DATOVÉ SCHRÁNKY

Datové schránky

Webové služby související s přístupem do ISDS

Vytvořeno dne: 15.1.2010
Aktualizováno: 31.10.2022
Verze: 2.76
Klasifikace: Veřejný dokument

Obsah

1. Webové služby související s přístupem do ISDS

1.1. Komu jsou služby určené

Tento dokument specifikuje návrh podpůrných webových služeb ISDS, které se dotýkají přístupu do systému. Vyžívat je mohou všichni uživatelé ISDS s výjimkou interních uživatelů.

Jsou to služby definované pomocí souborů `db_access.wsdl` verze 2.3x. Použité datové typy jsou definovány souborem `dbTypes.xsd`.

Přehled webových služeb:

- Získání informací o schránce přihlášeného uživatel – **GetOwnerInfoFromLogin2**.
- Získání informací o přihlášeném uživatel – **GetUserInfoFromLogin2**.
- Získání informace o expiraci hesla - **GetPasswordInfo**.
- Změna hesla – **ChangeISDSPassword**.

Další pomocné služby jsou popsány ve veřejné příručce *ISDS_OTP_autentizace.pdf*. Jedná se o služby:

- Změna hesla při OTP nebo SMS přihlašování – **ChangePasswordOTP**.
- Zaslání SMS přihlašovacího kódu – **SendSMSCode**.

1.1.1. URL pro přístup

URL pro ze popsané webové služby je `https://ws1.mojedatovaschranka.cz/DS/DsManage` při použití Basic autentizace a přihlášením pomocí jména hesla. Pro jiné způsoby přihlášení použijte URL popsaná v příručce *WS_manipulace_s_datovymi_zpravami.pdf* v kapitole *Základní URL pro webové služby*.

Pro navázání komunikace je nutná podpora protokolu **TLS verze 1.2**.

1.1.2. Testovací prostředí

Při přístupu na veřejné testovací prostředí se pro zde uvedené služby používá URL ve tvaru `https://ws1.czebox.cz/DS/DsManage`.

1.2. Reakce při plánované odstávce

V době plánovaných odstávek systém neodpovídá na požadavky webových služeb. Místo toho se vrací následující statická odpověď:

```
HTTP/1.1 503 Service Temporarily Unavailable
Date: Thu, 21 Oct 2010 08:53:55 GMT
Accept-Ranges: bytes
```

1.3. Chybové stránky

V případě zadání špatných (neplatných) přístupových údajů vrací komponenta na vstupu do ISDS HTML text:

Authentication required!

```
This server could not verify that you are authorized to access the URL
"/DS/df". You either supplied the wrong credentials (e.g., bad
password), or your browser doesn't understand how to supply the
credentials required.

In case you are allowed to request the document, please check your
user-id and password and try again.
```

Error 401

V případě, že přístup je dočasně blokován (Nx zadána špatná kombinace přístupových údajů), je vrácen HTML text obsahující údaj, kdy bude blokování ukončeno (doba blokování se různí podle opakování a intenzity):

Authentication required!

```
This server could not verify that you are authorized to access the URL
"/DS/df".

Prihlaseni blokovano do / Login blocked until: 13:04:39

In case you are allowed to request the document, please check your
user-id and password and try again.
```

Error 401

Průběžně se vyhodnocují pokusy o přihlašování z různých hledisek a v případě podezření na útok nebo hádání přístupových hesel dochází k časově omezenému blokování, obvykle výchozí IP adresy. Volání WS v takovém případě končí HTTP chybou 401. Více informací o konkrétním případu blokování získáte na Infolince 954 200 200.

V případě, že přístup je zakázán z důvodu blokace IP adresy, je vrácen HTML text:

Authentication required!

```
This server could not verify that you are authorized to access the URL
"/DS/df".

In case you are allowed to request the document, please check your
user-id and password and try again.
```

Error 401

1.4. Typy schránkových uživatelů

Ve službě pro vrácení seznamu uživatelů schránky se používají identifikátory typů uživatelů dle následující tabulky.

Hodnoty ve sloupci **Označ**. jsou hodnoty, které vrací rozhraní ExtIS v elementu `userType` (ExtIS = přístupová brána pro externí aplikace).

