



Dokumentace

k projektu Czech POINT

JIP/KAAS: Autentizační webová služba

Procesní popis

Vytvořeno dne: 27. 9. 2011

Aktualizováno: 03. 12. 2024

Verze: 3.2

© 2011-2023 MVČR

© 2023-2024 DIA

Obsah

1.	Úvod	3
1.1.	Účel dokumentu	3
1.2.	Manažerské shrnutí	3
1.3.	Definice pojmů	3
2.	Informace o autentizačních službách JIP/KAAS	4
2.1.	Přehled autentizačních webových služeb JIP/KAAS	4
2.2.	Registrace AIS pro využívání autentizačních služeb JIP/KAAS	4
2.3.	Řízení přístupu uživatelů do AIS	5
2.4.	Správa činnostních rolí uživatelů v JIP	5
2.5.	Nakládání s osobními údaji	5
2.6.	Důležité odkazy	6
3.	Autentizační webová služba JIP/KAAS	7
3.1.	Stručný popis	7
3.2.	Detailní popis procesu autentizace a autorizace	7
3.3.	Technické informace	8
3.4.	Scénář komunikace a přenosu dat	10
4.	Přímá autentizační webová služba	13
4.1.	Stručný popis	13
4.2.	Detailní popis procesu autentizace a autorizace	13
4.3.	Technické informace	15
4.4.	Scénář komunikace a přenosu dat	16
5.	Odhlášení uživatele z JIP/KAAS a případně z NIA	19
5.1.	Stručný popis	19
5.2.	Detailní popis procesu	19
5.3.	Technické informace	20
5.4.	Scénář komunikace a přenosu dat	20
6.	Seznam změn	21

1. Úvod

1.1. Účel dokumentu

Tento dokument obsahuje procesní popis autentizace uživatelů do agendových informačních systémů (AIS) za využití přihlašovacích údajů do Czech POINT nebo na základě ověření uživatele pomocí identity občana v Národním bodu pro identifikaci a autentizaci (dále zkráceně NIA). AIS získává informace o uživateli a jeho subjektu prostřednictvím autentizačních služeb JIP/KAAS.

1.2. Manažerské shrnutí

Komponenty JIP/KAAS Czech POINT zastávají funkci tzv. autentizačního informačního systému podle § 56a zákona č. 111/2009 Sb., o základních registrech.

Tento dokument popisuje principy využívání autentizačních služeb JIP/KAAS. Tyto služby mohou využívat agendové informační systémy (AIS) pro ověření identity přístupujících uživatelů do AIS. Uživatelé se hlásí do JIP/KAAS pomocí svých přihlašovacích údajů do Czech POINT, nebo jsou přesměrováni k ověření do NIA.

Dokument dále popisuje předpoklady, které musí AIS splnit, aby mohl využívat autentizační služby JIP/KAAS. Tyto předpoklady zahrnují registraci AIS do JIP a následné nastavení AIS jeho správcem, aby komunikace mezi AIS a JIP/KAAS mohla fungovat korektně.

Tento dokument je určen pro ty, kteří se potřebují dozvědět o základních principech fungování autentizačních služeb JIP/KAAS a podmínkách, za kterých je možné tyto služby využívat.

1.3. Definice pojmů

Zkratka nebo pojem	Vysvětlení
AIS	Agendový informační systém
AIFO	Agendový identifikátor fyzické osoby
Autentizace	Ověření identity uživatele
Autorizace	Přidělení přístupových práv uživateli po jeho úspěšné autentizaci
ISZR	Informační systém základních registrů
JIP	Jednotný identitní prostor, adresářová služba obsahující údaje pro autentizaci a autorizaci uživatelů.
KAAS	Katalog autentizačních a autorizačních služeb
NIA	Národní bod pro identifikaci a autentizaci
OVM	Orgán veřejné moci
ROB	Registr obyvatel
SPUÚ	Soukromoprávní uživatel údajů podle § 2 zákona č. 111/2009 Sb., o základních registrech
Subjekt	Orgány veřejné moci, orgány územní samosprávy a další úřady či právnické osoby, které jsou evidovány v JIP Czech POINT.
Token	Autentizační a autorizační data, která držitele tohoto softwarového tokenu opravňují ke vstupu do systému a provádění povolených činností. (Nejedná se o hardwarové autentizační zařízení!)
URL	Uniform Resource Locator
WS	Webová služba

2. Informace o autentizačních službách JIP/KAAS

2.1. Přehled autentizačních webových služeb JIP/KAAS

JIP/KAAS Czech POINT poskytuje nyní dva typy autentizačních služeb:

- (klasická) autentizační webová služba JIP/KAAS
- přímá autentizační webová služba JIP/KAAS

Obě autentizační služby zajistí AISům ověření uživatele pomocí přihlašovacích údajů uložených v JIP Czech POINT, nebo na základě ověření uživatele pomocí identity občana v NIA. Obě webové služby vrací v odpovědi údaje o autentizovaném uživateli a subjektu, z nějž pochází.

Autentizační služby se od sebe liší průběhem autentizačního procesu a požadovanými vstupními údaji v zasílaných požadavcích.

Autentizační webové službě JIP/KAAS se v požadavku předává tzv. autentizační token. Tento token získá AIS po úspěšném ověření uživatele v JIP/KAAS. AIS musí provádět přesměrování dosud neautentizovaných uživatelů na přihlašovací stránku JIP/KAAS.

Přihlášení do AIS pomocí autentizační webové služby JIP/KAAS je pro uživatele maximálně komfortní. Přesun uživatele mezi AIS a JIP/KAAS je plně automatizován.

Přímé autentizační webové službě JIP/KAAS (ve verzi v3_3 či novější!) se v požadavku předává k ověření jednorázové uživatelské jméno a heslo.

Tyto údaje uživateli vygeneruje speciální webová stránka JIP/KAAS poté, co se uživatel úspěšně přihlásí pomocí svých přihlašovacích údajů uložených v JIP, nebo se úspěšně ověří pomocí identity občana v NIA. AIS musí svým uživatelům poskytnout webový odkaz na tuto speciální webovou stránku JIP/KAAS.

Přihlášení do AIS pomocí přímé autentizační webové služby JIP/KAAS je pro uživatele méně komfortní, protože musí ručně zadávat jednorázové přihlašovací údaje do přihlašovací stránky AIS. AIS ale nemusí implementovat funkci přesměrování uživatele do JIP/KAAS a zpět.

2.2. Registrace AIS pro využívání autentizačních služeb JIP/KAAS

Aby bylo možné využívat webové služby JIP/KAAS, musí správce AIS požádat o registraci AIS do JIP. Žádost vytvoří pomocí publikovaného elektronického formuláře, který odešle do další datové schránky Digitální a informační agentury.

Po zaregistrování AIS do JIP nastaví osoba v roli lokální administrátor v administračním rozhraní Správa dat parametry AIS potřebné pro komunikaci s JIP/KAAS.

Lokální administrátor může v nastavení AIS jmenovat další osoby do role Garant AIS a delegovat na ně činnosti spojené se správou AIS ve Správě dat.

2.3. Řízení přístupu uživatelů do AIS

Správa přístupových rolí do AIS

Lokální administrátor nebo Garant AIS může v nastavení AIS definovat seznam přístupových rolí do AIS. Může se jednat např. o role Čtenář, Editor, Administrátor, apod. Nejedná se o činnostní role používané pro řízení přístupu k referenčním údajům v základních registrech.

