Dokumentace

k projektu Czech POINT

JIP/KAAS: Autentizační webová služba

Technický popis

Vytvořeno dne: 27. 9. 2011

Aktualizováno: 11. 10. 2021

Verze: 4.8

Obsah

1. Úvod

1.1. Účel dokumentu

Tento dokument obsahuje technický popis autentizace uživatelů do agendových informačních systémů (AIS) za využití přihlašovacích údajů do Czech POINT nebo na základě ověření uživatele v národním bodu pro identifikaci a autentizaci (dále zkráceně NIA). AIS získává informace o uživateli a jeho subjektu prostřednictvím autentizačních webových 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.

Technický popis přihlašování do AIS detailně popisuje rozhraní autentizační a přímé autentizační webové služby KAAS, kterou lze využít k autentizaci a autorizaci uživatelů přihlašujících se do agendových informačních systémů (AIS).

Dokument popisuje komunikaci mezi KAAS a AIS.

Tento dokument je určen pro vývojáře AIS, kteří potřebují do svých systémů implementovat funkcionalitu zajišťující komunikaci s autentizační webovou službou KAAS.

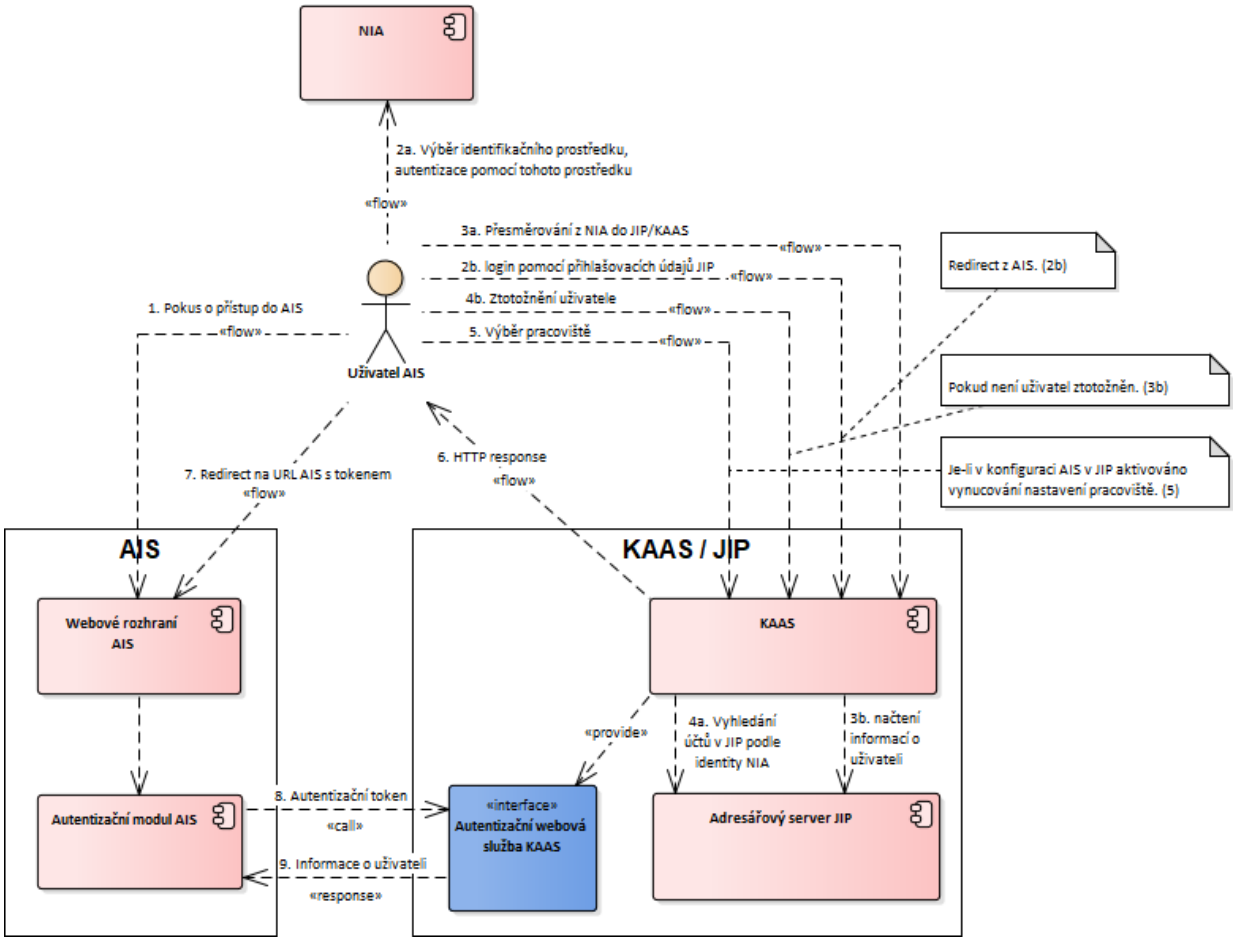
1.3. Definice pojmů

Zkratka nebo pojem	Vysvětlení
AIS	Agendový informační systém
Autentizace	Ověření identity uživatele
Autorizace	Přidělení přístupových práv uživateli po jeho úspěšné autentizaci
JIP	Jednotný identitní prostor, adresářová služba obsahující údaje pro autentizaci a autorizaci uživatelů.
KAAS	Katalog autentizačních a autorizačních služeb
KIVS	Komunikační infrastruktura veřejné správy
NIA	Národní bod pro identifikaci a autentizaci
OVM	Orgán veřejné moci
ROVM	Rejstřík OVM a SPUÚ
RPP	Registr práv a povinností
RUIAN	Registr územní identifikace, adres a nemovitostí
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!)
WS	Webová služba

2. Popis autentizace a autorizace

V následujících kapitolách je popsán postup, jak AIS provádí autentizaci a autorizaci přistupujícího uživatele za použití autentizační webové služby KAAS, nebo přímé autentizační webové služby KAAS.

2.1. Autentizační webová služba KAAS



Uživatel přistoupí na webovou stránku AIS (1).

Systém rozpozná, že uživatel není autentizován, a přesměruje jej na webovou stránku KAAS (viz specifikace v kapitolách „Rozhraní přihlašovací stránky“). Zde si uživatel vybere, jakým způsobem se přihlásí.

Pokud si uživatel zvolil přihlášení prostřednictvím 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 KAAS včetně jeho osobních údajů (3a).
- Na základě předaných údajů z NIA získá 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 KAAS ověří jejich správnost (2b).
- Po úspěšné autentizaci načte KAAS z JIP informace o uživateli, jeho domovském subjektu OVM/SPUÚ a přidělených rolích (3b).
- V případě jejich správnosti se zkontroluje, jestli je uživatel ztotožněn. Pokud ne, KAAS zobrazí webovou stránku pro ztotožnění osoby a uživatel musí zadat údaje pro provedení ztotožnění. 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, 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).

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

KAAS vygeneruje autentizační token pro uživatele a přesměruje uživatele s tokenem na definovanou adresu AIS – viz kapitoly „Rozhraní pro příjem autentizačního tokenu" (6+7).

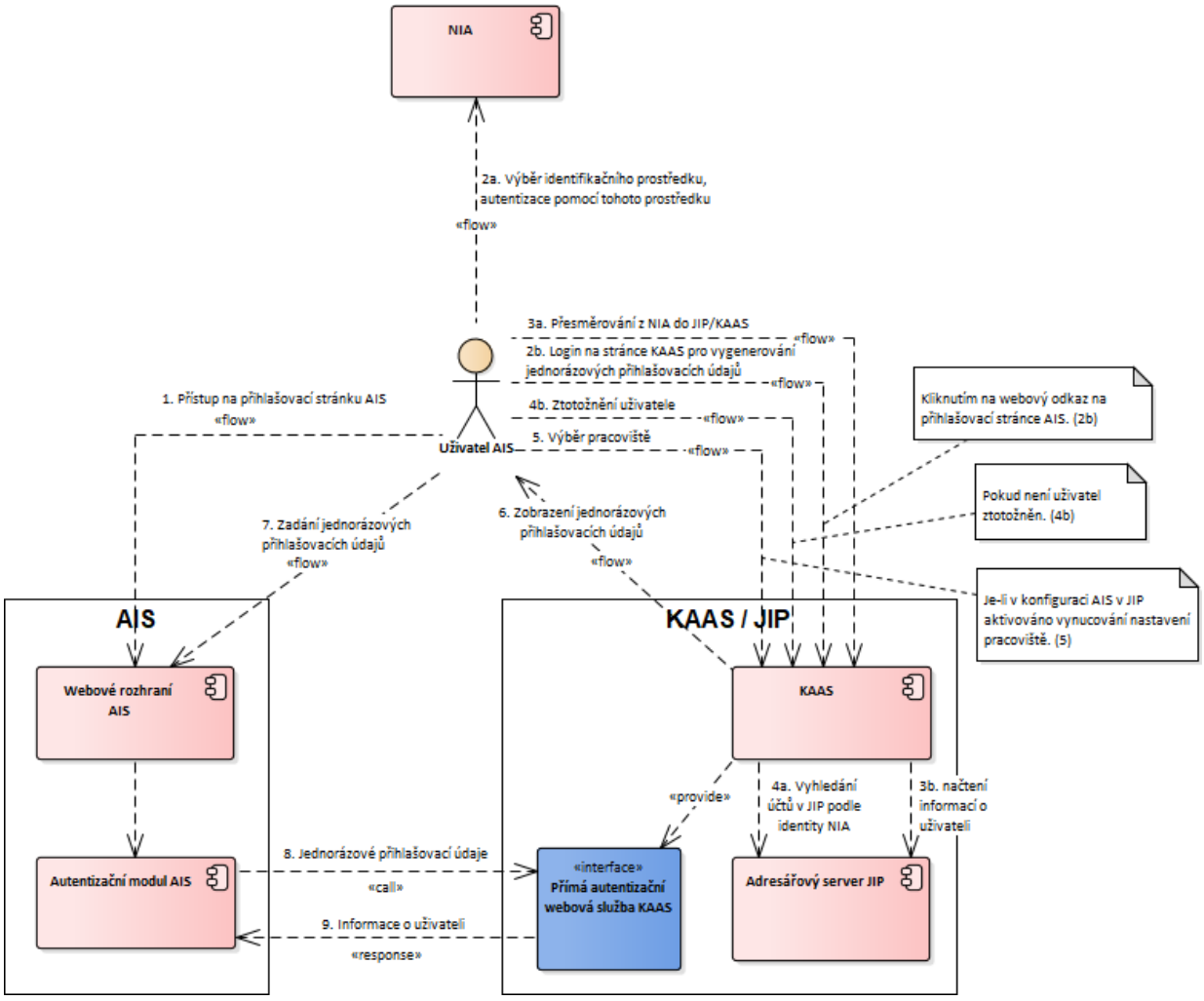
Autentizační modul AIS zavolá autentizační webovou službu KAAS za účelem získání informací o uživateli (viz specifikace v kapitolách „Způsob komunikace s webovou službou"). Webové službě předá autentizační token (8). Pokud je token platný, AIS v odpovědi obdrží informace o uživateli (9). Pokud AIS zavolá správnou verzi autentizační webové služby 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.

Poznámka: Další informace a diagram komunikace a přenosu dat jsou uvedeny v dokumentu „JIP/KAAS: Autentizační webová služba, Procesní popis".

2.2. Přímá autentizační webová služba KAAS

Poznámka: Následující způsob autentizace uživatele **neplatí** pro přímou autentizační webovou službu ve verzi **v1** popsanou v kapitole 8. Přímá autentizační webová služba v1 bude v dohledné době zrušena.



Uživatel přistoupí na webovou stránku AIS (1). Uživatel klikne na webový odkaz pro zobrazení webové stránky KAAS pro vygenerování jednorázových přihlašovacích údajů. Specifikace adresy webové stránky KAAS se nachází v kapitolách „Rozhraní pro vygenerování jednorázových přihlašovacích údajů".

Zde si uživatel vybere, jakým způsobem se přihlásí.

Pokud si uživatel zvolil přihlášení prostřednictvím 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 KAAS včetně jeho osobních údajů (3a).
- Na základě předaných údajů z NIA získá 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 KAAS ověří jejich správnost (2b).
- Po úspěšné autentizaci načte KAAS z JIP informace o uživateli, jeho domovském subjektu OVM/SPUÚ a přidělených rolích (3b).
- V případě jejich správnosti se zkontroluje, jestli je uživatel ztotožněn. Pokud ne, KAAS zobrazí webovou stránku pro ztotožnění osoby a uživatel musí zadat údaje pro provedení ztotožnění. 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, 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).

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

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 KAAS podle specifikace v kapitole 9.2 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 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.

Poznámka: Další informace a diagram komunikace a přenosu dat jsou uvedeny v dokumentu „JIP/KAAS: Autentizační webová služba, Procesní popis".

2.3. 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.

3. Popis rozhraní KAAS

3.1. Seznam autentizačních webových služeb

Autentizační webová služba je publikována v těchto verzích:

- **v2_1** – přidána metoda pro ověřování dostupnosti webové služby, maximální délka „Username" zvýšena na 50 znaků; viz kapitola 4
- **v3_4** – tato verze webové služby vrací více údajů o uživateli i subjektu (např. způsob přihlášení uživatele, název subjektu, e-mail uživatele i subjektu, příznak, zda je uživatel v JIP ztotožněn, pracoviště, v němž uživatel vykonává činnost, atd.); viz kapitola 5
- **v4_1** – tato verze webové služby vrací osobní údaje uživatelů podle § 56a odst. 5 zákona č. 111/2009 Sb., o základních registrech; viz kapitola 6
- **v4_2** – tato verze webové služby vrací v odpovědi identifikátor SPUÚ z ROVM, pokud autentizovaný uživatel pochází ze SPUÚ; dále pokud se uživatel autentizoval prostřednictvím NIA, v odpovědi se vrací úroveň záruk použitého identifikačního prostředku

Přímá autentizační webová služba je publikována v těchto verzích:

- **v1** – viz kapitola 8
- **v3_4** – tato verze přímé autentizační služby funguje na principu jednorázových přihlašovacích údajů; viz kapitola 9
- **v4_1** – tato verze přímé autentizační služby vrací osobní údaje uživatelů podle § 56a odst. 5 zákona č. 111/2009 Sb., o základních registrech; viz kapitola 10
- **v4_2** – tato verze webové služby vrací v odpovědi identifikátor SPUÚ z ROVM, pokud autentizovaný uživatel pochází ze SPUÚ; dále pokud se uživatel autentizoval prostřednictvím NIA, v odpovědi se vrací úroveň záruk použitého identifikačního prostředku

4. Webová služba verze v2_1

Tato webová služba poskytuje externímu systému (AIS) informace o uživateli, který se autentizoval za účelem získání přístupu do daného externího systému (AIS).

4.1. Rozhraní přihlašovací stránky

Po detekci nepřihlášeného uživatele provádí AIS přesměrování na přihlašovací stránku KAAS a předává identifikátor AIS, který je předáván v parametru „atsId".

Adresy přihlašovací stránky KAAS:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/login?atsId=exampleId
provozní	https://kaas.czechpoint.cz/as/login?atsId=exampleId

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

4.2. Rozhraní pro příjem autentizačního tokenu

KAAS přesměruje uživatele na URL adresu, která je definována v konfiguraci AIS v JIP. Toto URL, které je v plné režii AIS, musí přijímat parametr „sessionId", ve kterém je do AIS předáván vygenerovaný autentizační token. Tento token AIS použije pro volání autentizační webové služby, popsané v následující kapitole.

