Jednotný identitní prostor

Provozní dokumentace

Vytvořeno dne: 21. 2. 2012
Aktualizováno: 18. 8. 2020
Verze: 1.6

Obsah

1. Úvod

1.1. Účel provozní dokumentace

Tato dokumentace upravuje postupy, které souvisejí s Jednotným identitním prostorem a správou dat uložených v JIP. Jedná se zejména o postupy

- Aktualizace údajů subjektu v JIP
- Aktualizace seznamu lokálních administrátorů subjektu
- Registrace AIS do JIP

Dokument dále obsahuje informace týkající se podmínek pro přihlašování uživatelů do integrovaných AISů prostřednictvím JIP/KAAS a zpracování osobních údajů.

1.2. Související dokumenty

[1] *Seznam datových schránek – Příručka pro statutárního zástupce*; dostupný z http://www.czechpoint.cz/data/formulare/files/SOVM_statutarni_zastupce.pdf

[2] Příručka pro SPUÚ; dostupný z http://www.czechpoint.cz/data/formulare/files/SPUU_statutarni_zastupce.pdf

[3] *Seznam datových schránek – Formuláře*; dostupný z http://www.czechpoint.cz/data/formulare/files/SOVM_formulare.pdf

[4] *Seznam OVM – Příručka pro lokálního administrátora*; dostupný po přihlášení do Správy dat z odkazu „Dokumentace" v patičce webové stránky

[5] *Czech POINT – Příručka pro garanta AIS*; dostupný z http://www.czechpoint.cz/data/formulare/files/prirucka_garant_AIS.pdf

[6] Příručka pro OTP přihlašování; dostupný z https://www.czechpoint.cz/data/prirucky/files/prihlasovani_OTP.pdf

1.3. Definice pojmů

Zkratka nebo pojem	Vysvětlení
AIS	Agendový informační systém
Garant AIS	Osoba, která odpovídá za provoz daného AIS.
ISoISVS	Informační systém o informačních systémech veřejné správy
ISZR	Informační systém základních registrů
JIP	Jednotný identitní prostor, zabezpečená adresářová služba obsahující údaje pro autentizaci a autorizaci uživatelů.
KAAS	Katalog autentizačních a autorizačních služeb Webové služby pro autentizaci uživatelů do AIS a pro správu dat uložených v JIP.
Lokální administrátor	Role uživatele pro správu údajů o subjektu a uživatelích v JIP.
MV ČR	Ministerstvo vnitra České republiky
OVM	Orgán veřejné moci
Subjekt	Orgány veřejné moci, orgány územní samosprávy a další úřady, které jsou evidovány v JIP Czech POINT.
ZR	Základní registry

2. Aktualizace údajů subjektu

Aktualizace údajů subjektu znamená oznámení aktuálních údajů o subjektu OVM autorizovaným způsobem, kdy je zajištěno, že oznámení podala oprávněná osoba subjektu. Na základě tohoto oznámení se provede aktualizace údajů subjektu OVM v JIP.

Aktualizaci údajů subjektu je nutné provést, aby se uživatelé OVM mohli přihlašovat do agendových informačních systémů (AIS), které autentizují uživatele vůči JIP.

Postup pro aktualizaci údajů subjektu se skládá z těchto kroků:

1. Žádost o předvyplnění formuláře pro aktualizaci údajů subjektu
2. Kontrola a aktualizace údajů subjektu ve formuláři
3. Uložení změn v údajích subjektu do JIP

Poznámka: Oznámení aktuálních údajů subjektu se netýká subjektů SPUÚ. Jejich údaje jsou do JIP přebírány z Rejstříku OVM a SPUÚ.

2.1. Kontrola provedení aktualizace údajů subjektu

Informaci, že daný OVM provedl aktualizaci údajů subjektu, lze dohledat na dvou místech.

Zkontroluje:

Kdokoliv

1. Veřejně v datových souborech se seznamem OVM.
   Zde je uvedena informace, zda a kdy provedl subjekt aktualizaci svých údajů. Tyto datové soubory jsou uloženy ve formátu XML a jsou určeny pro strojové zpracování.

Zkontroluje:

Lokální administrátor

2. Neveřejně v administrační aplikaci Správa dat (https://www.czechpoint.cz/spravadat/).
   Zde je v detailu subjektu uvedeno datum aktualizace údajů subjektu. Není-li uvedeno žádné datum, aktualizace nebyla subjektem ještě provedena. Tuto informaci dokáže ze Správy dat zjistit např. lokální administrátor daného OVM.

