



Datové schránky

Podpora OTP autentizace v ISDS

Vytvořeno dne: 22.4.2011

Aktualizováno: 06.06.2019

Verze: 1.8

Klasifikace: Veřejný dokument

Obsah

| | | |
|----------|--|----------|
| 1 | Úvod | 3 |
| 1.1 | Zkratky a definice..... | 3 |
| 1.2 | Definice hostname pro prostředí ISDS | 3 |
| 2 | OTP autentizace..... | 3 |
| 2.1 | Autentizace pomocí HOTP | 4 |
| 2.1.1 | Autentizace | 4 |
| 2.1.1.1 | Žádost (request) | 4 |
| 2.1.1.2 | Odpověď (response) | 4 |
| 2.2 | Autentizace pomocí TOTP..... | 5 |
| 2.2.1 | Zaslání SMS | 5 |
| 2.2.1.1 | Žádost (request) | 5 |
| 2.2.1.2 | Odpověď (response) | 6 |
| 2.2.2 | Autentizace | 6 |
| 2.2.2.1 | Žádost (request) | 6 |
| 2.2.2.2 | Odpověď (response) | 7 |
| 2.3 | Zneplatnění cookie | 7 |
| 3 | Webová služba pro změnu hesla | 7 |
| 3.1 | Komu je služba určena | 7 |
| 3.1.1 | URL pro přístup | 8 |
| 3.2 | Změna hesla..... | 8 |
| 3.3 | Zaslání SMS kódu | 9 |

1 Úvod

Tento dokument popisuje podporu pro práci s datovými zprávami v případě, že používaný uživatelský účet má aktivovaný jeden z nadstandardních typů přihlašování - OTP autentizací ve variantě SMS kód nebo Bezpečnostní kód (HOTP).

V ISDS od léta 2019 se nepovažuje HOTP kód jako bezpečný a nadále nebude podporován. Aplikace, které jej podporují pro nějaký účet, nastavený dříve, budou i nadále (do odvolání) funkční. Nové HOTP registrace však již nejde nastavit.

Zde popisovaný programový způsob přístupu k ISDS je doporučeno použít pouze v případě, že zadávání autentizačních údajů (SMS nebo bezpečnostní kód) je prováděné v aplikaci interaktivně (ručně). Přístup na toto rozhraní je doporučen pro jednu instanci aplikace maximálně 1x za cca několik minut (tedy není vhodné, aby aplikace s využitím softwarového generátoru bezpečnostních klíčů tímto způsobem autentizovala každý požadavek).

Cílem je umožnit vývojářům klientských interaktivních aplikací (typu doplňku do emailových klientů) stejnou funkcionalitu, jakou nabízí klientský Portál ISDS.

1.1 Zkratky a definice

| Zkratka | Význam |
|---------|---|
| AGW | Access Gateway |
| OTP | One time password |
| HOTP | HMAC-Based One time password algorithm. K přihlášení je použit bezpečnostní kód ze specializované aplikace. |
| TOTP | Time-based One time password. K přihlášení je použit kód z příchozí SMS. |
| ISDS | Informační systém datových schránek |
| ATS | Aplikace třetích stran |

1.2 Definice hostname pro prostředí ISDS

| Název | Adresa prostředí |
|--------------|---------------------------|
| Veřejný test | www.czebox.cz |
| Produkce | www.mojedatovaschranka.cz |

2 OTP autentizace

Aplikace třetích stran musí v prvním kroku projít autentizačním mechanismem pro získání autentizační cookie a poté pomocí této cookie odesílá potřebná data. Na konci relace volá aplikace třetích stran službu pro zneplatnění obdržené cookie. Při nečinnosti delší než 30 minut bude relace přerušena (cookie zneplatněna).

