Digitální a informační agentura

Příručka pro správce AIS, resp. SSVÚ

Stručný návod pro připojení OVM a SPUÚ k základním registrům

Duben 2023

Verze 2.6

Digitální a informační agentura

Na Vápence 915/14

130 00 Praha 3

https://dia.gov.cz/, www.szrcr.cz

Obsah

1 Úvod

1.1 Cíl dokumentu

Cílem této příručky je především poskytnout orgánům veřejné moci (OVM) a soukromoprávním uživatelům údajů (SPUÚ) jednoduchý a srozumitelný návod, jak mají postupovat při připojování svého agendového informačního systému (AIS) / soukromoprávního systému pro využívání údajů (SSVÚ) k základním registrům.

Příručka neposkytuje žádné právní výklady a ani nepopisuje dopad základních registrů na činnost orgánu veřejné moci jako správního úřadu či činnost soukromoprávního uživatele údajů.

Podoba příručky není konečná, podle potřeby je průběžně aktualizována a doplňována.

Příručka není primárně určena pracovníkům v oblasti IT, ale správcům informačních systémů a jejich uživatelům. Snaží se proto používat srozumitelný jazyk. Je však třeba si uvědomit, že základní registry jsou IT projekty, a že se některým odborným termínům vyhnout nelze.

Příručka by měla přispět k orientaci ve způsobech přístupu k referenčním údajům v základních registrech, v rozdílech těchto přístupů a především k uživatelské orientaci v procesech vydávání a používání technických certifikátů a ověřování jejich důvěryhodnosti.

Postup při podání žádosti o umožnění přístupu k referenčním údajům v základních registrech a k údajům v AIS podle § 56 odst. 4 zákona o základních registrech, ve znění pozdějších předpisů (dále jen „**žádost o připojení k ZR**“) se skládá z pěti základních kroků, které jsou podrobně popsány v **kapitole 5.** Správce AIS podle nich postupuje tak, že nejprve

1) zajistí, aby on sám splňoval potřebné podmínky, dále pak
2) zajistí, aby AIS splňoval všechny podmínky pro přístup do základních registrů,
3) připraví svůj AIS pro „volání eGON služeb“ (**nutná součinnost s implementátorem AIS**),
4) vygeneruje technickou žádost o certifikát (**doporučená součinnost s pracovníkem IT**),
5) požádá Digitální a informační agenturu o povolení přístupu AIS k ZR, a nakonec
6) nainstaluje certifikát na svém serveru a začne využívat referenční údaje (**doporučená součinnost s pracovníkem IT**).

Pracovníkem IT se rozumí osoba se základní uživatelskou znalostí IT, která se orientuje v procesu vydávání certifikátů.

Pro dotazy k postupům podle této příručky využívejte výhradně aplikaci **Service Desk Manager, která je dostupná ze záložky Service desk Digitální a informační agentury** https://szrcr.cz/cs/sluzby/spravci-a-vyvojari/service-desk-spravy-zakladnich-registru. Naleznete zde informace, jak se do Service Desk Managera přihlašuje běžný uživatel (bez registrace v JIP) a jak uživatel s účtem v JIP (z internetu nebo

z KIVS). Dotazy obecného charakteru můžete zasílat na e-mailovou adresu podpora@dia.gov.cz, která je však primárně určena pro neautentizované uživatele.

1.2 Vymezení použitých pojmů a zkratek

Agenda je souhrn činností, výkon vymezeného okruhu vzájemně souvisejících činností v rámci působnosti orgánu veřejné moci.

AIS, agendový informační systém, je informační systém veřejné správy, který slouží k výkonu jedné nebo více agend. Jde o aplikaci (software), která obsahuje volání služeb základních registrů. Správcem AIS je orgán veřejné moci.

AIS_ID, jednoznačný **identifikátor agendového informačního systému**, který orgán veřejné moci získá při registraci v Rejstříku informačních systémů veřejné správy (Rejstříku ISVS), který je součástí základního registru práv a povinností (dříve v informačním systému o informačních systémech veřejné správy).

Asynchronní režim dotazů je takový režim, kdy dotaz bude zodpovězen později. Rozlišuje se dále „**pasivní asynchronní režim**“, při kterém se AIS, který dotaz odeslal, musí sám zajímat o jeho vyřízení (musí se zeptat, zda už je odpověď na dotaz k dispozici) a **„aktivní asynchronní režim“**, kdy AIS odpověď na dotaz obdrží automaticky s časovou prodlevou (typickým příkladem využití asynchronního aktivního režimu jsou volání služeb pro hromadné dotazy nebo změny).

Certifikát. Digitální nebo též elektronický certifikát je v asymetrické kryptografii digitálně podepsaný veřejný šifrovací klíč. K veřejnému šifrovacímu klíči, který je součástí certifikátu, existuje vždy také privátní klíč. Privátní klíč a veřejný klíč tvoří dvojici a je možné ověřit, že tyto dva klíče patří k sobě.

Certifikační autorita, **CA** je důvěryhodný subjekt, který je zřízen k vytváření certifikátů veřejných klíčů. Činnost certifikační autority je popsána její certifikační politikou, která definuje nejen korektní způsob činnosti, ale i obsah certifikátů, které jsou v průběhu její činnosti vytvářeny.

CIS, informační systém cizinců, je informační systém, který spravuje a provozuje Policie ČR při výkonu působnosti podle zákona č. 224/2011 Sb., o pobytu cizinců na území České republiky, ve znění pozdějších předpisů.

CMS, centrální místo služeb, zajišťuje vzájemné řízené a bezpečné propojování subjektů veřejné a státní správy, dále zajišťuje komunikaci subjektů veřejné a státní správy s jinými subjekty ve vnějších sítích (např. Internet nebo komunikační infrastruktura Evropské unie). CMS tvoří jediné logické místo propojení operátorů telekomunikačních infrastruktur poskytujících služby pro KIVS.

Czech POINT, Český Podací Ověřovací Informační Národní Terminál, je kontaktní místo veřejné správy.

DIA je **Digitální a informační agentura.**

ISECD, informační systém evidence cestovních dokladů, je informační systém, který spravuje a provozuje Ministerstvo vnitra.

ISDS, informační systém datových schránek, je informační systém veřejné správy, který obsahuje informace o datových schránkách a jejich uživatelích. Správcem tohoto systému je Ministerstvo vnitra, provozovatelem Česká pošta.

ISEO, informační systém evidence obyvatel, je informační systém veřejné správy, který spravuje a provozuje Ministerstvo vnitra.

ISEOP, informační systém evidence občanských průkazů, je informační systém, který spravuje a provozuje Ministerstvo vnitra.

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. Správcem i provozovatelem ISZR je Digitální a informační agentura.

JIP, jednotný identitní prostor, je funkční součástí Czech POINT; obsahuje informace o informačních systémech veřejné správy a uživatelích těchto systémů připojených (registrovaných) v centrále Czech POINT.

