



# Datové schránky

## Odesílací brána ISDS

### Technická specifikace

Vytvořeno dne: 25.1.2016

Aktualizováno: 25.9.2024

Verze: 1.8

Kategorie: Veřejný dokument

## Obsah

|           |   |           |
|-----------|---|-----------|
| <b>1.</b> | <b>Úvod .....</b>   | <b>3</b>  |
| 1.1.      | Cíl dokumentu .....   | 3         |
| 1.2.      | Zkratky a definice.....   | 3         |
| 1.3.      | Poznámky k verzi 1.4 .....  | 4         |
| 1.4.      | Poznámky k verzi 1.7 .....  | 5         |
| 1.5.      | Poznámky k verzi 1.8 .....  | 5         |
| <b>2.</b> | <b>Popis .....</b>  | <b>5</b>  |
| 2.1.      | Odesílací brána (OB) .....  | 5         |
| 2.2.      | Základní pojmy.....   | 5         |
| 2.3.      | Požadavky.....  | 5         |
| 2.4.      | Konfigurace odesílací brány .....                                 | 6         |
| 2.5.      | Požadovaný certifikát.....  | 8         |
| 2.6.      | Využití odesílací brány .....                                     | 8         |
| <b>3.</b> | <b>Aplikace poskytovatele pro využití OB .....</b>                | <b>10</b> |
| 3.1.      | Technické požadavky na Aplikaci poskytovatele .....               | 10        |
| 3.2.      | Popis webové služby pro získání timeLimitedId .....               | 10        |
| 3.2.1.    | Příklad komunikace WS .....                                       | 11        |
| 3.2.2.    | Vysvětlivky .....   | 11        |
| 3.2.3.    | Popis stavů výsledku zpracování .....                             | 11        |
| 3.3.      | Popis webové služby pro vložení VoDZ příloh do konceptu .....     | 12        |
| 3.4.      | Popis webové služby pro uložení konceptu .....                    | 12        |
| 3.5.      | Popis webové služby na ukončení platnosti timeLimitedId .....     | 14        |
| 3.5.1.    | Příklad komunikace WS .....                                       | 14        |
| 3.5.2.    | Popis stavů výsledku zpracování .....                             | 14        |
| 3.6.      | Popis webové služby pro informace o možnostech odesílání PDZ..... | 15        |
| 3.6.1.    | Příklad komunikace WS .....                                       | 16        |
| <b>4.</b> | <b>Seznam předávaných atributů .....</b>                          | <b>17</b> |
| 4.1.      | Speciální atributy .....  | 17        |

# 1. Úvod

## 1.1. Cíl dokumentu

Tento dokument slouží jako zdroj technických informací pro vývojáře externích aplikací, kteří budou připravovat aplikaci poskytovatele a používat popsané rozhraní.

## 1.2. Zkratky a definice

| Zkratka                     | Význam  |
|-----------------------------|---|
| Autentizace                 | Ověření identity uživatele  |
| Autorizace                  | Přidělení přístupových práv uživateli po jeho úspěšné autentizaci   |
| CRL                         | Certificate Revocation List   |
| ISDS                        | Informační systém datových schránek   |
| MV ČR                       | Ministerstvo vnitra ČR  |
| Poskytovatel                | Ten, kdo poskytuje službu, která využívá OB prostřednictvím aplikace poskytovatele.   |
| WS                          | Webové služby na bázi protokolu SOAP v1.1   |
| WSDL                        | Popis rozhraní webové služby  |
| appToken                    | Parametr pro identifikaci, odkud byl uživatel přesměrován na autentizační bránu. Může být uveden současně s přesměrováním v přístupovém URL. V tomto parametru si může aplikace poskytovatele udržet identifikaci, odkud je uživatel přesměrován na login stránku služby v ISDS. Tento parametr bude zpět předán aplikaci poskytovatele za předpokladu, že byl součástí přístupového URL. Tento parametr obsahuje maximálně 20 číslic. <i>appToken</i> bude také vrácen jako součást návratového URL. |
| Uživatel                    | V tomto textu se jedná o uživatele ISDS, který může využívat služby ISDS prostřednictvím aplikace poskytovatele.  |
| [url-adresa-prostředí-isds] | Adresy prostředí:<br>Veřejný test:<br><code>czebox.cz</code><br>Produkční prostředí:<br><code>mojedatovaschranka.cz</code>  |
| OB                          | Odesílací Brána   |
| DS                          | Datová schránka ISDS  |
| DZ                          | Datová zpráva ISDS  |
| ISVS                        | Informační Systém Veřejné Správy  |
| OVM                         | Orgány Veřejné Moci   |
| PDZ                         | Poštovní datová zpráva  |
| VoDZ                        | Velkoobjemová datová zpráva   |

### **1.3. Poznámky k verzi 1.4**

V této verzi dokumentu byly aktualizovány screenshoty a text v kapitole 2.4.