Příklad URL: https://[url-adresa-ais]?sessionId=01-8c57c8b70acb41598456914f17ae933b

4.3. Rozhraní pro odhlášení uživatele

V okamžiku, kdy se uživatel odhlašuje z AIS, by jej AIS měl z bezpečnostních důvodů přesměrovat do JIP/KAAS, kde rovněž dojde k odhlášení uživatele. Pokud se uživatel přihlásil do KAAS/JIP prostřednictvím NIA, JIP/KAAS provede rovněž přesěrování uživatele do NIA, kde dojde k odhlášení uživatele z NIA.

V okamžiku, kdy uživatel klikne na stránkách AIS na odkaz/tlačítko pro odhlášení, by AIS měl uživatele přesměrovat na následující adresu JIP/KAAS:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*
provozní	https://www.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

V parametru „atsId" se předává identifikátor AIS podobně jako v rozhraní přihlašovací stránky (viz výše).

V parametru „uri" se předává návratová adresa AIS, na kterou má JIP/KAAS uživatele přesměrovat po dokončení jeho odhlášení v JIP/KAAS a případně také v NIA. Předaná návratová adresa se ověřuje vůči „URL pro odhlášení", které je uloženo v konfiguraci AIS. „URL pro odhlášení" v konfiguraci se musí shodovat s počátkem návratové adresy v parametru „uri". Např. je-li v konfiguraci AIS uloženo „https://www.domena.cz/logout/", pak v parametru „uri" mohou být do JIP/KAAS předány návratové adresy „https://www.domena.cz/logout/?origin=jipkaas" nebo „https://www.domena.cz/logout/user/jnovak/" apod.

4.4. Způsob komunikace s webovou službou

Mezi autentizační webovou službou KAAS a AIS probíhá komunikace typu „request-response". Komunikace probíhá pomocí protokolu HTTPS, pro přenos zpráv se používá formát SOAP 1.1. Při volání webové služby je zapotřebí správně definovat a vyplňovat atribut „soapAction" v souladu s přiloženým odpovídajícím WSDL souborem.

Komunikace je zabezpečena pomocí šifrování. Používá se protokol TLS 1.2. Starší verze protokolu (SSL, TLS 1.0, TLS 1.1) jsou zakázány.

Ověření AIS je zajištěno pomocí autentizace certifikátem. AIS se musí vůči 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). Zejména v případě I.CA musí vydaný certifikát obsahovat v rozšíření certifikátu „extendedKeyUsage" atribut „Client Authentication" (id-kp-clientAuth, OID 1.3.6.1.5.5.7.3.2). Tento autentizační certifikát musí být zaregistrován v nastavení AIS, což se provede pomocí administrační aplikace Správa dat (https://www.czechpoint.cz/spravadat/).

Komunikaci iniciuje AIS, který zasílá na WS KAAS „request". WS KAAS poté vrací „response". AIS zasílá „request" na endpoint:

Prostředí KAAS	Adresa
testovací	https://cert.test.czechpoint.cz/asws/atsEndpoint
provozní	https://kaas-crt.czechpoint.cz/asws/atsEndpoint

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

4.5. Metoda heartBeat – ověření dostupnosti webové služby

4.5.1. Příklad komunikace WS

Request	<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <soapenv:Body> <m:heartBeatRequest xmlns:m="http://agw-as.cz/ats-ws/atsSzr/v2_1"> </m:heartBeatRequest> </soapenv:Body> </soapenv:Envelope>
Response	<?xml version="1.0" encoding="UTF-8"?> <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Header/> <soapenv:Body> <v2_1:heartBeatResponse xmlns:v2_1="http://agw-as.cz/ats-ws/atsSzr/v2_1"> <v2_1:status>OK</v2_1:status> </v2_1:heartBeatResponse> </soapenv:Body> </soapenv:Envelope>

4.5.2. Vysvětlivky

Hodnota	Význam
status	Strukturovaná informace o výsledku zpracování žádosti.
code	Kód s číslem chyby v případě nedostupnosti autentizační WS.
message	Textová informace o příčině nedostupnosti autentizační WS.

4.5.3. Popis stavů výsledku zpracování

Ve zprávách typu „response" se v elementu „status" vrací informace o výsledku zpracování žádosti, která může nabývat těchto hodnot:

Hodnota	Význam
OK	Požadavek byl zpracován korektně.
ERROR	Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.

4.6. Metoda authConfirmation – autentizace uživatelů

4.6.1. Příklad komunikace WS

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <soapenv:Body>
    <m:authConfirmationRequest xmlns:m="http://agw-as.cz/ats-ws/atsSzr/v2_1">
      <m:sessionId>00-c679c0687f2d43ebbcd766876f90da66</m:sessionId>
    </m:authConfirmationRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Response

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body>
    <v2_1:authConfirmationResponse xmlns:v2_1="http://agw-as.cz/ats-
ws/atsSzr/v2_1">
      <v2_1:status>OK</v2_1:status>
      <v2_1:userRequestIp>192.168.0.1</v2_1:userRequestIp>
      <v2_1:attributes>
        <v2_1:Username>jnovak</v2_1:Username>
        <v2_1:UzivatelId>E5TVdDM2zEXfkxOU1XQzNg==</v2_1:UzivatelId>
        <v2_1:ZkratkaSubjektu>JstrbLhota</v2_1:ZkratkaSubjektu>
        <v2_1:IcSubjektu>00235415</v2_1:IcSubjektu>
        <v2_1:Jmeno>Jan</v2_1:Jmeno>
        <v2_1:Prijmeni>Novák</v2_1:Prijmeni>
        <v2_1:TitulPred>Ing.</v2_1:TitulPred>
        <v2_1:TitulZa>CSc</v2_1:TitulZa>
        <v2_1:PristupoveRole>
          <v2_1:role>Administrator</v2_1:role>
        </v2_1:PristupoveRole>
        <v2_1:CinnostniRole>
          <v2_1:Agenda>
            <v2_1:KodAgendy>A100</v2_1:KodAgendy>
            <v2_1:KodCinnostniRole>ACR01</v2_1:KodCinnostniRole>
          </v2_1:Agenda>
          <v2_1:Agenda>
            <v2_1:KodAgendy>A101</v2_1:KodAgendy>
            <v2_1:KodCinnostniRole>ACR02</v2_1:KodCinnostniRole>
          </v2_1:Agenda>
        </v2_1:CinnostniRole>
      </v2_1:attributes>
    </v2_1:authConfirmationResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

4.6.2. Vysvětlivky

Hodnota	Význam
sessionId	Identifikace session uživatele. Token, získaný od KAAS po přesměrování uživatele do AIS (viz kapitola 2.1, bod 7).
status	Strukturovaná informace o výsledku zpracování žádosti.
userRequestIp	IP uživatele při přihlášení. Může být IPv6/IPv4. Pokud uživatel přistupuje přes proxy, bere se IP proxy, která je nejdále od uživatele.
attributes	Informace o autentizovaném uživateli. Viz kapitola 4.6.4.

4.6.3. Popis stavů výsledku zpracování

Ve zprávách typu „response" se v elementu „status" vrací informace o výsledku zpracování žádosti, která může nabývat těchto hodnot:

Hodnota	Význam
OK	Požadavek byl zpracován korektně.
SYSTEM_ERROR	Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.
SESSION_NOT_FOUND	Vrací v případě, že byl v požadavku zaslán neexistující token.

4.6.4. Seznam atributů předávaných do AIS

Atribut	Popis
ZkratkaSubjektu	Zkratka subjektu dotazujícího se nebo žádajícího uživatele. Jedinečný identifikátor subjektu v rámci JIP.
IcSubjektu	IČ subjektu dotazujícího se nebo žádajícího uživatele.
UzivatelId	Jedinečný identifikátor uživatele v rámci JIP.
Username	Uživatelské jméno uživatele v JIP.
Jmeno	Jméno uživatele
Prijmení	Příjmení uživatele
TitulPred	Titul před jménem
TitulZa	Titul za jménem
PristupoveRole	Seznam přístupových (aplikačních) rolí do AIS, které jsou přiřazeny uživateli.
role	Označení konkrétní přístupové (aplikační) role, přiřazené uživateli.
CinnostniRole	Seznam činnostních rolí, které jsou přiřazeny uživateli.
KodAgendy	Kód agendy, k níž je daná činnostní role přiřazena.
KodCinnostniRole	Kód činnostní role, přiřazené uživateli.

Poznámka: Typy atributů a definovaná omezení hodnot atributů jsou uvedena ve WSDL souboru – viz kapitola 4.7.

4.7. Seznam souborů

Detailní technická specifikace je uložena v těchto souborech:

Soubor	Popis
GetCredential_v2_1.wsdl	Definice autentizační webové služby KAAS ve verzi v2_1.

Poznámka: Ve WSDL souboru je uvedena adresa endpointu pro ostré provozní prostředí KAAS dostupné z internetu. V případě použití jiného prostředí je potřeba si adresu ručně opravit.

5. Webová služba verze v3_4

Tato webová služba poskytuje externímu systému (AIS) informace o uživateli, který se autentizoval za účelem získání přístupu do daného externího systému (AIS).

5.1. Rozhraní přihlašovací stránky

Po detekci nepřihlášeného uživatele provádí AIS přesměrování na přihlašovací stránku KAAS a předává identifikátor AIS, který je předáván v parametru „atsId".

Adresy přihlašovací stránky KAAS:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/login?atsId=exampleId
provozní	https://kaas.czechpoint.cz/as/login?atsId=exampleId

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

5.2. Rozhraní pro příjem autentizačního tokenu

KAAS přesměruje uživatele na URL adresu, která je definována v konfiguraci AIS v JIP. Toto URL, které je v plné režii AIS, musí přijímat parametr „sessionId", ve kterém je do AIS předáván vygenerovaný autentizační token. Tento token AIS použije pro volání autentizační webové služby, popsané v následující kapitole.

Příklad URL: https://[url-adresa-ais]?sessionId=01-8c57c8b70acb41598456914f17ae933b

5.3. Rozhraní pro odhlášení uživatele

V okamžiku, kdy se uživatel odhlašuje z AIS, by jej AIS měl z bezpečnostních důvodů přesměrovat do JIP/KAAS, kde rovněž dojde k odhlášení uživatele. Pokud se uživatel přihlásil do KAAS/JIP prostřednictvím NIA, JIP/KAAS provede rovněž přesěrování uživatele do NIA, kde dojde k odhlášení uživatele z NIA.

V okamžiku, kdy uživatel klikne na stránkách AIS na odkaz/tlačítko pro odhlášení, by AIS měl uživatele přesměrovat na následující adresu JIP/KAAS:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*
provozní	https://www.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

V parametru „atsId" se předává identifikátor AIS podobně jako v rozhraní přihlašovací stránky (viz výše).

V parametru „uri" se předává návratová adresa AIS, na kterou má JIP/KAAS uživatele přesměrovat po dokončení jeho odhlášení v JIP/KAAS a případně také v NIA. Předaná návratová adresa se ověřuje vůči „URL pro odhlášení", které je uloženo v konfiguraci AIS. „URL pro odhlášení" v konfiguraci se musí shodovat s počátkem návratové adresy v parametru „uri". Např. je-li v konfiguraci AIS uloženo „https://www.domena.cz/logout/", pak v parametru „uri" mohou být do JIP/KAAS předány návratové adresy „https://www.domena.cz/logout/?origin=jipkaas" nebo „https://www.domena.cz/logout/user/jnovak/" apod.

5.4. Způsob komunikace s webovou službou

Mezi autentizační webovou službou KAAS a AIS probíhá komunikace typu „request-response". Komunikace probíhá pomocí protokolu HTTPS, pro přenos zpráv se používá formát SOAP 1.1. Při volání webové služby je zapotřebí správně definovat a vyplňovat atribut „soapAction" v souladu s přiloženým odpovídajícím WSDL souborem.

Komunikace je zabezpečena pomocí šifrování. Používá se protokol TLS 1.2. Starší verze protokolu (SSL, TLS 1.0, TLS 1.1) jsou zakázány.

Ověření AIS je zajištěno pomocí autentizace certifikátem. AIS se musí vůči 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). Zejména v případě I.CA musí vydaný certifikát obsahovat v rozšíření certifikátu „extendedKeyUsage" atribut „Client Authentication" (id-kp-clientAuth, OID 1.3.6.1.5.5.7.3.2). Tento autentizační certifikát musí být zaregistrován v nastavení AIS, což se provede pomocí administrační aplikace Správa dat (https://www.czechpoint.cz/spravadat/).

Komunikaci iniciuje AIS, který zasílá na WS KAAS „request". WS KAAS poté vrací „response". AIS zasílá „request" na endpoint:

Prostředí KAAS	Adresa
testovací	https://cert.test.czechpoint.cz/asws/atsEndpoint
provozní	https://kaas-crt.czechpoint.cz/asws/atsEndpoint

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

5.5. Metoda heartBeat – ověření dostupnosti webové služby

5.5.1. Příklad komunikace WS

Request	<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <soapenv:Body> <m:heartBeatRequest xmlns:m="http://agw-as.cz/ats-ws/atsSzr/v3_4"> </m:heartBeatRequest> </soapenv:Body> </soapenv:Envelope>
Response	<?xml version="1.0" encoding="UTF-8"?> <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Header/> <soapenv:Body> <v3_4:heartBeatResponse xmlns:v3_4="http://agw-as.cz/ats-ws/atsSzr/v3_4"> <v3_4:status>OK</v3_4:status> </v3_4:heartBeatResponse> </soapenv:Body> </soapenv:Envelope>

5.5.2. Vysvětlivky

Hodnota	Význam
status	Strukturovaná informace o výsledku zpracování žádosti.
code	Kód s číslem chyby v případě nedostupnosti autentizační WS.
message	Textová informace o příčině nedostupnosti autentizační WS.

5.5.3. Popis stavů výsledku zpracování

Ve zprávách typu „response" se v elementu „status" vrací informace o výsledku zpracování žádosti, která může nabývat těchto hodnot:

Hodnota	Význam
OK	Požadavek byl zpracován korektně.
ERROR	Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.

