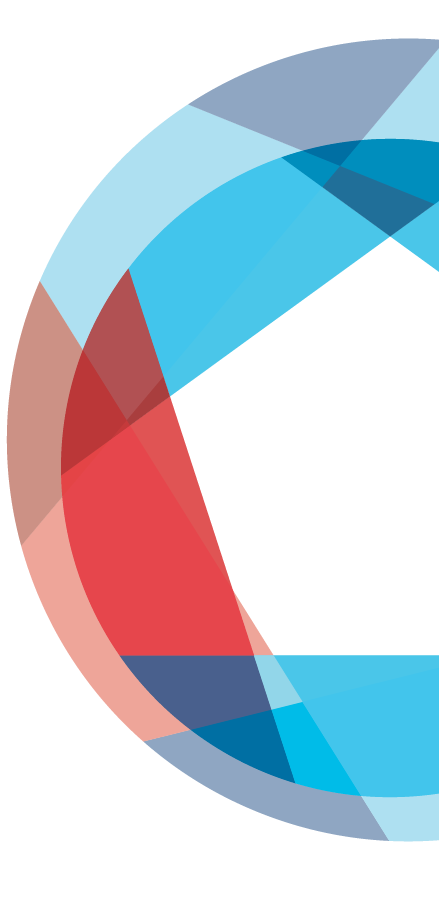
CAAIS: Autentizační webová služba – Technický popis

Verze 1.0

11.5.2022



Zpracoval: Milan Babic

Obsah

[1. Úvod 5](#_Toc103322024)

[2. Proces autentizace a autorizace 6](#_Toc103322025)

[3. Verze autentizačních webových služeb CAAIS 6](#_Toc103322026)

[4. Autentizační webová služba CAAIS (klasická) 6](#_Toc103322027)

[4.1. Rozhraní a komunikace 6](#_Toc103322028)

[4.1.1 URL pro přihlášení v CAAIS 7](#_Toc103322029)

[4.1.2 URL pro příjem autentizačního tokenu na straně AIS 7](#_Toc103322030)

[4.1.3 URL pro odhlášení v CAAIS 7](#_Toc103322031)

[4.1.4 Komunikace s WS a její zabezpečení 8](#_Toc103322032)

[4.2. Základní atributy metod 9](#_Toc103322033)

[4.2.1 heartBeat 9](#_Toc103322034)

[4.2.2 authConfirmation 9](#_Toc103322035)

[4.3. Návratové hodnoty metod 9](#_Toc103322036)

[4.4. Autentizační WS (klasická) verze v2\_1 10](#_Toc103322037)

[4.4.1 Metoda heartBeat 10](#_Toc103322038)

[4.4.2 Metoda authConfirmation 11](#_Toc103322039)

[4.5. Autentizační WS (klasická) verze v3\_4 13](#_Toc103322040)

[4.5.1 Metoda heartBeat 13](#_Toc103322041)

[4.5.2 Metoda authConfirmation 14](#_Toc103322042)

[4.6. Autentizační WS (klasická) verze v4\_1 17](#_Toc103322043)

[4.6.1 Metoda heartBeat 17](#_Toc103322044)

[4.6.2 Metoda authConfirmation 18](#_Toc103322045)

[4.7. Autentizační WS (klasická) verze v4\_2 23](#_Toc103322046)

[4.7.1 Metoda heartBeat 23](#_Toc103322047)

[4.7.2 Metoda authConfirmation 24](#_Toc103322048)

[5. Přímá autentizační webová služba CAAIS 29](#_Toc103322049)

[5.1. Rozhraní a komunikace 29](#_Toc103322050)

[5.1.1 URL pro vygenerování jednorázových přihlašovacích údajů 29](#_Toc103322051)

[5.1.2 URL pro odhlášení v CAAIS 29](#_Toc103322052)

[5.1.3 Komunikace s WS a její zabezpečení 30](#_Toc103322053)

[5.2. Základní atributy metod 31](#_Toc103322054)

[5.2.1 directAuthUser 31](#_Toc103322055)

[5.3. Návratové hodnoty metod 32](#_Toc103322056)

[5.4. Přímá autentizační WS verze v1 32](#_Toc103322057)

[5.5. Přímá autentizační WS verze v3\_4 32](#_Toc103322058)

[5.5.1 Metoda directAuthUser 32](#_Toc103322059)

[5.6. Přímá autentizační WS verze v4\_1 36](#_Toc103322060)

[5.6.1 Metoda directAuthUser 36](#_Toc103322061)

[5.7. Přímá autentizační WS verze v4\_2 41](#_Toc103322062)

[5.7.1 Metoda directAuthUser 41](#_Toc103322063)

[6. Číselníky 46](#_Toc103322064)

[6.1. Typ instituce 46](#_Toc103322065)

[6.2. Typ přihlášení 46](#_Toc103322066)

[7. Zkratky, pojmy, definice 48](#_Toc103322067)

[8. Přílohy 49](#_Toc103322068)

[8.1. Soubory WSDL pro autentizační WS 49](#_Toc103322069)

Seznam tabulek

[Tabulka 1: Základní atributy metod - heartBeat 9](#_Toc103322070)

[Tabulka 2: Základní atributy metod - authConfirmation 9](#_Toc103322071)

[Tabulka 3: Popis jednotlivých atributů - authConfirmation v2-1 12](#_Toc103322072)

[Tabulka 4: Popis jednotlivých atributů - authConfirmation v3-4 15](#_Toc103322073)

[Tabulka 5: Popis jednotlivých atributů - authConfirmation v4-1 20](#_Toc103322074)

[Tabulka 6: Popis jednotlivých atributů - authConfirmation v4-2 25](#_Toc103322075)

[Tabulka 7: Základní atributy metod - directAuthUser 31](#_Toc103322076)

[Tabulka 8: Popis jednotlivých atributů - directAuthUser v3-4 34](#_Toc103322077)

[Tabulka 9: Popis jednotlivých atributů - directAuthUser v4-1 38](#_Toc103322078)

[Tabulka 10: Popis jednotlivých atributů - directAuthUser v4-2 43](#_Toc103322079)

Verze dokumentu

|  |  |  |  |
| --- | --- | --- | --- |
| **Verze** | **Stručný popis změn** | **Zpracoval** | **Datum** |
| 1.0 | Nový dokument | Milan Babic | 11.5.2022 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Úvod

Účelem tohoto dokumentu je technicky specifikovat uživatelské autentizace do agendových informačních systémů (AIS), které jsou registrovány v systému CAAIS. Uživatel používá buď přihlašovací údaje do systému CAAIS-IdP (modul interního IdP CAAIS), který zde plní funkci autentizačního informačního systému dle § 56a zákona č. 111/2009 Sb., o základních registrech, nebo se uživatel ověřuje pomocí NIA.

Součástí popisu jsou detaily komunikace mezi systémy CAAIS a AIS a detaily rozhraní dvou typů autentizačních webových služeb:

* (klasická) autentizační webová služba CAAIS
* přímá autentizační webová služba CAAIS

Tyto služby jsou využívány systémy AIS k autentizaci a autorizaci uživatelů přihlašujících se do těchto AIS.

# Proces autentizace a autorizace

Podrobný popis procesu autentizace a autorizace pomocí autentizační webové služby CAAIS (klasické) a přímé autentizační webové služby CAAIS je uveden v dokumentu: "CAAIS: Autentizační webová služba – Procesní popis".

# Verze autentizačních webových služeb CAAIS

* **(klasická) Autentizační WS CAAIS** je implementována v následujících verzích:
  + v2\_1 – oproti předchozím verzím byla přidána metoda pro ověření dostupnosti WS a maximální délka atributu "Username" byla zvýšena na 50 znaků (viz kapitola 4.4).
  + v3\_4 – WS navíc oproti verzi v2\_1 vrací více údajů o uživateli a jeho subjektu (viz kapitola 4.5).
  + v4\_1 – WS navíc oproti verzi v3\_4 vrací osobní údaje uživatelů podle § 56a odst. 5 zákona č. 111/2009 Sb., o základních registrech (viz kapitola 4.5.2).
  + v4\_2 – WS navíc oproti verzi v4\_1 vrací identifikátor SPUÚ z ROVM, pokud autentizovaný uživatel pochází ze SPUÚ a dále úroveň LoA pro NIA, pokud se uživatel autentizoval prostřednictvím NIA (viz kapitola 4.7).
* Přímá autentizační WS CAAIS je implementována v následujících verzích:
  + v1 – neimplementováno, verze byla zrušena
  + v3\_4 – WS autentizuje pomocí přihlašovacích údajů (viz kapitola 5.5).
  + v4\_1 – WS navíc oproti verzi v3\_4 vrací osobní údaje uživatelů podle § 56a odst. 5 zákona č. 111/2009 Sb., o základních registrech (viz kapitola 5.6).
  + v4\_2 – WS navíc oproti verzi v4\_1 vrací identifikátor SPUÚ z ROVM, pokud autentizovaný uživatel pochází ze SPUÚ a dále úroveň LoA pro NIA, pokud se uživatel autentizoval prostřednictvím NIA (viz kapitola 5.7).

# Autentizační webová služba CAAIS (klasická)

WS poskytuje externímu systému (AIS) informace o uživateli, který se autentizuje a chce přistoupit do AIS.

## Rozhraní a komunikace

Definice rozhraní a způsob komunikace je shodný pro všechny verze (v2\_1, v3\_4, v4\_1, v4\_2) autentizační WS CAAIS.

### URL pro přihlášení v CAAIS

Pokud systém AIS zjistí, že uživatel přistupující na stránku AIS není přihlášen, přesměruje uživatele na přihlašovací stránku CAAIS a zároveň předává v parametru "atsId" identifikátor AIS. URL přihlašovací stránky CAAIS je následující:

|  |  |
| --- | --- |
| Prostředí | Adresa |
| testovací NAKIT | https://externalauthapi.caais-test-ext.gov.cz/login?atsId=*exampleId* |
| provozní | https://externalauthapi.caais.*[doména]*/login?atsId=*exampleId*  kde *[doména]* je **gov.cz** nebo **cms2.cz** |

### URL pro příjem autentizačního tokenu na straně AIS

V systému CAAIS je v konfiguraci AIS definována URL, na kterou je po úspěšném ověření uživatel přesměrován. Na tuto URL se v parametru "sessionId" předává v CAAIS vygenerovaný autentizační token. Na této URL operuje AIS a danou response s tokenem přijímá. Tento token pak AIS předává do autentizační WS CAAIS.

|  |
| --- |
| Příklad URL |
| http://*localhost/*?sessionId=*i7cXoUsE3NwQWy9zK8X1qxoKlLpaCeYSkM--r5Bhppb3JwD8Or* |

### URL pro odhlášení v CAAIS

V případě, že uživatel provádí odhlášení v systému AIS (např. tlačítkem "Odhlásit se" nebo odkazem pro odhlášení), měl by systém AIS v tu chvíli z bezpečnostních důvodů přesměrovat na odhlášení v systému CAAIS. Pokud byl uživatel přihlášen přes NIA, systém CAAIS zároveň přesměruje uživatele do NIA, kde se také odhlásí. URL pro odhlášení v CAAIS je následující:

|  |  |
| --- | --- |
| Prostředí | Adresa |
| testovací NAKIT | https://externalauthapi.caais-test-ext.gov.cz/processLogout?atsId=*exampleId*&uri=*adresa* |
| provozní | https://externalauthapi.caais.*[doména]*/processLogout?atsId=*exampleId*&uri=*adresa*  kde *[doména]* je **gov.cz** nebo **cms2.cz** |

V parametru "atsId" se stejně jako v případě URL pro přihlášení v CAAIS předává identifikátor AIS.

V parametru "uri" se předává návratová adresa AIS, kam je uživatel přesměrován po odhlášení v CAAIS (případně v NIA). Tato návratová URL adresa se v CAAIS porovnává s parametrem "URL pro odhlášení" v konfiguraci AIS.