## 1.4. Poznámky k verzi 1.7

Úprava popisu funkčnosti v kapitole 2.4

Pokud provozovatel odesílací brány chce umožnit uživateli v případě chyby nebo vypršení požadavku návrat do své aplikace, musí vyplnit v nastavení odesílací brány URL při chybě.

## 1.5. Poznámky k verzi 1.8

Přidání VoDZ/SetBigConcept

# 2. Popis

## 2.1. Odesílací brána (OB)

Tato služba umožňuje aplikaci poskytovatele předání konceptu DZ do perimetru ISDS, kde tento koncept může autentizovaný uživatel schválit a odeslat. Tato služba je k dispozici všem držitelům datových schránek.

## 2.2. Základní pojmy

Aplikace poskytovatele je libovolná webová aplikace, která implementuje přípravu konceptu DZ pomocí přihlašovacích údajů do ISDS.

ISDS zprostředkuje pro aplikaci poskytovatele službu ISDS zadáním přístupových údajů uživatelem.

Zadání přístupových údajů do ISDS a jejich ověření probíhá v perimetru ISDS. Ověření má stejné metody a úroveň ověření uživatele přistupujícího do aplikace poskytovatele jako při přihlášení do ISDS. Jedná se o následující přístupové údaje, které bude uživatel zadávat:

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

Toto ověřování přístupových údajů je umožněno všem typům uživatelů datové schránky.

Využití odesílací brány není chápáno jako přihlášení do datové schránky ve smyslu zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů v platném znění. Autentizace uživatele tak nezpůsobuje doručení dodaných datových zpráv.

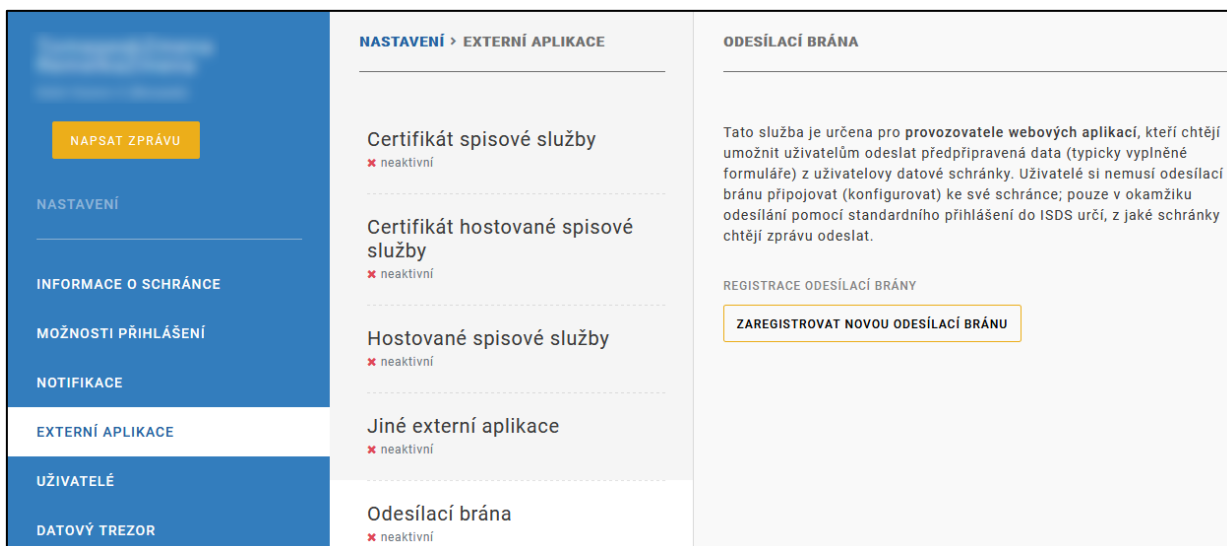
Od 11.9.2016, pokud je už uživatel úspěšně přihlášen do portálu ISDS, není nucen znovu zadávat přihlašovací údaje a je automaticky přihlášen. Před přesměrováním do aplikace poskytovatele je ale upozorněn, že byl automaticky přihlášen a bude po odsouhlasení přesměrován.

## 2.3. Požadavky

Základním požadavkem na poskytovatele je jeho vlastní datová schránka ISDS. K jedné datové schránce je možné zaregistrovat více Aplikací poskytovatele. Konfiguraci odesílací brány může provést samotný držitel schránky.

## 2.4. Konfigurace odesílací brány

Registraci a případnou následnou konfiguraci služby OB může provést kterýkoliv administrátor nebo držitel schránky jakéhokoliv typu (patřící Poskytovateli služby). Toto se provádí na klientském portálu – v sekci „Nastavení“ se v levém menu klikne na položku „Externí aplikace“, napravo od menu se zobrazí nový pruh a v něm se klikne na položku „Odesílací brána“. Nakonec se stiskne tlačítko **Zaregistrovat novou odesílací bránu**.



