AIS2 je mimo odpovědnost provozovatele ISZR. ISZR může jen garantovat včasné doručení dotazu na svém výstupu (vstupní frontě AIS2) a včasné doručení odpovědi po obdržení odpovědi na dotaz z AIS2. ISZR není zodpovědný za správnost informací v odpovědi. ISZR uchovává informaci o dotazu/odpovědi stejným způsobem, jakým loguje dotazy do ZR.

Nutnost komunikace AIS-AIS prostřednictvím ZR je dána především faktem, že v jednotlivých agendách jsou osoby vedeny pod specifickým AIFO. Převod jednotlivých AIFO pro různé AIS může provádět pouze ORG prostřednictvím ISZR.

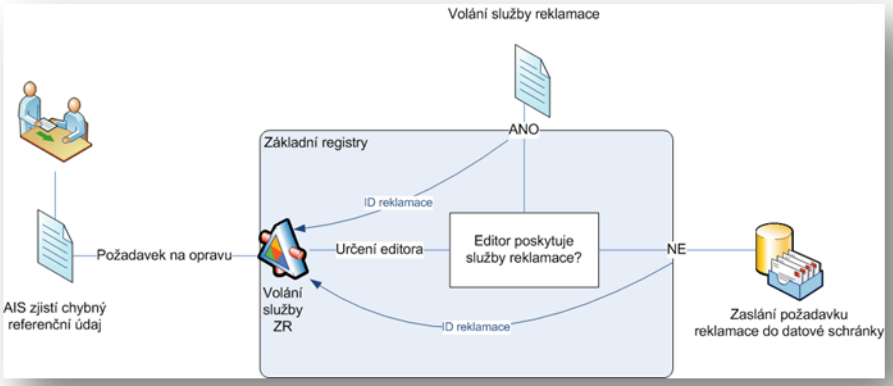
Příklady komunikace AIS-AIS:

- Čtení údaje
  - údaje obsažené v AIS2, které nejsou obsaženy v ZR
- Dotaz na historii údaje
  - historie údaje, včetně údajů obsažených v ZR, u nichž je AIS2 editorem
- Změny údajů



1.3.2.4. Proces reklamace (zpochybnění referenčního údaje)

Jiným případem, kdy spolu komunikují dva AIS mezi s sebou prostřednictvím ISZR je scénář „reklamace“ – zpochybnění referenčního údaje, kterého je AIS2 příslušným editorem. Pokud AIS2 bude mít implementovánu službu „reklamace“, bude proces zpochybnění referenčního údaje realizován pomocí volání této služby. V opačném případě bude k vyvolání procesu opravy použita datová schránka příslušná k AIS2. Tento proces zpochybnění údajů lze aplikovat i na údaje, které AIS2 uchovává nad rámec referenčních údajů.



1.3.2.5. Vstupní a výstupní fronty

Tyto fronty slouží jako komunikační kanály pro Agendové informační systémy (AIS) pro předávní požadavků na základní registry nebo jiné eGON služby. Každý AIS registrovaný pro komunikaci se systémem základních registrů má přidělenu jednu vstupní a jednu výstupní frontu.

Pro každý AIS oprávněný ke komunikaci budou vytvářeny virtuální primární vstupní/výstupní kanály (fronty), pomocí kterých budou od tohoto subjektu přijímány požadavky na služby základních registrů a následně předávány zpět výsledky těchto služeb.

Řízení vstupních a výstupních front bude splňovat následující kriteria:

- Fronty příslušející různým subjektům musí být logicky odděleny tak, aby nemohlo dojít ke kompromitaci údajů.
- Každý požadavek přijatý ve vstupní frontě je označen vnitřním jednoznačným identifikátorem Universal Unique Identifier (**UUID**) – 128 bitový identifikátor.
- Každý požadavek přijatý ve vstupní frontě je označen vnitřní časovou značkou pro sledování úrovně poskytovaných služeb.
- Je umožněna priorizace požadavků ze strany žadatele.
- Je umožněna priorizace požadavků ze strany ISZR.

Vnější komunikační rozhraní publikuje seznam služeb, které jsou poskytovány systémem základních registrů.

Na vstupní a výstupní frontu může být AIS připojen definovaným počtem vláken (paralelně zpracovávaných). Počet povolených vláken je součástí registračního postupu.

Zpracování jednotlivých požadavků (zpráv) je z principu asynchronní a pracuje podle následujícího schématu:

- AIS naváže komunikaci se vstupní a výstupní frontou. Po počáteční autentizaci je kanál otevřen a může být použit pro zasílání požadavků a čtení odpovědí.
- V otevřeném kanálu vstupní fronty je zaslán požadavek na využití služeb základních registrů. Formát požadavku je popsán v odpovídající kapitole. AIS přidělí požadavku své jednoznačné identifikační číslo. Zaslání požadavku je ukončená transakce.

- V otevřeném kanálu výstupní fronty jsou čteny zprávy systému základních registrů. Tyto zprávy mohou být různého typu (odpovědi na požadavky AIS, informační zprávy, požadavky pocházející z jiného AIS)

Pro omezenou množinu eGON služeb poskytovaných jednotlivým agendovým systémům budou k dispozici synchronní alternativy služby. Pro tyto služby bude vytvořena jedna logická vstupně/výstupní cesta. Synchronní služby budou omezeny pouze na primitivní dotazy (viz katalog služeb), jejichž doba odezvy je v rámci SLA malá. Konkrétní hodnota tohoto omezení bude určena ve spolupráci s architekty jednotlivých základních registrů při dopracování návrhu architektury. Pokud požadavek nebude vyřízen do omezeného času, pak celá transakce bude bez náhrady zrušena. AIS pak může buď použít asynchronní volání eGON služby nebo se pokusí o opětné volání synchronní alternativy.

1.3.3. Služby interního komunikačního rozhraní

Interní komunikační rozhraní slouží pro komunikaci mezi jednotlivými registry (ROB, ROS, RUIAN,RPP) a ISZR. Poskytuje také komunikaci s převodníkem identifikátorů (ORG). Základním předpokladem je nedostupnost tohoto rozhraní mimo systém základních registrů. Komunikace na interním komunikačním rozhraní probíhá v otevřené formě a slouží k interní bezpečné komunikaci mezi jednotlivými komponentami systému základních registrů. Toto komunikační rozhraní musí zajistit konektivitu jednotlivých komponent systému základních registrů na požadované úrovni. Současně musí být prováděn kontinuální monitoring z hledisek:

- **Provozní** – všechny komponenty komunikačního rozhraní jsou dostupné. Jsou sbírána data pro stanovení metrik a stanovení úrovně dodávaných služeb.
- **Bezpečností** – monitoring oprávněnosti komunikace. Detekce pokusů o obejití či narušení bezpečnostních pravidel.

Interní komunikační rozhraní pracuje s citlivými daty, a proto musí být fyzicky odpojeno od veřejných informačních systémů a nesmí být žádným způsobem dostupné mimo systém základních registrů.

1.3.3.1. Servisní rozhraní

Správa základních registrů zřízená dle zákona musí provádět dohled a správu informačního systému základních registrů. Pro tyto účely slouží servisní rozhraní, které pro jednotlivé komponenty poskytuje:

- **Události (events)** – údaje o provozním stavu jednotlivých komponent informačního systému základních registrů a změnách těchto stavů.
- **Metriky** – údaje o provozních údajích jednotlivých částí informačního systému základních registrů a číselné vyjádření jednotlivých provozních parametrů.
- **Varování (warnings)** – údaje o kritických stavech jednotlivých komponent, které mohou mít vliv na úroveň dodávaných služeb.
- **Logy** – záznamy o transakcích prováděných v rámci informačního systému základních registrů.
- **Publikace aplikací** – aplikace pro správu informačního systému základních registrů a speciální aplikace (AIS) pro správu jednotlivých základních registrů, pokud budou těmito registry poskytovány. Tyto aplikace jsou provozovány v rámci jednotlivých registrů. Na servisním rozhraní jsou pouze publikovány.
- **Řízení přístupu** – Univerzální správa identit v rámci informačního systému základních registrů. Tato správa identit bude cílově navázána na informace o osobách v registru ROB. Autentizační mechanismus bude

poskytován jak pro přístup k informačnímu systému základních registrů, tak pro autentizační mechanismy v AIS jednotlivých agend.

Servisní rozhraní poskytuje správě základních registrů tyto údaje jak z hlediska provozního, tak z hlediska bezpečnostního. Správa základních registrů vytváří na základě získaných informací reporty o provozu a stavu celého informačního systému základních registrů a úrovni poskytovaných eGON služeb.

Jednotlivé základní registry budu do tohoto sytému poskytovat údaje o stavu základního registru a úrovni poskytovaných interních služeb základních registrů.

Servisní rozhraní neslouží k přístupu k obsahu referenčních údajů obsažených v základních registrech.

1.3.3.2. Správa identit a jejich oprávnění

Z hlediska informačního systému základních registrů je nutná správa identit a jejich oprávnění ve dvou oblastech.

Autentizace pro využití eGON služeb – udržuje, v souladu se zákonem č. 111/2009 sb. o základních registrech, autentizační údaje osob pro účely využívání eGON služeb.

Přístup k servisnímu rozhraní – určuje osoby/role, které mají oprávnění k přístupu k servisnímu rozhraní, a definuje rozsah operací, které může identita provádět. Tyto identity nemají přístup k obsahu referenčních údajů v základních registrech. Na základě oprávnění (autorizace) pak uživatel získá přístup k jednotlivým publikovaným aplikacím pro správu informačního systému základních registrů a případně konkrétních registrů.

1.3.3.3. Bezpečnostní vrstva

Každá komponenta informačního systému základních registrů musí poskytovat bezpečnostní údaje o provozu. Jsou zaznamenávány úspěšné i neúspěšné pokusy o přístup k eGON službám ISZR, které jsou poskytovány na externím i interním komunikačním rozhraní ISZR.

Tato vrstva kontinuálně vyhodnocuje a detekuje stavy narušující bezpečnost celého ISZR. Současně přebírá bezpečnostní informace z jednotlivých základních registrů. Je tedy centrálním bodem pro vyhodnocení celkového bezpečnostního stavu základních registrů.

1.3.4. požadavky na KIVS

KIVS je využíván jako komunikační rozhranní. KIVS musí zajistit:

1. **Důvěrnost dat** (definice z ČSN 13335: zajištění, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni) – přenášená data jsou chráněna před prozrazením v důsledku chyb i úmyslných akcí (např. odposlech, vydávání se za oprávněnou stanu komunikace).
2. **Dostupnost služeb** (zajištění, že informace/služba je pro oprávněné uživatele přístupná v okamžiku její potřeby) – parametry dostupnosti a spolehlivosti sítě odpovídající požadavkům na dostupnost a spolehlivost systémů a jejich služeb, které budou stanoveny

Pro zajištění autentizace pomocí certifikátů je nutné brát v úvahu stanovisko Ministerstva vnitra: "Kvalifikovaní poskytovatelé certifikačních služeb ukončí vydávání kvalifikovaných certifikátů s algoritmem SHA-1 do 31. 12. 2009. Od 1. 1. 2010 budou tito poskytovatelé vydávat kvalifikované certifikáty podporující některý z algoritmů SHA-2. Zároveň je od uvedeného data stanovena minimální přípustná délka kryptografického klíče pro algoritmus RSA na 2048 bitů.”

Požadavek na nepopíratelnost původu dat je nutné vnímat rozšířeně jak o schopnost rozhodnout, jestli určitá data jsou nebo nejsou shodná s daty, která byla systémem odeslána, přímo na úrovni sítě a o reakci na případnou nekorektnost přímo na síťové úrovni. Současně vzhledem k provozování systémů různými organizacemi je potřebné, aby existovaly mechanismy k řešení případných sporů o odpovědnost za (ne)provedené změny, poskytnuté informace (referenční údaje) apod.


evropský
sociální
fond v ČR
EVROPSKÁ UNIE
OPERAČNÍ PROGRAM
LIDSKÉ ZDROJE
A ZAMĚSTNANOST
PODPORUJEME
VAŠI BUDOUCNOST
www.esfcr.cz

2. Datový obsah služeb/ Datová architektura

2.1. Základní východiska

Návrh datové architektury systému základních registrů vychází z podkladových materiálů přiložených k soutěžním podmínkám.

Informační systém základních registrů je definován zadavatelem jako referenční rozhraní pro přístup k základním registrům. ISZR poskytuje oprávněným subjektům komplexní služby nad základními registry s ohledem na jejich oprávnění v registru práv a povinností.

