



# Datové schránky

## **Přístupové rozhraní** **Technická specifikace pro poskytovatele**

Vytvořeno dne: 12.12.2011

Aktualizováno: 23.03.2026

Verze: 2.11

Kategorie: Veřejný dokument

# Obsah

<b>1.</b>	<b>Úvod .....</b>	<b>3</b>
1.1.	Cíl dokumentu .....	3
1.2.	Zkratky a definice.....	4
<b>2.</b>	<b>Přístupové rozhraní .....</b>	<b>5</b>
<b>3.</b>	<b>Přístupová služba uživatele .....</b>	<b>6</b>
3.1.	Základní pojmy.....	6
3.2.	Požadavky .....	7
3.3.	Konfigurace přístupové služby uživatele .....	7
3.4.	Přístupy aplikace poskytovatele .....	7
3.5.	Povolení přístupu uživatelem .....	8
<b>4.</b>	<b>Autentizační modul .....</b>	<b>8</b>
4.1.	Základní pojmy.....	8
4.2.	Přihlášení uživatele do ExtIS přes ISDS .....	9
<b>5.</b>	<b>Aplikace poskytovatele pro využití Autentizačního modulu.....</b>	<b>10</b>
5.1.	Technické požadavky na Aplikaci poskytovatele .....	10
5.2.	Popis webových služeb Autentizačního modulu.....	10
5.2.1.	WS získání VirtualID .....	11
5.2.1.1.	Příklad komunikace WS .....	11
5.2.1.2.	Vysvětlivky .....	11
5.2.1.3.	Popis stavů výsledku zpracování.....	12
5.2.2.	WS zrušení VirtualID .....	12
5.2.2.1.	Příklad komunikace WS .....	12
5.2.2.2.	Vysvětlivky .....	12
5.2.2.3.	Popis stavů výsledku zpracování.....	12
5.2.3.	WSDL definice .....	13
<b>6.</b>	<b>Bezpečnostní incidenty Poskytovatele .....</b>	<b>13</b>
<b>7.</b>	<b>Akceptace Aplikace poskytovatele .....</b>	<b>13</b>
<b>8.</b>	<b>Účtování služby.....</b>	<b>13</b>
8.1.	Způsob účtování .....	13
8.2.	Příklady výsledků účtování.....	14

# 1. Úvod

## 1.1. Cíl dokumentu

Tento dokument slouží jako podklad pro vytvoření textové přílohy provozního řádu ISDS.

## 1.2. Zkratky a definice

Zkratka	Význam
AGW	Autentizační brána
Autentizace	Ověření identity uživatele
AutExtIS	Autentizační modul ISDS pro ExtIS
Autorizace	Přidělení přístupových práv uživateli po jeho úspěšné autentizaci
CRL	Certificate Revocation List
DS	Datová Schránka
ExtIS	Aplikace poskytovatele (externí informační systém)
HSSU	Technický název pro Přístupové rozhraní; rozšíření ISDS, umožňující provádět v ISDS operace, na které má nárok uživatel, pod jehož účtem aplikace poskytovatele přistupuje do ISDS.
ISDS	Informační systém datových schránek
ISDS/AGW	Systém autentizační brány AGW v perimetru ISDS
MV ČR	Ministerstvo vnitra ČR
Poskytovatel	Osoba poskytující své služby (viz Věstník MV ČR)
Token	Autentizační a autorizační data, která držitele tohoto softwarového tokenu opravňují ke vstupu do systému a provádění povolených činností. (Nejedná se o autentizační hardwarové zařízení.)
[url-adresa-prostředí-isds]	Adresy prostředí: Veřejný test: <code>datovka-test.gov.cz</code> Produkční prostředí: <code>datovka.gov.cz</code>
WS	Webové služby na bázi protokolu SOAP v1.1
WSDL	Popis rozhraní webové služby
VirtualId	Virtuální (zdánlivé) ID uživatele pro přístup do Přístupové služby uživatele (pro HSSU). Toto zdánlivé ID uživatele maskuje skutečné ID a je použitelné pouze pro konkrétní Aplikaci poskytovatele. Tento parametr je předáván Autentizačním modulem pouze v případě komfortního povolení přístupu uživatelem, nelze použít jinak. Pokud se pro povolení nepoužije Autentizační modul, získá uživatel toto Virtuální ID při ručním povolení Aplikace poskytovatele a předá jej Poskytovateli, jak je uvedeno v tomto dokumentu.