KAAS, katalog autentizačních a autorizačních služeb, je funkční součástí Czech POINT; obsahuje informace o poskytovaných službách. Tyto služby představují funkcionalitu centrály Czech POINT.

Katalog eGON služeb je seznam služeb informačního systému základních registrů. Informace uvedené v Katalogu eGON služeb jsou určené implementátorům (programátorům) agendových informačních systémů k tomu, aby agendové informační systémy připravili pro komunikaci se základními registry, případně s jinými agendovými informačními systémy.

KIVS, komunikační infrastruktura veřejné správy, představuje sjednocení různých datových linek subjektů veřejné správy do jedné datové sítě. Jedná se o datovou síť veřejné správy.

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, fyzická nebo právnická osoba, byla-li jí svěřena působnost v oblasti veřejné správy, notář, soudní exekutor a archiv, v souladu s definicí v zákoně č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

Orgány veřejné moci jsou všechna ministerstva, organizace orgánů veřejné moci (např. různé úřady zřizované ministerstvy), hlavní město Praha, městské části hlavního města Prahy, krajské úřady, statutární města, města, městyse, obce a některé fyzické a právnické osoby, kterým byla svěřena působnost v oblasti veřejné správy (např. Hospodářská komora, exekutoři, notáři, Česká televize, Český rozhlas, zdravotní pojišťovny).

RAZR, registrační autorita základních registrů, je webová aplikace, kterou orgány veřejné moci (OVM) a další zmocněné subjekty používají k žádosti o přístup k základním registrům ČR pro své agendové informační systémy (AIS). RAZR vyřizuje žádosti o přístup do produkčního i testovacího prostředí základních registrů.

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.

Rejstřík ISVS, rejstřík informačních systémů veřejné správy, je provozován podle zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů. Aktuálně je součástí registru práv a povinností. Orgány veřejné moci a soukromoprávní uživatelé údajů jsou povinny v tomto rejstříku evidovat základní informace o dostupnosti a obsahu svého informačního systému veřejné správy / soukromoprávního systému využívání údajů.

SSVÚ, soukromoprávní systém pro využívání údajů je informační systém, který slouží k výkonu jedné nebo více agend. Jde o aplikaci (software), která obsahuje volání služeb základních registrů. Správcem SSVÚ je soukromoprávní uživatel údajů.

SSVÚ ID, jednoznačný **identifikátor soukromoprávního systému pro využívání údajů**, který soukromoprávní uživatel údajů získá při registraci do základního registru práv a povinností.

SPAIS, SpoluPublikující AIS, který ve vazbě na některý ze základních registrů, (spolu)publikuje na vnějším rozhraní ISZR tzv. kompozitní eGON služby, tedy služby, které k referenčním údajům načteným ze základních registrů připojují údaje ze SPAIS. Příkladem SPAIS je ISEO, který své služby spolupublikuje ve vazbě na ROB.

SPUÚ, soukromoprávní uživatel údajů, je podnikající fyzická osoba nebo právnická osoba, která není orgánem veřejné moci a je podle jiného právního předpisu oprávněna využívat údaje ze základního registru nebo z agendového informačního systému.

Synchronní režim dotazů je takový režim, při kterém odpověď na dotaz (nebo zpráva, že odpověď není k dispozici) AIS obdrží ihned po odeslání dotazu (tedy obratem).

SZR je Sekce správy základních registrů Digitální a informační agentury.

ZR, Základní registry jsou základní registr obyvatel (**ROB**), základní registr právnických osob, podnikajících osob a orgánů veřejné moci (**ROS**), základní registr územní identifikace, adres a nemovitostí (**RÚIAN**) a základní registr agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností (**RPP**).

Zvláštní postavení v systému základních registrů má **ORG**, který představuje informační systém zajišťující ochranu osobních identifikátorů uložených v základních registrech.

1.3 Výčet některých právních předpisů souvisejících se základními registry

Nařízení eIDAS č. 910/2014, tj. nařízení Evropského parlamentu a Rady (EU) o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES,

nařízení GDPR č. 2016/679, tj. nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů),

zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů (kde je vymezen obsah základních registrů, informačního systému základních registrů a kde jsou stanoveny práva a povinnosti související s vytvářením základních registrů, jejich užíváním a provozem), ve znění pozdějších předpisů,

zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů,

zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů,

zákon č. 12/2020 Sb., o právu na digitální služby, ve znění pozdějších předpisů, který mj. stanoví působnost Digitální a informační agentury,

zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů (kde jsou stanovena práva a povinnosti správců informačních systémů veřejné správy a dalších subjektů, jež souvisí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy),

vyhláška č. 329/2020 Sb., o seznamu položek popisu informačního systému veřejné správy, která obsahuje seznam položek popisu ISVS,

zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů (kde jsou mj. upraveny elektronické úkony orgánů veřejné moci vůči fyzickým a právnickým osobám a naopak prostřednictvím datových schránek),

zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů. Základním cílem zákona je zvýšit bezpečnost kybernetického prostoru a zejména se snažit ochránit tu část infrastruktury, která je pro fungování státu důležitá a jejíž narušení by vedlo k poškození nebo ohrožení zájmu České republiky. Cílem zákona není řešit všechna rizika v kyberprostoru, jako je např. porušování autorských práv, různé podvodné aktivity, úniky elektronických dat či šíření závadného elektronického obsahu,

zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů, který navazuje na obecné nařízení o ochraně osobních údajů a upravuje práva a povinnosti při zpracování osobních údajů.

2 Systém základních registrů

2.1 Popis systému základních registrů

Systém základních registrů tvoří: ISZR, ROB, ROS, RÚIAN, RPP a převodník ORG. Základní registry a ORG mezi sebou komunikují prostřednictvím **vnitřního** rozhraní ISZR.

Uživatelé z OVM mohou přistupovat k referenčním údajům v základních registrech (případně k údajům obsaženým ve spolupublikujících agendových informačních systémech) **výhradně prostřednictvím AIS**, a to voláním služeb vystavených na **vnějším** rozhraní ISZR.

Uživatelé z SPUÚ mohou přistupovat k referenčním údajům v základních registrech (případně k údajům obsaženým ve spolupublikujících agendových informačních systémech) **prostřednictvím soukromoprávních systémů pro využívání údajů (SSVÚ) nebo prostřednictvím AIS, jehož správce jim využívání AIS povolil.**

Zjednodušený popis fungování systému základních registrů je na **obr. 1**., kde jsou jako uživatelé základních registrů znázorněni: OVM (na obrázku jsou to „Ústřední orgány“, „Kraje“ a „Obce“), právnické osoby (na obrázku jako „Podnikatel“) a fyzické osoby (na obrázku jako „Občan“).

Obr. 1

2.2 Popis vnějšího rozhraní ISZR

Vnější rozhraní ISZR, též „eGON rozhraní“, je oblast ISZR, ve které jsou publikovány eGON služby poskytované ISZR, základními registry a spolupublikujícími agendovými informačními systémy (SPAIS).