ISZR úzce spolupracuje s řídící částí RPP, kdy lze přirovnat ISZR ke směrovači s logikou Access listů uloženou v RPP (především se jedná o matici oprávnění k přístupu do základních registrů).

2.2. Cíle

Cílem návrhu datové architektury je návrh datového modelu ZR respektující:

- Aspekty zákona č.111/2009 sb. o základních registrech
- Koncepci stanovenou Operační strategií Základních registrů.

Architektura návrhu musí pružně podporovat budoucí požadavky související se změnami zákonů, úprav v architektuře základních registrů a agendových informačních systémů.

2.3. Souhrnný popis

Data obsažená v dotazech a odpovědích ze základních registrů ISZR neuchovává, pouze zajišťuje jejich bezpečné a zaručené doručení adresátovi. ISZR uchovává záznamy o jednotlivých transakcích, tak aby byl naplněn požadavek zákona na audit systému.

Interní data ISZR lze rozdělit na:

- **provozní data** = data sloužící k rychlému a bezpečnému doručení zpráv,
- **reportovací data** = data sloužící pro dohled nad ISZR, pro reporting stavu systému a pro audit fungování ISZR.

ISZR sám neobsahuje a neposkytuje referenční údaje, pouze z RPP pro svoje provozní potřeby využívá některé údaje. Jedná se především o:

1. Seznam služeb z Katalogu služeb.
2. Seznam kódů agend.
3. Seznam rolí.
4. Matice oprávnění k přístupu a zápisu do základních registrů.

Reportovací data slouží pro správu a dohled ISZR z hlediska:

- dostupnosti,
- výkonu,
- bezpečnosti.

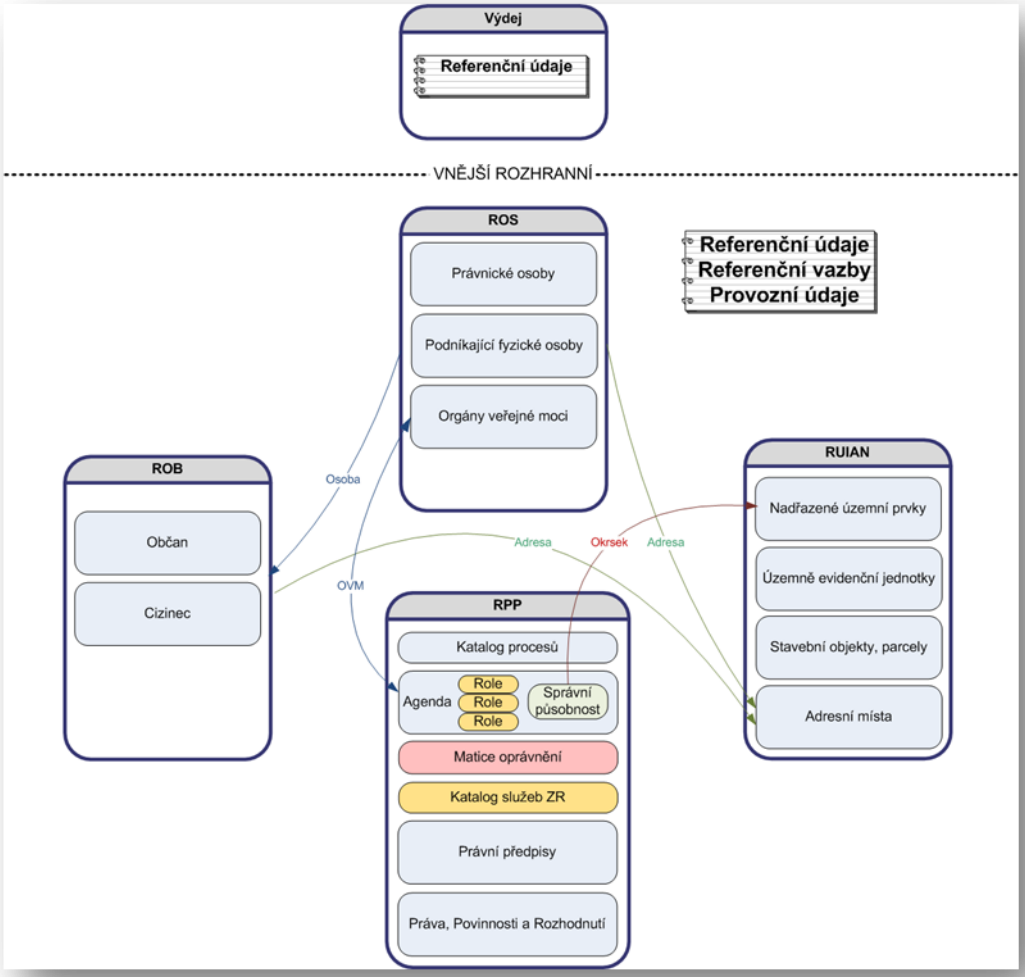
Tato data jsou logována a slouží potřebám řízení úrovně služeb (Service Level Management), pro zlepšování kvality a řešení incidentů a problémů (dle ITIL terminologie).

Dále ISZR uchovává log svých transakcí (hlaviček dotazů a odpovědí) na externím rozhraní.

Katalog služeb základních registrů publikuje na venek pro potřeby veřejnosti i agendových systémů.

2.3.1. Koncepce datové architektury

Koncepce datové architektury popisuje konceptuální členění systému na související části. V rámci systému jsou uloženy veškeré datové zdroje nutné pro požadovanou činnost systému nezávisle na okolních systémech. Následující schéma zobrazuje nejdůležitější vztahy mezi daty v jednotlivých registrech.



Návrh koncepce datové architektury respektuje základní požadavek, že na vnějším rozhranní jsou poskytovány referenční údaje a referenční vazby, které mohou být doplněny přímo referenčními údaji odkazovaného registru. Dále jsou zde poskytovány i doplňující, technické a provozní údaje v mezích zákona č. 111/2009 Sb.

Základním prvkem zajištění důvěrnosti dat v ZR je využívání mechanismu ZIFO <-> AIFO. Jestliže ORG mění AIFO (řešení nedostatků přidělení AIFO), pak tato změna musí být propagována do všech dílčích registrů (záměna AIFO->AIFO).

Pokud je v rámci registru RUIAN zrušen prvek, pak registr tuto skutečnost zajistí nastavením interního příznaku „zrušen“. Na následující dotazy na tento prvek pak vrací stav „neexistuje“. Editační AIS musí na zrušení prvku reagovat a provést opravu referenční vazby. O zrušení prvku je informován standardní službou notifikace změn.

Obecně pro libovolný subjekt/objekt v rámci základních registrů platí, že o jeho zrušení jsou informovány odpovídající editační AIS (pomocí zaregistrované standardní notifikační služby). Dále je při dotazu na tento subjekt/objekt vracen stav neexistuje a ppřípadně je navracena informační hodnota zrušeného objektu/subjektu.

2.3.2. Datový model

2.3.2.1. Entity datového modelu

Tato kapitola obsahuje informace o účelu, kontextu procesu a atributech jednotlivých entit datového modelu informačního sytému základních registrů.

Vnější vstupní (virtuální) fronta

Fronta pro příjem požadavků na služby vystavené na vnějším komunikačním rozhraní.

V případě nekorektní zprávy nebo chybě oprávnění není zpráva do fronty zařazena a informace o chybě je vrácena synchronně volajícímu systému.

U korektní zprávy je v okamžiku přijetí této zprávy přidělen ID zprávy (UUID) a vygenerováno časové razítko, obě tyto informace jsou synchronně vráceny volajícímu systému, ID zprávy pro dotazování na stav zpracování zprávy, časové razítko (s využitím digitálních podpisů) jako potvrzení přijetí požadavku ke zpracování.

Pokud je volána primitivní služba (obsahuje právě jednu primitivní službu jednoho registru) a služba je definována jako volitelně synchronní, pak je možné po stanovenou dobu očekávat synchronní odpověď. Pokud je tato doba překročena (time-out), pak je volání služby neúspěšné. Služba může být opětovně volná v synchronním či asynchronním režimu.

Klíčovými atributy této fronty jsou:

Vstupní požadavek	Originální vstupní datová zpráva
Priorita	Priorita zpracování požadovaná zdrojovým systémem. Priorita vložená zdrojovým systémem může být ISZR při zpracování potlačena.
Datum vložení	Datum a čas vložení požadavku do fronty
Volající systém	Informace o systému, který zprávu vkládá
ID zprávy (UUID)	Jedinečný identifikátor zprávy přidělený ISZR při přijetí zprávy
Časové razítko	Časové razítko přijaté zprávy vygenerované ISZR a odeslané AIS jako potvrzení přijetí zprávy

Vnější výstupní (virtuální) fronta

Fronta pro zařazování odpovědí na zpracované požadavky. Z pohledu ISZR jde o frontu, do které jsou postupně zařazovány zpracované zprávy ze vstupní fronty. Z pohledu vnějšího AIS jde o úložiště s řízeným přístupem, tedy vnější systém vybírá zprávy z fronty.

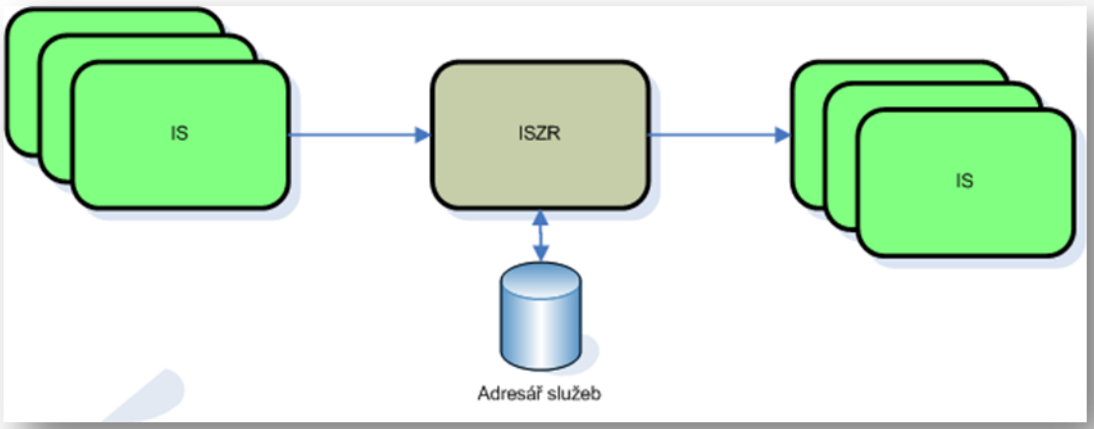
ID zprávy (UUID)	Jedinečný identifikátor zprávy, převzatý ze vstupní zprávy

Datum zpracování	Datum vložení odpovědi do fronty
Výstupní zpráva	Odpověď na zpracovanou vstupní zprávu. Tato zpráva bude odeslána zpět na AIS při požadavku na vyzvednutí zprávy. Součástí výstupní zprávy jsou všechny informace o výsledku zpracování.
Výsledek zpracování	Kód přiřazený na základě výsledku zpracování zprávy

2.3.3. Obecné vnitřní datové rozhraní

Datové rozhraní ISZR slouží pro příjem zpráv z participujících systémů a jejich bezpečné a zaručené předání na jiné participující systémy. V rámci své funkce je monitorován stav rozhraní a jsou generována data pro zabezpečení garantované kvality služeb poskytovaných rozhraním.

Základní princip funkce datového rozhraní je následující. Volající systém (jednotlivé základní registry, interní aplikační servery) předává zprávu na komunikační rozhraní. V rámci zprávy je kromě klíčového identifikátoru zprávy dále předávána identifikace zdrojového (volajícího) a cílového (volaného) systému a jeho služby. Procesy obsluhující datové rozhraní zprávu převezmou a ověří její platnost. Ve vnitřním adresáři ISZR služeb identifikují cílový systém a jeho vstupní bod a provedou předání datové zprávy na vstupní bod cílového systému.



Datové zprávy předávané na vstupní datové rozhraní ISZR jsou obecné, jednotné pro všechny systémy generující požadavky na ISZR.

Preferovanou variantou řešení je společná definice datových zpráv předávaných na vstupní bod cílových systému. Důvod pro upřednostnění této varianty spočívá jak v následné obecnosti systému ISZR, tak i v aspektech týkajících se dalšího rozšiřování řešení na další systémy – jako rychlost nasazení, udržovatelnost řešení, bezpečnost provozu apod.

Technicky je možné řešit i varianty rozdílné specifikace vstupních bodů cílových registrů, a to za podmínky dodržení logické definice datové zprávy. Tato varianta ale vnáší do obecného řešení ISZR nestandardní prvky.