appToken	Pro identifikaci, odkud byl uživatel přesměrován na autentizační bránu, může být současně s přesměrováním v přístupovém URL uveden parametr appToken. V tomto parametru si může aplikace poskytovatele udržet identifikaci, odkud je uživatel přesměrován do autentizačního modulu. Tento parametr bude zpět předán aplikaci poskytovatele WS getCredential za předpokladu, že byl součástí přístupového URL. Tento parametr obsahuje maximálně 20 číslic.
IDExtAcc	ID odpovídající uživateli v aplikaci poskytovatele.
Billingový účet	Jeden billingový účet je vymezen unikátní kombinací ID Aplikace poskytovatele, ID uživatele v ISDS a ID odpovídající uživateli v aplikaci poskytovatele. Jeden billingový účet obsahuje datové pole, které je nenulové v případě alespoň jednoho přístupu na Přístupovou službu uživatele v kalendářním roce. Dále billingový účet obsahuje položku Rozhodné datum, kde je uloženo datum prvního přístupu na Přístupovou službu uživatele v kalendářním roce.
Tabulka billingových účtů	Tabulka billingových účtů eviduje všechny billingové účty pro jeden kalendářní rok.
Uživatel	V tomto textu se jedná o uživatele ISDS, který může využívat služeb Přístupového rozhraní prostřednictvím aplikace poskytovatele.
Rozhodné datum	Datum prvního použití Přístupové služby uživatele na billingovém účtu v kalendářním roce.

## 2. Přístupové rozhraní

Novelou zákona č. 300/2008Sb. provedenou zákonem č. 263/2011Sb. byla doplněna možnost využívat rozhraní ISDS poskytovateli internetových služeb. Systém ISDS byl v souvislosti s touto změnou zákonů rozšířen o přístupové rozhraní zahrnující tyto funkce:

- přístupová služba uživatele
- autentizační modul

Tento dokument popisuje způsob využívání přístupového rozhraní pro aplikace poskytovatelů internetových služeb. Aplikace poskytovatele internetových služeb je aplikace, která využívá Přístupové rozhraní.



Přístupové rozhraní umožňuje aplikacím poskytovatele internetových služeb provádět operace v datových schránkách svých uživatelů (např. získání seznamu datových zpráv, stažení datové zprávy, odeslání datové zprávy) s využitím Přístupové služby uživatele. Dále toto rozhraní umožňuje implementovat registraci uživatelů pro přístupovou službu prostřednictvím autentizačního modulu.

### 3. Přístupová služba uživatele

Prostřednictvím přístupové služby uživatele má aplikace poskytovatele povoleny v ISDS operace, na které má nárok uživatel, pod jehož účtem aplikace poskytovatele přistupuje do ISDS. Z důvodu bezpečnosti nepřistupuje aplikace poskytovatele do ISDS pod ID reálného uživatelského účtu. Místo toho je využíváno tzv. virtuální ID, které je svázáno s konkrétním reálným účtem a konkrétním poskytovatelem internetových služeb. Aplikace poskytovatele se autorizuje do ISDS pomocí tohoto virtuálního ID. ISDS během procesu autorizace z virtuálního ID odvodí ID reálného účtu. Přístupové služby uživatele jsou navrženy tak, že jeden uživatel aplikace poskytovatele internetových služeb může mít ve svém profilu v aplikaci poskytovatele zaregistrováno více virtuálních ID (jedna fyzická osoba má ISDS účet ve více schránkách). Takový interní uživatel aplikace poskytovatele pak může prostřednictvím přístupové služby uživatele přistupovat pod více uživatelskými účty do ISDS, a tedy i do více datových schránek.



#### 3.1. Základní pojmy

Přístupová služba uživatele je rozhraní ISDS pro aplikace poskytovatelů internetových služeb. Aplikace poskytovatele internetových služeb může využívat toto rozhraní pro přístup do ISDS pod účty svých uživatelů. Toto rozhraní je placená služba. V jedné datové schránce může být zaregistrována nejvýše jedna Aplikace poskytovatele využívající Přístupovou službu na uživatele. Naproti tomu uživatel může ve svém účtu povolovat přístup i více Aplikací poskytovatele.