OVM, který je připojen do KIVS, může přistupovat k vnějšímu rozhraní informačního systému základních registrů nejen cestou samotného KIVS, ale i cestou Internetu (z veřejné IP adresy). OVM, který není připojen do KIVS, nemá jinou možnost přístupu k vnějšímu rozhraní než z veřejné IP adresy.

SPUÚ mohou přistupovat k vnějšímu rozhraní ISZR pouze přes KIVS.

Komunikace agendových informačních systémů s vnějším rozhraním ISZR neprobíhá napřímo, ale vždy prostřednictvím centrálního místa služeb (CMS).

Názvy jednotlivých prostředí a jejich DNS jména najdou implementátoři AIS na webových stránkách Sekce SZR https://szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu v sekci pro vývojáře. Najdou zde i odkaz na tzv. referenčního agenta, který jim slouží jako pomůcka pro pochopení způsobu volání eGON služeb.

Poznámka:

- Testovací prostředí slouží k otestování připojení AIS k vnějšímu rozhraní ISZR. Jeho účelem je ověřit, zda je AIS schopen komunikovat se základními registry. Na webových stránkách Sekce SZR v sekci Správci a vývojáři je odkaz tzv. „Nástroj referenční agent a testovací data“, který slouží jako pomůcka pro pochopení způsobu volání eGON služeb (https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu#agent).
- Testovací prostředí zůstalo pro správce AIS v provozu i po zahájení provozu produkčního prostředí a je určeno zejména implementátorům k ověřování funkčnosti změn AIS.

Pozor! Každý AIS musí být před připojením do produkčního prostředí otestován v prostředí testovacím (viz **kapitola 5.1.6**).

3 Způsoby přístupu k referenčním údajům

Uživatelé z řad OVM mohou přistupovat k referenčním údajům dvěma způsoby, a to prostřednictvím

1. Czech POINT,
2. agendového informačního systému.

Jednotlivé způsoby přístupu k referenčním údajům mají svá specifika a každý je určen jinému účelu.

3.1 Přístup úřadu přes z Czech POINT@office

Přístup je určen pro potřeby samotného OVM jako úřadu. Jedná se obvykle o neveřejné pracoviště úřadu, kde úředník samostatně čerpá informace nebo ověřuje údaje, které potřebuje v rámci probíhajícího řízení v některé z agend.

Přístup prostřednictvím Czech POINT@office využijí zejména malé obce, které nepoužívají pro výkon žádné ze svých agend vlastní AIS.

Czech POINT@office je součástí AIS „Czech POINT - systém kontaktních míst veřejné správy“. Obce k němu mohou získat samostatný přístup, a to po vyplnění a odeslání registračního formuláře uveřejněného na http://www.czechpoint.cz/public/, v záložce „KONTAKTNÍ MÍSTA“ (**Obr. 2**).

Obr. 2

Do Czech POINT@office lze přistupovat s využitím certifikátu získaného u některé z CA (První certifikační autorita, a. s. (I.CA) – https://www.ica.cz/, Česká pošta, s. p. (PostSignum) – http://www.postsignum.cz/,

eIdentity, a. s.: http://www.eidentity.cz/CustomerSupport.html, Národní CA - https://www.narodni-ca.cz/. Komerční certifikát a kvalifikovaný certifikát (elektronický podpis) úředník získá u CA na základě zadání, které mu připraví pracovník zabezpečující v rámci jeho úřadu interní IT. Odpovídající roli úředníkovi nastaví lokální administrátor úřadu prostřednictvím internetové aplikace „Správa dat OVM“, která je dostupná na https://www.czechpoint.cz/spravadat/.

V současné době CzechPOINT@office nabízí úřadům formuláře žádostí pro následující výpisy ze základních registrů*:

- výpis údajů z registru obyvatel,
- výpis údajů z registru osob,
- výpis využití údajů z registru obyvatel, agendového informačního systému evidence obyvatel a agendového informačního systému cizinců**,
- seznam voličů v členění podle volebních okrsků

a formuláře žádostí o

- reklamace údajů při zjištění nesouladu v registru obyvatel,
- reklamace údajů při zjištění nesouladu v registru osob.

OVM obdrží cestou CzechPOINT@office výpisy ze základních registrů bezplatně.

*U všech OVM nemusí být dostupné všechny výše uvedené výpisy, jelikož oprávnění k využití závisí na ohlášení agendy v RPP a nastavení práv ve Správě dat od lokálního administrátora.

** Pro využití těchto údajů postupují obce dle „Manuálu pro obce“, který je uveřejněn na webových stránkách (viz **kapitola 7**).

3.2 Přístup k referenčním údajům prostřednictvím AIS, respektive SSVÚ

Přístup k referenčním údajům prostřednictvím AIS je určen OVM, které pro výkon agendy používají AIS zaevidovaný v registru práv a povinností. **Jedná se o základní a nejdůležitější způsob přístupu OVM k referenčním údajům**.

Přístup k referenčním údajům prostřednictvím SSVÚ je určen SPUÚ, které pro výkon agendy používají SSVÚ zaevidovaný v registru práv a povinností. SPUÚ mohou pro přístup k referenčním údajům používat také těch AIS, jejichž použití jim povolil správce AIS (tzn. nějaký OVM).

Na rozdíl od přístupů popsaných v **kapitolách 3.1** tento přístup umožňuje OVM, resp. SPUÚ využívat i eGON služby určené pro hromadné výstupy nebo aktualizace (synchronní nebo asynchronní).

Následující kapitoly poskytují OVM, resp. SPUÚ návod, jak mají postupovat při zajišťování tohoto přístupu k referenčním údajům.

4 Co by měl OVM a SPUÚ znát, než požádá o připojení AIS nebo SSVÚ k ZR

4.1 AIS

Správce AIS žádá o povolení přístupu do základních registrů podáním žádosti na Digitální a informační agenturu, a to pro každý AIS zvlášť.

Pokud má AIS využívat JIP/KAAS jako autentizační, případně autorizační systém, tak musí být AIS registrovaný v JIP.

Správcem AIS je ten OVM, který je za AIS odpovědný. Jeden OVM může být správcem více AIS.

DIA vyžaduje, aby správce AIS jmenoval pro každý AIS odpovědnou osobu.

4.2 SSVÚ

Správce SSVÚ žádá o povolení přístupu do základních registrů podáním žádosti na Digitální a informační agenturu, a to pro každý SSVÚ zvlášť.

Pokud má SSVÚ využívat JIP/KAAS jako autentizační, případně autorizační systém, tak musí být SSVÚ registrovaný v JIP.

Správcem SSVÚ je ten SPUÚ, který je za SSVÚ odpovědný. Jeden SPUÚ může být správcem více SSVÚ.

DIA vyžaduje, aby správce SSVÚ jmenoval pro každý SSVÚ odpovědnou osobu.

4.3 Agendy

Správce AIS, respektive SSVÚ v žádosti o přístup do základních registrů uvádí seznam agend, ke kterým má mít AIS, respektive SSVÚ přístup.