5.6. Metoda authConfirmation – autentizace uživatelů

5.6.1. Příklad komunikace WS

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <soapenv:Body>
    <m:authConfirmationRequest xmlns:m="http://agw-as.cz/ats-ws/atsSzr/v3_4">
      <m:sessionId>00-c679c0687f2d43ebbcd766876f90da66</m:sessionId>
    </m:authConfirmationRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Response

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body>
    <kaas:authConfirmationResponse xmlns:kaas="http://agw-as.cz/ats-ws/atsSzr/v3_4">
      <kaas:status>OK</kaas:status>
      <kaas:userRequestIp>192.168.0.1</ kaas:userRequestIp>
      < kaas:attributes>
        <kaas:Username>jnovak</kaas:Username>
        <kaas:UzivatelId>E5TVdDM2zEXfkxOU1XQzNg==</kaas:UzivatelId>
        <kaas:ZkratkaSubjektu>JstrbLhota</kaas:ZkratkaSubjektu>
        <kaas:IcSubjektu>00235415</kaas:IcSubjektu>
        <kaas:Jmeno>Jan</kaas:Jmeno>
        <kaas:Prijmeni>Novák</kaas:Prijmeni>
        <kaas:TitulPred>Ing.</kaas:TitulPred>
        <kaas:TitulZa>CSc</kaas:TitulZa>
        <kaas:PristupoveRole>
          <kaas:role>Administrator</kaas:role>
        </kaas:PristupoveRole>
        <kaas:CinnostniRole>
          <kaas:Agenda>
            <kaas:KodAgendy>A100</kaas:KodAgendy>
            <kaas:KodCinnostniRole>ACR01</kaas:KodCinnostniRole>
          </kaas:Agenda>
          <kaas:Agenda>
            <kaas:KodAgendy>A101</kaas:KodAgendy>
            <kaas:KodCinnostniRole>ACR02</kaas:KodCinnostniRole>
          </kaas:Agenda>
        </kaas:CinnostniRole>
        <kaas:Email>jnovak@jestrabi-lhota.cz</kaas:Email>
        <kaas:NazevSubjektu>Městský úřad Jestřábí Lhota</kaas:NazevSubjektu>
        <kaas:EmailSubjektu/>
      <kaas:TypInstituce>9</kaas:TypInstituce>
      <kaas:OvmPrimarni>FALSE</kaas:OvmPrimarni>
      <kaas:TypPrihlaseni>p-cert</kaas:TypPrihlaseni>
      <kaas:OsobaZtotoznena>false</kaas:OsobaZtotoznena>
      <kaas:TokenAifo/>
        <kaas:Pracoviste>
          <kaas:Id>DislPracPrah</kaas:Id>
          <kaas:Nazev>Dislokované pracoviště Praha</kaas:Nazev>
          <kaas:Adresa>Na žertvách 132/24, Libeň - Praha 8, 18000 Praha</kaas:Adresa>
          <kaas:KodAdresy>22376097</kaas:KodAdresy>
        </kaas:Pracoviste>
        <kaas:IdentifikatorOvm>12345678</kaas:IdentifikatorOvm>
        <kaas:TimeLimitedId>T00-b899e113cbfa47c08f8fb7fdaa571f4f</kaas:TimeLimitedId>
```

```
        </kaas:attributes>
    </kaas:authConfirmationResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

5.6.2. Vysvětlivky

Hodnota	Význam
sessionId	Identifikace session uživatele. Token, získaný od KAAS po přesměrování uživatele do AIS (viz kapitola 2.1, bod 7).
status	Strukturovaná informace o výsledku zpracování žádosti.
userRequestIp	IP uživatele při přihlášení. Může být IPv6/IPv4. Pokud uživatel přistupuje přes proxy, bere se IP proxy, která je nejdále od uživatele.
attributes	Informace o autentizovaném uživateli. Viz kapitola 5.6.4.

5.6.3. Popis stavů výsledku zpracování

Ve zprávách typu „response" se v elementu „status" vrací informace o výsledku zpracování žádosti, která může nabývat těchto hodnot:

Hodnota	Význam
OK	Požadavek byl zpracován korektně.
SYSTEM_ERROR	Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.
SESSION_NOT_FOUND	Vrací v případě, že byl v požadavku zaslán neexistující token.

5.6.4. Seznam atributů předávaných do AIS

Atribut	Popis
ZkratkaSubjektu	Zkratka subjektu dotazujícího se nebo žádajícího uživatele. Jedinečný identifikátor subjektu v rámci JIP.
IcSubjektu	IČ subjektu dotazujícího se nebo žádajícího uživatele.
UzivatelId	Jedinečný identifikátor uživatele v rámci JIP.
Username	Uživatelské jméno uživatele v JIP.
Jmeno	Jméno uživatele
Prijmení	Příjmení uživatele
TitulPred	Titul před jménem
TitulZa	Titul za jménem
PristupoveRole	Seznam přístupových (aplikačních) rolí do AIS, které jsou přiřazeny uživateli.
role	Označení konkrétní přístupové (aplikační) role, přiřazené uživateli.
CinnostniRole	Seznam činnostních rolí, které jsou přiřazeny uživateli.
KodAgendy	Kód agendy, k níž je daná činnostní role přiřazena.
KodCinnostniRole	Kód činnostní role, přiřazené uživateli.
Email	E-mailová adresa uživatele.
NazevSubjektu	Název subjektu dotazujícího se nebo žádajícího uživatele.
EmailSubjektu	E-mailová adresa subjektu.
TypInstituce	Typ instituce. Číselník viz kap. 12.1.
OvmPrimarni	Hodnota „true" nebo „false" označující hlavní subjekt pro subjekty s duplicitním IČ.

Atribut	Popis
TypPrihlaseni	Způsob přihlášení uživatele do KAAS. Číselník viz kap. 12.2.
OsobaZtotoznena	Indikátor, zda byla daná osoba ztotožněna vůči ROB. Může nabývat hodnot „true" nebo „false".
TokenAifo	Datová struktura v kódování Base64 pro získání AIFO osoby. Aktuálně není implementováno z důvodu chybějící webové služby základních registrů!
Pracoviste	Údaje o pracovišti, ve kterém uživatel vykonává svoji práci.
Id	Alfanumerický identifikátor pracoviště
Nazev	Název pracoviště
Adresa	Adresa pracoviště
KodAdresy	Kód adresy pracoviště ve formě kódu adresního místa z RUIAN.
IdentifikatorOvm	Identifikátor OVM, uvedený v Rejstříku OVM.
TimeLimitedId	Speciální autorizační token, který se používá pro přístup k vybraným webovým službám. Vrací se jen v případě, že daný autentizovaný uživatel je lokálním administrátorem. Token má omezenou platnost – další informace jsou uvedeny v dokumentaci k příslušným webovým službám.

Poznámka: Typy atributů a definovaná omezení hodnot atributů jsou uvedena ve WSDL souboru – viz kapitola 5.7.

5.7. Seznam souborů

Detailní technická specifikace je uložena v těchto souborech:

Soubor	Popis
GetCredential_v3_4.wsdl	Definice autentizační webové služby KAAS ve verzi v3_4.

Poznámka: Ve WSDL souboru je uvedena adresa endpointu pro ostré provozní prostředí KAAS dostupné z internetu. V případě použití jiného prostředí je potřeba si adresu ručně opravit.

6. Webová služba verze v4_1

Tato webová služba poskytuje externímu systému (AIS) informace o uživateli, který se autentizoval za účelem získání přístupu do daného externího systému (AIS).

Předávané informace o uživateli jsou v souladu s § 56a odst. 5 zákona č. 111/2009 Sb., o základních registrech.

6.1. Rozhraní přihlašovací stránky

Po detekci nepřihlášeného uživatele provádí AIS přesměrování na přihlašovací stránku KAAS a předává identifikátor AIS, který je předáván v parametru „atsId".

Adresy přihlašovací stránky KAAS:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/login?atsId=exampleId
provozní	https://kaas.czechpoint.cz/as/login?atsId=exampleId

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

6.2. Rozhraní pro příjem autentizačního tokenu

KAAS přesměruje uživatele na URL adresu, která je definována v konfiguraci AIS v JIP. Toto URL, které je v plné režii AIS, musí přijímat parametr „sessionId", ve kterém je do AIS předáván vygenerovaný autentizační token. Tento token AIS použije pro volání autentizační webové služby, popsané v následující kapitole.

Příklad URL: https://[url-adresa-ais]?sessionId=01-8c57c8b70acb41598456914f17ae933b

6.3. Rozhraní pro odhlášení uživatele

V okamžiku, kdy se uživatel odhlašuje z AIS, by jej AIS měl z bezpečnostních důvodů přesměrovat do JIP/KAAS, kde rovněž dojde k odhlášení uživatele. Pokud se uživatel přihlásil do KAAS/JIP prostřednictvím NIA, JIP/KAAS provede rovněž přesěrování uživatele do NIA, kde dojde k odhlášení uživatele z NIA.

V okamžiku, kdy uživatel klikne na stránkách AIS na odkaz/tlačítko pro odhlášení, by AIS měl uživatele přesměrovat na následující adresu JIP/KAAS:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*
provozní	https://www.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

V parametru „atsId" se předává identifikátor AIS podobně jako v rozhraní přihlašovací stránky (viz výše).

V parametru „uri" se předává návratová adresa AIS, na kterou má JIP/KAAS uživatele přesměrovat po dokončení jeho odhlášení v JIP/KAAS a případně také v NIA. Předaná návratová adresa se ověřuje vůči „URL pro odhlášení", které je uloženo v konfiguraci AIS. „URL pro odhlášení" v konfiguraci se musí shodovat s počátkem návratové adresy v parametru „uri". Např. je-li v konfiguraci AIS uloženo „https://www.domena.cz/logout/", pak v parametru „uri" mohou být do JIP/KAAS předány návratové adresy „https://www.domena.cz/logout/?origin=jipkaas" nebo „https://www.domena.cz/logout/user/jnovak/" apod.

6.4. Způsob komunikace s webovou službou

Mezi autentizační webovou službou KAAS a AIS probíhá komunikace typu „request-response". Komunikace probíhá pomocí protokolu HTTPS, pro přenos zpráv se používá formát SOAP 1.1. Při volání webové služby je zapotřebí správně definovat a vyplňovat atribut „soapAction" v souladu s přiloženým odpovídajícím WSDL souborem.

Komunikace je zabezpečena pomocí šifrování. Používá se protokol TLS 1.2. Starší verze protokolu (SSL, TLS 1.0, TLS 1.1) jsou zakázány.

Ověření AIS je zajištěno pomocí autentizace certifikátem. AIS se musí vůči 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). Zejména v případě I.CA musí vydaný certifikát obsahovat v rozšíření certifikátu „extendedKeyUsage" atribut „Client Authentication" (id-kp-clientAuth, OID 1.3.6.1.5.5.7.3.2). Tento autentizační certifikát musí být zaregistrován v nastavení AIS, což se provede pomocí administrační aplikace Správa dat (https://www.czechpoint.cz/spravadat/).

Komunikaci iniciuje AIS, který zasílá na WS KAAS „request". WS KAAS poté vrací „response". AIS zasílá „request" na endpoint:

Prostředí KAAS	Adresa
testovací	https://cert.test.czechpoint.cz/asws/atsEndpoint
provozní	https://kaas-crt.czechpoint.cz/asws/atsEndpoint

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

6.5. Metoda heartBeat – ověření dostupnosti webové služby

6.5.1. Příklad komunikace WS

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <soapenv:Body>
    <m:heartBeatRequest xmlns:m="http://agw-as.cz/ats-ws/atsSzr/v4_1">
    </m:heartBeatRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Response

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body>
    <v4_1:heartBeatResponse xmlns:v4_1="http://agw-as.cz/ats-ws/atsSzr/v4_1">
      <v4_1:status>OK</v4_1:status>
    </v4_1:heartBeatResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

6.5.2. Vysvětlivky

Hodnota	Význam
status	Strukturovaná informace o výsledku zpracování žádosti.
code	Kód s číslem chyby v případě nedostupnosti autentizační WS.
message	Textová informace o příčině nedostupnosti autentizační WS.

6.5.3. Popis stavů výsledku zpracování

Ve zprávách typu „response" se v elementu „status" vrací informace o výsledku zpracování žádosti, která může nabývat těchto hodnot:

Hodnota	Význam
OK	Požadavek byl zpracován korektně.
ERROR	Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.

6.6. Metoda authConfirmation – autentizace uživatelů

6.6.1. Příklad komunikace WS

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <soapenv:Body>
    <m:authConfirmationRequest xmlns:m="http://agw-as.cz/ats-ws/atsSzr/v4_1">
      <m:sessionId>00-c679c0687f2d43ebbcd766876f90da66</m:sessionId>
    </m:authConfirmationRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Response

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <kaas:authConfirmationResponse xmlns:kaas="http://agw-as.cz/ats-ws/atsSzr/v4_1">
      <kaas:status>OK</kaas:status>
      <kaas:userRequestIp>192.168.0.1</kaas:userRequestIp>
      <kaas:attributes>
        <kaas:Username>jnovak</kaas:Username>
        <kaas:UzivatelId>xrtWW0Ug0UtchMa7VltFIA==</kaas:UzivatelId>
        <kaas:ZkratkaSubjektu>JstrbLhota</kaas:ZkratkaSubjektu>
        <kaas:IcSubjektu>00235415</kaas:IcSubjektu>
        <kaas:Jmeno>Jan</kaas:Jmeno>
        <kaas:Prijmeni>Novak</kaas:Prijmeni>
        <kaas:TitulPred>Bc.</kaas:TitulPred>
        <kaas:TitulZa/>
        <kaas:PristupoveRole>
          <kaas:role>Administrator</kaas:role>
        </kaas:PristupoveRole>
        <kaas:CinnostniRole>
          <kaas:Agenda>
            <kaas:KodAgendy>A113</kaas:KodAgendy>
            <kaas:KodCinnostniRole>CR1011</kaas:KodCinnostniRole>
          </kaas:Agenda>
        </kaas:CinnostniRole>
        <kaas:Email>jnovak@jestrabi-lhota.cz</kaas:Email>
        <kaas:NazevSubjektu>Městský úřad Jestřábí Lhota</kaas:NazevSubjektu>
        <kaas:EmailSubjektu/>
        <kaas:TypInstituce>9</kaas:TypInstituce>
        <kaas:OvmPrimarni>TRUE</kaas:OvmPrimarni>
        <kaas:TypPrihlaseni>p-cert</kaas:TypPrihlaseni>
        <kaas:OsobaZtotoznena>false</kaas:OsobaZtotoznena>
        <kaas:TokenAifo/>
        <kaas:Pracoviste>
          <kaas:Id>DislPracPrah</kaas:Id>
          <kaas:Nazev>Dislokované pracoviště Praha</kaas:Nazev>
          <kaas:Adresa>Na žertvách 132/24, Libeň - Praha 8, 18000 Praha</kaas:Adresa>
          <kaas:KodAdresy>22376097</kaas:KodAdresy>
        </kaas:Pracoviste>
        <kaas:MistoNarozeni stav="nespravny">
          <kaas:MistoNarozeniCr mop="false"
nazev="Arnoltice">562343</kaas:MistoNarozeniCr>
          <kaas:MistoNarozeniSvet>
            <kaas:stat nazev="Ukrajina">804</kaas:stat>
            <kaas:misto>KYJEV</kaas:misto>
          </kaas:MistoNarozeniSvet>
```

```
            </kaas:MistoNarozeni>
            <kaas:DatumNarozeni stav="spravny">1978-04-02</kaas:DatumNarozeni>
            <kaas:DatumUmrti/>
            <kaas:Doklady>
               <kaas:Doklad stav="spravny" typ="P">11111908</kaas:Doklad>
               <kaas:Doklad stav="spravny" typ="ID">111111908</kaas:Doklad>
            </kaas:Doklady>
            <kaas:NeevidovatOsobniUdaje>false</kaas:NeevidovatOsobniUdaje>
            <kaas:IdentifikatorOvm>12345678</kaas:IdentifikatorOvm>
            <kaas:TimeLimitedId>T00-
b899e113cbfa47c08f8fb7fdaa571f4f</kaas:TimeLimitedId>
         </kaas:attributes>
      </kaas:authConfirmationResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```


6.6.2. Vysvětlivky

Hodnota	Význam
sessionId	Identifikace session uživatele. Token, získaný od KAAS po přesměrování uživatele do AIS (viz kapitola 2.1, bod 7).
status	Strukturovaná informace o výsledku zpracování žádosti.
userRequestIp	IP uživatele při přihlášení. Může být IPv6/IPv4. Pokud uživatel přistupuje přes proxy, bere se IP proxy, která je nejdále od uživatele.
attributes	Informace o autentizovaném uživateli. Viz kapitola 6.6.4.