2.3.4. Distribuce dat externím subjektům

Externím subjektům budou poskytovány exporty dat ve formě **nereferenčních údajů.** Jakýkoliv export se tedy v okamžiku vydání stává nereferenčním. Může být využíván v rámci jednotlivých agend v situacích, kdy není požadavek na referenční validitu údajů. V opačném případě je nutné vždy vyžádat referenční data přímo od systému základních registrů.

Jednotlivé exporty budou přesně definovány z hlediska obsahu (ochrana osobních dat) a hlediska dostupnosti tohoto exportu (registrace agendy pro příjem exportu). Exporty budou prováděny v následujícím režimu:

- **Plný export** – pravidelně.
- **Rozdílový export** - změny oproti poslednímu plnému exportu.

3. Základní procesy /Procesní architektura

3.1. Základní východiska

Návrh procesní architektury systému Základních registrů vychází z podkladových materiálů přiložených k soutěžním podmínkám.

Informační systém základních registrů je definován zadavatelem jako referenční rozhraní pro přístup k základním registrům. ISZR poskytuje oprávněným subjektům komplexní služby nad základními registry s ohledem na jejich oprávnění v registru práv a povinností.

3.2. Cíle

Cílem návrhu procesní architektury je identifikace aktorů procesní architektury (vystupují v jednotlivých procesech), rozčlenění procesů probíhajících v systému Základních registrů a logické členění těchto procesů do skupin.

3.3. Souhrn základních procesů

V rámci systému základních registrů se jednotlivé procesy dělí do následujících skupin:

I. Životní cyklus agendy

II. AIS jako poskytovatel eGON služeb prostřednictvím ISZR

III. Životní cyklus eGON služby

IV. Užití eGON služby Základních registrů a zprostředkovaných služeb AIS

V. Výpis záznamů o událostech souvisejících s provozováním základních registrů.

I. - Životní cyklus agendy tvoří následující procesy:

I-1. Registrace agendy v Katalogu agend.

I-2. Pilotní provoz agendy.

I-3. Spuštění ostrého provozu agendy.

I-4. Změna/oprava procesů agendy a souvisejících parametrů.

I-5. Pozastavení agendy.

I-6. Zrušení agendy.

II. - AIS jak poskytovatel eGON služeb tvoří následující procesy:

II-1. Žádost o registraci AIS jako poskytovatele služeb.

II-2. Publikace eGON služeb registrovaného AIS.

II-3. Zrušení eGON služeb AIS při ukončení agendy.

III. - Životní cyklus eGON služby tvoří následující procesy:

III-1. Registrace eGON služby.

III-2. Pilotní provoz eGON služby.

III-3. Spuštění ostrého provozu eGON služby.

III-4. Změna/oprava procesů eGON služby a souvisejících parametrů volání služby.

III-5. Pozastavení eGON služby.

III-6. Zrušení eGON služby.

IV. - Užití eGON služby tvoří následující procesy:

IV-1. Volání externí eGON služby.

IV-2. Volání interní eGON služby (služby pro vnitřní potřebu ISZR).

V. - Výpis záznamů o událostech. Skupinu tvoří procesy související s vnitřním fungováním systému Základních registrů, slouží k dohledu a správě úrovně služeb ISZR (SLA), slouží k monitoringu a reportingu bezpečnostních incidentů. Zvláštním procesem v této skupině je proces vyvolaný fyzickou osobou při dotazu na historii dat, které o něm ISZR poskytla agendovým informačním systémům. Jsou to především následující procesy:

V-1. Reporting využití služeb ISZR,

V-2. Nastavení SLA služby ISZR.

V-3. Dohled SLA služby ISZR.

V-4. Incident management služby ISZR.

V-5. Problem management služby ISZR.

V-6. Reporting SLA služby ISZR.

V-7. Duplikace číselníků RPP (katalogu služeb, …) pro potřeby ISZR.

V-8. Dotaz fyzické osoby na zpracovávaná data v ZR.

Většina procesů ISZR má charakter podpůrných procesů ve vztahu k celkové funkčnosti základních registrů, proto doplnění seznamu a detailní členění bude dále precizováno v rámci dopracování soutěžního návrhu na základě požadavků architektů základních registrů a architektů vybraných agendových informačních systémů. Tam, kde to bude účelné, budou popsány i podprocesy uvedených procesů.

3.3.1. Změny referenčních a nereferenčních údajů ZR

- Editace údaje
- Reklamace údaje
- Notifikace o změně údaje
- Likvidace údaje

Historii změn údajů si vedou editoři ZR.

3.3.2. Čtení referenčních a nereferenčních údajů ZR

- Čtení referenčního údaje
- Čtení nereferenčního údaje

3.3.3. Činnosti s nereferenční kopií dat ze ZR pro účely AIS

- Registrace exportu nereferenčních dat (určení obsahu a oprávněných příjemců)
- Export obsahu ZR pro vytvoření nereferenční kopie dat
- Průběžná aktualizace exportů ZR na základě publikace změn.

3.3.4. Práce s řídící částí RPP

- Registrace OVM
- Registrace agendy
- Správa rolí agendy
- Autentizace agendy/AIS

3.3.5. Zprostředkování komunikace mezi AIS-AIS

Komunikace mezi dvěma AIS probíhá pomocí volání eGON služeb. Je tedy řešena sadami procesů popsaných výše v podkapitole, především v části „**IV - Užití eGON služby“**

- Registrace agend poskytujících služby ostatním AIS
- Publikace služeb agendy
- Předání požadavků AIS-AIS

3.4. Souhrn základních aktorů

- Agenda VS
- ISDS
- ISZR
- Orgán veřejné moci
- Osoba
  - právnická osoba
  - soukromá osoba
- Správce ZR
- Úřad

4. Technologická architektura/ Základní rámec technologické architektury

4.1. Základní východiska

Základním předpokladem je, že ISZR poskytuje společný základ pro technologickou architekturu všech komponent základních registrů. Komponenty jsou využívány jednotlivými základními registry (nepovinně). Technologicky je možné sdílet tyto komponenty v rámci jednotlivých registrů a ISZR:

- Hardwarová platforma (síťové prvky, load balancing (vyrovnávání zátěže), diskové pole, infrastruktura pro zálohování, záloha napájení atd.)
- Síťové služby (DNS, časový sever NTP, atd.)
- Správa a monitoring (Identity and Access management, portál pro správu, nástroje pro management a monitoring, audit)
- Infrastruktura veřejných klíčů (PKI).

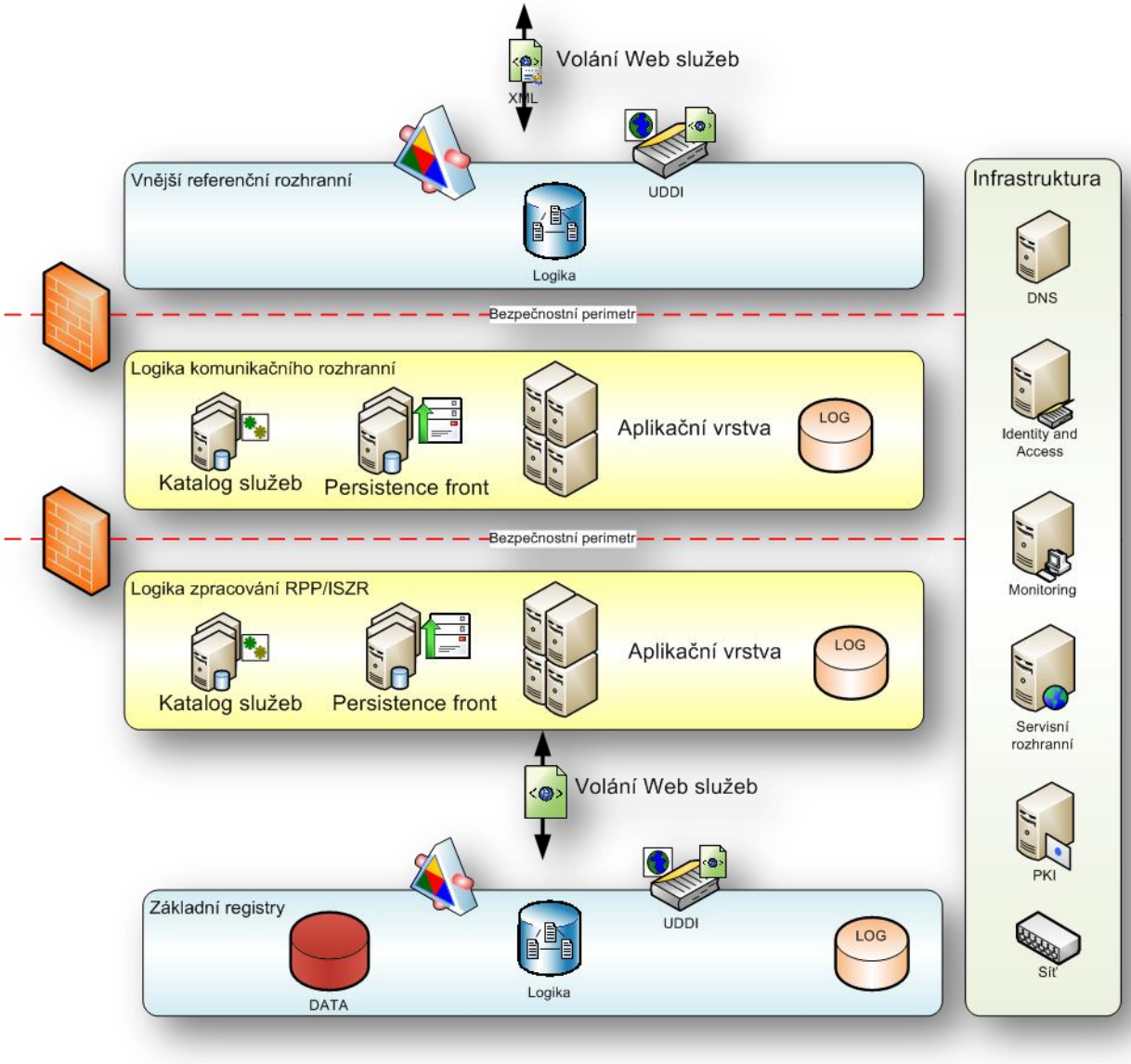
4.2. Cíle

Cílem návrhu je stanovení závazných standardů a vazeb technologické architektury. Není stanoveno konkrétní naplnění jednotlivých komponent (výrobce a použitý produkt).

Vzhledem k nutné spolupráci s několika subjekty (jednotlivé základní registry, existující a budoucí agendové systémy) je nutné zajistit spolupráci mezi různými platformami a zajistit transparentnost poskytovaných služeb.

4.3. HW schéma/Souhrnný popis

Architektura Informačního systému základních registrů vychází striktně z přístupu Service-Oriented Architecture (SOA). Tento přístup je využit jak pro architekturu vnějšího referenčního rozhraní, tak pro architekturu vnitřního komunikačního rozhraní.



Z hlediska Agendových informačních systémů je systém základních registrů prezentován Web službami eGON publikovanými pomocí privátního Universal Description, Discovery, and Integration (UDDI) registru.

Z hlediska ISZR jsou jednotlivé základní registry (RPP, ROB, ROS, RUIAN) a Převodník identifikátoru fyzických osob (ORG) prezentovány Web službami publikovanými v jednom společném UDDI registru. Tento společný katalog bude spravován Informačním systémem základních registrů.

Pro výměnu zpráv mezi jednotlivými komponentami bude použit formát XML. Zprávy přenášené po veřejné datové síti budu obsahovat veřejnou část (nešifrovaná hlavička zprávy) a datovou část (šifrované tělo zprávy). Zprávy přenášené po vnitřním rozhranní (KIVS) budou přenášeny v plně otevřeném tvaru. Zabezpečení zpráv je založeno na požadavcích na KIVS popsaných výše.

Veškeré použité technologie musí být postaveny na základě všeobecných standardů. Nesmí být použita žádná proprietární technologie, která by způsobila zvýšení nákladů na provoz a správu systému jako celku.

4.3.1. Komponenty návrhu technologické architektury

Veškeré komponenty technologické architektury musí splňovat požadavky na plynulou škálovatelnost a vysokou dostupnost. Primárním požadavkem je zajištění odezvy systému základních registrů pro čtení referenčních údajů vyhovující požadavkům na SLA dle kapitoly 6.5.

4.3.1.1. Síťové prostředí

Předpokladem je schopnost vytváření bezpečného a vysoce dostupného síťového prostředí pro činnost systému základních registrů. Použité síťové prvky tedy musí splňovat minimálně následující požadavky:

- Veškeré prvky musí umožňovat dálkovou správu a dohled.
- Veškeré prvky musí obsahovat technologii VLAN.
- Veškeré prvky musí podporovat technologii 802.1x pro autentifikaci klientů.
- Jednotlivé části sítě budou zabezpečeny pomocí ochranných perimetrů.
- Veškeré části sítě musí být implementovány redundantně.