Řízení přístupu na úrovni OVM

Lokální administrátor nebo Garant AIS definuje v administračním rozhraní Správa dat výčet „autorizovaných“ OVM, které mohou přistupovat do AIS. Těmto OVM přidělí seznam výše zmíněných přístupových rolí do AIS, na které má daný OVM nárok. Pro OVM mohou být přiřazeny všechny vytvořené přístupové role, ale také pouze jen některé z nich.

Lokální administrátor nebo Garant AIS následně uvědomí jednotlivé OVM o udělení přístupu do AIS.

Výčet „autorizovaných“ OVM lze kdykoliv změnit.

Řízení přístupu na úrovni uživatelů

Lokální administrátoři „autorizovaných“ OVM přidělí v administračním rozhraní Správa dat jednu nebo více přístupových rolí do AIS uživatelům v OVM, kteří budou do AIS přistupovat.

Lokální administrátor „autorizovaného OVM“ může kdykoliv přístupové role odebrat nebo je přidělit novému uživateli.

AIS bez přístupových rolí

Pokud nejsou v nastavení AIS definovány žádné přístupové role, KAAS povolí přístup do takového AIS všem uživatelům z jakéhokoliv subjektu.

Řízení přístupu uživatelů si na své straně provádí dotyčný AIS na základě informací o uživateli, které AIS obdržel od webové služby JIP/KAAS. AIS může uživateli povolit přístup např. na základě činnostních rolí nebo na základě vlastních aplikačních rolí.

2.4. Správa činnostních rolí uživatelů v JIP

Subjektu OVM/SPUÚ v JIP jsou přiřazeny agendy a činnostní role, které mu byly určeny v rámci registrace agendy do RPP. Probíhá automatická synchronizace agend a činnostních rolí mezi JIP a základními registry.

Ze seznamu činnostních rolí, přidělených k subjektu OVM/SPUÚ, následně lokální administrátor přiřazuje konkrétní činnostní role konkrétním uživatelům v subjektu.

2.5. Nakládání s osobními údaji

Komponenty JIP/KAAS Czech POINT jsou autentizačním informačním systémem podle § 56a zákona č. 111/2009 Sb., o základních registrech.

Na základě tohoto legislativního zmocnění jsou v JIP Czech POINT uloženy osobní údaje uživatelů, které jsou předávány agendovým informačním systémům.

Další informace o zpracování osobních údajů v autentizačním informačním systému jsou uvedeny v [prohlášení o zpracování osobních údajů](#).

2.6. Důležité odkazy

Webová stránka s elektronickým formulářem pro registraci AIS do JIP a s příručkou pro Garanta AIS:

<http://www.czechpoint.cz/public/vyvojari/ke-stazeni/>

Webová adresa administrační aplikace Správa dat:

<https://www.czechpoint.cz/spravadat/>

3. Autentizační webová služba JIP/KAAS

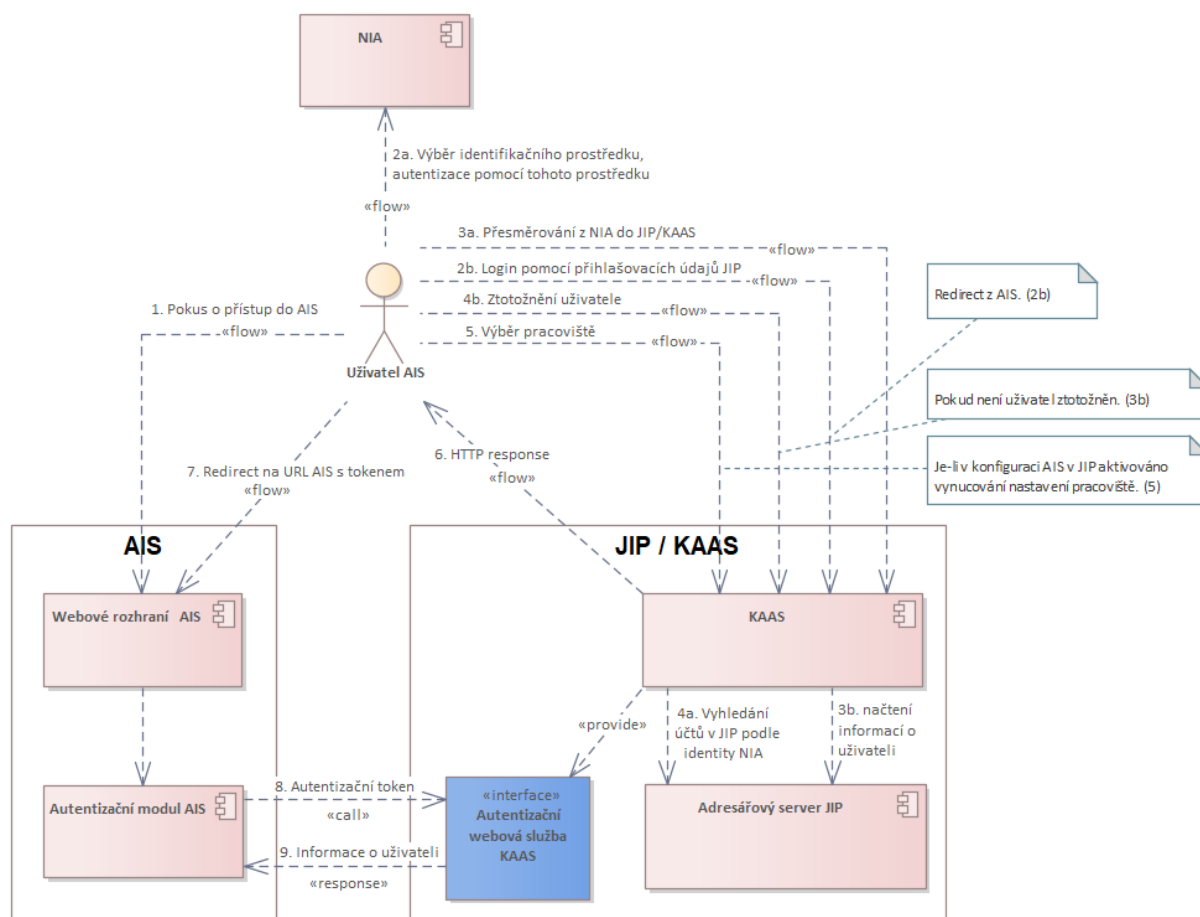
3.1. Stručný popis

Autentizační webová služba JIP/KAAS funguje na následujícím principu.

AIS přesměruje neautentizované uživatele do JIP/KAAS. Zde si uživatel vybere způsob přihlášení. Vybere-li si ověření prostřednictvím identity občana, je přesměrován do NIA, kde si zvolí identifikační prostředek a jeho prostřednictvím prokáže svoji identitu, následně je přesměrován zpět do JIP/KAAS. Pokud si uživatel vybere v JIP/KAAS jinou autentizační metodu, zadá odpovídající přihlašovací údaje a JIP/KAAS ověří jejich platnost v JIP. Ověřený uživatel je přesměrován zpět do AIS. AIS následně odešle požadavek do autentizační webové služby JIP/KAAS a v odpovědi získá údaje o autentizovaném uživateli.

