CAAIS: Ostatní webové služby - Technický popis

Verze 1.0

5.5.2022



Zpracoval: Milan Babic

Obsah

[1. Úvod 4](#_Toc102649360)

[2. Speciální webová služba CAAIS 5](#_Toc102649361)

[2.1. Používání služby 5](#_Toc102649362)

[2.2. Komunikace 6](#_Toc102649363)

[2.3. Autentizace 6](#_Toc102649364)

[3. Metody speciální webové služby 8](#_Toc102649365)

[3.1. GetUserListRole 8](#_Toc102649366)

[3.1.1 GetUserListRoleRequest 8](#_Toc102649367)

[3.1.2 GetUserListRoleResponse 8](#_Toc102649368)

[4. Typy chybových zpráv 10](#_Toc102649369)

[4.1. Odpověď ErrorResponse 10](#_Toc102649370)

[5. Zkratky, pojmy, definice 12](#_Toc102649371)

[6. Přílohy 12](#_Toc102649372)

Seznam tabulek

[Tabulka 1: Popis jednotlivých atributů - GetUserListRoleRequest 8](#_Toc102649373)

[Tabulka 2: Popis jednotlivých atributů - GetUserListRoleResponse 8](#_Toc102649374)

[Tabulka 3: Popis jednotlivých atributů - ErrorResponse 10](#_Toc102649375)

[Tabulka 4: Číselník chybových kódů (atribut „code“) 10](#_Toc102649376)

Verze dokumentu

|  |  |  |  |
| --- | --- | --- | --- |
| **Verze** | **Stručný popis změn** | **Zpracoval** | **Datum** |
| 1.0 | Nový dokument | Milan Babic | 5.5.2022 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Úvod

V následujících kapitolách je uveden technický popis speciální webové služby CAAIS sloužící pro dotažení seznamu uživatelů (uživatelských profilů) s definovanou přístupovou rolí do AIS:

- GetUserListRole

# Speciální webová služba CAAIS

## Používání služby

Na vstupu webové služby GetUserListRole se předává kód přístupové role do AIS a služba pak pro daný subjekt vrací seznam uživatelů (uživatelských profilů), kteří mají tuto roli přiřazenu.

Pro volání této služby musí být splněny tyto podmínky:

* Garant AIS (lokální administrátor) musí daný AIS, který volá tuto službu, zaregistrovat do CAAIS.
* Volání služby musí být autorizované účtem lokálního administrátora (podrobný popis viz kapitola 2.3 Autentizace).
* AIS, který volá tuto službu, musí mít v CAAIS definovánu danou přístupovou roli, na kterou se doptává.

Kompletní proces využití služby GetUserListRole je následující:

1. AIS potřebuje zavolat webovou službu GetUserListRole
2. AIS notifikuje lokálního administrátora daného subjektu o tom, že je od něj potřeba provést přihlášení do systému CAAIS a autorizovat tak volání této služby. V notifikaci (např. pop-up okno) se musí také předat důvod této autorizace
3. AIS provede přesměrování lokálního administrátora do autentizační webové služby CAAIS, kde lokální administrátor zadá přihlašovací údaje a po úspěšné autentizaci je přesměrován zpátky do AIS. AIS pak zavolá metodu authConfirmation a v odpovědi dostane údaje lokálního administrátora včetně atributu "TimeLimitedId" (technický atribut pro předávání tokenů, podrobný popis viz dokument "klasická a přímá autentizace - technický popis").
4. AIS následně využije atribut "TimeLimitedId" pro autentizaci do webové služby GetUserListRole (viz kapitola 2.3 Autentizace)
5. AIS zavolá službu GetUserListRole s vyplněnými parametry "přístupová role" a "důvod" (akci a důvod lokální administrátor potvrdil).
6. V odpovědi služby GetUserListRole se do AIS předá seznam uživatelů s danou přístupovou rolí pod stejným subjektem jako je lokální administrátor.
7. AIS dle potřeby zpracuje přijatou odpověď.

