

B2B rozhraní VZP ČR

Popis rozhraní pro partnery v privátní síti

Obsah

| | |
|---|-----------|
| SEZNAM OBRÁZKŮ | 3 |
| HISTORIE DOKUMENTU | 4 |
| ÚVOD | 5 |
| 1. KOMUNIKACE PARTNERŮ V PRIVÁTNÍ SÍTI | 6 |
| 1.1 Aplikační rozhraní..... | 7 |
| 1.1.1 Odeslání zpráv | 7 |
| 1.1.2 Získání seznamu zpráv | 9 |
| 1.1.3 Načtení zpráv | 11 |
| 1.1.4 Potvrzení o načtení zpráv..... | 14 |
| 1.2 Stav vyřízení požadavku | 15 |
| 1.3 SOAP Message Security | 16 |
| 1.4 Service endpoint ve WSDL | 17 |
| 1.4.1 Chybové výstupy | 18 |
| 1.5 Poskytované služby na B2B rozhraní..... | 18 |
| 1.5.1 Nastavení B2B účtu | 18 |
| 1.5.2 Nastavení B2B účtu 2 | 20 |
| 2. ČASTO Kladené otázky | 22 |
| 3. SEZNAM ZKRATEK..... | 23 |
| 4. Použitá literatura..... | 24 |

Seznam obrázků

| | |
|--|-----------|
| <i>Obrázek 1 Komunikace partnera s novým rozhraním B2B.....</i> | <i>7</i> |
| <i>Obrázek 2 Digitálně podepsaná SOAP zpráva.....</i> | <i>16</i> |
| <i>Obrázek 3 Digitální podpis používající BinarySecurityToken.....</i> | <i>17</i> |

Historie dokumentu

| Verze | Datum | Autor | Popis |
|-------|-----------|------------|-----------------------|
| 1.0 | 14.6.2015 | HPServices | Založení dokumentu |
| 1.1 | 22.6.2015 | HPServices | Zpracované připomínky |
| 1.2 | 1.7.2015 | HPServices | Zpracované připomínky |
| | | | |
| | | | |
| | | | |

Úvod

Tento dokument popisuje specifikaci alternativního asynchronního rozhraní pro partnery VZP ČR, jejichž infrastruktura není nepřetržitě připojena k internetu, nebo nemá pevnou IP adresu. Platnost popsaného alternativního asynchronního rozhraní je od 06/2015. Simulační prostředí B2B slouží pro ověření funkčnosti vyvinutého konektoru dodavatele ASW pro partnery.

1. Komunikace partnerů v privátní síti

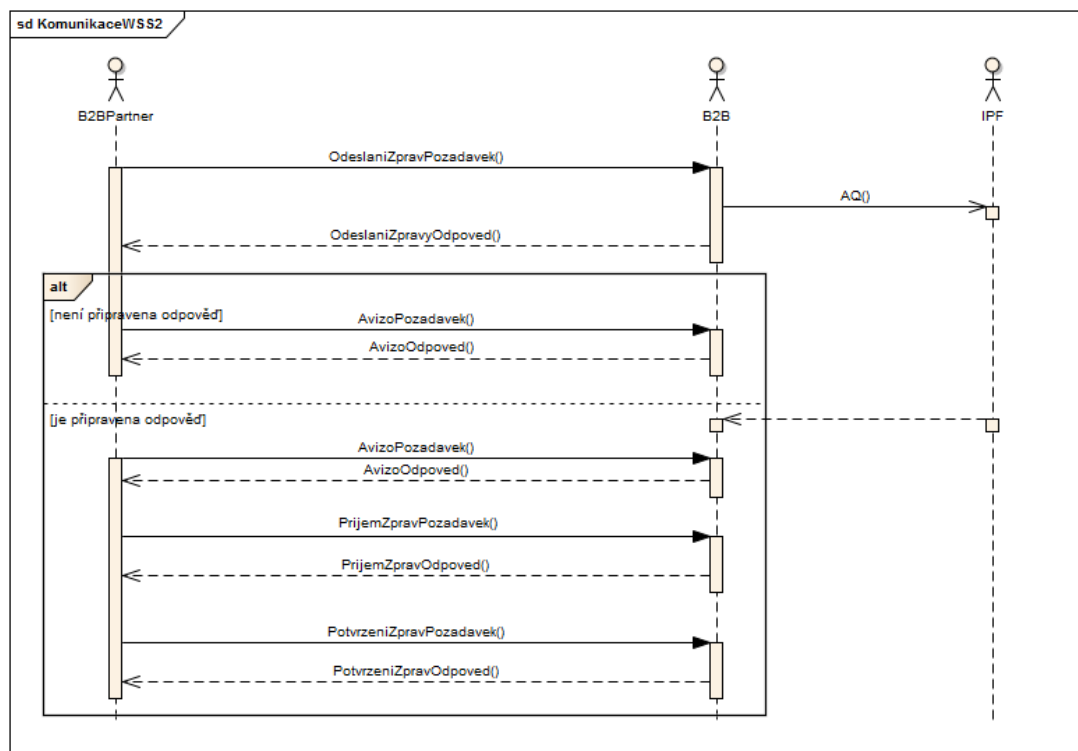
Pro partnery VZP ČR, kteří nemohou používat standardní aplikační rozhraní AS2, nebo je pro ně použití tohoto rozhraní výhodnější, je určena skupina zabezpečených synchronních webových služeb (Odeslání zpráv, Získání seznamu zpráv, Načtení zpráv, Potvrzení o načtení zpráv), s jejichž pomocí partner komunikuje s B2B bránou VZP ČR pomocí protokolu SOAP. Zabezpečený přenos využívá standardu WS-Security specifikovaného v dokumentaci [9]. Příklad využívaného podpisu XMLSig je uveden v kapitole 1.3.