Přístupová služba uživatele poskytuje:

- Webové služby rozhraní ISDS pro manipulaci s datovými zprávami
- Webové služby rozhraní ISDS pro správu datových schránek
- Webové služby rozhraní ISDS pro vyhledávání datových schránek
- Webové služby související s přístupem do ISDS

### 3.2. Požadavky

Základním požadavkem na poskytovatele je jeho vlastní datová schránka ISDS. Ostatní požadavky na poskytovatele a na aplikaci poskytovatele jsou uvedeny ve Věstníku MVČR k přístupovému rozhraní ISDS.

### 3.3. Konfigurace přístupové služby uživatele

První konfigurace služby je provedena zároveň s její registrací. Registraci provádí správce ISDS.

Během registrace je každé službě přiděleno unikátní ID. Konfigurace služby v průběhu její existence zahrnuje tyto operace:

- registrace nového přístupového certifikátu služby
- odregistrace přístupového certifikátu služby
- nastavení návratového URL pro aplikaci komfortního povolení přístupu uživatelem (viz níže)
- aktivace a deaktivace služby
- je zde možné zjistit identifikátor registrované služby, který je nutný pro nastavení aplikace pro komfortní povolení přístupu uživatelem (viz níže)

Všechny tyto operace provádí správce ISDS. Poskytovatel v případě potřeby žádá správce o změnu konfigurace.

Poznámka:

1. Pro využití služby je nutné použít komerční certifikát vydaný certifikační autoritou provozovanou kvalifikovaným poskytovatelem služeb vytvářejících důvěru, působícím v ČR. Certifikát musí být platný a nesmí být umístěn na CRL. Certifikát nesmí mít omezení, vylučující jeho použití jako SSL/TLS klient. Pro autentizaci certifikátem je využíván SSL protokol.
2. V jednu chvíli je možné mít zaregistrováno více certifikátů. Je to zejména z toho důvodu, aby byl před vypršením starého již připraven nový.

### 3.4. Přístupy aplikace poskytovatele

Aplikace poskytovatele využívá pro Přístupovou službu uživatele následující URL:

- [https://ws1c.\[url-adresa-prostředí-isds\].cz/hssu/DS/df](https://ws1c.[url-adresa-prostředí-isds].cz/hssu/DS/df)
- [https://ws1c.\[url-adresa-prostředí-isds\].cz/hssu/DS/dx](https://ws1c.[url-adresa-prostředí-isds].cz/hssu/DS/dx)
- [https://ws1c.\[url-adresa-prostředí-isds\].cz/hssu/DS/dz](https://ws1c.[url-adresa-prostředí-isds].cz/hssu/DS/dz)
- [https://ws1c.\[url-adresa-prostředí-isds\].cz/hssu/DS/DsManage](https://ws1c.[url-adresa-prostředí-isds].cz/hssu/DS/DsManage)

SSL spojení musí být navázáno pomocí registrovaného přístupového certifikátu aplikace poskytovatele. V autentizační hlavičce HTTP protokolu (Basic autentizace podle RFC 2617) se musí uvádět ID odpovídající uživateli v aplikaci poskytovatele (v poli userid) a platné virtuální ID uživatele v ISDS (v poli password), na jehož účet přistupuje aplikace do ISDS (viz kap. 3.5).

Z bezpečnostních důvodů není vhodné udávat přímo ID uživatele stejné s použitím v aplikaci poskytovatele. Toto ID smí obsahovat pouze alfanumerické znaky a znaky . (tečka), - (pomlčka) a \_ (podtržítko). Délka musí být od 1 do 40 znaků.

### **3.5. Povolení přístupu uživatelem**

Uživatel poskytovatele internetových služeb musí povolit přístup aplikaci poskytovatele prostřednictvím rozhraní ISDS. Jsou dva způsoby schválení přístupu.

