INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA
CESKE REPUBLIKY

GLOBÁLNÍ ARCHITEKTURA ZÁKLADNÍCH REGISTRŮ

DOPLNĚK

Projekt „Informační systém základních registrů“ je spolufinancován Evropskou unií z Evropského fondu pro regionální rozvoj.

Obsah

1 Cíle dokumentu

Tento dokument byl připraven jako dodatek dokumentu „Globální architektura základních registrů“, který je součástí zadávací dokumentace pro všechny veřejné zakázky na součásti základních registrů jako příloha 1a:

- VZ 60026134 „Informační systém základních registrů CZ.1.06/1.1.00/03.05891“(Implementace informačního systému)
- VZ 60026100 „Registr práv a povinností CZ 1.06/1.1.00/03.05890“ (Implementace informačního systému)
- VZ 60026098 „Registr obyvatel CZ 1.06/1.1.00/03.05889“ (Implementace informačního systému)

Cílem dokumentu je uvedení dodatečných informací, které zpřesňují původní dokument tak, aby uchazeči mohli podávat srovnatelné nabídky. Dokument vychází ze současného stavu rozpracování detailních architektur jednotlivých součástí základních registrů.

V tomto dodatku nejsou popisovány pojmy, principy a údaje uvedené v dokumentu „Globální architektura základních registrů“ ani v dokumentech „Globální architektura Registru práv a povinností“, „Globální architektura ROB“, „Globální architektura ROS“ a „Globální architektura RUIAN“. Z těchto dokumentů dodatek vychází a je tedy jejich nedílnou součástí.

2 Funkční dekompozice

2.1 Rozdělení rolí Editační AIS a Základní registry

V základních registrech jsou uchovávána referenční data. Je nutné zdůraznit, že v rámci základních registrů žádná referenční data nevznikají ani není udržována historie těchto referenčních dat. Pro veškerá data uložená v základních registrech musí existovat editační AIS. Tento editační AIS je zodpovědný za uložení referenčních údajů do základních registrů. Role jednotlivých částí jsou tedy následující:

- **Editační AIS -** pro jednotlivý registr může existovat i více editačních AIS. V rámci editačních AIS jsou vytvářeny odpovídající údaje po celý jejich životní cyklus. Jestliže editační AIS má k dispozici údaje, které mají být uloženy v základních registrech, pak tyto údaje zapíše pomocí eGON služeb do základních registrů. **Editační AIS je tedy zodpovědný za správnost referenčních údajů**
- **Základní registr -** slouží „pouze“ k uložení a publikaci referenčních údajů. Nezkoumá jejich věcnou správnost ani je nevytváří. Základní registr ověřuje pouze správnost pravidel vydaných daným registrem (datové typy, vztahy mezi datovými prvky apod.)
- **Referenční rozhraní –** rozhraní, na kterém jsou poskytovány referenční údaje uživatelům (referenční odkazy jsou standardně nahrazeny referenčními údaji)
- **ISZR –** slouží jako referenční rozhraní. Nezkoumá správnost přenášených dat ani je neukládá. Ukládá logy o využívání údajů v základních registrech a jednosměrně šifrované kopie vstupních a výstupních zpráv pro účely auditu (provoz ISZR není schopen zašifrované údaje přečíst, tuto schopnost má pouze audit)
    - Na vnějším rozhraní poskytuje eGON služby základních registrů. Toto rozhraní je referenční
    - Na vnitřním rozhraní poskytují jednotlivé registry služby, které může konzumovat pouze ISZR. Toto rozhraní není referenční

Existuje více metod pro jednosměrné šifrování. Jednou z metod je taková, kdy ISZR šifruje data veřejným klíčem a audit vlastní pouze soukromý klíč. V tomto případě nemůže ISZR dále číst šifrovaná data a audit nemůže vytvářet a tedy ani měnit šifrovaná data. Konkrétní návrh implementace tohoto požadavku je očekáván od uchazeče o implementaci.

Pro některé základní registry existují role primární a sekundární editor. Toto rozdělení není tedy univerzálně platné a je specifikováno v globálních architekturách jednotlivých registrů.

- **Primární editor** – editační AIS je oprávněn vytvářet nový záznam (např. novou osobu)
- **Sekundární editor** – editační AIS je oprávněn vytvářet referenční údaj u existujícího záznamu (např. číslo občanského průkazu)

Jednotlivý základní registr musí vnitřními procesy zajistit konzistenci dat vzhledem k editorům tohoto registru, a pokud má definovány role primárních a sekundárních editorů, pak musí zajistit izolaci záznamů mezi primárními editory.

Konkrétní požadavky tohoto typu jsou uvedeny v Globální architektuře jednotlivých registrů a budou detailizovány v detailních architekturách jednotlivých registrů.

Každý referenční údaj má tedy přesně definováno, kdo je jeho editorem a pouze a jen tento editor může referenční údaj změnit. V případě zpochybnění tohoto údaje je nastartován pro-

ces reklamace a pouze tento editor může údaj označit za „nesprávný údaj“ do doby vyřízení reklamace.

