SPRÁVA ZÁKLADNÍCH REGISTRŮ

Příručka pro obce

Stručný návod pro připojení OVM k základním registrům

Srpen 2019

Verze 2.3

Správa základních registrů

Na Vápence 14

130 00 Praha 3

www.szrcr.cz

Obsah

1 Úvod

1.1 Cíl dokumentu

Cílem této příručky je především poskytnout orgánům veřejné moci jednoduchý a srozumitelný návod, jak mají postupovat při připojování svého agendového informačního systému k základním registrům.

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

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

Cílovou skupinou jsou především uživatelé referenčních údajů, zejména z řad orgánů veřejné moci územní samosprávy (**obce**).

Příručka není primárně určena pracovníkům v oblasti IT, ale úředníkům. 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 úředníků ve způsobech přístupu k referenčním údajům v základních registrech, v rozdílech těchto přístupů a především k uživatelské orientaci úředníků v procesech vydávání a používání technických certifikátů a ověřování jejich důvěryhodnosti.

Postup OVM 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 ISZR**“) se skládá z pěti základních kroků, které jsou podrobně popsány v **kapitole 5.** OVM podle nich postupuje tak, že nejprve

1) zajistí, aby AIS splňoval všechny podmínky pro připojení, dále pak
2) připraví svůj AIS pro „volání eGON služeb“ (**nutná součinnost s implementátorem AIS**),
3) vygeneruje si technickou žádost o certifikát (**doporučená součinnost s pracovníkem IT**),
4) požádá SZR o připojení AIS k ISZR, a nakonec
5) 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 Správy základních registrů** 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 s

využitím KIVS). Dotazy obecného charakteru můžete zasílat na e-mailovou adresu podpora@szrcr.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.

AIS_ID, jednoznačný **identifikátor agendového informačního systému**, který orgán veřejné moci získá při registraci v 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).

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.

ISCD, informační systém 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.

IS o ISVS, informační systém o informačních systémech veřejné správy, je provozován podle zákona

365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů. Aktuálně je součástí registru práv a povinností. 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., o informačním systému o informačních systémech veřejné správy, ve znění pozdějších předpisů.

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 Správa základních registrů.

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 a fyzická nebo právnická osoba, byla-li jí svěřena působnost v oblasti veřejné správy, 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, městysy, 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 sysémy (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.

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.

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 Správa základních registrů.

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),

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

nařízení vlády č. 161/2011 Sb., o stanovení harmonogramu a technického způsobu provedení opatření podle § 64 až 68 zákona o základních registrech (kterým vláda České republiky stanovila závazný harmonogram pro plnění úkolů vyplývajících ze zákona o základních registrech, a to na straně Správy základních registrů a některých orgánů veřejné moci),

zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění zákona č. 183/2017 Sb. (představuje zahájení adaptace právního řádu České republiky na nařízení eIDAS),

zákon č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů,

zákon č. 250/2017 Sb., o elektronické identifikaci (představuje ukončení adaptace právního řádu České republiky na nařízení eIDAS),

zákon č. 251/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronické identifikaci.

Dalšími souvisejícími důležitými právními předpisy jsou například:

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. 528/2006 Sb., o formě a technických náležitostech předávání údajů do informačního systému, který obsahuje základní informace o dostupnosti a obsahu zpřístupněných informačních systémů veřejné správy (vyhláška o informačním systému o informačních systémech veřejné správy),

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, který navazuje na obecné nařízení o ochraně osobních údajů a upravuje práva a povinnosti při zpracování osobních údajů.

