



Provozní řád

Informační systém základních registrů (ISZR)

Verze 1.1

Účinnost od: 1. 9. 2026



Obsah

1. Historie dokumentu	3
2. Vymezení použitých pojmů a zkratk	4
3. Úvod	6
4. Subjekty provozního řádu	7
4.1 Správcem a provozovatelem ISZR je DIA	7
4.2 Správce AIS	7
4.3 Provozovatel AIS	8
4.4 Správce SSVÚ	8
5. Provozní řád vnějšího rozhraní ISZR	8
5.1 Informační bezpečnost	8
5.2 Provozní doba ISZR a parametry poskytovaných služeb	9
5.3 Uživatelská podpora (Service Desk)	9
5.4 Pravidla pro rizikové činnosti informačního systému	9
5.4.1 Rizikové činnosti	9
5.4.2 Neplánovaná nedostupnost ISZR a základních registrů	10
6. Zajištění bezpečnosti základních registrů	11
6.1 Ochrana před neúměrným provozním zatížením a nesprávným používání eGON služby	11
6.2 Služby registrační a certifikační autority	12
6.3 Podmínky pro připojení AIS a SSVÚ k ISZR	12
6.3.1 Postup při připojování AIS nebo SSVÚ k ISZR	12
6.3.2 Změny údajů o AIS nebo SSVÚ	13
6.3.3 Připojení AIS nebo SSVÚ do ISZR	13
6.3.4 Úprava konfigurace kryptografických prostředků ISZR	14



1. Historie dokumentu

Verze	Datum	Autor	Popis
1.0	25.3.2023	Ing. Jitka Sládková Ph.D.	Vznik dokumentu
1.1	11.8.2026	Mgr. Rostislav Teplárek, MBA a kol.	Úprava a doplnění dle struktury vyžadované ve vyhlášce č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy

2. Vymezení použitých pojmů a zkratek

Pojem / Zkratka	Definice
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 vnějšího rozhraní informačního systému základních registrů. Správcem AIS je orgán veřejné moci.
AIS editační	je agendový informační systém, který edituje prostřednictvím speciálních služeb referenční údaje v základních registrech.
AIS spolupublikující (SPAIS)	je agendový informační systém, který ve vazbě na některý ze základních registrů, (spolu)publikuje na vnějším rozhraní ISZR nereferenční údaje ve vazbě na referenční údaje základních registrů. Příkladem SPAIS je informační systém evidence obyvatel (ISEO), který nereferenční data spolupublikuje ve vazbě na registr obyvatel.
DIA	je Digitální a informační agentura .
eGON služba	je webová služba publikovaná na vnějším rozhraní ISZR. Jde o služby poskytující referenční údaje ze základních registrů i služby poskytující zprostředkované údaje z jiných registrovaných AIS. Popisy formátu a struktury dotazu zaslaného AIS a formátu a struktury odpovědi ISZR a další potřebné informace jsou uvedeny v dokumentech publikovaných na webu DIA na https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari .
ISVS	Informační systém veřejné správy je provozován podle zákona o informačních systémech veřejné správy.
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.
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 se agendové informační systémy připravily 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.
NAKIT	je Národní agentura pro komunikační a informační technologie, s.p.
OVM	Orgán veřejné moci , je státní orgán, územní samosprávný 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.
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) nebo soukromoprávní systémy pro využívání údajů (SSVÚ). 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 a soukromoprávních systémů pro využívání údajů , je provozován podle zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů. 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.
SDM	Service Desk Manager je programová aplikace určená jako technologická podpora jednotného kontaktního místa pro uživatele služeb ISZR. Aplikace uživatelům umožňuje zadávat požadavky, sledovat jejich řešení, komunikovat s týmem podpory a získávat informace o všech důležitých provozních stavech poskytovaných služeb.
SSVÚ	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.
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.
Uživatel	je orgán veřejné moci nebo soukromoprávní uživatel údajů, který přistupuje jako čtenář nebo editor k referenčním údajům v základních registrech a k údajům v AIS, nebo který je správcem SPAIS



Vnější rozhraní ISZR	Hlavním uživatele jsou agendové informační systémy (služby umožňující využívání údajů ze základních registrů a editorů základních registrů).
Vnitřní rozhraní ISZR	hlavním uživatelem je pouze ISZR vůči základním registrům (vnitřní služby, které může využívat pouze ISZR pro získávání a dereferenci údajů z jednotlivých základních registrů)
Základní registry	Informační systémy veřejné správy uvedené v § 3 zákona č. 111/2009 Sb. Základními registry jsou Registr obyvatel (ROB), Registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci (ROS), Registr územní identifikace, adres a nemovitostí (RÚIAN) a 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 převod a ochranu osobních identifikátorů uložených v základních registrech.