Z hlediska hardware budou pro jednotlivé části systému Základních registrů vybrány produkty jednoho dodavatele, který je schopen zajistit celou škálu a následnou podporu vybavení. Ideálním stavem je dodržení tohoto pravidla pro celý systém Základních registrů. Minimálním požadavkem je vzájemná kompatibilita z hlediska provozu i monitoringu.

4.3.1.2. Hardwarová platforma

Celá architektura základních registrů obsahuje jak prostředky Informačního systému základních registrů (ISZR), tak prostředky jednotlivých základních registrů (RPP, ROB, ROS, RUIAN). Bez ohledu na konkrétní výběr dodavatele je preferovanou variantou výběr jednoho výrobce pro všechny servery minimálně v rámci jedné komponenty systému základních registrů (jednotlivý registr). Pro dodávku budou standardizovány následující role serverů:

- Aplikační servery.
- Databázové servery.
- Provozní servery.

Žádný ze serverů nesmí být potenciálním bodem pádu systému při výpadku. Současně musí být zajištěna vysoká škálovatelnost každé části systému pro navýšení průchodnosti jednotlivých částí v případě potřeby. Pro splnění těchto požadavků budou standardně využívány technologie:

- **Cluster** – dva a více serverů poskytující současně stejnou funkcionalitu (typicky databázové servery).
- **Farma –** více serverů současně poskytujících stejnou funkcionalitu. Jejich služby jsou publikovány pomocí hardwarového či softwarového loadbalancingu.
- **Storage Area Network (SAN) –** Externí diskové pole s vysokou dostupností poskytující diskový prostor pro všechny servery.

Celé řešení musí splňovat parametry GeoCluster (dvě rovnocenné lokality schopné samostatně poskytovat veškeré služby a sdílející stejná data).

4.3.1.3. Operační systém, aplikační platforma a databázový server

Operační systém bude vybrán na základě specifikace zadavatele. Cílem je minimalizace typů provozovaných systémů a zajištění jejich jednotné správy (monitoring, management, security monitoring, Identity a Access management).

4.3.1.4. Web služby

Web služby jsou souborem standardů, které umožňují interoperabilitu mezi heterogenními systémy a procesy. Poskytují společný standard jako klíč ke vzájemné komunikaci mezi systémy. Tato vlastnost je zásadní pro implementaci Service-Oriented Architecture (SOA). Webové služby budou implementovány podle obecných standardů.

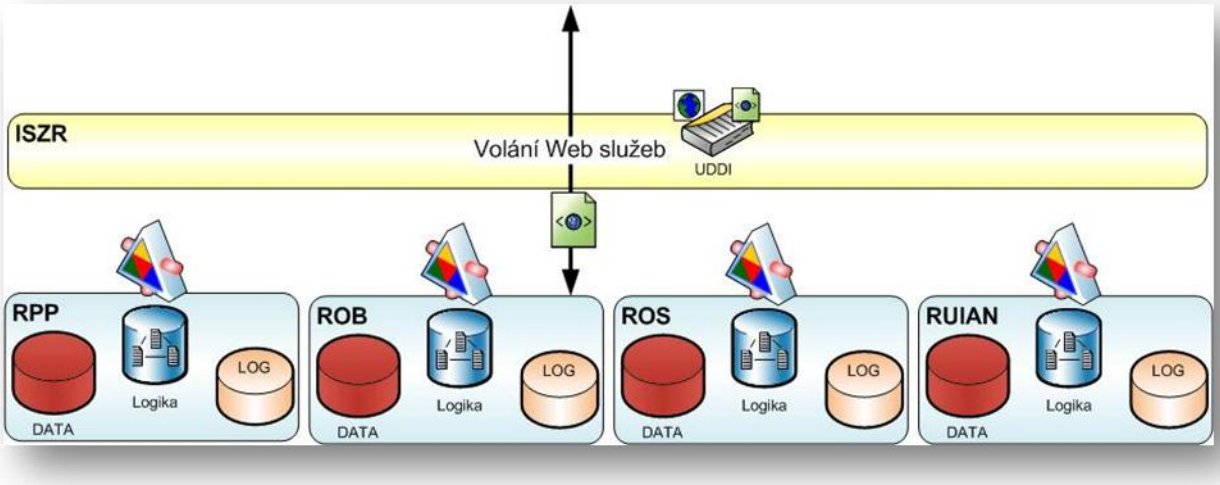
- HTTP/HTTPS - Hypertext Transfer Protocol
- XML, XSLT - Extensible Markup Language, Extensible Stylesheet Language Transformations
- WDSL - Web Services Description Language
- UDDI - Universal Description Discovery and Integration.

4.3.1.5. Disaster recovery

Pro zajištění dostupnosti služeb a obnovy služeb v případě výpadku budou poskytovány pro ISZR a všechny základní registry služby zálohy a obnovy dat včetně scénářů obnovy služeb.

4.3.2. Distribuované uložení jednotlivých základních registrů

Jednotlivé základní registry budou uloženy v prostorách jednotlivých gestorů v oddělených fyzických prostorech. Vzájemná komunikace bude zajištěna a provozována pomocí KIVS.



Správa jednotlivých základních registrů bude přistupovat k infrastruktuře pomocí definovaného rozsahu funkcí a oprávnění. Musí být zajištěno logování těchto aktivit.

5. Postup plnění daty

Kapitola Postup naplnění systému daty bude dále rozpracována v úzké součinnosti s relevantními zástupci zadavatele a jednotlivých týmů architektury základních registrů.

5.1. Základní východiska

Postup plnění dat musí respektovat závislosti mezi jednotlivými referenčními údaji. Je nutné určit zdroje referenčních údajů (agendové informační systémy a případný další zdroje), způsob jejich ověření a způsobu jejich průběžné aktualizace.

5.2. Cíle

Definovat a navrhnout postup naplnění systému daty ve smyslu zadaném v soutěžních podmínkách. Postup naplnění systému daty bude obsahovat metodu ověřování kvality dat včetně kritérií jejich správnosti. Dále bude vypracován jednoznačný harmonogram naplnění systému daty a bude navržen i způsob průběžné aktualizace dat.

5.3. Souhrnný popis

Jak vyplývá z příslušné legislativy, neukládá ISZR žádná referenční data. Z tohoto důvodu nepředpokládáme nutnost samostatně řešit otázku naplnění systému daty z již existujících systémů. V rámci ISZR budou ukládány pouze provozní logy, jejich naplnění bude prováděno automaticky za běhu systému. Dále předpokládáme, že bude nezbytné provést naplnění katalogu služeb, nicméně tato činnost bude prováděna samotnými registry.

Zákon o Základních registrech určuje, že Základní registry obsahují autentizační údaje. Z globálního návrhu technologické architektury plyne, že by v rámci ISZR měla být naplněna a udržována databáze správy identit a autentizační data správců registrů.

Autentizační údaje v rámci Základních registrů je možné rozdělit na:

- **Oprávnění agendy k využívání eGON služby** – autentizační údaje jsou uloženy v rámci Registru práv a povinností jako vazba mezi eGON službou, identifikátorem agendy a registrovanou rolí agendy. ISZR tedy neověřuje autentizaci konkrétní osoby (úředníka). Tento údaj je pouze logován pro případný audit.
- **Oprávnění fyzické osoby pro přímý přístup k prostředkům ZR** – IZSR i základní registry musí být udržovány a spravovány fyzickými osobami – **správci**. Pro identifikaci těchto správců musí být k dispozici centrální systém pro správu identit a oprávnění.

5.3.1. Postup naplnění autentizačních údajů

Autentizační údaje jsou jediná data, která je potřeba naplnit před zahájením poskytování služeb ISZR.

ISZR při příjmu požadavku na eGON službu musí provést kontrolu oprávnění ve vazbě:

- Identifikátor agendy
- Identifikátor role v agendě
- Identifikátor eGON služby.

Tyto údaje jsou podmnožinou dat uchovávaných v rámci RPP. V rámci ISZR bude vytvořen mechanismus čtení těchto údajů z RPP tak, aby mohly být požadavky kontrolovány již v rámci vstupních front. Mechanismus čtení těchto údajů bude postaven na Web službě dodávané RPP, kterou bude ISZR oprávněno volat.

- ISZR bude tuto matici oprávnění užívat pouze v uvedené formě a aktuálním stavu bez historie.

Autentizační údaje správců jednotlivých systémů budou uchovávány v rámci řešení Identity managementu s následujícími vazbami:

- Každá část základních registrů (ISZR, RPP, ROB, ROS, RUIAN, ORG) poskytne seznam rolí pro správu této části základních registrů.
- Předpokládáme, že každý správce je osobou a existuje tedy ekvivalentní záznam v základním registru ROB.
- Na základě procesu schválení správce bude vytvořen účet tohoto správce pro přístup k prostředkům základních registrů.
- Identity management základních registrů bude chápán jako agenda a tudíž bude přiděleno odpovídající AIFO správce (audit pak může provést vazbu na ROB).

Pro prvotní naplnění data v základních registrech (zvláště ROB) budou vytvořeny servisní účty bez vazby na ROB. Použití těchto účtů bude auditováno a povoleno pouze do okamžiku základního naplnění registrů.

Identity management musí být schopen komunikovat se stávajícími IdM systémy využívanými v rámci veřejné správy (CzechPoint, Informační systém Datových schránek).

5.4. Návaznost plnění jednotlivých registrů

5.4.1. RUIAN

Plnění RUIAN bude možné zahájit až po zprovoznění ISZR a naplnění základních autentizačních a autorizačních údajů do RPP.

Do této doby bude probíhat migrace ze zdrojových systémů do ISUI a další čištění dat v ISUI. Pro agendové editační systémy ostatních registrů, které budou potřebovat data RUIAN již před jeho naplněním, bude možné z ISUI (případně z ISKN) poskytnout předem pro čištění adresních údajů pracovní data.

Po dosažení požadované kvality dat budou údaje u ISUI a ISKN naplněna do RUIAN (v této fázi předpokládáme naplněnost > 95%), a během pilotního provozu bude pokračovat další čištění dat.

5.4.2. ROB

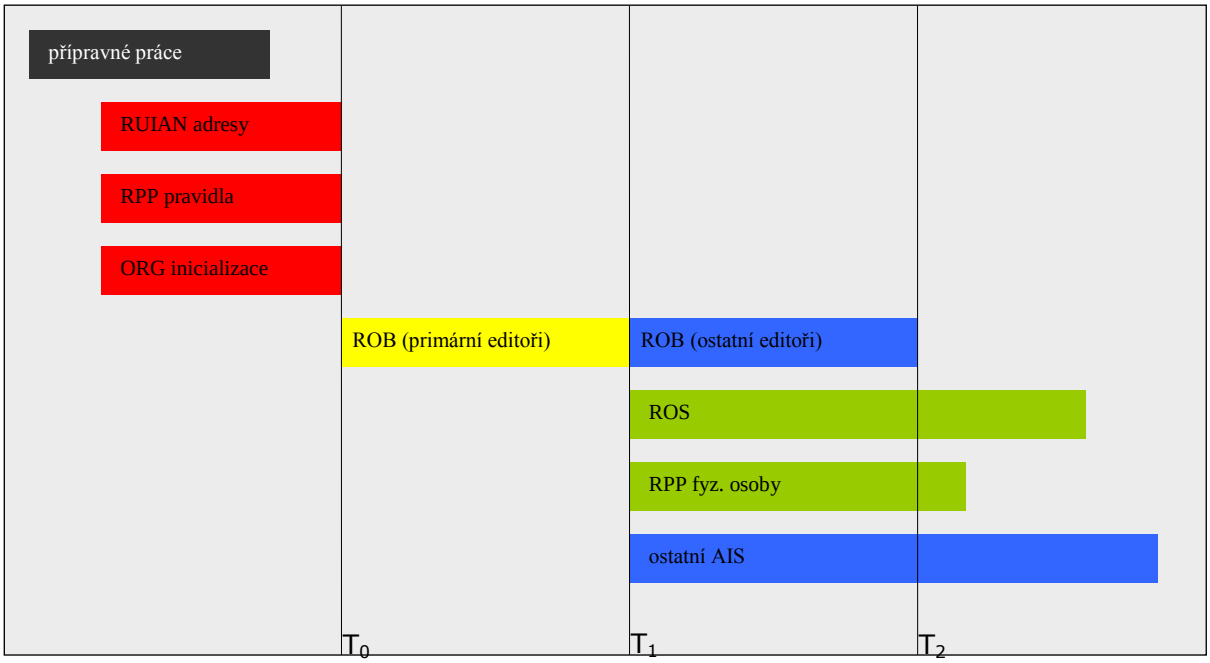
Při plnění základních registrů musí být splněny následující podmínky:

Čas	Dokončeno	Zahajuje se
T_0	přípravné práce naplněna adresní část RUIAN naplněna pravidla RPP inicializace ORG	primární plnění ROB z AIS EO a AIS CIS

T_1	primární naplnění ROB	plnění ROB z AIS OP, AIS CD, AIS DS plnění ROS plnění RPP připojení ostatních AIS
T_2	dokončeno plnění ROB	standardní provoz s ROB

Poznámka – Plnění dat ROS a RPP lze v T_1 zahájit pouze v případě, že z ROB nebude potřeba využívat informace o zpřístupnění datové schránky, o čísle elektronického identifikačního dokladu popř. bezpečnostním osobním kódu. V opačném případě je nutné posunout zahájení těchto kroků na čas T_2.

