Zabezpečení připojení AIS

Studium přehledně seznamuje s jednotlivými bezpečnostními prvky nastavenými v systému základních registrů: anonymizace osobních údajů, využití převodníku identifikátoru fyzických osob, centralizované umístění referenčních údajů do čtyř nezávislých základních registrů, oddělení zodpovědnosti za správu údajů a jejich editaci.

Cílem studia je projít postupně všechny bezpečnostní prvky nastavené v systému základních registrů se zaměřením na zabezpečení připojení agendovým informačním systémům. Od základního popisu fungování celého systému, možností připojení agendových informačních systémů, ověřování oprávnění jak na straně informačního systému, tak na straně úřední osoby až po nastavenou certifikační politiku a bezpečnostní požadavky pro AIS. Důraz je kladen na povinnosti pro správce agendových informačních systémů vyplývající zejména ze zákonů č. 365/2000 Sb. o ISVS a zákona č. 111/2009 Sb. o základních registrech.

Obsah

1 | Informace ke studiu

Vzdělávání v oblasti základních registrů a dalších kmenových projektů eGovernmentu, registrační číslo projektu: CZ 1.04/ 4.1.00/A3.00004

Tento kurz byl vytvořen v rámci projektu financovaného z prostředků Evropského sociálního fondu ČR, operačního programu Lidské zdroje a zaměstnanost a je součástí souboru devíti eLearningových kurzů:

1. Použití základních registrů
2. Agendové informační systémy a Informační systémy veřejné správy
3. Služby soukromoprávního sektoru
4. Zabezpečení přístupu k datům
5. Zabezpečení připojení AIS
6. Programové období 2014 - 2020
7. CzechPOINT@office
8. Open data
9. Datové schránky

1.1 | Význam piktogramů

V kurzu se budete setkávat s piktogramy, které vám usnadní orientaci v textu, upozorní vás na důležité informace, právní předpisy, doporučenou literaturu apod. Piktogramy jsou společné pro všechny kurzy, je tedy možné, že s některými z nich se v tomto kurzu nesetkáte. Přesto je vhodné se před zahájením studia se všemi seznámit.

	důležité informace		odkaz na právní předpis, na paragraf
	dobrý tip		kontrolní otázka
	doporučená literatura		shrnutí učiva
	test		

1.2 | Použité zkratky a terminologie 1.část

V kurzu jsou používané následující zkratky a terminologie :

ZKRATKA	VÝZNAM
AIFO	agendový identifikátor fyzické osoby

AIS	agendový informační systém
ID_AIS	jednoznačný identifikátor agendového informačního systému
IDM	identity management
ISDS	informační systém datových schránek
ISVS	informační systém veřejné správy
ISZR	informační systém základních registrů
JIP	jednotný identitní prostor
KAAS	katalog autentizačních a autorizačních služeb

1.3 | Použité zkratky a terminologie 2.část

V kurzu jsou používané následující zkratky a terminologie :

ZKRATKA	VÝZNAM
KIVS	komunikační infrastruktura veřejné správy
ORG	informační systém zajišťující převod identifikátorů fyzických osob
OVM	orgán veřejné moci
PVS	portál veřejné správy
ROB	základní registr obyvatel
ROS	základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci
RPP	základní registr agend orgánů veřejné moci a některých práv a povinností
RUIAN	základní registr územní identifikace adres a nemovitostí
SZR	správa základních registrů, zřízená zákonem č. 111/2009 Sb. k 1. 1. 2010
ZIFO	zdrojový identifikátor fyzické osoby je neveřejným identifikátorem, ze kterého nelze odvodit osobní ani jiné údaje fyzické osoby, které byl přiřazen v ORG

1.4 | Definice použitých pojmů 1.část

Agenda v působnosti ústředního správního orgánu (USU) je definována konkrétním právním předpisem, který upravuje způsob výkonu konkrétního úseku působnosti. Agendu vykonávají orgány veřejné moci (OVM) určené tímto zákonem.

Agenda je obecně souhrn činností, výkon vymezeného okruhu vzájemně souvisejících činností v rámci působnosti orgánu veřejné moci. Agenda je vykonávána jako souhrn činností. Pro každou činnost je definovaný rozsah oprávnění úřední osoby k přístupu k referenčním údajům v základních registrech nebo k údajům v agendových informačních systémech.

AIFO, agendový identifikátor fyzické osoby podle § 9 zákona o základních registrech. AIFO je unikátním identifikátorem konkrétního obyvatele v rámci agendy. AIFO je různé pro stejného obyvatele v různých agendách. Z AIFO nelze odvodit zdrojový identifikátor fyzické osoby (ZIFO) ani jiné osobní údaje o fyzické osobě, které byl přiřazen v ORG.

AIS, agendový informační systém, je informační systém veřejné správy, který slouží k výkonu jedné nebo více agend.

AIS editační je agendový informační systém, který referenční údaje v základních registrech zakládá, mění nebo ruší. Editorem takového AIS je orgán veřejné moci, který je v rámci některé z agend editorem referenčního údaje.

AIS čtenářský je agendový informační systém, který nemění údaje v základních registrech. Velkým čtenářským AIS je např. Integrovaný informační systém České správy sociálního zabezpečení.

AIS spolupublikující je agendový informační systém, který ve vazbě na některý ze základních registrů, přidává údaje ze svých uložených údajů, které se k referenčním údajům načteným ze základních registrů připojují.

Asymetrická kryptografie je kryptografická technika založená na použití veřejného a soukromého klíče. Zprávu zašifrovanou soukromým klíčem lze dešifrovat veřejným klíčem a naopak. To umožňuje utajeně komunikovat bez výměny klíčů nebo jednoznačně prokazovat totožnost odesílatele.

Autentizace je prokázání totožnosti.

Autorizace je prokázání oprávnění již dříve autentizovaného subjektu.

Certifikát je datový záznam vydaný certifikační autoritou, který potvrzuje vlastnictví veřejného klíče. Digitální, elektronický certifikát je v asymetrické kryptografii digitálně podepsaný veřejný šifrovací klíč. Certifikáty jsou používány pro identifikaci při vytváření zabezpečeného spojení.

ID_AIS, jednoznačný identifikátor agendového informačního systému, který orgán veřejné moci získá při registraci v informačním systému o informačních systémech veřejné správy.

Identifikace je obecný pojem zahrnující autentizaci a autorizaci.

Identifikátor OVM, jednoznačná identifikace OVM, využívá se v souvislosti se základními registry IČO.

IDM, identity management, centrální správy uživatelských účtů. Identity management je informační systém, který dokáže z jednoho místa ovládat životní cyklus všech uživatelských účtů v organizaci.

ISVS, informační systém veřejné správy, který je provozován podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy. Orgány veřejné moci jsou povinny v tomto informačním systému evidovat základní informace o dostupnosti a obsahu svého informačního systému veřejné správy, a to postupem podle zvláštního právního předpisu, kterým je vyhláška č. 528/2006 Sb.

ISZR, informační systém základních registrů poskytuje služby, které zajišťují vazby mezi jednotlivými základními registry; mezi základními registry a agendovými informačními systémy a mezi agendovými informačními systémy navzájem.

JIP, jednotný identitní prostor, je součástí centrály Czech POINT, Obsahuje informace nutné k autentizaci a autorizaci uživatelů pro přístup do samotného systému CzechPOINT a rovněž do agendových informačních systémů.

