



Datové schránky

Odesílací brána a autentizační služba ISDS

Technická specifikace

Vytvořeno dne: 25.1.2016

Aktualizováno: 29.11.2021

Verze: 2.5

Klasifikace: Veřejný dokument

Obsah

1 Úvod.....	4
1.1 Cíl dokumentu.....	4
1.2 Zkratky a definice.....	4
1.3 Poznámky k verzím.....	5
1.3.1 Poznámky k verzi 1.5.....	5
1.3.2 Poznámky k verzi 1.8.....	5
1.3.3 Poznámky k verzi 1.9 – březen 2020.....	5
1.3.4 Poznámky k verzi 2.0 – květen 2020.....	5
1.3.5 Poznámky k verzi 2.1 – červen 2020.....	5
1.3.6 Poznámky k verzi 2.2 – leden 2021.....	5
1.3.7 Poznámky k verzi 2.3 – červen 2021.....	5
1.3.8 Poznámky k verzi 2.4 – říjen 2021.....	5
1.3.9 Poznámky k verzi 2.5 – listopad 2021.....	5
2 Popis služby.....	6
2.1 Základní pojmy.....	6
2.2 Požadavky.....	7
2.3 Konfigurace služby v klientské portálu.....	7
2.3.1 Konfigurace Odesílací brány.....	7
2.3.2 Konfigurace Autentizační služby.....	9
2.4 Požadovaný certifikát.....	10
2.5 Využití odesílací brány.....	10
2.6 Předání informací o uživateli aplikaci poskytovatele.....	12
3 Aplikace využívající OB nebo AS.....	12
3.1 Technické požadavky na Aplikaci poskytovatele.....	12
3.2 Popis webové služby pro získání informací.....	13
3.3 Příklad komunikace WS.....	13
3.3.1 Vysvětlivky.....	14
3.3.2 Popis stavů výsledku zpracování.....	14
3.4 Popis webové služby pro uložení konceptu.....	14
3.5 Popis webové služby na ukončení platnosti timeLimitedId.....	15
3.5.1 Příklad komunikace WS.....	16
3.5.2 Popis stavů výsledku zpracování.....	16
3.6 Popis webové služby pro informace o možnostech odesílání PDZ.....	16
3.6.1 Příklad komunikace WS.....	18
3.7 Popis webové služby pro informaci o stavu služby.....	18
3.7.1 Příklad komunikace WS.....	18

4 Seznam předávaných atributů.....	20
4.1 Atributy datové schránky.....	20
4.2 Atributy uživatele.....	20
4.3 Speciální atributy.....	21

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
Poskytovatel	Ten, kdo poskytuje službu, která využívá AS nebo 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: Veřejný test: czebox.cz Produkční prostředí: mojedatovaschranka.cz
OB	Odesílací Brána
AS	Autentizační služba
DS	Datová schránka ISDS
DZ	Datová zpráva ISDS
OVM	Orgány Veřejné Moci
PDZ	Poštovní datová zpráva

1.3 Poznámky k verzím

1.3.1 Poznámky k verzi 1.5

V této verzi dokumentu byly aktualizovány screenshoty a text v kapitole 2.3.1.

1.3.2 Poznámky k verzi 1.8

Přidány nové atributy Autentizační služby `adDistrict`, `adCode` a `aifoTicket`.

1.3.3 Poznámky k verzi 1.9 – březen 2020

Přidán popis služby `heartBeat`.

1.3.4 Poznámky k verzi 2.0 – květen 2020

Oprava drobných chyb, doplnění WSDL.

1.3.5 Poznámky k verzi 2.1 – červen 2020

Přidán popis registrace Autentizační služby pod OVM schránkou z klientského portálu.

1.3.6 Poznámky k verzi 2.2 – leden 2021

Přidána specifikace časového intervalu pro převzetí informací o uživateli z ISDS.

1.3.7 Poznámky k verzi 2.3 – červen 2021

Oprava formátování tabulek v kap. 4 a úprava funkčnosti v kap. 2

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.

1.3.8 Poznámky k verzi 2.4 – říjen 2021

Vyjmenování jednotlivých typů uživatele v 4.2 Atributy uživatele.

1.3.9 Poznámky k verzi 2.5 – listopad 2021

Oprava číslování kapitol.

2 Popis služby

Odesílací brána (OB)

Tato služba umožňuje aplikaci poskytovatele předání konceptu datové zprávy, vytvořené v externí aplikaci do perimetru ISDS, kde tento koncept může (a měl by) autentizovaný uživatel schválit a poté odeslat.

