Digitální a informační
agentura

Připojení agendových informačních systémů k základním registrům

– sdílení připojení

Verze 2.6

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.

OBSAH:

1 Úvod

1.1 Účel dokumentu

Tento dokument upřesňuje a doplňuje existující provozní dokumentaci Digitální a informační agentury (dále též „DIA“), publikovanou na webových stránkách DIA (viz kapitola 1.3.1 tohoto dokumentu).

Hlavním cílem dokumentu je stanovení pravidel pro připojování agendových informačních systémů (dále jen „AIS“) k základním registrům (dále také jen "ZR") v prostředí sdílených aplikací a sdílených technologií. AIS komunikují se základními registry 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 základním registrům a využívání informací z nich.

1.2 Rozsah působnosti

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

1.3 Vymezení pojmů

1.3.1 Síťové (IP) adresy

Bližší podrobnosti k používání IP adres a k problematice autorizace připojení jsou k dispozici v dokumentech:

- **„Příručka pro obce – Stručný návod pro připojení OVM k základním registrům“**[1] (v kapitole 5.1.5),
- **„Síťová konektivita ISZR“**[2] (v kapitole „Připojení k ISZR“),
- **„Bezpečnostní požadavky na AIS“**[3]
- **„Certifikační politika“**[4].

1.3.2 Správce

Správce AIS je orgán veřejné moci (dále jen „OVM“)[5]. Správce AIS musí být uveden v seznamu OVM 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 základními registry.

Správce AIS odpovídá za to, že AIS je provozovaný v souladu s právními předpisy[6], a dále odpovídá za dodržování provozních podmínek AIS ve vztahu k základním registrům. Přitom postupuje v souladu s provozní dokumentací Digitální a informační agentury, která je uveřejněna na webu DIA.

[1] Dokument je uveřejněn na https://www.szrcr.cz/cs/dulezite-dokumenty.
[2] Dokument je uveřejněn na https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2.
[3] Dokument je uveřejněn na https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2.
[4] Dokument je uveřejněn na https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu-2.
[5] § 2 písm. c) zákona č. 111/2009 Sb., o základních registrech
[6] Agendový informační systém slouží k výkonu agendy nebo agend, které orgán veřejné moci vykonává podle konkrétních právních předpisů.

Z hlediska využívání AIS různými OVM 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. Typickým příkladem sdíleného AIS jsou různé systémy elektronické spisové služby (sdílená aplikace).

Správce AIS v žádosti o certifikát, kterou zasílá na Digitální a informační agenturu, uvádí mj. vždy své IČO, AIS_ID, seznam agend, které AIS vykonává. Pokud správcovské OVM nemá působnost v agendě, kterou žádá přidat k certifikátům, požádá o nastavení elektronicky na mailové adrese ra@dia.gov.cz.

Správce sdíleného AIS je povinen zajistit, aby v hlavičce dotazů zasílaných na vnější rozhraní ISZR byly vždy uvedeny identifikační údaje o uživatelském OVM (viz kapitola 1.3.4). Tato identifikace žádajícího orgánu veřejné moci se následně promítá do denních reportů o provozu základních registrů[7].

1.3.3 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.

1.3.4 Uživatel

Uživatelem AIS je subjekt (OVM), který při své činnosti využívá referenční údaje obsažené v příslušném základním registru[8]. Uživatel AIS může být totožný s jeho správcem i provozovatelem.

OVM k referenčním údajům v základních registrech (příp. k údajům v jiných AIS) přistupuje vždy prostřednictvím AIS.

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

1.3.5 Certifikát

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

1.3.6 KIVS

Komunikační infrastruktura veřejné správy.

[7] § 7 odst. 2 písm. h), j) zákona č. 111/2009 Sb.
[8] § 5 odst. 1 zákona č. 111/2009 Sb.