Hodnoty v těchto parametrech se musí shodovat v začátku řetězce. Např. je-li v konfiguraci AIS uložena hodnota "https://www.domena.cz/logout/", pak v parametru "uri" mohou být do CAAIS předány návratové adresy "https://www.domena.cz/logout/?origin=caais" nebo "https://www.domena.cz/logout/user/jnovak/".

### Komunikace s WS a její zabezpečení

Systémy CAAIS a AIS spolu komunikují pomocí protokolu HTTPS a předávají si zprávy Request-Response ve formátu SOAP 1.1. Při volání WS je nutné vkládat správné hodnoty do atributu "soapAction" dle přiložených WSDL souborů (viz kapitola 8.1).

Pro zabezpečení komunikace je dovoleno používat pouze šifrování protokolem TLS 1.2, ostatní verze (SSL, TLS 1.0, TLS 1.1) nejsou povoleny.

WS CAAIS při komunikaci s AIS vyžaduje autentizaci komerčním serverovým certifikátem. AIS tedy musí službu volat s certifikátem vydaným jednou z podporovaných certifikačních autorit:

* I.CA - vydaný musí certifikát obsahovat v rozšíření certifikátu "extendedKeyUsage" atribut "Client Authentication" (id kp clientAuth, OID 1.3.6.1.5.5.7.3.2)
* PostSignum
* eIdentity
* NCA

Tento serverový certifikát je uložen v konfiguraci AIS v CAAIS.

Komunikaci zahajuje AIS, kdy zasílá Request na WS CAAIS a CAAIS pak odpovídá pomocí Response. Request je z AIS předáván na endpoint:

|  |  |
| --- | --- |
| Prostředí | Adresa |
| testovací NAKIT | https://cert-externalauthapi.caais-test-ext.gov.cz/asws/atsEndpoint |
| provozní | https://cert-externalauthapi.caais.*[doména]*/asws/atsEndpoint  kde *[doména]* je **gov.cz** nebo **cms2.cz** |

## Základní atributy metod

### heartBeat

Struktura request i response je pro tuto metodu ve všech verzích WS stejná, liší se pouze v označení verze v elementu "heartBeatRequest" a "heartBeatResponse".

Tabulka 1: Základní atributy metod - heartBeat

|  |  |  |
| --- | --- | --- |
| Název atributu WS | Req./Resp. | Popis atributu WS |
| status | Response | Výsledek zpracování žádosti v definované struktuře. |
| code | Response | Chybový kód v případě nedostupnosti autentizační WS. |
| message | Response | Doplňková textová informace k chybovému kódu v případě nedostupnosti autentizační WS. |

### authConfirmation

Struktura Request i Response je pro tuto metodu ve všech verzích WS stejná, liší se pouze v označení verze v elementu "authConfirmationRequest" a "authConfirmationResponse".

Tabulka 2: Základní atributy metod - authConfirmation

|  |  |  |
| --- | --- | --- |
| Název atributu WS | Req./Resp. | Popis atributu WS |
| sessionId | Request | Identifikace uživatelské session. Jedná se o autentizační token vygenerovaný v CAAIS a předaný do AIS při přesměrování uživatele. |
| status | Response | Výsledek zpracování žádosti v definované struktuře. |
| userRequestIp | Response | IP adresa uživatele při přihlášení. Může být IPv6/IPv4. Pokud uživatel využívá proxy pro přístup, předává se IP proxy, která je nejdále od uživatele. |
| attributes | Response | Údaje o autentizovaném uživateli. |

## Návratové hodnoty metod

V metodách autentizačních WS CAAIS se v Response vrací výsledek zpracování žádosti v elementu "status". Pro různé verze WS nabývá stejných hodnot:

|  |  |  |
| --- | --- | --- |
| Hodnota | Metoda | Význam |
| OK | heartBeat  authConfirmation | Výsledek zpracování požadavku je OK. |
| ERROR | heartBeat | Interní chyba systému CAAIS. Musí se buď počkat na vyřešení chyby nebo poslat požadavek znovu. |
| SYSTEM\_ERROR | authConfirmation | Interní chyba systému CAAIS. Musí se buď počkat na vyřešení chyby nebo poslat požadavek znovu. |
| SESSION\_NOT\_FOUND | authConfirmation | Chyba v případě, že byl v požadavku předán neexistující token. |

## Autentizační WS (klasická) verze v2\_1

### Metoda heartBeat

Slouží pro ověření dostupnosti webové služby. Atributy requestu a response jsou uvedeny v kapitole 4.2.1 a návratové hodnoty v kapitole 4.3.

|  |
| --- |
| **Příklad Request** |
| *<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v2="http://agw-as.cz/ats-ws/atsSzr/v2\_1">*  *<soapenv:Header/>*  *<soapenv:Body>*  *<v2:heartBeatRequest/>*  *</soapenv:Body>*  *</soapenv:Envelope>* |

|  |
| --- |
| **Příklad Response** |
| *<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">*  *<SOAP-ENV:Header/>*  *<SOAP-ENV:Body>*  *<ns2:heartBeatResponse xmlns:ns2="http://agw-as.cz/ats-ws/atsSzr/v2\_1">*  *<ns2:status>OK</ns2:status>*  *</ns2:heartBeatResponse>*  *</SOAP-ENV:Body>*  *</SOAP-ENV:Envelope>* |

### Metoda authConfirmation

Slouží pro autentizaci uživatelů. Atributy requestu a response jsou uvedeny v kapitole 4.2.2 a návratové hodnoty v kapitole 4.3.

|  |
| --- |
| **Příklad Request** |
| *<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v2="http://agw-as.cz/ats-ws/atsSzr/v2\_1">*  *<soapenv:Header/>*  *<soapenv:Body>*  *<v2:authConfirmationRequest>*  *<v2:sessionId>m7bvLLRAziPR8QJAg1-ZOkxAIEaPbTkPvTQ1BK8TAbi2CZTtI3</v2:sessionId>*  *</v2:authConfirmationRequest>*  *</soapenv:Body>*  *</soapenv:Envelope>* |

|  |
| --- |
| **Příklad Response** |
| *<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">*  *<SOAP-ENV:Header/>*  *<SOAP-ENV:Body>*  *<ns2:authConfirmationResponse xmlns:ns2="http://agw-as.cz/ats-ws/atsSzr/v2\_1">*  *<ns2:status>OK</ns2:status>*  *<ns2:userRequestIp>0.0.0.0</ns2:userRequestIp>*  *<ns2:attributes>*  *<ns2:Username>miluse\_ficnarova</ns2:Username> <ns2:UzivatelId>NGM2MDYxMjUtMDQyZS00MzRhLTkyMDYtNGIzMWVlZWZiNDYz</ns2:UzivatelId>*  *<ns2:ZkratkaSubjektu>HOLYSOV</ns2:ZkratkaSubjektu>*  *<ns2:IcSubjektu>253367</ns2:IcSubjektu>*  *<ns2:Jmeno>Miluše</ns2:Jmeno>*  *<ns2:Prijmeni>Ficnarová</ns2:Prijmeni>*  *<ns2:TitulPred>PhDr.</ns2:TitulPred>*  *<ns2:TitulZa>PhD.</ns2:TitulZa>*  *<ns2:PristupoveRole>*  *<ns2:role>TestAISAuthRole1</ns2:role>*  *</ns2:PristupoveRole>*  *<ns2:CinnostniRole>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11206</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11207</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11205</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11204</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11210</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *</ns2:CinnostniRole>*  *</ns2:attributes>*  *</ns2:authConfirmationResponse>*  *</SOAP-ENV:Body>*  *</SOAP-ENV:Envelope>* |

Tabulka 3: Popis jednotlivých atributů - authConfirmation v2-1

|  |  |  |
| --- | --- | --- |
| Název atributu WS | Popis atributu WS | Atribut z datového modelu |
| ZkratkaSubjektu | Zkratka subjektu, pod který patří uživatel. Jde o jedinečné ID subjektu v systému CAAIS. | "Subjekt"."zkratka" (Subject.shortcut) |
| IcSubjektu | IČ subjektu, pod který patří uživatel. | "Subjekt"."ič" (Subject.identificationNumber) |
| UzivatelId | Jedinečné ID uživatele (profilu) v systému CAAIS. | "Mapování SeP"." SePBSI" (ServiceMapping.sepBsi) pro daný "Profil"."uživatelské jméno" (Profile.loginName), poznámka - BSI se generuje v CAAIS nové, nemigruje se z JIP/KAAS |
| Username | Uživatelské jméno uživatele (profilu) v systému CAAIS. | "Profil"."uživatelské jméno" (Profile.loginName) |
| Jmeno | Jméno | "Profil"."Fyzická osoba"."jméno" (Profile.PhysicalPerson.firstName) |
| Prijmení | Příjmení | "Profil"."Fyzická osoba"."příjmení" (Profile.PhysicalPerson.lastName) |
| TitulPred | Titul před jménem | "Profil"."Fyzická osoba"."titul před" (Profile.PhysicalPerson.degreeBefore) |
| TitulZa | Titul za jménem | "Profil"."Fyzická osoba"."titul za" (Profile.PhysicalPerson.degreeAfter) |
| PristupoveRole | Seznam přístupových rolí do AIS přiřazených uživateli. | "Profil"."Přístupová role" (Profile.AccessRole) – pouze aktivní a ty co mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role, dotahují se přes ně odpovídající přístupové role. Dále se dotahují i delegované přístupové role přes "Vazební profil".  V seznamu přístupových rolí se vrací pouze role pro daný AIS, do kterého se uživatel autentizuje. |
| role | Kód přístupové role. | "Přístupová role"."zkratka" (AccessRole.shortcut) |
| CinnostniRole | Seznam činnostních rolí přiřazených uživateli. | "Profil"."Činnostní role" (Profile.ActivityRole) – aktivní a ty co mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role dotahují se přes ně odpovídající činnostní role a agendy. Dále se dotahují i delegované činnostní role a agendy přes "Vazební profil". |
| KodAgendy | Kód agendy činnostní role. | "Činnostní role"."Agenda"."kód" (ActivityRole.Agenda.code) |
| KodCinnostniRole | Kód činnostní role. | "Činnostní role"."kód" (ActivityRole.code) |

Datové typya omezení jsou definovány ve WSDL souboru (viz kapitola 8.1).

## Autentizační WS (klasická) verze v3\_4

### Metoda heartBeat

Slouží pro ověření dostupnosti webové služby. Atributy requestu a response jsou uvedeny v kapitole 4.2.1 a návratové hodnoty v kapitole 4.3.

|  |
| --- |
| **Příklad Request** |
| *<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v3="http://agw-as.cz/ats-ws/atsSzr/v3\_4">*  *<soapenv:Header/>*  *<soapenv:Body>*  *<v3:heartBeatRequest/>*  *</soapenv:Body>*  *</soapenv:Envelope>* |

|  |
| --- |
| **Příklad Response** |
| *<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">*  *<SOAP-ENV:Header/>*  *<SOAP-ENV:Body>*  *<ns2:heartBeatResponse xmlns:ns2="http://agw-as.cz/ats-ws/atsSzr/v3\_4">*  *<ns2:status>OK</ns2:status>*  *</ns2:heartBeatResponse>*  *</SOAP-ENV:Body>*  *</SOAP-ENV:Envelope>* |

### Metoda authConfirmation

Slouží pro autentizaci uživatelů. Atributy requestu a response jsou uvedeny v kapitole 4.2.2 a návratové hodnoty v kapitole 4.3.