Identifikátor	Popis	Označ.
PRIMARY_USER	Primárně oprávněná osoba, u FO a PFO jen jedna (vlastník DS), u OVM jen jeden vedoucí nebo více statutárů (např.	S

	komory), u PO jeden nebo více statutárních zástupců.	
ENTRUSTED_USER	Pověřený uživatel s omezeným oprávněním. Lze přidávat ke každému typu DS dle § 8 odst. 6	P
ADMINISTRATOR	Administrátor dle § 8 odst. 7	A
LIQUIDATOR	Likvidátor společnosti (u PO nebo OVM), má stejná neměnná maximální práva jako PRIMARY_USER	L
GUARDIAN	Opatrovník právnické osoby - soudem určená osoba podle § 486 zákona č. 89/2012 Sb. (OZ) se stejnými právy a povinnostmi jako statutární orgán, má stejná neměnná maximální práva jako PRIMARY_USER	G
RECEIVER	Nucený správce - nahrazuje statutární orgán a přebírá jeho práva a povinnosti; jen v zákonech vyjmenovaných situacích (banky, pojišťovny apod.), má stejná neměnná maximální práva jako PRIMARY_USER	R

Webové služby pro manipulaci se zprávami pracují jen s obecnějšími rolemi, nerozlišují mezi statutárem, likvidátorem, opatrovníkem PO a nuceným správcem – vše je `PRIMARY_USER`.

1.5. Expirace hesla

Uživatelé schránek si mohou v Nastavení svého účtu zvolit devadesáti denní expiraci (vypršení) hesla. Týká se to uživatelů přistupujících do schránky pomocí jména a hesla nebo pomocí jména, hesla a klientského certifikátu.

Pokud uživatel nechá heslo expirovat, nemá uživatel možnost se přihlásit pomocí rozhraní webových služeb, může však se přihlásit na klientský portál ISDS, kde je mu umožněno heslo změnit.

Vývojář aplikace se o termínu expirace dozví pomocí WS **GetPasswordInfo** a heslo může včas změnit pomocí WS **ChangeISDSPassword**.

1.6. Získání informací o schránce přihlášeného uživatele

Operace: **GetOwnerInfoFromLogin2**

Vstup:

- prázdný řetězec v elementu `dbDummy`.

Výstup:

- ID DS, typ DS a údaje o majiteli DS ve struktuře `tDbOwnerInfo`,
- výsledek operace.

Popis:

Služba dovoluje získat informace o schránce, do níž je přihlášená osoba, pod jejímž účtem se tato služba volá. Údaje o schránce a údaje o uživateli se mohou u některých typů schránek překrývat. Popis údajů ve struktuře `tDbOwnerInfo` je v dokumentaci o webových službách pro vyhledávání (u služby **FindDataBox2**). Použití není omezeno právy, protože se týká jen účtu přihlášeného uživatele oprávněného k přístupu do DS.

Z důvodu ochrany osobních údajů držitele schránky je omezena množina údajů ze struktury `tDbOwnerInfo`, vracených touto službou. Pokud službu volá pověřená osoba nebo administrátor u schránky typu FO nebo PFO, nevrátí se tyto osobní údaje majitele DS: datum narození (`biDate`), místo narození (`biCity`), okres narození (`biCounty`), stát narození (`biState`) a státní občanství u DS typu FO a PFO (`nationality`).

`aifoIsds` je příznak u schránek, kde je držitelem fyzická osoba (FO, PFO, PFO podtypy (profesní), OVM_FO, OVM_PFO), je-li tato osoba ztotožněna s daty v centrálním Registru osob (ROB). Taková osoba má svá referenční data synchronizována se Základními registry.

Údaj v poli `dbIdOVM` se vrací jen pro schránky typu OVM a jejich podtypy. Pro OVM_REQ (aditivní, podřízená) má `dbIdOVM` význam interního kódu pro editorskou aplikaci, ve všech ostatních OVM schránkách jde o identifikátor OVM ze základního registru RPP (unikátní klíč pro Rejstřík OVM)

V ostatních případech se vrací všechny údaje (i při přístupu aplikace pomocí serverového certifikátu).

1.7. Získání informací o přihlášeném uživateli

Operace: **GetUserInfoFromLogin2**

Vstup:

- prázdný řetězec v elementu `dbDummy`.

Výstup:

- ID uživatele, typ uživatele a další údaje o uživateli,
- výsledek operace.

Popis:

Služba dovoluje získat informace o uživateli ISDS, který volá tuto službu. Údaje o schránce získané pomocí **GetOwnerInfoFromLogin2** a údaje o uživateli se mohou u některých typů schránek překrývat.