K odeslání původně asynchronní zprávy využije partner připravenou službu Odeslání zpráv. Partner se dozví v odpovědi, zda tato zpráva byla správně odeslána (proces probíhá v rámci jedné relace). Vyzvednutí zprávy provede partner dotazem na webovou službu Získání seznamu zpráv. Služba partnerovi odpoví v rámci jedné relace identifikátorem zprávy k vyzvednutí. Po vyzvednutí zprávy službou Načtení zpráv partner potvrdí, že zprávu převzal, což je proces podobný asynchronnímu přenosu protokolem AS2. Potvrzení proběhne zavoláním webové služby Potvrzení o načtení zpráv, které je předán identifikátor vyzvednuté zprávy. Pokud partner nepotvrdí převzetí vyzvednuté zprávy a počet nevyzvednutých zpráv překročí stanovené limity, nebude povoleno odeslání další zprávy stejného typu. V případě nepotvrzení zprávy bude odpověď na požadavek služby Získání seznamu zpráv obsahovat nepotvrzenou zprávu.

Pro zajištění správné funkce a stability synchronní komunikace pro partnery v privátní síti je potřeba dodržovat dohodnutá kritéria komunikace. Speciálně musí být zajištěno, aby nebylo rozhraní bezdůvodně přetěžováno dávkovým zpracováním nebo opakovaným dotazováním na existenci zprávy v B2B. Partner se dotáže, v případě očekávané odpovědi na odeslané zprávy, nejdříve za deset minut po odeslání první zprávy. Každý partner v privátní síti se dotáže na nové zprávy jednou denně. Proti přetížení adaptéru má každý partner povolený počet dotazu na dohodnutou dobu. Tento způsob komunikace není určen pro subjekty typu nemocnice, protože může dojít ke značnému omezení možnosti komunikace malých subjektů. Standardně probíhá asynchronní komunikace protokolem AS2, která nevyžaduje dotazování, zda je zpráva připravena.

Proces zpracování zabezpečené synchronní zprávy odpovídá podobě průběhu asynchronní komunikace. Příjemce zprávy vždy potvrdí zasílateli přijetí. Systém vzájemného potvrzení přijímaných zpráv zajišťuje neodmítnutelnost podání. Pokud je v rámci zpracování zprávy vyžadovaná další komunikace s odesílatelem (např. odeslání výsledků zpracování), je tato navazující komunikace řešena opět zabezpečenou synchronní službou, kterou si partner vyzvedne zprávu.