|  |
| --- |
| **Příklad Request** |
| *<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v3="http://agw-as.cz/ats-ws/atsSzr/v3\_4">*  *<soapenv:Header/>*  *<soapenv:Body>*  *<v3:authConfirmationRequest>*  *<v3:sessionId>wpO8zyVjsCfO-9nfcOQRUGqtFRmpWAmRksX56WkgG4azudTpoD</v3:sessionId>*  *</v3:authConfirmationRequest>*  *</soapenv:Body>*  *</soapenv:Envelope>* |

|  |
| --- |
| **Příklad Response** |
| *<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">*  *<SOAP-ENV:Header/>*  *<SOAP-ENV:Body>*  *<ns2:authConfirmationResponse xmlns:ns2="http://agw-as.cz/ats-ws/atsSzr/v3\_4">*  *<ns2:status>OK</ns2:status>*  *<ns2:userRequestIp>0.0.0.0</ns2:userRequestIp>*  *<ns2:attributes>*  *<ns2:Username>miluse\_ficnarova</ns2:Username>*  *<ns2:UzivatelId>NGM2MDYxMjUtMDQyZS00MzRhLTkyMDYtNGIzMWVlZWZiNDYz</ns2:UzivatelId>*  *<ns2:ZkratkaSubjektu>HOLYSOV</ns2:ZkratkaSubjektu>*  *<ns2:IcSubjektu>253367</ns2:IcSubjektu>*  *<ns2:Jmeno>Miluše</ns2:Jmeno>*  *<ns2:Prijmeni>Ficnarová</ns2:Prijmeni>*  *<ns2:TitulPred>PhDr.</ns2:TitulPred>*  *<ns2:TitulZa>PhD.</ns2:TitulZa>*  *<ns2:PristupoveRole>*  *<ns2:role>TestAISAuthRole1</ns2:role>*  *</ns2:PristupoveRole>*  *<ns2:CinnostniRole>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11207</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11210</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11206</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11205</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11204</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *</ns2:CinnostniRole>*  *<ns2:Email>miluse@ficnarova.cz</ns2:Email>*  *<ns2:NazevSubjektu>Město Holýšov</ns2:NazevSubjektu>*  *<ns2:EmailSubjektu>radnice@mestoholysov.cz</ns2:EmailSubjektu>*  *<ns2:TypInstituce>6</ns2:TypInstituce>*  *<ns2:OvmPrimarni/>*  *<ns2:TypPrihlaseni>p-pwd</ns2:TypPrihlaseni>*  *<ns2:OsobaZtotoznena>true</ns2:OsobaZtotoznena>*  *<ns2:Pracoviste/>*  *<ns2:IdentifikatorOvm>00253367</ns2:IdentifikatorOvm>*  *<ns2:TimeLimitedId>b6a33b1e-1a0e-4bb1-98df-a513591168d9</ns2:TimeLimitedId>*  *</ns2:attributes>*  *</ns2:authConfirmationResponse>*  *</SOAP-ENV:Body>*  *</SOAP-ENV:Envelope>* |

Tabulka 4: Popis jednotlivých atributů - authConfirmation v3-4

|  |  |  |
| --- | --- | --- |
| Název atributu WS | Popis atributu WS | Atribut z datového modelu |
| ZkratkaSubjektu | Zkratka subjektu, pod který patří uživatel. Jde o jedinečné ID subjektu v systému CAAIS. | "Subjekt"."zkratka" (Subject.shortcut) |
| IcSubjektu | IČ subjektu, pod který patří uživatel. | "Subjekt"."ič" (Subject.identificationNumber) |
| UzivatelId | Jedinečné ID uživatele (profilu) v systému CAAIS. | "Mapování SeP"." SePBSI" (ServiceMapping.sepBsi) pro daný "Profil"."uživatelské jméno" (Profile.loginName), poznámka - BSI se generuje v CAAIS nové, nemigruje se z JIP/KAAS |
| Username | Uživatelské jméno uživatele (profilu) v systému CAAIS. | "Profil"."uživatelské jméno" (Profile.loginName) |
| Jmeno | Jméno | "Profil"."Fyzická osoba"."jméno" (Profile.PhysicalPerson.firstName) |
| Prijmení | Příjmení | "Profil"."Fyzická osoba"."příjmení" (Profile.PhysicalPerson.lastName) |
| TitulPred | Titul před jménem | "Profil"."Fyzická osoba"."titul před" (Profile.PhysicalPerson.degreeBefore) |
| TitulZa | Titul za jménem | "Profil"."Fyzická osoba"."titul za" (Profile.PhysicalPerson.degreeAfter) |
| PristupoveRole | Seznam přístupových rolí do AIS přiřazených uživateli. | "Profil"."Přístupová role" (Profile.AccessRole)  pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role dotahují se přes ně odpovídající přístupové role. Dále se dotahují i delegované přístupové role přes "Vazební profil".  V seznamu přístupových rolí se vrací pouze role pro daný AIS, do kterého se uživatel autentizuje. |
| role | Kód přístupové role. | "Přístupová role"."zkratka" (AccessRole.shortcut) |
| CinnostniRole | Seznam činnostních rolí přiřazených uživateli. | "Profil"."Činnostní role" (Profile.ActivityRole) – pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role dotahují se přes ně odpovídající činnostní role a agendy. Dále se dotahují i delegované činnostní role a agendy přes "Vazební profil". |
| KodAgendy | Kód agendy činnostní role. | "Činnostní role"."Agenda"."kód" (ActivityRole.Agenda.code) |
| KodCinnostniRole | Kód činnostní role. | "Činnostní role"."kód" (ActivityRole.code) |
| Email | Email uživatele. | "Profil"."email" (Profile.email) |
| NazevSubjektu | Název subjektu, pod který patří uživatel. | "Subjekt"."název" (Subject.name) |
| EmailSubjektu | Email subjektu. | "Subjekt"."Kontakt"."Email"."adresa" (Subject.Contact.Email.address) kde "Email"."Typ emailu"."název" (Email.EmailType.name) = "Oficiální" |
| TypInstituce | Typ instituce pro subjekt. Číselník viz kap. 6.1. | "Subjekt"."Typ instituce"."kód" (Subject.InstitutionType.code) |
| OvmPrimarni | Hlavní subjekt pro subjekty s duplicitním IČ (hodnoty true/false). | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| TypPrihlaseni | Způsob přihlášení uživatele. Číselník viz kap. 6.2. | viz hodnota ve sloupci "Hodnota z datového modelu" v kapitole 6.2. |
| OsobaZtotoznena | Příznak, že byla fyzická osoba (uživatel) ztotožněn v ROB. | "Profil"."Fyzická osoba"."osoba evidována v rob" (Profile.PhysicalPerson.personInRob) |
| TokenAifo | Datová struktura pro získání AIFO fyzické osoby (kódování Base64). Aktuálně se nic nevrací (v ROB není implementována odpovídající WS). | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| Pracoviste | Pracoviště uživatele. | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| Id | Identifikátor pracoviště | <neuvádí\_se> |
| Nazev | Název pracoviště | <neuvádí\_se> |
| Adresa | Adresa pracoviště | <neuvádí\_se> |
| KodAdresy | Kód adresy RUIAN pro pracoviště. | <neuvádí\_se> |
| IdentifikatorOvm | Identifikátor OVM z ROVM. | "Subjekt"."kód ovm v rovm" (Subject.ovmInRovmCode) |
| TimeLimitedId | Speciální autorizační token s omezenou dobou platnosti pro přístup k vybraným WS. Vrací se pouze pokud je uživatel lokální administrátor. | Technický atribut pro ukládání tokenů (neuveden v DM) |

Datové typya omezení jsou definovány ve WSDL souboru (viz kapitola 8.1).

## Autentizační WS (klasická) verze v4\_1

Předávané osobní údaje uživatele jsou poskytovány dle § 56a odst. 5 zákona č. 111/2009 Sb., o základních registrech.

### Metoda heartBeat

Slouží pro ověření dostupnosti webové služby. Atributy requestu a response jsou uvedeny v kapitole 4.2.1 a návratové hodnoty v kapitole 4.3.

|  |
| --- |
| **Příklad Request** |
| *<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v4="http://agw-as.cz/ats-ws/atsSzr/v4\_1">*  *<soapenv:Header/>*  *<soapenv:Body>*  *<v4:heartBeatRequest/>*  *</soapenv:Body>*  *</soapenv:Envelope>* |

|  |
| --- |
| **Příklad Response** |
| *<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">*  *<SOAP-ENV:Header/>*  *<SOAP-ENV:Body>*  *<ns2:heartBeatResponse xmlns:ns2="http://agw-as.cz/ats-ws/atsSzr/v4\_1">*  *<ns2:status>OK</ns2:status>*  *</ns2:heartBeatResponse>*  *</SOAP-ENV:Body>*  *</SOAP-ENV:Envelope>* |

### Metoda authConfirmation

Slouží pro autentizaci uživatelů. Atributy requestu a response jsou uvedeny v kapitole 4.2.2 a návratové hodnoty v kapitole 4.3.

|  |
| --- |
| **Příklad Request** |
| *<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v4="http://agw-as.cz/ats-ws/atsSzr/v4\_1">*  *<soapenv:Header/>*  *<soapenv:Body>*  *<v4:authConfirmationRequest>*  *<v4:sessionId>vcsnYfy-8XfTvmmrnhDy4E-sQ8D8rwP1YmT3ndZzBFnoA9J1tl</v4:sessionId>*  *</v4:authConfirmationRequest>*  *</soapenv:Body>*  *</soapenv:Envelope>* |

|  |
| --- |
| **Příklad Response** |
| *<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">*  *<SOAP-ENV:Header/>*  *<SOAP-ENV:Body>*  *<ns2:authConfirmationResponse xmlns:ns2="http://agw-as.cz/ats-ws/atsSzr/v4\_1">*  *<ns2:status>OK</ns2:status>*  *<ns2:userRequestIp>0.0.0.0</ns2:userRequestIp>*  *<ns2:attributes>*  *<ns2:Username>miluse\_ficnarova</ns2:Username>*  *<ns2:UzivatelId>NGM2MDYxMjUtMDQyZS00MzRhLTkyMDYtNGIzMWVlZWZiNDYz</ns2:UzivatelId>*  *<ns2:ZkratkaSubjektu>HOLYSOV</ns2:ZkratkaSubjektu>*  *<ns2:IcSubjektu>253367</ns2:IcSubjektu>*  *<ns2:Jmeno>Miluše</ns2:Jmeno>*  *<ns2:Prijmeni>Ficnarová</ns2:Prijmeni>*  *<ns2:TitulPred>PhDr.</ns2:TitulPred>*  *<ns2:TitulZa>PhD.</ns2:TitulZa>*  *<ns2:PristupoveRole>*  *<ns2:role>TestAISAuthRole1</ns2:role>*  *</ns2:PristupoveRole>*  *<ns2:CinnostniRole>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11207</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11210</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11206</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11205</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11204</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *</ns2:CinnostniRole>*  *<ns2:Email>miluse@ficnarova.cz</ns2:Email>*  *<ns2:NazevSubjektu>Město Holýšov</ns2:NazevSubjektu>*  *<ns2:EmailSubjektu>radnice@mestoholysov.cz</ns2:EmailSubjektu>*  *<ns2:TypInstituce>6</ns2:TypInstituce>*  *<ns2:OvmPrimarni/>*  *<ns2:TypPrihlaseni>p-pwd</ns2:TypPrihlaseni>*  *<ns2:OsobaZtotoznena>true</ns2:OsobaZtotoznena>*  *<ns2:Pracoviste/>*  *<ns2:MistoNarozeni>*  *<ns2:MistoNarozeniCr mop="false" nazev="">531065</ns2:MistoNarozeniCr>*  *</ns2:MistoNarozeni>*  *<ns2:DatumNarozeni>1966-10-25Z</ns2:DatumNarozeni>*  *<ns2:Doklady>*  *<ns2:Doklad stav="spravny" typ="P">11111931</ns2:Doklad>*  *</ns2:Doklady>*  *<ns2:NeevidovatOsobniUdaje>false</ns2:NeevidovatOsobniUdaje>*  *<ns2:IdentifikatorOvm>00253367</ns2:IdentifikatorOvm>*  *<ns2:TimeLimitedId>88e3544b-5f30-488f-ae28-85042acca029</ns2:TimeLimitedId>*  *</ns2:attributes>*  *</ns2:authConfirmationResponse>*  *</SOAP-ENV:Body>*  *</SOAP-ENV:Envelope>* |