6.6.3. Popis stavů výsledku zpracování

Ve zprávách typu „response" se v elementu „status" vrací informace o výsledku zpracování žádosti, která může nabývat těchto hodnot:

Hodnota	Význam
OK	Požadavek byl zpracován korektně.
SYSTEM_ERROR	Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.
SESSION_NOT_FOUND	Vrací v případě, že byl v požadavku zaslán neexistující token.

6.6.4. Seznam atributů předávaných do AIS

Atribut	Popis
ZkratkaSubjektu	Zkratka subjektu dotazujícího se nebo žádajícího uživatele. Jedinečný identifikátor subjektu v rámci JIP.
IcSubjektu	IČ subjektu dotazujícího se nebo žádajícího uživatele.
UzivatelId	Jedinečný identifikátor uživatele v rámci JIP.
Username	Uživatelské jméno uživatele v JIP.
Jmeno	Jméno uživatele
Prijmení	Příjmení uživatele
TitulPred	Titul před jménem
TitulZa	Titul za jménem
PristupoveRole	Seznam přístupových (aplikačních) rolí do AIS, které jsou přiřazeny uživateli.
role	Označení konkrétní přístupové (aplikační) role, přiřazené uživateli.
CinnostniRole	Seznam činnostních rolí, které jsou přiřazeny uživateli.

Atribut	Popis
KodAgendy	Kód agendy, k níž je daná činnostní role přiřazena.
KodCinnostniRole	Kód činnostní role, přiřazené uživateli.
Email	E-mailová adresa uživatele.
NazevSubjektu	Název subjektu dotazujícího se nebo žádajícího uživatele.
EmailSubjektu	E-mailová adresa subjektu.
TypInstituce	Typ instituce. Číselník viz kap. 12.1.
OvmPrimarni	Hodnota „true" nebo „false" označující hlavní subjekt pro subjekty s duplicitním IČ.
TypPrihlaseni	Způsob přihlášení uživatele do KAAS. Číselník viz kap. 12.2.
OsobaZtotoznena	Indikátor, zda byla daná osoba ztotožněna vůči ROB. Může nabývat hodnot „true" nebo „false".
TokenAifo	Datová struktura v kódování Base64 pro získání AIFO osoby. Aktuálně není implementováno z důvodu chybějící webové služby základních registrů!
Pracoviste	Údaje o pracovišti, ve kterém uživatel vykonává svoji práci.
Id	Alfanumerický identifikátor pracoviště
Nazev	Název pracoviště
Adresa	Adresa pracoviště
KodAdresy	Kód adresy pracoviště ve formě kódu adresního místa z RUIAN.
Mistonarozeni	Údaje o místě narození uživatele.
MistoNarozeniCr	Údaj o místě narození v ČR – kód z RUIAN. Atributy v elementu mají následující význam: • „mop" – atribut s příznakem, zda se jedná o kód městského obvodu • „nazev" – atribut s názvem místa narození v ČR
MistoNarozeniSvet	Údaje o místě narození v zahraničí
stat	Kód státu. Číselník států viz webové stránky Správy základních registrů. Atribut „nazev" obsahuje textový název státu.
misto	Název místa narození v zahraničí.
DatumNarozeni	Datum narození.
DatumUmrti	Datum úmrtí.
Doklady	Seznam elektronicky čitelných dokladů.
Doklad	Číslo dokladu. Atributy v elementu mají následující význam: • typ – atribut uvádějící typ dokladu. Číselník typů dokladů viz webové stránky Správy základních registrů.
NeevidovatOsobniUdaje	Příznak, zda je pro daný uživatelský účet zakázáno evidování osobních údajů.
IdentifikatorOvm	Identifikátor OVM, uvedený v Rejstříku OVM.
TimeLimitedId	Speciální autorizační token, který se používá pro přístup k vybraným webovým službám. Vrací se jen v případě, že daný autentizovaný uživatel je lokálním administrátorem. Token má omezenou platnost – další informace jsou uvedeny v dokumentaci k příslušným webovým službám.

Poznámka: Některé elementy obsahují atribut „stav", který nabývá hodnot „spravny" nebo „nespravny". Tento atribut udává, zda je daný údaj v registru obyvatel označený jako nesprávný.

Poznámka: Typy atributů a definovaná omezení hodnot atributů jsou uvedena ve WSDL souboru – viz kapitola 6.7.

6.7. Seznam souborů

Detailní technická specifikace je uložena v těchto souborech:

Soubor	Popis
GetCredential_v4_1.wsdl	Definice autentizační webové služby KAAS ve verzi v4_1.

Poznámka: Ve WSDL souboru je uvedena adresa endpointu pro ostré provozní prostředí KAAS dostupné z internetu. V případě použití jiného prostředí je potřeba si adresu ručně opravit.

7. Webová služba verze v4_2

Tato webová služba poskytuje externímu systému (AIS) informace o uživateli, který se autentizoval za účelem získání přístupu do daného externího systému (AIS).

Předávané informace o uživateli jsou v souladu s § 56a odst. 5 zákona č. 111/2009 Sb., o základních registrech.

Pochází-li uživatel ze SPUÚ, webová služba vrací v odpovědi identifikátor SPUÚ z ROVM.

Pokud se uživatel autentizoval prostřednictvím NIA, webová služba vrací v odpovědi hodnotu úrovně záruk použitého identifikačního prostředku.

7.1. Rozhraní přihlašovací stránky

Po detekci nepřihlášeného uživatele provádí AIS přesměrování na přihlašovací stránku KAAS a předává identifikátor AIS, který je předáván v parametru „atsId".

Adresy přihlašovací stránky KAAS:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/login?atsId=exampleId
provozní	https://kaas.czechpoint.cz/as/login?atsId=exampleId

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

7.2. Rozhraní pro příjem autentizačního tokenu

KAAS přesměruje uživatele na URL adresu, která je definována v konfiguraci AIS v JIP. Toto URL, které je v plné režii AIS, musí přijímat parametr „sessionId", ve kterém je do AIS předáván vygenerovaný autentizační token. Tento token AIS použije pro volání autentizační webové služby, popsané v následující kapitole.

Příklad URL: https://[url-adresa-ais]?sessionId=01-8c57c8b70acb41598456914f17ae933b

7.3. Rozhraní pro odhlášení uživatele

V okamžiku, kdy se uživatel odhlašuje z AIS, by jej AIS měl z bezpečnostních důvodů přesměrovat do JIP/KAAS, kde rovněž dojde k odhlášení uživatele. Pokud se uživatel přihlásil do KAAS/JIP prostřednictvím NIA, JIP/KAAS provede rovněž přesěrování uživatele do NIA, kde dojde k odhlášení uživatele z NIA.

V okamžiku, kdy uživatel klikne na stránkách AIS na odkaz/tlačítko pro odhlášení, by AIS měl uživatele přesměrovat na následující adresu JIP/KAAS:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*
provozní	https://www.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

V parametru „atsId" se předává identifikátor AIS podobně jako v rozhraní přihlašovací stránky (viz výše).

V parametru „uri" se předává návratová adresa AIS, na kterou má JIP/KAAS uživatele přesměrovat po dokončení jeho odhlášení v JIP/KAAS a případně také v NIA. Předaná návratová adresa se ověřuje vůči „URL pro odhlášení", které je uloženo v konfiguraci AIS. „URL pro odhlášení" v konfiguraci se musí shodovat s počátkem návratové adresy

v parametru „uri". Např. je-li v konfiguraci AIS uloženo „https://www.domena.cz/logout/", pak v parametru „uri" mohou být do JIP/KAAS předány návratové adresy „https://www.domena.cz/logout/?origin=jipkaas" nebo „https://www.domena.cz/logout/user/jnovak/" apod.

7.4. Způsob komunikace s webovou službou

Mezi autentizační webovou službou KAAS a AIS probíhá komunikace typu „request-response". Komunikace probíhá pomocí protokolu HTTPS, pro přenos zpráv se používá formát SOAP 1.1. Při volání webové služby je zapotřebí správně definovat a vyplňovat atribut „soapAction" v souladu s přiloženým odpovídajícím WSDL souborem.

Komunikace je zabezpečena pomocí šifrování. Používá se protokol TLS 1.2. Starší verze protokolu (SSL, TLS 1.0, TLS 1.1) jsou zakázány.

Ověření AIS je zajištěno pomocí autentizace certifikátem. AIS se musí vůči 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). Zejména v případě I.CA musí vydaný certifikát obsahovat v rozšíření certifikátu „extendedKeyUsage" atribut „Client Authentication" (id-kp-clientAuth, OID 1.3.6.1.5.5.7.3.2). Tento autentizační certifikát musí být zaregistrován v nastavení AIS, což se provede pomocí administrační aplikace Správa dat (https://www.czechpoint.cz/spravadat/).

Komunikaci iniciuje AIS, který zasílá na WS KAAS „request". WS KAAS poté vrací „response". AIS zasílá „request" na endpoint:

Prostředí KAAS	Adresa
testovací	https://cert.test.czechpoint.cz/asws/atsEndpoint
provozní	https://kaas-crt.czechpoint.cz/asws/atsEndpoint

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

7.5. Metoda heartBeat – ověření dostupnosti webové služby

7.5.1. Příklad komunikace WS

Request	<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <soapenv:Body> <m:heartBeatRequest xmlns:m="http://agw-as.cz/ats-ws/atsSzr/v4_2"> </m:heartBeatRequest> </soapenv:Body> </soapenv:Envelope>
Response	<?xml version="1.0" encoding="UTF-8"?> <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Header/> <soapenv:Body> <v4_2:heartBeatResponse xmlns:v4_2="http://agw-as.cz/ats-ws/atsSzr/v4_2"> <v4_2:status>OK</v4_1:status> </v4_2:heartBeatResponse> </soapenv:Body> </soapenv:Envelope>

7.5.2. Vysvětlivky

Hodnota	Význam
status	Strukturovaná informace o výsledku zpracování žádosti.
code	Kód s číslem chyby v případě nedostupnosti autentizační WS.
message	Textová informace o příčině nedostupnosti autentizační WS.

7.5.3. Popis stavů výsledku zpracování

Ve zprávách typu „response" se v elementu „status" vrací informace o výsledku zpracování žádosti, která může nabývat těchto hodnot:

Hodnota	Význam
OK	Požadavek byl zpracován korektně.
ERROR	Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.

7.6. Metoda authConfirmation – autentizace uživatelů

7.6.1. Příklad komunikace WS

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <soapenv:Body>
    <m:authConfirmationRequest xmlns:m="http://agw-as.cz/ats-ws/atsSzr/v4_2">
      <m:sessionId>00-c679c0687f2d43ebbcd766876f90da66</m:sessionId>
    </m:authConfirmationRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Response

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <kaas:authConfirmationResponse xmlns:kaas="http://agw-as.cz/ats-ws/atsSzr/v4_2">
      <kaas:status>OK</kaas:status>
      <kaas:userRequestIp>192.168.0.1</kaas:userRequestIp>
      <kaas:attributes>
        <kaas:Username>jnovak</kaas:Username>
        <kaas:UzivatelId>xrtWW0Ug0UtchMa7VltFIA==</kaas:UzivatelId>
        <kaas:ZkratkaSubjektu>spuu_00836265.9999</kaas:ZkratkaSubjektu>
        <kaas:IcSubjektu>836265</kaas:IcSubjektu>
        <kaas:Jmeno>Jan</kaas:Jmeno>
        <kaas:Prijmeni>Novak</kaas:Prijmeni>
        <kaas:TitulPred>Bc.</kaas:TitulPred>
        <kaas:TitulZa/>
        <kaas:PristupoveRole>
          <kaas:role>Administrator</kaas:role>
        </kaas:PristupoveRole>
        <kaas:CinnostniRole/>
        <kaas:Email/>
        <kaas:NazevSubjektu>BULGER a ASSOCIATES</kaas:NazevSubjektu>
        <kaas:EmailSubjektu/>
        <kaas:TypInstituce>101</kaas:TypInstituce>
        <kaas:OvmPrimarni>FALSE</kaas:OvmPrimarni>
        <kaas:TypPrihlaseni>p-cert</kaas:TypPrihlaseni>
        <kaas:TypPrihlaseniNia/>
        <kaas:OsobaZtotoznena>false</kaas:OsobaZtotoznena>
        <kaas:TokenAifo/>
        <kaas:Pracoviste>
          <kaas:Id>spuu_00836265.9999</kaas:Id>
          <kaas:Nazev>BULGER a ASSOCIATES</kaas:Nazev>
          <kaas:Adresa>Novákových 456/8, Libeň - Praha 8, 18000 Praha</kaas:Adresa>
          <kaas:KodAdresy>22378235</kaas:KodAdresy>
        </kaas:Pracoviste>
        <kaas:MistoNarozeni/>
```

```
            <kaas:Doklady/>
            <kaas:NeevidovatOsobniUdaje>false</kaas:NeevidovatOsobniUdaje>
            <kaas:IdentifikatorSpuu>00836265.9999</kaas:IdentifikatorSpuu>
            <kaas:TimeLimitedId/>
        </kaas:attributes>
    </kaas:authConfirmationResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

7.6.2. Vysvětlivky

Hodnota	Význam
sessionId	Identifikace session uživatele přihlášeného do KAAS. Token, získaný od KAAS po přesměrování uživatele do AIS (viz kapitola 2.1, bod 7).
status	Strukturovaná informace o výsledku zpracování žádosti.
userRequestIp	IP uživatele při přihlášení. Může být IPv6/IPv4. Pokud uživatel přistupuje přes proxy, bere se IP proxy, která je nejdále od uživatele.
attributes	Informace o autentizovaném uživateli. Viz kapitola 7.6.4.

7.6.3. Popis stavů výsledku zpracování

Ve zprávách typu „response" se v elementu „status" vrací informace o výsledku zpracování žádosti, která může nabývat těchto hodnot:

Hodnota	Význam
OK	Požadavek byl zpracován korektně.
SYSTEM_ERROR	Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.
SESSION_NOT_FOUND	Vrací v případě, že byl v požadavku zaslán neexistující token.

7.6.4. Seznam atributů předávaných do AIS

Poznámka: Subjektem v níže uvedeném textu může být jak OVM, tak i SPUÚ.

Atribut	Popis
ZkratkaSubjektu	Zkratka subjektu dotazujícího se nebo žádajícího uživatele. Jedinečný identifikátor subjektu v rámci JIP.
IcSubjektu	IČ subjektu dotazujícího se nebo žádajícího uživatele.
UzivatelId	Jedinečný identifikátor uživatele v rámci JIP.
Username	Uživatelské jméno uživatele v JIP.
Jmeno	Jméno uživatele
Prijmení	Příjmení uživatele
TitulPred	Titul před jménem
TitulZa	Titul za jménem
PristupoveRole	Seznam přístupových (aplikačních) rolí do AIS, které jsou přiřazeny uživateli.
role	Označení konkrétní přístupové (aplikační) role, přiřazené uživateli.
CinnostniRole	Seznam činnostních rolí, které jsou přiřazeny uživateli.
KodAgendy	Kód agendy, k níž je daná činnostní role přiřazena.
KodCinnostniRole	Kód činnostní role, přiřazené uživateli.
Email	E-mailová adresa uživatele.