## Komunikace

Aplikace třetích stran mohou komunikovat se speciální webovou službou GetUserListRole pomocí protokolu HTTPS v režimu "request-response", přičemž aplikace třetí strany zasílá POST request s požadovanou metodou na adresu:

|  |  |
| --- | --- |
| Prostředí | Adresa |
| testovací AC | https://cert-externaleditapi11.caais-test.ocp.cea01.dscen.cz/spravadat/ws-edit/5/call/*[zkratka‑subjektu]*/  příklad: https://cert-externaleditapi11.caais-test.ocp.cea01.dscen.cz/spravadat/ws-edit/5/call/MDopravy/ |
| testovací NAKIT | https://cert-externaleditapi11.caais-test-ext.gov.cz/spravadat/ws-edit/5/call/*[zkratka-subjektu]*/  příklad: https://cert-externaleditapi11.caais-test-ext.gov.cz/spravadat/ws-edit/5/call/MDopravy/ |
| provozní | https://cert-externaleditapi11.caais.*[doména]*/spravadat/ws-edit/5/call/*[zkratka-subjektu]*/  příklad: https://cert-externaleditapi11.caais.*[doména]*/spravadat/ws-edit/5/call/MDopravy/  kde *[doména]* je **gov.cz** nebo **cms2.cz** |

[zkratka-subjektu] se uvádí pro určení subjektu, z něhož se bude získávat seznam uživatelů. V odpovědi autentizační služby CAAIS (pro ověření lokálního administrátora) se tato zkratka subjektu také vrací v atributu "ZkratkaSubjektu".

Na tento endpoint se pak přes HTTPS předává požadavek v podobě XML, který má strukturu metod podle XSD schématu uvedeném na adrese:

|  |  |
| --- | --- |
| Prostředí | Adresa |
| testovací AC | https://cert-externaleditapi11.caais-test.ocp.cea01.dscen.cz/spravadat/ws-edit/5/descriptor |
| testovací NAKIT | https://cert-externaleditapi11.caais-test-ext.gov.cz/spravadat/ws-edit/5/descriptor |
| provozní | https://cert-externaleditapi11.caais.*[doména]*/spravadat/ws-edit/5/descriptor  kde *[doména]* je **gov.cz** nebo **cms2.cz** |

Služba pak odpovídá pomocí "response". V kapitole 4 Typy chybových zpráv jsou uvedeny chybové kódy, které služba vrací v případe chyby.

## Autentizace

Dříve než může AIS volat webovou službu GetUserListRole, musí být nejprve tento AIS zaregistrován (pomocí elektronického formuláře) do systému CAAIS k danému subjektu.

AIS se pak musí do webové služby GetUserListRole autentizovat zároveň dvěma způsoby:

* certifikátem - jedná se o autentizaci komerčním serverovým certifikátem, který byl zaregistrován v systému CAAIS k danému AIS a vydán jednou z podporovaných certifikačních autorit:
  + I.CA - vydaný certifikát musí obsahovat v rozšíření certifikátu „extendedKeyUsage“ atribut „Client Authentication“ (id kp clientAuth, OID 1.3.6.1.5.5.7.3.2).
  + PostSignum
  + eIdentity
  + NCA
* BASIC autentizací - dle RFC 2617, kdy se parametru "userid" vkládá prázdný řetězec a do parametru "password" se vkládá hodnota tokenu "TimeLimitedId", který AIS dostal v odpovědi od autentizační webové služby CAAIS po úspěšném ověření lokálního administrátora. O použití tohoto tokenu je lokální administrátor informován viz postup v kapitole 2.1 Používání služby.

**Upozornění!** Token "TimeLimitedId" lze použít maximálně 5x a má omezenou platnost 30 minut.

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

# Metody speciální webové služby

## GetUserListRole

Metoda GetUserListRole na základě požadavku GetUserListRoleRequest vrací v odpovědi GetUserListRoleResponse seznam uživatelů s danou přístupovou rolí pod daným subjektem (určen z endpointu webové služby).