1.5 | Definice použitých pojmů 2.část

Katalog eGON služeb je základní a ucelený aktuální přehled služeb, které jsou poskytovány na eGON rozhraní Informačního systému základních registrů. Tento přehled je rozšiřován dle stavu a nově identifikovaných potřeb.

KAAS, Katalog autentizačních a autorizačních služeb je funkční součást centrály Czech POINT, který

obsahuje informace o poskytovaných autorizačních a autentizačních službách. Tyto služby zajišťují implementaci registračních procesů a výkon identifikačních, autentizačních a autorizačních procesů, tedy zajišťují „chování“ centrály Czech POINT.

Lokální data AIS, jednotlivé AIS pracují se svými lokálními daty. V systému základních registrů jsou uloženy referenční údaje. Pod pojmem lokální data AIS se v tomto dokumentu rozumí hodnoty údajů, jejichž referenční hodnoty jsou vedeny v ZR. Pojem lokální data se tedy nijak nevztahuje na ostatní data AIS.

ORG je informační systém zajišťující ochranu osobních identifikátorů uložených v základních registrech. Správcem i provozovatelem ORG je Úřad pro ochranu osobních údajů.

OVM, orgán veřejné moci, je státní orgán, územní samosprávní celek a fyzická nebo právnická osoba, byla-li jí svěřena působnost v oblasti veřejné správy, v souladu s definicí v zákoně 111/2009 Sb. o základních registrech.

PVS, Portál veřejné správy je oficiální webová stránka veřejné správy ČR, portal.gov.cz.

Působnost v agendě, působnost ústředního správního orgánu je dána zejména zákonem č. 2/1969 Sb., kompetenční zákon, který komplexně definuje povinnosti tohoto úřadu.

Referenční údaj je údaj vedený v základním registru, který je jako referenční údaj označen (viz § 2 písm. b) zákona o základních registrech). Definuje aktuální právně platnou hodnotu příslušného údaje. Pokud není referenční údaj zpochybněn, je považován za správný a jednotlivé orgány veřejné moci mají povinnost jeho hodnotu využívat při své práci.

ROB, základní registr obyvatel.

ROS, základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci.

RPP, základní registr agend orgánů veřejné moci a některých práv a povinností.

RUIAN, základní registr územní identifikace adres a nemovitostí.

Role znamená souhrn oprávnění konkrétního úředníka přistupovat či měnit referenční údaje v jednotlivých základních registrech či agendových informačních systémech.

SZR je Správa základních registrů, zřízená zákonem č. 111/2009 Sb. k 1. 1. 2010.

Šifrování – základními pojmy šifrování jsou otevřený text a šifrový tj. text a klíč. Zašifrovat znamená převést pomocí šifrovacího algoritmu otevřený text na šifrový, při dešifrování je tomu opačně. V obou případech je potřeba klíč, tzn. informace o způsobu šifrování (parametr šifrovacího algoritmu).

Veřejný klíč je součástí dvojice veřejný/soukromý klíč v asymetrické kryptografii. Veřejný klíč je určen k publikování. Jeho znalost nemůže pomoci k dešifrování zachycené zprávy.

Vnější rozhraní ISZR, také eGON rozhraní je oblast ISZR, ve které jsou publikovány eGON služby poskytované ISZR, základními registry a spolupublikujícími AIS.

ZIFO, zdrojový identifikátor fyzické osoby je neveřejným identifikátorem, ze kterého nelze odvodit osobní ani jiné údaje fyzické osoby, které byl přiřazen v ORG.

2 | Agendové informační systémy

Hlavní část kurzu, kde naleznete veškeré potřebné informace o dané problematice.

2.1 | Legislativa

zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů, vymezuje obsah jednotlivých základních registrů, informačního systému základních registrů a ORG. Jsou zde stanovena práva a povinnosti související se základními registry, jejich užíváním a provozem,

nařízení vlády č. 161/2011 Sb., o stanovení harmonogramu a technického způsobu provedení opatření podle § 64 až 68 zákona o základních registrech, Nařízením vláda České republiky stanovila závazný harmonogram pro plnění úkolů vyplývajících ze zákona o základních registrech.

vyhláška č. 359/2011 Sb. o základním registru územní identifikace, adres a nemovitostí,

zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů. Zde zákon stanoví práva a povinnosti správců informačních systémů veřejné správy. Ukládá povinnosti související s vytvářením, užíváním, provozem a rozvojem ISVS,

vyhláška č. 528/2006 Sb., o formě a technických náležitostech předávání údajů do informačního systému. Vyhláška obsahuje základní informace o dostupnosti a obsahu zpřístupněných informačních systémů veřejné správy

2.2 | Stručný popis systému základních registrů

Základní registry poskytují aktuální informace, tzv. referenční údaje, o klíčových subjektech, se kterými pracuje veřejná správa, tj. o fyzických osobách, o právnických osobách, podnikajících fyzických osobách a orgánech veřejné moci, o nemovitostech, adresách a dalších územních prvcích, o samotné veřejné správě a právech a povinnostech právnických a fyzických osob. Uživatelé mohou čerpat referenční údaje v základních registrech (případně k údajům obsaženým ve spolupublikujících informačních systémech) pouze prostřednictvím agendových informačních systémů, a to konkrétně voláním eGon služeb vystavených na vnějším rozhraní ISZR.

2.2.1 | Systém základních registrů

Celý systém základních registrů tvoří:

- čtyři základní registry, kterými jsou:
  a. registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci (ROS),
  b. registr obyvatel (ROB),
  c. registr územní identifikace, adres a nemovitostí (RÚIAN),
  d. registr agend orgánů veřejné moci a některých práv a povinností (RPP),

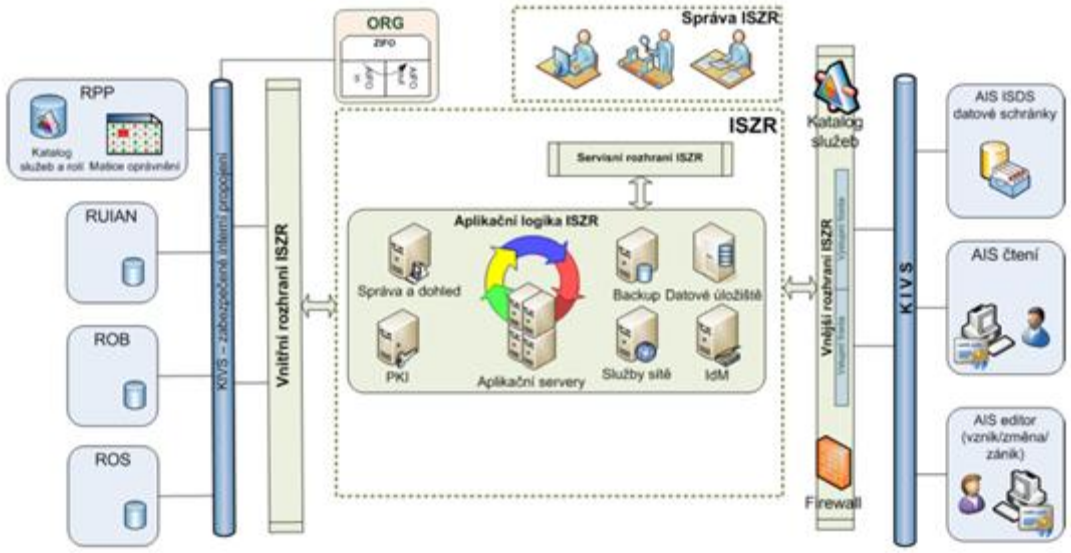
- informační systém základních registrů (ISZR) jako vstupní brána do systému základních registrů zodpovědná za zajištění ochrany a bezpečnosti základních registrů,

- informační systém ORG (převodník agendových identifikátorů fyzických osob) související s ochranou osobních údajů v celém systému základních registrů,

- do celého systému lze zahrnout i připojené agendové informační systémy, které se dělí na:
  a. editační, které editují/mění/ruší/zakládají data základních registrů,
  b. čtenářské, které uživatelům pouze poskytují data ze základních registrů,
  c. spolupublikující, které doplňují referenční údaje svými vlastními daty.