Závislosti jsou graficky znázorněny na následujícím obrázku:



5.4.3. ROS

Plnění ROS bude možné zahájit až po zprovoznění ISZR, zprovoznění ORG, naplnění základních autentizačních a autorizačních údajů do RPP, naplnění RUIAN a naplnění ROB.

Do této doby bude probíhat příprava zdrojových dat v agendových informačních systémech. Již v této fázi je však nutné připravovat ve zdrojových datech referenční vazby na budoucí RUIAN a ROB. Proto bude třeba zajistit spolupráci s projekty RUIAN a ROB a využívat pro potřeby ROS také pracovní datové zdroje, které budou používány k přípravě zdrojových dat pro RUIAN a ROB. V této fázi budou využívány také jiné datové zdroje pro křížové validace (např. RES apod.), bude proto třeba zajistit jejich dostupnost. Pro malé agendy, které budou využívat centrální IAIS ROS, bude příprava zdrojových dat pro iniciální naplnění probíhat v tomto centrálním AIS.

Po úvodním naplnění RUIAN a ROB v rámci pilotního provozu bude zahájeno inkrementální iniciální plnění ROS na základě připravených metrik. Přepokládá se, že do ROS budou naplněny i referenční údaje osob, které nebudou odpovídat všem předepsaným věcným pravidlům. Řešení těchto nekorektních situací bude probíhat ve spolupráci správce ROS a správce příslušné agendy.

5.4.4. RPP

Registr práv a povinností bude naplňován provozními a nezbytnými referenčními údaji postupně v závislosti na potřebách pilotního a ostrého provozu, tak aby bylo vytvořeno prostředí pro ostatní registry se základními funkcemi pro jejich paralelní dílčí plnění.

Na rozdíl od ostatních základních registrů nebude tento registr přebírat (až na některé výjimky) data, která již v současnosti existují a tvořit z nich referenční data. Tento registr bude naplňován daty, která ve velké míře vzniknou až poté, co vznikne tento registr (historická rozhodnutí OVM nebudou do registru zpětně zaváděna). Budou v něm používány odkazy na údaje ze všech ostatních základních registrů, a to ve vztahu k právům, působnosti či povinnostem, které entity popisované v jednotlivých registrech mají nebo jichž se tato práva či povinnosti týkají.

Hlavní kroky naplnění RPP prvotními daty:

- Provozní a řídící data IS RPP - nejprve budou naplněna provozní a řídící data IS RPP (číselníky, fronty, parametry aplikačního serveru apod.) proto, aby bylo umožněno plnění ostatních registrů
- Katalog služeb a část Katalogu agendových rolí - paralelně budou naplněna data Katalogu služeb a data o agendách
- Referenční údaje o právních předpisech - budou naplněna data o právních předpisech, zároveň dojde k navázání agend na právní předpisy
- Část Katalogu agendových rolí - budou zaznamenány role v agendách
- Matice oprávnění - rolím budou vytvořeny záznamy v matici oprávnění, čímž rolím vzniknou práva spouštět služby z Katalogu služeb
- Referenční údaje o právech a povinnostech osob - budou vytvořeny záznamy a vazby o rozhodnutích agend - na základě jakých právních předpisů - s účinky na referenční údaje dalších registrů (ROS, RON, RUIAN).

6. Katalog funkcí (skupiny, principy)/ Katalog služeb, poskytovaných a vyžadovaných v systému Základních registrů

Informační systém základních registrů (ISZR) vytváří prostředí pro komunikaci mezi základními registry a Agendovými informačními systémy (AIS) a mezi AIS vzájemně. Jako jediný komunikuje s Generátorem agendového identifikátoru (ORG).

ISZR tedy publikuje eGON služby, pomocí kterých zprostředkovává tuto komunikaci. Současně ISZR spravuje katalog služeb jednotlivých registrů (RPP, ROB, ROS, RUIAN a ORG) v jednotném celku včetně služeb které poskytuje ISZR jako takové.

6.1. Základní východiska

- Katalog služeb veřejné správy obsahuje seznam služeb, které poskytují jednotlivé Orgány veřejné moci.
- Katalog eGON služeb obsahuje seznam služeb, které jsou realizovány prostřednictvím informačních systémů veřejné správy a slouží pro přístup a editaci dat v nich vedených.
- eGON služby základních registrů jsou kompozitem služeb dílčích systémů: ISZR, ZR, ORG, připojené AIS.
- Katalog služeb zajišťuje i mapování eGON služeb ke službám veřejné správy.
- Služby ZR a služby dílčích AIS jsou volány samostatně. Neexistuje služba, která by směšovala služby ZR a dílčích AIS v jednom volání.
- K referenčním údajům základních registrů lze přistupovat jen a pouze z AIS prostřednictvím eGON služeb ISZR.
- Komunikace mezi AIS probíhá prostřednictvím eGON služeb, které zprostředkuje ISZR na základě katalogu služeb AIS.
- Fyzická osoba je oprávněna k získání informací z ISZR (na základě protokolu o poskytovaných službách), jaké jiné subjekty o ní zjišťovaly informace.

6.2. Cíle

Navrhnout katalog služeb IZSR, který zajistí:

- Jednoznačnou definici množiny eGON služeb, které ZR poskytují svému okolí. Služba je nejnižší možný prvek komunikace.
- Integritu a jednotnou definici volání služeb, které bude jednoznačně popsáno svými vstupními a výstupními parametry pro zprostředkování přístupu k referenčním datům.
- Dostupnost popis služby v katalogu, který jednoznačně definuje, jak se služba užívá (co musíme a co můžeme dodat za vstupní parametry, abychom dostali informační výstup s předem definovanou strukturou).
- ISZR má implementován mechanismus pro řízení distribuované transakce v dílčích registrech. Navazující registry ROB, RPP a zejména ORG musí mít zajištěnu podporu tohoto požadavku. Do doby potvrzení celé

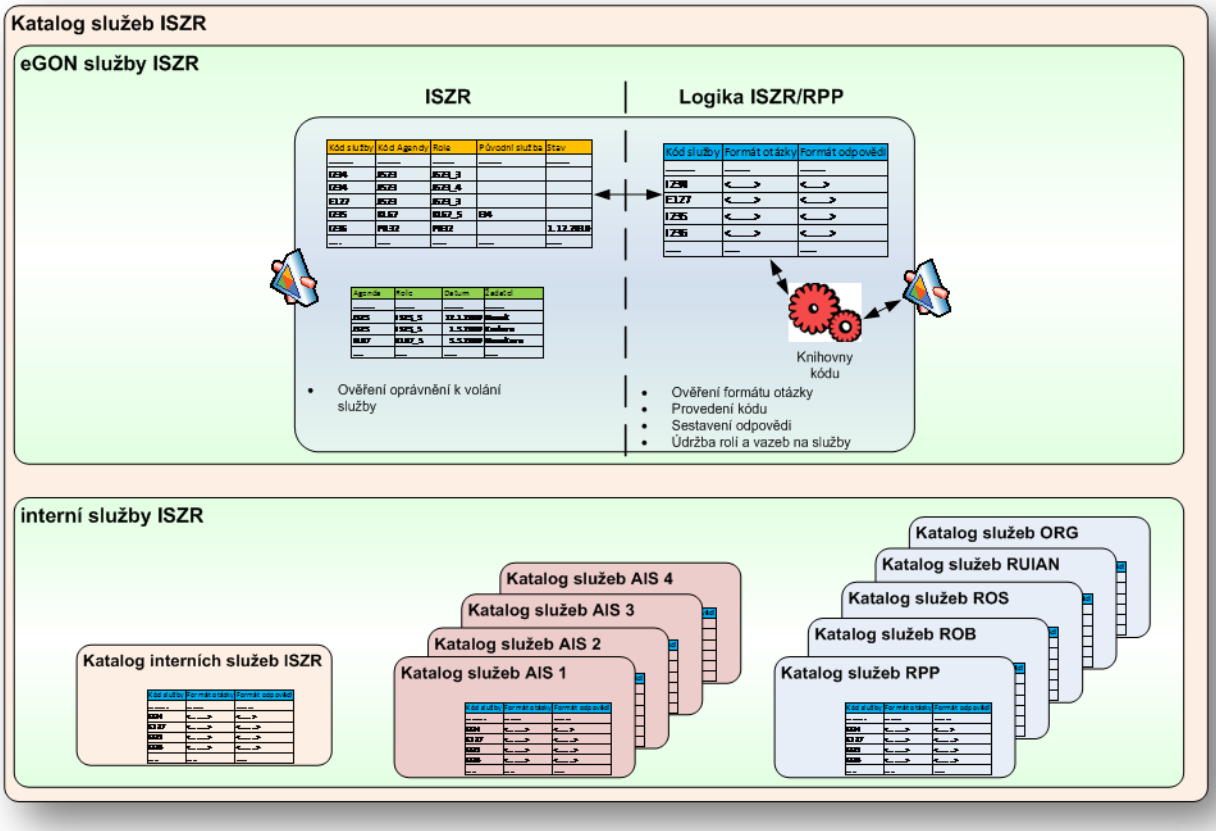
transakce ze strany ISZR nesmí dílčí registry a ORG poskytovat tyto změněné údaje pro služby, které požadují čtení tohoto referenčního záznamu.

6.3. Souhrnný popis

Katalog služeb ISZR je vytvářen na základě souhrnu katalogů služeb jednotlivých základních registrů, agendových informačních systémů a interních služeb ISZR. Provádí publikaci těchto služeb směrem k jednotlivým AIS a základním registrům.

Základní registry poskytují minimalizovanou sadu primitivních služeb se zaměřením na rychlost odezvy. Tyto služby jsou v rámci jednotlivých základních registrů implementovány s ohledem na minimalizaci doby odezvy při volání služby.

Aplikační logika ISZR dále provádí kompozici těchto primitivních funkcí a poskytuje komplexnější funkce na externím rozhraní ISZR. Při využití těchto služeb opět provádí zpětnou dekompozici na primitivní funkce jednotlivých základních registrů.



6.3.1. eGON služby vnějšího referenčního rozhraní

Pro potřeby definice katalogu služeb je pod pojmem AIS chápán jakýkoliv externí systém, který má právo využívat eGON služby základních registrů. Toto obecné právo na komunikaci je dáno legislativou a je vyjádřeno záznamem v matici oprávnění v RPP. Na základě registrace AIS je především poskytováno oprávnění číst UDDI katalog eGON služeb ZR. Pro užití konkrétní služby z Katalogu služeb ZR je nutné další oprávnění registrované v matici oprávnění RPP. eGON služby z Katalogu služeb mohou být využívány konkrétním AIS v případě provedené registrace AIS a jeho rolí ve vztahu ke konkrétní službě. Tyto údaje a vazby jsou uloženy v Registru práv a povinností.

V katalogu eGON služeb ZR je uvedeno minimálně:

- Kód služby.
- Platnost služby.
- Kód služby, kterou nahrazuje nebo prázdný údaj.
- Typ služby (synchronní/asynchronní).
- Maximálně povolený počet odpovědí navrácených v jedné transakci.
- Typ SLA služby.

Konkretizace množiny údajů uvedených v katalogu eGON služeb bude provedena ve spolupráci s architekty základních registrů, zvláště pak s architektem Registru práv a povinností.

6.3.2. Služby vnitřního důvěryhodného rozhraní

Vnitřní důvěryhodné rozhraní slouží ke komunikaci mezi ISZR včetně připojeného převodníku ORG a základními registry (ROB, ROS, RUIAN, RPP).

Současně je na tomto rozhraní připojeno administrativní rozhraní sloužící pro správu a monitoring komunikačního prostředí ISZR.

