JIP/KAAS_

HELENA DUFFKOVÁ_
PAVEL TESAŘ_
ŠÁRKA HORNEKOVÁ_

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

ORGANIZAČNÍ ZÁLEŽITOSTI_

- Upozorňujeme účastníky, že z akce bude na základě oprávněného zájmu správce pořízen záznam.
- Pokud si nepřejete být na nahrávce identifikovatelní, prosím vypněte si kameru a mikrofon a pro komunikaci využívejte otázky a odpovědi (O+O/Q&A), které budou průběžně moderovány.
- Záznam bude zpřístupněn oprávněným uživatelům DIA a bude také zveřejněn neomezenému počtu uživatelů na YouTube kanálu Digitální a informační agentury, odkaz na něj umístíme na web Czech POINT (www.czechpoint.cz/public)

OBSAH_

- Co je JIP/KAAS / Správa dat
- Role a odpovědnosti
- Uživatel
- Lokální administrátor
- Registrace AIS do JIP
- Dokumentace / Kontakty

CO JE JIP/KAAS_

JIP (Jednotný identitní prostor)

- slouží ke správě uživatelů, jejich identifikaci, autentizaci a autorizaci, včetně jejich přístupových rolí a oprávnění;
- je autentizačním informačním systémem podle § 56a zákona č. 111/2009 Sb., o základních registrech.

KAAS (Katalog autentizačních a autorizačních služeb)

- představuje nadstavbu pro správu přístupů, poskytuje webové služby pro identifikaci, autentizaci a autorizaci uživatelů evidovaných v JIP;
- jeho služby jsou určeny pro přihlašování uživatelů aplikací informačního systému Czech POINT a Správy dat, jsou dostupné pro všechny registrované AISy jiných OVM, které je mohou využít jako sdílenou službu eGovernmentu.

CO JE JIP/KAAS_

- **JIP/KAAS je součástí referenční architektury eGovernmentu**
- **Je to zároveň součást kritické informační infrastruktury státu ve smyslu zákona o kybernetické bezpečnosti.**
- **Služba je provozována jako součást AIS Czech POINT**
- **Propojení s JIP využívá řádově 80 připojených agendových informačních systémů (AIS)**

SPRÁVA DAT_

Webová aplikace sloužící k administraci údajů Jednotného identitního prostoru

Aplikace je dostupná na adrese: https://www.czechpoint.cz/spravadat

Aplikaci mohou užívat všichni uživatelé s platnými přístupovými údaji, a to v rozsahu, který odpovídá jejich oprávněním (rolím).

ROLE_

Uživatel

- Držitel platných přístupových údajů informačního systému Czech POINT, fyzická osoba evidovaná v JIP.
- Může mít přiděleny různé role pro přístup do AISů registrovaných v JIP a/nebo činnostní role.

Lokální administrátor

- Spravuje uživatele jednotlivých subjektů využívajících informační systém Czech POINT.
- Je zodpovědný za celý životní cyklus uživatele v systému: zřizování účtů, přidělování rolí, deaktivace účtů.
- Zajišťuje správnost údajů o statutárním zástupci.
- Přihlašuje se pomocí uživatelského jména, hesla a OTP nebo komerčního certifikátu.

ROLE_

Statutární zástupce subjektu evidovaného v JIP

- Odpovídá za jmenování alespoň jednoho lokálního administrátora subjektu.
- Lokálním administrátorem může být i statutární zástupce samotný.

Národní administrátor

- Pracovník DIA, který zakládá nové subjekty v kategorii obcí a org. složek státu.

Garant AIS

- Mění konfiguraci AISu registrovaného v JIP.

ZDROJE DAT_

- Probíhá obousměrná výměna dat mezi JIP <---> RPP <–-> ROS
- JIP (aplikace Správa dat) načítá všechny nové OVM a SPUÚ z RPP a pokud v JIP nejsou, tak je zde založí a načte údaje o jejich statutárním zástupci z ROS.
- JIP načítá z RPP všechny působnosti v agendách a zapisuje je k subjektům OVM a SPUÚ.
- Zároveň je ale JIP editorem vybraných právních forem a zapisuje do ROS významnou skupinu subjektů:
  - obce, kraje, ministerstva a další organizační složky státu
  - státní vysoké školy ad.
- Pro tento účel máme proces samoobslužné aktualizace údajů o subjektu (pomocí datových schránek)

UŽIVATEL_

- Správa vlastního uživatelského účtu
- Kontrola přidělených rolí
- Přihlašování do agendových informačních systémů prostřednictvím JIP
- Zapomenuté heslo – resetuje Lokální administrátor
- Pokud nevíte, kdo je LA vaší organizace, mělo by to být v org. řádu nebo se lze dotázat helpdesku Czech POINT.