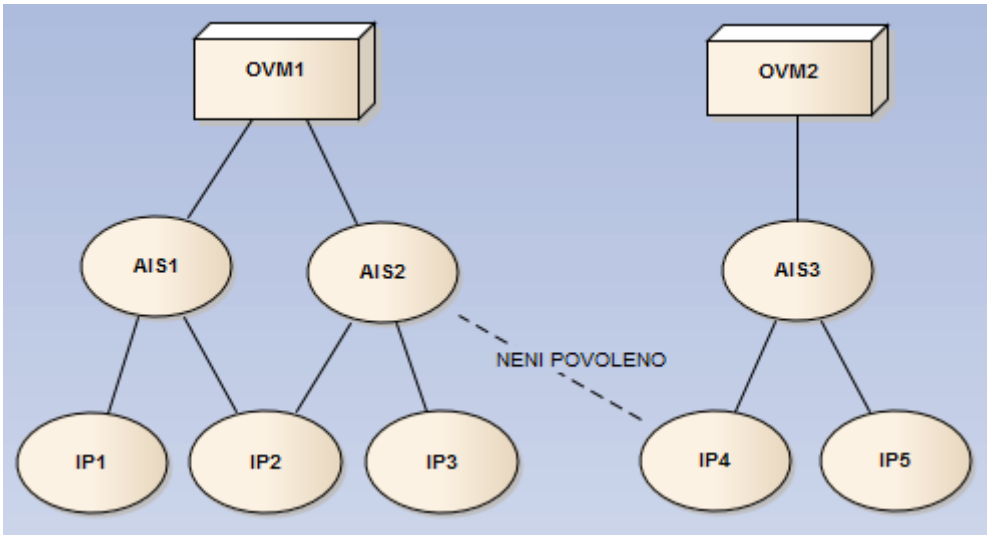
2 Připojování AIS k základním registrům

2.1 Hlavní zásady

V této kapitole jsou stručně shrnuty hlavní zásady, které je nezbytné dodržovat při připojování AIS k základním registrům. 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:



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 nepřípustné,
- 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).

IP adresu/IP adresy, přes kterou/které AIS komunikuje s vnějším rozhraním ISZR, uvádí správce AIS v žádosti o certifikát. 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 SZR detekovatelné pouze na síťové úrovni, SZR 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".

  DIA proto jako kompromis povolila sdílení IP adres mezi AISy téhož správce. 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 Další zásady pro připojování AIS k základním registrům

Další zásady jsou popsány zejména v dokumentu „**Příručka pro obce – stručný návod pro připojení OVM k základním registrům**". Jedná se o následující zásady:

- OVM žádá o certifikáty pro AIS, které jsou v jeho správě (je jejich správcem). Správcovství OVM pro AIS ověřuje DIA v RPP, neboť už při registraci AIS v RPP (dříve v IS o ISVS) musí být u AIS uveden OVM, který jej spravuje.

- OVM nesmí certifikát a soukromý klíč použít pro jiný AIS, než pro který mu byl vydán. Nesmí je ani předat jinému OVM, a to ani v případě, kdy tentýž AIS přejde pod správu jiného OVM (viz dokument „**Certifikační politika**").

- Správce AIS může povolit používání AIS libovolnému počtu uživatelských OVM. Jejich identifikační čísla (IČO) se objevují ve voláních eGON služeb a jejich oprávnění kontroluje ISZR podle obsahu RPP. O uživatelských OVM nevede DIA žádné informace.

- Správce AIS nemusí sám tento svůj AIS uživatelsky používat (tj. nemusí jeho prostřednictvím údaje ze základních registrů 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 příslušného AISu. O výjimkách rozhoduje DIA.

- V certifikátu je uvedeno IČO správcovského OVM a číslo AIS. Z certifikátu nelze vyčíst, které uživatelské OVM 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 základními registry 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 (dříve v IS o ISVS) 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 musela AISu udělit výjimku pro používání dalších agend.

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“. Sdílený AIS má pouze jednoho správce, který odpovídá za dodržování pravidel a za bezpečnost v souladu s dokumentací DIA. V tomto případě uživatelský OVM, 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 základními registry, zvláště v oblasti identifikace až na úroveň uživatele, který klade dotaz do základních registrů. Identifikace uživatelského OVM se následně promítá do denních reportů a do záznamů o využívání údajů.

2.3.1 Žádost o připojení sdíleného AIS

Současný aplikační systém podávání žádostí o certifikát (RAZR) 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

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

3 Shrnutí – závěr

Při připojování sdílených AIS a AIS hostovaných v technologických centrech je nutné sladit požadavky na správcovství AIS s reálnými technickými možnostmi adresace jednotlivých AIS. Využití omezeného počtu IP adres pro více AIS je možné pouze v případě, že existuje OVM, které může být správcem většího počtu AIS.