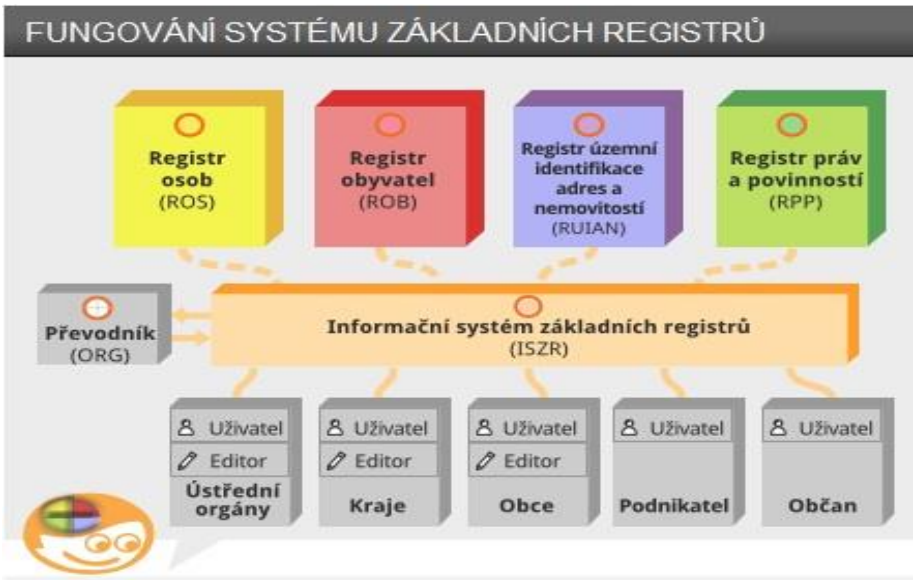
2 Systém základních registrů

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 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.

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. 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 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 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 mohou přistupovat k referenčním údajům třemi způsoby, a to prostřednictvím

1. komunikačních kanálů Czech POINT,
2. datové schránky,
3. agendového informačního systému.

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

3.1 Přístup prostřednictvím „Czech POINT – systém kontaktních míst veřejné správy“

3.1.1 Přístup z kontaktního místa veřejné správy (Czech POINT)

Přístup prostřednictvím „Czech POINT – systém kontaktních míst veřejné správy“ je určen pro uživatele z řad fyzických nebo právnických osob (podnikatelů), kteří se dostaví na Czech POINT. Žadatel žádá o výpis referenčních údajů, o jejich reklamaci ke své osobě, příp. k osobě, jejímž je uživatel zákonným zástupcem, opatrovníkem nebo zmocněncem. Žadatel – fyzická osoba – může na Czech POINT poskytnout rovněž souhlas s poskytnutím svých referenčních údajů z ROB jiné fyzické osobě nebo právnické osobě.

V současné době mají kontaktní místa veřejné správy k dispozici formuláře žádostí pro následující výpisy:

- výpis údajů z registru obyvatel,
- výpis údajů z registru osob,
- veřejný výpis údajů z registru osob,
- neveřejný výpis údajů podnikající fyzické osoby z registru osob,
- výpis o využití údajů z registru obyvatel,
- výpis o využití údajů z registru osob,

a dále formuláře žádostí o

- změnu údajů při zjištění nesouladu v registru obyvatel,
- změnu údajů při zjištění nesouladu v registru osob,
- poskytnutí referenčních údajů jiné osobě,
- odvolání souhlasu s poskytováním referenčních údajů z registru obyvatel jiné osobě.

Pracovník Czech POINT ověří totožnost žadatele a následně mu vydá ověřený výpis, za který žadatel zaplatí správní poplatek, jehož výše je závislá na počtu listů požadovaného výpisu. Z tohoto důvodu je vhodné se na délku výpisu informovat.

3.1.2 Přístup z úřadu (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 registračního formuláře uveřejněného na http://www.czechpoint.cz/public/, v záložce „KONTAKTNÍ MÍSTA“ (**Obr. 2**) a po jeho zaslání na MV ČR.

Obr. 2

Do Czech POINT@office lze přistupovat s využitím certifikátu získaného u některé z CA (I.CA – https://www.ica.cz/, PostSignum – http://www.postsignum.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 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,