Zjednodušený popis fungování systému základních registrů je na obr. 1., kde jsou jednotlivé části celého systému. V levé části jednotlivé registry za vnitřním rozhraním ISZR, v pravé části jsou zobrazeny jednotlivé přistupující AIS k vnějšímu rozhraní ISZR přes komunikační infrastrukturu veřejné správy (KIVS).

Obr. 1 Schéma systému základních registrů



Gestoři systému základních registrů:

- Gestoři správnosti referenčních údajů: MV, ČSÚ, ČUZK
- Gestor ochrany osobních údajů v základních registrech (násobná digitální identita): ÚOOÚ
- Gestor zajištění ochrany a bezpečnosti vnějšího rozhraní systému základních registrů a provozu: SZR

Přístup k referenčním údajům prostřednictvím AIS je určen OVM, které pro výkon agendy používají AIS zaevidovaný v IS o ISVS. Jedná se o základní a nejdůležitější způsob přístupu OVM k referenčním údajům. Pro komunikace AIS se základními registry je klíčové vnější rozhraní ISZR. V této oblasti jsou publikovány eGon služby v souladu s platným popisem služeb v Katalogu eGon služeb. Vnější rozhraní je dostupné cestou KIVS nebo cestou internetu z veřejné IP adresy. K základním registrům přistupují AIS centrální a lokální.

2.3 | Agendové informační systémy ve vazbě správce a agendy

Agendové informační systémy lze rozdělit na:

- Centrální
- Lokální

Centrální AIS
Centrální AIS využívají většinou OVM, která jsou zároveň editory příslušných údajů. Zodpovědnost za připravenost centrálního AIS pro napojení a čerpání údajů ze základních registrů zodpovídá správce systému (např. u centrálního registru řidičů Ministerstvo dopravy, u informačního systému evidence obyvatel Ministerstvo vnitra). Správce zajišťuje a zodpovídá za jednoznačnou identifikaci (autentizaci a autorizaci) úředních osob, které budou se systémem pracovat. Centrální systémy většinou využívají k přiřazení úředních osob k jednotlivým agendám a správě uživatelů možnosti jednotného identitního prostoru (JIP/KAAS).

Lokální AIS
Pro připojení a komunikaci se základními registry lokálním vlastním AIS, je potřeba znát několik základních

podmínek, které jsou uvedeny v kapitole 2.7 , např. správce musí registrovat AIS do informačního systému o informačních systémech veřejné správy (IS o ISVS). Pouze registrovaný AIS, který se registroval a splnil náležitosti zákona č. 365/2000 Sb. o ISVS lze připojit k rozhraní ISZR.

2.3.1 | Přístupy AIS do základních registrů

Do základních registrů přistupují agendové informační systémy:

I) prostřednictvím jednoagendového lokálního AIS, tzn. 1 AIS = přistupování v rámci 1 agendy,

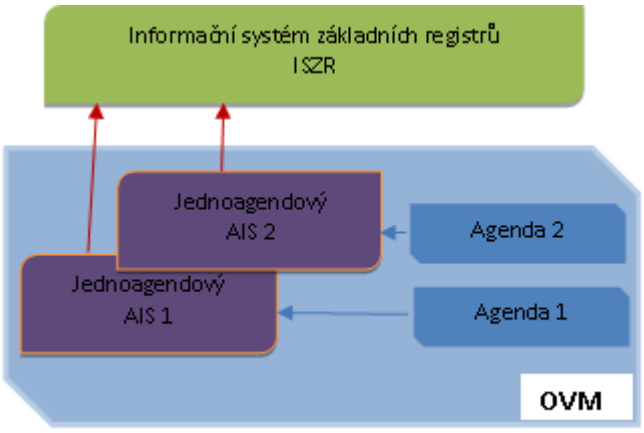
II) prostřednictvím integrovaného lokálního AIS, tzn. AIS = přistupování v rámci více agend,

III) prostřednictvím integrační platformy.

Prakticky mohou nastat různé kombinace těchto možností, kdy OVM bude mít část agendových informačních systémů integrovánu pomocí integrační platformy, zbylé budou komunikaci s ISZR zajišťovat přímo. Návrh konkrétního řešení záleží na zvolené strategii daného OVM.

2.3.1.1 | Přístup k referenčním údajům prostřednictvím jednoagendového lokálního AIS

Jednoagendový lokální agendový informační systém přistupuje k základním registrům a čerpá nebo ověřuje údaje pro potřeby pouze jedné agendy, např. agendy A343 obecní zřízení ohlášené na základě zákona č. 128/2000 Sb., o obcích, ve znění pozdějších předpisů. Správcem lokálního AIS je vždy příslušné OVM, které má pro danou agendu ohlášenou působnost v registru práv a povinností.



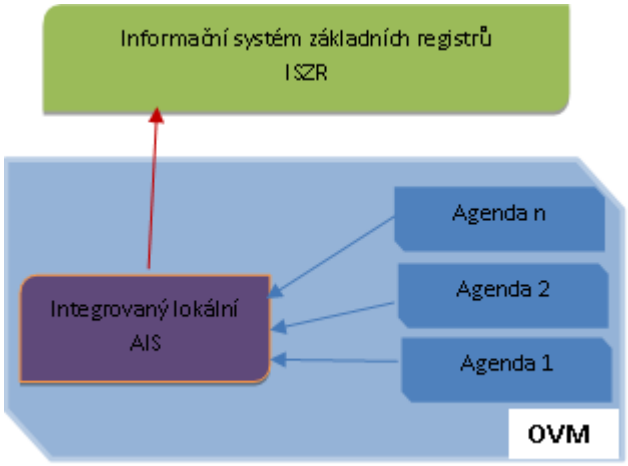
Jednoagendové AIS jsou zpravidla různé architektury a od různých dodavatelů. Ve většině případů nedisponují společným aplikačním základem, nemají jednotnou správu uživatelů a aplikačních oprávnění. Nastavení aplikace je v rámci každého AIS různé a každý systém má svoje vlastní číselníky a kmenová data.

Výhody řešení
Každý AIS je určen pro podporu činností právě jedné agendy, proto mají všechny fyzické osoby uložené v lokální databázi a aktualizované do základních registrů jednoduše přidělené jedno agendové AIFO. Úprava AIS na nastavení pro komunikaci se základními registry se řeší pouze s jedním dodavatelem bez nutnosti respektovat vazby.