**Obrázek 1 Zahájení registrace nové odesílací brány**

Během registrace je ke každé službě přiděleno unikátní ID. Konfigurace zahrnuje tyto operace:

- Zadání názvu služby
- Zadání návratového URL
- Zadání URL při chybě – Pokud provozovatel odesílací brány chce umožnit uživateli v případě chyby nebo vypršení požadavku návrat do své aplikace, musí vyplnit v nastavení odesílací brány URL při chybě.
- Nastavení doby platnosti konceptu DZ (doba, po kterou je možné předat koncept DZ do perimetru ISDS ke schválení. Doba začíná běžet zadáním přístupových údajů. Uživatel musí být přesměrován na schválení konceptu DZ před vypršením této doby.
- Vložení certifikátu (v PEM formátu).

Po zadání údajů nové odesílací brány k registraci je nejprve zobrazen čitelný obsah vloženého certifikátu, abyste mohli provést vizuální kontrolu, zda jste zadali správný certifikát. Po opětovném stisku tlačítka **Registrovat** dojde k zaregistrování nové odesílací brány.

Změna konfigurace OB se provádí pomocí následujícího postupu. Nejprve je potřeba zobrazit stránku se seznamem zaregistrovaných odesílacích bran tak, že se klikne na „Nastavení“, v levém menu se klikne na položku „Externí aplikace“, napravo od menu se

## Odesílací brána

zobrazí nový pruh a v něm se klikne na položku „Odesílací brána“. Zobrazí se seznam zaregistrovaných odesílacích bran včetně tlačítka pro zaregistrování nové odesílací brány:

**NASTAVENÍ > EXTERNÍ APLIKACE**

**ODESÍLACÍ BRÁNA**

Tato služba je určena pro provozovatele webových aplikací, kteří chtějí umožnit uživatelům odeslat předpřipravená data (typicky vyplněné formuláře) z uživatelské datové schránky. Uživatelé si nemusí odesílací bránu připojovat (konfigurovat) ke své schránce; pouze v okamžiku odesílání pomocí standardního přihlášení do ISDS určí, z jaké schránky chtějí zprávu odeslat.

REGISTROVANÉ ODESÍLACÍ BRÁNY

| ID služby        | Název služby | Registrace | Stav      |
|------------------|--------------|------------|-----------|
| e8bb01d94cb04... | Testovací OB | OB         | Neaktivní |

REGISTRACE ODESÍLACÍ BRÁNY

**ZAREGISTROVAT NOVOU ODESÍLACÍ BRÁNU**

**Obrázek 2 Seznam existujících odesílacích bran**

Na seznamu registrovaných OB je zobrazeno vygenerované unikátní ID služby, název služby, typ registrace (odesílací brána) a stav. Nakonec se tu nachází odkaz „Možnosti“, pomocí kterého lze stávající OB aktivovat či deaktivovat, editovat a odregistrovat.

Kliknutím na položku „Možnosti“ a vybráním položky „Upravit“ se zobrazí stránka pro editování existující OB:

**NASTAVENÍ > EXTERNÍ APLIKACE**

**ODESÍLACÍ BRÁNA** KROK 1/2

Zadejte parametry budoucí Odesílací brány. Podrobnosti naleznete v Provozním řádu ISDS, a částečně i v [nápoověď](#).

Název služby (povinný)  
Testovací OB

Návratové URL (povinný)  
https://www.test.cz/return-url,

URL při chybě  
www.obchyba.cz

PLATNOST KONCEPTU:  
60 minut

☐ ZAKÁZAT PŘIHLAŠOVÁNÍ PŘES EIDENTITA.CZ (NIA)?

**POKRAČOVAT**

[< ZPĚT](#)

**Obrázek 3 Změna nastavení odesílací brány**

Lze editovat název OB, návratové URL, změnit délku platnosti konceptu a odebrat či přidat certifikát.

### 2.5. Požadovaný certifikát

1. Pro využití služby je nutné použít komerční certifikát vydaný certifikační autoritou provozovanou kvalifikovaným poskytovatelem služeb vytvářejících důvěru 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 ve službě pouze jednou (nelze použít stejný certifikát pro dvě služby).

