Datové schránky

Autentizační služba Portálu veřejné správy

Technická specifikace

Vytvořeno dne: 7.12.2012

Aktualizováno: 26.8.2015

Verze: 1.7

Obsah

1. Úvod

1.1. Cíl dokumentu

Tento dokument slouží jako zdroj informací pro vývojáře externích aplikací, kteří budou používat popsané rozhraní.

1.2. Zkratky a definice

Zkratka	Význam
Autentizace	Ověření identity uživatele
ExtIS	Technický název této služby pro účely získání informací o osobě přihlašující se do DS.
Autorizace	Přidělení přístupových práv uživateli po jeho úspěšné autentizaci
CRL	Certificate Revocation List
ISDS	Informační systém datových schránek
MV ČR	Ministerstvo vnitra ČR
Poskytovatel	IS veřejné správy, resp. správce tohoto IS
WS	Webové služby na bázi protokolu SOAP v1.1
WSDL	Popis rozhraní webové služby
appToken	Pro identifikaci, odkud byl uživatel přesměrován na autentizační bránu, může být současně s přesměrováním v přístupovém URL uveden parametr *appToken*. V tomto parametru si může aplikace poskytovatele udržet identifikaci, odkud je uživatel přesměrován do autentizačního modulu. Tento parametr bude zpět předán aplikaci poskytovatele WS **getCredential** za předpokladu, že byl součástí přístupového URL. Tento parametr obsahuje maximálně 20 číslic. *appToken* bude také vrácen jako součást návratového URL.
Uživatel	V tomto textu se jedná o uživatele ISDS, který může využívat služeb ExtIS prostřednictvím aplikace poskytovatele.
`[url-adresa-prostředí-isds]`	Adresy prostředí: Veřejný test: **`czebox.cz`** Produkční prostředí: **`mojedatovaschranka.cz`**

2. Popis služby

Tato služba umožňuje aplikaci poskytovatele získat informace o uživateli ISDS (a jeho schránce), který aplikaci poskytovatele využívá.

Tento dokument popisuje způsob využívání ExtIS v aplikací poskytovatele.

2.1. Základní pojmy

Aplikace poskytovatele je libovolná webová aplikace, která implementuje autentizaci svých uživatelů pomocí přihlašovacích údajů do ISDS.

ISDS zprostředkuje pro aplikaci poskytovatele službu Autentizačního modulu pro uživatele ISDS.

Přihlášení uživatele pomocí přihlašovacích údajů do ISDS a ověření přihlašovacích údajů probíhá v perimetru ISDS.

ISDS předává do aplikace poskytovatele informace o přihlášeném uživateli a odpovídající datové schránce. Rozsah předávaných informací (atributů) je stanoven poskytovatelem při registraci aplikace poskytovatele do ISDS.

2.2. Požadavky

Základním požadavkem na poskytovatele je jeho vlastní datová schránka ISDS (v současné verzi typu OVM). K jedné datové schránce je možné zaregistrovat více Aplikací poskytovatele.

2.3. Konfigurace přístupové služby uživatele

První konfigurace služby je provedena zároveň s její registrací. Registraci provádí správce ISDS.

Během registrace je každé službě přiděleno unikátní ID. Konfigurace služby v průběhu její existence zahrnuje tyto operace:

- registrace nového přístupového certifikátu služby,
- odregistrace přístupového certifikátu služby,
- nastavení návratového URL,
- nastavení a změna množiny povolených atributů datové schránky a uživatele k předání aplikaci,
- aktivace a deaktivace služby.

Všechny tyto operace provádí správce ISDS. Poskytovatel v případě potřeby žádá správce o změnu konfigurace.

Poznámka:

1. Pro využití služby je nutné použít komerční certifikát vydaný certifikační autoritou provozovanou akreditovaným poskytovatelem certifikačních služeb v ČR. Certifikát musí být platný a nesmí být umístěn na CRL. Certifikát nesmí mít omezení, vylučující jeho použití jako SSL/TLS klient.
2. V jednu chvíli je možné mít zaregistrováno více certifikátů. Je to zejména z toho důvodu, aby byl před vypršením starého již připraven nový.
3. Použitý certifikát smí být zaregistrován v autentizační službě pouze jednou (nelze použít stejný certifikát pro dvě služby).

2.4. Předání informací o uživateli aplikaci poskytovatele

Aplikace poskytovatele využívá univerzální autentizační bránu v perimetru ISDS. Tento Autentizační modul poskytuje stejné metody a úroveň ověření uživatele přistupujícího do aplikace poskytovatele jako při přihlášení do ISDS.