3. Úvod

Systém základních registrů tvoří: ISZR, ROB, ROS, RÚIAN, RPP a převodník ORG. Základní registry a ORG mezi sebou komunikují prostřednictvím vnitřního rozhraní ISZR. Informační systém základních registrů (ISZR) je zřízen a provozován na základě zákona č. 111/2009 Sb., o základních registrech. Jeho správcem a provozovatelem je Digitální informační agentura. ISZR je informačním systémem veřejné správy ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.

Uživatelé mohou k referenčním údajům v základních registrech, příp. k údajům v jiných agendových informačních systémech (dále jen „AIS“), přistupovat prostřednictvím agendového informačního systému nebo soukromoprávního systému pro využívání údajů (dále jen „SSVÚ“). K přístupu využívají eGON služby publikované na vnějším rozhraní ISZR.

Provozní řád ISZR je souborem podmínek, pravidel a postupů, které jsou určující pro provoz ISZR. Zároveň vymezuje podmínky, za kterých provozovatel garantuje požadované funkce a služby poskytované informačním systémem. Provozní řád je závazný pro správce a provozovatele systému i pro všechny jeho uživatele. Při zjištění porušení tohoto Provozního řádu si správce informačního systému vyhrazuje právo zamezit uživatelům přístup k informačnímu systému do doby prokazatelného sjednání nápravy.

Tento provozní řád vydala Digitální a informační agentura jako správce informačního systému na základě vyhlášky č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy.



4. Subjekty provozního řádu

Tento provozní řád upravuje vztahy mezi jeho subjekty, kterými jsou:

- a) správce ISZR;
- b) provozovatel ISZR;
- c) správci základních registrů a převodníku ORG;
- d) správci AIS;
- e) provozovatelé AIS;
- f) správci SSVÚ;
- g) koncoví uživatelé.

4.1 Správcem a provozovatelem ISZR je DIA

4.2 Správce AIS

Správce AIS zajišťuje povinnosti podle zákona č. 111/2009 Sb., o základních registrech a odpovídá za to, že jím spravovaný AIS, jehož prostřednictvím přistupuje k vnějšímu rozhraní ISZR, je provozován v souladu se zákonem o základních registrech a v souladu s jinými právními předpisy.

Správce AIS, k tomu, aby mohl svůj AIS připojit k vnějšímu rozhraní ISZR musí dále:

- a) registrovat AIS v IS o ISVS – výjimku z registrace mají informační systémy veřejné správy, na které se nevztahuje zákon o informačních systémech veřejné správy; agendovým informačním systémům, které splňují tuto výjimku, přiděluje a vede identifikátor DIA a správce AIS žádá o jejich připojení k ISZR prostřednictvím zvláštního formuláře;
- b) mít v agendách, ve kterých AIS pracuje, oznámenou a zaregistrovanou působnost;
- c) mít konektivitu v KIVS na vnější rozhraní ISZR (výjimečně přístupem z internetu, není-li možné ji realizovat připojením přes KIVS);
- d) zajistit autentizaci a autorizaci všech úředníků přistupujících prostřednictvím AIS k vnějšímu rozhraní ISZR;

Správce editačního AIS navíc dále:

- a) zodpovídá za to, že jím zapsané referenční údaje jsou v souladu s údaji uvedenými v dokumentech, na jejichž základě jsou údaje do příslušného základního registru zapsány;
- b) zapisuje referenční údaj do základního registru nebo provádí jeho změnu prostřednictvím agendového informačního systému a bez zbytečného odkladu, nejpozději však do 3 pracovních dnů ode dne, kdy se o vzniku nebo o změně skutečnosti, kterou referenční údaj popisuje, dozví;
- c) v případě pochybnosti označuje referenční údaj jako nesprávný a toto označení odstraňuje neprodleně poté, co správnost údaje ověří;