Pro využívání autentizační služby JIP/KAAS musí AIS implementovat podporu přesměrování neautentizovaných uživatelů do JIP/KAAS a poskytovat webovou stránku, která přijímá ověřené uživatele z JIP/KAAS.

3.2. Detailní popis procesu autentizace a autorizace



Uživatel přistoupí na webovou stránku AIS (1).

Systém rozpozná, že uživatel není autentizován, a přesměruje jej na webovou stránku JIP/KAAS. Zde si uživatel vybere, jakým způsobem se přihlásí.

Pokud si uživatel zvolil přihlášení prostřednictvím identity občana (NIA), jsou provedeny tyto kroky:

- Uživatel je přesměrován do NIA (2a). V NIA si uživatel vybere identifikační prostředek, jeho prostřednictvím prokáže svoji identitu a vybere údaje, které chce poskytnout do JIP/KAAS.
- Následně je uživatel přesměrován zpět z NIA do JIP/KAAS včetně jeho osobních údajů (3a).
- Na základě předaných údajů z NIA získá JIP/KAAS identifikátor AIFO, pomocí kterého se pokusí vyhledat odpovídající uživatelský účet v JIP (4a).
- Pokud je nalezeno více odpovídajících účtů, uživatel si vybere, pod kterým účtem se chce přihlásit.

Pokud si uživatel zvolil přihlášení pomocí některé z autentizačních metod v JIP/KAAS, jsou provedeny tyto kroky:

- Uživatel zadá příslušné přihlašovací údaje a JIP/KAAS ověří jejich správnost (2b).
- Po úspěšné autentizaci načte JIP/KAAS z JIP informace o uživateli, jeho domovském subjektu OVM/SPUÚ a přidělených rolích (3b).
- V případě úspěšného přihlášení se dále zkontroluje, jestli je uživatel ztotožněn. Pokud ne, JIP/KAAS zobrazí webovou stránku pro ztotožnění osoby a uživatel musí zadat údaje pro provedení ztotožnění. JIP/KAAS, jakožto autentizační informační systém, získá z registru obyvatel AIFO a osobní údaje uživatele podle § 56a zákona č. 101/2009 Sb., o základních registrech (4b).

Další kroky jsou společné pro uživatele autentizovaného prostřednictvím NIA i autentizovaného prostřednictvím přihlašovacích údajů do JIP.

Pokud je v konfiguraci AIS v JIP aktivováno vynucování nastavení pracoviště, JIP/KAAS dále zobrazí uživateli webovou stránku pro nastavení pracoviště a uživatel musí buď potvrdit jemu aktuálně přiřazené pracoviště, nebo ze seznamu vybrat správné pracoviště, v němž vykonává činnost (5).

JIP/KAAS ověří, že autentizační metoda, kterou uživatel použil, splňuje požadavky na způsob autentizace, nastavené v konfiguraci AIS v JIP.

JIP/KAAS dále provede kontrolu rolí přidělených uživateli, zda je uživatel oprávněn přistoupit do AIS. Je-li kontrola úspěšná, pokračuje se dalším krokem, jinak je uživateli zobrazeno hlášení o zamítnutí přístupu.

JIP/KAAS vygeneruje autentizační token pro uživatele a přesměruje uživatele s tokenem na definovanou adresu AIS. Hodnotu adresy zjistí z konfigurace AIS v JIP. (6+7).

Autentizační modul AIS zavolá autentizační webovou službu JIP/KAAS za účelem získání informací o uživateli. Webové službě předá autentizační token (8). Pokud je token platný, AIS v odpovědi obdrží informace o uživateli (9). Pokud AIS zavolá správnou verzi autentizační webové služby JIP/KAAS, obdrží v odpovědi osobní údaje uživatele podle § 56a odst. 3 zákona č. 101/2009 Sb., o základních registrech.

AIS posoudí na základě předaných informací o uživateli, zda umožní uživateli přístup do AIS.

3.3. Technické informace

Pro komunikaci mezi JIP/KAAS a AIS se používá autentizační webová služba:

- WS na straně JIP/KAAS přijímá od AIS autentizační tokeny. V odpovědi vrací informace o uživateli, pro nějž byl token vystaven (v případě platného tokenu) nebo chybový kód (v případě neplatného tokenu).

Komunikace je zabezpečena pomocí protokolu TLS a autentizace certifikátem.

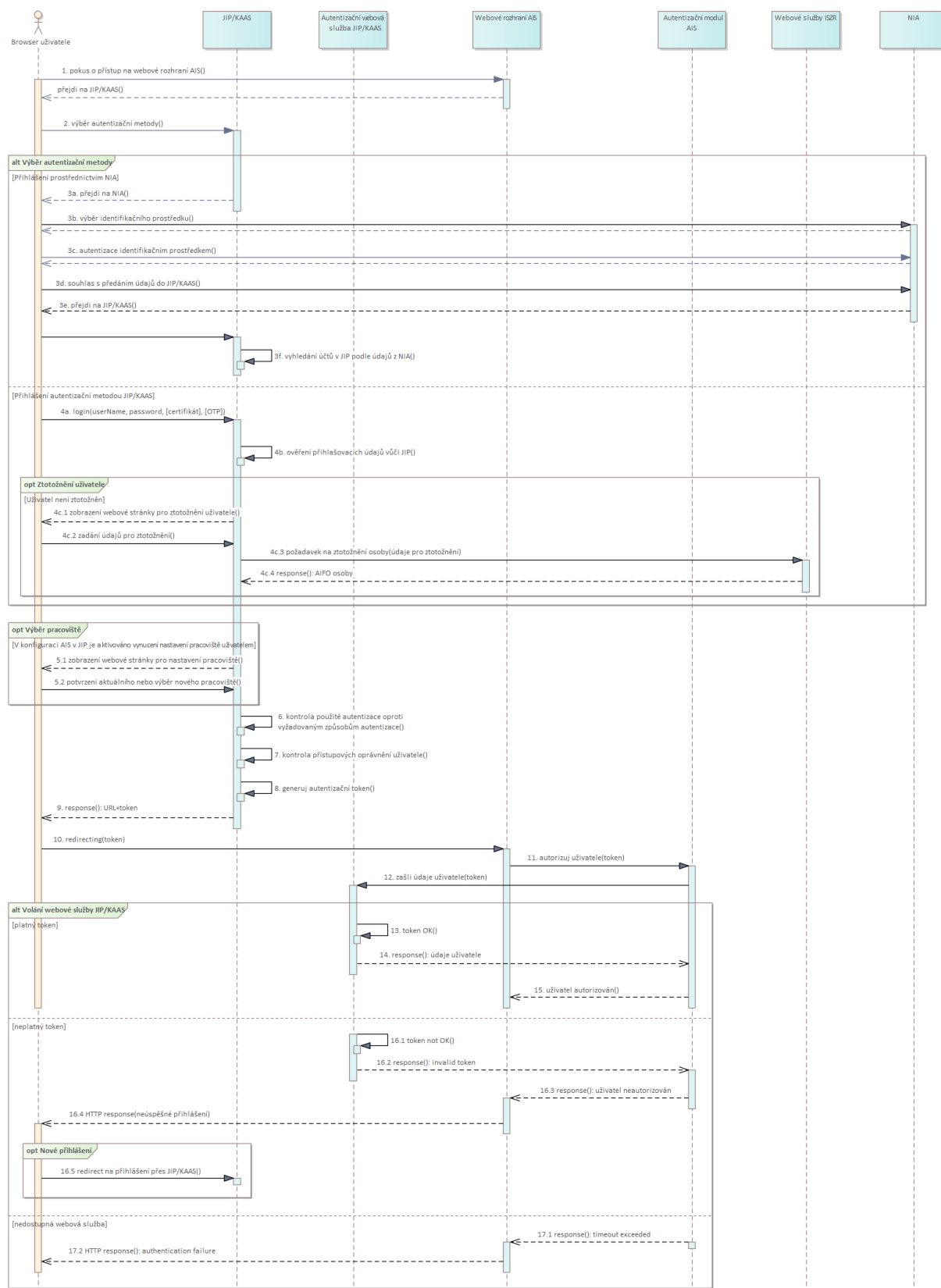
AIS se musí vůči JIP/KAAS autentizovat za použití komerčního serverového certifikátu vydaného komerční certifikační autoritou provozovanou českým kvalifikovaným poskytovatelem služeb vytvářejících důvěru (I.CA, PostSignum, eIdentity nebo Národní certifikační autorita).