Pro toto interní důvěryhodné rozhraní slouží oddělený privátní katalog služeb, které nejsou poskytovány mimo prostředí důvěryhodné interní sběrnice ISZR.

Konzumentem těchto služeb je pouze ISZR (včetně administrativního rozhraní). Tímto postupem je zajištěno, že služby, které jsou poskytovány přímo libovolným z registrů, nejsou dostupné jinak než prostřednictvím ISZR, tak jak je požadováno v zákoně o základních registrech.

Služby vnitřního důvěryhodného rozhraní jsou publikovány v privátním UDDI katalogu služeb, který může číst pouze ISZR.

6.4. Návrh katalogu služeb

Obecně je možné eGON i vnitřní služby rozlišit na:

- **Informační** – navrací referenční údaje podle požadavků
  - **Primitivní –** navrací referenční údaje pouze z jediného základního registru nebo AIS.
  - **Komplexní –** navrací referenční údaje z více registrů nebo AIS na základě referenčních vazeb. Není možné směšovat dotazy ze základních registrů a AIS ani dotazy z různých AIS.
- **Editační** – slouží editorům ke změně referenčních údajů a nastavení referenčních vazeb
  - **Primitivní –** provádí změny referenčních údajů pouze v jediném základním registru.
- **Servisní** – provádí operace mimo referenční údaje základních registrů
  - **Převodník ORG –** operace převodů AIFO a životního cyklu ZIFO/AIFO.
  - **Notifikační –** umožňuje získat oprávněným subjektům změny v referenčních údajích a referenčních vazbách.

- **Distribuční –** zasílá do datových schránek subjektů požadované informace.
- **Logování –** ukládá informace o aktivitách v rámci ISZR.

- **AIS ISZR** – služby samostatného AIS pro ISZR, které budou sloužit pro naplnění podmínek informování subjektů o údajích, které jsou o nich vedeny v rámci základních registrů a operacích, které byly jednotlivými agendami nad těmito údaji prováděny.

6.4.1. Katalogy služeb základních registrů

Systém základních registrů bude tedy obsahovat dva katalogy služeb (publikované prostřednictvím UDDI).

- **eGON služby základních registrů** – obsahuje služby poskytující přímo referenční údaje ze základních registrů i služby poskytující zprostředkované údaje z jiných registrovaných AIS.
- **Vnitřní služby základních registrů** – služby poskytované jednotlivými základními registry, převodníkem ORG. Tyto služby může konzumovat pouze ISZR.

6.4.2. Kategorizace služeb základních registrů

Je možné provést několik kategorizací služeb:

- Kategorizace dle typu odpovědi:
  - **Logická** – Potvrdí správnost či existenci údaje.
  - **Záznam** – Pracuje s konečným počtem referenčních údajů. Navrací či mění tyto referenční údaje.
- Kategorizace dle množiny výběru:
  - **Individuální** – Pracuje s referenčními daty nad jediným prvkem.
  - **Hromadné** - Pracuje s referenčními daty nad skupinou prvkem.
- Podle iniciátora:
  - **Pull služby** – Iniciátorem je AIS. Základní registry reagují na volání služby.
  - **Push služby** – Iniciátorem jsou základní registry. Tento typ služeb bude poskytován pouze směrem k datovým schránkám registrovaných subjektů (zasílání informací o změnách, na které má registrovaný subjekt právní nárok).
- Podle povahy informací:
  - **Referenční** – Poskytuje referenční údaje dle zákona 111/2009 sb. Pro referenční služby neexistují možnosti hromadného výdaje. Poskytují vždy aktuální data a předané informace jsou referenční dle zákona. O výdej referenčních údajů může požádat pouze registrovaná agenda orgánu veřejné moci příslušnou službou ZR.
  - **Informační** – Poskytují údaje vycházející z referenčních údajů. Vydané informace mají charakter „Veřejných údajů pro informační účely“. Výdej veřejných údajů není logován z hlediska obsahu odpovědi,

je zaznamenán pouze požadavek na výdej. Součástí veřejných údajů nesmí být žádné osobní údaje. O výdej veřejných údajů může požádat libovolný subjekt prostřednictvím centrálních AIS. Informační údaje mohou být vydávány hromadně.

- **Osobní –** Poskytují referenční údaje týkající se subjektů údajů v registru ROB. Tyto služby nesmí v žádné fázi zpracování obsahovat pro jeden subjekt údajů ROB agendové identifikátory fyzické osoby pro různé agendy. Výdej údajů pomocí těchto služeb je vždy logován. O výdej osobních údajů může požádat pouze registrovaná agenda orgánu veřejné moci příslušnou službou ZR.

- Kategorizace dle povahy operace s daty:
  - Služby realizující pouze **čtení** (select).
  - Služby realizující pouze **zápis** (insert).
  - Služby realizující **změnu** (update).
  - Služby realizující **výmaz** (delete).

Hromadné operace budou dostupné pouze ve zvláštním režimu a pouze vybraným uživatelům (např. orgánům krizového řízení) na základě platných právních předpisů.

Využívání individuálních služeb bude také omezeno (ve smyslu frekvence dotazů od jednotlivých subjektů), aby se zabránilo pokusům získat hromadná data sérií individuálních dotazů.

Za účelem naplnění principu práva občana získat informace o tom, kdo, kdy a na co se jiné subjekty ptaly, bude veden tzv. auditní log, tj. bude zaprotokolováno využití eGON služeb ISZR Agendami ve vztahu k občanovi.

6.4.3. Práce se službami

Způsob definice mají služby základní, informační i servisní stejný, liší se jen obsahem a způsobem zpracování.

Definici služeb ZR udržuje správce ISZR, který rovněž odpovídá za jejich:

- Zavedení
- Užití
- Zrušení.

Služby v katalogu vznikají dle potřeb AIS na základě schvalovacího procesu, který řídí správce ISZR. Definice služby po zavedení do katalogu služeb se nemění, změna definice služby vede k vytvoření nové služby. Existuje služba pro publikaci katalogu služeb včetně informace o platnosti služby (katalog služeb publikuje ISZR).

6.4.4. Nakládání s vícenásobnými odpověďmi

Voláním služby může agenda získat více odpovědí. **Počet předaných odpovědí je omezen definicí služby**, přičemž platí:

- Počet povolených odpovědí nesmí překročit **legislativní omezení.**
- Počet povolených odpovědí pro synchronní volání nesmí překročit **technické omezení.**

V případě existence většího počtu odpovědí, než je maximálně předávaný počet, je agenda o tomto faktu informována. AIS může zpřesnit volání služby tak, aby dosáhl synchronní odpovědi. ISZR může automaticky převést synchronní volání na asynchronní (přechod způsobu zpracování oznamuje IZSR AIS návratovým kódem).

6.4.5. Užití služeb

Je podmíněno Žádostí o registraci užívání služby (na základě výběru služeb z katalogu eGON služeb základních registrů nebo definici nové služby – vede k vytvoření a zavedení nové služby). Obsahuje:

- Seznam rolí, které budou službu užívat.
- Šifrovací klíč – veřejnou část.
- Popis požadovaného SLA – na základě výběru/odvození z nabízených SLA základních registrů.

6.4.6. Služby AIS, které poskytuje ostatním agendám

Základní registry provádí zprostředkování eGON služeb mezi jednotlivými AIS. Tyto služby umožní získat i jiné než referenční údaje přímo z agendy, která je zodpovědná za správu a vedení těchto údajů.

Každý registrovaný AIS může registrovat své eGON služby, které bude poskytovat jiným agendám prostřednictvím ISZR. Tato registrace je možná pouze v případě, že existuje jednoznačné místo poskytování služby (kód agendy, která je registrována pro komunikaci se ZR a splňuje definované technické podmínky pro poskytování služby).

Speciálním případem jsou služby poskytované AIS, které plní roli editorů referenčních údajů. Tyto AIS budou poskytovat následující služby:

- Historická data o editovaném prvku (v základních registrech je uložen pouze aktuální údaj).
- Služby pro podporu procesu reklamace (zpracovávají požadavek na opravu/zpochybnění referenčního údaje).

Výsledkem registrace agendy je vytvoření jednoho či více záznamů do katalogu oprávnění (perzistence v RPP), který obsahuje:

- Kód agendy.
- Kód služby.
- Role.
- Stav (oprávnění je či není platné z časového hlediska).

Pro každou roli agendy využívající jednu službu je v katalogu oprávnění vytvořen právě jeden záznam.

6.4.7. Rušení služeb

- Podnět pro zrušení dává **poskytovatel služby.**
- Podle katalogu oprávnění jsou informovány dotčené agendy.
- Zapíše se do katalogu datum ukončení platnosti.
- Služba je od data ukončení platnosti neaktivní (nebude nadále publikována v katalogu základních registrů), ale nebude fyzicky zrušena (audit, reklamace atd.).

Katalog služeb má historii definice služeb (je tedy možné dokladovat, jak se definovaly a prováděly služby ZR v minulosti).

6.5. Priorizace a separace služeb

6.5.1. Výchozí předpoklady

Služby poskytované systémem Základních registrů na vnějším rozhranní budou dodávány s různou dostupností a definovanou dobou odezvy (SLA).

Základním předpokladem je, že uživatelé (AIS) budou vytvářet v převážné většině požadavky na služby pro výdej informací ze systému Základních registrů (čtení). Ostatní provoz včetně četnosti požadavků na změnu referenčních údajů bude podle předpokladu minoritní (editace). Z toho vyplývá, že požadavky na výdej informací musí být vyřizovány s podstatně kratší dobou odezvy.

Lze očekávat, že subjektivní i objektivní vyhodnocení činnosti (rychlost) Základních registrů uživateli bude vyhodnocováno právě z odezvy a průchodnosti systému pro služby vydávající informace pro uživatele.

6.5.2. Separace služeb

Základním nástrojem pro zajištění úrovně dodávaných služeb je oddělené řízení zpracování služeb a odpovídající logiky na dvou úrovních:

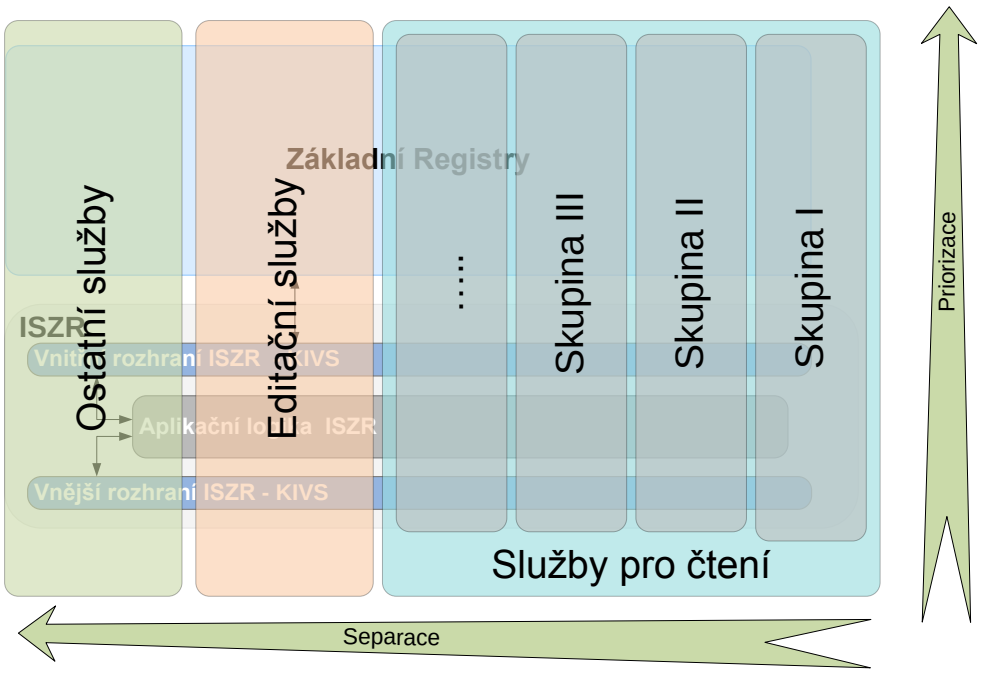
- **Oddělení služeb pro publikaci údajů od editace referenčních údajů** – služby pro výdej údajů ze Základních registrů musí být zpracovány pomocí oddělené logiky ISZR i jednotlivých Základních registrů. Využívání jiných služeb tedy nesmí v žádné své části ovlivnit tyto služby. Konkrétní realizace tohoto oddělení je závislá na použité hardwarové a softwarové implementaci ISZR a jednotlivých Základních registrů.
- **Rozdělení skupin služeb pro čtení publikaci údajů –** služby pro čtení údajů budou rozděleny do skupin podle předpokládané frekvence využití uživateli nároků na dobu odezvy těchto služeb. Jednotlivé skupiny musí být v rámci logiky ISZR i jednotlivých Základních registrů odděleny tak, aby nedocházelo k vzájemnému ovlivňování dodávky služeb mezi těmito skupinami. Konkrétní realizace tohoto oddělení je závislá na použité hardwarové a softwarové implementaci ISZR a jednotlivých Základních registrů.