Správce spolupublikujícího AIS (SPAIS), který je i editorem, navíc dále:

- a) ve spolupráci se správcem příslušného základního registru publikuje na vnějším rozhraní ISZR prostřednictvím eGON služeb nereferenční údaje;
- b) prostřednictvím správce ISZR stanovuje pravidla pro přístup AIS ke službám, pomocí kterých publikuje nereferenční údaje ze svého SPAIS, případně schvaluje přístupy AIS tamtéž;
- c) zajišťuje, že SPAIS obsahuje implementaci služby Probe (ověření funkčnosti obousměrné komunikační vazby mezi ISZR-SPAIS).



Správce spolupublikujícího AIS (SPAIS), který editorem není, zajišťuje podmínky stejně jako správce SPAIS, který je editorem.

Poznámky:

- Splnění podmínek uvedených pod písmenem d) správce AIS potvrzuje při odeslání žádosti prostřednictvím webové aplikace RAZR, kterou žádá o vydání certifikátu.
- Správcem AIS je obvykle jeho uživatel. Uživatel však nemusí spravovat AIS, jehož prostřednictvím přistupuje k referenčním údajům v základních registrech nebo k údajům v jiných AIS. Může k referenčním údajům a k údajům v jiných AIS přistupovat prostřednictvím tzv. „sdíleného AIS“. V takovém případě mluvíme o prostředí sdílených aplikací nebo sdílených technologií. Na správce AIS, který poskytuje přístup k referenčním údajům i jiným subjektům, než na který je AIS registrován v Rejstříku ISVS, se vztahuje odpovědnost v plném rozsahu i za přístup těchto jiných AIS.

4.3 Provozovatel AIS

Provozovatelem AIS je subjekt definovaný správcem AIS, který zajišťuje některé informační činnosti související s provozováním AIS.

4.4 Správce SSVÚ

Správce SSVÚ je povinen dodržovat všechny podmínky stanovené zákonem č. 111/2009 Sb., o základních registrech.

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.

5. Provozní řád vnějšího rozhraní ISZR

5.1 Informační bezpečnost

Za bezpečnost provozu AIS a SSVÚ a jeho bezpečné připojení k vnějšímu rozhraní ISZR odpovídá vždy jeho správce; stejně tak u sdíleného AIS, včetně k němu připojených AIS. Každý subjekt provozního řádu stanoví svým vnitřním předpisem nebo jiným způsobem pravidla informační bezpečnosti a s těmito pravidly své zaměstnance prokazatelně seznámí.

5.2 Provozní doba ISZR a parametry poskytovaných služeb

ISZR a Service Desk DIA jsou provozovány v nepřetržitém provozu.

Služby publikované na vnějším rozhraní ISZR jsou dostupné 24 hod denně, 7 dní v týdnu a jsou poskytovány s následujícími garantovanými parametry:

- a) maximální počet obdržených dotazů za sekundu 200; (součet všech požadavků registrovaných ke zpracování na vnějším rozhraní systému)
- b) maximální doba odezvy pro zpracování dotazu prioritní službou 2000 ms;
- c) maximální doba pro zpracování asynchronního dotazu 60 hodin.

Tato pravidla platí mimo plánované rizikové činnosti.

5.3 Uživatelská podpora (Service Desk)

Jediným kontaktním bodem mezi DIA a uživatelem, který uživateli poskytuje komplexní uživatelskou podporu, je oddělení Service Desk odboru Provoz IKT.

Uživatelé při řešení problémů souvisejících s využíváním ISZR využívají aplikaci Service Desk Manager (SDM).

Oddělení Service Desk (odbor Provoz IKT) neposkytuje uživatelskou podporu k dotazům nebo k žádostem o informace:

- na právní výklad zákonů;
- podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů;
- ke statistikám provozu ISZR;
- které nesouvisí s provozem ISZR.

Aplikace SDM je dostupná z webových stránek <https://helpdesk.dia.gov.cz/login-page>.