Autentizační služba (AS)

Tato služba může předávat do aplikace poskytovatele informace o autentizovaném uživateli a odpovídající datové schránce. Rozsah předávaných informací (atributů) je stanoven poskytovatelem při registraci služby v ISDS.

Autentizační služba (AS) je dostupná pouze pro aplikace veřejné správy (pod OVM schránkami). Odesílací brána (OB) je k dispozici všem poskytovatelům služeb bez ohledu na typ schránky.

S ohledem na dříve uvedené, že autentizační služba (AS) je dostupná pouze OVM aplikaci poskytovatele, mohou být služby využity následovně:

- Pouze předání konceptu DZ do ISDS ke schválení a odeslání (OB).
- Pouze získání informace o uživateli ISDS (AS).
- Společné získání informace o uživateli a následně předání konceptu DZ do ISDS ke schválení a odeslání (AS i OB).

Při registraci služby nejde OB vynechat, aplikace ji však nemusí používat.

2.1 Základní pojmy

Aplikace poskytovatele je libovolná webová aplikace, která implementuje přípravu konceptu datové zprávy a / nebo autentizaci svých uživatelů 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. Přímou na stránce autentizace je uvedeno, pro jakou aplikaci a u jakého poskytovatele se uživatel autentizuje. 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)

Kromě toho je možné se autentizovat:

- Mobilním klíčem;
- Prostřednictvím NIA (přes portál elidentita.cz) – při registraci služby lze tento způsob přihlašování zakázat.

Autentizace je umožněna všem typům uživatelů datové schránky.

Služby je možné nastavit tak, aby na jedno zadání přístupových údajů uživatele mohla aplikace poskytovatele získat informace o přihlášeném uživateli a odpovídající datové schránce (AS) a následně předat koncept zprávy do ISDS ke schválení a odeslání (OB).

Využití odesílací brány ani autentizační služby 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.

Pokud je už uživatel v jiném okně prohlížeče úspěšně přihlášen do portálu ISDS, není nucen znovu zadávat přihlašovací údaje a je automaticky přesměrován na schvalovací stránku a upozorněn, že došlo k automatickému přihlášení.

2.2 Požadavky

Základním požadavkem na poskytovatele služby je:

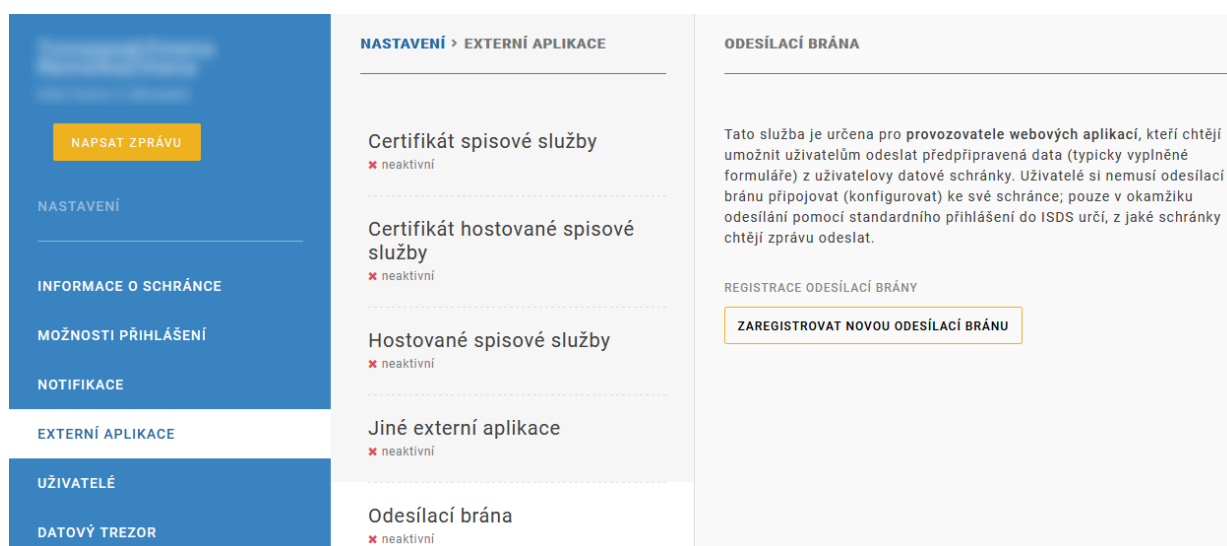
- vlastní datová schránka ISDS typu OVM pro AS, resp. jakéhokoliv typu pro OB.
- úspěšná registrace služby, buď přímo v klientském portálu, nebo zprostředkovaně správcem ISDS.