Atribut	Popis
NazevSubjektu	Název subjektu dotazujícího se nebo žádajícího uživatele.
EmailSubjektu	E-mailová adresa subjektu.
TypInstituce	Typ instituce. Číselník viz kap. 12.1.
OvmPrimarni	Hodnota „true" nebo „false" označující hlavní subjekt pro subjekty s duplicitním IČ.
TypPrihlaseni	Způsob přihlášení uživatele do KAAS. Číselník viz kap. 12.2.
TypPrihlaseniNia	Hodnota úrovně záruk použitého identifikačního prostředku, pokud se uživatel autentizoval prostřednictvím NIA.
OsobaZtotoznena	Indikátor, zda byla daná osoba ztotožněna vůči ROB. Může nabývat hodnot „true" nebo „false".
TokenAifo	Datová struktura v kódování Base64 pro získání AIFO osoby. Aktuálně není implementováno z důvodu chybějící webové služby základních registrů!
Pracoviste	Údaje o pracovišti, ve kterém uživatel vykonává svoji práci.
Id	Alfanumerický identifikátor pracoviště
Nazev	Název pracoviště
Adresa	Adresa pracoviště
KodAdresy	Kód adresy pracoviště ve formě kódu adresního místa z RUIAN.
Mistonarozeni	Údaje o místě narození uživatele.
MistoNarozeniCr	Údaj o místě narození v ČR – kód z RUIAN. Atributy v elementu mají následující význam: • „mop" – atribut s příznakem, zda se jedná o kód městského obvodu • „nazev" – atribut s názvem místa narození v ČR
MistoNarozeniSvet	Údaje o místě narození v zahraničí
stat	Kód státu. Číselník států viz webové stránky Správy základních registrů. Atribut „nazev" obsahuje textový název státu.
misto	Název místa narození v zahraničí.
DatumNarozeni	Datum narození.
DatumUmrti	Datum úmrtí.
Doklady	Seznam elektronicky čitelných dokladů.
Doklad	Číslo dokladu. Atributy v elementu mají následující význam: • typ – atribut uvádějící typ dokladu. Číselník typů dokladů viz webové stránky Správy základních registrů.
NeevidovatOsobniUdaje	Příznak, zda je pro daný uživatelský účet zakázáno evidování osobních údajů.
IdentifikatorOvm	Identifikátor OVM, uvedený v Rejstříku OVM.
IdentifikatorSpuu	Identifikátor SPUÚ, uvedený v Rejstříku OVM.
TimeLimitedId	Speciální autorizační token, který se používá pro přístup k vybraným webovým službám. Vrací se jen v případě, že daný autentizovaný uživatel je lokálním administrátorem. Token má omezenou platnost – další informace jsou uvedeny v dokumentaci k příslušným webovým službám.

Poznámka: Některé elementy obsahují atribut „stav", který nabývá hodnot „spravny" nebo „nespravny". Tento atribut udává, zda je daný údaj v registru obyvatel označený jako nesprávný.

Poznámka: Typy atributů a definovaná omezení hodnot atributů jsou uvedena ve WSDL souboru – viz kapitola 7.7.

7.7. Seznam souborů

Detailní technická specifikace je uložena v těchto souborech:

Soubor	Popis
GetCredential_v4_2.wsdl	Definice autentizační webové služby KAAS ve verzi v4_2.

Poznámka: Ve WSDL souboru je uvedena adresa endpointu pro ostré provozní prostředí KAAS dostupné z internetu. V případě použití jiného prostředí je potřeba si adresu ručně opravit.

8. Přímá autentizační webová služba verze v1

Tato webová služba provádí ověření, zda v JIP existuje účet s daným uživatelským jménem a autentizačními údaji. Externí systém (AIS) zasílá požadavek přímo na webovou službu; neplatí zde postupy autentizace popsané v kapitole 2.

Poskytování přímé autentizační služby v1 bude v nejbližší době ukončeno. Doporučujeme používat novější verze této webové služby.

8.1. Rozhraní pro odhlášení uživatele

V okamžiku, kdy se uživatel odhlašuje z AIS, by jej AIS měl z bezpečnostních důvodů přesměrovat do JIP/KAAS, kde rovněž dojde k odhlášení uživatele. Pokud se uživatel přihlásil do KAAS/JIP prostřednictvím NIA, JIP/KAAS provede rovněž přesěrování uživatele do NIA, kde dojde k odhlášení uživatele z NIA.

V okamžiku, kdy uživatel klikne na stránkách AIS na odkaz/tlačítko pro odhlášení, by AIS měl uživatele přesměrovat na následující adresu JIP/KAAS:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*
provozní	https://www.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

V parametru „atsId" se předává identifikátor AIS podobně jako v rozhraní přihlašovací stránky (viz výše).

V parametru „uri" se předává návratová adresa AIS, na kterou má JIP/KAAS uživatele přesměrovat po dokončení jeho odhlášení v JIP/KAAS a případně také v NIA. Předaná návratová adresa se ověřuje vůči „URL pro odhlášení", které je uloženo v konfiguraci AIS. „URL pro odhlášení" v konfiguraci se musí shodovat s počátkem návratové adresy v parametru „uri". Např. je-li v konfiguraci AIS uloženo „https://www.domena.cz/logout/", pak v parametru „uri" mohou být do JIP/KAAS předány návratové adresy „https://www.domena.cz/logout/?origin=jipkaas" nebo „https://www.domena.cz/logout/user/jnovak/" apod.

8.2. Způsob komunikace s webovou službou

Mezi autentizační webovou službou KAAS a AIS probíhá komunikace typu „request-response". Komunikace probíhá pomocí protokolu HTTPS, pro přenos zpráv se používá formát SOAP 1.1. Při volání webové služby je zapotřebí správně definovat a vyplňovat atribut „soapAction" v souladu s přiloženým odpovídajícím WSDL souborem.

Komunikace je zabezpečena pomocí šifrování. Používá se protokol TLS 1.2. Starší verze protokolu (SSL, TLS 1.0, TLS 1.1) jsou zakázány.

Ověření AIS je zajištěno pomocí autentizace certifikátem, který vydala komerční certifikační autorita provozovaná českým kvalifikovaným poskytovatelem služeb vytvářejících důvěru (I.CA, PostSignum, eIdentity nebo Národní certifikační autorita). Zejména v případě I.CA musí vydaný certifikát obsahovat v rozšíření certifikátu „extendedKeyUsage" atribut „Client Authentication" (id-kp-clientAuth, OID 1.3.6.1.5.5.7.3.2). Tento autentizační certifikát musí být zaregistrován v nastavení AIS, což se provede pomocí administrační aplikace Správa dat (https://www.czechpoint.cz/spravadat/).

Komunikaci iniciuje AIS, který zasílá na WS KAAS „request". WS KAAS poté vrací „response". AIS zasílá „request" na endpoint:

Prostředí KAAS	Adresa
testovací	https://cert.test.czechpoint.cz/asws/directAuthUserEndpoint
provozní	https://kaas-crt.czechpoint.cz/asws/directAuthUserEndpoint

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

8.3. Metoda directAuthUser - ověření uživatelského účtu

8.3.1. Příklad komunikace WS

Request	<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <soapenv:Body> <m:directAuthUserRequest xmlns:m="http://agw-as.cz/ats-ws/atsUser/v1"> <m:username>jnovak</m:username> <m:password>TajneHeslo1</m:password> <m:otp>165657</m:otp> <m:certificate>E5TVdDM2zEXfkxOU1XQzNg...</m:certificate> </m:directAuthUserRequest> </soapenv:Body> </soapenv:Envelope>
Response	<?xml version="1.0" encoding="UTF-8"?> <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Header/> <soapenv:Body> <v1:m:directAuthUserResponse xmlns:v1="http://agw-as.cz/ats-ws/atsUser/v1"> <v1:status>OK</v1:status> <v1:description>Autentizace proběhla úspěšně.</v1:description> </v1:m:directAuthUserResponse> </soapenv:Body> </soapenv:Envelope>

8.3.2. Vysvětlivky

Atributy v requestu:

Do requestu jsou vloženy credentials podle úrovně zabezpečení účtu uživatele v JIP.

Atribut	Význam
username	Uživatelské jméno účtu. Povinný údaj.
password	Přihlašovací heslo. Povinný údaj.
otp	Jednorázový OTP kód. Do requestu má smysl vkládat jen v případě, že účet má aktivovánu OTP autentizaci. **Poznámka:** Platí principy OTP přihlašování – OTP kód použitý v jednom requestu (přihlášení) nelze použít v druhém requestu (přihlášení) nebo pro regulérní přihlášení uživatele do systému.
certificate	Přihlašovací certifikát v binárním formátu DER, který je zakódován do Base64 kódování. Do requestu má smysl vkládat jen v případě, že účet má aktivováno přihlašování certifikátem. **Důležité:** AIS je zodpovědný za ověření, že přihlašující se uživatel disponuje soukromým klíčem, který odpovídá předávanému certifikátu. Jinými slovy AIS má implementováno přihlašovací rozhraní pro autentizaci certifikátem a certifikát uživatele získává

Atribut	Význam
	z autentizační session uživatele.

Atributy v response:

Atribut	Význam
status	Strukturovaná informace o výsledku zpracování žádosti.
description	Textový komentář s výsledkem operace. V případě chyby je zde uvedena podrobnější chybová hláška.

8.3.3. Popis stavů výsledku zpracování

Ve zprávách typu „response" se v elementu „status" vrací informace s výsledkem ověření autentizačních údajů:

Hodnota	Význam
OK	Ověření účtu proběhlo úspěšně. Účet se zadanými přihlašovacími údaji v JIP existuje.
SYSTEM_ERROR	Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.
VERIFICATION_FAILED	Ověření účtu nebylo úspěšné. Bylo zadáno nesprávné jméno účtu nebo nesprávné přihlašovací údaje.

Přítomné elementy v requestu musí odpovídat aktivovaným autentizačním metodám v účtu v JIP. Tj. pokud má účet aktivovánu OTP autentizaci, musí se v requestu nacházet element „otp", jinak ověření skončí výsledkem VERIFICATION_FAILED. Obdobně pokud má uživatel zaregistrován ve svém účtu v JIP komerční certifikát, musí být v requestu přítomen element „certificate".

8.4. Seznam souborů

Detailní technická specifikace je uložena v těchto souborech:

Soubor	Popis
DirectAuth_v1.wsdl	Definice přímé autentizační webové služby KAAS ve verzi v1.

Poznámka: Ve WSDL souboru je uvedena adresa endpointu pro ostré provozní prostředí KAAS dostupné z internetu. V případě použití jiného prostředí je potřeba si adresu ručně opravit.

9. Přímá autentizační webová služba verze v3_4

Tato webová služba provádí ověření uživatele pomocí jednorázových přihlašovacích údajů, které uživateli vygeneroval KAAS Czech POINT na základě provedeného přihlášení uživatele do JIP/KAAS (pomocí skutečných přihlašovacích údajů do JIP, nebo prostřednictvím NIA).

Tato přímá autentizační webová služba neslouží k ověřování skutečných přihlašovacích údajů, které jsou uloženy v JIP. Pokus o ověření skutečných přihlašovacích údajů touto přímou autentizační webovou službou skončí neúspěšně.

Detailní popis správného používání této přímé autentizační webové služby je popsán v kapitole 2.2.

9.1. Rozhraní pro vygenerování jednorázových přihlašovacích údajů

AIS musí uživateli poskytnout odkaz na webovou stránku KAAS pro vygenerování jednorázových přihlašovacích údajů. Může se jednat např. o webový odkaz umístěný na přihlašovací stránce AIS. Je doporučeno otevírat příslušnou stránku v novém okně (panelu) prohlížeče (v elementu <a> použijte atribut target="_blank").

Adresa webové stránky KAAS pro vygenerování jednorázových přihlašovacích údajů je následující:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/login?atsId=exampleId&**providerType=directAuth**
provozní	https://kaas.czechpoint.cz/as/login?atsId=exampleId&**providerType=directAuth**

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

V parametru „atsId" musí být předán identifikátor AIS. V adrese musí být povinně uveden parametr „providerType=directAuth".

9.2. Rozhraní pro odhlášení uživatele

V okamžiku, kdy se uživatel odhlašuje z AIS, by jej AIS měl z bezpečnostních důvodů přesměrovat do JIP/KAAS, kde rovněž dojde k odhlášení uživatele. Pokud se uživatel přihlásil do KAAS/JIP prostřednictvím NIA, JIP/KAAS provede rovněž přesěrování uživatele do NIA, kde dojde k odhlášení uživatele z NIA.

V okamžiku, kdy uživatel klikne na stránkách AIS na odkaz/tlačítko pro odhlášení, by AIS měl uživatele přesměrovat na následující adresu JIP/KAAS:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*
provozní	https://www.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

V parametru „atsId" se předává identifikátor AIS podobně jako v rozhraní přihlašovací stránky (viz výše).

V parametru „uri" se předává návratová adresa AIS, na kterou má JIP/KAAS uživatele přesměrovat po dokončení jeho odhlášení v JIP/KAAS a případně také v NIA. Předaná návratová adresa se ověřuje vůči „URL pro odhlášení", které je uloženo v konfiguraci AIS. „URL pro odhlášení" v konfiguraci se musí shodovat s počátkem návratové adresy v parametru „uri". Např. je-li v konfiguraci AIS uloženo „https://www.domena.cz/logout/", pak v parametru „uri" mohou být do JIP/KAAS předány návratové adresy „https://www.domena.cz/logout/?origin=jipkaas" nebo „https://www.domena.cz/logout/user/jnovak/" apod.

9.3. Způsob komunikace s webovou službou

Mezi autentizační webovou službou KAAS a AIS probíhá komunikace typu „request-response". Komunikace probíhá pomocí protokolu HTTPS, pro přenos zpráv se používá formát SOAP 1.1. Při volání webové služby je zapotřebí správně definovat a vyplňovat atribut „soapAction" v souladu s přiloženým odpovídajícím WSDL souborem.

Komunikace je zabezpečena pomocí šifrování. Používá se protokol TLS 1.2. Starší verze protokolu (SSL, TLS 1.0, TLS 1.1) jsou zakázány.

Ověření AIS je zajištěno pomocí autentizace certifikátem, který vydala komerční certifikační autorita provozovaná českým kvalifikovaným poskytovatelem služeb vytvářejících důvěru (I.CA, PostSignum, eIdentity nebo Národní certifikační autorita). Zejména v případě I.CA musí vydaný certifikát obsahovat v rozšíření certifikátu „extendedKeyUsage" atribut „Client Authentication" (id-kp-clientAuth, OID 1.3.6.1.5.5.7.3.2). Tento autentizační certifikát musí být zaregistrován v nastavení AIS, což se provede pomocí administrační aplikace Správa dat (https://www.czechpoint.cz/spravadat/).