Registrace agend je proces v působnosti Digitální a informační agentury. Registrace agend probíhá podle § 53 až § 54a zákona o základních registrech, ve znění pozdějších předpisů a je k tomu určena agenda A113 – Registrace agend a orgánů veřejné moci pro výkon agendy.

SPUÚ kontaktuje ohlašovatele agendy. Agendu ohlašuje ten ústřední správní úřad, do jehož působnosti agenda spadá. Součástí ohlášení agendy je definice OVM, respektive SPUÚ, které mají v agendě působnost (tj. kterých z nich se agenda týká).

Po registraci agendy příslušné OVM, resp. SPUÚ obdrží do své datové schránky oznámení, že byla agenda zaregistrována, a OVM, resp. SPUÚ je současně vyzván, aby do 30 dnů oznámil výkon své působnosti v dané agendě. Tj. aby oznámil, že skutečně bude agendu vykonávat.

Správce AIS musí mít v RPP registrovanou působnost v agendách, ke kterým má mít AIS přístup. Výjimkou jsou tzv. "integrované" AIS – viz dále v této kapitole. Registrace OVM pro výkon agendy probíhá podle § 55 až § 57 zákona o základních registrech, ve znění pozdějších předpisů.

Mezi referenční údaje o agendě patří činnostní role, což je výčet a popis činností, které mají být vykonávány v agendě; má-li činnost vykonávat územní samosprávný celek, je součástí popisu informace, zda je činnost výkonem státní správy vykonávané v přenesené působnosti.

DIA předpokládá, že správce AIS je také jediným uživatelem AIS. Mohou existovat výjimky. V těchto výjimečných případech může správce AIS povolit jiným OVM anebo SPUÚ používat AIS.

V případě takových výjimek nemusí mít správce AIS působnost v agendách, ke kterým bude mít AIS přístup a které bude správce pro AIS požadovat v žádosti o přístup AIS do základních registrů. Typickým příkladem jsou „integrované“ AIS (v některých dokumentech publikovaných na webových stránkách Sekce SZR se používá termín „sdílený“ AIS), jejichž správcem je např. některý ústřední správní úřad nebo krajský úřad a jednotlivé OVM mají do takového AIS přístup. Pro "integrované" AIS musí mít působnost v agendách, ke kterým má AIS přístup, OVM které AIS používají.

Sdílené AIS, případně sdílené SSVÚ jsou nyní povolovány administrativně Digitální a informační agenturou na žádost správce sdíleného AIS, případně sdíleného SSVÚ. Správce sdíleného AIS, případně SSVÚ musí písemně informovat DIA o tom, že jeho systém bude sdílený a pro koho. DIA kontroluje „oprávnění sdílet“ AIS/SSVÚ na základě údajů z RPP.

Odpovědnost za použití AIS/SSVÚ jiným OVM/SPUÚ než správcem a za správné naplnění údajů v RPP je na správci sdíleného AIS/SSVÚ. Finální kontrola a schválení údajů v RPP je na správci RPP, resp. editorovi příslušného údaje.

Pozor! Existují agendy, ve kterých mají OVM působnost (tj. byly pro výkon agendy na základě oznámení působnosti v agendě zaregistrovány), ale k základním registrům v rámci těchto agend přistupovat nemohou. Jedná se o agendy vyhrazené správcům registrů nebo speciálním AIS.

Seznam agend není konečný. Budou vznikat nové agendy, zaregistrované agendy se budou měnit, bude docházet ke změnám činnostních rolí a některé agendy také mohou zanikat v souladu s tím, jak se mění právní předpisy, na kterých jsou agendy postavené. Je úkolem ohlašovatele každé agendy (tedy ústředního správního úřadu), aby jeho agenda byla ohlášena a registrována v aktuální podobě. Po každé změně registrované agendy bude vždy OVM, resp. SPUÚ vyzván k tomu, aby znovu oznámil působnost v agendě.

4.4 Přístup k nereferenčním údajům z AISEO, AISC, AISEOP, AISECD

Pokud OVM (orgán obce, orgán kraje nebo orgán hl. města Prahy), resp. SPUÚ potřebuje pro plnění svých úkolů v rámci libovolné agendy kromě referenčních údajů z registru obyvatel i nereferenční údaje z ISEO, CIS, ISEOP, ISECD, požádá o přístup do těchto informačních systémů (tedy do SPAIS) dle pokynů uvedených v dokumentech „Proces připojování AIS k AISEO“, „Proces připojování AIS k AISC“ a Proces připojování AIS k AISEOP, AISECD“ umístěných na webových stránkách Sekce SZR (viz **kapitola 7**). Je-li přístup povolen, je tato skutečnost oznámena žadateli a DIA. Přístup k údajům ve SPAIS schvaluje jejich správce, který přitom posuzuje zejména oprávněnost požadavku.

4.5 Autentizace a autorizace přístupů a logování

K zajištění autentizace a autorizace přístupů uživatelů (fyzických osob, kterým správce AIS povolí používat AIS) se správce AIS zavazuje při podání žádosti o připojení k základním registrům, kdy prohlašuje, „že si je vědom své plné odpovědnosti za jednoznačnou autentizaci a autorizaci všech osob,

které budou při výkonu své působnosti v zaregistrované agendě prostřednictvím AIS přistupovat ke službám vnějšího rozhraní ISZR, a že tyto osoby budou k dané činnosti oprávněny“.

V praxi to znamená, že správce AIS musí zajistit ověřování, zda uživatel (úředník OVM nebo zaměstnanec SPUÚ), který přistupuje prostřednictvím AIS k referenčním i nereferenčním údajům, je tím, za koho se vydává (**autentizace**), zda přístup uživatele 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**).

AIS musí zajistit, že každý uživatel může přistupovat k referenčním údajům jen v těch činnostních rolích, ke kterým je oprávněn.

K evidenci, autentizaci a autorizaci uživatelů může AIS použít JIP/KAAS, prostředky AIS (tj. funkce, které jsou součástí aplikace), nebo externí aplikaci (Identity management), případně jejich kombinaci. V každém případě musí AIS ve spolupráci s JIP/KASS anebo externí aplikací umožňovat přiřazení činnostních rolí z RPP konkrétním uživatelům (fyzickým osobám).

4.6 Certifikáty

K autentizaci připojení AIS a SSVÚ k základním registrům používá DIA privátní klíče a digitální certifikáty. Každý AIS i SSVÚ musí mít vlastní privátní klíč a k němu příslušející certifikát. O certifikát žádá správce AIS, respektive SSVÚ v žádosti o přístup AIS, respektive SSVÚ do základních registrů. K žádosti přikládá příslušný veřejný klíč. V případě pozitivního vyřízení žádosti pošle DIA správci AIS, respektive SSVÚ certifikát.