K jedné datové schránce je možné zaregistrovat více Aplikací poskytovatele. Konfiguraci služby může provést samotný držitel nebo administrátor schránky nebo správce ISDS na žádost – podrobnosti viz provozní řád ISDS.

2.3 Konfigurace služby v klientské portálu

2.3.1 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

Otevře se dvoukrokový formulář, v němž postupně vyplníte všechna požadovaná pole a vložíte certifikát v textové podobě přes schránku.

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.
- Případný zákaz přihlašování přes NIA pro tuto službu
- 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 textovém 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. Přitom je ke službě přiděleno unikátní ID, které budou vývojáři používat při komunikaci s ISDS.

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 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:

Obrázek 2 Seznam existujících odesílacích bran

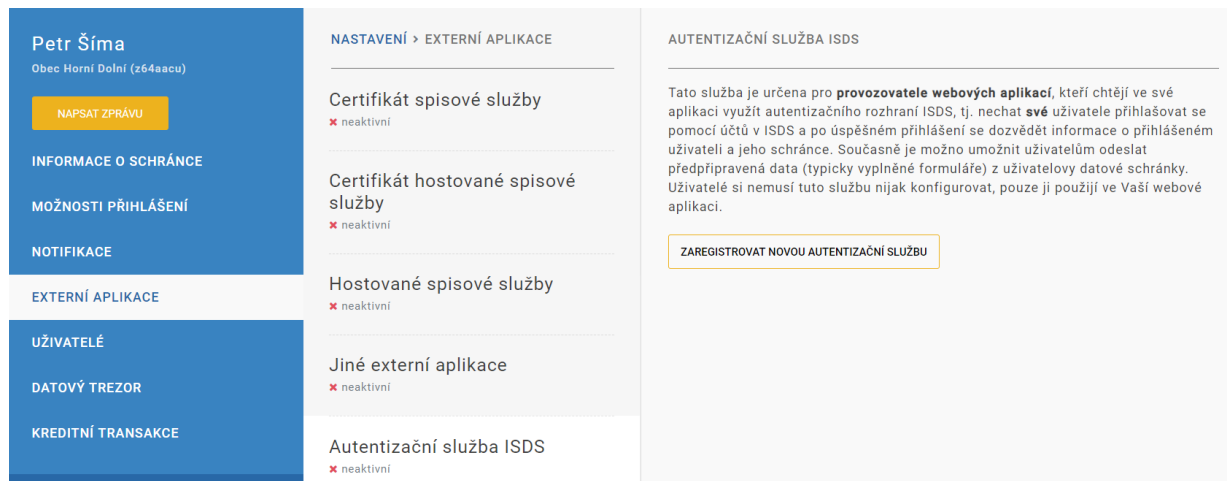
Na seznamu registrovaných OB je zobrazeno vygenerované unikátní ID služby, název služby, typ registrace (odesílací brána) a stav. Nakonec se tu nachází odkaz „Možnosti“, pomocí kterého lze stávající OB aktivovat či deaktivovat, editovat a odregistrovat.

Kliknutím na položku „Možnosti“ a vybráním položky „Upravit“ se zobrazí obdobný dvoukrokový formulář jako při registraci. Nejčastějším důvodem k editaci parametrů fungující služby je periodická výměna certifikátů – expirovaný certifikát znemožní fungování služby! Před expirací certifikátu zasílá ISDS do schránky Poskytovatele 2x systémovou zprávu s upozorněním.

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

2.3.2 Konfigurace Autentizační služby

Registraci a případnou následnou konfiguraci služby AS může provést kterýkoliv administrátor nebo držitel schránky typu OVM, 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 „Autentizační služba ISDS“. Nakonec se stiskne tlačítko **Zaregistrovat novou autentizační službu**.



Obrázek 3 – Zahájení registrace Autentizační služby

Otevře se tříkrokový formulář, v němž postupně vyplníte všechna požadovaná pole a vložíte certifikát v textové podobě přes schránku.