1. Pro komfortní povolení přístupu uživatelem je implementován Autentizační modul. Jeho využití umožní uživateli jednoduché povolení bez komplikovaných poznamenávání různých přístupových kódů. Aplikace poskytovatele a Autentizační modul si potřebné informace navzájem vymění automaticky. Aplikace poskytovatele internetových služeb přesměruje uživatele na přihlášení do ISDS a po přihlášení může uživatel schválit přístup poskytovatele. Aplikace poskytovatele získá přihlašovací virtuální ID pomocí WS autentizačního modulu (viz Popis webové služby Autentizačního modulu dále v tomto dokumentu). Každé komfortní povolení přístupu generuje nové virtuální ID a zároveň ruší to předchozí. Mezi vygenerováním virtuálního ID a použitelností tohoto přístupu může existovat drobná prodleva. Na uživatelský účet ISDS je předána informace o ID DS poskytovatele, prostřednictvím které se povoluje přístup aplikaci poskytovatele na účet uživatele. Detailní popis přihlášení uživatele do Autentizačního modulu je popsán v kapitole 5 . Pro komfortní povolení se využívá stejné konfigurace, která je využita i pro Přístupovou službu uživatele. Jedinou informací, kterou v tomto případě Autentizační modul sděluje, je virtuální ID. Není tedy třeba žádat o registraci zvláštního přístupu k Autentizačnímu modulu. Toto komfortní povolení přístupu není určeno pro běžnou autorizaci, tedy nenahrazuje autorizaci uživatele do externí aplikace.
2. Při manuálním přihlášení se uživatel standardně přihlásí pod svým účtem do ISDS. V nástroji nastavení zvolí „Povolení přístupu poskytovateli internetových služeb“, zadá ID datové schránky poskytovatele a odsouhlasí povolení přístupu. Uživateli je zobrazeno jedinečné přihlašovací virtuální ID, které sdělí poskytovateli služeb. S tímto virtuálním ID bude nakládáno jako se sdíleným tajemstvím.

Uživatel může na stránkách nastavení svého účtu zrušit povolení přístupu poskytovatele po přihlášení na Portále datových schránek.

## **4. Autentizační modul**

Autentizační modul byl vyvinut pro komfortní povolování přístupu na účet uživatele ISDS hostovanou spisovou službou.

### **4.1. Základní pojmy**

Aplikace poskytovatele (ExtIS) je libovolná webová aplikace, která implementuje autentizaci svých uživatelů pomocí přihlašovacích údajů do ISDS.

ISDS zprostředkuje pro aplikaci poskytovatele jen službu Autentizačního modulu pro uživatele ISDS, který se přihlašuje do systému poskytovatele.

Autentizace uživatele pomocí přihlašovacích údajů do ISDS a ověření přihlašovacích údajů probíhá v perimetru ISDS.

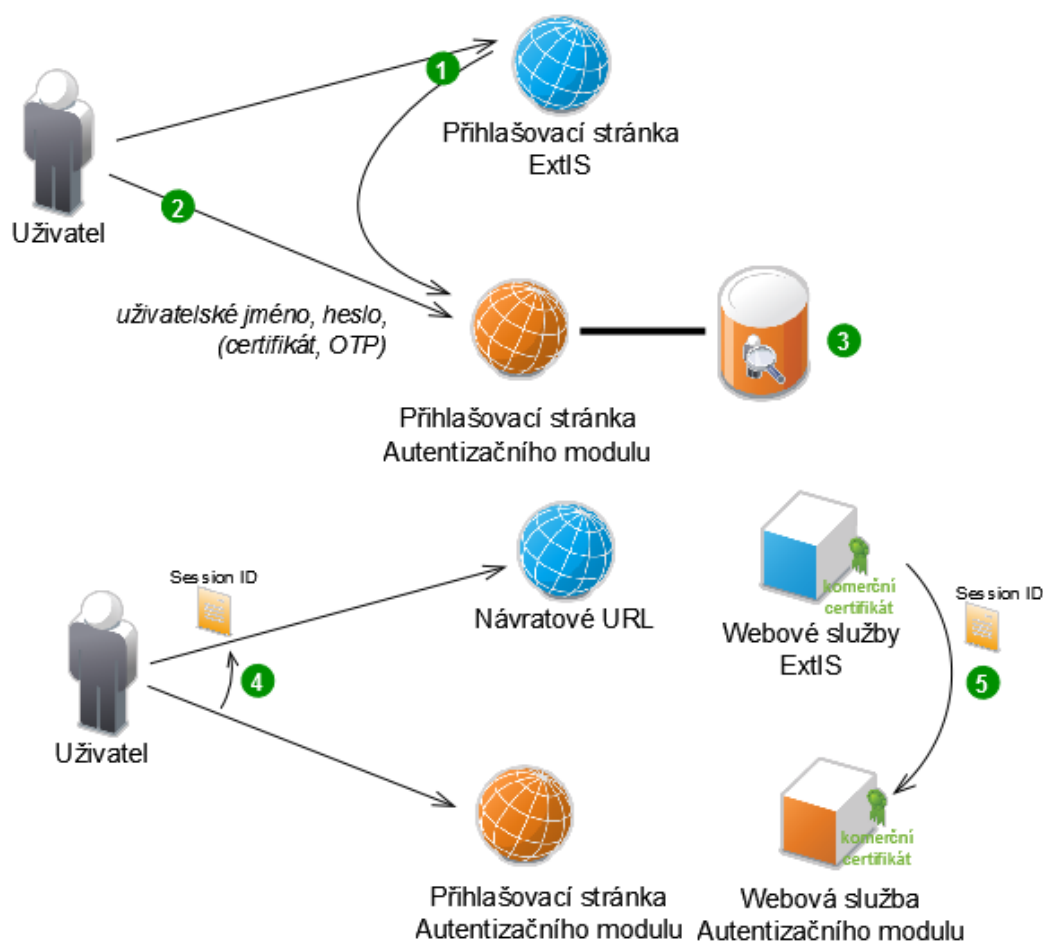
## 4.2. Přihlášení uživatele do ExtIS přes ISDS