Uživatel se do aplikace může přihlásit bez autentizace (přístup „Občan“), nebo prostřednictvím svého účtu v JIP/KAAS či CAAIS (přístup „Orgán veřejné moci“). Aplikace poskytuje uživateli přehled o zadaném požadavku a o průběžném stavu jeho řešení. SDM je provozován v nepřetržitém provozu 24 hodin denně, 7 dní v týdnu, přičemž v časech od 18:00 do 7:00 hod, o víkendech a svátcích je poskytovaná podpora zaměřena pouze na řešení kritických incidentů – výpadků služeb.

5.4 Pravidla pro rizikové činnosti informačního systému

5.4.1 Rizikové činnosti

V rámci provozování informačního systému DIA, udržování vysoké dostupnosti a zachování jejich výkonnostních parametrů je nutné provádět některé technologické operace, které mohou mít dočasně vliv na kvalitu poskytovaných služeb. Pro tuto činnost jsou vydefinovány sledující stavy:

Jednotlivé kategorie rizikových činností jsou charakterizovány takto:

- a) **Riziková činnost kategorie „A“**



Operace, na provozním nebo testovacím prostředí, která nebude mít dopad na poskytování služeb na vnějším rozhraní systému. Všechna KPI a SLA zůstávají v platnosti.

Procesní parametry:

- Vyhrazené servisní okno není definováno.
- Povinnost provozovatele ohlásit plánovanou činnost nejméně 2 pracovní dny předem.
- DIA provede zanesení oznámení do celkového přehledu aktivit v rámci standardních informačních kanálů DIA.
- Provozovatel v komentáři oznámení uvede plánovaný počátek a konec odstávky s přesností na jednu hodinu.

b) Riziková činnost kategorie „B“

Operace, na provozním nebo testovacím prostředí, která způsobí snížení plnění kvalitativních parametrů, nikoliv však ztrátu dostupnosti služeb ve vyhrazeném servisním okně. V souladu s hodnocením SLA podle jednotlivých smluv je mezní hodnotou pro tuto kategorii rizikové činnosti 50% výkonnosti (KPI-2). Pod touto hranicí je systém považován za nedostupný.

Procesní parametry:

- Vyhrazené servisní okno pro rizikovou činnost kategorie „B“ je od pondělí do pátku v časovém okně od 22:00 do 06:00 hodin následujícího dne, v sobotu a v neděli, nebo o státních svátcích bez omezení.
- Žádost o povolení zasílá žadatel na DIA nejpozději do 12:00 hod, minimálně sedm pracovních dnů před samotnou realizací spolu s harmonogramem prací.
- DIA provede posouzení, potřebnou koordinaci a zašle žadateli souhlasné, nebo negativní stanovisko nejpozději do dvou pracovních dnů po doručení žádosti. DIA provede zanesení oznámení do celkového přehledu aktivit v rámci standardních informačních kanálů DIA.
- Žadatel v komentáři požadavku uvede plánovaný počátek a konec odstávky s přesností na jednu hodinu.

c) Riziková činnost kategorie „C“

Operace, na provozním nebo testovacím prostředí, která způsobí snížení plnění kvalitativních parametrů pod limit uvedený v písm. b), včetně řízené ztráty dostupnosti služeb ve vyhrazeném servisním okně.

Procesní parametry:

- Vyhrazené servisní okno pro rizikovou činnost kategorie „C“ je od pátku 22:00 do soboty 08:00 hodin a od 22:00 hod v sobotu do neděle 08:00 hodin.
- Žádost o povolení zasílá žadatel na DIA minimálně šest týdnů před samotnou realizací spolu s harmonogramem prací.
- DIA provede posouzení, potřebnou koordinaci a zašle žadateli souhlasné, nebo negativní stanovisko nejpozději do deseti pracovních dnů po doručení žádosti.
- DIA zabezpečí informování všech dotčených subjektů.
- Žadatel v komentáři požadavku uvede plánovaný počátek a konec odstávky s přesností na jednu hodinu.

