Datové schránky

Podpora autentizace Mobilním klíčem v rozhraní WS v ISDS

Vytvořeno dne: 25.4.2019
Aktualizováno: 07.05.2019
Verze: 1.1
Klasifikace: Veřejný dokument

Obsah

1 Úvod

Tento dokument popisuje, jak se mohou externí aplikace, využívající rozhraní webových služeb, přihlašovat do schránky ISDS pomocí **Mobilního klíče**, způsobu přihlašování zavedeného v létě 2019.

1.1 Použité zkratky

Zkratka	Význam
ATS	Aplikace třetí strany, externí aplikace, která se chce přihlašovat do ISDS
MK	Mobilní klíč
WS	webové služby (SOAP)

1.2 Definice hostname pro prostředí ISDS

Název	Adresa prostředí
Veřejný test	`www.czebox.cz`
Produkce	`www.mojedatovaschranka.cz`

2 Autentizace pomocí Mobilního klíče

Externí aplikace třetích strany (ATS) musí v prvním kroku projít autentizačním mechanismem pro získání autentizační cookie (přitom dojde k potvrzení přihlášení pomocí Mobilního klíče uživatelem) a poté pomocí této cookie odesílá potřebná data. Na konci relace volá ATS službu pro zneplatnění obdržené cookie. Při nečinnosti delší než 30 minut bude relace přerušena (cookie zneplatněna).

Webové služby ISDS pro aplikace třetích stran jsou dostupné na adrese

```
https://<adresa_prostředí>/apps/DS/<endpoint_webové_služby>
```

Pro text v hlavičkách `X-Response-message-text` je použita znaková sada UTF-8 a hodnota v hlavičce je kódována podle RFC 822 / RFC 2047 (`http://www.ietf.org/rfc/rfc2047.txt`), kde je použita metoda B (base64 enkódování). Pokud text přesahuje 70 znaků, je rozdělen do více bloků – viz příklad:

```
X-Response-message-text: =?UTF-
8?B?SmVkbm9yw6F6b3bDvSBrw7NkIG5lbW9obCBiw710IHphc2w=?= =?UTF-
8?B?w6FuLiBaa3VzdGUgdG8sIHByb3PDrW0sIHBvemTEm2ppLg==?=
```

Při každém požadavku by měla aplikace zasílat svoji jedinečnou identifikaci v hlavičce `User-agent`, aby bylo možné v případě hledání v logu snadno odlišit požadavky jedné ATS od jiných - viz příklad:

```
User-agent: Email connector 1.0
```

Kompletní ukázkový příklad v jazyce JAVA je k dispozici na vývojářském webu https://team.smartadministration.cz v sekci *Testovací prostředí* > *Dokumentace a formuláře*.

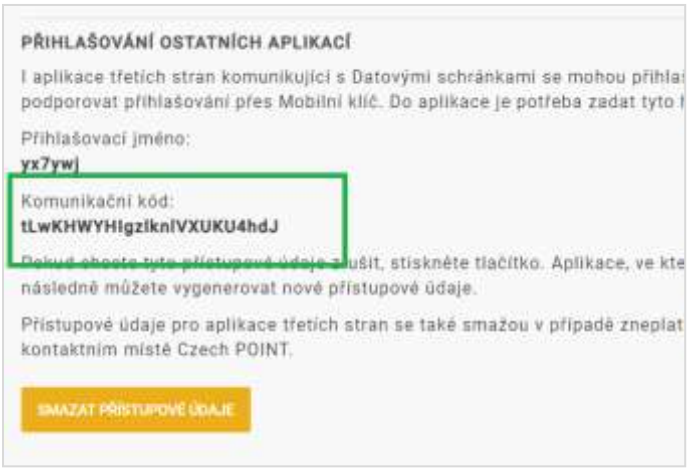
2.1 Postup

1) V prostředí klientského portálu ISDS (https://www.mojedatovaschranka.cz) je třeba pro účet, jenž bude používán pro toto přihlašování, aktivovat Mobilní klíč a poté pro tento účet vygenerovat tzv. komunikační kód. Podrobnosti v kap. 2.1.1.
2) ATS zasílá POST požadavek s basic autentizací, v níž je použito uživatelské jméno k účtu a komunikační kód jako heslo. Podrobnosti v kap. 2.1.2.
3) Systém ISDS vrací odpověď, je získána pracovní S-COOKIE. Podrobnosti v kap. 2.1.3.
4) Aplikace Mobilní klíč obdrží PUSH notifikaci a vyžádá si od uživatele potvrzení přihlášení.
5) ATS periodicky kontroluje stav přihlášení pomocí získané S-COOKIE. Podrobnosti v kap. 2.1.4
6) Po získání potvrzení o přihlášení pomocí Mobilního klíče se zasílá POST požadavek s basic autentizací - stejně jako v bodě 2 (uživatelské jméno a komunikační kód jako heslo) + je přidána S-cookie. Podrobnosti v kap. 2.1.5.
7) V odpovědi ATS získá autentizační cookie IPCZ-X-COOKIE. Tato cookie slouží k autentizaci při volání webových služeb a má platnost 30 minut. Podrobnosti v kap. 2.1.6.
8) ATS další komunikaci, již pomocí standardních WS z rozhraní ISDS, provádí s pomocí získané IPCZ-X-COOKIE na adrese `https://<adresa_prostředí>/apps/DS/<endpoint_webové_služby>`
9) Po ukončení komunikace ATS volá službu pro zneplatnění IPCZ-X-COOKIE podle kapitoly 2.1.7