Konfigurace služby v průběhu její existence zahrnuje tyto operace:

- Zadání názvu služby a nastavení návratového URL,
- zadání důvodu předávání osobních dat z ISDS do externí aplikace a dobu jejich uchovávání (zákonné požadavky),
- případný zákaz přihlašování přes NIA pro tuto službu,
- vložení nového přístupového certifikátu služby,
- nastavení a změna množiny povolených atributů datové schránky a uživatele k předání z ISDS do externí aplikace,
- aktivace a deaktivace služby.

Po skončení registrace je každé autentizační službě přiděleno unikátní ID, které budou vývojáři používat při komunikaci s ISDS.

Podrobný popis registrace služby a její editace v prostředí klientského portálu ISDS je uveden v nápovědě k portálu, na adrese

https://www.mojedatovaschranka.cz/static/ISDS/help/page8.html#8_4_5

2.4 Požadovaný certifikát

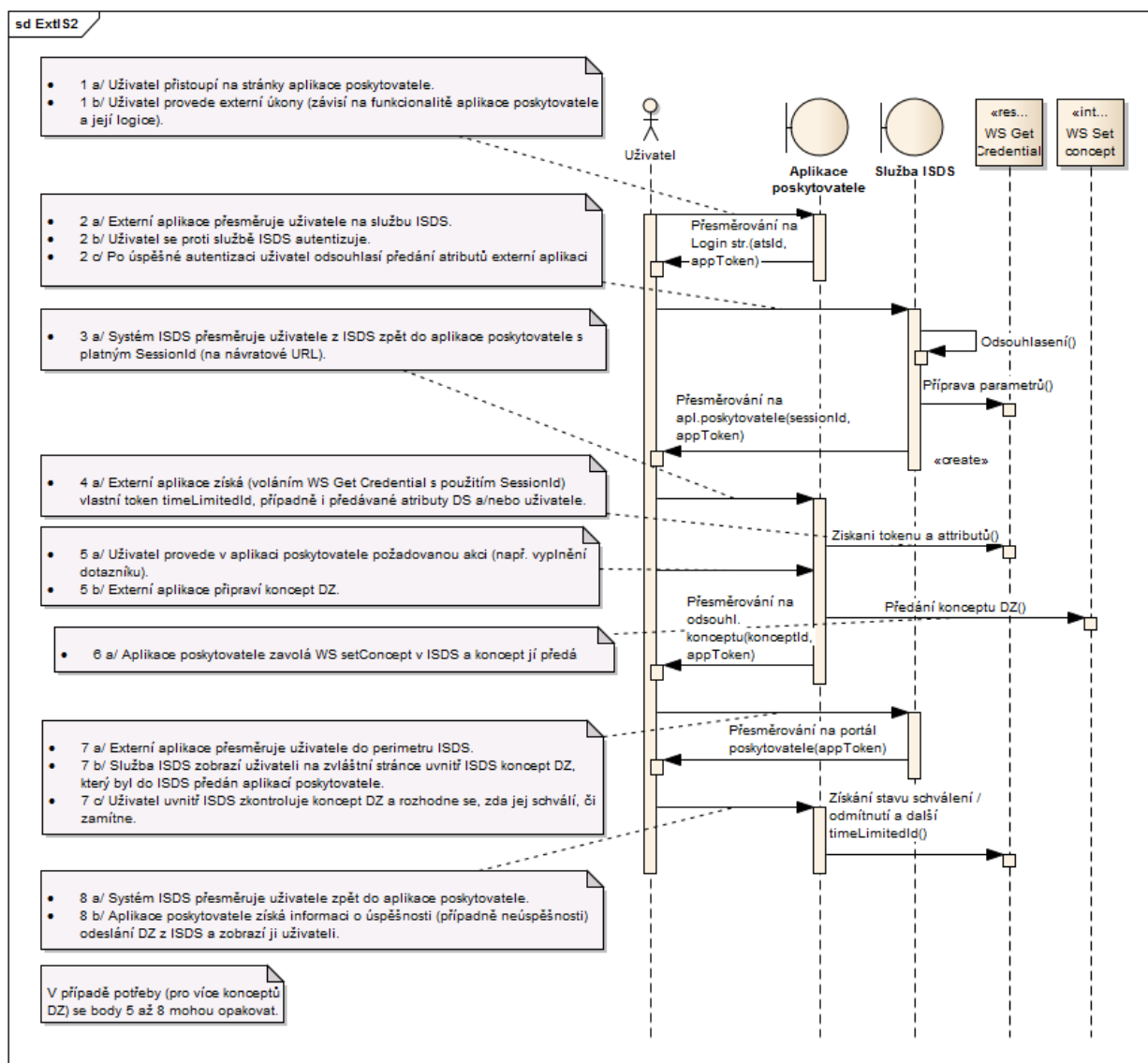
- Pro využití služby je nutné použít komerční certifikát vydaný certifikační autoritou provozovanou kvalifikovaným poskytovatelem služeb vytvářejících důvěru v ČR. Certifikát musí být platný a nesmí být umístěn na CRL. Certifikát nesmí mít omezení, vylučující jeho použití jako SSL/TLS klient.
- V jednu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

2.5 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 zamítne 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.