Tabulka 5: Popis jednotlivých atributů - authConfirmation v4-1

|  |  |  |
| --- | --- | --- |
| Název atributu WS | Popis atributu WS | Atribut z datového modelu |
| ZkratkaSubjektu | Zkratka subjektu, pod který patří uživatel. Jde o jedinečné ID subjektu v systému CAAIS. | "Subjekt"."zkratka" (Subject.shortcut) |
| IcSubjektu | IČ subjektu, pod který patří uživatel. | "Subjekt"."ič" (Subject.identificationNumber) |
| UzivatelId | Jedinečné ID uživatele (profilu) v systému CAAIS. | "Mapování SeP"." SePBSI" (ServiceMapping.sepBsi) pro daný "Profil"."uživatelské jméno" (Profile.loginName), poznámka - BSI se generuje v CAAIS nové, nemigruje se z JIP/KAAS |
| Username | Uživatelské jméno uživatele (profilu) v systému CAAIS. | "Profil"."uživatelské jméno" (Profile.loginName) |
| Jmeno | Jméno | "Profil"."Fyzická osoba"."jméno" (Profile.PhysicalPerson.firstName) |
| Prijmení | Příjmení | "Profil"."Fyzická osoba"."příjmení" (Profile.PhysicalPerson.lastName) |
| TitulPred | Titul před jménem | "Profil"."Fyzická osoba"."titul před" (Profile.PhysicalPerson.degreeBefore) |
| TitulZa | Titul za jménem | "Profil"."Fyzická osoba"."titul za" (Profile.PhysicalPerson.degreeAfter) |
| PristupoveRole | Seznam přístupových rolí do AIS přiřazených uživateli. | "Profil"."Přístupová role" (Profile.AccessRole)  pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role dotahují se přes ně odpovídající přístupové role. Dále se dotahují i delegované přístupové role přes "Vazební profil".  V seznamu přístupových rolí se vrací pouze role pro daný AIS, do kterého se uživatel autentizuje. |
| role | Kód přístupové role. | "Přístupová role"."zkratka" (AccessRole.shortcut) |
| CinnostniRole | Seznam činnostních rolí přiřazených uživateli. | "Profil"."Činnostní role" (Profile.ActivityRole) – pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role dotahují se přes ně odpovídající činnostní role a agendy. Dále se dotahují i delegované činnostní role a agendy přes "Vazební profil". |
| KodAgendy | Kód agendy činnostní role. | "Činnostní role"."Agenda"."kód" (ActivityRole.Agenda.code) |
| KodCinnostniRole | Kód činnostní role. | "Činnostní role"."kód" (ActivityRole.code) |
| Email | Email uživatele. | "Profil"."email" (Profile.email) |
| NazevSubjektu | Název subjektu, pod který patří uživatel. | "Subjekt"."název" (Subject.name) |
| EmailSubjektu | Email subjektu. | "Subjekt"."Kontakt"."Email"."adresa" (Subject.Contact.Email.address) kde "Email"."Typ emailu"."název" (Email.EmailType.name) = "Oficiální" |
| TypInstituce | Typ instituce pro subjekt. Číselník viz kap. 6.1. | "Subjekt"."Typ instituce"."kód" (Subject.InstitutionType.code) |
| OvmPrimarni | Hlavní subjekt pro subjekty s duplicitním IČ (hodnoty true/false). | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| TypPrihlaseni | Způsob přihlášení uživatele. Číselník viz kap. 6.2. | viz hodnota ve sloupci "Hodnota z datového modelu" v kapitole 6.2. |
| OsobaZtotoznena | Příznak, že byla fyzická osoba (uživatel) ztotožněn v ROB. | "Profil"."Fyzická osoba"."osoba evidována v rob" (Profile.PhysicalPerson.personInRob) |
| TokenAifo | Datová struktura pro získání AIFO fyzické osoby (kódování Base64). Aktuálně se nic nevrací (v ROB není implementována odpovídající WS). | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| Pracoviste | Pracoviště uživatele. | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| Id | Identifikátor pracoviště | <neuvádí\_se> |
| Nazev | Název pracoviště | <neuvádí\_se> |
| Adresa | Adresa pracoviště | <neuvádí\_se> |
| KodAdresy | Kód adresy RUIAN pro pracoviště. | <neuvádí\_se> |
| Mistonarozeni | Místo narození uživatele. | Pokud "Profil"."Fyzická osoba"."Místo narození"."Stát"."kód" (Profile.PhysicalPerson.BirthPlace. Country.code) = 203 (tzn. jedná se o ČR) vyplňuje se atribut WS MistoNarozeniCr, jinak se vyplňuje atribut WS MistoNarozeniSvet |
| MistoNarozeniCr | Pokud je uživatel narozen v ČR, je uveden kód místa z RUIAN.  Další atributy v elementu:   * "mop" – příznak, zda se jedná o kód městského obvodu * "nazev" – název místa narození v ČR | "Místo narození"."Obec"."kód" (BirthPlace.Municipality.code)  pokud "Místo narození"."Obec"."pražský obvod" (BirthPlace.Municipality.praguePart) = 1  -> vyplní se atribut WS "mop" = true  "Místo narození"."Obec"."název" (BirthPlace.Municipality.name) -> do atributu WS "nazev" |
| MistoNarozeniSvet | Název místa narození v zahraničí. |  |
| stat | Kód státu. Číselník států ze Správy základních registrů.  Další atributy v elementu:   * "nazev" - název státu. | "Místo narození"."Stát"."kód" (BirthPlace.Country.code)  "Místo narození"."Stát"."krátký název" (BirthPlace.Country.shortName) -> do atributu WS "nazev" |
| misto | Název místa narození v zahraničí. | "Místo narození"."název" (BirthPlace.name) |
| DatumNarozeni | Datum narození. | "Profil"."Fyzická osoba"."datum narození" (Profile.PhysicalPerson.birthDate) |
| DatumUmrti | Datum úmrtí. | "Profil"."Fyzická osoba"."datum úmrtí" (Profile.PhysicalPerson.deathDate) |
| Doklady | Seznam dokladů. | V CAAIS je pouze 1 doklad |
| Doklad | Číslo dokladu.  Další atributy v elementu:   * "typ" – druh dokladu. Číselník typů dokladů ze Správy základních registrů. | "Profil"."Fyzická osoba"."druh dokladu" (Profile.PhysicalPerson.documentType)  a  "Profil"."Fyzická osoba"."číslo dokladu" (Profile.PhysicalPerson.documentId) |
| NeevidovatOsobniUdaje | Příznak, že je zakázáno pro daného uživatele evidovat osobní údaje. | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| IdentifikatorOvm | Identifikátor OVM z ROVM. | "Subjekt"."kód ovm v rovm" (Subject.ovmInRovmCode) |
| TimeLimitedId | Speciální autorizační token s omezenou dobou platnosti pro přístup k vybraným WS. Vrací se pouze pokud je uživatel lokální administrátor. | Technický atribut pro ukládání tokenů (neuveden v DM) |

Datové typya omezení jsou definovány ve WSDL souboru (viz kapitola 8.1).

## Autentizační WS (klasická) verze v4\_2

Předávané osobní údaje uživatele jsou poskytovány dle § 56a odst. 5 zákona č. 111/2009 Sb., o základních registrech.

Pokud je subjekt uživatele typu SPUÚ, vrací se v odpovědi WS identifikátor SPUÚ z ROVM.

Pokud uživatel použil pro autentizaci NIA, vrací se v odpovědi WS úroveň LoA použitého identifikačního prostředku.

### Metoda heartBeat

Slouží pro ověření dostupnosti webové služby. Atributy requestu a response jsou uvedeny v kapitole 4.2.1 a návratové hodnoty v kapitole 4.3.

|  |
| --- |
| **Příklad Request** |
| *<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v4="http://agw-as.cz/ats-ws/atsSzr/v4\_2">*  *<soapenv:Header/>*  *<soapenv:Body>*  *<v4:heartBeatRequest/>*  *</soapenv:Body>*  *</soapenv:Envelope>* |

|  |
| --- |
| **Příklad Response** |
| *<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">*  *<SOAP-ENV:Header/>*  *<SOAP-ENV:Body>*  *<ns2:heartBeatResponse xmlns:ns2="http://agw-as.cz/ats-ws/atsSzr/v4\_2">*  *<ns2:status>OK</ns2:status>*  *</ns2:heartBeatResponse>*  *</SOAP-ENV:Body>*  *</SOAP-ENV:Envelope>* |

### Metoda authConfirmation

Slouží pro autentizaci uživatelů. Atributy requestu a response jsou uvedeny v kapitole 4.2.2 a návratové hodnoty v kapitole 4.3.

|  |
| --- |
| **Příklad Request** |
| *<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v4="http://agw-as.cz/ats-ws/atsSzr/v4\_2">*  *<soapenv:Header/>*  *<soapenv:Body>*  *<v4:authConfirmationRequest>*  *<v4:sessionId>FHHWSleXsJuyMhbogK2Jq1qJFYvzBFhNkeaBrCMmI1R1xdufvG</v4:sessionId>*  *</v4:authConfirmationRequest>*  *</soapenv:Body>*  *</soapenv:Envelope>* |

|  |
| --- |
| **Příklad Response** |
| *<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">*  *<SOAP-ENV:Header/>*  *<SOAP-ENV:Body>*  *<ns2:authConfirmationResponse xmlns:ns2="http://agw-as.cz/ats-ws/atsSzr/v4\_2">*  *<ns2:status>OK</ns2:status>*  *<ns2:userRequestIp>0.0.0.0</ns2:userRequestIp>*  *<ns2:attributes>*  *<ns2:Username>miluse\_ficnarova</ns2:Username>*  *<ns2:UzivatelId>NGM2MDYxMjUtMDQyZS00MzRhLTkyMDYtNGIzMWVlZWZiNDYz</ns2:UzivatelId>*  *<ns2:ZkratkaSubjektu>HOLYSOV</ns2:ZkratkaSubjektu>*  *<ns2:IcSubjektu>253367</ns2:IcSubjektu>*  *<ns2:Jmeno>Miluše</ns2:Jmeno>*  *<ns2:Prijmeni>Ficnarová</ns2:Prijmeni>*  *<ns2:TitulPred>PhDr.</ns2:TitulPred>*  *<ns2:TitulZa>PhD.</ns2:TitulZa>*  *<ns2:PristupoveRole>*  *<ns2:role>TestAISAuthRole1</ns2:role>*  *</ns2:PristupoveRole>*  *<ns2:CinnostniRole>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11206</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11204</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11210</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11207</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11205</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *</ns2:CinnostniRole>*  *<ns2:Email>miluse@ficnarova.cz</ns2:Email>*  *<ns2:NazevSubjektu>Město Holýšov</ns2:NazevSubjektu>*  *<ns2:EmailSubjektu>radnice@mestoholysov.cz</ns2:EmailSubjektu>*  *<ns2:TypInstituce>6</ns2:TypInstituce>*  *<ns2:OvmPrimarni/>*  *<ns2:TypPrihlaseni>p-pwd</ns2:TypPrihlaseni>*  *<ns2:TypPrihlaseniNia>http://eidas.europa.eu/LoA/low</ns2:TypPrihlaseniNia>*  *<ns2:OsobaZtotoznena>true</ns2:OsobaZtotoznena>*  *<ns2:Pracoviste/>*  *<ns2:MistoNarozeni>*  *<ns2:MistoNarozeniCr mop="false" nazev="">531065</ns2:MistoNarozeniCr>*  *</ns2:MistoNarozeni>*  *<ns2:DatumNarozeni>1966-10-25Z</ns2:DatumNarozeni>*  *<ns2:Doklady>*  *<ns2:Doklad stav="spravny" typ="P">11111931</ns2:Doklad>*  *</ns2:Doklady>*  *<ns2:NeevidovatOsobniUdaje>false</ns2:NeevidovatOsobniUdaje>*  *<ns2:IdentifikatorOvm>00253367</ns2:IdentifikatorOvm>*  *<ns2:IdentifikatorSpuu/>*  *<ns2:TimeLimitedId>359a2fd2-19b9-4c11-a842-2c86d7214486</ns2:TimeLimitedId>*  *</ns2:attributes>*  *</ns2:authConfirmationResponse>*  *</SOAP-ENV:Body>*  *</SOAP-ENV:Envelope>* |