Primárním účelem základních registrů je poskytování referenčních údajů pro všechny informační systémy veřejné zprávy s ohledem na jejich oprávnění k přístupu. Účelem tedy není změna referenčních údajů v reálném čase na úkor konzistence vydávaných referenčních údajů.

Každá změna údaje v editačním AIS se tedy nemusí okamžitě promítat do změny referenčního údaje v systému Základních registrů. Publikace nové hodnoty údaje jako referenčního spočívá v celém procesu (validace v rámci editačního AIS, přenos do systému základních registrů, potvrzení úspěšného zápisu, uvolnění k publikaci), který je nutné dodržet pro zajištění konzistence dat.

Naopak při výdeji referenčních údajů nesmí nastat situace, kdy jsou pro jeden referenční údaj vydávány různé hodnoty v závislosti na vnitřním stavu a logice systému základních registrů.

2.2 Rozdělení rolí ISZR a RPP

Požadavkem zadavatele je, že Informační systém základních registrů (ISZR) poskytuje referenční rozhraní pro přístup k základním registrům. ISZR poskytuje komplexní eGON služby nad základními registry oprávněným subjektům s ohledem na jejich aktuální oprávnění v Registru práv a povinností.

V Registru práv a povinností (RPP) jsou dle zákona 111/2009 Sb. vedeny referenční údaje o agendách orgánů veřejné moci a to včetně údajů o oprávněních přístupu k datům vedeným v základních registrech a seznamu názvů agend a jejich číselných kódů. V registru jsou dále vedeny referenční údaje o právech a povinnostech fyzických a právnických osob a právech a povinnostech k věcem, pokud jsou údaje o těchto osobách a věcech vedeny v základních registrech, a to včetně údajů o rozhodnutích orgánů veřejné moci.

Z hlediska bezpečnosti provozu základních registrů je činnost ISZR a RPP oddělena následovně:

- ISZR nemá přímý přístup k referenčním údajům uloženým v jednotlivých základních registrech, tedy ani v RPP. ISZR není oprávněn požadovat referenční údaje z jednotlivých základních registrů mimo zprostředkování volání eGON služeb. ISZR není oprávněn k jejich ukládání.
- RPP nemá přístup k procesům probíhajícím v rámci ISZR. Nezná tedy obsah jednotlivých zpráv zpracovávaných v rámci ISZR.

Správci ISZR a RPP musí být odděleni z hlediska personálního i procesního. Jen tímto způsobem je možné zajistit, že neexistuje jeden bod, ve kterém je možné sloučení referenčních a provozních dat za účelem jejich zneužití.

2.2.1 Referenční a řídící část RPP

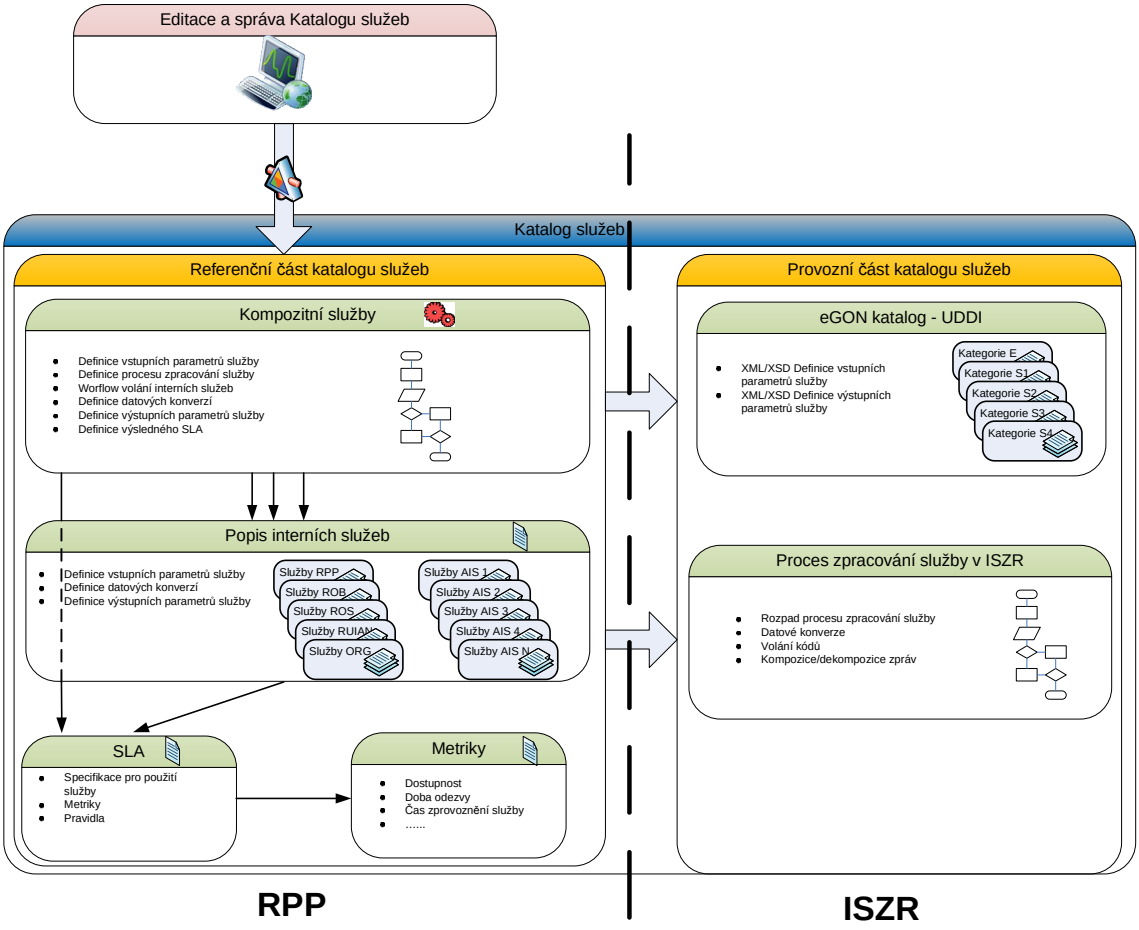
RPP má výjimečné postavení z hlediska globální architektury základních registrů. Z pohledu této globální architektury obsahuje dvě základní oblasti dat

