Digitální
a informační
agentura

Připojení agendových informačních systémů k základním registrům – sdílení připojení

Verze 2.8

Digitální a informační agentura
Na Vápence 915/14, 130 00 Praha 3
posta@dia.gov.cz

HISTORIE DOKUMENTU

Verze	Datum	Autor (útvar)	Popis
2.2	31. 05. 2013	OPICT a OKR SZR	Pracovní verze slučující předcházející verze. Neuveřejněno.
2.3	30. 06. 2013	OKR SZR	Formální úprava dokumentu podle směrnice SZR SME- 71/2013, řízení dokumentace (interní dokumentace SZR).
2.4	11. 07.2019	OPIKT SZR	RPP nahradil ISoISVS. Nová aplikace RAZR pro zadávání požadavků na správu přístupů AIS do základních registrů. Úprava pravidel pro agendy, které může mít AIS povolené.
2.5.	14.10. 2019	OSČ a OPIKT SZR	Aktualizace odkazů na dokumenty na novém webu SZR. Drobné upřesnění a úprav formátu dokumentu k publikaci.
2.6	1.4. 2023	OSČ	Aktualizace dokumentu v souvislosti s transformací SZR na DIA.
2.7	21.8.2025	Oddělení certifikačních autorit	▪ Grafická úprava dokumentu. ▪ Úprava kontaktu pro zasílání žádostí ohledně sdíleného AIS (kapitoly 1.4.1 a 2.2.1). ▪ Úprava pravidel pro používání IP adres (kapitola 2.1).
2.8.	20.8.2026	Oddělení řízení přístupu k referenčnímu rozhraní	▪ Grafická úprava dokumentu dle jednotného vizuálního stylu.

Obsah

HISTORIE DOKUMENTU 2
1. Úvod 4
1.1. Účel dokumentu 4
1.2. Rozsah působnosti 4
1.3. Existující dokumentace 4
1.4. Vymezení pojmů 4
1.4.1. Správce 4
1.4.2. Provozovatel 5
1.4.3. Uživatel 5
1.4.4. Certifikát 5
1.4.5. KIVS 5
2. Připojování AIS k ZR 6
2.1. Hlavní zásady 6
2.1.1. Zásady pro používání IP adres 6
2.1.2. Zásady pro připojování AIS k ZR 7
2.2. Technologický hosting 8
2.2.1. Technologická centra 8
2.2.2. Magistráty vs. městské části 8
2.3. Sdílený AIS 8
2.3.1. Žádost o připojení sdíleného AIS 9
2.3.2. Změny u uživatelských OVM/SPUÚ 9
3. Shrnutí – závěr 9

1. Úvod

1.1. Účel dokumentu

Tento dokument upřesňuje a doplňuje existující provozní dokumentaci Digitální a informační agentury (dále „DIA“), publikovanou na webových stránkách DIA (viz kapitola 1.3 tohoto dokumentu).

Hlavním cílem dokumentu je stanovení pravidel pro připojování agendových informačních systémů (dále jen „AIS“) a soukromoprávních systémů pro využívání údajů (dále jen „SSVÚ“) k základním registrům (dále jen "ZR") v prostředí sdílených aplikací a sdílených technologií. AIS komunikují se ZR prostřednictvím vnějšího rozhraní Informačního systému základních registrů (dále jen „ISZR“).

Dokument se nezabývá popisem výkonu státní správy ani výkladem souvisejících právních předpisů. Pojmy vymezené v tomto dokumentu jsou použity výhradně pro popis aspektů připojování k ZR a využívání informací z nich.

Pokud je v dokumentu uvedeno "AIS", myslí se tím jak AIS, tak SSVÚ.

1.2. Rozsah působnosti

Dokument je určen všem subjektům, které využívají data ze ZR, zejména správcům AIS.

1.3. Existující dokumentace[1]

- Příručka pro správce AIS a SSVÚ - připojení k základním registrům.
- Bezpečnostní požadavky na AIS.
- Certifikační politika.