### GetUserListRoleRequest

Tabulka 1: Popis jednotlivých atributů - GetUserListRoleRequest

|  |  |  |
| --- | --- | --- |
| Atribut | Popis | Atribut z datového modelu |
| start | Počáteční pozice záznamu, od kterého bude vrácen seznam záznamů. Používá se v případě velkého množství záznamů pro stránkování a výchozí hodnota je 1. |  |
| role | Povinný atribut - kód (zkratka) přístupové role pro AIS, která se vyhledává u uživatelů pod daným subjektem. Role musí existovat pod daným AIS. | hledá se seznam "Subjekt"."Profil"."Přístupová role"."zkratka" (Subject.Profile.AccessRole.shortcut) = hodnota atributu WS "role"  pouze ty přístupové role, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role dotahují se přes ně odpovídající přístupové role |
| purpose | Povinný atribut - text důvodu, proč se volá metoda GetUserListRole. |  |

### GetUserListRoleResponse

Tabulka 2: Popis jednotlivých atributů - GetUserListRoleResponse

|  |  |  |
| --- | --- | --- |
| Atribut | Popis |  |
| row | Jedna položka v seznamu uživatelů. |  |
| path | Zkratka subjektu, ve kterém se hledají uživatelé. | "Subjekt"."zkratka" (Subject.shortcut) |
| objectId | Uživatelské jméno. | "Profil"."uživatelské jméno" (Profile.loginName) |
| firstname | Jméno | "Profil"."Fyzická osoba"."jméno" (Profile.PhysicalPerson.firstName) |
| surname | Příjmení | "Profil"."Fyzická osoba"."jméno" (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) |
| userAisRole | Seznam všech přístupových rolí daného AIS, které má uživatel přiřazeny.  Nevrací se přístupové role přiřazené uživateli z jiných AIS. | "Profil"."Přístupová role" (Profile.AccessRole) - pouze ty přístupové role, které jsou aktivní a mají aktivní přiřazení subjektu a zároveň se jedná o role "SeP"."Přístupová role", kde daný subjekt je konzument SeP (vazební tabulka "Konzument SeP" (SePConsumer))  Pokud má profil přiřazeny Skupiny rolí nebo Business role dotahují se přes ně odpovídající přístupové role |
| item | Zkratka přístupové role. | "Přístupová role"."zkratka" (AccessRole.shortcut) |
| text | Název přístupové role. | "Přístupová role"."název" (AccessRole.name) |
| email | Emailová adresa uživatele | "Profil"."email" (Profile.email) |
| phone | První telefonní číslo v seznamu uživatele (mobilní nebo stolní telefon). | první "Profil"."Telefon"."hodnota" (Profile.PhoneNumber.value) |
| casPosledniZmeny | Datum a čas poslední změny v údajích uživatele. | čas poslední změny profilu v historických tabulkách |

# Typy chybových zpráv

Pokud nastane chyba v systému CAAIS při pokusu o zpracování požadavku, vrátí se v odpovědi webové služby kód a popis chyby.

## Odpověď ErrorResponse

Tabulka : Popis jednotlivých atributů - ErrorResponse

|  |  |
| --- | --- |
| Název atributu WS | Popis atributu WS |
| code | Kód chyby. |
| message | Popis chyby. |

Tabulka : Číselník chybových kódů (atribut „code“)