Jedná se tedy o následující přihlašovací údaje, které bude uživatel zadávat:

- uživatelské jméno (povinný údaj)
- heslo (povinný údaj)
- komerční certifikát nebo OTP nebo SMS (volitelně)

Po ověření Autentizační modul vrátí výsledek do aplikace poskytovatele. Autentizační modul umožňuje ověřování přístupových údajů všem typům uživatelů datové schránky.

Příklad postupu:

1. Uživatel vstoupí na webovou stránku aplikace poskytovatele. Uživatel vyjádří potřebu využít funkčnost, která využije předání informací o uživateli z DS. Systém provede přesměrování na stránku Autentizačního modulu. V tomto požadavku aplikace poskytovatele předá Autentizačnímu modulu číselný identifikátor služby, pod kterým je daná služba poskytovatele zaregistrována v ISDS. Tento identifikátor je předán v parametru *atsId*. Pokud aplikace poskytovatele potřebuje uchovat identifikaci, odkud byl uživatel přesměrován, může přidat i parametr *appToken*. Tento řetězec je složen z maximálně 20 číslic.

Vzor:

```
https://www.[url-adresa-prostředí-isds]/as/login?atsId=exampleId
```

případně:

```
https://www.[url-adresa-prostředí-isds]/as/login?atsId=exampleId&appToken=123
```

2. Po přesměrování zobrazí Autentizační modul uživateli webovou stránku s autentizačním (přihlašovacím) formulářem. Uživatel je vyzván k zadání svých přístupových údajů, které používá ke klasickému přihlášení do ISDS. Uživatel zadá přístupové údaje do 5 minut.

3. Autentizační modul ověří vůči identitnímu prostoru ISDS správnost přístupových údajů. V případě neúspěšného ověření přístupových údajů je uživateli zobrazeno upozornění typu „Chyba přihlášení, znovu zadejte údaje.“. V případě úspěšného ověření přístupových údajů je uživatel požádán o souhlas s předáním informací (povolených atributů) aplikaci poskytovatele. Uživatel projeví souhlas s předáním informací do 5 minut.

4. Autentizační modul přesměruje uživatele na návratové URL, které je uvedeno v nastavení služby ExtIS v datové schránce provozovatele. Toto URL, které je plně v režii ExtIS, musí přijímat parametr "*sessionId*", který poté ExtIS použije pro volání webové služby. Kromě toho může být touto cestou vrácen také *appToken*, pokud byl aplikací poskytovatele použit.

Vzor:

```
https://[url-adresa-aplikace]?sessionId=01-8c57c8b70acb41598456914f17ae933b
```

případně:

```
https://[url-adresa-aplikace]/?sessionId=01-8c57c8b70acb41598456914f17ae933b
&appToken=123
```

5. Aplikace převezme *sessionId* a případně *appToken*, který přišel s redirectem z Autentizačního modulu a s *sessionId* zavolá webovou službu Autentizačního modulu. Získání informací z ISDS za pomocí daného *sessionId* je možné pouze jednou. Zároveň s *sessionId* získá *appToken*, pokud byl autentizačnímu modulu předán v požadavku (viz bod 1).

Technická specifikace volání webové služby přihlášení je popsána v následující kapitole.

3. Aplikace poskytovatele pro využití služby

3.1. Technické požadavky na Aplikaci poskytovatele

1. Musí být dostupná z Internetu a přístup do ní musí být zabezpečen přes webový prohlížeč pomocí protokolu HTTPS.

2. Implementuje přihlašovací stránku pro příjem sessionId podle specifikace uvedené v kapitole 2.4 Předání informací o uživateli aplikaci poskytovatele.

3. Požadavky na klienta: aplikace implementuje klientskou část WS podle WSDL specifikace v kapitole 3.2. Pro přístup na WS bude aplikace využívat komerční serverový certifikát vydaný certifikační autoritou provozovanou akreditovaným poskytovatelem certifikačních služeb v ČR. Certifikát musí být platný a nesmí být umístěn na CRL. Certifikát nesmí mít omezení vylučující použití jako SSL/TLS klient. Tento certifikát musí být zaregistrován v konfiguraci služby na straně ISDS.