Aplikace poskytovatele (ExtIS) využívá univerzální autentizační bránu v režii ISDS. Tento Autentizační modul poskytuje stejné metody a úroveň ověření uživatele přistupujícího do ExtIS jako při přihlášení do ISDS.

Jedná se tedy o následující přihlašovací údaje, které bude uživatel zadávat:

- uživatelské jméno (povinný údaj)
- heslo (povinný údaj)
- komerční certifikát a/nebo OTP (volitelný)

Po ověření Autentizační modul vrátí výsledek do ExtIS. Autentizační modul umožňuje ověřování přístupových údajů všem typům osob datové schránky.



Obrázek 1: Procesní schéma autentizace

1. Uživatel vstoupí na webovou stránku ExtIS. Systém detekuje nepřihlášeného uživatele a provede přesměrování na stránku Autentizačního modulu. V tomto požadavku ExtIS předá Autentizačnímu modulu identifikátor ExtIS, 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://[url-adresa-prostředí-isds]/as/login?atsId=exampleId`

případně:

`https://[url-adresa-prostředí-isds]/as/login?atsId=exampleId&appToken=123`

2. Po přesměrování zobrazí Autentizační modul uživateli webovou stránku s autentizačním (přihlašovacím) formulářem. Uživatel je vyzván k zadání svých přístupových údajů, které používá ke klasickému přihlášení do ISDS.
3. Autentizační modul ověří vůči identitnímu prostoru ISDS správnost přístupových údajů. V případě neúspěšného ověření přístupových údajů je uživateli zobrazeno upozornění typu „Chyba přihlášení, znovu zadejte údaje.“. V případě úspěšného ověření přístupových údajů je uživatel požádán o souhlas s předáním informací aplikaci poskytovatele. Předávané informace jsou uživateli zobrazeny.
4. Autentizační modul přesměruje uživatele na návratové URL, které je uvedeno v nastavení ExtIS v datové schránce provozovatele. Toto URL, které je v plné režii ExtIS, musí přijímat parametr "sessionId", který poté ExtIS použije pro volání webové služby.

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

5. ExtIS převezme sessionId, který přišel s redirectem z Autentizačního modulu a s ním zavolá webovou službu Autentizačního modulu pro získání virtuálního ID přihlášeného uživatele. Získání informací z ISDS za pomoci daného sessionId je možné pouze jednou. Zároveň s virtuálním ID získá appToken, pokud byl autentizačnímu modulu předán v požadavku (viz bod 1.). Takto získané virtuální ID uživatele si aplikace poskytovatele bezpečně uchová, aby jej využívala v rámci přístupové služby uživatele.

Technická specifikace volání webové služby přihlášení je popsána v následující kapitole.