Práce se Správou dat je popsána v příručce pro lokálního administrátora **[4]**.

2.2. Žádost o předvyplnění formuláře pro aktualizaci údajů subjektu

Provádí:

Statutární zástupce nebo jím pověřená osoba

Statutární zástupce OVM nebo jím pověřená osoba si stáhne elektronický formulář pro aktualizaci údajů OVM, který je vystaven na adrese:

http://www.czechpoint.cz/public/urednik/ke-stazeni/

Otevře si stažený formulář a požádá o předvyplnění formuláře.

Formulář odešle do definované datové schránky MV ČR pomocí funkcionality ve formuláři nebo pomocí spisové služby úřadu.

Formulář je automaticky zpracován a do datové schránky OVM je doručen předvyplněný formulář.

Podrobné informace jsou popsány v příručce pro statutárního zástupce **[1]** a v pokynech pro práci s formuláři **[3]**.

2.3. Kontrola a aktualizace údajů subjektu ve formuláři

Provádí:

Statutární zástupce nebo jím pověřená osoba

Statutární zástupce OVM nebo jím pověřená osoba si stáhne doručený předvyplněný elektronický formulář z datové schránky.

Zkontroluje uvedené údaje subjektu ve formuláři a podle potřeby opraví neaktuální údaje.

Zkontrolovaný (případně i opravený) formulář odešle do definované datové schránky MV ČR pomocí funkcionality ve formuláři nebo pomocí spisové služby.

Podrobné informace jsou popsány v příručce pro statutárního zástupce **[1]** a v pokynech pro práci s formuláři **[3]**.

2.4. Uložení změn v údajích subjektu do JIP

Formulář je automaticky zpracován a údaje subjektu jsou uloženy do JIP. Do datové schránky OVM je doručena odpověď o výsledku zpracování formuláře.

3. Aktualizace seznamu lokálních administrátorů

Aktualizace seznamu lokálních administrátorů slouží k autorizovanému ověření správnosti seznamu lokálních administrátorů a autorizovanému oznámení případných změn na tomto seznamu.

Aktualizaci seznamu lokálních administrátorů je nutné provést, aby se uživatelé OVM mohli přihlašovat do agendových informačních systémů (AIS), které autentizují uživatele vůči JIP.

Postup pro aktualizaci seznamu lokálních administrátorů se skládá z těchto kroků:

1. Žádost o předvyplnění formuláře pro aktualizaci seznamu lokálních administrátorů
2. Kontrola a aktualizace seznamu lokálních administrátorů ve formuláři
3. Promítnutí změn v seznamu lokálních administrátorů do JIP

3.1. Kontrola provedení aktualizace seznamu lokálních administrátorů

Zkontroluje:

Lokální administrátor

Informaci, že daný OVM/SPUÚ provedl aktualizaci seznamu lokálních administrátorů, lze dohledat v administrační aplikaci Správa dat (https://www.czechpoint.cz/spravadat/).

Datum aktualizace seznamu lokálních administrátorů subjektu je uvedeno v detailu subjektu. Není-li uvedeno žádné datum, aktualizace nebyla ještě provedena. Tuto informaci dokáže ze Správy dat zjistit lokální administrátor.

Práce se Správou dat je popsána v příručce pro lokálního administrátora **[4]**.

3.2. Žádost o předvyplnění formuláře pro správu lokálních administrátorů

Provádí:

Statutární zástupce nebo jím pověřená osoba

Statutární zástupce OVM/SPUÚ nebo jím pověřená osoba si stáhne elektronický formulář pro správu lokálních administrátorů, který je vystaven na adrese:

http://www.czechpoint.cz/public/urednik/ke-stazeni/

Otevře si stažený formulář a požádá o předvyplnění formuláře. Formulář odešle do definované datové schránky MV ČR pomocí funkcionality ve formuláři nebo pomocí spisové služby.

Formulář je automaticky zpracován a do datové schránky OVM/SPUÚ je doručen formulář s aktuálním seznamem lokálních administrátorů, kteří jsou oprávněni spravovat OVM.

Podrobné informace jsou popsány v příručce pro statutárního zástupce OVM **[1]**, příručce pro SPUÚ **[2]** a v pokynech pro práci s formuláři **[3]**.