Nevýhody řešení
V případě používání jednoagendového lokálního AIS je třeba realizovat úpravy pro komunikaci s ISZR pro každý AIS zvlášť. Nevýhodou je také nejednotná správa uživatelů, roztříštěná pro každý AIS zvlášť a z toho vyplývá více potřebných přihlašovacích údajů pro uživatele/úřední osoby.

2.3.1.2 | Přístup k referenčním údajům prostřednictvím integrovaného lokálního AIS

Další možností přístupu k referenčním údajům je, když jeden AIS podporuje více agend. Ve většině případů je takovýto integrovaný AIS vytvořen na společném aplikačním jádře v rámci jedné technologie. Zpravidla má jednotnou správu uživatelů a aplikačních oprávnění, která může být integrována na lokální, nebo centrální adresářové služby.



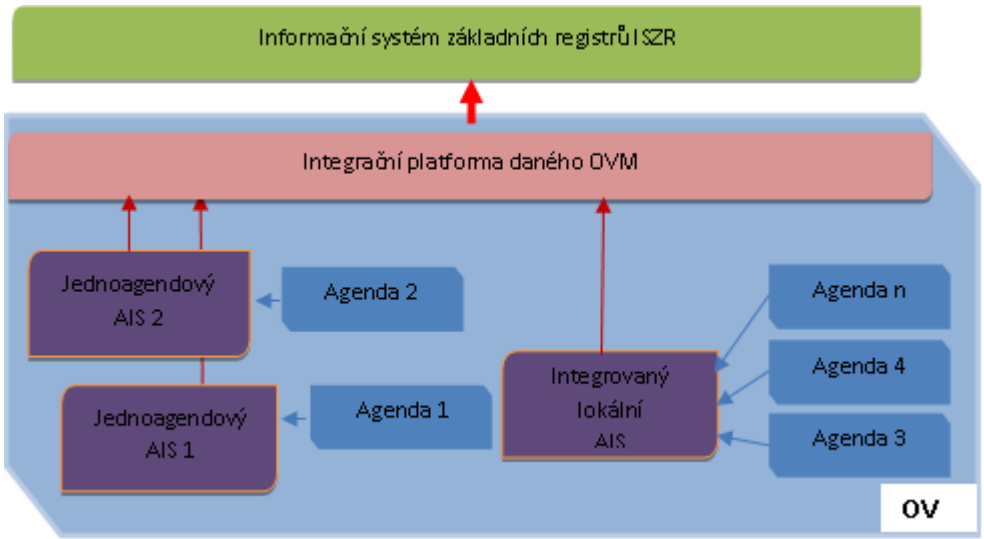
Ve většině případů má společnou funkcionalitu administrace aplikace, jednu evidenci číselníků a kmenových dat.

Výhody řešení
Výhodou je možnost jednotného logování a zajištění jednotné bezpečnosti. Další výhodou je nutnost zajistit pouze jeden technický certifikát pro zajištění přístupu agend k referenčním datům.

Nevýhody řešení
Komplikací tohoto řešení může být požadavek na přiřazování AIFO fyzické osobě v rámci 1 agendy, tj. pro každou z agend, které jsou v takovémto řešení integrovány, musí mít fyzická osoba přiřazené jiné AIFO. Zásadním požadavkem je pak v tomto případě zajištění takové míry zabezpečení aplikace, aby nemohlo dojít k účelovému sdružování údajů o fyzické osobě.

2.3.1.3 | Přístup k referenčním datům prostřednictvím integrační platformy

Pokud se k základním registrům připojuje větší OVM, které má hodně informačních systémů a působnost v mnoha agendách, může být komunikace s ISZR realizována prostřednictvím integrační platformy. Z hlediska aplikační architektury se jedná o podobný způsob řešení jako u integrovaného AIS. Toto řešení představuje nastavení jako pro jeden informační systém veřejné správy. Jde o registraci tohoto jednoho AIS podporující výkon ve více agendách. S tím souvisí i podání žádosti o jeden technický certifikát pro komunikaci s ISZR. Možným řešením je i registrace každého AIS



samostatně do ISVS, pak získá každý AIS vlastní technický certifikát. V tomto případě bude úloha integrační platformy sloužit jako zprostředkovatel komunikace s ISZR, který však bude zároveň představovat jedno místo pro centrální logování komunikace a řízení integračních procesů.

Výhody řešení
Výhodou je jedno centrální místo pro komunikaci se systémem základních registrů, včetně jednotného způsob logování a zajištění úrovně zabezpečení komunikace. Jednotný bude i systém správy uživatelů, tyn. Budou mít pouze jedny přihlašovací údaje do všech používaných aplikací.

Nevýhody řešení
Integrační platforma je náročná na zajištění součinnosti všech zúčastněných stran, na provoz dalšího aplikačního vybavení, včetně získání poměrně značných technických kompetencí pro správce systému. Náročné je také zajištění přiřazení více AIFO k jedné fyzické osobě, pokud se tato osoba vyskytuje v různých agend, což je téměř jisté. Protože zákon o základních registrech zakazuje možnost účelovému sdružování údajů o fyzické osobě.

2.4 | Identifikace (autentifizace a autorizace) a logování

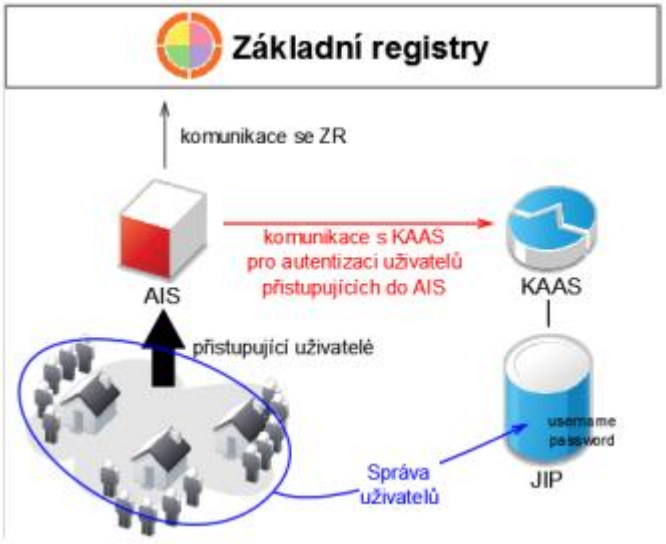
V rámci naplnění požadavku na zajištění evidence přístupů k údajům v základních registrech musí OVM přiřadit konkrétní zaměstnance k jednotlivým agendám a jejich činnostním rolím. Pro většinu centrálních AIS platí, že je uživatel zaveden v JIP/KAAS.


Pro lokální AIS existují následující možnosti zajištění životního cyklu identity:

1. Využití služeb JIP/KAAS

2. Zajištění životního cyklu identity vlastními prostředky

2.4.1 | Využití služeb JIP/KAAS



Tato možnost řešení využívá služeb katalogu autentizačních a autorizačních služeb pro správu identit potřebných pro práci s lokálním AIS. Implementace této možnosti řešení spočívá buď v úpravě lokálního AIS, který bude komunikovat prostřednictvím webo-vých služeb s JIP/KAAS za účelem autentizace uživatele, nebo v synchro-nizaci vybraných identit s lokálními adresářovými službami

AIS využívající řešení JIP/KAAS
Provozovatel AIS neřeší správu uživatelů, protože tu zajišťují nástroje JIP.
Přistupující uživatelé do AIS jsou autentizováni prostřednictvím KAAS.