Důsledkem separace služeb je nutnost rozdělení logiky ISZR a Základních registrů včetně odpovídajících částí vnějšího a vnitřního rozhranní tak, aby nedocházelo k ovlivňování SLA jednotlivých skupin služeb. V případě zavedení další skupiny služeb je nutné postupovat podle téhož principu.

6.5.3. Priorizace služeb

V rámci jedné skupiny služeb budou dále jednotlivé služby priorizovány podle požadavku na SLA jednotlivých služeb. Tato priorizace je součástí definice služby a musí být zajištěna pro danou službu v celém systému Základních registrů.

Priorizace služeb v rámci jedné skupiny nesmí mít žádný vliv na dodávku služeb a jejich priorizaci v rámci ostatních skupin.



7. Zajištění bezpečnosti systému Základních registrů / Bezpečnostní architektura

7.1. Základní východiska

Bezpečnostní architektura systému je navržena jako „koordinace bezpečnosti“, která bude mít jeden společný metodicko-procesní základ, z nějž budou odvozována závazná pravidla a požadavky pro řešitele všech dílčích subsystémů Základních registrů, kteří se budou pohybovat v tomto definovaném rámci s možností přístupu k řešení bezpečnosti podle specifických potřeb. Tento koncept bezpečnosti formou „koordinace bezpečnosti“ umožní vytvořit jednotně koordinovaný proces pro návrh, implementaci a provozování „bezpečnosti“ systému Základních registrů díky sledu vzájemně provázaných dílčích aktivit, které bezezbytku pokryjí všechna identifikovaná rizika systému Základních registrů, jak z pohledu celku, tak i v požadovaném detailu. Tuto „koordinaci bezpečnosti“ zajistí pracovní skupina bezpečnosti systému ZR, do které jmenují své zástupce organizace, které budou provádět implementaci jednotlivých subsystémů a tedy i řešení bezpečnosti všech subsystémů.

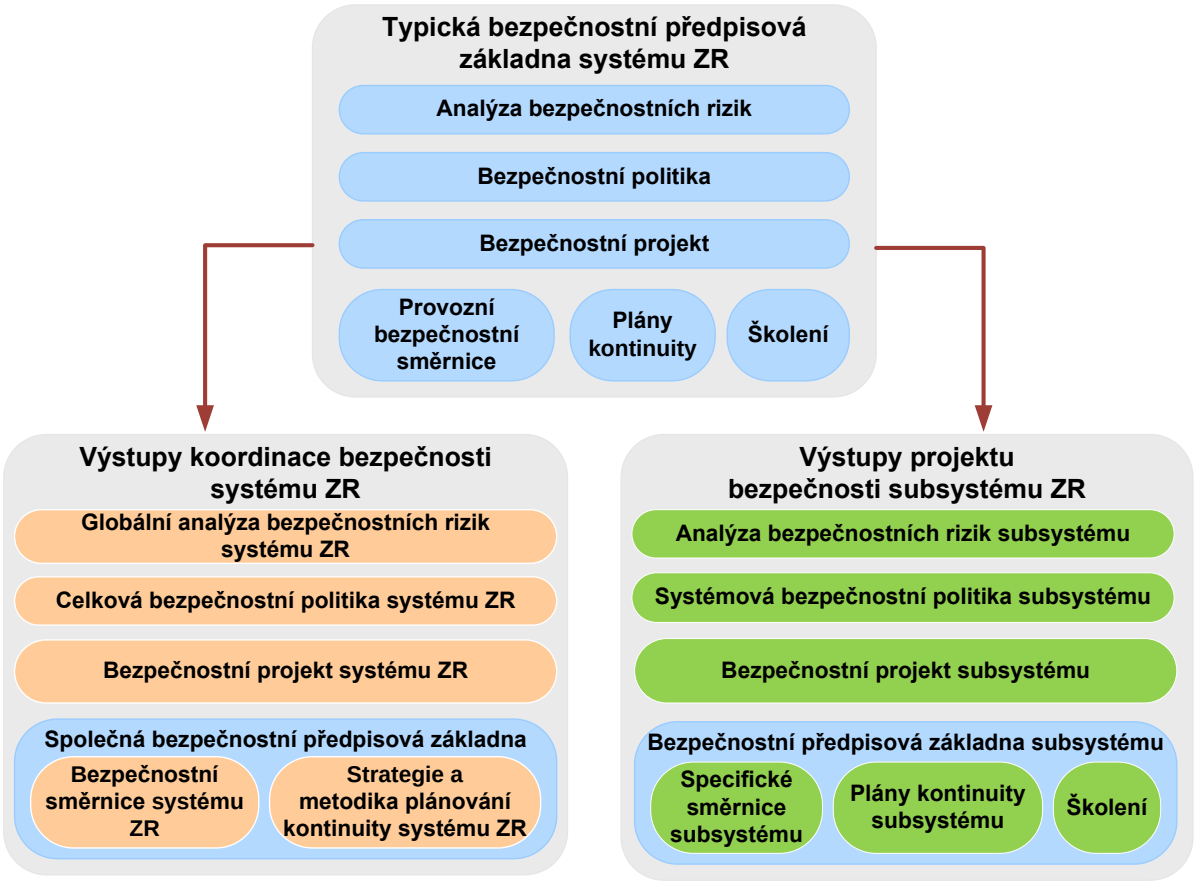
7.2. Cíle

- Bezpečnost je nutné prosadit do všech fází životního cyklu systému Základních registrů,
- Vytvořit a nasadit „Bezpečnostní projekt“ pro celý systém Základních registrů,
- Řešit detailní bezpečnost v dílčích Registrech a ISZR individuálně podle specifických potřeb, ale podle stejných pravidel a pod stejnou metodikou, odvozených z Bezpečnostního projektu,
- Uplatňovat jednotný „bezpečnostní projektový/implementační dohled“ nad činnostmi řešitelů jednotlivých částí systému Základních registrů, rizika identifikovat a ošetřovat ve vzájemných souvislostech,
- Z procesu jednotně řízené „implementace bezpečnosti“ půjdou snáze definovat vzájemně provázaná, společná i dílčí pravidla a politiky pro následnou „údržbu bezpečnosti“ jednotlivých subsystémů Základních registrů při provozu.

7.3. Souhrnný popis

Komplexnost požadavků kladených na Základní registry a nezbytnost prosazení jednotné úrovně bezpečnosti všech subsystémů Základních registrů vyžaduje koordinovat procesy řešení bezpečnosti systému Základních registrů společné pro všechny řešitele.

Struktura rozdělení aktivit řešení bezpečnosti systému Základních registrů je znázorněna na následujícím schématu:



Vysvětlivky pojmů k předchozímu obrázku:

- Bezpečnostní projekt – výstupní dokument (součást předpisové základny);
- Bezpečnostní projekt systému ZR - výstupní dokument z koordinace bezpečnosti systému ZR;
- Projekt bezpečnosti subsystému ZR – souhrn činností souvisejících s řešením bezpečnosti jednotlivých subsystémů;
- Bezpečnostní projekt subsystému – výstupní dokument z projektu bezpečnosti subsystému.

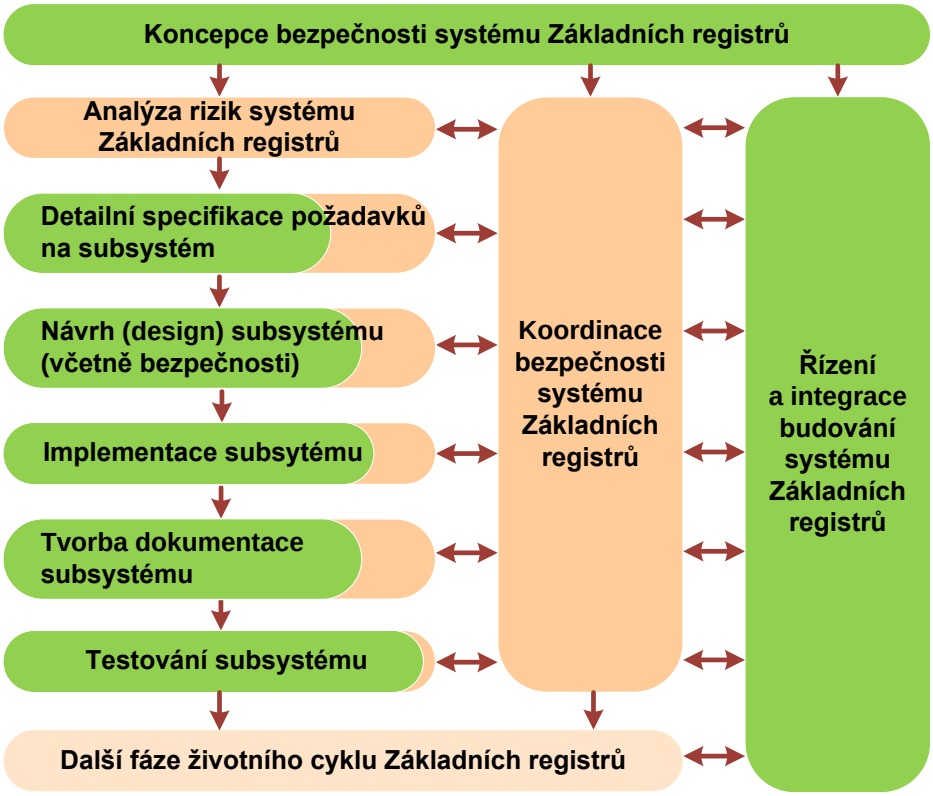
Hlavní předností uvedeného pojetí je ucelené a efektivní provedení činností na úrovni analýzy rizik bezpečnosti informací (dále jen „analýza rizik“), přípravy bezpečnostních specifikací subsystémů ISZR (bezpečnostní profily) a přípravy společné provozní bezpečnostní dokumentace a předpisové základny. Současně s tím bude zajištěna celková integrita bezpečnostní dokumentace vytvářené jednotlivými řešiteli prostřednictvím supervize jejího zpracování.

7.4. Koncepce procesu řešení bezpečnosti systému Základních registrů

Řešení bezpečnosti systému Základních registrů v průběhu celého životního cyklu se opírá o přípravu a údržbu bezpečnostního profilu systému Základních registrů a bezpečnostních profilů jeho jednotlivých subsystémů, které definují bezpečnostní cíle a vymezené bezpečnostní požadavky a mechanismy, včetně požadavků na specifickou bezpečnostní dokumentaci, na bezpečnostní dohled nad změnami systému a požadavků na audit a testování celého systému.

7.4.1. Působnost koordinace bezpečnosti systému Základních registrů

Navrhované pojetí koordinace bezpečnosti pro systém Základních registrů a její zapojení do celkového rámce řízení bezpečnosti projektu ZR znázorňuje následující schéma:



7.5. Struktura koordinace bezpečnosti systému Základních registrů

Účinné prosazení a řízení bezpečnosti (návrh, prosazení, řízení a údržba) systému Základních registrů předpokládá průběžný dohled nad bezpečností systému v rámci celého jeho životního cyklu. V rámci životního cyklu systému Základních registrů lze z hlediska bezpečnosti vymezit:

- Fáze návrhu a implementace systému Základních registrů, v rámci níž musí být navržen a při implementaci prosazen a ustaven efektivní bezpečnostní rámec.
- Fáze provozu a užívání systému Základních registrů, v rámci níž musí být stanovený bezpečnostní rámec sledován, udržován a dále přizpůsobován zejména v souvislosti se změnami cílového systému.

Koordinace bezpečnosti systému Základních registrů se vztahuje k vlastnímu budování systému Základních registrů (tedy fázi „návrh a implementace“ životního cyklu systému) a je navrhována v následujících krocích:

- **Příprava Bezpečnostního projektu** zahrnujícího analýzu bezpečnostních aspektů celého projektu ZR včetně stanovení bezpečnostních cílů a analýzy rizik, návrh efektivních bezpečnostních opatření ve formě specifikace bezpečnostních funkcí a návrh realizace bezpečnostních funkcí ve formě specifikace a postupu realizace bezpečnostních mechanismů na úrovni jednotlivých řešitelů.
- **Bezpečnostní projektový dohled** zahrnující dohled nad realizací a prosazováním bezpečnostních funkcí a bezpečnostních mechanismů v souladu s obsahem Bezpečnostního projektu systému Základních registrů.
- **Příprava konzistentní provozní bezpečnostní dokumentace**, která bude sloužit provozovatelům jednotlivých částí systému jako podklad pro nastavení procesů provozu systému Základních registrů.