3.3. Kontrola a aktualizace seznamu lokálních administrátorů ve formuláři

Provádí:

Statutární zástupce nebo jím pověřená osoba

Statutární zástupce OVM/SPUÚ nebo jím pověřená osoba si stáhne doručený předvyplněný elektronický formulář z datové schránky.

Zkontroluje seznam lokálních administrátorů ve formuláři a podle potřeby v něm provede změny – tj. opraví údaje v účtech lokálních administrátorů a zakáže účty pro osoby, které již nezastávají roli lokálního administrátora.

Zkontrolovaný (resp. aktualizovaný) formulář odešle do definované datové schránky MV ČR pomocí funkcionality ve formuláři nebo pomocí spisové služby.

Podrobné informace jsou popsány v příručce pro statutárního zástupce **[1]**, příručce pro SPUÚ **[2]** a v pokynech pro práci s formuláři **[3]**.

3.4. Promítnutí změn v seznamu lokálních administrátorů do JIP

Formulář je automaticky zpracován a v JIP jsou provedeny operace s účty lokálních administrátorů podle pokynů ve formuláři. Do datové schránky OVM/SPUÚ je doručena odpověď o výsledcích provedených operací.

4. Registrace AIS do JIP

Registraci AIS do JIP je nutné provést, aby AIS mohl komunikovat s autentizační webovou službou KAAS pro autentizaci uživatelů do AIS při použití přihlašovacích údajů do Czech POINT, nebo na základě přihlášení uživatele prostřednictvím NIA.

Registrace AIS do JIP je určena pouze pro OVM. SPUÚ nemohou zaregistrovat své AISy do JIP Czech POINT. Uživatelé SPUÚ ale mohou přistupovat prostřednictvím JIP/KAAS do AISů, které mají v JIP zaregistrované orgány veřejné moci.

Postup registrace AIS do JIP se skládá z těchto kroků:

1. Podání žádosti o registraci AIS do JIP garantem AIS
2. Posouzení žádosti o registraci oprávněným pracovníkem MV ČR
3. Nastavení parametrů AIS pro komunikaci s KAAS
4. Povolení přístupu do AIS pro subjekty a uživatele

4.1. Podání žádosti o registraci AIS do JIP

Provádí:

Garant AIS

Garant AIS požádá o registraci AIS do JIP prostřednictvím elektronického formuláře, který je vystaven na adrese:

https://www.czechpoint.cz/public/vyvojari/ke-stazeni/

Pro registraci AIS do JIP není vyžadováno, aby byl AIS zaregistrován do ISoISVS ani do základních registrů.

Garant AIS v prvním kroku požádá pomocí formuláře o předvyplnění formuláře. Formulář odesílá do definované datové schránky MV ČR pomocí funkcionality ve formuláři nebo pomocí spisové služby.

Formulář je automaticky zpracován a do datové schránky subjektu garanta AIS je doručen formulář s předvyplněnými údaji.

Garant AIS doplní do předvyplněného formuláře základní informace o AIS – název AIS, účel použití, výčet legislativních předpisů, informace o provozovateli AIS. Vyplněný formulář odesílá do definované datové schránky MV ČR pomocí funkcionality ve formuláři nebo pomocí spisové služby.

Formulář je automaticky zpracován a do datové schránky subjektu garanta AIS je doručena odpověď o přijetí žádosti o registraci AIS a jejím zařazení do fronty žádostí ke schválení.

Podrobné informace jsou popsány v příručce pro garanta AIS **[5]**.

4.2. Posouzení žádosti o registraci AIS

Provádí:

Ministerstvo vnitra ČR

Pověřený pracovník MV ČR posoudí údaje v doručené žádosti o registraci AIS a rozhodne, zda bude žádost schválena nebo odmítnuta.

Výsledek rozhodnutí je odeslán do datové schránky subjektu garanta AIS. V případě zamítnutí žádosti se zasílá důvod zamítnutí, který uvedl pověřený pracovník MV ČR při zamítání žádosti.

4.3. Nastavení parametrů AIS pro komunikaci s KAAS

4.3.1. Přiřazení garanta AIS k zaregistrovanému AIS

Lokální administrátor v subjektu garanta AIS přiřadí ve Správě dat (https://www.czechpoint.cz/spravadat/) k zaregistrovanému AIS jednoho nebo více garantů AIS, kteří budou spravovat parametry AIS uložené v JIP.

Správu AISů však může provádět i samotný lokální administrátor; přiřazování garanta AIS v takovém případě není potřeba.