K samotné autentizaci uživatele do AIS dochází až po autentizaci a autorizaci v JIP/KAAS, odkud je proveden redirect uživatele na URL AIS. V redirectu je obsažen jednorázový autentizační token s omezenou dobou platnosti, který vydal JIP/KAAS. Redirect je autonomní akce webového prohlížeče uživatele AIS.

Přenos identity je umožněn pouze jednosměrně – z JIP/KAAS do AIS.

3.4. Scénář komunikace a přenosu dat

Komunikace mezi uživatelem, AIS a JIP/KAAS je detailně popsána na následujícím obrázku. Popis jednotlivých kroků následuje níže.



Popis

1. Uživatel se pokusí přistoupit na webovou stránku AIS. Systém AIS zjistí, že session uživatele neobsahuje přihlašovací údaje, a přesměruje uživatele na JIP/KAAS.
2. Uživateli se zobrazí přihlašovací stránka JIP/KAAS. Uživatel vybere způsob přihlášení.
3. Pokud uživatel zvolil přihlášení prostřednictvím identity občana (NIA), jsou provedeny následující kroky:
 - a. Uživatel je přesměrován do NIA.
 - b. V NIA si vybere identifikační prostředek, kterým hodlá prokázat svoji identitu.
 - c. Pomocí tohoto prostředku se autentizuje.
 - d. Nakonec odsouhlasí předání svých osobních údajů do JIP/KAAS.
 - e. Uživatel je přesměrován spolu s jeho údaji zpět do JIP/KAAS.
 - f. JIP/KAAS vyhledá v JIP odpovídající uživatelské účty podle předaných údajů uživatele z NIA. Pokračuje se krokem 5.
4. Pokud uživatel zvolil přihlášení prostřednictvím některé autentizační metody JIP/KAAS, jsou provedeny následující kroky:
 - a. Uživatel zadá na přihlašovací stránce JIP/KAAS přihlašovací údaje.
 - b. JIP/KAAS zkontroluje správnost přihlašovacích údajů vůči JIP.
 - c. Pokud nebyl uživatel ztotožněn, JIP/KAAS zobrazí uživateli webovou stránku pro ztotožnění osoby a uživatel zadá požadované údaje. JIP/KAAS provede ztotožnění uživatele vůči ROB zavoláním webových služeb ISZR. Tímto JIP/KAAS získá AIFO a vybrané osobní údaje uživatele.
5. Pokud je v konfiguraci AIS v JIP aktivováno vynucování nastavení pracoviště, JIP/KAAS zobrazí uživateli webovou stránku pro výběr pracoviště. Uživatel potvrdí aktuálně přiřazené pracoviště, nebo ze seznamu vybere správné pracoviště.
6. JIP/KAAS dále zkontroluje uživatelem použitou autentizační metodu oproti požadavkům na způsob autentizace, které jsou nastaveny v konfiguraci AIS v JIP.
7. JIP/KAAS zkontroluje oprávnění uživatele přistoupit do AIS.
8. JIP/KAAS vygeneruje pro uživatele token.
9. JIP/KAAS posílá webovému prohlížeči uživatele v HTTP response informace pro přesměrování do AIS – URL a token.
10. Webový prohlížeč je s autentizačním tokenem přesměrován na URL AIS, definované v konfiguraci AIS uložené v JIP.
11. AIS se pokusí příchozího uživatele autorizovat následujícím způsobem...
12. Autentizační modul AIS provede synchronní volání autentizační WS JIP/KAAS pro získání informací o uživateli. Požadavek obsahuje autentizační token.
13. Požadavek je akceptován, pokud je token platný a validní.
14. Autentizační WS JIP/KAAS odešle v odpovědi údaje uživatele a zneplatní danou session uživatele.
15. Uživatel je autorizován a dále může pracovat s AIS.

Neúspěšné získání informací o uživateli z JIP/KAAS může být zapříčiněno z těchto důvodů:

- neplatnost nebo nevalidita tokenu

- nedostupnost autentizační WS JIP/KAAS
16. V případě neplatného tokenu vrací autentizační WS JIP/KAAS chybový stav a AIS zobrazí uživateli hlášku typu „neúspěšné přihlášení“.
17. V případě nedostupnosti autentizační WS JIP/KAAS zobrazí AIS uživateli hlášku typu „nedostupnost autentizační služby“.