5.4.2 Neplánovaná nedostupnost ISZR a základních registrů

V případě výpadků a jiných neplánovaných událostí Digitální a informační agentura využije pro informování uživatelů dvou komunikačních kanálů (alespoň jeden z nich bude vždy dostupný):



- a) informace jsou zveřejňovány na webu DIA;
- b) a také na <https://helpdesk.dia.gov.cz> a <https://sd.dia.gov.cz>.

6. Zajištění bezpečnosti základních registrů

Zajišťování bezpečnosti provozu celého systému základních registrů je jedním z hlavních úkolů Digitální a informační agentury, při jehož naplňování se řídí především zákonem o základních registrech a právními předpisy týkajícími se kybernetické bezpečnosti. Dojde-li k jakémukoliv narušení bezpečnosti ISZR, přijímá okamžitá opatření k jejímu obnovení. V případě, kdy zaznamenaná událost souvisí s nějakým AIS nebo SSVÚ, dle charakteru incidentu přijímá odpovídající bezpečnostní opatření a následně kontaktuje administrátora nebo správce dotčeného AIS nebo SSVÚ. V krajním případě provede dočasné zamezení přístupu z důvodu zabránění možnému narušení bezpečnosti ISZR. Návrat do původního stavu je vždy podmíněn vyřešením bezpečnostního incidentu.

DIA při monitorování vnějšího rozhraní ISZR zaznamenává zejména tyto události:

- a) neúspěšné pokusy o připojení k ISZR;
- b) neautorizované pokusy o volání eGON služeb na vnějším rozhraní ISZR;
- c) výskyt škodlivého kódu v ISZR;
- d) podezření na zneužití osobních údajů.

DIA zaznamenanou událost řeší.

Nebezpečné chování (bezpečnostní incident) nemusí být nutně zaznamenáno jen Digitální a informační agenturou. Může ji zaznamenat i sám uživatel (např. kompromitaci svého certifikátu nebo privátní části jeho klíče, zjištěným neoprávněným přístupem k referenčním údajům nebo k údajům v AIS nebo SSVÚ, zaznamenanou nedostupností dříve dostupné služby, chybějícími dříve dostupnými referenčními údaji). V takovém případě je uživatel (správce AIS nebo SSVÚ) povinen, v souladu s dokumenty „Certifikační politika“ a „Bezpečnostní požadavky na AIS“ nebezpečné chování (bezpečnostní incident) Digitální a informační agentuře neprodleně oznámit. Kybernetické bezpečnostní incidenty DIA hlásí Národnímu úřadu pro kybernetickou a informační bezpečnost.

Orgán veřejné moci se zavazuje dodržovat ustanovení zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů a jeho prováděcí právní předpisy, pokud se na něj vztahují. V této souvislosti např. významným informačním systémem podle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, není informační systém, jehož správcem je obec.

Má-li DIA důvodnou pochybnost, že orgán veřejné moci nebo soukromoprávní uživatel údajů neoprávněně přistupuje k osobním údajům, informuje neprodleně Úřad pro ochranu osobních údajů.

6.1 Ochrana před neúměrným provozním zatížením a nesprávným používáním eGON služby

V případě, že dochází k neúměrné zátěži ISZR nebo aktivity některého AIS či SSVÚ jsou v rozporu s pravidly a předpisy uvedenými v tomto dokumentu, si DIA vyhrazuje právo dočasně nebo trvale omezit přístup AIS nebo SSVÚ k rozhraní ISZR. Zrušení omezení je vždy podmíněno řádným ověřením DIA, že AIS nebo SSVÚ již tyto problémové aktivity neprovádí, resp. že nedochází k neúměrné zátěži ISZR.



6.2 Služby registrační a certifikační autority

Digitální a informační agentura za účelem umožnění přístupu orgánů veřejné moci ke službám vnějšího rozhraní ISZR vydává certifikáty, kterými se AIS nebo SSVÚ a jejich správci na vnějším rozhraní ISZR autentizují.

Digitální a informační agentura plní úkoly registrační a certifikační autority.