4.3.2. Nastavení parametrů AIS

Provádí:

Garant AIS

Garant AIS se přihlásí do aplikace Správa dat a zobrazí si detail zaregistrovaného AIS.

Nastaví parametry AIS, nezbytné pro komunikaci AIS s JIP – zejména webovou adresu pro příjem uživatelů z KAAS a autentizační certifikát (viz dokumentace s technickým popisem webových služeb KAAS).

Jako autentizační certifikát lze použít komerční serverový (systémový) certifikát, vydaný u některého z českých kvalifikovaných poskytovatelů služeb vytvářejících důvěru (I.CA, PostSignum, eIdentity).

Podrobné informace jsou popsány v příručce pro garanta AIS **[5]**.

4.4. Povolení přístupu do AIS pro subjekty a uživatele

Níže popsané řízení přístupu uživatelů do AIS, které nabízí JIP/KAAS, je volitelné. Pokud nebudou v AIS definovány žádné přístupové role do AIS, bude umožněn přístup do AIS jakémukoliv úspěšně autentizovanému uživateli. V tomto případě bude AIS autorizovat uživatele jiným způsobem (např. pomocí činnostních rolí).

4.4.1. Autorizace OVM/SPUÚ pro přístup do AIS

Provádí:

Garant AIS

Garant AIS definuje v aplikaci Správa dat seznam přístupových rolí pro přístup do samotného AIS.

Dále určí výčet autorizovaných OVM/SPUÚ, které budou mít povolen přístup do AIS. Těmto OVM/SPUÚ přiřadí definované přístupové role (všechny ze seznamu nebo jen vybrané), které potřebují pro práci v AIS.

Podrobné informace jsou popsány v příručce pro garanta AIS **[5]**.

4.4.2. Autorizace uživatelů OVM/SPUÚ pro přístup do AIS

Provádí:

Lokální administrátor

Lokální administrátoři autorizovaných OVM/SPUÚ přiřadí přístupové role do AIS konkrétním uživatelům v OVM/SPUÚ. Uživatelům mohou přiřadit jen ty role, které garant AIS přiřadil danému OVM/SPUÚ v nastavení AIS.

Podrobné informace jsou popsány v příručce pro lokálního administrátora **[4]**.

5. Přihlašování uživatelů do AISů integrovaných s JIP/KAAS

5.1. Podmínky pro úspěšné přihlášení uživatele

5.1.1. Uživatelský účet

Aby se mohl uživatel úspěšně přihlásit do AISu integrovaného s JIP/KAAS, musí mít zejména zřízen svůj uživatelský účet v JIP Czech POINT. Účet každého uživatele slouží pro specifikaci přístupových oprávnění uživatele do AISů. Účet musí mít i uživatelé, kteří se přihlašují prostřednictvím NIA.

Uživatelské účty zřizují lokální administrátoři subjektů OVM/SPUÚ.

5.1.2. Ztotožnění uživatele

Uživatel musí být dále tzv. ztotožněn – na základě identifikačních údajů uživatele (např. typ a číslo dokladu totožnosti) je ze základních registrů získán identifikátor AIFO, který je přiřazen k uživatelskému účtu. Identifikátor AIFO následně slouží pro jednoznačnou identifikaci osoby uživatele a je používán také během přihlašování uživatele prostřednictvím NIA.

Má-li uživatel v JIP založeno více uživatelských účtů (v jednom, ale i více subjektech), musí provést ztotožnění pro každý svůj uživatelský účet zvlášť.

Ztotožnění uživatele může provést lokální administrátor již při zakládání uživatelského účtu.

Neztotožnění uživatelé jsou ke ztotožnění vyzváni při prvním přihlášení pomocí přihlašovacích údajů do JIP Czech POINT. Přihlašování není dokončeno, dokud nedokončí ztotožnění.

Pokud uživatel zvolí v JIP/KAAS přihlášení prostřednictvím NIA, není vyzván k provedení ztotožnění. Při následném mapování identity NIA uživatele na účty v JIP jsou však neztotožněné účty uživatele ignorovány. Proto by uživatel měl provést ztotožnění u všech svých účtů, než začne používat přihlašování prostřednictvím NIA.

5.2. Autentizační metody JIP/KAAS

Garant AIS může v nastavení AIS v JIP specifikovat, jaké autentizační metody JIP/KAAS bude AIS „uznávat". Uživatelé pak musí používat některou z povolených autentizačních metod, aby se do AIS úspěšně přihlásili.