- **Referenční data –** z tohoto pohledu se jedná o „standardní“ základní registr

- **Řídící data -** data odvozená od referenčních dat (viz. následující obrázek). Tato data jsou předávána ISZR pro výkon jeho činnosti

Z výše uvedeného rozdělení je zřejmé rozdělení zodpovědnosti ISZR a RPP za proces zpracovávání požadavků jednotlivých uživatelů (Agendových informačních systémů – AIS – agend orgánů veřejné moci).

Toto rozdělení zodpovědnosti je možné ilustrovat na následujícím schématu pro Katalog služeb:



Referenční část katalogu služeb je uložena v RPP a je spravována externím AIS, pomocí kterého je prováděn celý životní cyklus dat uložených v katalogu služeb. Tento AIS pracuje stejně jako jakýkoliv Editační AIS. Používá tedy publikované eGON služby základních registrů pro vkládání, editaci a rušení referenčních dat v RPP.

Pro zahájení provozu je nutné Referenční část katalogu služeb naplnit prvotními údaji tak, aby činnost tohoto editačního AIS mohla být zahájena (základní služby, referenční údaje a oprávnění pro přístup editačního AIS).

Provozní část katalogu služeb je vytvářena na základě referenční části pomocí řídící části RPP a je publikována pro ISZR s použitím interní služby na vnitřním rozhraní ISZR. Tyto služby tedy může konzumovat pouze ISZR. Výsledkem je, že ISZR získá následující data

- **eGON katalog -** katalog služeb, který po transformaci zveřejňuje na vnějším rozhraní ISZR ve formě UDDI. eGON katalog obsahuje pouze eGON služby publikované na vnějším rozhranní ISZR. Neobsahuje vnitřní služby základních registrů (služby publikované jednotlivými základními registry a spolupracujícími AIS, jejichž konzumentem je pouze ISZR) ani dekompozici eGON služeb na vnitřní služby. eGON katalog obsahuje veškeré údaje nutné pro užívání eGON služeb uživateli a pouze tyto údaje
    - **WSDL** popisující službu
    - **XML/XSD** definice vstupních parametrů služby
    - **XML/XSD** definice výstupních parametrů služby
    - **Endpoint,** kde je služba poskytována
    - **Umístění dokumentace** služby
    - **Další případné údaje nutné pro konkrétní použitou technologii**
- **Proces zpracování služby –** informace pro ISZR, jak má zpracovávat konkrétní službu. V rámci tohoto popisu získá ISZR následující údaje
    - **Dekompozice eGON služby na vnitřní služby –** workflow procesu zpracování služby
    - **Datové konverze –** nutné v jednotlivých krocích pro transformaci vstupních parametrů služby při dekompozici
    - **Volání kódů -** které zajišťují výkon jednotlivých kroků procesu zpracování služby
    - **Kompozice/dekompozice zpráv –** popisující, jak je nutné dekomponovat přijaté zprávy (volání služby) pro účely zpracování služby, jak jsou vytvářeny zprávy (volání služby) pro interní služby a jak je komponována výsledná zpráva (odpověď na volání eGON služby)

Z uvedeného popisu je zřejmé, že RPP je zodpovědný za věcný obsah provozní části katalogu služeb a za proces aktualizace této provozní části tak, aby odpovídala referenční části katalogu služeb. ISZR je zodpovědný za výkon služeb podle obsahu této provozní části katalogu služeb.

Vzhledem k faktu, že ISZR a RPP budou implementovány různými subjekty, nelze detailně předjímat konkrétní realizaci výše uvedených požadavků, jelikož toto provedení bude závislé na způsobu řešení. Technologie realizace je navrhována implementátorem, nikoliv architektem. V rámci realizace je nutné provést synchronizaci návrhů implementátorů ISZR a RPP tak, aby tyto požadavky byly naplněny.