Webové služby ISDS aplikace třetích stran budou dostupné na nové 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 problémů kontaktovat autory - viz příklad:

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

2.1 Autentizace pomocí HOTP

- 1) Uživatel si podle svého uvážení v ATS vybere typ autentizace, kterým je zabezpečena požadovaná datová schránka.
- 2) ATS zasílá POST požadavek bez autentizačních údajů na uvedenou adresu v kapitole 2.1.1.1
- 3) Systém ISDS vrací odpověď podle kapitoly 2.1.1.2
- 4) Požadavek není autentizován a služba vrací v návratové hlavičce WWW-Authenticate: hotp požadovanou metodu autentizace a vyzve uživatele k zadání autentizačních údajů: uživatelské jméno, heslo a HOTP kód. ATS zasílá tyto údaje podle kapitoly 2.1.1.1
- 5) Systém ISDS provede autentizaci a vrací odpověď podle kapitoly 2.1.1.2
- 6) ATS zpracuje odpověď a další komunikaci provádí na webové služby s pomocí získané IPCZ-X-COOKIE na adrese
`https://<adresa_prostředí>/apps/DS/<endpoint_webové_služby>`
- 7) Po ukončení komunikace ATS volá službu pro zneplatnění IPCZ-X-COOKIE podle kapitoly 5

2.1.1 Autentizace

2.1.1.1 Žádost (request)

Autentizace probíhá odesláním POST požadavku na adresu:

```
https://<adresa_prostředí>/as/processLogin?type=hotp&uri=https://<adresa_prostředí>/apps/DS/<endpoint_webové_služby>
```

Tato služba je zabezpečena zmodifikovanou Basic autentizací, tj. v požadavku musí být zaslána hlavička v tomto tvaru **hodnotaA:hodnotaB** a zakódován metodou Base64.

HodnotaA je tvořena z uživatelského jména.

HodnotaB je tvořena řetězcem, který je složen z hesla uživatele a HOTP kódem.

2.1.1.2 Odpověď (response)

Autentizace proběhla úspěšně:

Služba vrací HTTP status 302 Found a tyto hlavičky:

```
Set-Cookie: IPCZ-X-COOKIE=01-5c1047cb9f3545f68cf987e6750acac4;  
Domain=.mojedatovaschranka.cz; secure, HttpOnly  
Location: https://<adresa_prostředí>/apps/DS/<endpoint_webové_služby>
```

Autentizace proběhla neúspěšně:

Služba vrací HTTP status 401 Unauthorized a tyto hlavičky:

WWW-Authenticate: hotp

X-Response-message-code: authentication.error.userIsNotAuthenticated

X-Response-message-text: =?UTF-

8?B?Q2h5YmEgcMWZaWhsw6HFoWVuw60sIHpub3Z1IHphZGVqdGUgw7pkYWplLg==?=

| X-Response-message-code | X-Response-message-text |
|---|--|
| authentication.error.userIsNotAuthenticated | Chyba přihlášení, znovu zadejte údaje. |
| authentication.error.intruderDetected | Váš přístup byl na 60 minut zablokován. |
| authentication.error.passwordExpired | Platnost Vašeho hesla skončila. |
| authentication.error.badRole | Pro přístup na požadovanou stránku nemá Váš účet potřebné oprávnění. |

2.2 Autentizace pomocí TOTP

- 1) Uživatel si v ATS vybere typ autentizace, kterým je zabezpečena požadovaná datová schránka.
- 2) ATS zasílá POST požadavek bez autentizačních údajů na uvedenou adresu v kapitole 2.2.1.1
- 3) Systém ISDS vrací odpověď podle kapitoly 2.2.1.2
- 4) Požadavek není autentizován a služba vrací v návratové hlavičce `WWW-Authenticate: totpsendsms` požadovanou metodu autentizace a vyzve uživatele k zadání autentizačních údajů: uživatelské jméno, heslo a tlačítko pro odeslání SMS. ATS zasílá tyto údaje podle kapitoly 2.2.1.1
- 5) Systém ISDS provede ověření uživatelského jména a hesla a zašle Premium SMS na telefonní číslo uvedené u uživatelského účtu a vrací odpověď ve tvaru podle kapitoly 2.2.1.2.
- 6) ATS vyzve uživatele k zadání kódu z obdržené SMS. Uživatel vyplní pole pro SMS kód. ATS odesílá uživatelské jméno, heslo a SMS kód podle kapitoly 2.2.2.1
- 7) Systém ISDS provede autentizaci a vrací odpověď podle kapitoly 2.2.2.2
- 8) ATS zpracuje odpověď a další komunikaci provádí na webové služby s pomocí získané IPCZ-X-COOKIE na adresu
`https://<adresa_prostředí>/apps/DS/<endpoint_webové_služby>`
- 9) Po ukončení komunikace formulář volá službu pro zneplatnění IPCZ-X-COOKIE podle kapitoly 2.3

2.2.1 Zaslání SMS

2.2.1.1 Žádost (request)

Žádost o odeslání SMS probíhá odesláním POST požadavku na adresu

`https://<adresa_prostředí>/as/processLogin?type=totp&sendSms=true&uri=https://<adresa_prostředí>/apps/DS/<endpoint_webové_služby>`

Tato služba je zabezpečena Basic autentizací, tj. v požadavku musí být zaslána hlavička v tomto tvaru **hodnotaA:hodnotaB** a zakódován metodou Base64.