4. Přímá autentizační webová služba

4.1. Stručný popis

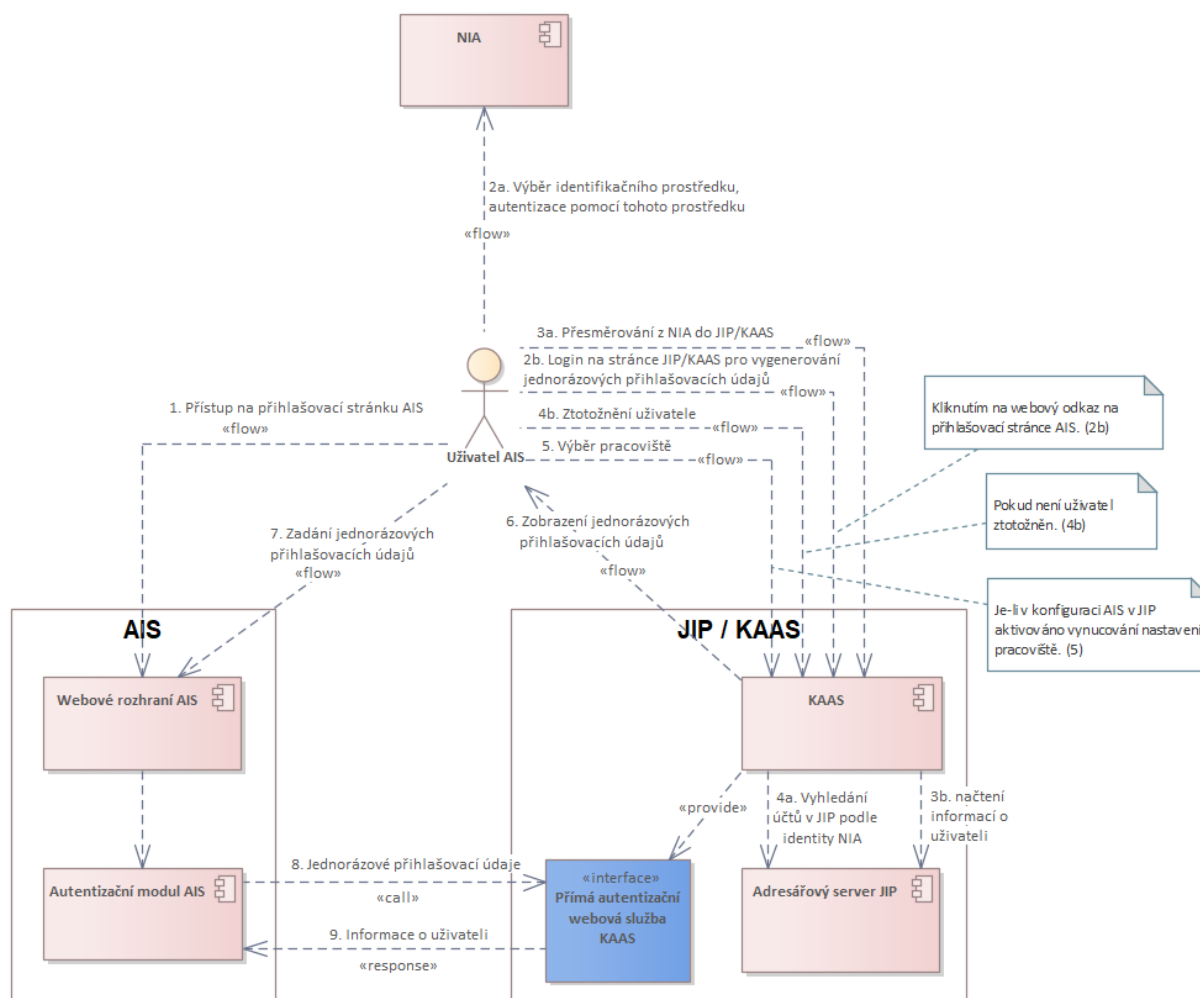
Následující informace platí jen pro přímou autentizační webovou službu ve verzi v3_3 nebo novější! Přímá autentizační webová služba ve verzi v1 v současnosti není využívána a v nejbližší době bude její poskytování ukončeno. Proto není v tomto dokumentu vůbec popisována.

Přímá autentizační služba JIP/KAAS funguje na následujícím principu.

Uživatel si zobrazí přihlašovací stránku AIS a klikne na odkaz, který otevře webovou stránku JIP/KAAS pro vygenerování jednorázového jména a hesla. Uživatel se na této stránce přihlásí pomocí přihlašovacích údajů do JIP, případně se přihlásí prostřednictvím NIA a získá jednorázové přihlašovací údaje. Uživatel zadá tyto jednorázové přihlašovací údaje na přihlašovací stránce AIS a AIS provede jejich ověření odesláním požadavku na přímou autentizační webovou službu JIP/KAAS, která v odpovědi vrátí údaje o autentizovaném uživateli.

AIS musí svým uživatelům poskytovat odkaz na webovou stránku JIP/KAAS pro vygenerování jednorázových přihlašovacích údajů.

4.2. Detailní popis procesu autentizace a autorizace



Uživatel přistoupí na webovou stránku AIS (1). Uživatel klikne na webový odkaz pro zobrazení webové stránky JIP/KAAS pro vygenerování jednorázových přihlašovacích údajů.

Zde si uživatel vybere, jakým způsobem se přihlásí.

Pokud si uživatel zvolil přihlášení prostřednictvím identity občana (NIA), jsou provedeny tyto kroky:

- Uživatel je přesměrován do NIA (2a). V NIA si uživatel vybere identifikační prostředek, jehož prostřednictvím prokáže svoji identitu a vybere údaje, které chce poskytnout do JIP/KAAS.
- Následně je uživatel přesměrován zpět z NIA do JIP/KAAS včetně jeho osobních údajů (3a).
- Na základě předaných údajů z NIA získá JIP/KAAS identifikátor AIFO, pomocí kterého se pokusí vyhledat odpovídající uživatelský účet v JIP (4a).
- Pokud je nalezeno více odpovídajících účtů, uživatel si vybere, pod kterým účtem se chce přihlásit.

Pokud si uživatel zvolil přihlášení pomocí některé z autentizačních metod v JIP/KAAS, jsou provedeny tyto kroky:

- Uživatel zadá příslušné přihlašovací údaje a JIP/KAAS ověří jejich správnost (2b).
- Po úspěšné autentizaci načte JIP/KAAS z JIP informace o uživateli, jeho domovském subjektu OVM/SPUÚ a přidělených rolích (3b).
- V případě úspěšného přihlášení se dále zkontroluje, jestli je uživatel ztotožněn. Pokud ne, JIP/KAAS zobrazí webovou stránku pro ztotožnění osoby a uživatel musí zadat údaje pro provedení ztotožnění. JIP/KAAS, jakožto autentizační informační systém, získá z registru obyvatel AIFO a osobní údaje uživatele podle § 56a zákona č. 101/2009 Sb., o základních registrech (4b).

Další kroky jsou společné pro uživatele autentizovaného prostřednictvím NIA i autentizovaného prostřednictvím přihlašovacích údajů do JIP.

Pokud je v konfiguraci AIS v JIP aktivováno vynucování nastavení pracoviště, JIP/KAAS dále zobrazí uživateli webovou stránku pro nastavení pracoviště a uživatel musí buď potvrdit jemu aktuálně přiřazené pracoviště, nebo ze seznamu vybrat správné pracoviště, v němž vykonává činnost (5).

JIP/KAAS ověří, že autentizační metoda, kterou uživatel použil, splňuje požadavky na způsob autentizace, nastavené v konfiguraci AIS v JIP.

JIP/KAAS dále provede kontrolu rolí přidělených uživateli, zda je uživatel oprávněn přistoupit do AIS. Je-li kontrola úspěšná, pokračuje se dalším krokem, jinak je uživateli zobrazeno hlášení o zamítnutí přístupu.

JIP/KAAS vygeneruje jednorázové uživatelské jméno a heslo a zobrazí je uživateli na webové stránce (6).

Uživatel opíše nebo zkopíruje jednorázové přihlašovací údaje do přihlašovací stránky AIS a stiskne tlačítko pro přihlášení (7).

Autentizační modul AIS zavolá přímou autentizační webovou službu JIP/KAAS za účelem získání informací o uživateli. Webové službě předá jednorázové přihlašovací údaje (8). Pokud jsou jednorázové přihlašovací údaje platné, AIS v odpovědi obdrží informace o uživateli (9). Pokud AIS zavolá správnou verzi přímé autentizační webové služby JIP/KAAS, obdrží v odpovědi osobní údaje uživatele podle § 56a odst. 3 zákona č. 101/2009 Sb., o základních registrech.

AIS posoudí na základě předaných informací o uživateli, zda umožní uživateli přístup do AIS.