Detailní postup:

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

případně:

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

- 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 (v tomto případě pouze *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).

2.6 Předání informací o uživateli aplikaci poskytovatele

Předání informací je obdobné odesílací bráně. Liší se pouze v bodě č. 5 a to tím, že převezme kromě *timeLimitedId* i ostatní požadované informace.

1. Aplikace převezme *sessionId* a případně *appToken*, který přišel s redirectem ze služby ISDS. Se *sessionId* zavolá webovou službu pro získání informací. Tuto službu je možné zavolat pouze jednou do 5 minut od převzetí *sessionId*. Technická specifikace volání webové služby přihlášení je popsána v následující kapitole.

3 Aplikace využívající OB nebo AS

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. 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 se službou ISDS probíhá vždy zabezpečeným způsobem přes protokol **TLS verze 1.2**. Služba využívá k šifrování komerční serverový certifikát vydaný akreditovanou certifikační autoritou ČR

3.2 Popis webové služby pro získání informací

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.

Webová služba je zveřejněná ve dvou verzích, které jsou popsány ve formátu WSDL v souborech GetCredential.wSDL a GetCredentialV1_1.wSDL (obsahuje navíc informaci o chybě ve formátu dotazu viz 3.3.2 Popis stavů výsledku zpracování).

URL webové služby verze 1:

`https://cert.[url-adresa-prostředí-isds]/asws/extIs2Endpoint`

URL webové služby verze 1_1:

`https://cert.[url-adresa-prostředí-isds]/asws/atsEndpoint11`

3.3 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 předávat další osobní údaje.

Request	<pre><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="http://agw-as.cz/ats-ws/v1"> <m:sessionId>00-c679c0687f2d43ebbcd766876f90da66</m:sessionId> </m:authConfirmationRequest> </SOAP-ENV:Body> </SOAP-ENV:Envelope></pre>
Response	<pre><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="appToken" value="123"/> <m:attribute name="timeLimitedId" value="T01-7616671e421f4efb8fa1f7bc5b80a913"/> <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></pre>

3.3.1 Vysvětlivky

Hodnota	Význam
sessionId	Identifikace session uživatele přihlášeného do Autentizačního modulu. Token získaný po přesměrování v kapitole 2.5, Detailní postup 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 aplikací poskytovatele.

3.3.2 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
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.
INVALID_SOAP_PAYLOAD	Vrací v případě, že tělo SOAP zprávy nebylo správně vyplněné (ve verzi v1_1).
INVALID_SOAP_ENVELOPE	Vrací v případě, že SOAP obálka nebyla správně vyplněná (ve verzi v1_1).

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 zabezpečená 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 3.3 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/atsld, 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 předání předchozího. Dále také není možné, aby uživatel měl vloženo více paralelně rozpracovaných konceptů a to ani pro různé poskytovatele.

WSDL obsahuje dvě webové služby, a to **SetConcept** a **SetMultipleConcept**. **SetConcept** má stejné vstupy i výstupy jako **CreateMessage**, **SetMultipleConcept** má vstup stejný jako **CreateMultipleMessage**, ale výstup je obdobný jako v **CreateMessage**, konkrétně existuje jen jedno id konceptu. Přesný popis **CreateMessage** a **CreateMultipleMessage** je v dokumentaci *WS_ISDS_Manipulace_s_datovymi_zpravami.pdf*.

Služby mají rozdílné omezení a to konkrétně:

- Zpráva může obsahovat maximálně 5 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.

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 vrací „response“.