## 5. Aplikace poskytovatele pro využití Autentizačního modulu

### 5.1. Technické požadavky na Aplikaci poskytovatele

1. ExtIS musí být aplikace dostupná z Internetu a přístup do ní musí být zabezpečen přes webový prohlížeč pomocí protokolu HTTPS.
2. ExtIS implementuje přihlašovací stránku pro příjem sessionId podle specifikace uvedené v kapitole 5 .
3. Požadavky na klienta: ExtIS implementuje klientskou část WS podle WSDL specifikace v kapitole 5.2. Pro přístup na WS autentizačního modulu musí ExtIS využívat komerční serverový certifikát vydaný certifikační autoritou provozovanou kvalifikovaným poskytovatelem služeb vytvářejících důvěru, působícím 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 s ExtIS probíhá vždy zabezpečeným způsobem přes protokol SSLv3/TLS 1.2. Služba využívá k šifrování komerční serverový certifikát vydaný kvalifikovaným poskytovatelem služeb vytvářejících důvěru, působícím v ČR.

### 5.2. Popis webových služeb Autentizačního modulu

Služba ExtIS jako klient WS Autentizačního modulu a WS Autentizačního modulu 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 `GetCredential.wsdl`. URL webové služby:

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

**Komunikace autorizace:**

Komunikaci iniciuje systém ExtIS, který zasílá na WS Autentizačního modulu ISDS „request“.

WS Autentizačního modulu poté vrátí „response“.

**5.2.1. WS získání VirtualID**

**5.2.1.1. 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;m:authConfirmationRequest xmlns:m="Some-URI"&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="Some-URI"&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="virtualId" value="123456789"/&gt;       &lt;/m:attributes&gt;     &lt;/m:authConfirmationResponse&gt;   &lt;/SOAP-ENV:Body&gt; &lt;/SOAP-ENV:Envelope&gt;</pre>

**5.2.1.2. Vysvětlivky**

Hodnota	Význam
<b>sessionId</b>	Identifikace session uživatele přihlášeného do Autentizačního modulu. Token získaný po přesměrování v kapitole 5, bod 4.
<b>status</b>	Strukturovaná informace o výsledku zpracování žádosti.
<b>userRequestIp</b>	IP uživatele při přihlášení. Může být IPv6/IPv4, pokud uživatel přistupuje přes proxy bere se IP proxy, která je nejdále od uživatele.
<b>attributes</b>	V tomto případě se jedná pouze o jeden atribut s názvem <code>virtualId</code> , popis níže.
<b>attribute</b>	Atribut z identitního prostoru pod názvem „name“ a s hodnotou „value“. Zde se jedná pouze o atribut <code>virtualId</code> . K předávaným atributům může být přidán také <code>appToken</code> .

### 5.2.1.3. 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 vyřešena, případně požadavek zkusit zaslat znovu.
<b>SESSION_NOT_FOUND</b>	Vrací v případě, že byl zaslán neexistující token.

### 5.2.2. WS zrušení VirtualID

Umožňuje odvolat souhlas s přístupem ke službě.

#### 5.2.2.1. Příklad komunikace WS

<b>Request</b>	<pre>&lt;SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"&gt;   &lt;SOAP-ENV:Header/&gt;   &lt;SOAP-ENV:Body&gt;     &lt;ns2:RevokeConfirmationRequest xmlns:ns2="http://agw-as.cz/ats-ws/v1"&gt;       &lt;ns2:VirtualID&gt;vwix97e6mg3t4pkk&lt;/ns2:VirtualID&gt;       &lt;ns2:atsId&gt;testAts&lt;/ns2:atsId&gt;     &lt;/ns2:RevokeConfirmationRequest&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/"&gt;   &lt;SOAP-ENV:Header/&gt;   &lt;SOAP-ENV:Body&gt;     &lt;ns2:RevokeConfirmationResponse xmlns:ns2="http://agw-as.cz/ats-ws/v1"&gt;       &lt;ns2:status&gt;OK&lt;/ns2:status&gt;     &lt;/ns2:RevokeConfirmationResponse&gt;   &lt;/SOAP-ENV:Body&gt; &lt;/SOAP-ENV:Envelope&gt;</pre>

#### 5.2.2.2. Vysvětlivky

Hodnota	Význam
<b>VirtualID</b>	Dříve získané VirtuálID.
<b>atsId</b>	Identifikátor ExtIS, pod kterým je daná služba poskytovatele zaregistrována v ISDS.
<b>status</b>	Strukturovaná informace o výsledku zpracování žádosti.