4.3. Technické informace

Pro komunikaci mezi JIP/KAAS a AIS se používá přímá autentizační webová služba:

- WS na straně JIP/KAAS přijímá od AIS jednorázové uživatelské jméno a heslo. V odpovědi vrací informace o uživateli, pro nějž byly jednorázové přihlašovací údaje vystaveny (v případě platných jednorázových přihlašovacích údajů) nebo chybový kód (v případě neplatných jednorázových přihlašovacích údajů).

Komunikace je zabezpečena pomocí protokolu TLS a autentizace certifikátem.

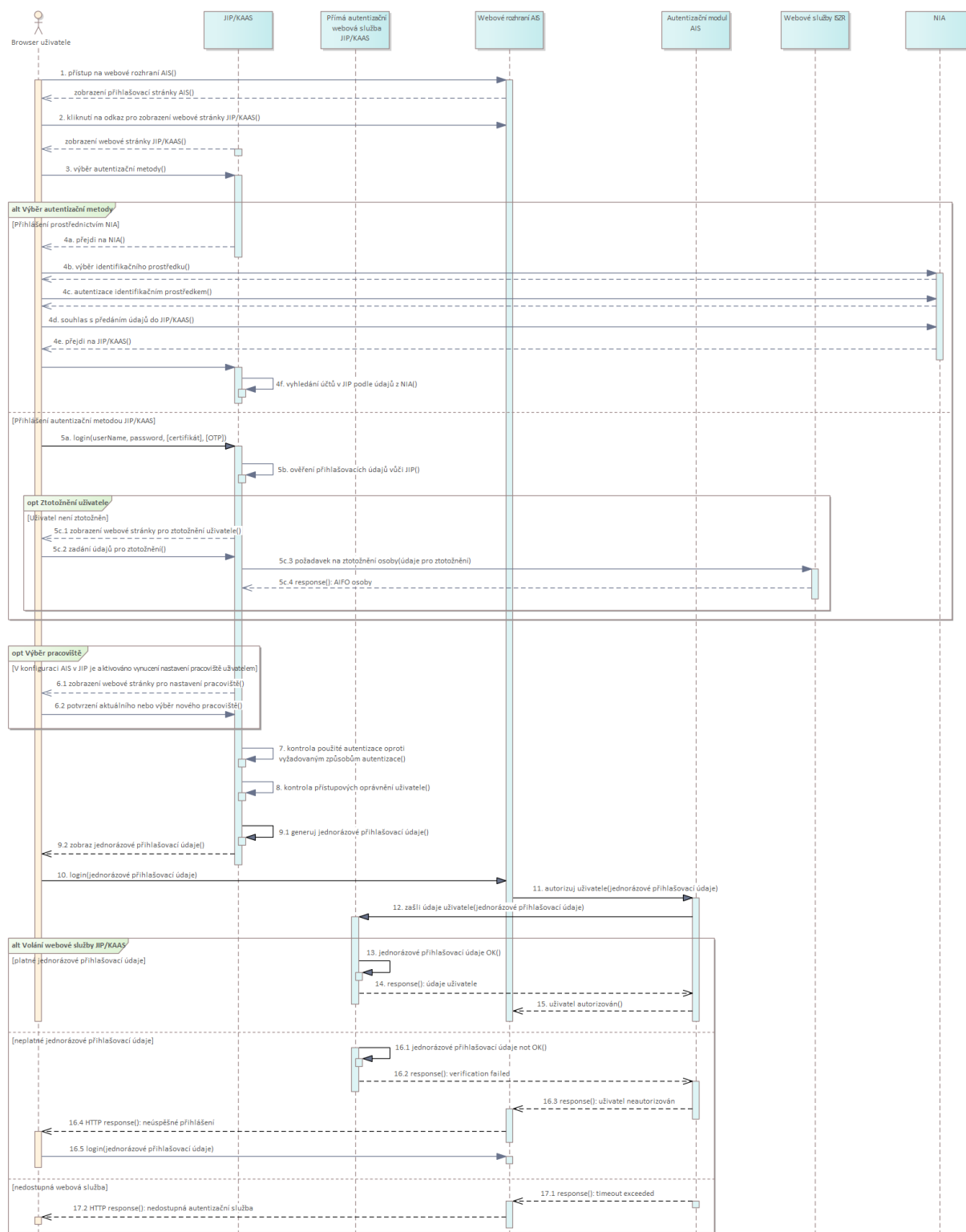
AIS se musí vůči JIP/KAAS autentizovat za použití komerčního serverového certifikátu vydaného komerční certifikační autoritou provozovanou českým kvalifikovaným poskytovatelem služeb vytvářejících důvěru (I.CA, PostSignum, eIdentity nebo Národní certifikační autorita).

K samotné autentizaci uživatele do AIS dochází až po autentizaci a autorizaci v JIP/KAAS, kde uživatel obdrží vygenerované jednorázové přihlašovací údaje a zadá je na přihlašovací stránce AIS. Jednorázové přihlašovací údaje mají omezenou dobu platnosti 30 minut od okamžiku jejich vygenerování a jsou automaticky zneplatněny po jejich úspěšném ověření přímou autentizační webovou službou.

Přenos identity je umožněn pouze jednosměrně – z JIP/KAAS do AIS.

4.4. Scénář komunikace a přenosu dat

Komunikace mezi uživatelem, AIS a JIP/KAAS je detailně popsána na následujícím obrázku. Popis jednotlivých kroků následuje níže.



Popis

1. Uživatel přistoupí na webovou stránku AIS. Systém AIS zobrazí uživateli přihlašovací stránku.
 2. Uživatel klikne na odkaz pro zobrazení webové stránky JIP/KAAS, která slouží k vygenerování jednorázových přihlašovacích údajů.
 3. Uživateli se zobrazí přihlašovací stránka JIP/KAAS. Uživatel vybere způsob přihlášení.
 4. Pokud uživatel zvolil přihlášení prostřednictvím identity občana (NIA), jsou provedeny následující kroky:
 - a. Uživatel je přesměrován do NIA.
 - b. V NIA si vybere identifikační prostředek, kterým hodlá prokázat svoji identitu.
 - c. Pomocí tohoto prostředku se autentizuje.
 - d. Nakonec odsouhlasí předání svých osobních údajů do JIP/KAAS.
 - e. Uživatel je přesměrován spolu s jeho údaji zpět do JIP/KAAS.
 - f. JIP/KAAS vyhledá v JIP odpovídající uživatelské účty podle předaných údajů uživatele z NIA. Pokračuje se krokem 6.
 5. Pokud uživatel zvolil přihlášení prostřednictvím některé autentizační metody JIP/KAAS, jsou provedeny následující kroky:
 - a. Uživatel zadá na přihlašovací stránce JIP/KAAS přihlašovací údaje.
 - b. JIP/KAAS zkontroluje správnost přihlašovacích údajů vůči JIP.
 - c. Pokud nebyl uživatel ztotožněn, JIP/KAAS zobrazí uživateli webovou stránku pro ztotožnění osoby a uživatel zadá požadované údaje. JIP/KAAS provede ztotožnění uživatele vůči ROB zavoláním webových služeb ISZR. Tímto JIP/KAAS získá AIFO a vybrané osobní údaje uživatele.
 6. Pokud je v konfiguraci AIS v JIP aktivováno vynucování nastavení pracoviště, JIP/KAAS zobrazí uživateli webovou stránku pro výběr pracoviště. Uživatel potvrdí aktuálně přiřazené pracoviště, nebo ze seznamu vybere správné pracoviště.
 7. JIP/KAAS dále zkontroluje uživatelem použitou autentizační metodu oproti požadavkům na způsob autentizace, které jsou nastaveny v konfiguraci AIS v JIP.
 8. JIP/KAAS zkontroluje oprávnění uživatele přistoupit do AIS.
 9. JIP/KAAS vygeneruje pro uživatele jednorázové přihlašovací údaje a zobrazí je uživateli na webové stránce.
 10. Uživatel zadá jednorázové přihlašovací údaje na přihlašovací stránce AIS.
 11. AIS se pokusí příchozího uživatele autorizovat následujícím způsobem...
 12. Autentizační modul AIS provede synchronní volání přímé autentizační WS JIP/KAAS pro získání informací o uživateli. Požadavek obsahuje jednorázové přihlašovací údaje zadané uživatelem.
 13. Požadavek je akceptován, pokud jsou jednorázové přihlašovací údaje platné a validní.
 14. Přímá autentizační WS JIP/KAAS odešle v odpovědi údaje uživatele a zneplatní dané jednorázové přihlašovací údaje.
 15. Uživatel je autorizován a dále může pracovat s AIS.
- Neúspěšné získání informací o uživateli z JIP/KAAS může být zapříčiněno z těchto důvodů:
- neplatnost nebo nevalidita jednorázových přihlašovacích údajů
 - nedostupnost přímé autentizační WS JIP/KAAS