a formuláře žádostí o

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

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

3.2 Přístup prostřednictvím datových schránek

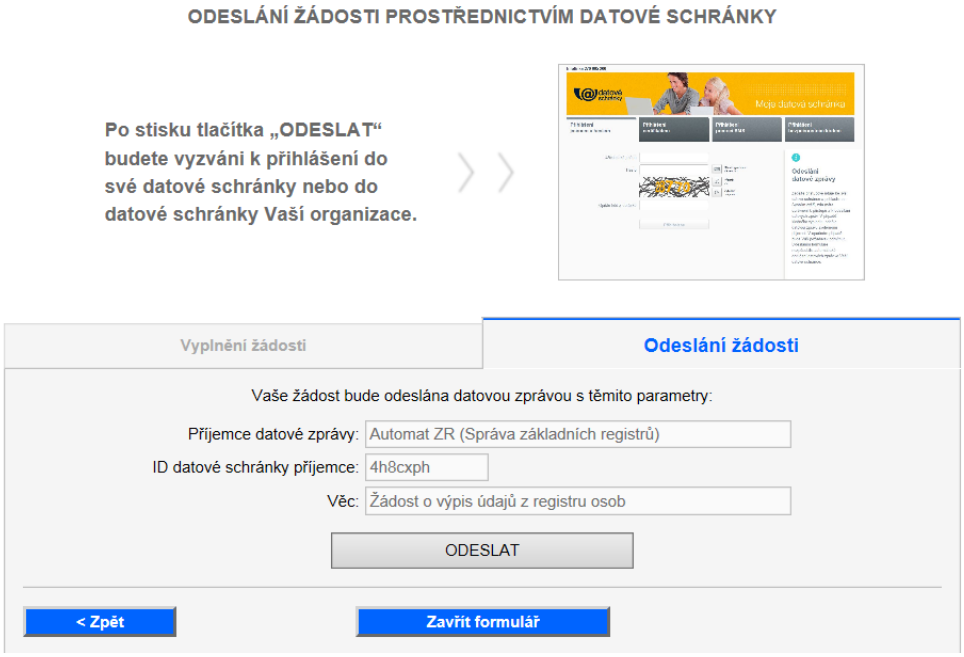
Přístup k referenčním údajům prostřednictvím datové schránky subjektu údajů je určen uživatelům z řad fyzických nebo právnických osob (podnikatelů), kteří mají vlastní datovou schránku. Tito uživatelé mohou s využitím formulářů uveřejněných na Portálu veřejné správy (https://www.portal.gov.cz/obcan/) posílat do základních registrů dotazy na referenční údaje **ke své osobě**. Platné formuláře jsou dostupné pod tzv. „dlaždicí“ s názvem „Formuláře“ (**obr. 3**).

Obr. 3

Po kliknutí na dlaždici „Formuláře“ se zobrazí nabídka všech dostupných formulářů (ukázka na **obr. 4**).

Obr. 4

Po vyplnění formuláře jsou před odesláním dotazu uživatelé vyzváni, aby se přihlásili do své datové schránky a vyplněný formulář její cestou odeslali. Zobrazí se jim přitom obrazovka na **obr. 5**.



Obr. 5

Vlastníci datových schránek rovněž jejich prostřednictvím dostávají bezplatně záznam o využívání údajů v základních registrech (výpisy jsou zasílány osobě, o které jsou tyto údaje vedeny), a to vždy za uplynulý

kalendářní rok a výpisy referenčních údajů při změně referenčního údaje. Datovými schránkami mají přístup do základních registrů i orgány veřejné moci.

Od března 2014 je obcím bez vlastního AIS umožněno využít údaje z registru obyvatel a agendového informačního systému evidence obyvatel na základě zákona č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů, zákona č. 131/2000 Sb., o hlavním městě Praze, ve znění pozdějších předpisů, a zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů, což nahrazuje dřívější praxi poskytování tzv. „změnových sestav“ obecními úřady s rozšířenou působností obcím I. a II. typu. Pro využití těchto údajů postupují obce dle „Manuálu pro obce“, který je uveřejněn na webových stránkách MV ČR (viz **kapitola 7**) a obsahuje aktuální odkaz na formulář.

3.3 Přístup k referenčním údajům prostřednictvím AIS

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**. Na rozdíl od přístupů popsaných v **kapitolách 3.1 a 3.2** tento přístup umožňuje OVM využívat i eGON služby určené pro hromadné výstupy nebo aktualizace (synchronní nebo asynchronní).

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

4 Co by měl OVM znát, než požádá o připojení AIS k ISZR

4.1 Identifikace AIS

OVM žádá o umožnění přístupu k referenčním údajům v základních registrech vznesením požadavku na SZR o vydání elektronického certifikátu, a to pro každý AIS zvlášť.

Každý AIS připojený k ISZR je jednoznačně identifikován následujícími údaji:

IČO úřadu identifikační číslo OVM, který je správcem AIS,

AIS_ID identifikátor AIS podle RPP (dříve podle IS o ISVS)

SN číslo certifikátu (**S**erial**N**umber),

Seznam agend seznam agend s registrovanou působností OVM, ve kterých AIS pracuje.

4.2 Správce AIS a působnost OVM v agendě

Správcem AIS je OVM. OVM má registrovanou působnost v agendě, ve které AIS pracuje. Správcovské OVM odpovídá za AIS i za účel a prostředky zpracovávání informací.

V některých případech správce AIS není totožný s OVM, který má působnost v agendě AIS. Typickým příkladem jsou „integrované“ AIS (v některých dokumentech publikovaných na webových stránkách 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 (buď v roli čtenáře anebo v roli editora).