Popis údajů o uživateli schránky pro různé typy schránek:

	FO	PFO	PO	OVM
`aifoIsds`	Příznak ztotožnění uživatele (fyzické osoby) s ROB, referenční údaje ztotožněné osoby jsou synchronizovány s Registrem obyvatel			
`pnGivenNames`	Jména (první a další) uživatele			
`pnLastName`	Příjmení uživatele			
`adCode`	Kód adresního místa z RUIAN, je-li znám			
`adCity`	Adresa [1] – obec			
`adDistrict`	Adresa – část obce			
`adStreet`	Adresa – ulice			
`adNumberInStreet`	Adresa – č. orientační			
`adNumberInMunicipality`	Adresa – č. popisné (začíná-li „e", jedná se o číslo evidenční)			
`adZipCode`	Adresa – PSČ			
`adState`	Adresa – stát			
`biDate`	Datum narození osoby, je-li známo			

isdsID	Unikátní ID uživatele ISDS	
userType	ENTRUSTED_USER, ADMINISTRATOR, PRIMARY_USER, LIQUIDATOR, GUARDIAN, RECEIVER (viz kap. 1.4)	
userPrivils	Přidělená práva 0-255	
ic	X	IČ společnosti [2)]
firmName	X	název společnosti [2)]
caStreet	Nepovinná adresa *kontaktní* – ulice a číslo	
caCity	Adresa *kontaktní* – město	
caZipCode	Adresa *kontaktní* – PSČ	
caState (nepovinný element)	Adresa *kontaktní* – stát, není-li element v odpovědi nebo je prázdný, jedná se o stát ČR	

[1)] U FO se jedná o adresu bydliště z ROB, u PFO se jedná o adresu sídla PFO, u PO a OVM jde o adresu pobytu uživatele hlášenou obvykle z externího registru (ROS, ROVM, ROB).

[2)] v datech z ROS mohou jako Primární oprávněné osoby (statutární zástupci, likvidátoři, opatrovníci PO) vystupovat i jiné právnické osoby. ISDS proto zavedla koncept Nepřímých uživatelů – oprávněných osob, jejichž vztah k DS plyne nepřímo přes jinou PO – a tato jiná PO je u nepřímého uživatele zaznamenaná v polích ic a firmName.

Pokud přijde z ROS adresa či jméno v nestrukturovaném tvaru, bude celé jméno vráceno v poli pro příjmení (pnLastName) a celá adresa v poli pro obec (adCity).

Službu má smysl použít jen v případě přístupu pomocí jména a hesla (resp. jména a hesla a klientského certifikátu), ne v případě přístupu do schránky pomocí serverového certifikátu, protože takový přístup (virtuální uživatel) nemá odpovídající záznam v evidenci uživatelů (vrátí se chyba č. 2102). Nelze použít pro interního uživatele (vrátí se chyba č. 2103).

Použití není omezeno právy, protože se týká jen účtu přihlášeného uživatele oprávněného k přístupu do DS.

Ukázka odpovědi:

```
      <p:GetUserInfoFromLoginResponse xmlns:p="http://isds.czechpoint.cz/v30"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
         <p:dbUserInfo>
            <p:aifoIsds>false</p:aifoIsds>
            <p:pnGivenNames>Jan Petr</p:pnGivenNames>
            <p:pnLastName>Šmída</p:pnLastName>
            <p:adCode>54879887</p:adCode>
            <p:adCity>Náchod</p:adCity>
            <p:adDistrict>Staré Město</p:adCity>
            <p:adStreet>Pražská</p:adStreet>
            <p:adNumberInStreet xsi:nil="true"/>
            <p:adNumberInMunicipality>139</p:adNumberInMunicipality>
            <p:adZipCode>54900</p:adZipCode>
            <p:adState>CZ</p:adState>
            <p:biDate>1967-01-07</p:biDate>
            <p:isdsID>DS_wexphsydx</p:isdsID>
            <p:userType>PRIMARY_USER</p:userType>
            <p:userPrivils>255</p:userPrivils>
            <p:ic xsi:nil="true"/>
            <p:firmName xsi:nil="true"/>
            <p:caStreet>Korunní 123</p:caStreet>
            <p:caCity>Praha 2</p:caCity>
            <p:caZipCode>12000</p:caZipCode>
            <p:caState>CZ</p:caState>
         </p:dbUserInfo>
         <p:dbStatus>
            <p:dbStatusCode>0000</p:dbStatusCode>
```

```
            <p:dbStatusMessage>Provedeno úspěšně.</p:dbStatusMessage>
         </p:dbStatus>
      </p:GetUserInfoFromLoginResponse>
```

1.8. Získání informace o expiraci hesla

Operace: **GetPasswordInfo**

Vstup:

- prázdný řetězec v elementu `dbDummy`.