HodnotaA je tvořena z uživatelského jména.

HodnotaB je tvořena z hesla uživatele.

2.2.1.2 Odpověď (response)

Autentizace proběhla úspěšně a SMS byla odeslána:

Služba vrací HTTP status 302 Found a tyto hlavičky:

X-Response-message-code: authentication.info.totpSended

X-Response-message-text: =?UTF-

8?B?SmVkbm9yw6F6b3bDvSBrw7NkIG9kZXNsw6FuLg==?=

Location:

https://<adresa_prostředí>/as/processLogin?type=otp&uri=https://<adresa_prostředí>/apps/DS/<endpoint_webové_služby>

| X-Response-message-code | X-Response-message-text |
|--------------------------------|--------------------------|
| authentication.info.totpSended | Jednorázový kód odeslán. |

Autentizace proběhla neúspěšně nebo SMS se nepodařilo odeslat:

Služba vrací HTTP status 401 Unauthorized a tyto hlavičky:

WWW-Authenticate: totpsendsms

X-Response-message-code: authentication.error.userIsNotAuthenticated

X-Response-message-text: =?UTF-

8?B?Q2h5YmEgcMWZaWhsw6HFoWVuw60sIHpub3Z1IHphZGVqdGUgw7pkYWplLg==?=

| X-Response-message-code | X-Response-message-text |
|---|---|
| authentication.error.userIsNotAuthenticated | Chyba přihlášení, znovu zadejte údaje. |
| authentication.error.intruderDetected | Váš přístup byl na 60 minut zablokován. |
| authentication.error.passwordExpired | Platnost Vašeho hesla skončila. |
| authentication.info.cannotSendQuickly | Jednorázový kód lze poslat jednou za 30 sekund. <i>Pozn.: Časový údaj se může změnit, je závislý na délce nastaveného okna generování TOTP kódů.</i> |
| authentication.error.badRole | Pro přístup na požadovanou stránku nemá Váš účet potřebné oprávnění. |
| authentication.info.totpNotSended | Jednorázový kód nemohl být zaslán. Zkuste to, prosím, později. |

2.2.2 Autentizace

2.2.2.1 Žádost (request)

Autentizace probíhá odesláním POST požadavku na adresu:

`https://<adresa_prostředí>/as/processLogin?type=totp&uri=https://<adresa_prostředí>/apps/DS/<endpoint_webové_služby>`

Tato služba je zabezpečena zmodifikovanou Basic autentizací, tj. v požadavku musí být zaslána hlavička v tomto tvaru **hodnotaA:hodnotaB** a zakódován metodou Base64.

HodnotaA je tvořena z uživatelského jména.

HodnotaB je tvořena řetězcem, který je složen z hesla uživatele a kódem z SMS.

2.2.2.2 Odpověď (response)

Autentizace proběhla úspěšně:

Služba vrací HTTP status 302 Found a tyto hlavičky:

```
Set-Cookie: IPCZ-X-COOKIE=01-5c1047cb9f3545f68cf987e6750acac4;
Domain=.mojedatovaschranka.cz; secure, HttpOnly
Location: https://<adresa_prostředí>/apps/DS/<endpoint_webové_služby>
```

Autentizace proběhla neúspěšně:

Služba vrací HTTP status 401 Unauthorized a tyto hlavičky:

```
WWW-Authenticate: totp
X-Response-message-code: authentication.error.userIsNotAuthenticated
X-Response-message-text: =?UTF-
8?B?Q2h5YmEgcMWZaWhsw6HfOWVuw60sIHpub3ZlIHphZGVqdGUgw7pkYWplLg==?=
```

| X-Response-message-code | X-Response-message-text |
|---|--|
| authentication.error.userIsNotAuthenticated | Chyba přihlášení, znovu zadejte údaje. |
| authentication.error.intruderDetected | Váš přístup byl na 60 minut zablokován. |
| authentication.error.passwordExpired | Platnost Vašeho hesla skončila. |
| authentication.error.badRole | Pro přístup na požadovanou stránku nemá Váš účet potřebné oprávnění. |