2.4.2 | Zajištění životního cyklu identity vlastními prostředky

Lokální AIS řeší správu identit buď ve svém vlastním prostředí (v rámci daného informačního systému), nebo prostřednictvím lokálních adresářových služeb (LDAP), které nejsou synchronizovány s JIP.

Provozovatel AIS musí vybudovat a poskytovat vlastní řešení pro správu uživatelů, které umožní:
- zřízení, zrušení, změna uživatele a totéž pro heslo,
- správu aplikačních rolí
- správu agendových činnostních rolí z JIP
- průkazný audit povinně uložených údajů, např. logů

Provozovatel nese zodpovědnost za správnost a aktuálnost údajů.

Každé OVM, které povinně využívá údaje ze základních registrů, se musí na správu uživatelských identit (Identity Management, IdM) dobře připravit, protože ze zákona č. 111/2009 Sb. mu vyplývají v tomto směru povinnosti:
§56 odst. 3 OVM, který byl zaregistrován pro výkon agendy, odpovídá za:

a) Určení úředních osob, které působí v jednotlivých rolích, a za změnu v těchto určeních,
b) Uplatnění odpovídajících opatření, která zabrání neoprávněnému přístupu k údajům vedeným v AIS a k referenčním údajům vedeným v základních registrech na základě oprávnění, které získal.

§57 odst. 1 OVM, který byl zaregistrován pro výkon agendy, vede záznamy o přístupu k uvedeným údajům obsaženým v základních registrech, nejde-li o přístup k údajům veřejně přístupným, a uchovává je po dobu 1 roku; záznam obsahuje:

a) Uživatelské jméno oprávněné úřední osoby, která přístup učinila.
b) Roli, ve které úřední osoba přístup učinila.
c) Výčet údajů. Ke kterým úřední osoba získala přístup.
d) Datum a čas přístupu.
e) Důvod a konkrétní účel přístupu.

V praxi to znamená, že OVM musí zajistit ověřování, zda uživatel (úředník OVM), který přistupující prostřednictvím AIS k referenčním údajům je tím, za koho se vydává (autentizace), zda přístup k základním registrům je oprávněný **(autorizace)** a dále musí bezpečně (bez možnosti změny nebo výmazu nepovolanou osobou) zaznamenat tento přístup v rozsahu uvedeném v § 57 odst. 1 zákona o základních registrech **(logování).**

Každý uživatel by měl přistupovat k referenčním údajům jen v těch činnostních rolích (registrovaných agend, ve kterých má OVM oznámenou působnost), ke kterým je oprávněn. Nejjednodušší možností, jak toto zajistit, je využít ověřování uživatelů v JIP/KAAS.

2.5 | Aktualizace údajů ze základních registrů

Každý agendový informační systém pracuje s údaji vedenými v rámci agendového informačního systému. Tyto údaje se skládají z údajů, které AIS nevytváří a z údajů, které se v rámci AIS vytváří.
Údaje, které AIS nevytváří, mohou být zároveň referenčními údaji z některého základního registru a to nikoliv v plném rozsahu. Cílem je takový stav, kdy údaje, které jsou obsaženy v základních registrech jako referenční, jsou aktualizovány v AIS. Aby osoba pracující s AIS v dané agendě mohla pracovat v důvěře ve správnost referenčního údaje obsaženého v základních registrech (zákon č. 111/2009 Sb. §4 odst. 7).

Pro aktualizaci údajů v agendových informačních systémech jsou k dispozici následující procesy:

- notifikační proces - AIS si pravidelně automaticky aktualizuje svoje data podle obsahu základních registrů.,
- čtení v reálném čase – při dotazu se vrací aktuální hodnota referenčního údaje,
- pravidelný výdej změnových vět registrů prostřednictvím hromadné distribuce změn.

Jednotlivé možnosti jsou detailněji popsány níže:

1) Agendové informační systémy přednostně využívají pro svoji činnost lokálně uložené údaje. U těchto údajů ukládá informaci, kdy a jakých údajů byla provedena aktualizace ze systému základních registrů.

2) Pravidelná aktualizace prostřednictvím procesu notifikace – ISZR připravuje každý den pravidelně v nočních hodinách sadu informací, v rámci které jsou vystavovány změny, AIS musí tento proces spouštět v definovaném časovém rozmezí s definovanými parametry. AIS ukládá informaci o posledním datu a čase aktualizace.

- notifikace RUIAN - v rámci této notifikace získává AIS informace o změnách v RUIAN,
- notifikace ORG – v rámci této notifikace získává AIS informace o změnách AIFO,
- notifikace ROB – v rámci této notifikace získává AIS informace o změnách v ROB,
- notifikace ROS - v rámci této notifikace získává AIS informace o změnách v ROS.

3) Čtení v reálném čase použije AIS pro následující situace:

♣ - Je nezbytná okamžitá identifikace fyzické osoby, tato operace musí být vždy prováděna pomocí okamžitého čtení údaje v základních registrech,
♣ - úřední proces vyžaduje naprostou jistotu, že se pracuje s aktuálními údaji,
♣ - jde o on-line čtení jednoho nebo několika základních údajů na základě referenčních vazeb mezi registry,
♣ - vzniká pochybnost o správnosti údaje,
♣ - do AIS je zaváděn nový subjekt a dochází k jeho vyhledání (ztotožnění) v základních registrech.

4) Hromadná distribuce změn je proces, ve kterém AIS může získat informace o změnách provedených v systému ZR a tím aktualizovat lokální svoje údaje najednou.

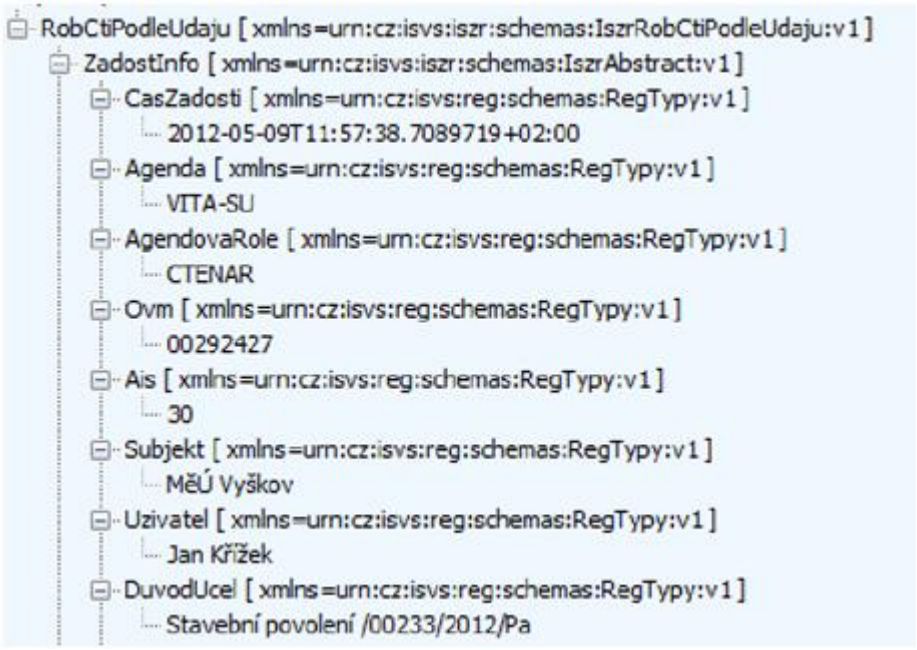
Kdykoli během dne je možné získat notifikace o změnách, které nastaly během tohoto dne do okamžiku dotazu a stav údajů v AIS synchronizovat se stavem referenčních údajů.