16. V případě neplatných jednorázových přihlašovacích údajů vrátí přímá autentizační WS JIP/KAAS chybový stav a AIS zobrazí uživateli hlášku typu „neúspěšné přihlášení“.
17. V případě nedostupnosti přímé autentizační WS JIP/KAAS zobrazí AIS uživateli hlášku typu „nedostupnost autentizační služby“.

5. Odhlášení uživatele z JIP/KAAS a případně z NIA

5.1. Stručný popis

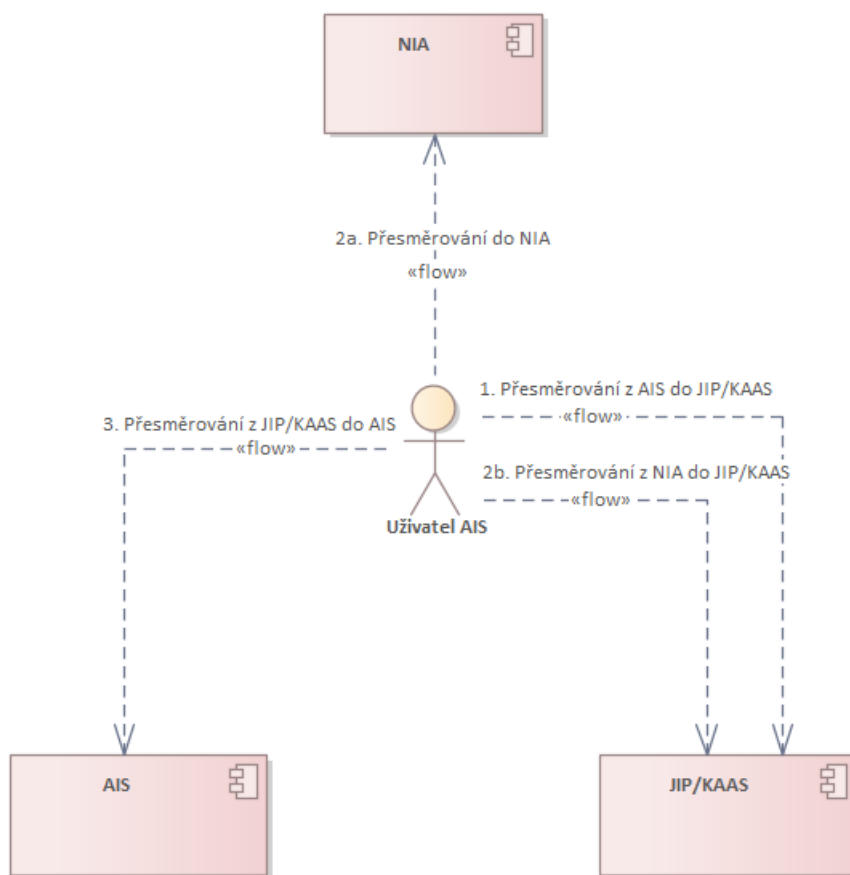
JIP/KAAS nabízí rozhraní, pomocí kterého mohou AISy provést odhlášení uživatele z JIP/KAAS a případně z NIA, pokud se uživatel přihlásil do JIP/KAAS prostřednictvím NIA.

AISy by měly toto rozhraní z bezpečnostních důvodů volat v okamžiku, kdy se uživatel odhlašuje z AIS kliknutím na příslušné tlačítko nebo odkaz pro odhlášení.

Odhlášení uživatele probíhá tak, že je uživatel přesměrován z AIS na definovanou adresu JIP/KAAS, zde dojde k odhlášení uživatele z JIP/KAAS a případně také z NIA a nakonec je uživatel přesměrován zpět do AIS, kde může být dokončeno jeho odhlášení např. zobrazením zprávy o úspěšném odhlášení uživatele.

Všechny potřebné adresy, na které je uživatel přesměrováván, jsou uvedeny v technickém popisu k webovým službám JIP/KAAS. Adresa AIS, kam je uživatel přesměrován na konci procesu odhlášení je definována v konfiguraci AIS.

5.2. Detailní popis procesu



Uživatel klikne v AIS na tlačítko/odkaz pro odhlášení. Je přesměrován na definovanou adresu JIP/KAAS (1).

JIP/KAAS ověří, zda se uživatel přihlásil prostřednictvím NIA:

- Pokud ano, je uživatel přesměrován do NIA, kde se provede odhlášení uživatele z NIA (2a). Uživatel je poté přesměrován z NIA zpět do JIP/KAAS (2b).