4. Konfigurace serveru: Komunikace s ExtIS probíhá vždy zabezpečeným způsobem přes protokol SSLv3/TLSv1. Služba využívá k šifrování komerční serverový certifikát vydaný akreditovanou certifikační autoritou ČR

3.2. Popis webové služby pro získání informací

Aplikace jako klient WS ExtIS komunikuje způsobem „request-response". Komunikace probíhá pomocí protokolu HTTPS, pro přenos zpráv se používá formát SOAP 1.1. Komunikace je zabezpečená pomocí SSL. Popis webové služby ve formátu WSDL je uveden v souboru `GetCredential.wsdl`. URL webové služby:

`https://cert.[url-adresa-prostředí-isds]/asws/atsEndpoint`

3.2.1. Příklad komunikace WS

Příklad: Přihlásí se oprávněná osoba („majitel", type=„S") aktivní (stav=1) schránky typu PFO Advokát (typ=„31"). Při registraci služby nebylo dovoleno další předávat osobní údaje.

Request

```
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
      <m:authConfirmationRequest xmlns:m="Some-URI">
        <m:sessionId>00-c679c0687f2d43ebbcd766876f90da66</m:sessionId>
      </m:authConfirmationRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Response

```
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
      <m:authConfirmationResponse xmlns:m="http://agw-as.cz/ats-ws/v1">
        <m:status>OK</m:status>
        <m:userRequestIp>192.168.0.1</m:userRequestIp>
        <m:attributes>
           <m:attribute name="dbID" value="qw6rty3"/>
           <m:attribute name="dbType" value="31"/>
           <m:attribute name="dbState" value="1"/>
           <m:attribute name="userType" value="S"/>
         </m:attributes>
      </m:authConfirmationResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

3.2.2. Vysvětlivky

Hodnota	Význam
sessionId	Identifikace session uživatele přihlášeného do Autentizačního modulu. Token získaný po přesměrování v kapitole 2.4, bod 4.
status	Strukturovaná informace o výsledku zpracování žádosti.
userRequestIp	IP uživatele při přihlášení.
attribute	Atribut z identitního prostoru pod názvem „name" a s hodnotou "value". Jde o atributy „appToken" a seznam atributů předávaných aplikaci poskytovatele.

3.2.3. Popis stavů výsledku zpracování

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

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

4. Seznam předávaných atributů

Seznam všech atributů, které mohou být zasílány přes webovou službu **getCredential** do externí aplikace. Seznam atributů je definován při registraci služby do ISDS.

4.1. Atributy datové schránky

Název ve WS/API	Význam
dbDescription	Složený název schránky (PO a OVM – název firmy, FO – jméno, další jména a příjmení, PFO - jméno, další jména a příjmení + pomlčka + název subjektu)
biCity	místo narození (FO, PFO)
biCounty	okres narození (FO, PFO)
biDate	datum narození (FO, PFO) ve formátu YYYY-MM-DD
biState	země narození (FO, PFO)
firmName	název subjektu (OVM, PO, PFO)
ic	IČ subjektu (OVM, PO, PFO)
pnFirstName	křestní jméno osoby (FO, PFO)
pnLastName	příjmení osoby (FO, PFO)
pnMiddleName	další jména osoby (FO, PFO)
adCity	adresa – obec
adStreet	adresa – ulice
adNumberInMunicipality	adresa – číslo domu
adNumberInStreet	adresa – číslo orientační

Název ve WS/API	Význam
adZipCode	adresa – PSČ
adState	adresa – stát
fullAddress	Kompletní složená adresa (ulice + čísla + PSČ + obec nebo nestrukturovaná adresa)
dbEffectiveOVM	TRUE/FALSE; TRUE = schránka OVM nebo schránka povýšená na OVM
dbType	typ schránky podle číselníku (10 = OVM apod.)
dbID	ID schránky (7 znaků)
dbState	Stav schránky podle číselníku (1 až 6) – jen stav 1 znamená aktivní schránku

4.2. Atributy uživatele

Název ve WS/API	Význam
fullUserName	Kompletní složené jméno uživatele nebo nestrukturované jméno
userType	Typ uživatele; nabývá hodnot S = Oprávněná osoba, A = Administrátor, P = Pověřená osoba, L = likvidátor, U = interní uživatel
userPrivils	Informace o následujících právech uživatele (každé právo je reprezentováno jedním bitem): 0x1 Číst zprávy (kromě zpráv do vlastních rukou) 0x2 Číst zprávy – všechny 0x4 Posílat zprávy 0x8 Zobrazovat seznamy a dodejky 0x10 Vyhledávat schránky 0x20 Primární uživatel nebo administrátor 0x80 Mazat zprávy v trezoru