JIP/KAAS nabízí následující autentizační metody pro ověření uživatelů.

5.2.1. Uživatelské jméno a heslo

Jedná se o základní autentizační metodu. Zvolené heslo musí splňovat bezpečnostní požadavky na složitost hesla.

5.2.2. Uživatelské jméno, heslo a certifikát

Uživatel se autentizuje pomocí komerčního certifikátu a následně pomocí uživatelského jména a hesla. Jedná se tedy o dvoufaktorovou autentizaci.

Komerční certifikát musí být vydán komerční certifikační autoritou, kterou provozuje český poskytovatel služeb vytvářejících důvěru (I.CA, PostSignum České pošty, eIdentity).

5.2.3. Uživatelské jméno, heslo a OTP kód

Uživatel se autentizuje pomocí uživatelského jména, hesla a jednorázového OTP kódu, který si vygeneruje v hardwarovém zařízení, nebo v mobilní aplikaci. Jedná se o dvoufaktorovou autentizaci.

Způsob aktivace a používání této autentizační metody včetně seznamu kompatibilních mobilních aplikací lze nalézt v příručce pro OTP přihlašování **[6]**.

5.2.4. Přihlášení prostřednictvím NIA

V tomto případě provádí ověření uživatele Národní bod pro identifikaci a autentizaci (NIA) a JIP/KAAS čerpá údaje o ověřeném uživateli jako Service Provider.

Uživatel je z JIP/KAAS přesměrován do NIA. Zde si uživatel vybere identifikační prostředek a pomocí něj provede ověření své identity. Uživatel vybere, které své osobní údaje chce předat do JIP/KAAS, a následně je přesměrován zpět do JIP/KAAS.

JIP/KAAS se na základě údajů o uživateli pokusí vyhledat uživatelské účty uživatele v JIP. Uživateli nabídne seznam nalezených účtů a uživatel si vybere účet, pod nímž se hodlá přihlásit do cílového AISu. JIP/KAAS následně předá AISu údaje o uživateli, které načte ze zvoleného uživatelského účtu.

AIS ani JIP/KAAS nemohou přímo ovlivnit, jakou autentizační metodu si uživatel v rámci NIA vybere. Garant AIS však může v nastavení AIS v JIP definovat minimální úroveň záruk a uživatel pak bude muset v NIA použít identifikační prostředek, odpovídající definované úrovni záruk nebo vyšší.

6. Nakládání s osobními údaji

Nakládání s osobními údaji se řídí zákonem č. 110/2019 Sb., o zpracování osobních údajů a evropským nařízením č. 679/2016, tzv. GDPR.

6.1. Osobní údaje v účtech neztotožněných uživatelů

V uživatelských účtech úředníků v JIP musí být povinně uvedeno uživatelské jméno, jméno a příjmení. Tyto údaje jednoznačně určují subjekt osobních údajů jako fyzickou osobu.

Založením uživatelského účtu tedy dochází ke zpracování osobních údajů uživatele minimálně v rozsahu uživatelské jméno, jméno a příjmení.

Uživatel nebo lokální administrátor mohou nepovinně zadat do uživatelského účtu další údaje, jako je např. e-mailová adresa či telefonní číslo, které mohou být rovněž považovány za osobní údaje.

Subjekt údajů si může zobrazit rozsah uchovávaných osobních údajů o jeho osobě v JIP přihlášením do webové aplikace Správa dat a zobrazením profilu jeho uživatelského účtu.

Subjekt údajů může provést výmaz svých osobních údajů z JIP přihlášením do webové aplikace Správa dat, zobrazením profilu jeho uživatelského účtu a smazáním hodnot nepovinných dodatečných údajů. Subjekt údajů může požádat o výmaz těchto údajů také svého lokálního administrátora. Povinné údaje nelze smazat, ale lze jim za určitých okolností nastavit jiné hodnoty. Uživatelské jméno však změnit nelze.

6.2. Osobní údaje v účtech ztotožněných uživatelů

V okamžiku ztotožnění uživatele vůči registru obyvatel dochází v JIP k uložení osobních údajů uživatele pro potřeby autentizačního informačního systému podle § 56a zákona č. 111/2009 Sb, o základních registrech. Další informace o zpracování osobních údajů v autentizačním informačním systému jsou uvedeny v prohlášení o zpracování osobních údajů.