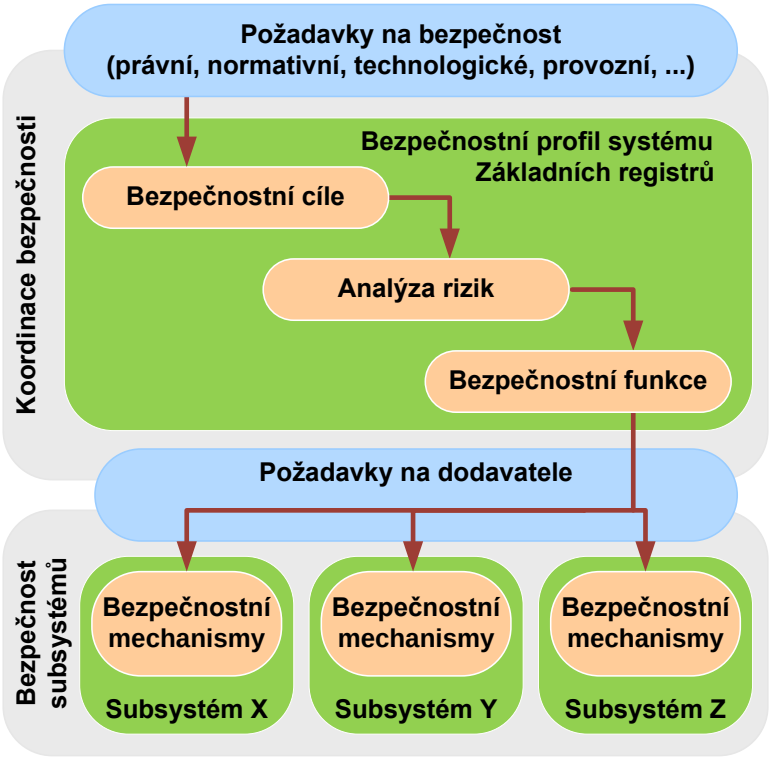
Jako navazující krok je doporučen:

- **Závěrečný bezpečnostní audit řešení** za účelem ověření funkčnosti bezpečnostních funkcí a bezpečnostních mechanismů včetně jejich prosazení do relevantních interních procesů provozovatele v souladu s Bezpečnostním projektem systému Základních registrů.

Ve fázi provozu systému Základních registrů pak bude zajištěno:

- **Řízení a údržba bezpečnosti při provozu systému** zahrnující zejména udržení souladu stavu bezpečnost s bezpečnostními požadavky prostředí a udržení souladu stavu bezpečnosti s bezpečnostními potřebami systému Základních registrů v souvislosti s jeho změnami prováděnými v rámci jeho provozu a užívání.

Jednotlivé složky, jejich návaznosti a postup realizace bezpečnosti systému Základních registrů jsou znázorněny na následujícím schématu (popis jednotlivých kroků a složek řešení je uveden v podkapitolách následujících za schématem).



7.6. Příprava bezpečnostního projektu systému Základních registrů

Cílem přípravy bezpečnostního projektu bude zpracovat souhrnný podkladový dokument **Bezpečnostní projekt** systému Základních registrů popisující postup a výsledky analýzy rizik, přehled posuzovaných bezpečnostních opatření, přehled a odůvodnění bezpečnostních opatření vybraných k realizaci, a postup a způsob realizace bezpečnostních opatření.

V rámci Bezpečnostního projektu systému Základních registrů budou stanoveny bezpečnostní požadavky, provedena analýza rizik, navržena bezpečnostní opatření a zajištěna jejich realizace příslušnými řešiteli tak, aby byly splněny požadavky zákona č. 101/2000 Sb., v platném znění, dalších relevantních předpisů.

7.6.1. Analýza požadavků systému Základních registrů

Účelem analýzy požadavků na bezpečnost systému Základních registrů je stanovení bezpečnostních cílů. Pro stanovení bezpečnostních cílů je určující účel a role IT systémů Základních registrů spolu s možnostmi jejich vývojového a

provozního prostředí. Bezpečnostní cíle musí být stanoveny ve vazbě na hodnoty aktiv a služeb IT systémů a na bezpečnostní charakteristiky jejich prostředí.

Bezpečnostní požadavky jsou základem pro další práce při návrhu a realizaci systému a musí být odsouhlaseny na vrcholové úrovni projektu ZR.

7.6.2. Analýza rizik Základních registrů

V rámci analýzy rizik budou identifikovány jednotlivé hrozby, které by mohly využít zranitelnosti systému a mohly by mít negativní dopad na činnost systému Základních registrů, proto rozsah analýzy rizik nepokrývá všechna rizika provozovatele systému. U zjištěných rizik bude kvalitativně ohodnocena míra pravděpodobnosti výskytu nechtěné události, popsán jejich možný dopad na aktiva zúčastněných subjektů a činnost jednotlivých subsystémů.

7.6.3. Návrh bezpečnostních opatření

Pro naplnění bezpečnostních cílů a snížení bezpečnostních rizik by měla být zavedena vyvážená kombinaci technických a netechnických bezpečnostních opatření pro IT systémy. Vhodná bezpečnostní opatření mohou předejít, omezit, nebo zabránit uplatnění hrozby, jež by mohla poškodit činnost systému Základních registrů.

Opatření budou rozdělena na dvě skupiny: jednu představující zadání pro řešitele systémů, a druhou představující požadavky na prostředí, ve kterém bude systém provozován (do té budou současně promítnuty všechny předpoklady o bezpečnosti prostředí).

Druhá skupina bude zahrnovat opatření, na jejichž existenci budou spoléhat bezpečnostní opatření implementovaná v informačním systému (příkladem může být pravidelná analýza auditních záznamů), i opatření, která budou chránit před hrozbami (omezovat rizika), proti kterým nebudou opatření implementovaná v IS účinná (příkladem může být zajištění spolehlivé dodávky elektrické energie kombinací UPS a generátoru).

7.6.4. Detailní specifikace bezpečnostních požadavků

Detailní specifikace bezpečnostních požadavků bude představovat zadání pro řešitele subsystémů systému Základních registrů. Tato zadání budou obsahovat upřesněné a konkretizované znění požadavků na bezpečnostní funkce, na záruky bezpečnosti a vývojové bezpečnosti stanovené v Bezpečnostním profilu systému Základních registrů. Důležitou částí specifikace bezpečnostních požadavků na subsystém je stanovení struktury a obsahu bezpečnostní dokumentace pro subsystém, který bude daný řešitel realizovat.

7.6.5. Postup realizace bezpečnostních požadavků

Cílem tohoto kroku je stanovit projektové parametry prosazení bezpečnosti, tj. upřesnit organizaci, metodiku řízení, projektové postupy a harmonogram Bezpečnostního projektu systému Základních registrů.

7.7. Řešení bezpečnosti subsystémů systému Základních registrů

7.7.1. Analýza požadavků

Budou analyzovány specifické bezpečnostní požadavky na daný subsystém Základních registrů, pokud existují. Na jejich základě budou stanoveny specifické bezpečnostní cíle, mj. jako vstupy pro analýzu rizik subsystému.

Specifické bezpečnostní cíle jsou základem pro další práce při návrhu a realizaci daného subsystému a musí být odsouhlaseny na vrcholové úrovni projektu ZR.

7.7.2. Analýza rizik subsystému

Pro daný subsystém bude vypracována analýza bezpečnostních rizik subsystému, která se bude zabývat zejména riziky souvisejícími se specifickými bezpečnostními cíly (pokud existují) a s konkrétním prostředím provozovatele subsystému.

Analýza rizik bude provedena podle jednotné metodiky pro všechny subsystémy stanovené v rámci koordinace bezpečnosti.

7.7.3. Návrh bezpečnostních opatření a jejich realizace

Na základě analýzy rizik a detailní specifikace bezpečnostních požadavků na subsystém bude vytvořen detailní návrh bezpečnostních opatření pro subsystém. I tento soubor bezpečnostních opatření bude rozdělen do dvou částí: požadavky na prostředí a opatření, která budou implementována v daném subsystému a při jeho vývoji.

Pro opatření, která budou implementována v daném subsystému a při jeho vývoji, bude navržena jejich realizace.

7.7.4. Implementace bezpečnostních opatření

Bezpečnostní požadavky budou implementovány do architektury a realizace subsystému i do procesu (a prostředí) jeho vývoje.

7.7.5. Vytvoření bezpečnostní dokumentace

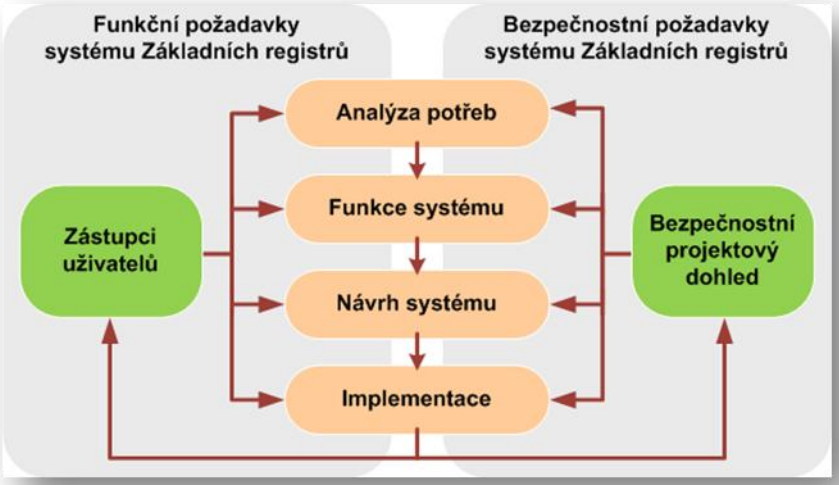
Pro každý subsystém bude podle centrálně stanovených zásad vytvořena příslušná provozní bezpečnostní dokumentace.

7.8. Bezpečnostní projektový dohled systému Základních registrů

Nástrojem k prosazení potřebné míry bezpečnosti IT systémů, zejména v oblasti záruk, je definovaný a řízený bezpečnostní projektový dohled, který zajistí pracovní skupina bezpečnosti systému ZR.

Pokud nebudou stanoveny v rámci řízení celého projektu ZR, budou v rámci bezpečnostního projektového dohledu stanoveny následující řídící procedury:

- Sledování postupu projektu
- Zajištění kvality a strategie ověřování
- Řízení problémů
- Řízení změn
- Konfigurační řízení



7.9. Testování subsystémů

Budou provedeny následující bezpečnostní testy:

- **Prověření konfigurace systému** (prověření shody s definovanými bezpečnostními požadavky popisujícími bezpečnostní vlastnosti a bezpečnostní parametry standardních komponent systému)
- **Prověření bezpečnostních funkcí systému** (prověření shody s definovanými bezpečnostními požadavky popisujícími žádoucí bezpečnostní chování systému)
- **Ohodnocení zranitelností systému** (investigativní test)

7.10. Provozní bezpečnostní dokumentace

Jelikož systém bude provozován více subjekty, je nutné, aby provozní bezpečnostní dokumentace byla konzistentní.

V rámci implementace budou vypracovány základy následujících dokumentů provozní bezpečnostní dokumentace:

- **Systémová bezpečnostní politika** – společná pro všechny součásti systému Základních registrů
- **Systémové bezpečnostní politiky** - jednotlivých subsystémů (pokud bude vhodné detailněji řešit specifika některé komponenty systému Základních registrů)
- **Bezpečnostní směrnice pro činnosti správců**
- **Havarijní plán systému Základních registrů a jednotlivých subsystémů**

Zároveň bude také nastaven způsob aktualizace těchto dokumentů tak, aby byla stále zachována jejich vzájemná konzistence u jednotlivých provozovatelů systému Základních registrů.

7.11. Řízení a údržba bezpečnosti při provozu systému ISZR

Udržení a rozvoj bezpečnostního rámce systému Základních registrů vyžaduje řízení a údržbu systému bezpečnosti také po skončení projektu systému Základních registrů, resp. po ukončení fáze „návrh a implementace“ životního cyklu systému Základních registrů. To zahrnuje zejména následující cíle:

- udržení souladu stavu bezpečnost s bezpečnostními požadavky prostředí,

- udržení souladu stavu bezpečnost s bezpečnostními potřebami systému Základních registrů v souvislosti s jeho změnami v rámci jeho provozu a užívání.