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

Tabulka 6: Popis jednotlivých atributů - authConfirmation v4-2

|  |  |  |
| --- | --- | --- |
| Název atributu WS | Popis atributu WS | Atribut z datového modelu |
| ZkratkaSubjektu | Zkratka subjektu, pod který patří uživatel. Jde o jedinečné ID subjektu v systému CAAIS. | "Subjekt"."zkratka" (Subject.shortcut) |
| IcSubjektu | IČ subjektu, pod který patří uživatel. | "Subjekt"."ič" (Subject.identificationNumber) |
| UzivatelId | Jedinečné ID uživatele (profilu) v systému CAAIS. | "Mapování SeP"." SePBSI" (ServiceMapping.sepBsi) pro daný "Profil"."uživatelské jméno" (Profile.loginName), poznámka - BSI se generuje v CAAIS nové, nemigruje se z JIP/KAAS |
| Username | Uživatelské jméno uživatele (profilu) v systému CAAIS. | "Profil"."uživatelské jméno" (Profile.loginName) |
| Jmeno | Jméno | "Profil"."Fyzická osoba"."jméno" (Profile.PhysicalPerson.firstName) |
| Prijmení | Příjmení | "Profil"."Fyzická osoba"."příjmení" (Profile.PhysicalPerson.lastName) |
| TitulPred | Titul před jménem | "Profil"."Fyzická osoba"."titul před" (Profile.PhysicalPerson.degreeBefore) |
| TitulZa | Titul za jménem | "Profil"."Fyzická osoba"."titul za" (Profile.PhysicalPerson.degreeAfter) |
| PristupoveRole | Seznam přístupových rolí do AIS přiřazených uživateli. | "Profil"."Přístupová role" (Profile.AccessRole)  pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role dotahují se přes ně odpovídající přístupové role. Dále se dotahují i delegované přístupové role přes "Vazební profil".  V seznamu přístupových rolí se vrací pouze role pro daný AIS, do kterého se uživatel autentizuje. |
| role | Kód přístupové role. | "Přístupová role"."zkratka" (AccessRole.shortcut) |
| CinnostniRole | Seznam činnostních rolí přiřazených uživateli. | "Profil"."Činnostní role" (Profile.ActivityRole) – pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role dotahují se přes ně odpovídající činnostní role a agendy. Dále se dotahují i delegované činnostní role a agendy přes "Vazební profil". |
| KodAgendy | Kód agendy činnostní role. | "Činnostní role"."Agenda"."kód" (ActivityRole.Agenda.code) |
| KodCinnostniRole | Kód činnostní role. | "Činnostní role"."kód" (ActivityRole.code) |
| Email | Email uživatele. | "Profil"."email" (Profile.email) |
| NazevSubjektu | Název subjektu, pod který patří uživatel. | "Subjekt"."název" (Subject.name) |
| EmailSubjektu | Email subjektu. | "Subjekt"."Kontakt"."Email"."adresa" (Subject.Contact.Email.address) kde "Email"."Typ emailu"."název" (Email.EmailType.name) = "Oficiální" |
| TypInstituce | Typ instituce pro subjekt. Číselník viz kap. 6.1. | "Subjekt"."Typ instituce"."kód" (Subject.InstitutionType.code) |
| OvmPrimarni | Hlavní subjekt pro subjekty s duplicitním IČ (hodnoty true/false). | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| TypPrihlaseni | Způsob přihlášení uživatele. Číselník viz kap. 6.2. | viz hodnota ve sloupci "Hodnota z datového modelu" v kapitole 6.2. |
| TypPrihlaseniNia | Hodnota LoA použitého identifikačního prostředku, pokud uživatel použil autentizaci přes NIA. | hodnota z výčtu:   * http://eidas.europa.eu/LoA/low * http://eidas.europa.eu/LoA/substantial * http://eidas.europa.eu/LoA/high |
| OsobaZtotoznena | Příznak, že byla fyzická osoba (uživatel) ztotožněn v ROB. | "Profil"."Fyzická osoba"."osoba evidována v rob" (Profile.PhysicalPerson.personInRob) |
| TokenAifo | Datová struktura pro získání AIFO fyzické osoby (kódování Base64). Aktuálně se nic nevrací (v ROB není implementována odpovídající WS). | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| Pracoviste | Pracoviště uživatele. | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| Id | Identifikátor pracoviště | <neuvádí\_se> |
| Nazev | Název pracoviště | <neuvádí\_se> |
| Adresa | Adresa pracoviště | <neuvádí\_se> |
| KodAdresy | Kód adresy RUIAN pro pracoviště. | <neuvádí\_se> |
| Mistonarozeni | Místo narození uživatele. | Pokud "Profil"."Fyzická osoba"."Místo narození"."Stát"."kód" (Profile.PhysicalPerson.BirthPlace. Country.code) = 203 (tzn. jedná se o ČR) vyplňuje se atribut WS MistoNarozeniCr, jinak se vyplňuje atribut WS MistoNarozeniSvet |
| MistoNarozeniCr | Pokud je uživatel narozen v ČR, je uveden kód místa z RUIAN.  Další atributy v elementu:   * "mop" – příznak, zda se jedná o kód městského obvodu * "nazev" – název místa narození v ČR | "Místo narození"."Obec"."kód" (BirthPlace.Municipality.code)  pokud "Místo narození"."Obec"."pražský obvod" (BirthPlace.Municipality.praguePart) = 1  -> vyplní se atribut WS "mop" = true  "Místo narození"."Obec"."název" (BirthPlace.Municipality.name) -> do atributu WS "nazev" |
| MistoNarozeniSvet | Název místa narození v zahraničí. |  |
| stat | Kód státu. Číselník států ze Správy základních registrů.  Další atributy v elementu:  "nazev" - název státu. | "Místo narození"."Stát"."kód" (BirthPlace.Country.code)  "Místo narození"."Stát"."krátký název" (BirthPlace.Country.shortName) -> do atributu WS "nazev" |
| misto | Název místa narození v zahraničí. | "Místo narození"."název" (BirthPlace.name) |
| DatumNarozeni | Datum narození. | "Profil"."Fyzická osoba"."datum narození" (Profile.PhysicalPerson.birthDate) |
| DatumUmrti | Datum úmrtí. | "Profil"."Fyzická osoba"."datum úmrtí" (Profile.PhysicalPerson.deathDate) |
| Doklady | Seznam dokladů. | V CAAIS je pouze 1 doklad |
| Doklad | Číslo dokladu.  Další atributy v elementu:   * "typ" – druh dokladu. Číselník typů dokladů ze Správy základních registrů. | "Profil"."Fyzická osoba"."druh dokladu" (Profile.PhysicalPerson.documentType)  a  "Profil"."Fyzická osoba"."číslo dokladu" (Profile.PhysicalPerson.documentId) |
| NeevidovatOsobniUdaje | Příznak, že je zakázáno pro daného uživatele evidovat osobní údaje. | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| IdentifikatorOvm | Identifikátor OVM z ROVM. | "Subjekt"."kód ovm v rovm" (Subject.ovmInRovmCode) |
| IdentifikatorSpuu | Identifikátor SPUÚ z ROVM. | "Subjekt"."kód spuú" (Subject.spuuCode) |
| TimeLimitedId | Speciální autorizační token s omezenou dobou platnosti pro přístup k vybraným WS. Vrací se pouze pokud je uživatel lokální administrátor. | Technický atribut pro ukládání tokenů (neuveden v DM) |

Datové typya omezení jsou definovány ve WSDL souboru (viz kapitola 8.1).

# Přímá autentizační webová služba CAAIS

Jde o WS, která zajišťuje ověření uživatele pomocí jednorázových přihlašovacích údajů. Tyto údaje uživateli vygeneroval systém CAAIS na základě provedeného přihlášení uživatele do CAAIS (pomocí skutečných přihlašovacích údajů do CAAIS-IdP, nebo prostřednictvím NIA).

Účelem této přímé autentizační WS tedy není ověřovat skutečné přihlašovací údaje, které jsou uloženy v CAAIS-IdP, ale ověřit ty jednorázové. V případě, že jsou zadány skutečné přihlašovací údaje, přímá autentizační WS vyhodnotí pokus jako neúspěšný.

## Rozhraní a komunikace

Definice rozhraní a způsob komunikace je shodný pro všechny verze (v3\_4, v4\_1, v4\_2) přímé autentizační WS CAAIS.

### URL pro vygenerování jednorázových přihlašovacích údajů

AIS musí mít pro uživatele přístupný odkaz (např. odkaz na přihlašovací stránce AIS) na webovou stránku CAAIS pro vygenerování jednorázových přihlašovacích údajů.

Doporučuje se tuto stránku CAAIS otvírat v novém okně nebo panelu.

URL webové stránky pro vygenerování jednorázových přihlašovacích údajů v CAAIS je následující:

|  |  |
| --- | --- |
| Prostředí | Adresa |
| testovací NAKIT | https://externalauthapi.caais-test-ext.gov.cz/login?atsId=*exampleId*&**providerType=directAuth** |
| provozní | https://externalauthapi.caais.*[doména]*/login?atsId=*exampleId*&**providerType=directAuth**  kde *[doména]* je **gov.cz** nebo **cms2.cz** |

Do parametru "atsId" se vyplňuje identifikátor AIS a v parametru "providerType" konstanta "directAuth".

### URL pro odhlášení v CAAIS

V případě, že uživatel provádí odhlášení v systému AIS (např. tlačítkem "Odhlásit se" nebo odkazem pro odhlášení), měl by systém AIS v tu chvíli z bezpečnostních důvodů přesměrovat na odhlášení v systému CAAIS. Pokud byl uživatel přihlášen přes NIA, systém CAAIS zároveň přesměruje uživatele do NIA, kde je se také odhlásí. URL pro odhlášení v CAAIS je následující:

|  |  |
| --- | --- |
| Prostředí | Adresa |
| testovací NAKIT | https://externalauthapi.caais-test-ext.gov.cz/processLogout?atsId=*exampleId*&uri=*adresa* |
| provozní | https://externalauthapi.caais.*[doména]*/processLogout?atsId=*exampleId*&uri=*adresa*  kde *[doména]* je **gov.cz** nebo **cms2.cz** |

V parametru "atsId" se stejně jako v případě URL pro vygenerování jednorázových přihlašovacích údajů v CAAIS předává identifikátor AIS.

V parametru "uri" se předává návratová adresa AIS, kam je uživatel přesměrován po odhlášení v CAAIS (případně v NIA). Tato návratová URL adresa se v CAAIS porovnává s parametrem "URL pro odhlášení" v konfiguraci AIS.

Hodnoty v těchto parametrech se musí shodovat v začátku řetězce. Např. je-li v konfiguraci AIS uložena hodnota "https://www.domena.cz/logout/", pak v parametru "uri" mohou být do CAAIS předány návratové adresy "https://www.domena.cz/logout/?origin=caais" nebo "https://www.domena.cz/logout/user/jnovak/".

### Komunikace s WS a její zabezpečení

Systémy CAAIS a AIS spolu komunikují pomocí protokolu HTTPS a předávají si zprávy Request-Response ve formátu SOAP 1.1. Při volání WS je nutné vkládat správné hodnoty do atributu "soapAction" dle přiložených WSDL souborů (viz kapitola 8.1).

Pro zabezpečení komunikace je dovoleno používat pouze šifrování protokolem TLS 1.2, ostatní verze (SSL, TLS 1.0, TLS 1.1) nejsou povoleny.

WS CAAIS při komunikaci s AIS vyžaduje autentizaci komerčním serverovým certifikátem. AIS tedy musí službu volat s certifikátem vydaným jednou z podporovaných certifikačních autorit:

* I.CA - vydaný musí certifikát obsahovat v rozšíření certifikátu "extendedKeyUsage" atribut "Client Authentication" (id kp clientAuth, OID 1.3.6.1.5.5.7.3.2)
* PostSignum
* eIdentity
* NCA

Tento serverový certifikát je uložen v konfiguraci AIS v CAAIS.