Komunikaci iniciuje AIS, který zasílá na WS KAAS „request". WS KAAS poté vrací „response". AIS zasílá „request" na endpoint:

Prostředí KAAS	Adresa
testovací	https://cert.test.czechpoint.cz/asws/directAuthUserEndpoint
provozní	https://kaas-crt.czechpoint.cz/asws/directAuthUserEndpoint

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

9.4. Metoda directAuthUser – ověření jednorázových přihlašovacích údajů

9.4.1. Příklad komunikace WS

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
   <soapenv:Body>
      <m:directAuthUserRequest xmlns:m="http://agw-as.cz/ats-ws/atsUser/v3_4">
         <m:username>k3qrto7u</m:username>
         <m:password>No.df5sc+6zrv</m:password>
      </m:directAuthUserRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Response

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
   <soapenv:Header/>
   <soapenv:Body>
    <kaas:directAuthUserResponse xmlns:kaas="http://agw-as.cz/ats-ws/atsUser/v3_4">
      <kaas:status>OK</kaas:status>
      <kaas:description>Autentizace proběhla úspěšně.</kaas:description>
      <kaas:userRequestIp>90.181.150.14</kaas:userRequestIp>
      <kaas:attributes>
```

```
        <kaas:Username>jnovak</kaas:Username>
        <kaas:UzivatelId>7rsuG2KxZUIEku67LhtisQ==</kaas:UzivatelId>
        <kaas:ZkratkaSubjektu>JstrbLhota</kaas:ZkratkaSubjektu>
        <kaas:IcSubjektu>00235415</kaas:IcSubjektu>
        <kaas:Jmeno>Jan</kaas:Jmeno>
        <kaas:Prijmeni>Novák</kaas:Prijmeni>
        <kaas:TitulPred>Ing.</kaas:TitulPred>
        <kaas:TitulZa>CSc</kaas:TitulZa>
        <kaas:PristupoveRole>
          <kaas:role>Szr</kaas:role>
        </kaas:PristupoveRole>
        <kaas:CinnostniRole>
          <kaas:Agenda>
            <kaas:KodAgendy>A100</kaas:KodAgendy>
            <kaas:KodCinnostniRole>ACR01</kaas:KodCinnostniRole>
          </kaas:Agenda>
        </kaas:CinnostniRole>
        <kaas:Email>jnovak@jestrabi-lhota.cz</kaas:Email>
        <kaas:NazevSubjektu>Městský úřad Jestřábí Lhota</kaas:NazevSubjektu>
        <kaas:EmailSubjektu>test@email.cz</kaas:EmailSubjektu>
        <kaas:TypInstituce>9</kaas:TypInstituce>
        <kaas:OvmPrimarni>FALSE</kaas:OvmPrimarni>
        <kaas:TypPrihlaseni>p-cert</kaas:TypPrihlaseni>
        <kaas:OsobaZtotoznena>false</kaas:OsobaZtotoznena>
        <kaas:TokenAifo/>
        <kaas:Pracoviste>
          <kaas:Id>DislPracPrah</kaas:Id>
          <kaas:Nazev>Dislokované pracoviště Praha</kaas:Nazev>
          <kaas:Adresa>Na Žertvách 132/24, Libeň - Praha 8, 18000 Praha</kaas:Adresa>
        </kaas:Pracoviste>
        <kaas:IdentifikatorOvm>12345678</kaas:IdentifikatorOvm>
        <kaas:TimeLimitedId>T00-b899e113cbfa47c08f8fb7fdaa571f4f</kaas:TimeLimitedId>
      </kaas:attributes>
    </kaas:directAuthUserResponse>
  </soapenv:Body>
</soapenv:Envelope>
```


9.4.2. Vysvětlivky

Atributy v requestu:

Atribut	Význam
username	Jednorázové uživatelské jméno.
password	Jednorázové heslo.

Poznámka: Jednorázové přihlašovací údaje mají omezenou platnost 30 minut od okamžiku jejich vygenerování a jsou automaticky zneplatněny po jejich úspěšném ověření přímou autentizační webovou službou.

Atributy v response:

Atribut	Význam
status	Strukturovaná informace o výsledku zpracování žádosti.
description	Textový komentář s výsledkem operace. V případě chyby je zde uvedena podrobnější chybová hláška.
userRequestIp	IP uživatele při přihlášení. Může být IPv6/IPv4. Pokud uživatel přistupuje přes proxy, bere se IP proxy, která je nejdále od uživatele.
attributes	Informace o autentizovaném uživateli. Viz kapitola 9.4.4.

9.4.3. Popis stavů výsledku zpracování

Ve zprávách typu „response" se v elementu „status" vrací informace s výsledkem ověření autentizačních údajů:

Hodnota	Význam
OK	Ověření účtu proběhlo úspěšně. Účet se zadanými přihlašovacími údaji v JIP existuje.
SYSTEM_ERROR	Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.
VERIFICATION_FAILED	Ověření účtu nebylo úspěšné. Byly zadány nesprávné přihlašovací údaje.

9.4.4. Seznam atributů předávaných do AIS

Atribut	Popis
ZkratkaSubjektu	Zkratka subjektu dotazujícího se nebo žádajícího uživatele. Jedinečný identifikátor subjektu v rámci JIP.
IcSubjektu	IČ subjektu dotazujícího se nebo žádajícího uživatele.
UzivatelId	Jedinečný identifikátor uživatele v rámci JIP.
Username	Uživatelské jméno uživatele v JIP.
Jmeno	Jméno uživatele
Prijmení	Příjmení uživatele
TitulPred	Titul před jménem
TitulZa	Titul za jménem
PristupoveRole	Seznam přístupových (aplikačních) rolí do AIS, které jsou přiřazeny uživateli.
role	Označení konkrétní přístupové (aplikační) role, přiřazené uživateli.
CinnostniRole	Seznam činnostních rolí, které jsou přiřazeny uživateli. V response se vrací jen v případě, že AIS je zaregistrován do základních registrů.
KodAgendy	Kód agendy, k níž je daná činnostní role přiřazena.
KodCinnostniRole	Kód činnostní role, přiřazené uživateli.
Email	E-mailová adresa uživatele.
NazevSubjektu	Název subjektu dotazujícího se nebo žádajícího uživatele.
EmailSubjektu	E-mailová adresa subjektu.
TypInstituce	Typ instituce. Číselník viz kap. 12.1.
OvmPrimarni	Hodnota „true" nebo „false" označující hlavní subjekt pro subjekty s duplicitním IČ.
TypPrihlaseni	Způsob přihlášení uživatele do KAAS. Číselník viz kap. 12.2.
OsobaZtotoznena	Indikátor, zda byla daná osoba ztotožněna vůči ROB. Může nabývat hodnot „true" nebo „false".
TokenAifo	Datová struktura v kódování Base64 pro získání AIFO osoby. Aktuálně není implementováno z důvodu chybějící webové služby základních registrů!
Pracoviste	Údaje o pracovišti, ve kterém uživatel vykonává svoji práci.
Id	Alfanumerický identifikátor pracoviště
Nazev	Název pracoviště
Adresa	Adresa pracoviště
KodAdresy	Kód adresy pracoviště ve formě kódu adresního místa z RUIAN.

Atribut	Popis
IdentifikatorOvm	Identifikátor OVM, uvedený v Rejstříku OVM.
TimeLimitedId	Speciální autorizační token, který se používá pro přístup k vybraným webovým službám. Vrací se jen v případě, že daný autentizovaný uživatel je lokálním administrátorem. Token má omezenou platnost – další informace jsou uvedeny v dokumentaci k příslušným webovým službám.

Poznámka: Typy atributů a definovaná omezení hodnot atributů jsou uvedena ve WSDL souboru – viz kapitola 9.5.

9.5. Seznam souborů

Detailní technická specifikace je uložena v těchto souborech:

Soubor	Popis
DirectAuth_v3_4.wsdl	Definice přímé autentizační webové služby KAAS ve verzi v3_4.

Poznámka: Ve WSDL souboru je uvedena adresa endpointu pro ostré provozní prostředí KAAS dostupné z internetu. V případě použití jiného prostředí je potřeba si adresu ručně opravit.

10. Přímá autentizační webová služba verze v4_1

Tato webová služba provádí ověření uživatele pomocí jednorázových přihlašovacích údajů, které uživateli vygeneroval KAAS Czech POINT na základě provedeného přihlášení uživatele do JIP/KAAS (pomocí skutečných přihlašovacích údajů do JIP, nebo prostřednictvím NIA).

Tato přímá autentizační webová služba neslouží k ověřování skutečných přihlašovacích údajů, které jsou uloženy v JIP. Pokus o ověření skutečných přihlašovacích údajů touto přímou autentizační webovou službou skončí neúspěšně.

Detailní popis správného používání této přímé autentizační webové služby je popsán v kapitole 2.2.

Předávané informace o uživateli jsou v souladu s § 56a odst. 5 zákona č. 111/2009 Sb., o základních registrech.

10.1. Rozhraní pro vygenerování jednorázových přihlašovacích údajů

AIS musí uživateli poskytnout odkaz na webovou stránku KAAS pro vygenerování jednorázových přihlašovacích údajů. Může se jednat např. o webový odkaz umístěný na přihlašovací stránce AIS. Je doporučeno otevírat příslušnou stránku v novém okně (panelu) prohlížeče (v elementu <a> použijte atribut target="_blank").

Adresa webové stránky KAAS pro vygenerování jednorázových přihlašovacích údajů je následující:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/login?atsId=exampleId&**providerType=directAuth**
provozní	https://kaas.czechpoint.cz/as/login?atsId=exampleId&**providerType=directAuth**

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

V parametru „atsId" musí být předán identifikátor AIS. V adrese musí být povinně uveden parametr „providerType=directAuth".

10.2. Rozhraní pro odhlášení uživatele

V okamžiku, kdy se uživatel odhlašuje z AIS, by jej AIS měl z bezpečnostních důvodů přesměrovat do JIP/KAAS, kde rovněž dojde k odhlášení uživatele. Pokud se uživatel přihlásil do KAAS/JIP prostřednictvím NIA, JIP/KAAS provede rovněž přesěrování uživatele do NIA, kde dojde k odhlášení uživatele z NIA.

V okamžiku, kdy uživatel klikne na stránkách AIS na odkaz/tlačítko pro odhlášení, by AIS měl uživatele přesměrovat na následující adresu JIP/KAAS:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*
provozní	https://www.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

V parametru „atsId" se předává identifikátor AIS podobně jako v rozhraní přihlašovací stránky (viz výše).

V parametru „uri" se předává návratová adresa AIS, na kterou má JIP/KAAS uživatele přesměrovat po dokončení jeho odhlášení v JIP/KAAS a případně také v NIA. Předaná návratová adresa se ověřuje vůči „URL pro odhlášení", které je uloženo v konfiguraci AIS. „URL pro odhlášení" v konfiguraci se musí shodovat s počátkem návratové adresy v parametru „uri". Např. je-li v konfiguraci AIS uloženo „https://www.domena.cz/logout/", pak v parametru „uri" mohou být do JIP/KAAS předány návratové adresy „https://www.domena.cz/logout/?origin=jipkaas" nebo „https://www.domena.cz/logout/user/jnovak/" apod.

10.3. Způsob komunikace s webovou službou

Mezi autentizační webovou službou KAAS a AIS probíhá komunikace typu „request-response". Komunikace probíhá pomocí protokolu HTTPS, pro přenos zpráv se používá formát SOAP 1.1. Při volání webové služby je zapotřebí správně definovat a vyplňovat atribut „soapAction" v souladu s přiloženým odpovídajícím WSDL souborem.

Komunikace je zabezpečena pomocí šifrování. Používá se protokol TLS 1.2. Starší verze protokolu (SSL, TLS 1.0, TLS 1.1) jsou zakázány.

Ověření AIS je zajištěno pomocí autentizace certifikátem, který vydala komerční certifikační autorita provozovaná českým kvalifikovaným poskytovatelem služeb vytvářejících důvěru (I.CA, PostSignum, eIdentity nebo Národní certifikační autorita). Zejména v případě I.CA musí vydaný certifikát obsahovat v rozšíření certifikátu „extendedKeyUsage" atribut „Client Authentication" (id-kp-clientAuth, OID 1.3.6.1.5.5.7.3.2). Tento autentizační certifikát musí být zaregistrován v nastavení AIS, což se provede pomocí administrační aplikace Správa dat (https://www.czechpoint.cz/spravadat/).

Komunikaci iniciuje AIS, který zasílá na WS KAAS „request". WS KAAS poté vrací „response". AIS zasílá „request" na endpoint:

Prostředí KAAS	Adresa
testovací	https://cert.test.czechpoint.cz/asws/directAuthUserEndpoint
provozní	https://kaas-crt.czechpoint.cz/asws/directAuthUserEndpoint

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

10.4. Metoda directAuthUser – ověření jednorázových přihlašovacích údajů

10.4.1. Příklad komunikace WS

Request	<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <soapenv:Body> <m:directAuthUserRequest xmlns:m="http://agw-as.cz/ats-ws/atsUser/v4_1"> <m:username>k3qrto7u</m:username> <m:password>No.df5sc+6zrv</m:password> </m:directAuthUserRequest> </soapenv:Body> </soapenv:Envelope>
Response	<?xml version="1.0" encoding="UTF-8"?> <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Header/> <soapenv:Body> <kaas:directAuthUserResponse xmlns:kaas="http://agw-as.cz/ats-ws/atsUser/v4_1"> <kaas:status>OK</kaas:status>