Výstup:

- datum a čas expirace hesla v elementu `pswExpDate`,
- výsledek operace.

Popis:

Přístupová hesla k datovým schránkám jednotlivých uživatelů mohou volitelně expirovat po 90 dnech. Pomocí této WS se automaticky se přihlašující systémy mohou dozvědět toto datum a heslo změnit pomocí WS **ChangeISDSPassword** dříve, než k expiraci dojde.

Službu má smysl použít jen v případě, kdy se systém přihlašuje pomocí jména a hesla (a případně klientského certifikátu), ne v případě přístupu aplikace pomocí serverového certifikátu.

Pokud heslo neexpiruje, vrací se NIL hodnota.

Ukázka odpovědi:

Heslo podle odpovědi vyexpiruje 6. 7. 2011 v 13:33:39 místního času.

```
<p:GetPasswordInfoResponse xmlns:p="http://isds.czechpoint.cz/v20"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <p:pswExpDate>2011-07-06T13:33:39.000+02:00</p:pswExpDate>
  <p:dbStatus>
    <p:dbStatusCode>0000</p:dbStatusCode>
    <p:dbStatusMessage>Provedeno úspěšně.</p:dbStatusMessage>
  </p:dbStatus>
</p:GetPasswordInfoResponse>
```

1.9. Změna hesla

Operace: **ChangeISDSPassword**

Vstup:

- původní (staré, ale dosud platné) heslo v elementu `dbOldPassword`,
- nové heslo v elementu `dbNewPassword`.

Výstup:

- výsledek operace.

Popis:

Služba umožňuje změnit přístupové heslo přihlášeného uživatele k datové schránce. Zadané staré heslo se porovná s aktuálním, a pokud je shodné, přepíše se novým heslem.

Není určeno pro změnu hesla účtu s aktivním OTP přihlašováním! Pro tento účel použije WS **ChangePasswordOTP** popsanou v dokumentu *OTP_autentizace.pdf*.

Pravidla pro vytvoření hesla jsou daná vyhláškou MV (a ještě zpřísněna) a jsou shodná s vytvářením hesel na Portálu ISDS:

1. Heslo do datové schránky musí být minimálně 8 a maximálně 64 znaků dlouhé.
2. Heslo musí obsahovat minimálně jedno velké písmeno, jedno malé písmeno a jedno číslo. Povolené znaky jsou písmena (a-z, A-Z), číslice (0-9) a speciální znaky (mezera ! # $ % & ( ) * + , - . : = ? @ [ ] _ { | } ~).
3. Nesmí obsahovat id (login) uživatele, jemuž se heslo mění.
4. V hesle se nesmí opakovat za sebou 3 a více stejných znaků.
5. Heslo nesmí začínat na „qwert", „asdgf", „12345".
6. Není povoleno heslo shodné s jedním z posledních použitých 255 hesel.

Služba vrací stav 0000 při úspěšné změně hesla, různé chybové stavy při rozpoznání nesprávného vstupu:

1066	Délka hesla musí být mezi 8 a 64 znaky (pravidlo 1).
1067	Nové heslo nesmí být stejné jako staré (pravidlo 6).
1079	Heslo nesmí obsahovat znak <znak> (pravidlo 2)
1080	Nové heslo musí obsahovat alespoň jedno velké písmeno, malé písmeno i číslici (pravidlo 2).
1081	Trojí opakování stejného znaku není dovoleno (pravidlo 4).
1082	Nové heslo nesmí obsahovat ID uživatele (pravidlo 3).
1083	Nové heslo nesmí mít takto triviální tvar (pravidlo 5).
1090	Zadané staré heslo není aktuálně platné
1091	Zadané nové heslo bylo již v minulosti použito (pravidlo 6)

V případě neočekávané chyby při zápisu hesla se může vrátit obecná chyba LDAP 9204.

Službu má smysl použít jen v případě přístupu pomocí jména a hesla (a případně klientského certifikátu), ne v případě přístupu aplikace pomocí serverového certifikátu.

Upozornění: při změně hesla je možné stávající relaci dokončit s heslem původním, přihlášení novým je v důsledku replikací v infrastruktuře možné nejprve za cca 15 vteřin.