Správce AIS, respektive SSVÚ musí privátní klíč zabezpečit proti jeho zneužití, ztrátě nebo poškození. Pokud správce AIS, respektive SSVÚ poskytne privátní klíč implementátorovi AIS, respektive SSVÚ za účelem otestování komunikace AIS, respektive SSVÚ se základními registry, je povinností správce AIS, respektive SSVÚ zavázat implementátora písemně k ochraně a nezneužití privátního klíče. Totéž platí v případě, že správce AIS, respektive SSVÚ pověří provozováním AIS, respektive SSVÚ nějaký subjekt a v rámci tohoto pověření mu umožní přístup k soukromému klíči používaného k autentizaci přístupu do základních registrů.

DIA stanovila svou certifikační politiku dokumentem „Certifikační politika Digitální a informační agentury“.

DIA provozuje 2 certifikační autority, jednu pro testovací a druhou pro produkční prostředí. Certifikační politika platí pro produkční prostředí. Pro testovací prostředí certifikační politika neexistuje, nicméně DIA postupuje při vydávání certifikátů pro testovací prostředí obdobně jako pro produkční prostředí. Pro produkční i testovací prostředí DIA vyžaduje délku RSA klíčů 2048 bitů a certifikáty jsou vydávány na 3 roky.

4.7 IP adresy

V žádosti o připojení AIS k základním registrům musí správce AIS / SSVÚ uvést IP adresu / IP adresy, kterou / které bude AIS / SSVÚ používat ke komunikaci se základními registry. Musí jít o IP adresy, které byl správce AIS / SSVÚ oprávněn používat.

Služby základních registrů jsou přístupné jednak z Internetu a za druhé z KIVS. Pro připojení z Internetu musí být v žádosti uvedeny **veřejné** IP adresy, které má správce AIS / SSVÚ rezervované u poskytovatele připojení do Internetu. Pro připojení z KIVS musí být v žádosti uvedeny tzv. **konsolidované** IP adresy, které má správce AIS / SSVÚ rezervované u provozovatele CMS.

DIA nezajišťuje přidělení jakýchkoli IP adres. To je věcí správce AIS.

Od této praxe připojování se ustupuje. AIS spravované ze strany OVM budou přistupovat pouze přes CMS2.

SSVÚ spravované ze strany SPUÚ přistupují pouze přes IPSec VPN nebo SSL VPN. Pro tyto subjekty je zakázáno použití veřejných IP adres.

Viz též kap. 5.7.

4.8 Provozní řád ISZR

Provozní řád ISZR vymezuje základní pravidla provozu vnějšího rozhraní ISZR a obsahuje informace o technické podpoře. Správce AIS, respektive SSVÚ využívající vnější rozhraní ISZR akceptují a dodržují tento řád.

5 Postup správce AIS, resp. SSVÚ pro připojení AIS, resp. SSVÚ k ZR

5.1 Registrace OVM, respektive SPUÚ v RPP

Aby OVM, respektive SPUÚ mohl vůči DIA vystupovat jako správce nějakého AIS / SSVÚ, musí být evidovaný v RPP v tzv. Rejstříku OVM (a SPUÚ).

Proces registrace OVM, respektive SPUÚ v RPP je podrobně popsána v samostatných dokumentech na webu Sekce SZR: https://szrcr.cz/cs/registr-prav-a-povinnosti/dokumenty-k-problematice-rpp. SPUÚ kontaktuje ohlašovatele agendy. Agendu ohlašuje ten ústřední správní úřad, do jehož působnosti agenda spadá. Součástí ohlášení agendy je definice OVM, respektive SPUÚ, které mají v agendě působnost (tj. kterých z nich se agenda týká).

Editoři rejstříku OVM a SPUÚ k tomu podle instrukcí správce RPP použijí AIS RPP působnostní a agendu A113 – Registrace agend a orgánů veřejné moci pro výkon agendy.

5.2 Registrace OVM, respektive SPUÚ v JIP

OVM, respektive SPUÚ musí být evidovány v JIP ze dvou důvodů:

- Aby mohly žádat pro AIS, resp. SSVÚ o přístup do základních registrů. Důvodem je to, že aplikace RAZR používá JIP/KAAS pro evidenci, autentizaci a autorizaci uživatelů.
- Aby mohly do RPP registrovat AIS, resp. SSVÚ. Důvodem je to, že aplikace AIS RPP působnostní používá JIP/KAAS pro evidenci, autentizaci a autorizaci uživatelů.

Dalším důvodem pro registraci AIS v JIP může být rozhodnutí, že AIS bude používat JIP/KAAS pro evidenci, autentizaci anebo autorizaci uživatelů.

Registrace OVM, respektive SPUÚ v JIP je proces blíže popsaný v dokumentu „RPP_kompendium_nove_OVM“ dostupném na https://www.mvcr.cz/clanek/navody-ke-stazeni.aspx

Konkrétní zaměstnance pak v JIP registruje lokální administrátor dané organizace.

5.3 Oznámení výkonu působnosti v agendě

Jakmile ohlašovatel agendy zaregistruje agendu, tj. zavede příslušné OVM, resp. SPUÚ do RPP a uvede, že má působnost v agendě, příslušné OVM, resp. SPUÚ obdrží do své datové schránky oznámení, že byla agenda zaregistrována, a OVM, resp. SPUÚ je současně vyzván, aby do 30 dnů oznámil výkon agendy.

V rámci oznámení výkonu agendy OVM, resp. SPUÚ oznamují, jaké jednotlivé činnostní role, případně jaké služby veřejné správy poskytují a na jakých adresách.

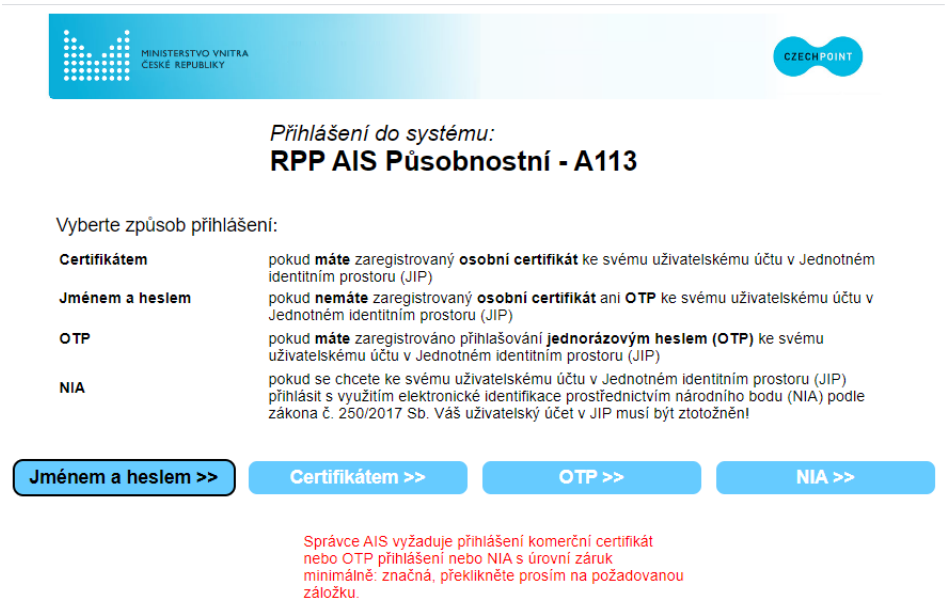
Blíže v dokumentech:

„RPP_kompendium_oznameni_vykonu_agendy OVM“,

nebo „RPP_kompendium_oznameni_vykonu_agendy SPUU“

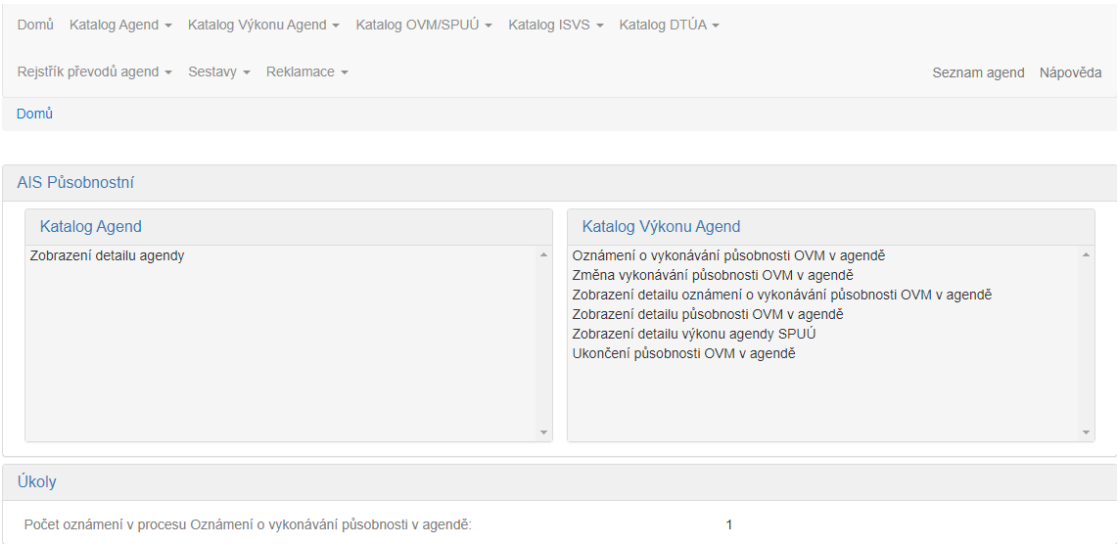
dostupných na https://www.mvcr.cz/clanek/navody-ke-stazeni.aspx

Oznámení provádí OVM, resp. SPUÚ 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 je na **obr. 7**.



Obr. 7

Po úspěšném přihlášení se zobrazí (**obr. 8**):



Obr. 8

OVM, resp. SPUÚ si vždy, když bude vyzván k oznámení výkonu působnosti v nové nebo změněné agendě, musí zkontrolovat, který AIS, resp. SSVÚ tuto agendu vykonává, a pokud již má AIS, resp. SSVÚ připojený k základním registrům (nebo o jeho připojení k základním registrům již požádal), musí oznámit k danému AIS, resp. SSVÚ změnu v agendách, ve kterých AIS, resp. SSVÚ pracuje.

OVM, resp. SPUÚ musí před podáním žádosti o připojení AIS, respektive SSVÚ k ZR mít oznámený výkon všech agend, ke kterým bude žádat o připojení k základním registrům. Při vyplňování formuláře žádosti o připojení k ZR budou OVM, resp. SPUÚ nabídnuty pouze agendy, ve kterých má oznámený výkon agendy.

5.4 Registrace AIS, resp. SSVÚ v RPP

Správce AIS, resp. SSVÚ může žádat o připojení k základním registrům pouze pro AIS, resp. SSVÚ, který je registrovaný v RPP v tzv. Rejstříku ISVS (a SSVÚ) a má tedy přidělený identifikátor.

Správu AIS/SSVÚ provádí OVM, resp. SPUÚ sám v aplikaci AIS RPP působnostní - https://rpp-ais.egon.gov.cz/AISP/verejne. K přihlášení použije svůj účet v JIP. Blíže popisuje dokument „RPP_kompendium_AIS_novy“ dostupný na https://www.mvcr.cz/clanek/navody-ke-stazeni.aspx

5.5 Autentizace všech uživatelů AIS

Autentizaci všech osob, které používají AIS, může správce AIS zajistit využitím JIP/KAAS.

Využívání JIP/KAAS není pro OVM povinné. Pokud se OVM rozhodne, že pro správu přístupů svých úředníků k základním registrům nebude JIP/KAAS využívat, musí si ve svém AIS vyřešit správu uživatelů sám.

Pokud se rozhodne JIP/KAAS používat, tak po registraci AIS v JIP bude správce AIS pro správu uživatelů používat nástroje JIP a uživatelé budou do AIS autentizováni prostřednictvím KAAS. Úředníci, kteří pracují s Czech POINT, byli do JIP zavedeni už před zahájením provozu základních registrů. K registraci uživatelů do JIP slouží aplikace „Správa dat OVM“, která je součástí ISDS – Seznamu orgánů veřejné moci. Aplikace, včetně příručky pro lokálního administrátora, je dostupná na https://www.czechpoint.cz/spravadat/.

JIP a RPP jsou aktualizovány informacemi o nových/rušených OVM z různých zdrojů a nezávisle na sobě. Pokud chce tedy OVM využívat JIP pro autentizaci uživatelů nějakého AIS, musí tento AIS zaregistrovat do JIP, nestačí registrace do RPP.

5.6 Autorizace všech uživatelů AIS, respektive SSVÚ

Autorizaci všech osob, které používají AIS, respektive SSVÚ, může správce AIS zajistit využitím JIP/KAAS nebo přímo prostředky AIS nebo využitím externí aplikace (autorizačního systému).

5.7 Zajištění konektivity

Bez zajištění konektivity mezi AIS a ISZR nemůže AIS, respektive SSVÚ komunikovat se ZR.

Údaj o konektivitě, kterou OVM, resp. SPUÚ zajistil pro AIS, respektive SSVÚ uvádí v žádosti o připojení k ZR.

Pro konektivity DIA stanovila pravidla, která OVM najde v dokumentu „Síťová konektivita ISZR“, a dále v dokumentu „Připojení AIS k ZR - Sdílení připojení“ (viz **kapitola 7**).

Základní pravidla jsou následující:

- každý AIS / SSVÚ má statickou IP adresu (min. jednu, max. čtyři),
- sdílet jednu IP adresu mohou AIS / SSVÚ téhož správce,
- AIS / SSVÚ různých správců nemohou sdílet IP adresu,
- jako IP adresu v žádosti o certifikát správce AIS / SSVÚ nesmí uvést
    - privátní IP adresu (s výjimkou konsolidovaných adres KIVS),
    - adresu protokolu IPv6 (lze používat pouze adresy IPv4),
    - IP adresu přidělenou poskytovatelům připojení k Internetu pro stát, který není členským státem Evropské unie.