1.4. Vymezení pojmů

1.4.1. Správce

Správce AIS je orgán veřejné moci (dále jen „OVM“)[2] a soukromoprávní uživatel údajů (dále jen „SPUÚ“).[3] Správce AIS musí být uveden v seznamu OVM/SPUÚ v Registru práv a povinností (dále jen "RPP"). Správce AIS musí mít AIS, který spravuje, zaregistrován v RPP.

Registrací v RPP získá AIS identifikátor (AIS_ID), který umožní jednoznačnou identifikaci AIS při jeho komunikaci se ZR.

[1] https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2
[2] § 2 písm. c) zákona č. 111/2009 Sb., o základních registrech
[3] § 2 písm. d) zákona č. 111/2009 Sb., o základních registrech

Správce AIS odpovídá za to, že AIS je provozovaný v souladu s právními předpisy[4], a dále odpovídá za dodržování provozních podmínek AIS ve vztahu k ZR. Přitom postupuje v souladu s provozní dokumentací DIA, která je uveřejněna na webu DIA.

Z hlediska využívání AIS různými OVM/SPUÚ je možné AIS rozdělit do dvou skupin:

- **„AIS“**, který slouží pouze k výkonu agend správce, ve kterých má správce zaregistrovanou vlastní působnost,
- **„sdílený AIS“,** který umožňuje, aby AIS využívalo více OVM/SPUÚ. Typickým příkladem sdíleného AIS jsou různé systémy elektronické spisové služby (sdílená aplikace).

Správce AIS v technické žádosti o certifikát uvádí mj. vždy své IČO a AIS_ID. Žádost následně pomocí aplikace RAZR zasílá na DIA. V RAZR dále mj. uvádí seznam agend, které AIS vykonává. Pokud správcovské OVM/SPUÚ nemá působnost v agendě, kterou žádá přidat, požádá o nastavení elektronicky na mailové adrese razr@dia.gov.cz (pouze pokud se jedná o agendy pro „sdílený AIS“).

Správce sdíleného AIS je povinen zajistit, aby v hlavičce dotazů zasílaných na vnější rozhraní ISZR byly vždy uvedeny identifikační údaje o uživatelském OVM/SPUÚ (viz kapitola 1.4.3). Tato identifikace žádajícího OVM/SPUÚ se následně promítá do denních reportů o provozu ZR[5].

1.4.2. Provozovatel

Provozovatel AIS je subjekt, u kterého je AIS provozován. Provozovatel AIS může být totožný se správcem AIS. Z hlediska DIA slouží údaj o provozovateli pouze pro případné dotazy k technické stránce AIS.

1.4.3. Uživatel

Uživatelem AIS je subjekt (OVM, SPUÚ), který při své činnosti využívá referenční údaje obsažené v příslušném ZR[6]. Uživatel AIS může být totožný s jeho správcem i provozovatelem.

OVM/SPUÚ k referenčním údajům v ZR (příp. k údajům v jiných AIS) přistupuje vždy prostřednictvím AIS.

Využívá-li OVM/SPUÚ pro přístup k referenčním údajům sdílený AIS, označujeme takový OVM/SPUÚ jako „**uživatelský OVM/SPUÚ**“ (viz kapitola 2.3).

1.4.4. Certifikát

Certifikát slouží k autorizaci připojení AIS k vnějšímu rozhraní ISZR. V certifikátu je mj. uvedeno IČO, které AIS spravuje včetně AIS_ID. Správce AIS nesmí soukromý klíč patřící k certifikátu poskytnout jinému AIS nebo jinému OVM/SPUÚ.

1.4.5. KIVS

Komunikační infrastruktura veřejné správy.

[4] AIS slouží k výkonu agendy nebo agend, které OVM vykonává podle konkrétních právních předpisů.

[5]) § 7 odst. 2 písm. h), j) zákona č. 111/2009 Sb.

[6])§ 5 odst. 1 zákona č. 111/2009 Sb.