```
        <kaas:description>Autentizace proběhla úspěšně.</kaas:description>
        <kaas:userRequestIp>90.181.150.14</kaas:userRequestIp>
        <kaas:attributes>
          <kaas:Username>jnovak</kaas:Username>
          <kaas:UzivatelId>7rsuG2KxZUIEku67LhtisQ==</kaas:UzivatelId>
          <kaas:ZkratkaSubjektu>JstrbLhota</kaas:ZkratkaSubjektu>
          <kaas:IcSubjektu>00235415</kaas:IcSubjektu>
          <kaas:Jmeno>Jan</kaas:Jmeno>
          <kaas:Prijmeni>Novák</kaas:Prijmeni>
          <kaas:TitulPred>Ing.</kaas:TitulPred>
          <kaas:TitulZa>CSc</kaas:TitulZa>
          <kaas:PristupoveRole>
            <kaas:role>Szr</kaas:role>
          </kaas:PristupoveRole>
          <kaas:CinnostniRole>
            <kaas:Agenda>
              <kaas:KodAgendy>A100</kaas:KodAgendy>
              <kaas:KodCinnostniRole>ACR01</kaas:KodCinnostniRole>
            </kaas:Agenda>
          </kaas:CinnostniRole>
          <kaas:Email>jnovak@jestrabi-lhota.cz</kaas:Email>
          <kaas:NazevSubjektu>Městský úřad Jestřábí Lhota</kaas:NazevSubjektu>
          <kaas:EmailSubjektu>test@email.cz</kaas:EmailSubjektu>
          <kaas:TypInstituce>9</kaas:TypInstituce>
          <kaas:OvmPrimarni>FALSE</kaas:OvmPrimarni>
          <kaas:TypPrihlaseni>p-cert</kaas:TypPrihlaseni>
          <kaas:OsobaZtotoznena>false</kaas:OsobaZtotoznena>
          <kaas:TokenAifo/>
            <kaas:Pracoviste>
              <kaas:Id>DislPracPrah</kaas:Id>
              <kaas:Nazev>Dislokované pracoviště Praha</kaas:Nazev>
              <kaas:Adresa>Na Žertvách 132/24, Libeň - Praha 8, 18000 Praha</kaas:Adresa>
              <kaas:KodAdresy>22376097</kaas:KodAdresy>
            </kaas:Pracoviste>
            <kaas:MistoNarozeni stav="nespravny">
              <kaas:MistoNarozeniCr mop="false"
nazev="Arnoltice">562343</kaas:MistoNarozeniCr>
              <kaas:MistoNarozeniSvet>
                <kaas:stat nazev="Ukrajina">804</kaas:stat>
                <kaas:misto>KYJEV</kaas:misto>
              </kaas:MistoNarozeniSvet>
            </kaas:MistoNarozeni>
            <kaas:DatumNarozeni stav="spravny">1978-04-02</kaas:DatumNarozeni>
            <kaas:DatumUmrti/>
            <kaas:Doklady>
              <kaas:Doklad stav="spravny" typ="P">11111908</kaas:Doklad>
              <kaas:Doklad stav="spravny" typ="ID">111111908</kaas:Doklad>
            </kaas:Doklady>
            <kaas:NeevidovatOsobniUdaje>false</kaas:NeevidovatOsobniUdaje>
            <kaas:IdentifikatorOvm>12345678</kaas:IdentifikatorOvm>
            <kaas:TimeLimitedId>T00-b899e113cbfa47c08f8fb7fdaa571f4f</kaas:TimeLimitedId>
        </kaas:attributes>
      </kaas:directAuthUserResponse>
    </soapenv:Body>
</soapenv:Envelope>
```


10.4.2. Vysvětlivky

Atributy v requestu:

Atribut	Význam
username	Jednorázové uživatelské jméno.
password	Jednorázové heslo.

Poznámka: Jednorázové přihlašovací údaje mají omezenou platnost 30 minut od okamžiku jejich vygenerování a jsou automaticky zneplatněny po jejich úspěšném ověření přímou autentizační webovou službou.

Atributy v response:

Atribut	Význam
status	Strukturovaná informace o výsledku zpracování žádosti.
description	Textový komentář s výsledkem operace. V případě chyby je zde uvedena podrobnější chybová hláška.
userRequestIp	IP uživatele při přihlášení. Může být IPv6/IPv4. Pokud uživatel přistupuje přes proxy, bere se IP proxy, která je nejdále od uživatele.
attributes	Informace o autentizovaném uživateli. Viz kapitola 10.4.4.

10.4.3. Popis stavů výsledku zpracování

Ve zprávách typu „response" se v elementu „status" vrací informace s výsledkem ověření autentizačních údajů:

Hodnota	Význam
OK	Ověření účtu proběhlo úspěšně. Účet se zadanými přihlašovacími údaji v JIP existuje.
SYSTEM_ERROR	Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.
VERIFICATION_FAILED	Ověření účtu nebylo úspěšné. Byly zadány nesprávné přihlašovací údaje.

10.4.4. Seznam atributů předávaných do AIS

Atribut	Popis
ZkratkaSubjektu	Zkratka subjektu dotazujícího se nebo žádajícího uživatele. Jedinečný identifikátor subjektu v rámci JIP.
IcSubjektu	IČ subjektu dotazujícího se nebo žádajícího uživatele.
UzivatelId	Jedinečný identifikátor uživatele v rámci JIP.
Username	Uživatelské jméno uživatele v JIP.
Jmeno	Jméno uživatele
Prijmení	Příjmení uživatele
TitulPred	Titul před jménem
TitulZa	Titul za jménem
PristupoveRole	Seznam přístupových (aplikačních) rolí do AIS, které jsou přiřazeny uživateli.
role	Označení konkrétní přístupové (aplikační) role, přiřazené uživateli.
CinnostniRole	Seznam činnostních rolí, které jsou přiřazeny uživateli. V response se vrací jen v případě, že AIS je zaregistrován do základních registrů.
KodAgendy	Kód agendy, k níž je daná činnostní role přiřazena.
KodCinnostniRole	Kód činnostní role, přiřazené uživateli.
Email	E-mailová adresa uživatele.
NazevSubjektu	Název subjektu dotazujícího se nebo žádajícího uživatele.
EmailSubjektu	E-mailová adresa subjektu.

Atribut	Popis
TypInstituce	Typ instituce. Číselník viz kap. 12.1.
OvmPrimarni	Hodnota „true" nebo „false" označující hlavní subjekt pro subjekty s duplicitním IČ.
TypPrihlaseni	Způsob přihlášení uživatele do KAAS. Číselník viz kap. 12.2.
OsobaZtotoznena	Indikátor, zda byla daná osoba ztotožněna vůči ROB. Může nabývat hodnot „true" nebo „false".
TokenAifo	Datová struktura v kódování Base64 pro získání AIFO osoby. Aktuálně není implementováno z důvodu chybějící webové služby základních registrů!
Pracoviste	Údaje o pracovišti, ve kterém uživatel vykonává svoji práci.
Id	Alfanumerický identifikátor pracoviště
Nazev	Název pracoviště
Adresa	Adresa pracoviště
KodAdresy	Kód adresy pracoviště ve formě kódu adresního místa z RUIAN.
Mistonarozeni	Údaje o místě narození uživatele.
MistoNarozeniCr	Údaj o místě narození v ČR – kód z RUIAN. Atributy v elementu mají následující význam: • „mop" – atribut s příznakem, zda se jedná o kód městského obvodu • „nazev" – atribut s názvem místa narození v ČR
MistoNarozeniSvet	Údaje o místě narození v zahraničí
stat	Kód státu. Číselník států viz webové stránky Správy základních registrů. Atribut „nazev" obsahuje textový název státu.
misto	Název místa narození v zahraničí.
DatumNarozeni	Datum narození.
DatumUmrti	Datum úmrtí.
Doklady	Seznam elektronicky čitelných dokladů.
Doklad	Číslo dokladu. Atributy v elementu mají následující význam: • typ – atribut uvádějící typ dokladu. Číselník typů dokladů viz webové stránky Správy základních registrů.
NeevidovatOsobniUdaje	Příznak, zda je pro daný uživatelský účet zakázáno evidování osobních údajů.
IdentifikatorOvm	Identifikátor OVM, uvedený v Rejstříku OVM.
TimeLimitedId	Speciální autorizační token, který se používá pro přístup k vybraným webovým službám. Vrací se jen v případě, že daný autentizovaný uživatel je lokálním administrátorem. Token má omezenou platnost – další informace jsou uvedeny v dokumentaci k příslušným webovým službám.

Poznámka: Některé elementy obsahují atribut „stav", který nabývá hodnot „spravny" nebo „nespravny". Tento atribut udává, zda je daný údaj v registru obyvatel označený jako nesprávný.

Poznámka: Typy atributů a definovaná omezení hodnot atributů jsou uvedena ve WSDL souboru – viz kapitola 10.5.

10.5. Seznam souborů

Detailní technická specifikace je uložena v těchto souborech:

Soubor	Popis
DirectAuth_v4_1.wsdl	Definice přímé autentizační webové služby KAAS ve verzi v4_1.

Poznámka: Ve WSDL souboru je uvedena adresa endpointu pro ostré provozní prostředí KAAS dostupné z internetu. V případě použití jiného prostředí je potřeba si adresu ručně opravit.

11. Přímá autentizační webová služba verze v4_2

Tato webová služba provádí ověření uživatele pomocí jednorázových přihlašovacích údajů, které uživateli vygeneroval KAAS Czech POINT na základě provedeného přihlášení uživatele do JIP/KAAS (pomocí skutečných přihlašovacích údajů do JIP, nebo prostřednictvím NIA).

Tato přímá autentizační webová služba neslouží k ověřování skutečných přihlašovacích údajů, které jsou uloženy v JIP. Pokus o ověření skutečných přihlašovacích údajů touto přímou autentizační webovou službou skončí neúspěšně.

Detailní popis správného používání této přímé autentizační webové služby je popsán v kapitole 2.2.

Předávané informace o uživateli jsou v souladu s § 56a odst. 5 zákona č. 111/2009 Sb., o základních registrech.

11.1. Rozhraní pro vygenerování jednorázových přihlašovacích údajů

AIS musí uživateli poskytnout odkaz na webovou stránku KAAS pro vygenerování jednorázových přihlašovacích údajů. Může se jednat např. o webový odkaz umístěný na přihlašovací stránce AIS. Je doporučeno otevírat příslušnou stránku v novém okně (panelu) prohlížeče (v elementu <a> použijte atribut target="_blank").

Adresa webové stránky KAAS pro vygenerování jednorázových přihlašovacích údajů je následující:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/login?atsId=exampleId&**providerType=directAuth**
provozní	https://kaas.czechpoint.cz/as/login?atsId=exampleId&**providerType=directAuth**

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

V parametru „atsId" musí být předán identifikátor AIS. V adrese musí být povinně uveden parametr „providerType=directAuth".

11.2. Rozhraní pro odhlášení uživatele

V okamžiku, kdy se uživatel odhlašuje z AIS, by jej AIS měl z bezpečnostních důvodů přesměrovat do JIP/KAAS, kde rovněž dojde k odhlášení uživatele. Pokud se uživatel přihlásil do KAAS/JIP prostřednictvím NIA, JIP/KAAS provede rovněž přesěrování uživatele do NIA, kde dojde k odhlášení uživatele z NIA.

V okamžiku, kdy uživatel klikne na stránkách AIS na odkaz/tlačítko pro odhlášení, by AIS měl uživatele přesměrovat na následující adresu JIP/KAAS:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*
provozní	https://www.czechpoint.cz/as/processLogout?atsId=*exampleId*&uri=*adresa*

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

V parametru „atsId" se předává identifikátor AIS podobně jako v rozhraní přihlašovací stránky (viz výše).

V parametru „uri" se předává návratová adresa AIS, na kterou má JIP/KAAS uživatele přesměrovat po dokončení jeho odhlášení v JIP/KAAS a případně také v NIA. Předaná návratová adresa se ověřuje vůči „URL pro odhlášení", které je uloženo v konfiguraci AIS. „URL pro odhlášení" v konfiguraci se musí shodovat s počátkem návratové adresy v parametru „uri". Např. je-li v konfiguraci AIS uloženo „https://www.domena.cz/logout/", pak v parametru „uri" mohou být do JIP/KAAS předány návratové adresy „https://www.domena.cz/logout/?origin=jipkaas" nebo „https://www.domena.cz/logout/user/jnovak/" apod.

11.3. Způsob komunikace s webovou službou

Mezi autentizační webovou službou KAAS a AIS probíhá komunikace typu „request-response". Komunikace probíhá pomocí protokolu HTTPS, pro přenos zpráv se používá formát SOAP 1.1. Při volání webové služby je zapotřebí správně definovat a vyplňovat atribut „soapAction" v souladu s přiloženým odpovídajícím WSDL souborem.

Komunikace je zabezpečena pomocí šifrování. Používá se protokol TLS 1.2. Starší verze protokolu (SSL, TLS 1.0, TLS 1.1) jsou zakázány.

Ověření AIS je zajištěno pomocí autentizace certifikátem, který vydala komerční certifikační autorita provozovaná českým kvalifikovaným poskytovatelem služeb vytvářejících důvěru (I.CA, PostSignum, eIdentity nebo Národní certifikační autorita). Zejména v případě I.CA musí vydaný certifikát obsahovat v rozšíření certifikátu „extendedKeyUsage" atribut „Client Authentication" (id-kp-clientAuth, OID 1.3.6.1.5.5.7.3.2). Tento autentizační certifikát musí být zaregistrován v nastavení AIS, což se provede pomocí administrační aplikace Správa dat (https://www.czechpoint.cz/spravadat/).

Komunikaci iniciuje AIS, který zasílá na WS KAAS „request". WS KAAS poté vrací „response". AIS zasílá „request" na endpoint:

Prostředí KAAS	Adresa
testovací	https://cert.test.czechpoint.cz/asws/directAuthUserEndpoint
provozní	https://kaas-crt.czechpoint.cz/asws/directAuthUserEndpoint

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

11.4. Metoda directAuthUser – ověření jednorázových přihlašovacích údajů

11.4.1. Příklad komunikace WS

Request	<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <soapenv:Body> <m:directAuthUserRequest xmlns:m="http://agw-as.cz/ats-ws/atsUser/v4_2"> <m:username>k3qrto7u</m:username> <m:password>No.df5sc+6zrv</m:password> </m:directAuthUserRequest> </soapenv:Body> </soapenv:Envelope>
Response	<?xml version="1.0" encoding="UTF-8"?> <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Header/> <soapenv:Body> <kaas:directAuthUserResponse xmlns:kaas="http://agw-as.cz/ats-ws/atsUser/v4_2"> <kaas:status>OK</kaas:status>

```
      <kaas:description>Autentizace proběhla úspěšně.</kaas:description>
      <kaas:userRequestIp>90.181.150.14</kaas:userRequestIp>
      <kaas:attributes>
        <kaas:Username>jnovak</kaas:Username>
        <kaas:UzivatelId>7rsuG2KxZUIEku67LhtisQ==</kaas:UzivatelId>
        <kaas:ZkratkaSubjektu>spuu_00836265.9999</kaas:ZkratkaSubjektu>
        <kaas:IcSubjektu>836265</kaas:IcSubjektu>
        <kaas:Jmeno>Jan</kaas:Jmeno>
        <kaas:Prijmeni>Novák</kaas:Prijmeni>
        <kaas:TitulPred>Ing.</kaas:TitulPred>
        <kaas:TitulZa>CSc</kaas:TitulZa>
        <kaas:PristupoveRole>
          <kaas:role>Szr</kaas:role>
        </kaas:PristupoveRole>
        <kaas:CinnostniRole>
          <kaas:Agenda>
            <kaas:KodAgendy>A100</kaas:KodAgendy>
            <kaas:KodCinnostniRole>ACR01</kaas:KodCinnostniRole>
          </kaas:Agenda>
        </kaas:CinnostniRole>
        <kaas:Email>jnovak@email.cz</kaas:Email>
        <kaas:NazevSubjektu>BULGER a ASSOCIATES</kaas:NazevSubjektu>
        <kaas:EmailSubjektu>test@email.cz</kaas:EmailSubjektu>
        <kaas:TypInstituce>101</kaas:TypInstituce>
        <kaas:OvmPrimarni>FALSE</kaas:OvmPrimarni>
        <kaas:TypPrihlaseni>p-cert</kaas:TypPrihlaseni>
        <kaas:TypPrihlaseniNia/>
        <kaas:OsobaZtotoznena>false</kaas:OsobaZtotoznena>
        <kaas:TokenAifo/>
          <kaas:Pracoviste>
             <kaas:Id>spuu_00836265.9999</kaas:Id>
             <kaas:Nazev>BULGER a ASSOCIATES</kaas:Nazev>
             <kaas:Adresa>Novákových 456/8, Libeň - Praha 8, 18000 Praha</kaas:Adresa>
             <kaas:KodAdresy>22378235</kaas:KodAdresy>
          </kaas:Pracoviste>
          <kaas:MistoNarozeni/>
          <kaas:Doklady>
             <kaas:Doklad stav="spravny" typ="P">11111908</kaas:Doklad>
             <kaas:Doklad stav="spravny" typ="ID">111111908</kaas:Doklad>
          </kaas:Doklady>
          <kaas:NeevidovatOsobniUdaje>false</kaas:NeevidovatOsobniUdaje>
          <kaas:IdentifikatorSpuu>00836265.9999</kaas:IdentifikatorSpuu>
          <kaas:TimeLimitedId>T00-b899e113cbfa47c08f8fb7fdaa571f4f</kaas:TimeLimitedId>
      </kaas:attributes>
    </kaas:directAuthUserResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

11.4.2. Vysvětlivky

Atributy v requestu:

Atribut	Význam
username	Jednorázové uživatelské jméno.
password	Jednorázové heslo.

Poznámka: Jednorázové přihlašovací údaje mají omezenou platnost 30 minut od okamžiku jejich vygenerování a jsou automaticky zneplatněny po jejich úspěšném ověření přímou autentizační webovou službou.