Pokud správce AIS / SSVÚ v žádosti o certifikát takovou adresu uvede, DIA žádost zamítne.

Od varianty přístupu přes Internet se ustupuje, v budoucnosti budou AIS a SSVÚ moci přistupovat pouze prostřednictvím CMS2.

SSVÚ spravované ze strany SPUÚ přistupují pouze přes IPSec VPN nebo SSL VPN. Pro tyto subjekty je zakázáno použití veřejných IP adres.

Správce AIS / SSVÚ:

- **plně zodpovídá za veškerý provoz pocházející z registrované IP adresy. Komunikace daného AIS / SSVÚ nebo s daným AIS / SSVÚ bude probíhat výlučně přes IP adresu uvedenou v registraci; správce AIS / SSVÚ bere na vědomí, že v případě nestandardního chování dané IP adresy může být i odpojen od ZR, a to až do sjednání nápravy.**
- **zajistí, že provoz AIS, respektive SSVÚ bude zajišťován poskytovatelem se sídlem v Evropské unii, a místem uložení dat budou datová centra na území členských států Evropské unie.**
- **společně s poskytovatelem provozu AIS, respektive SSVÚ musí zajistit zpracování osobních údajů v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů a s nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).**

Poznámky:

- Z bezpečnostních a správních důvodů DIA požaduje, aby každý OVM používal pro AIS, který spravuje, IP adresy, které pro komunikaci se ZR nesdílí s AIS spravovanými jiným OVM,

- DIA umožní pro určitou IP adresu přístup k ZR pouze pro OVM, který ji uvede v žádosti o přístup do ZR jako první. Pokud tuto adresu uvede v žádosti později jiný OVM, DIA tuto žádost zamítne. DIA neřeší spory o oprávněnosti OVM používat určitou IP adresu.

5.8 Splnění bezpečnostních požadavků na AIS a SSVÚ

DIA stanovila bezpečnostní požadavky na AIS, respektive SSVÚ dokumentem „Bezpečnostní požadavky na AIS pro připojení k produkčnímu prostředí základních registrů“ (viz kap. 7). Pro připojení k testovacímu prostředí ZR se tento dokument použije obdobně.

Správce AIS, respektive SSVÚ při podání žádosti o připojení k ZR prohlašuje, že se s dokumentem „Bezpečnostní požadavky na AIS pro připojení k produkčnímu prostředí základních registrů“ seznámil a že AIS, respektive SSVÚ tyto požadavky splňuje.

Pozor! Součástí bezpečnostních požadavků na AIS je řádné otestování AIS před jeho připojením do produkčního prostředí. Za řádné otestování AIS se považuje, že správce AIS před podáním žádosti o připojení do produkčního prostředí požádal o připojení do testovacího prostředí a následně AIS do testovacího prostředí úspěšně připojil, případně že připojení a funkčnost AIS řádně otestoval jeho dodavatel.

5.9 Volání eGON služeb v AIS, respektive SSVÚ

Přípravu na připojení AIS, respektive SSVÚ k základním registrům pro správce AIS, respektive SSVÚ **zabezpečuje vždy implementátor (programátor, dodavatel) AIS, respektive SSVÚ**. Jejím předmětem je nastavení (naprogramování) parametrů volání každé eGON služby tak, aby dotaz (v hlavičce dotazu) obsahoval informace identifikující OVM, resp. SPUÚ, agendu, činnostní roli, uživatele atd. Tyto informace musí být pro volání eGON služby vyplněny tak, aby byly ve shodě s údaji, které správce AIS, respektive SSVÚ uvedl v žádosti o povolení přístupu k ZR a s údaji v RPP.

Implementátoři najdou potřebné postupy a návody na https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari.

Správce AIS, respektive SSVÚ by měl mít s dodavatelem uzavřenou dohodu (smlouvu) o dodání AIS, respektive SSVÚ a jeho dalším vývoji. Dodavatel na základě smluvního vztahu v průběhu „života AIS, respektive SSVÚ“ poskytuje správci AIS, respektive SSVÚ podporu pro jeho další vývoj. DIA doporučuje, aby OVM měl smluvně zajištěno, že změny AIS vyvolané legislativními změnami v právním řádu ČR poskytuje dodavatel AIS pro OVM bezplatně.

5.10 Vygenerování technické žádosti o certifikát

Tato kapitola je určena zejména IT pracovníkům. Postup generování žádosti o certifikát a instalace certifikátu na počítači OVM, resp. SPUÚ je však na stránkách Sekce SZR v sekci Správci a vývojáři popsán tak podrobně, že jej mohou zvládnout i pracovníci OVM, resp. SPUÚ bez hlubších IT znalostí.

DIA zpracovala a uveřejnila návod postupu vygenerování žádosti o certifikát. Správce AIS, respektive SSVÚ tento návod nemusí používat. Žádost o certifikát však musí být vygenerována v souladu s certifikační politikou DIA a musí obsahovat údaje podle návodu.

Na stránkách Sekce SZR v sekci pro správce AIS je uveřejněn návod „Postup pro vytvoření žádosti o digitální certifikát“: https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2

5.11 Zaslání žádosti o připojení AIS k ZR

Správce AIS, respektive SSVÚ se přihlásí do aplikace RAZR.

Na webových stránkách Sekce SZR je v sekci Správci a vývojáři návod k připojení a uživatelský manuál „Příručka RAZR pro správce ais“: https://www.szrcr.cz/cs/dulezite-dokumenty/63-uzivatelska-prirucka-razr-pro-ovm.

- Aplikace RAZR je pro AIS OVM a jejich prostřednictvím SPUÚ v současné době dostupná ze sítí KIVS (Komunikační infrastruktura veřejné správy) prostřednictvím CMS2 (Centrální místo služeb 2. generace) a prostřednictvím Internetu, přičemž od přístupu přes Internet pro OVM a jejich prostřednictvím SPUÚ se ustupuje. V budoucnu bude pro AIS možný pouze přístup přes CMS2. Viz kap. 5.7.
  - URL z Internetu = https://razr.egon.gov.cz
  - URL z KIVS přes CMS2 = https://razr.egon.cms2.cz

- SSVÚ správcovských SPUÚ (soukromoprávní systémy využívání údajů správcovských soukromoprávních uživatelů údajů) mohou přistupovat přes IPSec VPN nebo SSL VPN. Pro tyto subjekty je zakázáno použití veřejných IP adres.

Pro přihlášení do aplikace RAZR je nutné splnit následující požadavky:

- mít účet v JIP (Jednotný identitní prostor);
- mít v JIP přidělenou roli, respektive role pro práci s RAZR.

Odesláním žádosti na DIA akceptuje správce AIS, respektive SSVÚ Certifikační politiku a Provozní řád.

Správce AIS, respektive SSVÚ žádá odděleně o připojení AIS, respektive SSVÚ do testovacího a do produkčního prostředí základních registrů. Pro přístup do testovacího prostředí se používají jiné certifikáty než pro přístup do produkčního prostředí.