UŽIVATEL_ DVOUFAKTOROVÉ OVĚŘOVÁNÍ

- Certifikát
  - Komerční certifikát
  - Kvalifikovaný certifikát
- OTP
- NIA

UŽIVATEL_

živá ukázka

LOKÁLNÍ ADMINISTRÁTOR_

- **Správa subjektu**
  - Každé OVM má automaticky účet v JIP, není potřeba žádat o přístup.
  - Hlášení některých změn probíhá prostřednictvím formulářů odesílaných z datové schránky subjektu do datové schránky Automat SOVM vu33nsr.
    - Je důležité odeslat správně vyplněný formulář ve formátu ZFO.
    - Formuláře jsou dvoukrokové, je potřeba projít všechny fáze.
- **Správa uživatelů**
  - Probíhá v aplikaci Správa dat.
  - Lokální administrátor zakládá nové uživatele, poskytuje jim iniciální přihlašovací údaje a přiděluje přístupové a činnostní role do agendových informačních systémů.

LOKÁLNÍ ADMINISTRÁTOR_ SPRÁVA ÚDAJŮ OVM

- **Formulář pro aktualizaci údajů OVM**
  - https://www.czechpoint.cz/data/formulare/files/aktualizace_udaju_OVM.zfo
  - Používá se pro změnu vybraných údajů, které není možné editovat přímo ve Správě dat.
  - Změněné údaje se z JIP propíší do ROS.
- **Formulář pro správu lokálních administrátorů**
  - https://www.czechpoint.cz/data/formulare/files/sprava_lokalnich_administratoru.zfo
  - Vytvoření nového účtu lokálního administrátora
  - Správa účtů stávajících lokálních administrátorů
  - Nastavení správy subjektu externími administrátory z jiného subjektu

LOKÁLNÍ ADMINISTRÁTOR_ PŘIDĚLOVÁNÍ ROLÍ

- JIP načítá z RPP všechny působnosti v agendách a zapisuje je k subjektům OVM a SPUÚ.
- Subjekt má přístup jen do těch AIS, ke kterým má oprávnění na základě působnosti v RPP a do AIS, do kterých mu povolí přístup garant daného systému.
- Pouze do těchto systémů poté přiděluje přístup uživatelům svého subjektu prostřednictvím přístupových a činnostních rolí.
- Pro správné přidělení rolí k AIS se LA musí seznámit s dokumentací daného systému, aby věděl jaké konkrétní role je potřeba přidělit vybraným uživatelům.

LOKÁLNÍ ADMINISTRÁTOR_ ČINNOSTNÍ ROLE

- Vychází z RPP
- Možnost hromadného přidělení

PŘÍSTUPOVÉ ROLE_

- Nejsou řízeny RPP, správce AIS uděluje přístup konkrétním subjektům
- Role se přidělují uživatelům jednotlivě

LOKÁLNÍ ADMINISTRÁTOR_ SPRÁVA UŽIVATELŮ

- **Nastavení statutárního zástupce subjektu**
  - Probíhá prostřednictvím ikony korunky ve Správě dat.
  - Nový statutární zástupce musí projít procesem ověření totožnosti.

- **Povinností lokálních administrátorů není jen zakládání nových uživatelů, ale i zneplatnění přístupu po ukončení jejich pracovního poměru**

LOKÁLNÍ ADMINISTRÁTOR_

živá ukázka

REGISTRACE AIS DO JIP_

- Nárok na registraci AIS mají všechny OVM.
- Zároveň mohou mít jedno nebo více testovacích prostředí, která fungují na principu sand boxu, tzn. nejsou vzájemně nijak propojena ani mezi sebou ani s produkčním prostředím.
- Registrovaný AIS může využít dvě skupiny služeb:
  - Autentizační služby (přihlášení)
  - Editační služby (správa uživatelů a jejich rolí)

REGISTRACE AIS DO JIP_

Garant AIS se může rozhodnout, jakou metodu pro řízení přístupu do svého AIS použije. JIP/KAAS nabízí 2 metody, které se dají vzájemně i kombinovat.