Je možné požádat o notifikace zpětně za delší časové období pro případ delšího výpadku AIS nebo hromadné distribuce změn.

2.6 | Ověřování přístupu k údajům ze základních registrů

Při volání eGON služby je AIS povinen předat informace:

- o agendě, na základě které volání probíhá,
- o agendové roli, která službu využívá,
- o OVM, pro který je služba vykonávána,
- o AIS, tj. ID_AIS, který službu volá,
- o subjektu, pro jehož účely se údaje využívají nebo poskytují, pokud to zákon požaduje,
- o identifikaci uživatele, který službu přímo či nepřímo inicioval – uživatelský identifikátor,
- o důvodu a konkrétním účelu využití služby, pokud to zákon požaduje.



Agendou se rozumí kód agendy, který byl přidělen v rámci procesu registrace agendy a OVM se přihlásilo k působnosti v této agendě.

Agendovou rolí se rozumí kód agendové činnosti, která byla registrována v rámci procesu registrace agendy a OVM ohlásilo působnost v této roli dle § 55 odst. 2 písm. c) zákona.

OVM se rozumí přidělený identifikátor OVM, v rámci kterého je eGON služba vyvolána, většinou se používá IČO. U AIS používaných pro více OVM musí být uveden právě jeden identifikátor OVM.

AIS se rozumí identifikátor AIS, který byl AIS přidělen v procesu registrace AIS dle zákona č. 365/2000 Sb. Do IS o ISVS.

Subjektem se rozumí subjekt údajů, pro jehož účely se údaje využívají nebo poskytují, pokud to zákon požaduje.

Uživatel se rozumí identifikátor úřední osoby pro přístup z AIS. Tento identifikátor nemusí být čitelný a srozumitelný pro systém základních registrů. AIS je povinen vést vazbu tohoto identifikátoru ke konkrétní osobě včetně historie podle § 57 zákona tak, aby bylo možné zpětně tyto informace na základě oprávněného požadavku dohledat podle § 57 odst. 3 zákona.

Důvod/účel se rozumí uvedení důvodu nebo účelu využití dat ze základních registrů, nejčastěji se uvádí číslo jednací nebo číslo spisu v rámci kterého k náhledu došlo.

Bezpečnost a blokování přístupu do ISZR
Systém ISZR obsahuje mechanismus, který umožňuje detekovat různé problematické stavy. Příkladem takového problematického stavu může být opakované volání služby, na kterou volající nemá právo nebo volání, které není formálně správné. Při překročení určitého prahu těchto problémů, může být volající AIS zablokován a ISZR se bude tomuto AIS jevit jako nedostupné.

2.7 | Podmínky, které musí AIS splňovat pro připojení k ISZR

Výčet stanovených podmínek

2.7.1 | Podmínka identifikace (autentizace a autorizace) přístupů všech uživatelů

Nezbytnost zajištění jednoznačné identifikace všech úředníků daného OVM přistupujících k vnějšímu rozhraní ISZR byla již popsána výše. Zajistit ji lze nejjednodušeji prostřednictvím využití služeb JIP/KAAS.

Pokud se OVM rozhodne, že pro správu přístupů svých úředníků k základním registrům nemusí JIP/KAAS využívat, musí si ale ve svém AIS vyřešit správu uživatelů včetně kvalitní průkaznosti sám.

2.7.2 | Podmínka registrace AIS v IS o ISVS

V souladu se zákonem č. 365/2000 Sb. je každý systém veřejné správy nahlášený v informačním systému o informačních systémech veřejné správy (IS o ISVS). Tento systém spravuje a provozuje Ministerstvo vnitra. Ověřit si svoje registrované informační systémy může každé OVM vzdáleně přímo ve veřejně dostupném IS o ISVS.

Registrací v tomto systému získá každý informační systém svůj jednoznačný identifikátor ID_AIS, který je pro přístup do základních registrů nezbytný. OVM může žádat o připojení k ISZR pouze pro agendový informační systém, který má tento jednoznačný identifikátor AIS_ID.

2.7.3 | Podmínka ohlášené působnosti v agendě

Registrace agend je proces probíhající v působnosti Ministerstva vnitra. Registrací agendy se zahajuje proces registrace OVM pro výkon agendy. Po registraci agendy vždy příslušné OVM obdrží do své datové schránky oznámení, že byla agenda zaregistrována, a OVM je vždy současně vyzváno, aby do 30 dnů oznámilo výkon své působnosti v dané agendě.

Proces registrace agend není konečný. Budou agendy vznikat a zanikat, měnit se. Povinností ohlašovatele agendy (tedy ústředního správního úřadu) je, aby jeho agenda byla ohlášena a registrována v aktuální

podobě. Oznámení provádí OVM po přihlášení do RPP AIS Působnostní. Přístupy do RPP AIS Působnostní se nastavují obdobně jako do Czech POINT@office.

Úvodní obrazovka pro RPP AIS_Působnostní.

OVM si vždy, když bude vyzváno k oznámení působnosti v nové nebo změněné agendě, musí zkontrolovat, který AIS tuto agendu vykonává, a pokud již má AIS připojený k základním registrům, musí oznámit k danému AIS změnu v agendách, ve kterých AIS pracuje.

OVM musí před podáním žádosti o připojení AIS k ISZR mít oznámenou působnost ve všech agendách, ke kterým bude žádat o připojení k základním registrům. Při vyplňování formuláře žádosti o připojení k ISZR budou OVM k vyplnění nabídnuty pouze agendy, ve kterých má ohlášenou působnost.

2.7.4 | Podmínka zajištění konektivity pro přístup do základních registrů

Bez zajištění konektivity nemůže AIS komunikovat s vnějším rozhraním ISZR. OVM proto musí mít zřízen přístup k Internetu nebo musí být subjektem KIVS. Údaj o způsobu zajištění konektivity OVM uvádí v žádosti o připojení k ISZR tj. v žádosti o certifikát.

Základní pravidla pro zajištění konektivity jsou následující:

- každý AIS má statickou IP adresu (min. jednu, max. čtyři),
- různá OVM nemohou sdílet jednu IP adresu,
- sdílet jednu IP adresu mohou
  ω- všechny AIS jednoho OVM pro jednu datovou schránku (pokud OVM využívá pro své IČO více datových schránek),
- jako IP adresu v žádosti o certifikát OVM nesmí uvést
  ω- privátní IP adresu (s výjimkou adres KIVS),
  ω- adresu protokolu IPv6 (lze používat pouze adresy IPv4),

ω- IP adresu přidělenou poskytovatelům připojení k Internetu pro jiný stát s výjimkou řešení pomocí cloudu.