|  |  |
| --- | --- |
| Kód chyby | Popis chyby |
| CAPP-0001 | Došlo k chybě při generování WSDL. |
| CAPP-0002 | Došlo k chybě při zpracování requestu. |
| CAPP-0003 | Funkce nebyla implementována. |
| CAPP-0000 | Jiná chyba aplikace. |
| CCFG-0001 | Uživatel má přiřazeno více rolí. |
| CCFG-0002 | Uživatel nemá přiřazenu žádnou roli. Jedná se o účet běžného uživatele. |
| CLDP-*číslo* | Chyba při komunikaci s CAAIS. Uváděné číslo odpovídá chybovému kódu, který vrací CAAIS. |
| CLDP-0000 | Jiná chyba při komunikaci s CAAIS. |
| CSAV-0001 | Uživatel nemá právo přistupovat k danému objektu. |
| CSAV-0002 | Uživatel nemá právo přistupovat k danému atributu. |
| CURL-001 | Neplatné volání webové služby. |
| CURL-002 | URL pro volání webové služby není kompletní. Chybí část URL se zkratkou subjektu. |
| CURL-003 | Bylo voláno URL s nepřístupným subjektem – subjekt buď neexistuje, nebo k němu nemá daný uživatel povolen přístup. |
| CVAL-0001 | Není vyplněna hodnota povinného atributu. |
| CVAL-0002 | Hodnota atributu neodpovídá platnému vzoru. |
| CVAL-0003 | Hodnota atributu je kratší než minimální vyžadovaná délka. |
| CVAL-0004 | Hodnota atributu je delší než maximální vyžadovaná délka. |
| CVAL-0005 | Hodnota atributu s binárními daty je větší než maximální povolená velikost. |
| CVAL-0006 | Uvedená hodnota atributu není možná. Je potřeba vybrat hodnotu ze seznamu. |
| CVAL-0010 | Požadavek neodpovídá schématu deskriptoru. |
| CVAL-0101 | Není vyplněna hodnota zkratky datového objektu (subjekt, uživatel, úřadovna, atd.). |
| CVAL-0102 | Zkratka objektu obsahuje nepovolené znaky. Povoleny jsou pouze znaky: a-z A-Z . \_ |
| CVAL-0110 | Uvedené uživatelské jméno je již použito. Každé uživatelské jméno v CAAIS musí být unikátní. |
| CVAL-0111 | Zadaná hesla se neshodují. |
| SREN-3050 | Adresa nebyla nalezena. |
| SREN-3051 | Bylo nalezeno více adres odpovídajících zadaným parametrům. |
| SREN-3052 | Došlo k chybě při pokusu o ověření adresy vůči UIR. |
| SREN-3060 | Osoba krizového řízení s daným jménem nebyla nalezena. |
| SREN-3061 | Bylo nalezeno více osob krizového řízení pro zadané jméno. |
| SREN-3070 | Nelze zpracovat zaslaný certifikát. |
| SREN-3072 | Přístupovou roli do AIS nebylo možné uživateli přiřadit, protože není přiřazena subjektu, do nějž uživatel patří. |
| SREN-3080 | Nelze ověřit platnost hodnoty; nelze najít hodnotu nadřazeného subjektu. |
| SREN-3081 | Nelze přiřadit hodnotu, kterou nemá přiřazenu nadřazený subjekt. |
| SREN-3091 | Nebyla nalezena nebo zadána agenda. |
| SREN-3092 | Agendovou činnostní roli nebylo možné uživateli přiřadit, protože není přiřazena subjektu, do nějž uživatel patří. |
| SVAL-3001 | Heslo musí obsahovat číslici. |
| SVAL-3101 | Uživatel nemůže mít současně přístup do ISUI pro obce i stavební úřady. |
| SVAL-3111 | Název aplikace AIS musí být unikátní. |
| SVAL-3112 | Subjekt nemůže přenášet svoji působnost, pokud je na něj přenesena působnost z jiného subjektu. |
| SVAL-3121 | Zkratka subjektu nebyla nalezena. |

# Zkratky, pojmy, definice

|  |  |
| --- | --- |
| **Zkratka/pojem** | **Vysvětlení** |
| AIS | Agendový informační systém |
| CAAIS | Centrální autorizační a autentizační informační systém, náhrada JIP/KAAS |
| HTTPS | Hypertext Transfer Protocol Secure |
| JIP | Jednotný identitní prostor, adresářová služba obsahující údaje pro autentizaci a autorizaci uživatelů. |
| KAAS | Katalog autentizačních a autorizačních služeb |
| SSL | Secure Sockets Layer |
| Subjekt | Orgány veřejné moci, orgány územní samosprávy a další úřady či právnické osoby, které jsou evidovány v CAAIS. |
| TLS | Transport Layer Security |
| WS | Webová služba |

# Přílohy

Dokument je bez příloh.