### 5.2.2.3. 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.

Hodnota	Význam
<b>ERROR</b>	Interní chyba systému. Je potřeba počkat, než bude chyba vyřešena, případně požadavek zkusit zaslat znovu.
<b>VIRTUAL_ID_NOT_FOUND</b>	Vrací v případě, že virtuální ID neexistuje, např. bylo zrušeno dříve, nebo patří jinému ExtIS.

### 5.2.3. WSDL definice

Popisy webové služby je uložen v souboru `GetCredential.wsdl`.

## 6. Bezpečnostní incidenty Poskytovatele

Poskytovatel je povinen nahlásit Správci jako bezpečnostní incident každý pokus o získání nebo zneužití informací souvisejících s Datovými Schránkami (DS) nepovolanou osobou. Nahlášení se provádí na Infolinku ISDS – technickou podporu.

## 7. Akceptace Aplikace poskytovatele

Poskytovatel provede proti testovacímu prostředí všechny operace komunikace s Přístupovým rozhraním a tato komunikace bude analyzována Provozovatelem. Při analýze bude posuzována přiměřenost (viz Provozní řád) a bude kontrolováno, zda komunikace splňuje specifikaci přístupového rozhraní.

Poskytovatel musí prokázat, že autentizace uživatelů do Aplikace poskytovatele je nabízena minimálně se stejně silným zabezpečením jako nabízí autentizace ISDS. Na rozdíl od identifikátoru služby nebo Session ID, jejichž použití je zabezpečeno certifikátem, musí Poskytovatel zajistit, aby nedošlo ke zneužití Virtuálního ID a zejména během přejímání nebylo možné jeho hodnotu zcizit.

## 8. Účtování služby

Poskytovatel platí za využívání Přístupové služby uživatele roční poplatek vypočtený jako součin částky uvedené v zákoně a počtu billingových účtů příslušejících Poskytovateli, pro které bylo v daném kalendářním roce využito přístupové rozhraní alespoň jednou.

### 8.1. Způsob účtování

Požadavek z Aplikace poskytovatele je přijat Přístupovou službou uživatele. Požadavek je autentizován. V případě, že autentizační údaje uvedené v požadavku jsou správné, je požadavek předán k provedení s těmito informacemi:

- dn služby HSSU (ID HSSU služby včetně ID schránky)
- dn uživatele (ID uživatele ISDS včetně ID jeho schránky)
- IDExtAcc

Před provedením je v billingové části zkontrolováno, zda pro kombinaci ID HSSU, ID uživatele ISDS a IDExtAcc je již zaznamenán přístup v aktuálním kalendářním roce. Pokud není, uloží současné datum do položky Rozhodné datum a nastaví Čítač bodů. Pokud je přístup již zaznamenán, tak neukládá rozhodné datum ani nenastavuje Čítač bodů. Poté zkontroluje oprávnění a provede požadavek.

Před vlastním vyúčtováním si Správce stáhne Tabulku billingových bodů, kterou použije pro výpočet částek pro vyúčtování. Součástí případné detailní informace o vyúčtování nesmí být ID uživatele ISDS.

## 8.2. Příklady výsledků účtování

V tomto příkladě je uvažováno, že částka uvedená v zákoně je rovna 100Kč.

Přístup na jeden uživatelský účet ISDS ze dvou účtů jedné Aplikace nebo ze dvou účtů více (v tomto případě dvou) Aplikací více poskytovatelů.

ID Přístupové služby uživatele	ID uživatele ISDS	IDExtAcc
111111	1	A
111111 nebo 111112	1	B

V tomto případě bude poskytovateli naúčtováno 2x100Kč. V případě dvou aplikací bude každému poskytovateli naúčtováno po 100Kč.

Přístup na dva ISDS uživatelské účty z jednoho účtu Aplikace poskytovatele.

ID Přístupové služby uživatele	ID uživatele ISDS	IDExtAcc
111111	1	A
111111	2	A

V tomto případě bude poskytovateli naúčtováno 2x100Kč.

Přístup na dva ISDS uživatelské účty ze dvou účtů Aplikace poskytovatele.

ID Přístupové služby uživatele	ID uživatele ISDS	IDExtAcc
111111	1	A
111111	2	A
111111	1	B
111111	2	B

V tomto případě bude poskytovateli naúčtováno 4x100Kč.