Požadovanou úrovní standardizace je, aby RPP poskytoval Web Services podle standardů WS-* popsaných v globální architektuře, jejichž konzumentem bude ISZR. Na základě volání těchto služeb pak ISZR získá požadované informace a je zodpovědný za výkon eGON služeb. ISZR nesmí nabízet a zpracovávat služby, které by nebyly definovány v provozní části katalogu služeb dodané RPP.

2.2.2 Matice oprávnění

Matice oprávnění je pojem popisující datovou strukturu, která udržuje stav oprávnění přístupu k eGON službám základních registrů. Pojem matice je zjednodušující pro účely globální architektury.

V rámci referenční části RPP jsou uchovávány tyto datové struktury nutné pro vytváření matice oprávnění:

- Referenční odkazy na orgány veřejné moci (OVM). Referenční údaje o OVM jsou dle zákona 111/2009 Sb. vedeny v registru osob
- Referenční data agend orgánů veřejné moci (Agenda)
- Referenční data agendových informačních systémů (AIS)
- Referenční data rolí v rámci agendových informačních systémů (Role)

Tyto referenční údaje jsou pak využívány řídící částí RPP pro vytváření provozní části matice oprávnění. Tato matice oprávnění obsahuje již údaje nutné pro ověření oprávnění přístupu k eGON službě. Tyto údaje jsou:

- OVM
- Agenda
- AIS
- Role
- Kód služby
- Oprávnění – ANO/NE

Provozní část matice oprávnění je poskytována ISZR pro výkon eGON služeb. ISZR v rámci přijetí požadavku na eGON službu na vnějším rozhraní provede kontrolu, zda kombinace poskytnutých údajů (OVM, Agenda, AIS, Role, Kód služby) je povolena či nikoli. Požadavek na zpracování eGON služby je pak následně předán na další zpracování nebo odmítnut.

Rozdělení zodpovědnosti je tedy obdobné, jak bylo uvedeno v popisu Katalogu služeb. RPP je tedy opět zodpovědný za vytváření a údržbu referenčních údajů (pomocí externího editačního AIS) a následně je v řídící části vytvářena provozní část matice oprávnění. ISZR je poskytnut přístup k údajům v matici oprávnění pro výkon eGON služeb.

Minimálním požadavkem tedy je, že RPP poskytuje ISZR WS-* službu, kterou ISZR využívá pro ověření oprávněnosti volání eGON služby.

3 Technologická architektura

Technologická architektura je v rámci Globální architektury uvedena pouze rámcově s důrazem na požadovanou funkcionalitu a požadované standardy, které řešení musí splňovat. Zadavatel nepreferuje konkrétní technologii a způsob řešení.

3.1 Fyzické umístění

V současné době není jednoznačně rozhodnuto o fyzickém umístění jednotlivých komponent systému základních registrů. S vysokou pravděpodobností lze předpokládat, že následující komponenty budou umístěny v rámci jednoho datového centra (myšleno obě datová centra pro zajištění požadované dostupnosti):

- ISZR
- RPP
- ROB
- ROS

Předpokládáme, že tímto datovým centrem bude existující Centrální místo služeb (CMS) a jeho další rozvojová verze.

Ostatní komponenty budou umístěny v oddělených datových centrech. Jako součást Globální architektury jsou následně uvedeny požadavky na propojení těchto lokalit (prostřednictvím Komunikační infrastruktury veřejné správy – KIVS) tak, aby byla zajištěna požadovaná funkcionalita a odezva.

Vzhledem k tomu, že není definitivně určeno umístění komponent ani nejsou známy způsoby řešení jednotlivých částí uchazeči, musí Globální architektura předpokládat následující axiomy:

- Jednotlivé komponenty základních registrů mohou využívat **služby** poskytované prostřednictvím ISZR
- Jednotlivé komponenty základních registrů budou po hardwarové stránce nabídnuty jako samostatné celky

Rozpracování jednotlivých axiomů je uvedeno v následujících kapitolách.

Z hlediska maximalizace efektivity vložených nákladů a synergie celého systému základních registrů je vhodné sdílení některých komponent (služeb, hardwarových prostředků) pro činnost jednotlivých částí systému základních registrů.

V okamžiku, kdy budou známa řešení jednotlivých vítězných implementátorů, bude provedeno vzájemné sladění těchto řešení a detailních architektur jednotlivých částí základních registrů. Cílem tohoto sladění je dosažení maximální synergie jednotlivých řešení a maximalizace efektivity vložených nákladů na výstavbu celkového řešení.

3.2 Služby poskytované ISZR pro jednotlivé základní registry

V rámci implementace ISZR budou implementovány následující služby, které mohou být využívány jednotlivými základními registry:

- DNS – registruje IP adresy a jména systémů v rámci ISZR a jednotlivých základních registrů. Konkrétní tvar jmenného prostoru bude určen podle umístění systému základních registrů
- NTP – vnitřní časový server stanovující závazný systémový čas v rámci systému základních registrů. Tento server bude synchronizován se standardním externím NTP serverem (variantně v rámci lokality, kde bude systém základních registrů umístěn nebo v síti internet).
- Identity and access management – řešení pro centrální správu identit a přístupových oprávnění uživatelů v rámci systému základních registrů. Uživateli jsou myšleni správci jednotlivých komponent systému základních registrů.
- Monitoring – nástroj pro monitoring, management a audit ISZR. Tento nástroj musí být v rámci ISZR navržen tak, aby mohl být využíván jako sběrný systém pro monitorovací nástroje jednotlivých základních registrů. Musí se tedy jednat o dostatečně otevřený systém.
- PKI – V rámci ISZR musí být vybudována certifikační autorita pro vydávání osobních i systémových certifikátů s možností definice privátní šablony. Tyto certifikáty budou využívány výhradně pro vnitřní procesy systému základních registrů a pro zajištění bezpečné komunikace na vnějším rozhranní.