V případě „integrovaných“ AIS musí jejich správce (**v součinnosti s implementátorem**) zajistit jednoznačnou identifikaci a autorizaci každého dotazu, resp. každého volání eGON služby, tj. AIS při volání příslušné eGON služby musí přenést v tzv. hlavičce dotazu informaci o tom, který OVM, v rámci které agendy a činnostní role konkrétní eGON službu volá. Toto zajistí buď využitím JIP/KAAS nebo vlastními prostředky.

4.3 Uživatelský AIS a jeho komunikace se základními registry

OVM v žádosti o certifikát uvádí vždy seznam agend, ve kterých AIS pracuje.

Pozor! Existují agendy, ve kterých mají OVM (obce) působnost (tj. byly Ministerstvem vnitra pro výkon agendy na základě oznámení působnosti v agendě zaregistrovány), ale k základním registrům v rámci těchto agend přistupovat nemohou.

Jedná se o následující agendy vyhrazené správcům registrů nebo speciálním AIS:

A100 Systém základních registrů,
A101 Základní registr – registr obyvatel,
A102 Základní registr – registr osob,
A103 Základní registr – registr územní identifikace,
A104 Základní registr – registr práv a povinností,
A110 Správa referenčních údajů RPP,
A112 Správa registru RPP,
A113 Registrace agend a orgánů veřejné moci pro výkon agendy,
A115 Evidence obyvatel a rodná čísla,
A116 Agenda cizinecká a ochrany státních hranic,
A117 Občanské průkazy,
A118 Cestovní doklady občanů České republiky,
A119 Informační systém datových schránek,
A124 Katastr nemovitostí,
A345 Czech Point – kontaktní místo veřejné správy.

Při podání žádosti o přístup k ZR pomocí aplikace RAZR OVM nemá možnost vybrat tyto agendy z nabídky agend, ke kterým lze získat certifikát pro přístup k ZR.

Přístup k nereferenčním údajům z AISEO a AISC:

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

4.4 Autentizace a autorizace přístupů a logování

K zajištění autentizace a autorizace přístupů uživatelů se OVM zavazuje při podání žádosti o připojení k ISZR, 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 OVM musí zajistit ověřování, zda uživatel (úředník OVM), který přistupuje 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 může přistupovat k referenčním údajům jen v těch činnostních rolích, ke kterým je oprávněn. Jednou z cest, jak toto zajistit, je využít ověřování uživatelů AIS v JIP.

4.4.1 Využití JIP/KAAS pro autentizaci a autorizaci

Základní vysvětlení, co znamenají zkratky JIP/KAAS lze nalézt v **kapitole 1.2** Vymezení použitých pojmů a zkratek.

JIP si lze představit jako zabezpečené adresářové úložiště informací o OVM, jeho AIS, uživatelích (úřednících) a jejich oprávněních. V rámci JIP se jednotlivým uživatelům přidělují agendy a činnostní role, ve kterých OVM oznámil působnost.

KAAS poskytuje služby pro autentizaci (tj. ztotožnění) uživatelů do AIS a pro editaci údajů v JIP. Používání služeb KAAS je podmíněno zaregistrováním AIS v JIP/KAAS, jeho nastavením ve Správě dat (funkční součást Czech POINT) a přidělením přístupových rolí podle RPP (podle údajů, jak OVM oznámil působnost v agendě).

Pokud OVM zaregistruje svůj AIS do JIP, potom přihlašovací údaje jednotlivých úředníků budou ověřovány vůči JIP prostřednictvím KAAS a bude zajištěno ověřování přidělených agendových činnostních rolí vůči matici oprávnění v RPP.

Uživatelé se pak do svého AIS přihlašují stejnými přihlašovacími údaji jako do Czech POINT a OVM nemusí vlastními prostředky řešit v rámci AIS autentizaci a autorizaci přístupů.

JIP/KAAS funguje tedy jako:

- nástroj, kterým OVM zaregistruje svůj AIS pro přístupy k základním registrům a plní úlohu správce přístupů k vnějšímu rozhraní ISZR, a jako
- nástroj pro správu uživatelských kont a dále jako
- nástroj pro přihlášení do aplikace RAZR

  Aplikace RAZR je v JIP registrována 2x:

  - RAZR-Internet: RAZR přístupný z Internetu na https://razr.egon.gov.cz
  - RAZR-KIVS: RAZR přístupný z KIVS na https://razr.egon.cms2.cz

  Dvojí registrace RAZR v JIP je vyžadována pravidly JIP pro registraci aplikací.