### 2.6. Využití odesílací brány

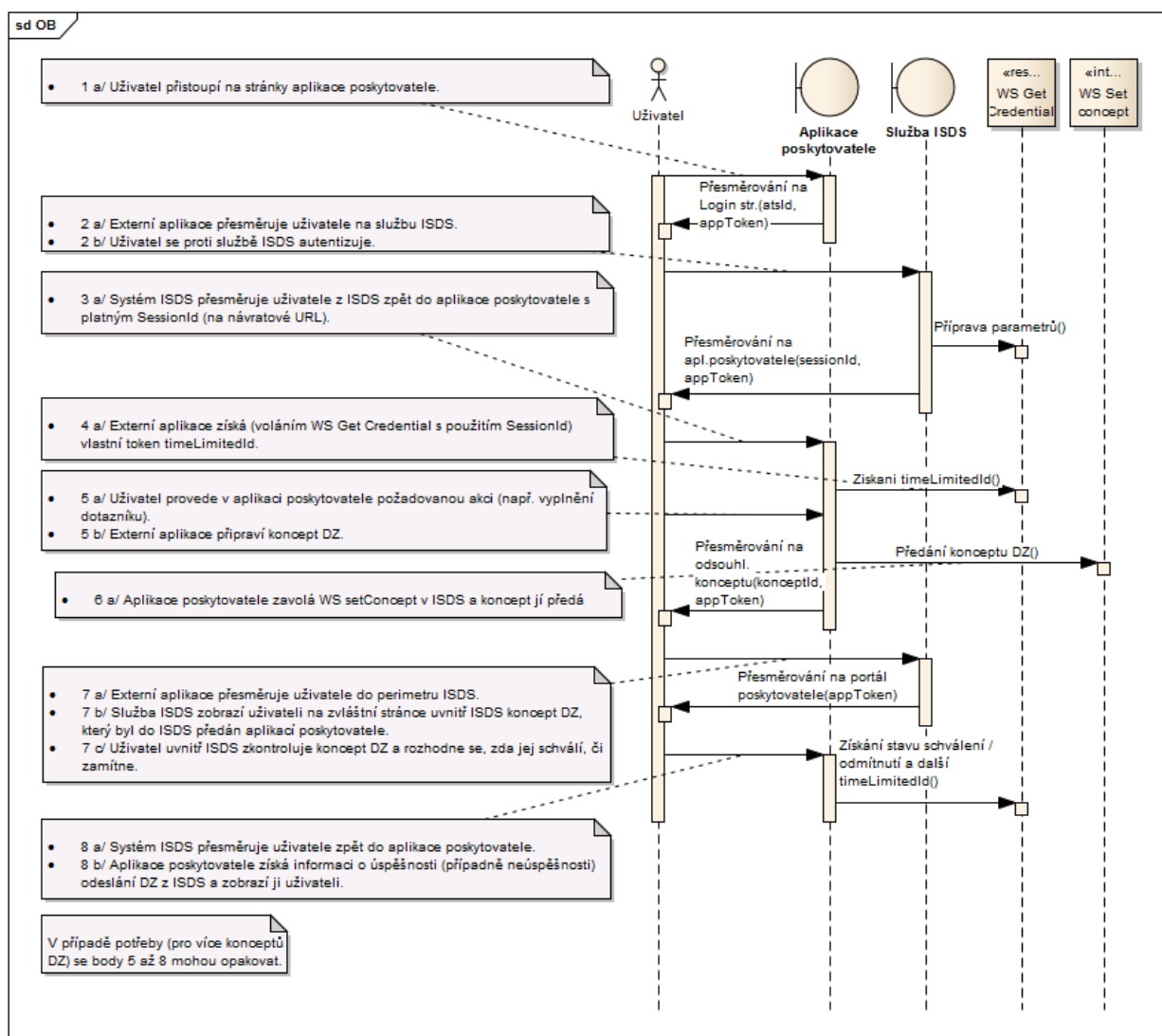
#### Zjednodušený postup:

1. Uživatel přistoupí na stránky aplikace poskytovatele.
2. Aplikace poskytovatele přesměruje uživatele na login stránku služby ISDS. Uživatel zadá své přístupové údaje.
3. Uživatel je přesměrován zpět na stránky aplikace poskytovatele.
4. Aplikace poskytovatele si vyzvedne parametr *timeLimitedId*.
5. Aplikace poskytovatele připraví koncept DZ.
6. Za použití *timeLimitedId* vloží aplikace poskytovatele koncept DZ do ISDS.
7. Aplikace poskytovatele přesměruje uživatele do ISDS ke schválení a odeslání konceptu DZ. Uživatel schválí nebo zamítně odeslání DZ.
8. Systém ISDS přesměruje uživatele zpět do aplikace poskytovatele. Aplikace poskytovatele zjistí stav konceptu (odesláno / zamítnuto).

V případě více různých konceptů je možné body 5 až 8 opakovat.



## Odesílací brána



### Detailní postup:

1. Uživatel vstoupí na webovou stránku aplikace poskytovatele. Uživatel vyjádří potřebu využít funkčnost odesílací brány. Systém provede přesměrování na login stránku služby ISDS. V tomto požadavku aplikace poskytovatele předá službě ISDS unikátní 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 se zobrazí login stránka uživateli. Uživatel je vyzván k zadání svých přístupových údajů, které používá k běžnému přihlášení do ISDS. Uživatel zadá přístupové údaje do 5 minut.

3. Služba ověří vůči identitnímu prostoru ISDS správnost přístupových údajů. V případě neúspěšného ověření přístupových údajů je uživateli zobrazeno upozornění typu „Chyba přihlášení, znovu zadejte údaje.“.