Komunikaci zahajuje AIS, kdy zasílá Request na WS CAAIS a CAAIS pak odpovídá pomocí Response. Request je z AIS předáván na endpoint:

|  |  |
| --- | --- |
| Prostředí | Adresa |
| testovací NAKIT | https://cert-externalauthapi.caais-test-ext.gov.cz/asws/directAuthUserEndpoint |
| provozní | https://cert-externalauthapi.caais.*[doména]*/asws/directAuthUserEndpoint  kde *[doména]* je **gov.cz** nebo **cms2.cz** |

## Základní atributy metod

### directAuthUser

Struktura request i response je pro tuto metodu ve všech verzích WS stejná, liší se pouze v označení verze v elementu "directAuthUserRequest" a "directAuthUserResponse".

Tabulka 7: Základní atributy metod - directAuthUser

|  |  |  |
| --- | --- | --- |
| Název atributu WS | Req./Resp. | Popis atributu WS |
| username | Request | Jednorázové uživatelské jméno. |
| password | Request | Jednorázové heslo. |
| status | Response | Výsledek zpracování žádosti v definované struktuře. |
| description | Response | Detailní popis výsledku zpracování žádosti. Při chybě je vložena chybová hláška. |
| userRequestIp | Response | IP adresa uživatele při přihlášení. Může být IPv6/IPv4. Pokud uživatel využívá proxy pro přístup, předává se IP proxy, která je nejdále od uživatele. |
| attributes | Response | Údaje o autentizovaném uživateli. |

Jednorázové přihlašovací údaje (username, password) mají omezenou platnost 30 minut a jsou automaticky zneplatněny po úspěšném ověření přímou autentizační WS.

## Návratové hodnoty metod

V metodách přímých autentizačních WS CAAIS se v Response vrací výsledek ověření autentizačních údajů v elementu "status". Pro různé verze WS nabývá stejných hodnot:

|  |  |  |
| --- | --- | --- |
| Hodnota | Metoda | Význam |
| OK | directAuthUser | Ověření uživatele proběhlo OK. Uživatel se zadanými přihlašovacími údaji v CAAIS existuje. |
| SYSTEM\_ERROR | directAuthUser | Interní chyba systému CAAIS. Musí se buď počkat na vyřešení chyby nebo poslat požadavek znovu. |
| VERIFICATION\_FAILED | directAuthUser | Ověření uživatele bylo neúspěšné (nesprávné přihlašovací údaje). |

## Přímá autentizační WS verze v1

Přímá autentizační WS v této verzi nebyla migrována z JIP/KAAS do CAAIS z důvodu ukončení její platnosti.

## Přímá autentizační WS verze v3\_4

### Metoda directAuthUser

Slouží pro ověření jednorázových přihlašovacích údajů. Atributy requestu a response jsou uvedeny v kapitole 5.2.1 a návratové hodnoty v kapitole 5.3.

|  |
| --- |
| **Příklad Request** |
| *<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v3="http://agw-as.cz/ats-ws/atsUser/atsSzr/v3\_4">*  *<soapenv:Header/>*  *<soapenv:Body>*  *<v3:directAuthUserRequest>*  *<v3:username>caais\_user\_3183500031</v3:username>*  *<v3:password>l#\*KjgCHC$e+VuTGlxwd</v3:password>*  *</v3:directAuthUserRequest>*  *</soapenv:Body>*  *</soapenv:Envelope>* |

|  |
| --- |
| **Příklad Response** |
| *<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">*  *<SOAP-ENV:Header/>*  *<SOAP-ENV:Body>*  *<ns2:directAuthUserResponse xmlns:ns2="http://agw-as.cz/ats-ws/atsUser/atsSzr/v3\_4">*  *<ns2:attributes>*  *<ns2:Username>miluse\_ficnarova</ns2:Username>*  *<ns2:UzivatelId>NGM2MDYxMjUtMDQyZS00MzRhLTkyMDYtNGIzMWVlZWZiNDYz</ns2:UzivatelId>*  *<ns2:ZkratkaSubjektu>HOLYSOV</ns2:ZkratkaSubjektu>*  *<ns2:IcSubjektu>253367</ns2:IcSubjektu>*  *<ns2:Jmeno>Miluše</ns2:Jmeno>*  *<ns2:Prijmeni>Ficnarová</ns2:Prijmeni>*  *<ns2:TitulPred>PhDr.</ns2:TitulPred>*  *<ns2:TitulZa>PhD.</ns2:TitulZa>*  *<ns2:PristupoveRole>*  *<ns2:role>TestAISAuthRole1</ns2:role>*  *</ns2:PristupoveRole>*  *<ns2:CinnostniRole>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11204</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11210</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11206</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11205</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11207</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *</ns2:CinnostniRole>*  *<ns2:Email>miluse@ficnarova.cz</ns2:Email>*  *<ns2:NazevSubjektu>Město Holýšov</ns2:NazevSubjektu>*  *<ns2:EmailSubjektu>radnice@mestoholysov.cz</ns2:EmailSubjektu>*  *<ns2:TypInstituce>6</ns2:TypInstituce>*  *<ns2:OvmPrimarni/>*  *<ns2:TypPrihlaseni>p-pwd</ns2:TypPrihlaseni>*  *<ns2:OsobaZtotoznena>true</ns2:OsobaZtotoznena>*  *<ns2:Pracoviste/>*  *<ns2:IdentifikatorOvm>00253367</ns2:IdentifikatorOvm>*  *<ns2:TimeLimitedId>5d5d3fbc-59bb-4c91-b75c-d96d905db951</ns2:TimeLimitedId>*  *</ns2:attributes>*  *<ns2:status>OK</ns2:status>*  *</ns2:directAuthUserResponse>*  *</SOAP-ENV:Body>*  *</SOAP-ENV:Envelope>* |

Tabulka 8: Popis jednotlivých atributů - directAuthUser v3-4

|  |  |  |
| --- | --- | --- |
| Název atributu WS | Popis atributu WS | Atribut z datového modelu |
| ZkratkaSubjektu | Zkratka subjektu, pod který patří uživatel. Jde o jedinečné ID subjektu v systému CAAIS. | "Subjekt"."zkratka" (Subject.shortcut) |
| IcSubjektu | IČ subjektu, pod který patří uživatel. | "Subjekt"."ič" (Subject.identificationNumber) |
| UzivatelId | Jedinečné ID uživatele (profilu) v systému CAAIS. | "Mapování SeP"." SePBSI" (ServiceMapping.sepBsi) pro daný "Profil"."uživatelské jméno" (Profile.loginName), poznámka - BSI se generuje v CAAIS nové, nemigruje se z JIP/KAAS |
| Username | Uživatelské jméno uživatele (profilu) v systému CAAIS. | "Profil"."uživatelské jméno" (Profile.loginName) |
| Jmeno | Jméno | "Profil"."Fyzická osoba"."jméno" (Profile.PhysicalPerson.firstName) |
| Prijmení | Příjmení | "Profil"."Fyzická osoba"."příjmení" (Profile.PhysicalPerson.lastName) |
| TitulPred | Titul před jménem | "Profil"."Fyzická osoba"."titul před" (Profile.PhysicalPerson.degreeBefore) |
| TitulZa | Titul za jménem | "Profil"."Fyzická osoba"."titul za" (Profile.PhysicalPerson.degreeAfter) |
| PristupoveRole | Seznam přístupových rolí do AIS přiřazených uživateli. | "Profil"."Přístupová role" (Profile.AccessRole)  pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role, dotahují se přes ně odpovídající přístupové role. Dále se dotahují i delegované přístupové role přes "Vazební profil".  V seznamu přístupových rolí se vrací pouze role pro daný AIS, do kterého se uživatel autentizuje. |
| role | Kód přístupové role. | "Přístupová role"."zkratka" (AccessRole.shortcut) |
| CinnostniRole | Seznam činnostních rolí přiřazených uživateli. | "Profil"."Činnostní role" (Profile.ActivityRole) – pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role, dotahují se přes ně odpovídající činnostní role a agendy. Dále se dotahují i delegované činnostní role a agendy přes "Vazební profil". |
| KodAgendy | Kód agendy činnostní role. | "Činnostní role"."Agenda"."kód" (ActivityRole.Agenda.code) |
| KodCinnostniRole | Kód činnostní role. | "Činnostní role"."kód" (ActivityRole.code) |
| Email | Email uživatele. | "Profil"."email" (Profile.email) |
| NazevSubjektu | Název subjektu, pod který patří uživatel. | "Subjekt"."název" (Subject.name) |
| EmailSubjektu | Email subjektu. | "Subjekt"."Kontakt"."Email"."adresa" (Subject.Contact.Email.address) kde "Email"."Typ emailu"."název" (Email.EmailType.name) = "Oficiální" |
| TypInstituce | Typ instituce pro subjekt. Číselník viz kap. 6.1. | "Subjekt"."Typ instituce"."kód" (Subject.InstitutionType.code) |
| OvmPrimarni | Hlavní subjekt pro subjekty s duplicitním IČ (hodnoty true/false). | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| TypPrihlaseni | Způsob přihlášení uživatele. Číselník viz kap. 6.2. | viz hodnota ve sloupci "Hodnota z datového modelu" v kapitole 6.2. |
| OsobaZtotoznena | Příznak, že byla fyzická osoba (uživatel) ztotožněn v ROB. | "Profil"."Fyzická osoba"."osoba evidována v rob" (Profile.PhysicalPerson.personInRob) |
| TokenAifo | Datová struktura pro získání AIFO fyzické osoby (kódování Base64). Aktuálně se nic nevrací (v ROB není implementována odpovídající WS). | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| Pracoviste | Pracoviště uživatele. | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| Id | Identifikátor pracoviště | <neuvádí\_se> |
| Nazev | Název pracoviště | <neuvádí\_se> |
| Adresa | Adresa pracoviště | <neuvádí\_se> |
| KodAdresy | Kód adresy RUIAN pro pracoviště. | <neuvádí\_se> |
| IdentifikatorOvm | Identifikátor OVM z ROVM. | "Subjekt"."kód ovm v rovm" (Subject.ovmInRovmCode) |
| TimeLimitedId | Speciální autorizační token s omezenou dobou platnosti pro přístup k vybraným WS. Vrací se pouze pokud je uživatel lokální administrátor. | Technický atribut pro ukládání tokenů (neuveden v DM) |

Datové typya omezení jsou definovány ve WSDL souboru (viz kapitola 8.1).

