



Dokumentace

k projektu Czech POINT

JIP/KAAS: Webová služba GetUserListRole Technický popis

Vytvořeno dne: 20. 10. 2017

Aktualizováno: 04. 12. 2024

Verze: 1.6

© 2017-2023 MVČR

© 2023-2024 DIA

Obsah

1.	Úvod	3
1.1.	Účel dokumentu	3
1.2.	Manažerské shrnutí	3
1.3.	Definice pojmů	3
2.	Popis webové služby GetUserListRole.....	4
2.1.	Účel webové služby	4
2.2.	Podmínky použití webové služby	4
2.3.	Postup používání webové služby	4
2.4.	Rozhraní webové služby	5
2.4.1.	Definice XSD schématu	5
2.4.2.	Komunikace s webovou službou	5
2.4.3.	Autentizace do webové služby	5
3.	Metody webové služby.....	7
3.1.	Metoda GetUserListRole	7
3.1.1.	Požadavek zasílaný na webovou službu.....	7
3.1.2.	Odpověď webové služby	7
4.	Seznam změn	9

1. Úvod

1.1. Účel dokumentu

Tento dokument obsahuje technický popis speciální webové služby KAAS – GetUserListRole, která slouží k získání seznamu uživatelů jednoho subjektu, kteří mají přidělenou určitou přístupovou roli do agendového informačního systému.

1.2. Manažerské shrnutí

Tento dokument detailně popisuje speciální webovou službu JIP/KAAS – GetUserListRole. Jsou popsány podmínky, za kterých je možné webovou službu volat. Je popsán postup, jak webovou službu správně používat a jak ji volat.

Tento dokument je určen pro vývojáře aplikací třetích stran, kteří potřebují z JIP Czech POINT získávat specifická data.

1.3. Definice pojmů

Zkratka nebo pojem	Vysvětlení
AIS	Agendový informační systém
HTTPS	Hypertext Transfer Protocol Secure
JIP	Jednotný identitní prostor, adresářová služba obsahující údaje pro autentizaci a autorizaci uživatelů.
KAAS	Katalog autentizačních a autorizačních služeb
KIVS	Komunikační infrastruktura veřejné správy
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
XSD	XML Schema Definition

2. Popis webové služby GetUserListRole

2.1. Účel webové služby

Webová služba GetUserListRole slouží ke specifickému účelu. Na základě předané přístupové role do AIS vrací webová služba seznam uživatelů určitého subjektu, kteří mají přiřazenu tuto přístupovou roli.

2.2. Podmínky použití webové služby

Z bezpečnostních důvodů jsou pro webovou službu GetUserListRole aplikována následující omezení:

- AIS, který chce volat webovou službu GetUserListRole, musí být zaregistrován jako AIS do JIP Czech POINT. Více viz sekce pro vývojáře na webovém portálu Czech POINT (<http://www.czechpoint.cz>).
- AIS zasílá webové službě GetUserListRole požadavek, který musí být autorizován lokálním administrátorem daného subjektu. Způsob autorizace je vysvětlen v další kapitole.
- Přístupová role v zasílaném požadavku musí „patřit“ AISu, který posílá požadavek. Tj. AIS se nemůže ptát na přístupovou roli do jiného AIS.

2.3. Postup používání webové služby

Webová služba GetUserListRole se používá následujícím způsobem:

1. Dojde k události, která vyžaduje, aby AIS zavolal webovou službu GetUserListRole.
2. AIS musí informovat lokálního administrátora příslušného subjektu (např. dialogovým oknem), že od něj vyžaduje autorizaci příslušné akce přihlášením do JIP Czech POINT. AIS musí lokálnímu administrátorovi zobrazit důvod autorizace příslušné akce.
3. AIS přesměruje lokálního administrátora do autentizační webové služby JIP/KAAS, kde lokální administrátor zadá své přihlašovací údaje a po jejich úspěšném ověření je přesměrován zpět do AIS. AIS po zavolání metody authConfirmation obdrží v odpovědi od autentizační webové služby JIP/KAAS údaje o lokálním administrátorovi včetně údaje „TimeLimitedId“ (viz dokument s technickým popisem autentizační webové služby JIP/KAAS).
4. AIS použije údaj „TimeLimitedId“ k autentizaci do webové služby GetUserListRole (více viz kapitola 2.4.3).
5. AIS zašle požadavek webové službě GetUserListRole. Požadavek obsahuje zkratku přístupové role a odůvodnění, proč je požadavek pokládán. Důvod zpracování požadavku na pozadí musí lokální administrátor znát a akci musí také explicitně potvrdit v daném AIS (viz krok 2).
6. AIS obdrží od webové služby GetUserListRole odpověď, která obsahuje seznam uživatelů s přidělenou danou přístupovou rolí a patřících do stejného subjektu jako lokální administrátor.
7. AIS zpracuje přijatou odpověď.