4. V případě úspěšného ověření služba přesměruje uživatele na návratové URL, které je uvedeno v nastavení služby v datové schránce provozovatele. Toto URL, které je plně v režii služby, musí přijímat parametr *sessionId*, který poté služba 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 ze služby ISDS. Se *sessionId* zavolá webovou službu pro získání informací. Získání informací (*timeLimitedId*) z ISDS za pomoci tohoto daného *sessionId* je možné pouze jednou. Zároveň s *sessionId* získá *appToken*, pokud byl autentizačnímu modulu předán v požadavku (viz bod 1).

## 3. Aplikace poskytovatele pro využití OB

### 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 stránku pro příjem *sessionId* podle specifikace uvedené v předcházející kapitole.
3. Požadavky na klienta: aplikace implementuje klientskou část WS podle WSDL specifikace v kapitole 3.2.
4. Aplikace poskytovatele musí pro přístup na WS používat certifikát specifikovaný v kapitole 2.5 Požadovaný certifikát.
5. Konfigurace serveru: Komunikace se službou ISDS probíhá vždy zabezpečeným způsobem přes protokol TLSv1.2. Služba využívá k šifrování komerční serverový certifikát vydaný akreditovanou certifikační autoritou ČR

### 3.2. Popis webové služby pro získání *timeLimitedId*

Aplikace jako klient WS služby ISDS 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/extIs2Endpoint](https://cert.[url-adresa-prostředí-isds]/asws/extIs2Endpoint)

### 3.2.1. Příklad komunikace WS

Příklad: Předání timeLimitedId.

|                 |  |
|-----------------|--|
| <b>Request</b>  | <pre>&lt;SOAP-ENV:Envelope   xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"   SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"&gt;   &lt;SOAP-ENV:Body&gt;     &lt;m:authConfirmationRequest xmlns:m="http://agw-as.cz/ats-ws/v1"&gt;       &lt;m:sessionId&gt;00-c679c0687f2d43ebbcd766876f90da66&lt;/m:sessionId&gt;     &lt;/m:authConfirmationRequest&gt;   &lt;/SOAP-ENV:Body&gt; &lt;/SOAP-ENV:Envelope&gt;</pre>  |
| <b>Response</b> | <pre>&lt;SOAP-ENV:Envelope   xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"   SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"&gt;   &lt;SOAP-ENV:Body&gt;     &lt;m:authConfirmationResponse xmlns:m="http://agw-as.cz/ats-ws/v1"&gt;       &lt;m:status&gt;OK&lt;/m:status&gt;       &lt;m:userRequestIp&gt;192.168.0.1&lt;/m:userRequestIp&gt;       &lt;m:attributes&gt;         &lt;m:attribute name="appToken" value="123"/&gt;         &lt;m:attribute name="timeLimitedId" value=" T01- 7616671e421f4efb8fa1f7bc5b80a913"/&gt;       &lt;/m:attributes&gt;     &lt;/m:authConfirmationResponse&gt;   &lt;/SOAP-ENV:Body&gt; &lt;/SOAP-ENV:Envelope&gt;</pre> |

### 3.2.2. Vysvětlivky

| Hodnota              | Význam   |
|----------------------|--|
| <b>sessionId</b>     | Identifikace session uživatele přihlášeného do Autentizačního modulu. Token získaný po přesměrování v kapitole 2.6, Detailní postup, bod 4.            |
| <b>status</b>        | Strukturovaná informace o výsledku zpracování žádosti.   |
| <b>userRequestIp</b> | IP uživatele při přihlášení.   |
| <b>attribute</b>     | 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   |
|---------------------|--|
| <b>OK</b>           | Požadavek byl zpracován korektně.                        |
| <b>SYSTEM_ERROR</b> | Interní chyba systému. Je potřeba počkat, než bude chyba |

## Odesílací brána

| Hodnota                  | Význam   |
|--------------------------|--|
|                          | vyřešena, případně požadavek zkusit zaslat znovu.        |
| <b>SESSION_NOT_FOUND</b> | Vrací v případě, že bylo zasláno neexistující sessionId. |

### 3.3. Popis webové služby pro vložení VoDZ příloh do konceptu

Tuto službu použijí aplikace poskytovatele, které chtějí připravit datovou zprávu za uživatele.

**1.** Komunikace probíhá pomocí protokolu HTTPS, pro přenos zpráv se používá formát SOAP 1.2 a volitelně MTOM/XOP. Komunikace je zabezpečena pomocí SSL. Popis webové služby **UploadAttachment** ve formátu WSDL je uveden v souboru `dm_VoDZ.wsdl`. URL webové služby:

`https://ws2c.[url-adresa-prostředí-isds]/extds/vodz`

V autentizační hlavičce HTTP protokolu (Basic autentizace podle RFC 2617) se musí uvádět řetězec „ExtWS“ v poli `userid` a platné `timeLimitedId` v poli `password`. `TimeLimitedId` je automaticky předáváno jako jeden z atributů ve WS definované v `GetCredential.wsdl` (viz kapitola 3.2.1 Příklad komunikace WS). Pokud `timeLimitedId` pozbylo svoji časovou platnost, bylo už spotřebováno, nebo bylo zrušeno WS popsanou v kapitole 3.5, může služba vrátit HTTP status 401. Služba také může vrátit chybu 401, pokud `timeLimitedId` patří jinému poskytovateli/`atsId`, který neodpovídá použitému klientskému certifikátu. Délka časové platnosti tokenu se řídí v nastavení služby.