## Přímá autentizační WS verze v4\_1

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

### Metoda directAuthUser

Slouží pro ověření jednorázových přihlašovacích údajů. Atributy requestu a response jsou uvedeny v kapitole 5.2.1 a návratové hodnoty v kapitole 5.3.

|  |
| --- |
| **Příklad Request** |
| *<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v4="http://agw-as.cz/ats-ws/atsUser/atsSzr/v4\_1">*  *<soapenv:Header/>*  *<soapenv:Body>*  *<v4:directAuthUserRequest>*  *<v4:username>caais\_user\_2899998347</v4:username>*  *<v4:password>uIX$rR;!TT:O#Wf-Zp4;</v4:password>*  *</v4:directAuthUserRequest>*  *</soapenv:Body>*  *</soapenv:Envelope>* |

|  |
| --- |
| **Příklad Response** |
| *<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">*  *<SOAP-ENV:Header/>*  *<SOAP-ENV:Body>*  *<ns2:directAuthUserResponse xmlns:ns2="http://agw-as.cz/ats-ws/atsUser/atsSzr/v4\_1">*  *<ns2:attributes>*  *<ns2:Username>miluse\_ficnarova</ns2:Username>*  *<ns2:UzivatelId>NGM2MDYxMjUtMDQyZS00MzRhLTkyMDYtNGIzMWVlZWZiNDYz</ns2:UzivatelId>*  *<ns2:ZkratkaSubjektu>HOLYSOV</ns2:ZkratkaSubjektu>*  *<ns2:IcSubjektu>253367</ns2:IcSubjektu>*  *<ns2:Jmeno>Miluše</ns2:Jmeno>*  *<ns2:Prijmeni>Ficnarová</ns2:Prijmeni>*  *<ns2:TitulPred>PhDr.</ns2:TitulPred>*  *<ns2:TitulZa>PhD.</ns2:TitulZa>*  *<ns2:PristupoveRole>*  *<ns2:role>TestAISAuthRole1</ns2:role>*  *</ns2:PristupoveRole>*  *<ns2:CinnostniRole>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11207</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11204</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11206</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11205</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11210</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *</ns2:CinnostniRole>*  *<ns2:Email>miluse@ficnarova.cz</ns2:Email>*  *<ns2:NazevSubjektu>Město Holýšov</ns2:NazevSubjektu>*  *<ns2:EmailSubjektu>radnice@mestoholysov.cz</ns2:EmailSubjektu>*  *<ns2:TypInstituce>6</ns2:TypInstituce>*  *<ns2:OvmPrimarni/>*  *<ns2:TypPrihlaseni>p-pwd</ns2:TypPrihlaseni>*  *<ns2:OsobaZtotoznena>true</ns2:OsobaZtotoznena>*  *<ns2:Pracoviste/>*  *<ns2:MistoNarozeni>*  *<ns2:MistoNarozeniCr mop="false" nazev="">531065</ns2:MistoNarozeniCr>*  *</ns2:MistoNarozeni>*  *<ns2:DatumNarozeni>1966-10-25Z</ns2:DatumNarozeni>*  *<ns2:Doklady>*  *<ns2:Doklad stav="spravny" typ="P">11111931</ns2:Doklad>*  *</ns2:Doklady>*  *<ns2:NeevidovatOsobniUdaje>false</ns2:NeevidovatOsobniUdaje>*  *<ns2:IdentifikatorOvm>00253367</ns2:IdentifikatorOvm>*  *<ns2:TimeLimitedId>ad881f15-5c65-42cf-8899-2595a658251d</ns2:TimeLimitedId>*  *</ns2:attributes>*  *<ns2:status>OK</ns2:status>*  *</ns2:directAuthUserResponse>*  *</SOAP-ENV:Body>*  *</SOAP-ENV:Envelope>* |

Tabulka 9: Popis jednotlivých atributů - directAuthUser v4-1

|  |  |  |
| --- | --- | --- |
| Název atributu WS | Popis atributu WS | Atribut z datového modelu |
| ZkratkaSubjektu | Zkratka subjektu, pod který patří uživatel. Jde o jedinečné ID subjektu v systému CAAIS. | "Subjekt"."zkratka" (Subject.shortcut) |
| IcSubjektu | IČ subjektu, pod který patří uživatel. | "Subjekt"."ič" (Subject.identificationNumber) |
| UzivatelId | Jedinečné ID uživatele (profilu) v systému CAAIS. | "Mapování SeP"." SePBSI" (ServiceMapping.sepBsi) pro daný "Profil"."uživatelské jméno" (Profile.loginName), poznámka - BSI se generuje v CAAIS nové, nemigruje se z JIP/KAAS |
| Username | Uživatelské jméno uživatele (profilu) v systému CAAIS. | "Profil"."uživatelské jméno" (Profile.loginName) |
| Jmeno | Jméno | "Profil"."Fyzická osoba"."jméno" (Profile.PhysicalPerson.firstName) |
| Prijmení | Příjmení | "Profil"."Fyzická osoba"."příjmení" (Profile.PhysicalPerson.lastName) |
| TitulPred | Titul před jménem | "Profil"."Fyzická osoba"."titul před" (Profile.PhysicalPerson.degreeBefore) |
| TitulZa | Titul za jménem | "Profil"."Fyzická osoba"."titul za" (Profile.PhysicalPerson.degreeAfter) |
| PristupoveRole | Seznam přístupových rolí do AIS přiřazených uživateli. | "Profil"."Přístupová role" (Profile.AccessRole)  pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role dotahují se přes ně odpovídající přístupové role. Dále se dotahují i delegované přístupové role přes "Vazební profil".  V seznamu přístupových rolí se vrací pouze role pro daný AIS, do kterého se uživatel autentizuje. |
| role | Kód přístupové role. | "Přístupová role"."zkratka" (AccessRole.shortcut) |
| CinnostniRole | Seznam činnostních rolí přiřazených uživateli. | "Profil"."Činnostní role" (Profile.ActivityRole) – pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role, dotahují se přes ně odpovídající činnostní role a agendy. Dále se dotahují i delegované činnostní role a agendy přes "Vazební profil". |
| KodAgendy | Kód agendy činnostní role. | "Činnostní role"."Agenda"."kód" (ActivityRole.Agenda.code) |
| KodCinnostniRole | Kód činnostní role. | "Činnostní role"."kód" (ActivityRole.code) |
| Email | Email uživatele. | "Profil"."email" (Profile.email) |
| NazevSubjektu | Název subjektu, pod který patří uživatel. | "Subjekt"."název" (Subject.name) |
| EmailSubjektu | Email subjektu. | "Subjekt"."Kontakt"."Email"."adresa" (Subject.Contact.Email.address) kde "Email"."Typ emailu"."název" (Email.EmailType.name) = "Oficiální" |
| TypInstituce | Typ instituce pro subjekt. Číselník viz kap. 6.1. | "Subjekt"."Typ instituce"."kód" (Subject.InstitutionType.code) |
| OvmPrimarni | Hlavní subjekt pro subjekty s duplicitním IČ (hodnoty true/false). | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| TypPrihlaseni | Způsob přihlášení uživatele. Číselník viz kap. 6.2. | viz hodnota ve sloupci "Hodnota z datového modelu" v kapitole 6.2. |
| OsobaZtotoznena | Příznak, že byla fyzická osoba (uživatel) ztotožněn v ROB. | "Profil"."Fyzická osoba"."osoba evidována v rob" (Profile.PhysicalPerson.personInRob) |
| TokenAifo | Datová struktura pro získání AIFO fyzické osoby (kódování Base64). Aktuálně se nic nevrací (v ROB není implementována odpovídající WS). | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| Pracoviste | Pracoviště uživatele. | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| Id | Identifikátor pracoviště | <neuvádí\_se> |
| Nazev | Název pracoviště | <neuvádí\_se> |
| Adresa | Adresa pracoviště | <neuvádí\_se> |
| KodAdresy | Kód adresy RUIAN pro pracoviště. | <neuvádí\_se> |
| Mistonarozeni | Místo narození uživatele. | Pokud "Profil"."Fyzická osoba"."Místo narození"."Stát"."kód" (Profile.PhysicalPerson.BirthPlace. Country.code) = 203 (tzn. jedná se o ČR) vyplňuje se atribut WS MistoNarozeniCr, jinak se vyplňuje atribut WS MistoNarozeniSvet |
| MistoNarozeniCr | Pokud je uživatel narozen v ČR, je uveden kód místa z RUIAN.  Další atributy v elementu:   * "mop" – příznak, zda se jedná o kód městského obvodu * "nazev" – název místa narození v ČR | "Místo narození"."Obec"."kód" (BirthPlace.Municipality.code)  pokud "Místo narození"."Obec"."pražský obvod" (BirthPlace.Municipality.praguePart) = 1  -> vyplní se atribut WS "mop" = true  "Místo narození"."Obec"."název" (BirthPlace.Municipality.name) -> do atributu WS "nazev" |
| MistoNarozeniSvet | Název místa narození v zahraničí. |  |
| stat | Kód státu. Číselník států ze Správy základních registrů.  Další atributy v elementu:  "nazev" - název státu. | "Místo narození"."Stát"."kód" (BirthPlace.Country.code)  "Místo narození"."Stát"."krátký název" (BirthPlace.Country.shortName) -> do atributu WS "nazev" |
| misto | Název místa narození v zahraničí. | "Místo narození"."název" (BirthPlace.name) |
| DatumNarozeni | Datum narození. | "Profil"."Fyzická osoba"."datum narození" (Profile.PhysicalPerson.birthDate) |
| DatumUmrti | Datum úmrtí. | "Profil"."Fyzická osoba"."datum úmrtí" (Profile.PhysicalPerson.deathDate) |
| Doklady | Seznam dokladů. | V CAAIS je pouze 1 doklad |
| Doklad | Číslo dokladu.  Další atributy v elementu:   * "typ" – druh dokladu. Číselník typů dokladů ze Správy základních registrů. | "Profil"."Fyzická osoba"."druh dokladu" (Profile.PhysicalPerson.documentType)  a  "Profil"."Fyzická osoba"."číslo dokladu" (Profile.PhysicalPerson.documentId) |
| NeevidovatOsobniUdaje | Příznak, že je zakázáno pro daného uživatele evidovat osobní údaje. | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| IdentifikatorOvm | Identifikátor OVM z ROVM. | "Subjekt"."kód ovm v rovm" (Subject.ovmInRovmCode) |
| TimeLimitedId | Speciální autorizační token s omezenou dobou platnosti pro přístup k vybraným WS. Vrací se pouze pokud je uživatel lokální administrátor. | Technický atribut pro ukládání tokenů (neuveden v DM) |

Datové typya omezení jsou definovány ve WSDL souboru (viz kapitola 8.1).

## Přímá autentizační WS verze v4\_2

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

### Metoda directAuthUser

Slouží pro ověření jednorázových přihlašovacích údajů. Atributy requestu a response jsou uvedeny v kapitole 5.2.1 a návratové hodnoty v kapitole 5.3.

|  |
| --- |
| **Příklad Request** |
| *<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v4="http://agw-as.cz/ats-ws/atsUser/atsSzr/v4\_2">*  *<soapenv:Header/>*  *<soapenv:Body>*  *<v4:directAuthUserRequest>*  *<v4:username>caais\_user\_964205941</v4:username>*  *<v4:password>g4zMVKkzjBbus:VW0RYa</v4:password>*  *</v4:directAuthUserRequest>*  *</soapenv:Body>*  *</soapenv:Envelope>* |

|  |
| --- |
| **Příklad Response** |
| *<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">*  *<SOAP-ENV:Header/>*  *<SOAP-ENV:Body>*  *<ns2:directAuthUserResponse xmlns:ns2="http://agw-as.cz/ats-ws/atsUser/atsSzr/v4\_2">*  *<ns2:attributes>*  *<ns2:Username>miluse\_ficnarova</ns2:Username>*  *<ns2:UzivatelId>NGM2MDYxMjUtMDQyZS00MzRhLTkyMDYtNGIzMWVlZWZiNDYz</ns2:UzivatelId>*  *<ns2:ZkratkaSubjektu>HOLYSOV</ns2:ZkratkaSubjektu>*  *<ns2:IcSubjektu>253367</ns2:IcSubjektu>*  *<ns2:Jmeno>Miluše</ns2:Jmeno>*  *<ns2:Prijmeni>Ficnarová</ns2:Prijmeni>*  *<ns2:TitulPred>PhDr.</ns2:TitulPred>*  *<ns2:TitulZa>PhD.</ns2:TitulZa>*  *<ns2:PristupoveRole>*  *<ns2:role>TestAISAuthRole1</ns2:role>*  *</ns2:PristupoveRole>*  *<ns2:CinnostniRole>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11204</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11210</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11205</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11206</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *<ns2:Agenda>*  *<ns2:KodAgendy>A1023</ns2:KodAgendy>*  *<ns2:KodCinnostniRole>CR11207</ns2:KodCinnostniRole>*  *</ns2:Agenda>*  *</ns2:CinnostniRole>*  *<ns2:Email>miluse@ficnarova.cz</ns2:Email>*  *<ns2:NazevSubjektu>Město Holýšov</ns2:NazevSubjektu>*  *<ns2:EmailSubjektu>radnice@mestoholysov.cz</ns2:EmailSubjektu>*  *<ns2:TypInstituce>6</ns2:TypInstituce>*  *<ns2:OvmPrimarni/>*  *<ns2:TypPrihlaseni>p-pwd</ns2:TypPrihlaseni>*  *<ns2:TypPrihlaseniNia>http://eidas.europa.eu/LoA/low</ns2:TypPrihlaseniNia>*  *<ns2:OsobaZtotoznena>true</ns2:OsobaZtotoznena>*  *<ns2:Pracoviste/>*  *<ns2:MistoNarozeni>*  *<ns2:MistoNarozeniCr mop="false" nazev="">531065</ns2:MistoNarozeniCr>*  *</ns2:MistoNarozeni>*  *<ns2:DatumNarozeni>1966-10-25Z</ns2:DatumNarozeni>*  *<ns2:Doklady>*  *<ns2:Doklad stav="spravny" typ="P">11111931</ns2:Doklad>*  *</ns2:Doklady>*  *<ns2:NeevidovatOsobniUdaje>false</ns2:NeevidovatOsobniUdaje>*  *<ns2:IdentifikatorOvm>00253367</ns2:IdentifikatorOvm>*  *<ns2:IdentifikatorSpuu/>*  *<ns2:TimeLimitedId>09110835-8e10-4136-a004-a5b483588f06</ns2:TimeLimitedId>*  *</ns2:attributes>*  *<ns2:status>OK</ns2:status>*  *</ns2:directAuthUserResponse>*  *</SOAP-ENV:Body>*  *</SOAP-ENV:Envelope>* |