Dále jsou blíže specifikovány jednotlivé služby.

3.2.1 DNS

Domain name system (DNS) bude vybudován pro vnitřní potřeby systému základních registrů. ISZR neumožní navázání interního DNS na vnější prostředí ani nebude poskytovat své služby mimo systém základních registrů. Tato služba bude poskytována s vysokou dostupností v obou datových centrech. Záznamy DNS v obou datových centrech musí být identické.

Služby DNS pro vnější eGON rozhranní budou poskytovány v rámci datového centra a komunikační infrastruktury veřejné správy.

3.2.2 NTP

Časový server NTP (Network time protocol) poskytuje časový etalon systémového času pro všechny komponenty systému základních registrů. Tento server bude vybudován v rámci ISZR a slouží pro vnitřní potřeby systému základních registrů. Služba NTP serveru nebude poskytována mimo systém základních registrů, ale tento časový etalon bude synchronizován s vybranými veřejnými NTP servery.

Čas poskytovaný tímto etalonem je závazný pro všechny komponenty a poskytuje i údaje pro časová razítka vytvářená jednotlivými komponentami systému základních registrů. Nejedná se o kvalifikované časové razítko ve smyslu zákona o elektronickém podpisu. Primárním účelem časových razítek je zajištění monitoringu úrovně dodávaných služeb a interní potřeby řízení toku zpráv.

3.2.3 Identity and Access management

V rámci ISZR bude vybudován IdM systém poskytující primárně služby centrální správy identit osob pracujících na jednotlivých komponentách systému základních registrů. Každá tato osoba (správce) musí být primárně registrována v tomto centrálním IdM systému včetně užívaných účtů na jednotlivých systémech.

Z hlediska zvýšení bezpečnosti není v rámci systému základních registrů navrhován žádný systém pro centrální správu účtů. Kompromitace jednoho účtu na jednom systému tedy není propagována na ostatní systémy.

Bude pravidelně prováděna kontrola existujících účtů v jednotlivých systémech, a pokud tyto účty nebudou registrovány v centrálním IdM systému, pak budou zakázány (reconciliation).

Při vytvoření účtu v centrálním IdM systému bude tato změna propagována na jednotlivé systémy podle definovaných pravidel.

Single sign on bude podporováno IdM řešením, není však povinnost pro jednotlivé systémy využívat SSO.

Z hlediska externích systémů musí být řešení IdM připraveno pro spolupráci s existujícími systémy správy identit (musí podporovat standardy pro využití federace, Secure Token Service (STS) používající metody WS-Trust nebo WS-Federation, SAML 1.1/2.0, Kerberos, X.509 certifikáty).

Pro potřeby centrálních AIS musí poskytovat službu access managementu (předávání informací o oprávnění identity v daném AIS na základě přiřazených rolí). Nároky na tuto službu nejsou v současné době detailně známy. Návrh musí umožňovat následné rozšíření bez ztráty investic.

3.2.4 Monitoring

Systém pro monitoring a management prostředí musí odpovídat granularitě řešení. Za každou část základních registrů (ISZR, jednotlivé registry) je zodpovědný jiný subjekt. Tyto subjekty musí mít schopnost provádět vlastní dohled a správu svých řešení.

Současně je nutné provádět sběr informací potřebných pro SLA management eGON služeb.

Všechny monitorovací systémy komponent základních registrů musí tedy splňovat následující požadavky:

- Systémy pro monitoring a management ISZR musí být schopny přijímat a odesílat události a hodnoty metrik od ostatních systémů (minimálně na úrovni SNMP)
- Systémy pro monitoring a management ISZR musí být schopny výměny událostí a hodnot metrik se systémy pro monitoring a management datového centra (minimálně na úrovni SNMP)
- Systémy pro monitoring a management jednotlivých základních registrů musí být schopny předávat události a hodnoty metrik systémům ISZR (minimálně na úrovni SNMP)

Implementátor v rámci nabídky navrhne konkrétní technologii a nabízené integrační protokoly a metody pro ostatní systémy. V rámci implementace jednotlivých systémů bude následně dohodnut a přesně specifikován okruh událostí a údajů, které budou předávány mezi jednotlivými systémy včetně metod předávání.