1) **Metoda založená na tzv. Přístupových rolích**
   - Garant vytvoří v JIP tolik přístupových rolí, kolik potřebuje.
   - Přidělí je jednotlivě nebo hromadně subjektům (OVM).
   - Lokální administrátoři přidělí ty role, které má jejich subjekt dostupný, svým uživatelům.
   - JIP po autentizaci uživatele ověří, zda uživatel má alespoň jednu přístupovou roli pro daný AIS. Pokud ji nemá, přihlášení se neumožní vůbec.
   - AIS obdrží z JIP sadu identifikačních a autorizačních údajů (identifikace subjektu, uživatele, přístupové a činnostní role) a následně se sám rozhodne, co v jeho prostředí může uživatel dělat.

REGISTRACE AIS DO JIP_

Garant AIS zvolí tzv. úroveň důvěry (Level of Assurance = LoA), kterou jeho AIS vyžaduje.

- Obvykle pro agendové informační systémy registrované v RPP a napojené na ISZR platí, že je vyžadováno vícefaktorové přihlášení, tzn. nestačí jméno a heslo (faktor znalosti), ale uživatel musí prokázat faktor vlastnictví přihlašovacího prostředku (certifikát nebo mobilní aplikace atd.).
- Uživatelé mohou využít buď přihlašovací údaje JIP nebo přihlášení pomocí Identity občana (NIA), pokud Garant AIS tyto možnosti neomezil.
- Pokud uživatel má u svého účtu JIP registrován certifikát, nesmí se přihlašovat bez něj, i kdyby cílový AIS druhý faktor nevyžadoval.

REGISTRACE AIS DO JIP_

Garant AIS se může rozhodnout, jakou metodu pro řízení přístupu do svého AIS použije. JIP/KAAS nabízí 2 metody, které se dají vzájemně i kombinovat.

2) **Metoda založená na činnostních rolích z RPP**

- Vychází se působností jednotlivých OVM, tak, jak jsou zapsána v RPP.
- Lokální administrátoři přidělí uživatelům činnostní role, ve kterých jejich subjekt má působnost, podle toho, jaké konkrétní uživatel potřebuje vzhledem k organizačnímu zařazení.
- JIP dovolí každému uživateli každého OVM přihlášení do zvoleného AIS.
- AIS obdrží z JIP sadu identifikačních a autorizačních údajů (identifikace subjektu, uživatele, přístupové a činnostní role) a následně se sám rozhodne, co v jeho prostředí může uživatel dělat.

Výhoda: Garant AIS nemusí ručně přidělovat přístup subjektům, protože spoléhá na RPP (referenční údaje).

REGISTRACE AIS DO JIP_

1. **Podání žádosti o naplnění formuláře daty**
    1. Stáhněte elektronický formulář z webových stránek Czech POINT.
    2. Vyplňte a odešlete formulář do datové schránky Automat SOVM.
    3. Při vyplňování uveďte název AIS, účel použití, legislativní podporu a údaje o provozovateli AIS.
2. **Vyplnění vráceného předvyplněného formuláře**
    1. Do datové schránky vašeho subjektu dorazí předvyplněný formulář.
    2. Vyplňte údaje o registraci AIS, zadejte název AIS a další potřebné informace.
    3. Odešlete žádost o registraci AIS do JIP.
3. **Odeslání žádosti o registraci AIS do JIP**
    1. Odeslání žádosti lze provést automaticky přes datovou schránku nebo prostřednictvím spisové služby.
4. **Příjem odpovědi**
    1. Do datové schránky dorazí odpověď s výsledkem schválení žádosti.
    2. Po schválení může garant AIS nebo lokální administrátor provést konfiguraci AIS ve Správě dat.

REGISTRACE AIS DO JIP_

živá ukázka

DOKUMENTACE_

Metodické a uživatelské návody:

https://www.dia.gov.cz/egovernment/navody-ke-stazeni/

Provozní řád:

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

Dokumentace pro garanty AIS a vývojáře:

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

Některé další příručky jsou zde:

https://www.czechpoint.cz/dokumentace/prirucky/

KONTAKTY_

Uživatelská a technická podpora dostupná v pracovní dny od 8 – 18 hodin:

- telefon: 222 13 13 13
- e-mail: helpdesk@czechpoint.cz

DĚKUJEME ZA POZORNOST_

PROSTOR PRO VAŠE DOTAZY

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_