5.12 Instalace certifikátu

Proces zpřístupnění základních registrů pro AIS, respektive SSVÚ dokončí správce AIS, respektive SSVÚ poté, co obdrží certifikát od DIA, jeho instalací ve svém prostředí takovým způsobem, aby ho AIS, respektive SSVÚ používal pro autentizaci AIS, respektive SSVÚ vůči ISZR. Při instalaci certifikátu postupuje správce AIS, respektive SSVÚ podle návodu „Postup pro vytvoření žádosti o digitální certifikát“.

Správce AIS, respektive SSVÚ odpovídá za bezpečné uložení certifikátu a především za bezpečné uložení privátního klíče.

5.13 Instalace certifikátů certifikačních autorit DIA

Instalaci certifikátů CA DIA provádí správce AIS, respektive SSVÚ **v součinnosti se svým implementátorem AIS, respektive SSVÚ** nebo **s pracovníkem pro IT záležitosti**. Bez nainstalovaných certifikátů CA DIA správce AIS, respektive SSVÚ neověří důvěryhodnost certifikátů vydaných DIA.

Generování technické žádosti o certifikát (viz **kapitola 5.13**) není závislé na nainstalování certifikátů CA DIA. V případě jakýchkoliv pochybností o správnosti certifikátů CA DIA příslušné certifikáty neinstalujte a kontaktujte Service Desk DIA.

6 Správa AIS, respektive SSVÚ (změny připojení nebo změny přístupů k ZR)

DIA vydává certifikát pro produkční i pro testovací prostředí se základní dobou platnosti 36 měsíců.

V průběhu doby platnosti certifikátu mohou nastat okolnosti, na jejichž základě je nutné provést některé změny (např. změnit nastavení konektivity, upravit seznam agend pro AIS, respektive SSVÚ nebo certifikát zneplatnit). Všechny změny řeší správce AIS, respektive SSVÚ pomocí aplikace RAZR.

6.1 Vydání nového certifikátu při skončení platnosti dosavadního certifikátu

Správce AIS, respektive SSVÚ sleduje dobu platnosti certifikátu, který mu byl vydán. O době platnosti certifikátu je vždy informován ve „sdělení o žádosti“, které obdrží od DIA spolu s certifikátem a dále registrační autoritou DIA minimálně měsíc před skončením platnosti certifikátu upozorněním na konec platnosti na e-mailovou adresu osoby, kterou správce AIS, respektive SSVÚ uvedl jako osobu odpovědnou za AIS, respektive SSVÚ. O nový certifikát správce AIS, respektive SSVÚ požádá vždy nejdříve 3 měsíce před uplynutím doby platnosti, pro kterou byl dosavadní certifikát vydán.

O nový certifikát správce AIS, respektive SSVÚ žádá postupem popsaným v **kapitole 5**.

6.2 Zneplatnění certifikátu na žádost správce AIS, resp. SSVÚ

Správce AIS, respektive SSVÚ může požádat o zneplatnění certifikátu. Jedná se zejména o okolnosti, kdy

- věcný obsah certifikátu nebo jeho část se stanou neplatnými před uplynutím doby jeho platnosti,
- držitel certifikátu porušil povinnosti uvedené v Certifikační politice DIA (OVM, resp. SPUÚ sám zaznamená bezpečnostní incident, jakým je např. ztráta privátního klíče nebo zjištěný neoprávněný přístup k referenčním údajům),
- dojde ke změně AIS_ID, respektive SSVÚ_ID
- dojde ke změně IČO správce AIS, respektive SSVÚ (držitel certifikátu zanikne).

Správce AIS, respektive SSVÚ o zneplatnění certifikátu požádá pomocí aplikace RAZR. DIA certifikát zneplatní bez zbytečného prodlení, zpravidla během jednoho pracovního dne.

6.3 Zneplatnění certifikátu z iniciativy DIA

Pokud DIA ve výjimečných případech přistoupí ke zneplatnění konkrétního certifikátu, postupuje takto:

a) pokud je nutný okamžitý zákaz používání certifikátu pro přístup k základním registrům, zablokuje použití certifikátu pro přístup k základním registrům;

b) informuje držitele certifikátu o zablokování certifikátu a zahájení procesu zneplatnění zasláním zprávy do jeho datové schránky;

c) pokud důvody pro zneplatnění trvají i po případném vyjádření držitele certifikátu, DIA certifikát bez zbytečného prodlení zneplatní a odešle informaci o zneplatnění do datové schránky držitele certifikátu.

7 Přehled webových odkazů

V této příručce jsou zmíněny předpisy, dokumenty nebo formuláře, které OVM, případně SPUÚ nalezne na následujících webových stránkách:

Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů	https://www.zakonyprolidi.cz/cs/2009-111
Zákon č. 12/2020 Sb., o právu na digitální služby, ve znění pozdějších předpisů	https://www.zakonyprolidi.cz/cs/2020-12
Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů	https://www.zakonyprolidi.cz/cs/2016-297
Zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů	https://www.zakonyprolidi.cz/cs/2017-250
Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších předpisů, ve znění pozdějších předpisů	https://www.zakonyprolidi.cz/cs/2000-365
Vyhláška č. 329/2020 Sb., o seznamu položek popisu informačního systému veřejné správy, která obsahuje seznam položek popisu ISVS	https://www.zakonyprolidi.cz/cs/2020-53
Zákon č. 300/2008 Sb., o elektronickém podpisu a autorizované konverzi dokumentů, ve znění pozdějších předpisů	https://www.zakonyprolidi.cz/cs/2008-300
Katalog eGON služeb (aktuální verze)	https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu
Popis hlaviček eGON služeb	https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu
Přehled referenčních údajů (odkaz „Referenční údaje v základních registrech ze zákona č. 111/2009 Sb.“)	https://www.szrcr.cz/cs/referencni-udaje
Registrační autorita základních registrů (RAZR) - Uživatelská příručka pro OVM	https://www.szrcr.cz/cs/dulezite-dokumenty/63-uzivatelska-prirucka-razr-pro-ovm
Postup pro vytvoření žádosti o digitální certifikát	https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2
Proces připojování AIS k AISEO, AISC, AISEOP, AISECD	https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/kompozitn%C3%AD-slu%C5%BEby-aiseo,-aiseop,-aiscd-a-aisc

Provozní řád ISZR	https://www.szrcr.cz/cs/dulezite-dokumenty
Certifikační politika DIA	https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2
Bezpečnostní požadavky na AIS	https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2
Síťová konektivita ISZR	https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2
Platné certifikáty CA DIA a HASH hodnoty certifikátů	https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2
Sdílení připojení AIS k ZR	https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2
Manuál pro obce (využívání údajů z ROB, AISEO a AISC)	https://www.szrcr.cz/cs/registr-obyvatel/dokumenty-k-problematice-rob
Bezpečnostní požadavky na AIS	https://szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2