2.7.5 | Podmínka akceptace certifikační politiky

OVM žádá o umožnění přístupu k referenčním údajům v základních registrech žádostí o vydání elektronického certifikátu, a to pro každý AIS zvlášť. Správa základních registrů provozuje 2 certifikační autority, jednu pro testovací a druhou pro produkční prostředí. Certifikační politika platí pro produkční prostředí. Pro testovací prostředí certifikační politika sice neexistuje, ale postupuje se stejně při vydávání certifikátů, pouze se neprovádí některé kontroly a připouští kratší délku klíčového páru - pro testovací prostředí stačí 1024 bitů, pro produkční prostředí se vyžaduje délka alespoň 2048 bitů. Certifikát pro produkční prostředí má základní dobou platnosti 36 měsíců, u certifikátu pro testovací prostředí je základní doba platnosti 12 měsíců.


Každý AIS připojený k ISZR je jednoznačně identifikován následujícími údaji:

- IČO úřadu identifikační číslo OVM, které je správcem AIS,
- AIS_ID identifikátor AIS podle IS o ISVS,
- SN číslo certifikátu (SerialNumber),
- Seznam agend, ve kterých má OVM ohlášenou působnost.

Zablokování certifikátu

Zablokování certifikátu je dočasná vratná operace. Znamená, že ISZR bude odmítat spojení s AIS, který použije zablokovaný certifikát. Používá se při bezpečnostních problémech způsobených agendovým informačním systémem, např. opakovaná volání služeb, na která nemá agendový informační systém nárok. Zablokovaný certifikát obecně zůstává v platnosti a jeho blokaci lze zrušit.

Zneplatnění certifikátu „z moci úřední“

Zneplatnění certifikátu z moci úřední se procesně řídí správním řádem a přistupuje se k tomuto řešení v případech, kdy se jedná o bezpečnostní ohrožení základních registrů. OVM je datovou zprávou zahájení řízení oznámeno a OVM současně obdrží i rozhodnutí o nařízení předběžného opatření spočívajícím v zablokování certifikátu.

2.7.6 | Podmínka splnění bezpečnostních požadavků

Mezi nejdůležitější bezpečnostní požadavky, které OVM musí zajistit, patří:

- bezpečnost privátní části asymetrického klíčového páru – tj. bezpečnost soukromého klíče
- bezpečnost počítače, na kterém je provozován,

- agendový informační systém musí být před připojením do produkčního prostředí otestován v testovacím prostředí,
- OVM má povinnost oznamovat Správě základních registrů každé narušení bezpečnosti agendového informačního systému nebo základních registrů,
- agendový informační systém se pro komunikaci s vnějším rozhraním ISZR autentizuje pomocí certifikátu vydaným Správou základních registrů.

Součástí bezpečnostních požadavků na agendové informační systémy je řádné otestování agendového informačního systému před jeho připojením do produkčního prostředí. Za řádné otestování agendového informačního systému se považuje, když OVM před podáním žádosti o připojení do produkčního prostředí úspěšně připojil agendový informační systém do testovacího prostředí nebo že připojení a funkčnost řádně otestoval jeho dodavatel.

3 | Kontrolní otázky

1) Po dobu kolika let má OVM ze zákona o základních registrech povinnost uchovávat záznamy o přístupu k uvedeným údajům obsaženým ze základních registrů?

2) Kdy se provádí čtení referenčních údajů v reálném čase?

3) Jakými způsoby může lokální informační systém přistupovat do systému základních registrů?

4) Co vše se uvádí v žádosti o certifikát OVM?

4 | Doporučená literatura

o Zákon č. 111/2009 Sb., o základních registrech ve znění pozdějších předpisů
o Katalog eGon služeb, SZR, 2013
o Informační bulletin č. 1/2012, UOOU, 2012
o Příručka pro obce, SZR, 2013
o Podmínky připojení AIS, SZR, 2013
o Procesní postup připojení AIS, SZR, 2013
o Ohlášení agend ve smyslu zákona č. 111/2009 Sb., o základních registrech, MŠMT, v platném znění
o Detailní návrh implementace ISZR, MV, 2010

5 | Souhrn

Koncepce základních registrů zavádí do datového modelu ISVS následující principy bezpečnosti:

Anonymizace osobních dat uložených i informačních systémech veřejné správy. Základní registry obsahují referenční údaje, které jsou odkazovány bezvýznamovými identifikátory z jednotlivých informačních systémů veřejné správy. Základní registry používají pro identifikaci občana bezvýznamový identifikátor, navíc odlišný v jednotlivých agendách. Vícenásobná digitální identita znemožňuje nekontrolované křížové identifikace v jednotlivých AIS a postupně vytěsní z veřejné správy celoplošné využívání rodného čísla.

Využití převodníku identifikátorů fyzických osob (ORG) jako jediného způsobu, jak sdružit informace o fyzické osobě z více základních registrů nebo agentových informačních systémů. Převodník identifikátorů komunikuje výhradně s ISZR a neobsahuje žádná osobní data.

Centralizované umístění referenčních údajů do čtyř nezávislých základních registrů namísto uchovávání shodných informací v různých informačních systémech bez možnosti automatické aktualizace změn. V základních registrech je každý údaj uložený pouze jednou s jasně definovaným editorem údaje, tj. kdo smí údaj založit, změnit nebo zrušit.

Komunikace mezi základními registry a agendovými informačními systémy probíhá pouze prostřednictvím ISZR.

Je oddělená zodpovědnost za správu dat od jejich editace.

K referenčním údajům základních registrů lze přistupovat pouze z agendových informačních systémů po ověření přístupových práv AIS, agendy a úředníka. I agendové informační systémy mezi sebou komunikují výhradně pomocí dohledovaných služeb.

ISZR poskytuje webové služby na základě oprávnění ze zákona.

Test:

1.1 | Agendový identifikátor fyzické osoby přiděluje v systému základních registrů:

- Registr osob
- Registr obyvatel
- ORG
  Komentář: AIFO se přiděluje v ORG, v gesci UOOU, ROB s ním pouze pracuje, přes ISZR AIFO chodí v dotazech, ROS má referenční vazbu do ROB v případě fyzických podnikajících osob nebo statutárních zástupců.
- Informační systém základních registrů

1.2 | Čtení referenčních údajů v reálném čase se neprovádí, když:

- Je nutná identifikace uživatele např. podle čísla elektronicky čitelného dokladu
- Úřední proces vyžaduje naprostou jistotu, že se pracuje s aktuálními údaji
- Úřední osoba zjistil nesoulad mezi údaji v AIS a listinnou podobou dokladu, který má občan u sebe
- Úřední osoba si chce aktualizovat údaje v agendovém informačním systému
  Komentář: Pro aktualizaci v AIS se nemají online dotazy používat, protože hrozí přetížení systému, pokud by to tak řešil každý. Aktualizace systému musí probíhat přes anotace nebo hromadnou dávkou.

1.3 | Gestorem za správnou adresu jako referenční údaj je v systému základních registrů:

- Ministerstvo vnitra
- Český statistický úřad
- Český úřad zeměměřický a katastrální
  Komentář: Zodpovědný za správnou adresu jako referenční údaj je CUZK, ostatní registry ROB a ROS si z RUIAN stahují adresu formou referenční vazby a hodnoty uložené nemají.
- Správa základních registrů

1.4 | Lokální informační systém do systému základních registrů nepřistoupí:

- Jednoagendovým AIS
- Integrovaným AIS
- Z integrační platformy
- Provozním AIS
  Komentář: Provozní systémy se k ISZR nepřipojují, protože nemají agendy, přistupovat mohou pouze AIS.