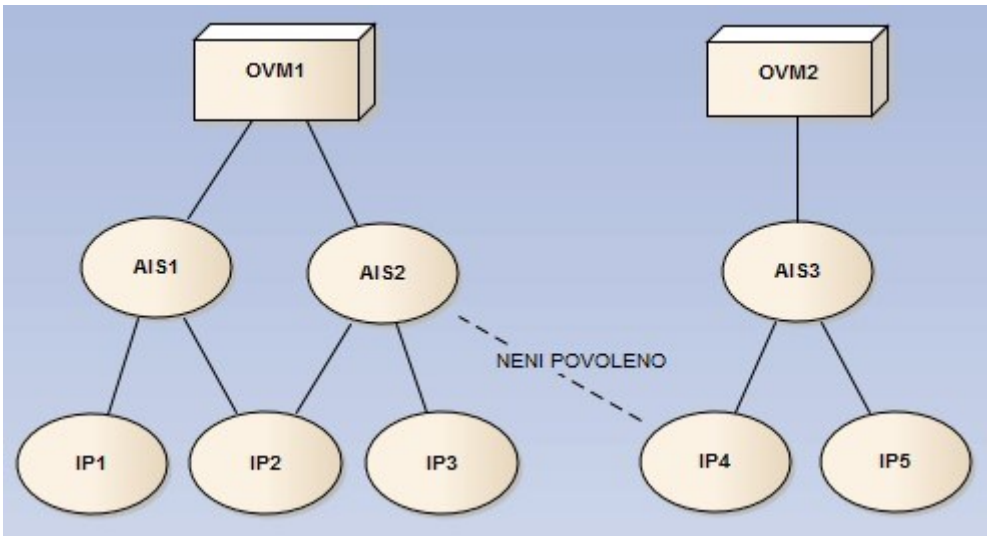
2. Připojování AIS k ZR

2.1. Hlavní zásady

V této kapitole jsou stručně shrnuty hlavní zásady, které je nezbytné dodržovat při připojování AIS k ZR. Tyto zásady jsou podrobněji popsány v dokumentech zmíněných v předchozích kapitolách. Jejich zopakování na tomto místě DIA považuje za užitečné, zejména z hlediska nutnosti jejich pamatování si a důsledného používání.

2.1.1. Zásady pro používání IP adres

Základní zásady pro používání IP adres vyplývají z následujícího obrázku:



Poznámka k obrázku: jedná se o výchozí stav, kdy ze strany DIA nebylo povoleno sdílení IP adresy mezi různými správci AIS.

Platí zejména, že:

- jeden AIS může používat maximálně 4 IP adresy,
- AISy různých správců nesmí používat stejné IP adresy – sdílení IP adres mezi správci je zakázáno, pokud jejich použití nepovolila DIA.
- IP adresy použité jedním správcem pro připojení AIS v testovacím prostředí nesmí být použity jiným správcem pro připojení AIS v produkčním prostředí,
- správce AIS může používat pro připojení AIS k ISZR pouze IP adresy, k jejichž používání je oprávněn (tj. byly mu přiděleny poskytovatelem služby připojení k síti internet nebo k síti KIVS nebo jiným subjektem na základě povolení DIA).

IP adresu/IP adresy, přes kterou/které AIS komunikuje s vnějším rozhraním ISZR, uvádí správce AIS při vyplňování žádosti o připojení do ZR v aplikaci RAZR. DIA vyžaduje, aby správce AIS zaregistroval pro AIS všechny IP adresy, které AIS používá. Dodržením uvedených pravidel je zajištěno jednoznačné přiřazení odpovědného správce AIS ke každé IP adrese.

DIA v dokumentu „**Bezpečnostní požadavky na AIS**“ správcům AIS dále doporučuje, aby:

- pro různé AIS používaly různé IP adresy (provoz jednotlivých AIS je potom identifikovatelný a oddělitelný na síťové vrstvě, což umožní jemnější diagnostiku a rychlejší a přesnější řešení případných problémů),
- používaly pro testovací a produkční prostředí různé IP adresy (umožní oddělení provozu v produkčním a testovacím prostředí již na síťové vrstvě).