2.4. Rozhraní webové služby

2.4.1. Definice XSD schématu

Metody webové služby jsou definovány podle XSD schématu, které je dostupné na adrese:

Prostředí	Adresa
testovací	https://cert.test.czechpoint.cz/spravadat/ws-edit/5/descriptor
provozní	https://kaas-crt.czechpoint.cz/spravadat/ws-edit/5/descriptor

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

Nejedná se o webovou službu podle prokolu SOAP! Na níže uvedený endpoint se zasílá XML odpovídající XSD z tohoto descriptoru.

2.4.2. Komunikace s webovou službou

Mezi webovou službou a AISem probíhá komunikace typu „request-response“. Komunikace probíhá pomocí protokolu HTTPS a je zabezpečena pomocí TLS 1.2. Starší verze protokolu (SSL, TLS 1.0, TLS 1.1) jsou zakázány.

Komunikaci iniciuje AIS, který volá webovou službu GetUserListRole zasláním POST „requestu“ na adresu:

Prostředí	Adresa
testovací	https://cert.test.czechpoint.cz/spravadat/ws-edit/5/call/[zkratka-subjektu]/
provozní	https://kaas-crt.czechpoint.cz/spravadat/ws-edit/5/call/[zkratka-subjektu]/

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

Na konci adresy je potřeba uvést zkratku subjektu (bez hranatých závorek), kterou se specifikuje subjekt, v jehož rámci se bude získávat seznam uživatelů.

Tip: Po ověření lokálního administrátora vrací autentizační webová služba JIP/KAAS zkratku subjektu v elementu „ZkratkaSubjektu“.

Např. pro získání seznamu uživatelů Královéhradeckého kraje je potřeba přistupovat na adresu:

Prostředí	Adresa
testovací	https://cert.test.czechpoint.cz/spravadat/ws-edit/5/call/kkralohrad/
provozní	https://kaas-crt.czechpoint.cz/spravadat/ws-edit/5/call/kkralohrad/

Požadavek odpovídá XSD dostupnému na adrese uvedené v předchozí kapitole.

Webová služba GetUserListRole poté vrací „response“.

2.4.3. Autentizace do webové služby

AIS se do webové služby GetUserListRole autentizuje pomocí certifikátu a basic autentizace, ve které se předává token „TimeLimitedId“.

AIS se autentizuje pomocí komerčního serverového certifikátu, který vydala certifikační autorita I.CA, PostSignum, eIdentity nebo Národní certifikační autorita. Zejména v případě I.CA musí vydaný certifikát obsahovat v rozšíření certifikátu „extendedKeyUsage“ atribut „Client Authentication“ (id-kp-clientAuth, OID 1.3.6.1.5.5.7.3.2). Tento autentizační certifikát musí být zaregistrován v nastavení AIS, což se provede pomocí administrační aplikace Správa dat (<https://www.czechpoint.cz/spravadat/>).

AIS se autentizuje pomocí basic autentizace podle RFC 2617, kdy parametr „userid“ obsahuje prázdný řetězec a parametr „password“ obsahuje hodnotu tokenu

„TimeLimitedId“, který AIS obdržel v odpovědi od autentizační webové služby JIP/KAAS na základě úspěšného ověření uživatele.

O použití tokenu TimeLimitedId při autentizaci do webové služby GetUserListRole musí být informován uživatel, na základě jehož autorizace AIS daný token obdržel. Příklad takového informování uživatele je uveden v postupu v kapitole 2.3.

Důležité! Token „TimeLimitedId“ je určen k okamžitému použití – má omezenou platnost 30 minut a lze jej použít pouze pětkrát.