3.2.5 PKI a Certifikační autorita

V rámci ISZR bude vybudována Certifikační autorita poskytující následující certifikáty:

- Systémové certifikáty pro AIS registrované pro komunikaci s ISZR (odhad 10000-100000 připojených AIS)
- Systémové certifikáty pro komponenty ISZR – počet certifikátů je závislý na nabídce implementátora a jím zvolených technologií
- Osobní certifikáty pro správce technologií ISZR a dílčích registrů – maximálně 1000 správců

Certifikační autorita musí být vybudována tak, aby splňovala veškeré požadavky na bezpečnost, důvěryhodnost a dostupnost řešení. Je možné předpokládat, že Certifikační autorita a objem vydaných certifikátů je téměř statický. Certifikát je vydáván pro nové AIS, které jsou registrovány pro komunikaci se systémem základních registrů, nové komponenty ISZR a pro nové správce.

Součástí nabídky implementace musí být zajištění celého životního cyklu certifikační autority a vydaných certifikátů (publikace CRL na vnějším rozhranní, změny v certifikátech, obnova certifikátů a podobně). Je však nutné vzít v úvahu, že tyto certifikáty jsou primárně používány pro systémovou komunikaci (navázání IP SSL komunikace mezi systémy a ověření klienta – AIS) jak ve vnitřním prostředí ISZR, vnitřním a vnějším rozhraní v rámci KIVS.

Vydané certifikáty nejsou užívány pro digitální podpisy ve smyslu zákona o elektronickém podpisu 227/2000 Sb. Není tedy potřeba řešit problematiku kvalifikovaného certifikátu ve smyslu tohoto zákona.

Certifikáty vydané certifikační autoritou nejsou určeny pro uživatele AIS ani pro veřejnost.

4 Procesní architektura

Pro pochopení procesní architektury je nutná přesná specifikace rolí jednotlivých subjektů, které se účastní níže popsaných procesů.

- **Uživatelé** - uživatelem základních registrů je zásadně AIS, tedy informační systém a nikoliv jednotlivý uživatel informačního systému. Jakýkoliv přístup k referenčním údajům je možný pouze prostřednictvím AIS.
- **Externí AIS** – Agendový informační systém pracující se základními registry
  - **Spolupracující AIS** – Takový externí AIS, který prostřednictvím ISZR nabízí své eGON služby
- **Správci** – Fyzické osoby, které spravují jednotlivé subsystémy základních registrů
- **Základní registry** – jednotlivé základní registry (RPP, ROB, ROS, RUIAN)
- **ORG** – převodník identifikátorů fyzické osoby
- **ISZR**- Informační systém základních registrů

4.1 Transakce

Z hlediska procesů je v Globální architektuře používán pojem transakce. Tento pojem není vnímán jako databázová transakce. Neplatí zde tedy obecně koncept ACID:

- **Atomičnost** – Transakce provede buď všechny operace nad databází, nebo žádnou
- **Konzistence** – Izolovaná transakce zachovává konzistenci databáze.
- **Izolovanost** – Dvě a více současně probíhajících transakcí nesmí být vzájemně ovlivněny ani na úrovni mezivýsledků.
- **Trvalost** – Změny v databázi provedené úspěšným dokončením transakce jsou uchovány i při případném výpadku systému

Tento pohled je v rámci globální architektury zobecněn a platí na různých úrovních.
V principu platí, že každý jednotlivý základní registr vnitřně splňuje ACID. Uživatelem základního registru je z tohoto pohledu ISZR. Pokud tedy ISZR při provádění eGON služby použije službu jednotlivého základního registru publikovanou na vnitřním rozhraní, pak provedení této služby musí zcela splňovat požadavky ACID.

4.1.1 Proces čtení referenčních údajů

Tento proces může být z hlediska externího AIS synchronní nebo asynchronní. Je na volbě externího AIS, zda použije synchronní či asynchronní variantu nabízené služby, pokud takové varianty existují. Pro synchronní variantu vždy platí časové omezení vyřízení požadavku. Pokud není do stanovené doby synchronní požadavek vyřízen, pak je navrácena chyba „Time out“. Je vnitřní volbou externího AIS, zda opět použije synchronní variantu služby, nebo přejde na asynchronní.

4.1.1.1 Synchronní varianta čtení

Synchronní varianta služeb je poskytována pouze pro služby, které nejsou kompozitní (poskytují referenční údaje z jednoho registru). Celé čtení je jedinou transakcí, která splňuje požadavky na atomičnost a izolovanost. Požadavky na konzistenci a trvanlivost nemají pro operaci čtení smysl.

Atomičnost: Výsledkem služby tedy je navrácení všech požadovaných údajů (hodnota *undefined* je jeden z povolených stavů referenčního údaje) nebo služba není vyřízena jako celek.

Izolovanost: Výsledek zpracování jednoho dotazu není žádným způsobem ovlivněn ostatními transakcemi

4.1.1.2 Asynchronní varianta čtení

Asynchronní čtení údajů je z celkového pohledu chápáno jako úplná transakce, ovšem pouze s požadavkem na atomičnost. Požadavky na konzistenci a trvanlivost nemají pro operaci čtení smysl.