Kompletní popis webové služby **UploadAttachment** je v dokumentaci *WS\_ISDS\_Manipulace\_s\_datovými\_zpravami.pdf*.

### 3.4. Popis webové služby pro uložení konceptu

Tuto službu použijí aplikace poskytovatele, které chtějí připravit datovou zprávu za uživatele.

**1.** Komunikace probíhá pomocí protokolu HTTPS, pro přenos zpráv se používá formát SOAP 1.1. Komunikace je zabezpečena pomocí SSL. Popis webové služby ve formátu WSDL je uveden v souboru `SetConcept.wsdl`. URL webové služby:

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

V autentizační hlavičce HTTP protokolu (Basic autentizace podle RFC 2617) se musí uvádět řetězec „ExtWS“ v poli `userid` a platné `timeLimitedId` v poli `password`. `TimeLimitedId` je automaticky předáváno jako jeden z atributů ve WS definované v `GetCredential.wsdl` (viz kapitola 3.2.1 Příklad komunikace WS). Pokud `timeLimitedId` pozbylo svoji časovou platnost, bylo už spotřebováno, nebo bylo zrušeno WS popsanou v kapitole 3.5, může služba vrátit HTTP status 401. Služba také může vrátit chybu 401, pokud `timeLimitedId` patří jinému poskytovateli/`atsId`, který neodpovídá použitému klientskému certifikátu. Délka časové platnosti tokenu se řídí v nastavení služby.

Na jedno `timeLimitedId` lze vložit pouze jeden koncept a tím je `timeLimitedId` spotřebováno. Další koncept je možné vložit po odsouhlasení (nebo zamítnutí) odeslání předchozího. Dále také není možné, aby uživatel měl vloženo více paralelně rozpracovaných konceptů a to ani od různých poskytovatelů.

WSDL obsahuje tři webové služby a to **SetConcept**, **SetMultipleConcept** a **SetBigConcept**. **SetConcept** má stejné vstupy i výstupy jako **CreateMessage**, **SetMultipleConcept** má vstup stejný jako **CreateMultipleMessage**, ale výstup je

## Odesílací brána

obdobný jako v **CreateMessage**, konkrétně existuje jen jedno id konceptu.

**SetBigConcept** má vstup a výstup odpovídající **CreateBigMessage**, vstup ale nesmí obsahovat přílohy v elementu **dmFile**. Přesný popis **CreateMessage**, **CreateMultipleMessage** a **CreateBigMessage** je v dokumentaci *WS\_ISDS\_Manipulace\_s\_datovými\_zpravami.pdf*.

Služby mají rozdílné omezení a to konkrétně:

- Zpráva může obsahovat maximálně 50 příloh.
- Zpráva může mít v případě **SetMultipleConcept** maximálně 5 příjemců.
- Není povoleno uvádět typ zprávy jako komerční, typ zprávy je automaticky označen až v okamžiku odsouhlasení konceptu.
- **SetBigConcept** obsahuje jen odkaz na soubory uploadované pomocí **UploadAttachment** viz. kapitola 3.3 (autentizované pomocí stejného `timeLimitedId`), a není možné uploadovat další přílohu v payloadu, jako je možné v **CreateBigMessage**.
- **SetConcept** a **SetMultipleConcept** neumožňují VoDZ tj. součet příloh o velikosti větší než 20MB.

**2.** Po vložení konceptu DZ musí aplikace poskytovatele uživatele přesměrovat zpět do ISDS. Uživatel si zde může prohlédnout obálku datové zprávy a stáhnout přílohy. Adresa pro přesměrování:

`https://www.[url-adresa-prostředí-isds]/as/koncept/view?konceptId=<dmId>`

Kde `dmId` bylo vráceno v `SetConceptResponse`. Aplikace poskytovatele může uvést znova `appToken`:

`https://www.[url-adresa-prostředí-isds]/as/koncept/view?konceptId=<dmId>&appToken=123`

**3.** Pokud uživatel odsouhlasí (nebo zamítne) odeslání konceptu, je přesměrován zpět do aplikace poskytovatele, na jeho návratovou adresu s novým `sessionId`

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

**4.** Aplikace poskytovatele pak znova volá WS definovanou v `GetCredential.wsdl` viz kap. 3.2, kdy dostane nové `timeLimitedId` a 3 nové položky:

- **conceptDmId** skutečné id datové zprávy v ISDS, pokud bylo zasláno více příjemcům pomocí metody **SetMultipleConcept** jsou jednotlivé ID zprávy odděleny znakem „|“. Pokud se některému příjemci nepovedlo odeslat, bude daný prostor prázdný tj. mohou se vyskytnout dvě svislítká za sebou.
- **conceptStatusCode** chybový kód skutečného odeslání v ISDS, ve speciálním případě zamítnutí konceptu uživatelem je vrácen kód 2305. V případě zaslání více příjemcům v **SetMultipleConcept**, nemusí být všechny zprávy doručitelné, uživatel ale nemůže zamítnout některé příjemce, musí schválit zprávu jako celek, nebo jí zamítnout jako celek. Více chybových kódů je, pouze v případě **SetMultipleConcept**, odděleno opět znakem „|“.
- **conceptStatusMessage** textový popis kódu

V případě, že aplikace chce zaslat další koncept, pokračuje krokem 1, tj. nesmí uživatele přesměrovat na login stránku, protože přesměrování na login stránku je bráno jako nové přihlášení, a `timeLimitedId` vrácené v kroku 4 pozbývá platnost.

### 3.5. Popis webové služby na ukončení platnosti `timeLimitedId`

Tuto službu využije aplikace poskytovatele, pokud se uživatel explicitně rozhodl zrušit svou práci v aplikaci poskytovatele např. odhlášením.

Aplikace jako klient WS služby ISDS a WS služby ISDS komunikují 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 `ExtWs.wsdl`. URL webové služby:

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

#### Komunikace autorizace:

Komunikaci iniciuje aplikace poskytovatele, která zasílá na WS „request“.

Tato WS poté vrátí „response“.

#### 3.5.1. Příklad komunikace WS

|                 |   |
|-----------------|---|
| <b>Request</b>  | <pre>&lt;SOAP-ENV:Envelope   xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"   SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"&gt;   &lt;SOAP-ENV:Body&gt;     &lt;v1:extWsLogoutRequest xmlns:v1="http://agw-as.cz/ats- ws/extWs/v1"&gt;       &lt;v1:timeLimitedId?&gt;&lt;/v1:timeLimitedId&gt;     &lt;/v1:extWsLogoutRequest&gt;   &lt;/SOAP-ENV:Body&gt; &lt;/SOAP-ENV:Envelope&gt;</pre> |
| <b>Response</b> | <pre>&lt;SOAP-ENV:Envelope   xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"   SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"&gt;   &lt;SOAP-ENV:Body&gt;     &lt;v1:extWsLogoutResponse xmlns:v1="http://agw-as.cz/ats- ws/extWs/v1"&gt;       &lt;v1:status&gt;OK&lt;/v1:status&gt;     &lt;/v1:extWsLogoutResponse&gt;   &lt;/SOAP-ENV:Body&gt; &lt;/SOAP-ENV:Envelope&gt;</pre>            |

#### 3.5.2. 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  |
|---------------------|---|
| <b>OK</b>           | Požadavek byl zpracován korektně. Z bezpečnostních důvodů je vráceno i v případě, že: <ul style="list-style-type: none"> <li><code>timeLimitedId</code> neexistuje</li> <li><code>timeLimitedId</code> vypršelo či bylo jinak spotřebováno</li> <li><code>timeLimitedId</code> patří jiné službě (platnost <code>timeLimitedId</code> ale pro tuto jinou službu nebyla ukončena)</li> </ul> |
| <b>SYSTEM_ERROR</b> | Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.  |

### 3.6. Popis webové služby pro informace o možnostech odesílání PDZ

Tuto službu využije aplikace poskytovatele, pokud potřebuje získat informaci o možnosti poslat komerční Poštovní datovou zprávu ze schránky, pro kterou uživatel zadal autentizační údaje a z níž má odejít PDZ, do jedné zvolené neOVM schránky. Na základě této informace může aplikace nabízet formuláře (služby), které vyžadují zaslání PDZ.

Komunikace a autentizace je stejná jako u služby v kapitole 3.3. Popis webové služby **GetPDZInfo** ve formátu WSDL je uveden v souboru `SetConcept.wsdl`. URL webové služby:

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

V autentizační hlavičce HTTP protokolu (Basic autentizace podle RFC 2617) se musí uvádět řetězec „ExtWS“ v poli `userid` a platné `timeLimitedId` v poli `password`. `timeLimitedId` je automaticky předáváno jako jeden z atributů ve WS definované v `GetCredential.wsdl` (viz kapitola 3.2.1 Příklad komunikace WS). Pokud `timeLimitedId` pozbylo svoji časovou platnost, bylo už spotřebováno, nebo bylo zrušeno WS popsanou v kapitole 3.5, může služba vrátit HTTP status 401. Služba také může vrátit chybu 401, pokud `timeLimitedId` patří jinému poskytovateli/`atsId`, který neodpovídá použitému klientskému certifikátu. Délka časové platnosti tokenu se řídí v nastavení služby.

Vstupy a výstupy této webové služby jsou stejné jako u WS `PDZSendInfo`.