3.5.1 Příklad komunikace WS

Request	<pre><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <v1:extWsLogoutRequest xmlns:v1="http://agw-as.cz/ats-ws/extWs/v1"> <v1:timeLimitedId>T00-dcc2282a038c46428d7c59333418bf5</v1:timeLimitedId > </v1:extWsLogoutRequest> </SOAP-ENV:Body> </SOAP-ENV:Envelope></pre>
Response	<pre><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <v1:extWsLogoutResponse xmlns:v1=" http://agw-as.cz/ats-ws/extWs/v1"> <v1:status>OK</v1:status> </v1:extWsLogoutResponse> </SOAP-ENV:Body> </SOAP-ENV:Envelope></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
OK	<p>Požadavek byl zpracován korektně. Z bezpečnostních důvodů je vráceno i v případě, že:</p> <ul style="list-style-type: none"> <i>timeLimitedId</i> neexistuje <i>timeLimitedId</i> vypršelo či bylo jinak spotřebováno <i>timeLimitedId</i> patří jiné službě (platnost <i>timeLimitedId</i> ale pro tuto jinou službu nebyla ukončena)
SYSTEM_ERROR	<p>Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.</p>

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 3.4. Popis webové služby **GetPDZInfo** ve formátu WSDL je uveden v souboru SetConcept.wsd1. 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 3.3 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.
- Pokud nebude zadaná protější 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 nespotřebovává (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

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

3.7 Popis webové služby pro informaci o stavu služby

Tato služba informuje poskytovatele o funkčnosti služby AS/OB. Vrací informaci, zda je systém ISDS dostupný a jestli právě neprobíhá odstávka ISDS, případně částečná odstávka (odstávka části ISDS mimo autentizační komponentu), kdy je dostupná jen AS v základním (omezením) režimu, ale není dostupná OB ani jiné WS, obzvláště ty, které slouží k odesílání zpráv.

Komunikace a autentizace je stejná jako u služby v kapitole 3.4. Popis webové služby **heartBeatRequest** ve formátu WSDL je uveden v souboru `Nas.wsd1`. URL webové služby:

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

Pokud je služba kompletně nedostupná dojde k HTTP chybě 503.

Výstup:

- status – OK, AS, ERROR

Hodnota **OK** znamená, že systém je plně funkční.

Hodnota **AS** znamená, že nebude dostupná odesílací brána (OB) a služba běží v omezeném režimu (nebude fungovat komunikace s ISZR kvůli předávání AIFO ticketů).

3.7.1 Příklad komunikace WS

Request	<pre><soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v1="http://agw-as.cz/nas/v1"> <soapenv:Header/> <soapenv:Body> <v1:heartBeatRequest/> </soapenv:Body></pre>
----------------	--

	</soapenv:Envelope>
Response	<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"> <SOAP-ENV:Header/> <SOAP-ENV:Body> <ns2:heartBeatResponse xmlns:ns2="http://agw-as.cz/nas/v1"> <ns2:status>AS</ns2:status> </ns2:heartBeatResponse> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

4 Seznam předávaných atributů

Seznam všech atributů, které mohou být předávány přes webovou službu definovanou `GetCredential.wsd1` do externí aplikace poskytovatele. Podmnožina níže uvedených atributů je definována při registraci služby, podle požadavků poskytovatele.

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)
adCode	RUIAN kód adresy – FO bydliště, PFO, PO, OVM – sídla; může být prázdný
adCity	adresa – obec
adDistrict	adresa – část obce (FO bydliště, PFO sídla); může být nevyplněný
adStreet	adresa – ulice
adNumberInMunicipality	adresa – číslo domu; je-li ve tvaru začínajícím znakem “e”, např. “e1”, jde o číslo evidenční, je-li bez “e”, např. “123”, jde o číslo popisné.
adNumberInStreet	adresa – číslo orientační
adZipCode	adresa – PSČ
adState	adresa – stát
fullAddress	Kompletní složená adresa, různá podoba podle zadaných elementů
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 (role ve schránce). Nabývá hodnot S = oprávněná osoba (držitel schránky), A = administrátor, P = pověřená osoba, L = likvidátor, R = nucený správce, G = opatrovník PO. Role L, R a G jsou z hlediska oprávnění rovnocenné s S.

Název ve WS/API	Význam
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
roblident	TRUE/FALSE podle toho, je-li uživatel ztotožněn vůči základnímu registru obyvatel (má AIFO)
aifoTicket	Token vrácený z ISZR službou e175 – <i>iszrUlozMapaAifo</i> , může být prázdný, pokud přihlášený uživatel není ztotožněn v ROB (nemá AIFO v ISDS). Aplikace jej může přeložit na AIFO pro svůj AIS pomocí služby e176 – <i>iszrPodejMapaAifo</i> . Nebude funkční v případě částečné odstávky ISDS – viz popis v kap. 3.7

4.3 Speciální atributy

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