Tato transakce se dále dělí na následující transakce odpovídající procesu zpracování požadavku:

- **Příjem požadavku –** transakce s požadavkem na atomičnost a izolovanost. Výstupem je předání UID přijatého požadavku s časovým údajem přijetí požadavku, nebo odmítnutí přijetí požadavku (neúplné předání požadavku na trase, neoprávněný požadavek a podobně). V případě odmítnutí přijetí požadavku je předán chybový kód důvodu odmítnutí požadavku.
- **Zpracování požadavku –** transakce zpracování požadavku aplikační logikou ISZR. Na tuto transakci jsou aplikovány požadavky na atomičnost. Výsledkem transakce je umístění výsledku nebo chybového kódu důvodu odmítnutí požadavku do virtuální výstupní fronty žadatele.
- **ISZR volá službu ZR –** základní nedělitelná transakce, kde ISZR na vnitřním rozhraní volá službu jednotlivého základního registru. Tato transakce musí splňovat požadavky ACID.

4.1.2 Proces zápisu referenčních údajů

Základní registry neudržují historii dat. Referenční údaje se tedy **pouze** zapisují nebo odstraňují bez vztahu na původní hodnotu referenčního údaje. Zápis referenčních údajů je vždy asynchronní operace s dodatečnými požadavky na proces zpracování vstupních a výstupních front editačního AIS (viz. kap. 1.3.2.1. Globální architektury základních registrů).

Stejně jako v případě asynchronního čtení údajů je zápis údajů chápán jako jedna celková transakce splňující požadavky ACID:

- **Atomičnost** – Transakce provede buď všechny operace nad všemi uvažovanými databázemi (registry) nebo žádnou. V současné době **není** předpoklad zápisu údajů současně do více registrů.
- **Konzistence** –Transakce zachovává konzistenci údajů ve všech relevantních databázích.
- **Izolovanost** –Transakce splňuje požadavky na izolovanost
- **Trvanlivost** – Změny ve všech databázích provedené úspěšným dokončením transakce jsou uchovány i při případném výpadku systému

Celková transakce je dále opět rozdělena na příjem a zpracování požadavku. Oproti specifikaci ACID může být editorem navíc požadováno serializované zpracování požadavků. ISZR pak musí zajistit, že do jednotlivých základních registrů jsou tyto požadavky předávány ve stejném pořadí, v jakém byly přijaty a to až po vyřízení předchozího požadavku jednotlivým základním registrem. V případě neúspěšně provedené transakce zápisu jsou všechny následující požadavky v dané sekvenci označeny za neúspěšné s vyznačením kódu chyby.

Požadavek serializace může být zadán pouze v rámci jednoho editora. Jeden editor tedy nemůže vyžadovat řazení požadavků v závislosti na požadavcích druhého editora.

4.2 Zajištění bezpečnosti provedení transakcí

Systém základních registrů poskytuje referenční údaje a z tohoto hlediska je konzistence dat primárním požadavkem. Musí být tedy zajištěno, že každý jednotlivý referenční údaj v daném referenčním záznamu má jednoznačného vlastníka (editační AIS) a každý referenční záznam má jednoznačného primárního editora, pokud je v rámci jednotlivého základního registru role primárního editora definována. Konkrétní provedení pro jednotlivé základní registry je řízeno v rámci tohoto registru.

V případě čtení referenčních údajů je primárním požadavkem respektování oprávněnosti ke čtení referenčních údajů zvláště pak pro oblast osobních údajů obyvatel.

4.2.1 Proces zápisu referenčních údajů

Editační AIS mohou požádat pouze o zápis referenčních údajů nebo o vytvoření nového záznamu (pokud k tomu mají oprávnění). Celý proces validace a přípravy údaje tedy probíhá v rámci editačního AIS.

Při vytváření nového záznamu (obyvatel, osoba, územní prvek, rozhodnutí orgánu veřejné moci a podobně) je vždy součástí požadavku na zápis identifikace OVM, Agendy a role v rámci AIS. Jednotlivý základní registr vyznačí u tohoto záznamu primárního editora na základě těchto údajů, pokud je tato role v rámci jednotlivého základního registru definována. Ostatní editoři jednotlivého základního registru pak nemohou tento záznam zrušit ani měnit referenční údaje, které má oprávnění měnit pouze primární editor. Pro každý základní registr pak platí dílčí pravidla, která jsou uvedena v globálních architekturách jednotlivých registrů a budou detailizována v detailních architekturách jednotlivých registrů.

Rozhodnutí o tom, zda požadavek tohoto typu je vznesen oprávněným editorem, je prováděno na úrovni jednotlivého základního registru. ISZR zpracuje každý oprávněný požadavek na službu, neboť nemá informace o oprávněném editorovi konkrétního záznamu nebo konkrétního referenčního údaje v rámci referenčního záznamu.

Sekundární editor má oprávnění k zápisu referenčních údajů pouze pro existující záznamy. Toto oprávnění je dáno konstrukcí eGON služeb na vnějším rozhraní ISZR a sekundární editor tedy z principu nemůže požadovat zápis jiných referenčních údajů než těch, na které má oprávnění.