2.3 Zneplatnění cookie

Zneplatnění cookie probíhá zasláním GET požadavku na adresu

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

3 Webová služba pro změnu hesla

3.1 Komu je služba určená

Pro změnu hesla účtu zde popisovaného z externí aplikace není možno použít webovou službu **ChangeISDSPassword** popsanou v dokumentu

WS_souvisejici_s_přístupem_do_ISDS.pdf. Místo ní použijte speciální WS nazvanou **ChangePasswordOTP**, která je zpracovávána odlišně a má jiný endpoint. Další pomocnou službou je **SendSMSCode** pro zaslání autentizačního SMS kódu.

Služby jsou definované pomocí souborů `ChangePassword.wsdl` verze 1.0. Použité datové typy jsou definovány souborem `ChangePasswordTypes.xsd`.

Pro provedení požadavku na změnu hesla, je třeba se přihlásit basic autentizací, kdy heslo je složeno s OTP kódem. Postup je podobný jako v kapitole 2.1.1.1 (autentizaci posílejte přímo na endpoint změny hesla). V případě zaregistrovaného přihlašování pomocí SMS je doporučeno TOTP kód možno získat pomocí služby **SendSMSCode**, která provede zaslání kódu na mobilní telefon uživatele.

3.1.1 URL pro přístup

URL pro webové služby je `https://www.mojedatovaschranka.cz/asws/changePassword`.

Při přístupu na veřejné testovací prostředí se pro zde uvedené služby používá URL ve tvaru `https://www.czebox.cz/asws/changePassword`.

3.2 Změna hesla

Operace: **ChangePasswordOTP**

Vstup:

- původní (staré, ale dosud platné) heslo v elementu `dbOldPassword`,
- nové heslo v elementu `dbNewPassword`,
- způsob autentizace v elementu `dbOTPType` (konstanta `HOTP` nebo `TOTP`).

Výstup:

- výsledek operace.

Popis:

Služba umožňuje změnit přístupové heslo přihlášeného uživatele k datové schránce pomocí OTP autentizace (HOTP = bezpečnostním kódem, TOTP = SMS). Zadané staré heslo se porovná s aktuálním, a pokud je shodné, přepíše se novým heslem.

Nelze použít pro změnu hesla účtu přihlašujícího se jménem a heslem nebo jménem heslem spolu s klientským certifikátem.

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 32 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“.

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

| | |
|------|--|
| 1066 | Délka hesla musí být mezi 8 a 32 znaky (pravidlo 1). |
|------|--|

| | |
|------|--|
| 1067 | Nové heslo nesmí být stejné jako staré (pravidlo 6). |
| 1082 | Nové heslo nesmí obsahovat ID uživatele (pravidlo 3). |
| 1083 | Nové heslo nesmí mít takto triviální tvar (pravidlo 5) nebo Heslo nesmí obsahovat znak <znak> (pravidlo 2) nebo Nové heslo musí obsahovat alespoň jedno velké písmeno, malé písmeno i číslici (pravidlo 2) nebo Trojí opakování stejného znaku není dovoleno (pravidlo 4). |
| 2300 | Neočekávaná chyba |

3.3 Zaslání SMS kódu

Operace: **SendSMSCode**

Vstup:

- nic

Výstup:

- výsledek operace.

Popis:

Služba umožňuje nechat si zaslat prémiovou SMS obsahující TOTP přihlašovací kód. Při úspěchu dorazí na telefonní číslo registrované u daného účtu požadovaná SMS s kódem. Kód se použije pro přihlášení k službě na změnu hesla.

Pro přihlášení k této službě není třeba zadávat OTP kód do basic autentizace.

Služba vrací stav 0000 při úspěchu, následující chyby při neúspěchu:

| | |
|------|--|
| 2300 | Neočekávaná chyba |
| 2301 | Jednorázový kód lze poslat jednou za 30 sekund. |
| 2302 | Jednorázový kód nemohl být zaslán. Zkuste to, prosím, později. |