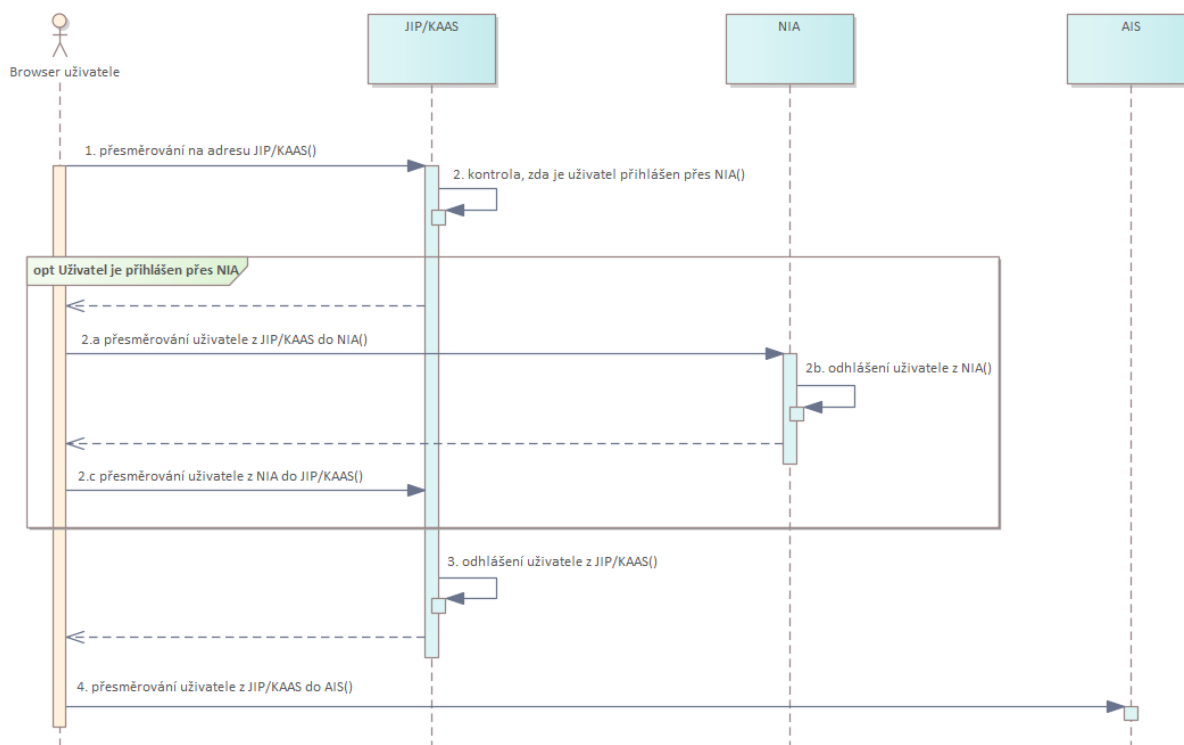
- Pokud se uživatel nepřihlásil přes NIA, pokračuje se ihned dalším krokem. Uživatel je odhlášen z JIP/KAAS a přesměrován zpět na definovanou adresu AIS (3).

5.3. Technické informace

Odhlášení uživatele z JIP/KAAS (a případně z NIA) je založeno na přesměrování uživatelské session do příslušného systému, kde dojde k odhlášení uživatele.

5.4. Scénář komunikace a přenosu dat

Komunikace mezi uživatelem, AIS a JIP/KAAS je detailně popsána na následujícím obrázku. Popis jednotlivých kroků následuje níže.



Popis

1. Uživatel klikne v prostředí AIS na tlačítko či odkaz pro odhlášení. AIS přesměruje uživatele na definovanou adresu JIP/KAAS.
2. JIP/KAAS zkontroluje, zda se uživatel přihlásil prostřednictvím NIA. Pokud ano, provedou se tyto kroky:
 - a. Uživatel je přesměrován na definovanou adresu NIA.
 - b. Je provedeno odhlášení uživatele z NIA.
 - c. Uživatel je přesměrován zpět do JIP/KAAS
3. JIP/KAAS provede odhlášení daného uživatele.
4. Uživatel je přesměrován zpět na definovanou adresu AIS.

6. Seznam změn

Níže je uveden seznam změn v jednotlivých verzích dokumentu. Uvedeny jsou jen veřejně publikované verze. Seznam uváděných změn obsahuje vždy změny vůči poslední veřejně publikované verzi dokumentu.

Verze 3.2

- celý dokument – opraveno označení KAAS na používanější JIP/KAAS, drobné opravy v textu

Verze 3.1

- kap. 3.3, 4.3 – na seznam podporovaných certifikačních autorit byla přidána Národní certifikační autorita

Verze 3.0

- kap. 5 – přidán popis procesu odhlášení uživatele z AIS, JIP/KAAS a NIA

Verze 2.9

- celý dokument – doplněna komunikace JIP/KAAS s NIA, uživatelé mohou pocházet i ze subjektů SPUÚ

Verze 2.8

- titulní strana – odstraněno neaktuální červené upozornění o plánovaném ukončení přímé autentizační webové služby v1
- kap. 4.1 – upraven text o přímé autentizační webové službě v1

Verze 2.7

- označení „KAAS/JIP“ v dokumentu změněno za užívanější „JIP/KAAS“

Verze 2.6

- kap. 2.6 – oprava nesprávného webového odkazu
- kap. 4.2 – drobná oprava textu, smazání nadbytečného slova

Verze 2.5

- kap. 3.2, 3.4, 4.2, 4.4 – přidán odstavec/odrážka s poznámkou o ověřování přístupových oprávnění uživatele
- oprava několika chyb a špatně používaných termínů v dokumentu

Verze 2.4

- kap. 1.2 – JIP/KAAS je autentizační informační systém podle zákona č. 111/2009 Sb.

- kap. 2.5 – nová kapitola o nakládání s osobními údaji uživatelů
- kap. 3.2, 4.2 – přidány poznámky o získání osobních údajů uživatele z ROB a jejich předání do AIS
- kap. 3.3, 4.3 – akreditovaný poskytovatel certifikačních služeb změněn na kvalifikovaného poskytovatele služeb vytvářejících důvěru
- kap. 3.4, 4.4 – přidána poznámka o získání osobních údajů z ROB

Verze 2.3

- kap. 3.2, 3.4, 4.2, 4.4 – do popisu procesu autentizace a autorizace přidána informace o ztotožnění uživatele a nastavení pracoviště během přihlašování uživatele do KAAS

Verze 2.2

- rozšíření dokumentu o procesní popis přímé autentizační služby
- kap. 2 – nová kapitola s obecnými informacemi o autentizačních službách
- kap. 4 – nová kapitola s popisem přímé autentizační webové služby

Verze 2.1

- kap. 1.3 – přidána chybějící zkratka KAAS
- kap. 2.1 – korigován popis procesu; KAAS nekomunikuje s ISZR během autentizace uživatele
- kap. 2.2 – zřízení Garanta AIS není povinné, nakonfigurování AIS ve Správě dat může udělat také samotný lokální administrátor
- kap. 2.3 – zřízení Garanta AIS není povinné, uváděné činnosti může provést také samotný lokální administrátor
- kap. 2.5 – nová kapitola
- kap. 3.1 – pro komunikaci s KAAS lze použít pouze komerční serverový certifikát od I.CA/PostSignum/eIdentity, KAAS vrací do AIS agendové činnostní role přidělené uživateli v případě, že daný AIS je zaregistrován do ISZR
- kap. 3.2 – korigován popis procesu; KAAS nekomunikuje s ISZR během autentizace uživatele

Verze 2.0

- kap. 2.3 – v nastavení AIS lze zřídit více přístupových rolí, pro OVM a uživatele lze nastavit více přístupových rolí
- kap. 3.1 – upřesněny požadavky na certifikát, který používá AIS pro komunikaci s KAAS
- kap. 4 – nová kapitola

Verze 1.9

- kap. 1.3 – přidána zkratka ISZR
- kap. 2.1 – do obrázku přidána vazba na základní registry, do textu přidány informace o agendových činnostních rolích a komunikaci s ISZR

- kap. 2.4 – nová kapitola
- kap. 3.1 – doplněno, že certifikát AIS musí vydat certifikační autorita základních registrů
- kap. 3.2 – do obrázku a textu přidána komunikace s ISZR pro získání aktuálního seznamu agendových činnostních rolí pro daný OVM

Verze 1.7

- kap. 3.1 – upřesněna autentizace AIS vůči KAAS (pouze certifikátem), specifikován seznam uznávaných certifikačních autorit

Verze 1.6

- první veřejně publikovaná verze dokumentu