  Správce přidělí jednotlivým uživatelům v JIP pro přístup do RAZR jednu nebo více z následujících rolí:

  - „Prohlížení AIS (RAZR-Internet)“, „Prohlížení AIS (RAZR-KIVS)“: tato role opravňuje uživatele k prohlížení údajů o všech AIS ve správě subjektu a k prohlížení všech rozpracovaných požadavků za subjekt.

Role „Prohlížení AIS (RAZR-Internet)“ a „Prohlížení AIS (RAZR-KIVS)“ obsahují stejná oprávnění, liší se pouze tím, zda se vztahují k přístupu k aplikaci RAZR z Internetu nebo z KIVS.

- „Editace AIS (RAZR-Internet)“, „Editace AIS (RAZR-KIVS)“: tyto role opravňují uživatele k editaci i k prohlížení údajů o všech AIS ve správě subjektu a k editaci i prohlížení všech rozpracovaných požadavků za subjekt.

  Tato role tedy zahrnuje oprávnění role „Prohlížení AIS (RAZR-Internet)“, respektive „Prohlížení AIS (RAZR-KIVS)“.

  Role „Editace AIS (RAZR-Internet)“ a „Editace AIS (RAZR-KIVS)“ obsahují stejná oprávnění, liší se pouze tím, zda se vztahují k přístupu k aplikaci RAZR z Internetu nebo z KIVS.

4.4.2 Autentizace a autorizace zajištěná AIS nebo jiným způsobem

Autentizaci a autorizaci přístupů si může OVM zajistit sám, a to přímo v AIS, kterým k referenčním údajům přistupuje. Tento postup využijí nejvíce malé OVM s jednoduchou IT infrastrukturou. Dostatečnou bezpečnost a důvěryhodnost správy uživatelů a jejich ověřování musí zajistit implementátor AIS.

U větších OVM bývá správa uživatelů a jejich autentizace/autorizace zajištěna centrálně v některém systému na správu uživatelských identit (Identity Management, IdM).

4.5 Co je to certifikát

Digitální nebo též elektronický **certifikát** je v asymetrické kryptografii digitálně podepsaný veřejný šifrovací klíč, který vydává CA SZR. SZR používá formát X.509, který kromě jiného obsahuje informace o majiteli veřejného klíče a vydavateli certifikátu (tvůrci digitálního podpisu, tj. CA). Certifikáty jsou používány pro identifikaci protistrany při vytváření zabezpečeného spojení (HTTPS, VPN atp.). 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 dva tyto klíče patří k sobě.

Zjednodušeně: certifikát je nástroj, který slouží k autorizaci připojení AIS k vnějšímu rozhraní ISZR.

OVM musí privátní klíč zabezpečit proti jeho případnému zneužití, ztrátě nebo poškození. Pokud OVM poskytne privátní klíč implementátorovi AIS za účelem otestování jeho komunikace s vnějším rozhraním ISZR, měl by implementátora AIS písemně zavázat k ochraně a nezneužití privátního klíče.

5 Postup OVM pro připojení AIS k ISZR

5.1 Podmínky, které musí AIS splňovat pro připojení k ISZR

5.1.1 Podmínka autentizace přístupů všech uživatelů (využití JIP/KAAS)

Autentizaci a autorizaci všech úředníků přistupujících k vnějšímu rozhraní ISZR OVM zajistí jednoduše registrací svého AIS v JIP/KAAS.

Využívání JIP/KAAS není pro OVM povinné – (viz **kapitola 4.4**). 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. Po registraci AIS v JIP/KAAS správu uživatelů zajistí nástroje JIP a přistupující uživatelé do AIS budou autentizováni prostřednictvím KAAS. Úředníci, kteří pracují s Czech POINT, byli do JIP/KAAS zavedeni už před zahájením provozu základních registrů. K registraci uživatelů do JIP/KAAS 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/.

Správa dat OVM a RPP AIS Působnostní jsou aktualizovány informacemi o nových/rušených OVM z různých zdrojů a nezávisle na sobě. Z toho důvodu musí být OVM, žádající o certifikát pro přístup do ISZR, registrován jak ve Správě dat OVM, tak v RPP AIS Působnostní.

Registrace OVM v aplikaci Správa dat OVM je tedy jednou z podmínek, kterou musí OVM splnit, aby mohl zažádat o certifikát pro přístup do ISZR.