Atributy v response:

Atribut	Význam
status	Strukturovaná informace o výsledku zpracování žádosti.
description	Textový komentář s výsledkem operace. V případě chyby je zde uvedena podrobnější chybová hláška.
userRequestIp	IP uživatele při přihlášení. Může být IPv6/IPv4. Pokud uživatel

Atribut	Význam
	přistupuje přes proxy, bere se IP proxy, která je nejdále od uživatele.
attributes	Informace o autentizovaném uživateli. Viz kapitola 10.4.4.

11.4.3. Popis stavů výsledku zpracování

Ve zprávách typu „response" se v elementu „status" vrací informace s výsledkem ověření autentizačních údajů:

Hodnota	Význam
OK	Ověření účtu proběhlo úspěšně. Účet se zadanými přihlašovacími údaji v JIP existuje.
SYSTEM_ERROR	Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.
VERIFICATION_FAILED	Ověření účtu nebylo úspěšné. Byly zadány nesprávné přihlašovací údaje.

11.4.4. Seznam atributů předávaných do AIS

Atribut	Popis
ZkratkaSubjektu	Zkratka subjektu dotazujícího se nebo žádajícího uživatele. Jedinečný identifikátor subjektu v rámci JIP.
IcSubjektu	IČ subjektu dotazujícího se nebo žádajícího uživatele.
UzivatelId	Jedinečný identifikátor uživatele v rámci JIP.
Username	Uživatelské jméno uživatele v JIP.
Jmeno	Jméno uživatele
Prijmení	Příjmení uživatele
TitulPred	Titul před jménem
TitulZa	Titul za jménem
PristupoveRole	Seznam přístupových (aplikačních) rolí do AIS, které jsou přiřazeny uživateli.
role	Označení konkrétní přístupové (aplikační) role, přiřazené uživateli.
CinnostniRole	Seznam činnostních rolí, které jsou přiřazeny uživateli. V response se vrací jen v případě, že AIS je zaregistrován do základních registrů.
KodAgendy	Kód agendy, k níž je daná činnostní role přiřazena.
KodCinnostniRole	Kód činnostní role, přiřazené uživateli.
Email	E-mailová adresa uživatele.
NazevSubjektu	Název subjektu dotazujícího se nebo žádajícího uživatele.
EmailSubjektu	E-mailová adresa subjektu.
TypInstituce	Typ instituce. Číselník viz kap. 12.1.
OvmPrimarni	Hodnota „true" nebo „false" označující hlavní subjekt pro subjekty s duplicitním IČ.
TypPrihlaseni	Způsob přihlášení uživatele do KAAS. Číselník viz kap. 12.2.
TypPrihlaseniNia	Hodnota úrovně záruk použitého identifikačního prostředku, pokud se uživatel autentizoval prostřednictvím NIA.
OsobaZtotoznena	Indikátor, zda byla daná osoba ztotožněna vůči ROB. Může nabývat hodnot „true" nebo „false".

Atribut	Popis
TokenAifo	Datová struktura v kódování Base64 pro získání AIFO osoby. Aktuálně není implementováno z důvodu chybějící webové služby základních registrů!
Pracoviste	Údaje o pracovišti, ve kterém uživatel vykonává svoji práci.
Id	Alfanumerický identifikátor pracoviště
Nazev	Název pracoviště
Adresa	Adresa pracoviště
KodAdresy	Kód adresy pracoviště ve formě kódu adresního místa z RUIAN.
Mistonarozeni	Údaje o místě narození uživatele.
MistoNarozeniCr	Údaj o místě narození v ČR – kód z RUIAN. Atributy v elementu mají následující význam: • „mop" – atribut s příznakem, zda se jedná o kód městského obvodu • „nazev" – atribut s názvem místa narození v ČR
MistoNarozeniSvet	Údaje o místě narození v zahraničí
stat	Kód státu. Číselník států viz webové stránky Správy základních registrů. Atribut „nazev" obsahuje textový název státu.
misto	Název místa narození v zahraničí.
DatumNarozeni	Datum narození.
DatumUmrti	Datum úmrtí.
Doklady	Seznam elektronicky čitelných dokladů.
Doklad	Číslo dokladu. Atributy v elementu mají následující význam: • typ – atribut uvádějící typ dokladu. Číselník typů dokladů viz webové stránky Správy základních registrů.
NeevidovatOsobniUdaje	Příznak, zda je pro daný uživatelský účet zakázáno evidování osobních údajů.
IdentifikatorOvm	Identifikátor OVM, uvedený v Rejstříku OVM.
IdentifikatorSpuu	Identifikátor SPUÚ, uvedený v Rejstříku OVM.
TimeLimitedId	Speciální autorizační token, který se používá pro přístup k vybraným webovým službám. Vrací se jen v případě, že daný autentizovaný uživatel je lokálním administrátorem. Token má omezenou platnost – další informace jsou uvedeny v dokumentaci k příslušným webovým službám.

Poznámka: Některé elementy obsahují atribut „stav", který nabývá hodnot „spravny" nebo „nespravny". Tento atribut udává, zda je daný údaj v registru obyvatel označený jako nesprávný.

Poznámka: Typy atributů a definovaná omezení hodnot atributů jsou uvedena ve WSDL souboru – viz kapitola 11.5.

11.5. Seznam souborů

Detailní technická specifikace je uložena v těchto souborech:

Soubor	Popis
DirectAuth_v4_2.wsdl	Definice přímé autentizační webové služby KAAS ve verzi v4_2.

Poznámka: Ve WSDL souboru je uvedena adresa endpointu pro ostré provozní prostředí KAAS dostupné z internetu. V případě použití jiného prostředí je potřeba si adresu ručně opravit.

12. Číselníky

12.1. Typ instituce

Kód	Typ instituce
1	Česká pošta
2	Hospodářská komora
3	Krajský úřad
4	Ministerstvo
5	Obec I. Typu
6	Obec II. Typu
7	Obec III. Typu
8	Statutární města (Magistráty) a jejich obvody
9	Testovací
10	Notáři
11	Orgán státní správy
12	Školení
13	Exekutoři
15	Advokáti
16	Zřizované organizace
17	PO zřízená ze zákona
18	PO
19	PFO
20	FO
21	Stavební úřad
22	Orgán veřejné moci
23	Organizační složka státu
24	Daňoví poradci
25	Insolvenční správci

Poznámka: Aktuální číselník typů institucí získáte zavoláním editační webové služby KAAS (metoda GetListOfValues) – viz samostatný dokument s popisem editační webové služby.

12.2. Typ přihlášení

Kód	Typ instituce
p-pwd	Přihlášení jménem a heslem
p-cert	Přihlášení jménem, heslem a certifikátem
p-hotp	Přihlášení jménem, heslem a OTP kódem
p-nia	Přihlášení prostřednictvím NIA

13. 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 4.8

- kap. 4.4, 5.4, 6.4, 7.4, 8.2, 9.3, 10.3, 11.3 – na seznam podporovaných certifikačních autorit byla přidána Národní certifikační autorita

Verze 4.7

- kap. 4.1, 4.3, 4.4, 5.1, 5.3, 5.4, 6.1, 6.3, 6.4, 7.1, 7.3, 7.4, 8.1, 8.2, 9.1, 9.2, 9.3, 10.1, 10.2, 10.3, 11.1, 11.2, 11.3 – odstraněny adresy s doménou czechpoint.cms2.cz

Verze 4.6

- celý dokument – do popisů všech webových služeb přidána kapitola „Rozhraní pro odhlášení uživatele"

Verze 4.5

- celý dokument - menší úpravy textu v souvislosti s integrací JIP/KAAS jako Service Providera s NIA a s evidováním SPUÚ v JIP
- kap. 7 - přidána nová autentizační webová služba v4_2, která vrací úroveň záruk identifikačního prostředku, pokud ověření uživatele proběhlo v NIA, a identifikátor SPUÚ, pokud uživatel pochází z SPUÚ
- kap. 11 – přidána nová přímá autentizační webová služba v4_2, která vrací úroveň záruk identifikačního prostředku, pokud ověření uživatele proběhlo v NIA, a identifikátor SPUÚ, pokud uživatel pochází z SPUÚ

Verze 4.4

- kap. 4.3, 5.3, 6.3, 7.1, 8.2, 9.2 – protokoly TLS 1.0 a TLS 1.1 jsou zakázány

Verze 4.3

- titulní strana – odstraněno neaktuální červené upozornění o plánovaném ukončení přímé autentizační webové služby v1
- kap. 2.1 – v krocích (6+7) a (8) doplněny chybějící odkazy na další kapitoly
- kap. 2.2, 7 – doplněna poznámka o přímé autentizační webové službě v1
- kap. 5.5.4, 6.5.4, 8.3.4, 9.3.4 – opraven popis atributu „TokenAifo"

Verze 4.2

- kap. 4.1, 4.3, 5.1, 5.3, 6.1, 6.3, 7.1, 8.1, 8.2, 9.1, 9.2 – odstraněny již neplatné adresy pro prostředí CMS
- označení „KAAS/JIP" v dokumentu změněno za užívanější „JIP/KAAS"

Verze 4.1

- kap. 4.1, 5.1, 6.1, 8.1, 9.1 – přidány adresy prostředí KAAS dostupných z CMS 2
- kap. 4.3, 5.3, 6.3, 7.1, 8.2, 9.2 – místo protokolu TLSv1.0 je potřeba použít TLSv1.2, přidáno upozornění na nutnost správného nastavování atributu „soapAction" a poznámky k autentizačnímu certifikátu AIS, přidány adresy prostředí KAAS dostupných z CMS 2,
- kap. 5.5.4, 6.5.4, 8.3.4, 9.3.4 – upřesněn popis atributu „TokenAifo"

Verze 4.0

- kap. 5, 6 – popis autentizačních webových služeb v3_3 a v4 byl nahrazen popisem nových služeb v3_4 a v4_1, které v response vracejí navíc identifikátor OVM z ROVM a token „TimeLimitedID"
- kap. 8, 9 – popis přímých autentizačních webových služeb v3_3 a v4 byl nahrazen popisem nových služeb v3_4 a v4_1, které v response vracejí navíc identifikátor OVM z ROVM a token „TimeLimitedID"
- oprava špatně používaných termínů v dokumentu

Verze 3.9

- celý dokument - akreditovaný poskytovatel certifikačních služeb změněn na kvalifikovaného poskytovatele služeb vytvářejících důvěru
- kap. 1.2 – JIP/KAAS je autentizační informační systém podle zákona č. 111/2009 Sb.
- kap. 2.1, 2.2 – přidány poznámky o získání osobních údajů uživatele z ROB a jejich předání do AIS
- kap. 2.3 – nová kapitola o nakládání s osobními údaji uživatelů
- kap 6 – nová kapitola s popisem autentizační webové služby ve verzi v4
- kap 9 – nová kapitola s popisem přímé autentizační webové služby ve verzi v4

Verze 3.8

- kap. 2.1, 2.2 – aktualizovány obrázky a text podle dokumentu s procesním popisem autentizačních webových služeb

Verze 3.7

- zapracování interních připomínek k verzi 3.6

Verze 3.6

- kap. 1.3 – přidána zkratka RUIAN
- kap. 2 – kapitola rozdělena na popis postupu autentizace pomocí autentizační webové služby a pomocí přímé autentizační webové služby ve verzi v3_3
- odstraněna kapitola s popisem autentizační webové služby ve verzi v2
- kap. 5 – nová kapitola s popisem autentizační webové služby ve verzi v3_3

- kap. 7 – nová kapitola s popisem přímé autentizační webové služby ve verzi v3_3
- kap. 8 – nová kapitola s číselníky

Verze 3.5

- kap. 1.3 - přidána zkratka CMS
- kap. 4.1, 4.3, 5.1, 5.3, 6.1 - doplněno testovací a provozní prostředí KAAS dostupné z CMS
- kap. 4.5, 5.6, 6.3 - upravena poznámka pod tabulkou

Verze 3.4

- kap. 4.3, 5.3, 6.1 - doplněna informace, že protokol SSLv3 není podporován; nutné použít TLSv1

Verze 3.3

- úvodní stránka – odstraněn červený rámeček s datem, od kdy dokument vstupuje v platnost; dokument je aktuálně platný
- kap. 1.1 – odstraněn odstavec s informací o datu, od kdy dokument vstupuje v platnost; dokument je aktuálně platný
- kap. 1.3 – doplněna chybějící zkratka KAAS
- kap. 2 – korigován popis procesu; KAAS nekomunikuje s ISZR během autentizace uživatele
- kap. 4.3, 5.3 – AIS se vůči KAAS autentizuje pouze komerčním serverovým certifikátem vydaným autoritou I.CA, PostSignum nebo eIdentity
- kap. 4.4.4, 5.5.4 – agendové činnostní role se vrací jen v případě, že AIS je zaregistrován do základních registrů

Verze 3.2

- úvodní stránka – zvýrazněno datum, od kdy dokument vstupuje v platnost

Verze 3.1

- kap. 2 – přidána poznámka, že text se nevztahuje na přímou autentizační webovou službu; zkorigovány odkazy na přesunuté kapitoly 3.x
- přesunuty původní kapitoly 3.x (3.1→4.1+5.1; 3.2→4.2+5.2, část 3.3→4.3+5.3+6.3); z konce původní kapitoly 3.3 se seznamem webových služeb se stala nová kapitola 3.1
- kap. 4.2.4, 5.3.4 – opraven odkaz na kapitolu se soubory WSDL
- kap. 4.4, 5.4, 5.5, 6.2 – do názvu kapitoly přidán název metody webové služby
- kap. 6.2.2 – upřesněno vysvětlení elementu „certificate"

Verze 3.0

- kap. 3.3 – přidán text s popisem přímé autentizační webové služby

- původní kapitola 6.1 se seznamem WSDL souborů rozdělena a přesunuta pod kapitoly 4 a 5
- kap. 6 – nová kapitola s popisem přímé autentizační služby

Verze 2.3

- přidání kapitoly 5 popisující novou verzi „v2_1" webové služby
- informace o nové verzi webové služby doplněny též do kapitol 3.3 a 6.1

Verze 2.2

- kap. 3.1 – přidány konkrétní adresy prostředí KAAS
- kap. 3.3 – přidány konkrétní adresy prostředí KAAS; upřesněny požadavky na certifikát, který používá AIS pro komunikaci s KAAS
- kap. 4.1 – přidána poznámka k adrese endpointu ve WSDL souboru
- kap. 5 – nová kapitola
- WSDL soubor – přidán element „wsdl:service"

Verze 2.1

- kap. 1.3 – přidána zkratka RPP
- kap. 2 – do obrázku přidána vazba na základní registry, do textu přidány informace o agendových činnostních rolích a komunikaci s ISZR
- kap. 3.3 – přidána informace, že AIS musí mít certifikát vydán od certifikační autority základních registrů
- kap. 3.4 – do response přidán atribut „CinnostniRole", ve kterém se vracejí agendové činnostní role přidělené uživateli
- kap. 3.7 – aktualizován seznam předávaných atributů podle aktualizované response

Verze 2.0

- kap. 3.2 – parametr „token" změněn na „sessionId"
- kap. 3.3 – autentizace AIS pouze certifikátem, přidán seznam uznávaných certifikačních autorit, upřesněna adresa pro zasílání requestů
- kap. 3.4 – aktualizován obsah requestu a response
- kap. 3.5 – odstraněn poslední řádek z tabulky
- kap. 3.7 – aktualizována tabulka podle aktualizované response

Verze 1.5

- první veřejně publikovaná verze dokumentu