1.5 | Mezi údaje, které musí agendový informační systém předat při odesílání dotazu na údaje do základních registrů, nepatří:

- ID_AIS, identifikátor agendového informačního systému
- Uživatelské heslo úřední osoby
  Komentář: Hesla se neposílají, naopak úřední osoba zodpovídá za to, že neumožní nikomu znát svoje přístupové údaje kamkoliv.
- IČO, identifikátor OVM
- Identifikátor agendy

1.6 | OVM má ze zákona o základních registrech povinnost uchovávat záznamy o přístupu k uvedeným údajům obsaženým ze základních registrů po dobu:

- Jednoho roku
  Komentář: Povinnost daná zákonem č. 111/2009 Sb.,
- Dvou let
- Pěti let
- Deseti let

1.7 | Pro zajištění konektivity do systému základních registrů z agendového informačního systému neplatí:

- Více OVM mohou sdílet jednu IP adresu
  Komentář: OVM sdílet IP adresu nesmí, což je provozně velký problém např. v případě hostovaných spisových služeb.
- Všechny AIS jednoho OVM mohou sdílet jednu IP adresu
- Každý AIS má minimálně jednu IP adresu
- Každý AIS má maximálně čtyři IP adresy

1.8 | Systém základních registrů pro správu uživatelů nepracuje s pojmem:

- Logování
- Autentizace
- Autorizace
- Validace

1.9 | Údajem, který musí OVM uchovávat, není:

- Uživatelské jméno oprávněné úřední osoby
- Role, ve které úřední osoba přístup učinila
- Datum a čas přístupu
- Agendový informační systém, ze kterého přístup učinila
  Komentář: Výčet povinností je dán zákonem 111/2009 Sb. A AIS tam uvedený není.

1.10 | V žádosti o certifikát OVM neuvádí:

- IČO, identifikátor OVM
- SN číslo certifikátu (serialNumber)
- Role, pod kterými bude přistupovat
  Komentář: V žádosti o certifikát se role neeviduje a neuvádí, pro přístup do registrů se tato informace dostává z RPP.
- ID_AIS, identifikátor agendového informačního systému

Test – správné odpovědi:

1.1 | Agendový identifikátor fyzické osoby přiděluje v systému základních registrů:

- Registr osob (nesprávná odpověď)
- Registr obyvatel (nesprávná odpověď)
- ORG (**správná odpověď**)
  Komentář: AIFO se přiděluje v ORG, v gesci UOOU, ROB s ním pouze pracuje, přes ISZR AIFO chodí v dotazech, ROS má referenční vazbu do ROB v případě fyzických podnikajících osob nebo statutárních zástupců.
- Informační systém základních registrů (nesprávná odpověď)

1.2 | Čtení referenčních údajů v reálném čase se neprovádí, když:

- Je nutná identifikace uživatele např. podle čísla elektronicky čitelného dokladu (nesprávná odpověď)
- Úřední proces vyžaduje naprostou jistotu, že se pracuje s aktuálními údaji (nesprávná odpověď)
- Úřední osoba zjistil nesoulad mezi údaji v AIS a listinnou podobou dokladu, který má občan u sebe (nesprávná odpověď)
- Úřední osoba si chce aktualizovat údaje v agendovém informačním systému (**správná odpověď**)
  Komentář: Pro aktualizaci v AIS se nemají online dotazy používat, protože hrozí přetížení systému, pokud by to tak řešil každý. Aktualizace systému musí probíhat přes anotace nebo hromadnou dávkou.

1.3 | Gestorem za správnou adresu jako referenční údaj je v systému základních registrů:

- Ministerstvo vnitra (nesprávná odpověď)
- Český statistický úřad (nesprávná odpověď)
- Český úřad zeměměřický a katastrální (**správná odpověď**)
  Komentář: Zodpovědný za správnou adresu jako referenční údaj je CUZK, ostatní registry ROB a ROS si z RUIAN stahují adresu formou referenční vazby a hodnoty uložené nemají.
- Správa základních registrů (nesprávná odpověď)

1.4 | Lokální informační systém do systému základních registrů nepřistoupí:

- Jednoagendovým AIS (nesprávná odpověď)
- Integrovaným AIS (nesprávná odpověď)
- Z integrační platformy (nesprávná odpověď)
- Provozním AIS (**správná odpověď**)
  Komentář: Provozní systémy se k ISZR nepřipojují, protože nemají agendy, přistupovat mohou pouze AIS.

1.5 | Mezi údaje, které musí agendový informační systém předat při odesílání dotazu na údaje do základních registrů, nepatří:

- ID_AIS, identifikátor agendového informačního systému (nesprávná odpověď)
- Uživatelské heslo úřední osoby (**správná odpověď**)
  Komentář: Hesla se neposílají, naopak úřední osoba zodpovídá za to, že neumožní nikomu znát svoje přístupové údaje kamkoliv.
- IČO, identifikátor OVM (nesprávná odpověď)
- Identifikátor agendy (nesprávná odpověď)

1.6 | OVM má ze zákona o základních registrech povinnost uchovávat záznamy o přístupu k uvedeným údajům obsaženým ze základních registrů po dobu:

- Jednoho roku (**správná odpověď**)
  Komentář: Povinnost daná zákonem č. 111/2009 Sb.,
- Dvou let (nesprávná odpověď)
- Pěti let (nesprávná odpověď)
- Deseti let (nesprávná odpověď)

1.7 | Pro zajištění konektivity do systému základních registrů z agendového informačního systému neplatí:

- Více OVM mohou sdílet jednu IP adresu (**správná odpověď**)
  Komentář: OVM sdílet IP adresu nesmí, což je provozně velký problém např. v případě hostovaných spisových služeb.
- Všechny AIS jednoho OVM mohou sdílet jednu IP adresu (nesprávná odpověď)
- Každý AIS má minimálně jednu IP adresu (nesprávná odpověď)
- Každý AIS má maximálně čtyři IP adresy (nesprávná odpověď)

1.8 | Systém základních registrů pro správu uživatelů nepracuje s pojmem:

- Logování (nesprávná odpověď)
- Autentizace (nesprávná odpověď)
- Autorizace (nesprávná odpověď)
- Validace (**správná odpověď**)

1.9 | Údajem, který musí OVM uchovávat, není:

- Uživatelské jméno oprávněné úřední osoby (nesprávná odpověď)
- Role, ve které úřední osoba přístup učinila (nesprávná odpověď)
- Datum a čas přístupu (nesprávná odpověď)
- Agendový informační systém, ze kterého přístup učinila (**správná odpověď**)
  Komentář: Výčet povinností je dán zákonem 111/2009 Sb. A AIS tam uvedený není.

1.10 | V žádosti o certifikát OVM neuvádí:

- IČO, identifikátor OVM (nesprávná odpověď)
- SN číslo certifikátu (serialNumber) (nesprávná odpověď)
- Role, pod kterými bude přistupovat (**správná odpověď**)
  Komentář: V žádosti o certifikát se role neeviduje a neuvádí, pro přístup do registrů se tato informace dostává z RPP.
- ID_AIS, identifikátor agendového informačního systému (nesprávná odpověď)