5.1.2 Podmínka registrace AIS v RPP (dříve IS o ISVS)

OVM může žádat o připojení k ISZR pouze pro AIS, který má přidělen identifikátor AIS_ID.

V rámci registru práv a povinností vede Ministerstvo vnitra evidenci informačních systémů veřejné správy. Před 25. 2. 2019 byla evidence vedena v Informačním systému o informačních systémech veřejné správy.

Pokud OVM neví, které z jeho AIS má zaregistrovány v RPP, přihlásí se do AIS Působnostního na https://rpp-ais.egon.gov.cz/AISP/verejne/domu.

Pro přístup k neveřejné části AIS Působnostní je třeba se přihlásit pomoci účtu v JIP, který Vám vytvoří Váš lokální administrátor. Učet v JIP pro roli editor ISVS musí mít následující oprávnění: "Přístup do informačních systémů", "RPP AIS Působnostní (Ministerstvo vnitra) Ohlašovatel působnosti v agendě", "Agendové činnostní role", "A113 – Registrace agend a orgánů veřejné moci pro výkon agendy", "CR56618 - Poskytování údajů o IS veřejné správy do evidence AIS".

5.1.3 Podmínka registrace agend

OVM může v žádosti o připojení k ISZR pro AIS uvést pouze agendy, ve kterých má oznámenou působnost.

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 vyzván, aby do 30 dnů oznámil výkon své působnosti v dané agendě.

Proces registrace agend není konečný. Stále budou vznikat nové agendy, zaregistrované agendy se budou v čase měnit, bude docházet ke změnám činnostních rolí a některé agendy také mohou zanikat. 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 vyzván k tomu, aby znovu oznámil působnost v agendě.

5.1.4 Podmínka oznámení působnosti v agendě

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.

Proces oznamování působnosti v agendě probíhá v působnosti Ministerstva vnitra. V rámci tohoto procesu OVM oznamují, kolik úředníků danou činnostní roli v agendě vykonává.

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 je na **obr. 7**.

Obr. 7

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

Obr. 8

a OVM zvolí jednu z nabízených možností.

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

5.1.5 Podmínka zajištění konektivity

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.

Pro zajištění konektivity SZR stanovila pravidla, která OVM najde v dokumentu „Síťová konektivita ISZR“, a dále v dokumentu „Sdílení připojení AIS k ZR verze 2“ (viz **kapitola 7**).

Základní pravidla pro zajištění konektivity jsou následující:

- každý AIS má statickou IP adresu (min. jednu, max. čtyři),
- sdílet jednu IP adresu mohou
    - všechny AIS jednoho OVM (pokud OVM využívá pro své IČO pouze jednu datovou schránku),
    - AIS jednoho OVM, které používají stejnou datovou schránku (pokud OVM využívá pro své IČO více datových schránek),
- různé OVM nemohou sdílet IP adresu,
- jako IP adresu v žádosti o certifikát OVM nesmí uvést
    - privátní IP adresu (s výjimkou 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 OVM v žádosti o certifikát takovou adresu uvede, SZR žádost zamítne.

OVM tedy:

- plně zodpovídá za veškerý provoz pocházející z registrované IP adresy. Komunikace daného OVM, nebo s daným OVM bude probíhat výlučně přes IP adresu uvedenou v registraci; OVM bere na vědomí, že v případě nestandardního chování dané IP adresy může být i odpojen od ISZR, a to až do sjednání nápravy.
- zajistí, že provoz AIS 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 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 SZR požaduje, aby každý OVM používal pro AIS, který spravuje,
- IP adresy, které pro komunikaci s ISZR nesdílí s AIS spravovanými jiným OVM; SZR umožní pro určitou IP adresu přístup k ISZR pouze pro OVM, který ji uvede v žádosti o certifikát jako první. Pokud tuto adresu uvede v žádosti později jiný OVM, SZR tuto žádost zamítne. SZR neřeší spory o oprávněnosti OVM používat určitou IP adresu.
- Při sdílení jednoho AIS více OVM (jedná se o případy různých integrovaných AIS) musí AIS zajistit správnou identifikaci toho OVM, který danou službu volá a údaje ze ZR využívá (v hlavičkách volání služby).
- Pokud je AIS provozován v lokální síti (používá privátní IP adresy), OVM v žádosti o certifikát uvádí adresu zařízení, které je poslední v článku propojení AIS – Internet. Pokud chce OVM pro daný AIS využívat asynchronní služby, musí si zajistit směrování odpovědí v rámci lokální sítě.