Může však dojít k situaci, kdy sekundární editor není oprávněn zapsat referenční údaj k záznamu s ohledem na primárního editora nebo jiná business pravidla na úrovni jednotlivého základního registru. Příkladem může být například referenční údaj *číslo elektronického občanského průkazu*. Tento údaj může být zapsán pouze u záznamů, jejichž primárním editorem je Informační systém evidence obyvatel (ISEO).

Rozhodnutí o oprávněnosti zápisu referenčního údaje pro jednotlivý záznam je tedy opět na straně jednotlivého základního registru, který disponuje informacemi o primárním editorovi záznamu.

4.2.2 Proces čtení referenčních údajů

Základním bezpečnostním opatřením je mechanismus přidělení oprávnění AIS k používání eGON služby na vnějším rozhraní ISZR. V rámci definice eGON služby je pomocí XSD šablony definováno, jaké referenční údaje a v jaké kombinaci mohou být pomocí služby čteny.

4.2.3 Problematika územní příslušnosti OVM

Dalším omezením je územní příslušnost jednotlivých OVM. V principu by neměl jednotlivý OVM pracovat s referenčními údaji mimo svoji územní příslušnost, pokud toto není vyžádáno procesem podloženým právní předpisem.

Tento požadavek je řešen tím, že v rámci Registru práv a povinností je pro každý OVM/Agenda uložena jeho územní příslušnost pomocí výčtu územních prvků. Každý AIS může tedy získat informace o své územní příslušnosti. Je zodpovědností OVM, aby v rámci příslušných AIS respektoval tato omezení s ohledem na zákonné požadavky. Vzhledem k tomu, že veškeré operace s referenčními údaji jsou logovány, je možné následně dohledat a přesně určit AIS a jednotlivé osoby, které tato omezení nerespektují.

Z hlediska ostatních subjektů údaje o územní a věcné příslušnosti OVM/Agenda uložené v RPP umožňují následné vyhledání OVM příslušného pro vyřízení konkrétního požadavku. Podobně OVM může zjistit všechny subjekty, které budou v daném okamžiku ovlivněny jeho rozhodnutím na základě věcné a územní příslušnosti.

*RPP ani ISZR tedy neověřuje územní příslušnost konkrétního požadavku od AIS. Poskytuje však referenční údaje, které může AIS používat v implementaci vnitřních procesů a oprávnění***.**

4.2.4 Shrnutí rozdělení zodpovědnosti pro editaci referenčních údajů

Editační AIS – je zodpovědný za správnost údajů, které vkládá do základních registrů jako referenční.
RPP – obsahuje referenční údaje o územní a věcné působnosti jednotlivých OVM. Dále obsahuje referenční část Katalogu služeb a matice oprávnění. Tyto údaje jsou vkládané speciálními editačními AIS, které podle výše uvedené zodpovědnosti zodpovídají za jejich správnost.
ISZR – zodpovídá za poskytování služeb podle provozní části katalogu služeb a matice oprávnění. Zodpovídá za logování požadavků na editaci a výdej referenčních údajů.
Jednotlivý základní registr – zodpovídá za izolaci záznamů mezi jednotlivými editory a za konzistenci uložených dat s ohledem na všechny editory příslušného registru

4.3 Úroveň poskytování služeb (SLA)

Systém základních registrů je komplexní systém sestávající z jednotlivých nezávislých komponent. Služby základních registrů jsou poskytovány na vnějším referenčním rozhraní ISZR ve formě eGON služeb. Pro každou jednotlivou eGON službu musí být definována úroveň poskytování této služby, kde musí být definováno minimálně:

- **Dostupnost služby-** ve formě procentuální dostupnosti služby mimo plánované odstávky služby.
- **Zaručená doba obnovení služby –** čas, za který je zaručeno obnovení dodávky služby v případě neplánovaného výpadku.

- **Odezva –** čas, za který je pro 90% požadavků předán výsledek volání služby
- **Průchodnost –** jaký je maximální počet volání služby za sekundu, který neovlivní výše uvedené parametry.

Na úroveň dodávky služeb na vnějším eGON rozhraní má vliv dodávka služeb jednotlivých komponent základních registrů

- ISZR
- Jednotlivé základní registry
- Spolupracující externí AIS
- Hardwarové prostředí datových center
- Síťová konektivita (interní i externí – konektivita k uživatelům)

Cílem globální architektury není stanovení mechanismu konstrukce SLA pro eGON služby ani jejich konkrétní definice. SLA bude stanoveno pro každou publikovanou eGON službu a konstrukce tohoto SLA musí být navržena implementátorem.

Současně musí implementátor nabídnout mechanismy pro řízení úrovně dodávky služeb (SLA management) s ohledem na navržené nástroje pro monitoring a správu spolu s návrhem odpovídajících procesů.

V rámci dokumentu „Katalog eGON služeb základních registrů“, který je součástí zadávací dokumentace jako příloha 1c (respektive 1b pro ISZR) je uveden pouze návrh tohoto katalogu s rámcovými požadavky. Specifikace metrik je uvedena pouze pro služby třídy S1. „Katalog eGON služeb základních registrů“ je dokument, který bude podléhat kompletnímu životnímu cyklu (zavádění, změna a rušení služeb) podle uvedených pravidel.