Důvody pro uvedené bezpečnostní požadavky jsou následující:

- ISZR nedokáže na síťové vrstvě identifikovat jednotlivé AISy komunikující na stejné IP adrese. AIS se na vnějším rozhraní identifikuje a autentizuje certifikátem. Po ustavení spojení není na úrovni IP paketů možné poznat, od kterého AIS paket pochází, nebo kterému AIS je paket určen. Dojde-li při komunikaci mezi AIS a ISZR k takovým problémům, které jsou ze strany DIA detekovatelné pouze na síťové úrovni, DIA potřebuje komunikovat pouze s jedním správcem. DIA nemá nástroj, který by umožnil určit, který AIS z těch AIS, které používají jednu IP adresu způsobuje ve vztahu k ZR problémy. Takový stav by představoval bezpečnostní riziko typu „není určen odpovědný subjekt“.
- Správci AIS ale musí akceptovat fakt, že pokud DIA zakáže přístup k ISZR z nějaké IP adresy, týká se zákaz všech AIS, které jejím prostřednictvím k ISZR přistupují.
- Zajištění bezpečnosti při vracení odpovědí AIS pomocí asynchronních volání v aktivním režimu. U těchto volání ISZR navazuje spojení na IP adresu a na port 443. Pokud by však na tomto portu na příslušné adrese „poslouchalo“ více AIS, muselo by být pečlivě nakonfigurováno, který AIS data dostane. Skutečnost, že by data mohl dostat jiný AIS, než má, představuje bezpečnostní riziko.

DIA toto riziko akceptuje pouze za předpokladu, že je jasně určen subjekt, který zodpovídá za všechny AISy, které na IP adrese mohou poslouchat.

2.1.2. Zásady pro připojování AIS k ZR

Další zásady jsou popsány zejména v dokumentu „**Příručka pro správce AIS a SSVÚ - připojení k základním registrům**“. Jedná se o následující zásady:

- OVM/SPUÚ žádá o certifikáty pro AIS, které jsou v jeho správě (je jejich správcem). Správcovství OVM/SPUÚ pro AIS ověřuje DIA v RPP, neboť už při registraci AIS v RPP musí být u AIS uveden OVM/SPUÚ, který jej spravuje.
- OVM/SPUÚ nesmí certifikát a soukromý klíč použít pro jiný AIS, než pro který mu byl vydán. Nesmí je ani předat jinému OVM/SPUÚ, a to ani v případě, kdy tentýž AIS přejde pod správu jiného OVM/SPUÚ (viz dokument „**Certifikační politika**“).
- Správce AIS může povolit používání AIS libovolnému počtu uživatelských OVM/SPUÚ. Jejich identifikační čísla (IČO) se objevují ve voláních eGON služeb a jejich oprávnění kontroluje ISZR podle obsahu RPP. O uživatelských OVM/SPUÚ nevede DIA žádné informace.
- Správce AIS nemusí sám tento svůj AIS uživatelsky používat (tj. nemusí jeho prostřednictvím údaje ze ZR využívat).

- Správce AIS musí být zaregistrován v RPP k působnosti ve všech agendách, které pro AIS žádá, tj. včetně těch, která budou používat uživatelské OVM/SPUÚ příslušného AISu. O výjimkách rozhoduje DIA.
- V certifikátu je uvedeno IČO správcovského OVM/SPUÚ a číslo AIS. Z certifikátu nelze vyčíst, které uživatelské OVM/SPUÚ příslušný AIS používají.
- Hlavním partnerem pro komunikaci s DIA je správce AIS. Provozovatel AIS je účastníkem pouze běžné informativní komunikace. K žádostem o správu přístupů AIS k ZR jsou správci AIS povinni používat aplikaci RAZR - https://razr.egon.gov.cz/ z Internetu nebo https://razr.egon.cms2.cz/ z prostředí KIVS. Návod je na webových stránkách DIA.

2.2. Technologický hosting

Technologickým hostingem se rozumí umístění AIS více správců v jedné logické lokalitě (sdílení společné technologie).

2.2.1. Technologická centra

V případě technologických center je z hlediska komunikace se ZR důležité, prostřednictvím kolika IP adres může tato komunikace probíhat.