Správce agendového informačního systému nebo soukromoprávního systému pro využívání údajů žádá Digitální a informační agenturu předepsaným postupem o vydání certifikátu, a to pro každý AIS nebo SSVÚ. Registrační autorita Digitální a informační agentury žádost přezkoumá, v součinnosti s provozovatelem Centrálního místa služeb (NAKIT, s. p.) zabezpečí konektivitu AIS nebo SSVÚ na vnější rozhraní ISZR a neshledá-li v žádosti nedostatky, předá žádost certifikační autoritě Digitální a informační agentury, která certifikát vydá. Registrační autorita Digitální a informační agentury následně nastaví příslušná oprávnění v ISZR a informaci o vypořádání žádosti včetně certifikátu odešle do datové schránky žadatele.

Základní doba platnosti certifikátů, postupy správce AIS nebo SSVÚ při změnách v průběhu doby platnosti certifikátu a další informace jsou uvedeny v příslušných dokumentech Digitální a informační agentury.

O nový certifikát správce AIS nebo SSVÚ žádá Digitální a informační agentury nejdříve 3 měsíce před skončením platnosti dosavadního certifikátu. V případě zneplatnění dosavadního certifikátu, pokud správce AIS nebo SSVÚ nadále splňuje podmínky pro využívání údajů ze základních registrů a nechce činnost AIS nebo SSVÚ ukončit, žádá správce AIS nebo SSVÚ o nový certifikát bez zbytečného prodlení.

Lhůta pro vyřízení žádosti o vydání certifikátu, o změny k vydanému certifikátu nebo o zneplatnění certifikátu je 30 dnů.

6.3 Podmínky pro připojení AIS a SSVÚ k ISZR

6.3.1 Postup při připojování AIS nebo SSVÚ k ISZR

Podrobný návod, jak mají OVM nebo soukromoprávní uživatelé údajů postupovat při připojování svého AIS nebo SSVÚ k ISZR a další základní informace, poskytuje „Příručka pro správce AIS a SSVÚ“, která je v aktuálním znění dostupná na webu Digitální a informační agentury v sekci „Důležité dokumenty“.

Zajištění podmínek připojení: Základní podmínkou připojení je registrace AIS nebo SSVÚ v Rejstříku ISVS. Dále OVM nebo soukromoprávní uživatel údajů musí mít oznámenou působnost ve všech (zaregistrovaných) agendách, které AIS nebo SSVÚ realizuje.

OVM nebo SPUÚ současně při podání žádosti o připojení k ISZR potvrzuje, že jeho AIS nebo SSVÚ splňuje podmínky dokumentu „Bezpečnostní požadavky na AIS pro připojení k produkčnímu prostředí základních registrů“, že se seznámil s dokumentem „Certifikační politika DIA“ a že certifikační politiku DIA akceptuje. Oba dokumenty jsou dostupné na informačním webu základních registrů a propojeného datového fondu DIA (www.szrcr.cz) v sekci „Správci a vývojáři“. Dále musí přijmout odpovědnost za jednoznačnou autentizaci a autorizaci všech osob, které budou při výkonu působnosti v zaregistrované agendě prostřednictvím AIS nebo SSVÚ přistupovat ke službám vnějšího rozhraní ISZR, a že tyto osoby budou k dané činnosti oprávněny.



Pro zajištění komunikace AIS s vnějším rozhraním ISZR musí mít OVM zřízen přístup k internetu nebo musí být subjektem KIVS. Správce SSVÚ musí být vždy subjektem KIVS.

Příprava AIS nebo SSVÚ pro „volání eGON služeb“:

Přípravu na připojení AIS nebo SSVÚ k základním registrům zabezpečuje implementátor AIS nebo SSVÚ. Jejím předmětem je nastavení parametrů volání každé eGON služby tak, aby dotaz (tzv. hlavička dotazu) obsahoval informace identifikující OVM nebo SPUÚ, agendu, činnostní roli, uživatele atd.

Implementátoři najdou potřebné postupy a návody na webu DIA na <https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu>.

Vygenerování technické žádosti o certifikát:

Postup generování žádosti o certifikát je popsán v dokumentu „Postup pro vytvoření žádosti o digitální certifikát pro přístup k základním registrům“ dostupném na webu DIA na <https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu2>.

Technickou žádostí o certifikát se rozumí veřejná část asymetrického klíčového páru, kterou OVM nebo SPUÚ připojuje k žádosti o připojení k ISZR. Zaslání žádosti o připojení AIS nebo SSVÚ k ISZR: OVM/SPUÚ vyplní žádost o připojení AIS nebo SSVÚ k ISZR prostřednictvím webové aplikace RAZR.