2.1.1 Registrace MK a získání komunikačního kódu

Nutným předpokladem pro použití MK při přihlášení do ISDS přes WS je úspěšná registrace MK k účtu v ISDS. Registrace se provádí v prostředí klientského portálu ISDS, stránka **Nastavení > Možnosti přihlášení > Přihlášení mobilním klíčem**. Postupujte dle návodu na stránce nebo v nápovědě portálu.

Po ověření funkčnosti MK přihlášením do portálu ISDS, si na výše uvedené stránce vygenerujte *komunikační kód* stisknutím tlačítka **Vygenerovat přístupové údaje**. Tento kód si poznamenejte.



Obrázek 1 - získání komunikačního kódu v Nastavení portálu

2.1.2 První POST požadavek

Získání S-cookie a vynucení přihlášení MK uživatelem proběhne po odeslání POST požadavku na adresu:

```
https://[adresa_prostredi]/as/processLogin?type=mep-ws&
applicationName=[jmeno_aplikace]&
uri=https://[adresa_prostredi]/apps/DS/[endpoint_webove_sluzby]
```

Tato služba je zabezpečena Basic autentizací, tj. v požadavku musí být zaslána hlavička v tomto tvaru `hodnotaA:hodnotaB`, zakódována do Base64.

`HodnotaA` je tvořena uživatelským jménem.

`HodnotaB` je tvořena komunikačním kódem.

`jmeno_aplikace` se předá do PUSH notifikace, aby uživatel věděl, k čemu se přihlašuje (jaké aplikaci povoluje přístup do své schránky).

2.1.3 Odpověď z ISDS

Pokud autentizace podle komunikačního kódu proběhla úspěšně, pak se vrací HTTP status 302 a redirect na url

```
https://[adresa_prostredi]/as/mepWsStateUpdate
```

a hlavička s S-COOKIE:

```
Set-Cookie:S-COOKIE=.....;
```

Pokud autentizace proběhla neúspěšně, pak se vrací HTTP status 401.

2.1.4 Periodická kontrola přihlášení

V této fázi ATS musí čekat, než uživatel na svém mobilním zařízení potvrdí přihlášení. PUSH notifikace (obsahující název aplikace, v detailu pak název schránky a jméno uživatele) zajistí spuštění aplikace a potvrzení.

Obrázek 2 - vzhled notifikace v liště

Aplikace periodicky (např. každou vteřinu) kontroluje status přihlašování na adrese: `https://[adresa_prostredi]/as/mepWsStateUpdate` s S-COOKIE získanou v předchozím kroku.

Možné hodnoty odpovědi (v těle odpovědi):

- "-1": request nerozpoznán (chyba)
- "1": zatím nepotvrzený požadavek / čeká se na potvrzeni v MEP
- "2": požadavek potvrzený
- "3": požadavku vypršela platnost (exspirovaný)

Pouze stav 2 znamená, že se uživatel přihlásil.

2.1.5 Druhý POST požadavek

Po získání stavu 2 v předchozím kroku je nutno odeslat znovu POST požadavek na adresu

```
https://[adresa_prostredi]/as/processLogin?type=mep-ws&
applicationName=[jmeno_aplikace]&
uri=https://[adresa_prostredi]/apps/DS/[endpoint_webove_sluzby]
```

Je použita Basic autentizace, shodná s prvním POST požadavkem (kap. 2.1.2) a je předána S-COOKIE.

2.1.6 Odpověď

V případě úspěchu se vrací vrátí HTTP status 302 a autentizační IPCZ-X-COOKIE

```
Set-Cookie:IPCZ-X-COOKIE=.......;
```

Tato cookie slouží k autentizaci pro následné volání webových služeb a má platnost 30 minut.

2.1.7 Zneplatnění cookie

Zneplatnění autentizační cookie probíhá zasláním GET požadavku na adresu

`https://<adresa_prostředí>/as/processLogout?uri=https://<adresa_prostredi>/apps/DS/<endpoint_webové_služby>`