Mají-li všechny AIS umístěné v technologickém centru komunikovat prostřednictvím jedné IP adresy, respektive jedné skupiny IP adres, pak musí mít všechny tyto AIS jednoho správce, který všechny AIS hostované v technologickém centru zaregistruje v RPP a požádá pro ně o certifikát u DIA. Podmínkou je, že správce AIS musí mít zaregistrovanou působnost ve všech agendách, které hostované AIS vykonávají, nebo DIA musí AISu udělit výjimku pro používání dalších agend. Správcovské OVM/SPUÚ o výjimku požádá na e-mailové adrese razr@dia.gov.cz

Pokud takový správce neexistuje, je třeba zajistit, aby každý hostovaný AIS komunikoval s ISZR z různých IP adres. Poskytovatel připojení (k internetu nebo do KIVS) musí každému AIS přidělit unikátní IP adresu, respektive adresy.

2.2.2. Magistráty vs. městské části

Pokud magistrát města vystupuje vůči DIA jako správce AIS pro všechny městské části, pak všechny AISy městských částí mohou komunikovat z jedné IP adresy, respektive skupiny IP adres.

Pokud magistrát nechce, nebo nemůže být správcem AIS městských částí, pak vůči DIA vystupuje jako správce AIS každá jednotlivá městská část, která sama žádá o připojení a musí komunikovat přes unikátní IP adresu, respektive unikátní skupinu IP adres. Tuto adresu nemůže sdílet s jinými správci/městskými částmi ani správcem/magistrátem.

2.3. Sdílený AIS

Sdíleným AIS se rozumí případ, kdy jeden AIS je používán více „uživatelskými OVM/SPUÚ“. Sdílený AIS má pouze jednoho správce, který odpovídá za dodržování pravidel a za bezpečnost v souladu s

dokumentací DIA. V tomto případě uživatelský OVM/SPUÚ, protože není správcem sdíleného AIS, o certifikát nežádá.

Správce sdíleného AIS odpovídá za to, že jeho AIS je schopen vyhovět požadavkům kladeným na komunikaci AIS se ZR, zvláště v oblasti identifikace až na úroveň uživatele, který klade dotaz do ZR. Identifikace uživatelského OVM/SPUÚ se následně promítá do denních reportů a do záznamů o využívání údajů.

2.3.1. Žádost o připojení sdíleného AIS

RAZR při vyřizování žádostí mj. o certifikát dovoluje do formuláře žádosti zadat pouze agendy, které má správce AIS žádající o připojení registrovány v RPP, plus agendy, pro které má AIS výjimku.

V případě, že daný AIS využívá více uživatelských subjektů, podá jeho správce standardní žádost o připojení k ZR pro své agendy plus případně pro agendy, pro které má AIS výjimku.

2.3.2. Změny u uživatelských OVM/SPUÚ

Veškeré změny u „uživatelských OVM/SPUÚ“ (změna agend, aktualizace, zrušení) budou řešeny způsobem určeným DIA, vždy přes správce AIS.

3. Shrnutí – závěr

- Sdílený AIS znamená, že jeden AIS využívá více uživatelských OVM/SPUÚ, přičemž existuje pouze jeden správce tohoto systému.
- Správce sdíleného AIS odpovídá za dodržování pravidel a bezpečnost podle dokumentace DIA.
- Uživatelský OVM/SPUÚ není oprávněn žádat o certifikát, protože tuto povinnost plní správce sdíleného AIS.
- AIS musí být technicky schopen komunikovat se ZR, včetně identifikace uživatele, který vkládá dotaz do ZR.
- Identifikace uživatelského OVM/SPUÚ se promítá do reportů a záznamů o využívání údajů ze ZR.
- Správce AIS podává žádost o připojení k ZR pouze pro agendy registrované v RPP, případně pro ty, na které má výjimku.
- Při připojování sdílených AIS v technologických centrech je nutné sladit požadavky na správu AIS s technickými možnostmi, zejména v otázce adresace a využití IP adres.
- Využití omezeného počtu IP adres pro více AIS je možné pouze v případě, že existuje OVM/SPUÚ, které může být správcem většího počtu AIS.