Instalace certifikátu:

DIA zajistí vygenerování certifikátu, zřízení služby připojení AIS nebo SSVÚ k ISZR, zavedení certifikátu do systému ISZR a ORG a odeslání certifikátů do datové schránky úřadu. Proces zpřístupnění AIS/SSVÚ k základním registrům OVM/SPUÚ dokončí instalací certifikátu na svém serveru. Při instalaci certifikátu postupuje podle návodu uveřejněného na internetových stránkách DIA v sekci pro vývojáře.

6.3.2 Změny údajů o AIS nebo SSVÚ

Dojde-li v průběhu doby platnosti certifikátu na straně OVM/SPUÚ ke změně údajů, které uvedl v žádosti o připojení AIS/SSVÚ k ISZR, požádá o jejich zavedení. Změny se mohou týkat:

- údajů o osobě odpovědné za AIS/SSVÚ;
- údajů o provozovateli AIS/SSVÚ;
- údajů o kontaktní osobě pro IT záležitosti;
- změna IP adresy, ze které AIS nebo SSVÚ přistupuje k základním registrům;
- změna seznamu agend v AIS nebo SSVÚ obsažených.

Změny všech údajů OVM/SPUÚ oznamuje DIA prostřednictvím webové aplikace RAZR

6.3.3 Připojení AIS nebo SSVÚ do ISZR

Procesní postupy připojování k základním registrům prostřednictvím ISZR a základní technické principy komunikace jsou stanoveny v dokumentu „Podmínky pro připojení AIS do ISZR“, který je v aktuální verzi dostupný na webu Digitální a informační agentury v sekci „Důležité dokumenty“: <https://www.szrcr.cz/cs/dulezite-dokumenty>.

V návazném dokumentu „Katalog eGON služeb“ je uveden aktuální přehled eGON služeb, které jsou poskytovány na rozhraní ISZR. Dokument je mj. dostupný prostřednictvím odkazu uvedeného v



předchozím odstavci. Podrobný popis služeb je publikovaný na <https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu> v „Podrobném popisu eGON služeb“.

S rozhraním ISZR musí jednotlivé AIS nebo SSVÚ komunikovat výhradně přes URL adresu volané služby. URL adresy jednotlivých služeb jsou uvedeny v „Katalogu eGON služeb“.

Dodržování stanovených podmínek připojení a souvisejících pokynů jsou pro správce i provozovatele AIS nebo SSVÚ závazné. Rovněž je jejich povinností zamezit zneužívání čerpání údajů ze základních registrů, jako jsou např. nadbytečné a neoprávněné dotazy do základních registrů. V případě nedodržení přijme Digitální a informační agentura přiměřená opatření k nápravě stavu.

Nejčastější chyby v konfiguraci a implementaci AIS nebo SSVÚ pro přístup k základním registrům jsou popsány na webu Digitální a informační agentury na <https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu>

6.3.4 Úprava konfigurace kryptografických prostředků ISZR

Pro komunikaci s ISZR musí AIS nebo SSVÚ používat pouze protokol TLS 1.2, který odpovídá aktuálním bezpečnostním požadavkům na provoz ISZR.

V následující tabulce je uveden seznam kryptografických algoritmů (cipher suites) povolených k výše uvedenému datu na vnějším rozhraní ISZR:

Cipher Suite	Name (OpenSSL)	KeyExchange	Encryption	Bits	Cipher Suite Name (IANA)
[0x2f]	AES128-SHA	RSA	AES	128	TLS_RSA_WITH_AES_128_CBC_SHA
[0x35]	AES256-SHA	RSA	AES	256	TLS_RSA_WITH_AES_256_CBC_SHA
[0x3c]	AES128-SHA256	RSA	AES	128	TLS_RSA_WITH_AES_128_CBC_SHA256
[0x3d]	AES256-SHA256	RSA	AES	256	TLS_RSA_WITH_AES_256_CBC_SHA256
[0xc030]	ECDHE-RSA-AES256-GCM-SHA384	ECDH	AESGCM	256	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384