5.1.6 Podmínka splnění bezpečnostních požadavků na AIS

SZR stanovila bezpečnostní požadavky na AIS dokumentem „Bezpečnostní požadavky na AIS pro připojení k produkčnímu prostředí základních registrů“. Pro připojení k testovacímu prostředí ISZR se tento dokument použije obdobně.

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

- bezpečnost privátní části asymetrického klíčového páru – tj. bezpečnost soukromého klíče (viz **kapitola 5.3**),
- bezpečnost počítače, na kterém je AIS provozován,
- AIS musí být před připojením do produkčního prostředí otestován v testovacím prostředí,

- OVM má povinnost oznamovat SZR (na ServiceDesk) každé narušení bezpečnosti AIS nebo základních registrů,
- AIS se pro komunikaci s vnějším rozhraním ISZR autentizuje pomocí certifikátu vydaným SZR.

OVM při podání žádosti o připojení k ISZR prohlašuje, že se s dokumentem „Bezpečnostní požadavky na AIS pro připojení k produkčnímu prostředí základních registrů“ seznámil a že AIS 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 OVM 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.

5.1.7 Podmínka akceptace certifikační politiky SZR

SZR stanovila svou certifikační politiku dokumentem „Certifikační politika Správy základních registrů“.

SZR 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 SZR postupuje při vydávání certifikátů pro testovací prostředí obdobně jako pro produkční prostředí. Pro produkční i testovací prostředí SZR vyžaduje délku klíčového páru 2048 bitů a certifikáty jsou vydávány na 3 roky.

OVM při podání žádosti o připojení k ISZR prohlašuje, že se seznámil s dokumentem „Certifikační politika Správy základních registrů“ a že certifikační politiku SZR akceptuje.

5.1.8 Podmínka akceptace Provozního řádu ISZR

Provozní řád ISZR upravuje především vztahy mezi jeho subjekty a dále vymezuje základní pravidla provozu vnějšího rozhraní ISZR či informace o technické podpoře. OVM využívající vnější rozhraní ISZR akceptují a dodržují tento řád.

5.2 Příprava AIS pro „volání eGON služeb“

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

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

OVM by měl mít s dodavatelem uzavřenou dohodu (smlouvu) o dodání AIS a jeho dalším vývoji. Dodavatel na základě smluvního vztahu v průběhu „života AIS“ poskytuje OVM podporu pro jeho další vývoj.

Doporučuje se, aby OVM měl smluvně zajištěno, že změny AIS vyvolané legislativními změnami v právním řádu ČR poskytuje dodavatel AIS pro OVM bezplatně.

5.3 Vygenerování technické žádosti o certifikát

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

(Technickou) žádostí o certifikát se rozumí veřejná část asymetrického klíčového páru, kterou OVM připojuje k žádosti o připojení k ISZR.

SZR zpracovala a uveřejnila návod postupu vygenerování žádosti o certifikát. OVM tento návod nemusí obligatorně používat. Žádost o certifikát však musí být vygenerována v souladu s certifikační politikou SZR a musí obsahovat údaje podle návodu.

Na stránkách SZR v sekci pro správce AIS je uveřejněn návod https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2

5.4 Zaslání žádosti o připojení AIS k ISZR

OVM poté, co zajistí, aby jeho AIS splňoval podmínky podle **kapitoly 5.1** a byl připraven (implementátorem naprogramován) na volání příslušných eGON služeb podle **kapitoly 5.2**, a poté, co vygeneruje žádost o certifikát podle **kapitoly 5.3**, přistoupí do aplikace RAZR.

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

Aplikace RAZR je dostupná ze sítí KIVS (Komunikační infrastruktura veřejné správy) a Internet prostřednictvím CMS2 (Centrální místo služeb 2. generace).

- URL z Internetu = https://razr.egon.gov.cz
- URL z KIVS přes CMS2 = https://razr.egon.cms2.cz

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.

5.5 Dokončení instalace certifikátu na serveru OVM

Proces zpřístupnění základních registrů pro AIS dokončí OVM poté, co obdrží certifikát od SZR, jeho instalací na svém serveru. Při instalaci certifikátu postupuje OVM podle návodu „Postup pro vytvoření žádosti o digitální certifikát“.

OVM odpovídá za bezpečné uložení certifikátu a především za bezpečné uložení privátního klíče.