#### Vstup:

- `dbId` – ID datové schránky, do které se má zaslat PDZ
- `PDZType` – řetězec „Normal“ = normální PDZ, nebo „Init“ = iniciační PDZ; je-li prázdné nebo nil, pak se uvažuje normální PDZ

#### Výstup:

- `PDZsiResult` – jediná hodnota Ano/Ne
- `dbStatus` – Status operace

#### Popis:

Služba podle volajícího najde jeho schránku a v tabulce pravidel PDZ zjistí, je-li možné podle nějakého pravidla zaslat alespoň jednu PDZ (když `PDZtype`="Normal") nebo alespoň dvě PDZ (když `PDZtype`="Init") do schránky zadaní na vstupu. Iniciační PDZ předplácí i odpověď, proto je třeba zjistit možnost poslání dvou PDZ.

Platí tato pravidla:

- Pokud bude zadaná protější schránka shodná se schránkou volajícího, vrátí se FALSE (lze použít ke zjištění ceny PDZ).
- Pokud bude zadaná protější schránka typu OVM, vrátí se vždy FALSE.
- Pokud bude volající uživatel ze schránky typu OVM, vrátí se FALSE.
- Pokud bude volající uživatel schránky ze povýšené na OVM, vrátí se TRUE nebo FALSE podle skutečného stavu možnosti poslat PDZ.
- Pokud bude zadaná protější schránka povýšená na OVM, vrátí se TRUE nebo FALSE podle povoleného příjmu PDZ.



## Odesílací brána

- Pokud nebude zadaná protějšší schránka zpřístupněná a s povoleným příjmem PDZ, vrátí se FALSE.
- Pokud bude volající uživatel pověřenou osobou bez práva odesílat zprávy (PRIVIL\_CREATE\_DM), vrátí se FALSE.
- Pokud není nalezena u schránky jedna z možností (paušál, kredit nebo dotace, odpovědních se netýká) poslat jednu resp. dvě zprávy, vrátí FALSE.
- Jinak vrátí TRUE.

Aplikace poskytovatele může zavolat GetPDZInfo s platným parametrem timeLimitedId a ostatními parametry stejnými jako používá služba PDZSendInfo pro zjištění možnosti odeslání PDZ. Použití timeLimitedId ve službě GetPDZInfo tento parametr nespotřebává (je možné ho použít vícekrát). Služba ale povolí na jedno timeLimitedId zjistit pouze jednu PDZ (stejný příjemce). Při dotazu na jinou PDZ (jiný příjemce PDZ) služba vrátí chybu. Na stejnou PDZ je možné se zeptat s jedním timeLimitedId i vícekrát (např. pro případ ztráty odpovědi). Služba bude vracet stejné hodnoty, jako vrací PDZSendInfo.

### 3.6.1. Příklad komunikace WS

|                 |   |
|-----------------|---|
| <b>Request</b>  | <pre>&lt;SOAP-ENV:Envelope   xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"   SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"&gt;   &lt;SOAP-ENV:Body&gt;     &lt;ns2:GetPDZInfo       xmlns:ns2="<a href="http://isds.czechpoint.cz/v20/koncept">http://isds.czechpoint.cz/v20/koncept</a>"&gt;       &lt;ns2:dbId&gt;umy3fsj&lt;/ns2:dbId&gt;       &lt;ns2:PDZType/&gt;     &lt;/ns2:GetPDZInfo&gt;   &lt;/SOAP-ENV:Body&gt; &lt;/SOAP-ENV:Envelope&gt;</pre>   |
| <b>Response</b> | <pre>&lt;SOAP-ENV:Envelope   xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"   SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"&gt;   &lt;SOAP-ENV:Body&gt;     &lt;GetPDZInfoResponse xmlns="<a href="http://isds.czechpoint.cz/v20/koncept">http://isds.czechpoint.cz/v20/koncept</a>"&gt;       &lt;PDZsiResult&gt;&gt;false&lt;/PDZsiResult&gt;       &lt;dbStatus&gt;         &lt;dbStatusCode&gt;0000&lt;/dbStatusCode&gt;         &lt;dbStatusMessage&gt;Provedeno úspěšně.&lt;/dbStatusMessage&gt;       &lt;/dbStatus&gt;     &lt;/GetPDZInfoResponse&gt;   &lt;/SOAP-ENV:Body&gt; &lt;/SOAP-ENV:Envelope&gt;</pre> |



## 4. Seznam předávaných atributů

Seznam atributů, které jsou předávány přes webovou službu definovanou GetCredential.wsdl při použití služby OB do externí aplikace poskytovatele.

### 4.1. Speciální atributy

| Název ve WS/API      | Význam   |
|----------------------|--|
| <b>timeLimitedId</b> | Jednorázový token pro autentizaci při odesílání konceptu, mohou dostat jen aplikace, které mají povoleno odesílání konceptů. |
| <b>appToken</b>      | Informace předané aplikací poskytovatele na autentizační bránu   |