Tabulka 10: Popis jednotlivých atributů - directAuthUser v4-2

|  |  |  |
| --- | --- | --- |
| Název atributu WS | Popis atributu WS | Atribut z datového modelu |
| ZkratkaSubjektu | Zkratka subjektu, pod který patří uživatel. Jde o jedinečné ID subjektu v systému CAAIS. | "Subjekt"."zkratka" (Subject.shortcut) |
| IcSubjektu | IČ subjektu, pod který patří uživatel. | "Subjekt"."ič" (Subject.identificationNumber) |
| UzivatelId | Jedinečné ID uživatele (profilu) v systému CAAIS. | "Mapování SeP"." SePBSI" (ServiceMapping.sepBsi) pro daný "Profil"."uživatelské jméno" (Profile.loginName), poznámka - BSI se generuje v CAAIS nové, nemigruje se z JIP/KAAS |
| Username | Uživatelské jméno uživatele (profilu) v systému CAAIS. | "Profil"."uživatelské jméno" (Profile.loginName) |
| Jmeno | Jméno | "Profil"."Fyzická osoba"."jméno" (Profile.PhysicalPerson.firstName) |
| Prijmení | Příjmení | "Profil"."Fyzická osoba"."příjmení" (Profile.PhysicalPerson.lastName) |
| TitulPred | Titul před jménem | "Profil"."Fyzická osoba"."titul před" (Profile.PhysicalPerson.degreeBefore) |
| TitulZa | Titul za jménem | "Profil"."Fyzická osoba"."titul za" (Profile.PhysicalPerson.degreeAfter) |
| PristupoveRole | Seznam přístupových rolí do AIS přiřazených uživateli. | "Profil"."Přístupová role" (Profile.AccessRole)  pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role dotahují se přes ně odpovídající přístupové role. Dále se dotahují i delegované přístupové role přes "Vazební profil".  V seznamu přístupových rolí se vrací pouze role pro daný AIS, do kterého se uživatel autentizuje. |
| role | Kód přístupové role. | "Přístupová role"."zkratka" (AccessRole.shortcut) |
| CinnostniRole | Seznam činnostních rolí přiřazených uživateli. | "Profil"."Činnostní role" (Profile.ActivityRole) – pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role, dotahují se přes ně odpovídající činnostní role a agendy. Dále se dotahují i delegované činnostní role a agendy přes "Vazební profil". |
| KodAgendy | Kód agendy činnostní role. | "Činnostní role"."Agenda"."kód" (ActivityRole.Agenda.code) |
| KodCinnostniRole | Kód činnostní role. | "Činnostní role"."kód" (ActivityRole.code) |
| Email | Email uživatele. | "Profil"."email" (Profile.email) |
| NazevSubjektu | Název subjektu, pod který patří uživatel. | "Subjekt"."název" (Subject.name) |
| EmailSubjektu | Email subjektu. | "Subjekt"."Kontakt"."Email"."adresa" (Subject.Contact.Email.address) kde "Email"."Typ emailu"."název" (Email.EmailType.name) = "Oficiální" |
| TypInstituce | Typ instituce pro subjekt. Číselník viz kap. 6.1. | "Subjekt"."Typ instituce"."kód" (Subject.InstitutionType.code) |
| OvmPrimarni | Hlavní subjekt pro subjekty s duplicitním IČ (hodnoty true/false). | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| TypPrihlaseni | Způsob přihlášení uživatele. Číselník viz kap. 6.2. | viz hodnota ve sloupci "Hodnota z datového modelu" v kapitole 6.2. |
| TypPrihlaseniNia | Hodnota LoA použitého identifikačního prostředku, pokud uživatel použil autentizaci přes NIA. | hodnota z výčtu:   * http://eidas.europa.eu/LoA/low * http://eidas.europa.eu/LoA/substantial * http://eidas.europa.eu/LoA/high |
| OsobaZtotoznena | Příznak, že byla fyzická osoba (uživatel) ztotožněn v ROB. | "Profil"."Fyzická osoba"."osoba evidována v rob" (Profile.PhysicalPerson.personInRob) |
| TokenAifo | Datová struktura pro získání AIFO fyzické osoby (kódování Base64). Aktuálně se nic nevrací (v ROB není implementována odpovídající WS). | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| Pracoviste | Pracoviště uživatele. | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| Id | Identifikátor pracoviště | <neuvádí\_se> |
| Nazev | Název pracoviště | <neuvádí\_se> |
| Adresa | Adresa pracoviště | <neuvádí\_se> |
| KodAdresy | Kód adresy RUIAN pro pracoviště. | <neuvádí\_se> |
| Mistonarozeni | Místo narození uživatele. | Pokud "Profil"."Fyzická osoba"."Místo narození"."Stát"."kód" (Profile.PhysicalPerson.BirthPlace. Country.code) = 203 (tzn. jedná se o ČR) vyplňuje se atribut WS MistoNarozeniCr, jinak se vyplňuje atribut WS MistoNarozeniSvet |
| MistoNarozeniCr | Pokud je uživatel narozen v ČR, je uveden kód místa z RUIAN.  Další atributy v elementu:   * "mop" – příznak, zda se jedná o kód městského obvodu * "nazev" – název místa narození v ČR | "Místo narození"."Obec"."kód" (BirthPlace.Municipality.code)  pokud "Místo narození"."Obec"."pražský obvod" (BirthPlace.Municipality.praguePart) = 1  -> vyplní se atribut WS "mop" = true  "Místo narození"."Obec"."název" (BirthPlace.Municipality.name) -> do atributu WS "nazev" |
| MistoNarozeniSvet | Název místa narození v zahraničí. |  |
| stat | Kód státu. Číselník států ze Správy základních registrů.  Další atributy v elementu:  "nazev" - název státu. | "Místo narození"."Stát"."kód" (BirthPlace.Country.code)  "Místo narození"."Stát"."krátký název" (BirthPlace.Country.shortName) -> do atributu WS "nazev" |
| misto | Název místa narození v zahraničí. | "Místo narození"."název" (BirthPlace.name) |
| DatumNarozeni | Datum narození. | "Profil"."Fyzická osoba"."datum narození" (Profile.PhysicalPerson.birthDate) |
| DatumUmrti | Datum úmrtí. | "Profil"."Fyzická osoba"."datum úmrtí" (Profile.PhysicalPerson.deathDate) |
| Doklady | Seznam dokladů. | V CAAIS je pouze 1 doklad |
| Doklad | Číslo dokladu.  Další atributy v elementu:   * "typ" – druh dokladu. Číselník typů dokladů ze Správy základních registrů. | "Profil"."Fyzická osoba"."druh dokladu" (Profile.PhysicalPerson.documentType)  a  "Profil"."Fyzická osoba"."číslo dokladu" (Profile.PhysicalPerson.documentId) |
| NeevidovatOsobniUdaje | Příznak, že je zakázáno pro daného uživatele evidovat osobní údaje. | <prázdná\_hodnota> (neexistuje odpovídající atribut) |
| IdentifikatorOvm | Identifikátor OVM z ROVM. | "Subjekt"."kód ovm v rovm" (Subject.ovmInRovmCode) |
| IdentifikatorSpuu | Identifikátor SPUÚ z ROVM. | "Subjekt"."kód spuú" (Subject.spuuCode) |
| TimeLimitedId | Speciální autorizační token s omezenou dobou platnosti pro přístup k vybraným WS. Vrací se pouze pokud je uživatel lokální administrátor. | Technický atribut pro ukládání tokenů (neuveden v DM) |

Datové typya omezení jsou definovány ve WSDL souboru (viz kapitola 8.1).

# Číselníky

## 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 |

## Typ přihlášení

|  |  |  |
| --- | --- | --- |
| Kód | Popis | Hodnota z datového modelu |
| p-pwd | Přihlášení jménem a heslem | Při přihlášení odpovídá LoA = nízká |
| p-cert | Přihlášení jménem, heslem a certifikátem | Při přihlášení odpovídá LoA = značná |
| p-hotp | Přihlášení jménem, heslem a OTP kódem | <nevrací se> - OTP není v CAAIS implementováno |
| p-nia | Přihlášení prostřednictvím NIA | Při přihlášení přes NIA |

# Zkratky, pojmy, definice

|  |  |
| --- | --- |
| **Zkratka/pojem** | **Vysvětlení** |
| AIFO | Agendový identifikátor fyzické osoby |
| AIS | Agendový informační systém |
| Autentizace | Ověření identity uživatele |
| Autorizace | Ověření přístupových oprávnění uživatele (často následuje po autentizaci). |
| CAAIS | Centrální autorizační a autentizační informační systém, náhrada JIP/KAAS |
| CAAIS-IdP | Interní Identity Provider v rámci systému CAAIS |
| JIP | Jednotný identitní prostor - zabezpečený adresář orgánů veřejné moci a uživatelských účtů úředníka, který je součástí systému |
| KAAS | Katalog autentizačních a autorizačních služeb |
| LoA | Level of Assurance = Úroveň záruk |
| 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, soukromoprávní uživatelé údajů a jiné úřady nebo právnické osoby evidované v CAAIS. |
| Token | Slouží pro uložení a přenos autentizačních a autorizačních data, díky kterým je držiteli tohoto SW tokenu (nejde o HW zařízení) umožněno vstoupit do systém a provádět zde definované činnosti. |
| URL | Uniform Resource Locator |
| WS | Webová služba |

# Přílohy

## Soubory WSDL pro autentizační WS

K dokumentu jsou přiloženy tyto soubory WSDL s detailní technickou specifikací autentizačních WS:

|  |  |
| --- | --- |
| Soubor | Popis |
| GetCredential\_v2\_1.wsdl | Definice autentizační WS CAAIS verze v2\_1. |
| GetCredential\_v3\_4.wsdl | Definice autentizační WS CAAIS verze v3\_4. |
| GetCredential\_v4\_1.wsdl | Definice autentizační WS CAAIS verze v4\_1. |
| GetCredential\_v4\_2.wsdl | Definice autentizační WS CAAIS verze v4\_2. |
| DirectAuth\_v3\_4.wsdl | Definice přímé autentizační WS CAAIS verze v3\_4. |
| DirectAuth\_v4\_1.wsdl | Definice přímé autentizační WS CAAIS verze v4\_1. |
| DirectAuth\_v4\_2.wsdl | Definice přímé autentizační WS CAAIS verze v4\_2. |

Ve WSDL souborech jsou vždy uvedeny URL endpointu pro produkční prostředí CAAIS. Pokud je potřeba použít jiné prostředí, je nutné ručně URL upravit.