5.6 Instalace certifikátů certifikačních autorit SZR

Instalaci certifikátů CA SZR provádí OVM **v součinnosti se svým implementátorem AIS** nebo **s pracovníkem pro IT záležitosti**. Bez nainstalovaných certifikátů CA SZR OVM neověří důvěryhodnost certifikátů vydaných SZR.

Generování technické žádosti o certifikát (viz **kapitola 5.3**) není závislé na nainstalování certifikátů CA SZR. V případě jakýchkoliv pochybností o správnosti certifikátů CA SZR příslušné certifikáty neinstalujte a kontaktujte Service Desk SZR.

6 Správa AIS (změny připojení nebo změny přístupů k ISZR)

SZR 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 nebo zkrátit základní dobu jeho platnosti, tedy přistoupit k jeho zneplatnění). Všechny změny řeší OVM pomocí aplikace RAZR.

6.1 Vydání nového certifikátu při skončení platnosti dosavadního certifikátu

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

O nový certifikát OVM žádá vždy postupem popsaným v **kapitole 5**.

6.2 Zneplatnění certifikátu na žádost OVM

OVM požádá o zneplatnění certifikátu v případech vymezených Certifikační politikou SZR. 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 SZR (OVM sám zaznamená bezpečnostní incident, jakým je např. ztráta privátního klíče nebo zjištěný neoprávněný přístup k referenčním údajům),
- dojde ke změně AIS_ID,
- dojde ke změně IČO správce AIS (držitel certifikátu zanikne).

OVM o zneplatnění certifikátu (tedy o zrušení připojení AIS k ISZR) požádá pomocí aplikace RAZR.

6.3 Zablokování nebo zneplatnění certifikátu

Certifikát může být zablokován (dočasně) nebo zneplatněn (trvale). K zablokování, respektive zneplatnění může dojít buď na žádost držitele certifikátu (tím je OVM), nebo z podnětu SZR.

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

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

b) registrační autorita 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, CA SZR certifikát zneplatní a registrační autorita SZR odešle informaci o zneplatnění do datové schránky držitele certifikátu. Certifikát, jehož zneplatnění je požadováno, je zneplatněn bez zbytečného prodlení, zpravidla během jednoho pracovního dne.

7 Přehled webových odkazů

V této příručce jsou zmíněny předpisy, dokumenty nebo formuláře, které OVM 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. 227/2009 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o základních registrech, ve znění pozdějších předpisů	https://www.zakonyprolidi.cz/cs/2009-227
Nařízení vlády č. 161/2011 Sb., o stanovení harmonogramu a technického způsobu provedení opatření podle § 64 až 68 zákona o základních registrech	https://www.zakonyprolidi.cz/cs/2011-161
Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění zákona č. 183/2017 Sb.	https://www.zakonyprolidi.cz/cs/2016-297
Zákon č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce	https://www.zakonyprolidi.cz/cs/2016-298
Zákon č. 250/2017 Sb., o elektronické identifikaci	https://www.zakonyprolidi.cz/cs/2017-250
Zákon č. 251/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronické identifikaci	https://www.zakonyprolidi.cz/cs/2017-251
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. 528/2006 Sb., o formě a technických náležitostech předávání údajů do informačního systému, který obsahuje základní informace o dostupnosti a obsahu zpřístupněných informačních systémů veřejné správy	https://www.zakonyprolidi.cz/cs/2006-528
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://szrcr.cz/cs/referencni-udaje
Registrační autorita základních registrů (RAZR) - Uživatelská příručka pro OVM	https://szrcr.cz/cs/dulezite-dokumenty/63-uzivatelska-prirucka-razr-pro-ovm
Postup pro vytvoření žádosti o digitální certifikát	https://szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2
Proces připojování AIS k AISEO a AISC	https://szrcr.cz/cs/sluzby/spravci-a-vyvojari/kompozitni-sluzby-aiseo-a-aisc
Provozní řád ISZR	https://szrcr.cz/cs/dulezite-dokumenty
Certifikační politika SZR	https://szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2
Bezpečnostní požadavky na AIS	https://szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2
Síťová konektivita ISZR	https://szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2
Platné certifikáty CA SZR a HASH hodnoty certifikátů	https://szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2
Sdílení připojení AIS k ZR	https://szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2
Manuál pro obce (využívání údajů z ROB a EO)	https://www.mvcr.cz/clanek/manual-pro-obce.aspx