3. Metody webové služby

3.1. Metoda GetUserListRole

Tato metoda vrátí seznam uživatelů, kteří mají přiřazenu specifikovanou přístupovou roli. Vrací se pouze seznam uživatelů z určitého subjektu, který je odvozen z použitého endpointu webové služby.

3.1.1. Požadavek zasílaný na webovou službu

Příklad požadavku GetUserListRoleRequest

```
<?xml version="1.0" encoding="UTF-8"?>
<GetUserListRoleRequest start="1" xmlns="http://userportal.novell.com/ws-edit/5/WS-5-1.1">
  <purpose>Získání seznamu uživatelů pro nastavení přístupu do CMS 2.</purpose>
  <role>ROLE</role>
</GetUserListRoleRequest>
```

Popis datové struktury požadavku

Atribut	Popis
start	Indikátor, od jakého záznamu má seznam uživatelů začínat. Slouží pro potřeby „stránkování“ (přeskočení prvních N záznamů).
role	Zkratka přístupové role do AIS, kterou mají mít uživatelé přiřazenu. Musí se jednat o přístupovou roli, kterou má vytvořenu AIS, který zasílá požadavek. Element musí obsahovat neprázdnou hodnotu.
purpose	Účel, za jakým je webová služba GetUserListRole AISem volána. Element je povinný.

3.1.2. Odpověď webové služby

Příklad odpovědi GetUserListRoleResponse

```
<?xml version="1.0" encoding="UTF-8"?>
<GetUserListRoleResponse total="1" xmlns="http://userportal.novell.com/ws-edit/5/WS-5-1.1">
  <row path="vzorov" objectId="aa2">
    <firstname>Josef</firstname>
    <surname>Novák</surname>
    <titulPred>Bc.</titulPred>
    <titulZa>MBA</titulZa>
    <userAisRole>
      <item text="Zkušební role">ROLE</item>
    </userAisRole>
    <email>josef@max.cz</email>
    <phone>123456789</phone>
    <casPosledniZmeny>1503318236</casPosledniZmeny>
  </row>
</GetUserListRoleResponse>
```

Popis datové struktury odpovědi

Atribut	Popis
row	Jeden záznam o uživateli.
path	Zkratka subjektu, ve kterém je zřízen účet daného uživatele.
objectId	Uživatelské jméno.
firstname	Jméno uživatele
surname	Příjmení uživatele

Atribut	Popis
titulPred	Titul před jménem
titulZa	Titul za jménem
userAisRole	Seznam přístupových rolí, přiřazených uživateli. Na seznamu se nacházejí pouze přístupové role, které spadají pod AIS, který zaslal požadavek. Nevracejí se přístupové role jiných AISů.
item	Zkratka přístupové role.
text	Atribut s názvem přístupové role.
email	První oficiální e-mailová adresa.
phone	První telefonní číslo (mobilní nebo stolní telefon).
casPosledniZmeny	Časový okamžik poslední změny v účtu uživatele.

4. Seznam změn

Níže je uvedena historie změn tohoto dokumentu. Uvedeny jsou jen veřejně publikované verze.

Verze 1.6

- celý dokument – opraveno označení KAAS na používanější JIP/KAAS

Verze 1.5

- kap. 2.4.3 – na seznam podporovaných certifikačních autorit byla přidána Národní certifikační autorita

Verze 1.4

- kap. 2.4.1, 2.4.2 – odstraněny adresy s doménou czechpoint.cms2.cz

Verze 1.3

- kap. 2.4.1, 2.4.2 – odstraněny již neplatné adresy prostředí dostupných z CMS 1
- kap. 2.4.2 - protokoly TLS 1.0 a TLS 1.1 jsou zakázány

Verze 1.2

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

Verze 1.1

- kap 2.3 – drobné upřesnění postupu
- kap. 2.4.1, 2.4.2 – přidány adresy prostředí dostupných z CMS 2
- kap. 2.4.2 – místo protokolu TLSv1.0 je potřeba použít TLSv1.2
- kap. 2.4.3 – přidáno upozornění na nutnost správného nastavení rozšíření „extendedKeyUsage“ v autentizačním certifikátu AIS

Verze 1.0

- první veřejně publikovaná verze dokumentu