Princip komunikace je znázorněn na následujícím diagramu



Obrázek 1 Komunikace partnera s novým rozhraním B2B

1.1 Aplikační rozhraní

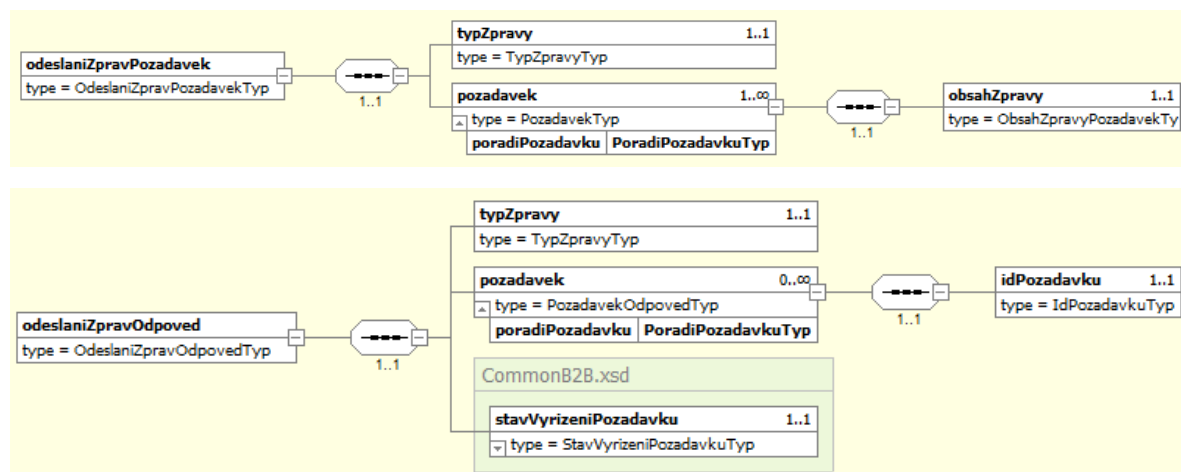
Všechny příklady vstupů i výstupů jsou očištěny o části související s WS-Security, jelikož tato část je samostatně definována v kapitole 1.3 SOAP Message Security.

1.1.1 Odeslání zpráv

Služba umožňuje partnerovi odeslat zprávu určenou k asynchronnímu zpracování a získat synchronní potvrzení o převzetí zprávy. V jednom volání může být odesláno až pět zpráv stejného typu.

Požadavek musí být podepsán partnerovým certifikátem, který je ve VZP evidován jako podpisový. Odpověď se stavem vyřízení podepsána není. Platí atomičnost operace, tedy projdou buď všechny zprávy, nebo žádná.

Z důvodu ochrany B2B brány před přetížením je stanoven limit jedné zprávy na 10 miliónů znaků, posílání většího množství dat v součtu zpráv se silně nedoporučuje a může být ze strany B2B odmítnuto.



Pokud partner očekává odpověď na odeslanou zprávu, zavolá podle kritérií předepsaných v kapitole 1 službu [avízo](#), kterou získá seznam zpráv k vyzvednutí. Vyzvednutí zprávy provede partner voláním služby [prijemZprav](#) a každou přečtenou zprávu následně potvrdí službou [potvrzeniZprav](#). K zamítnutí odeslání zprávy dojde tehdy, existuje-li pro partnera nevyzvednutá (nepotvrzená voláním služby potvrzeniZprav) zpráva libovolného typu starší než doba stanovená VZP nebo pokud počet zpráv stejného typu přesáhne určené množství nevyzvednutých zpráv. V takových případech bude navrácen stavVyrizeniPozadavku -8.

K dokumentu je přiloženo XSD schéma: b2bwssadapter2.xsd, CommonB2B.xsd
a WSDL soubor: odeslaniZprav.wsdl.

Název služby: odeslaniZprav, endpoint WSSOdeslaniZprav

Konzument: partner v privátní síti, který nemá možnost získat veřejnou IP adresu

Typ: synchronní

Požadavek:

| | | |
|------------------------|-----------------|-----|
| odeslaniZpravPozadavek | ComplexType | 1 |
| typZpravy | String | 1 |
| pozadavek | ComplexType | 1-5 |
| poradiPozadavku | Atribut:Integer | 1 |
| obsahZpravy | Base64 | 1 |

Odpověď:

| | | |
|-----------------------|-----------------|-----|
| odeslaniZpravOdpoved | ComplexType | 1 |
| typZpravy | String | 1 |
| pozadavek | ComplexType | 0-5 |
| poradiPozadavku | Atribut:Integer | 1 |
| idPozadavku | String | 1 |
| stavVyrizeniPozadavku | Enumeration | 1 |

Popis atributů zpráv:

- idPozadavku – element obsahuje unikátní identifikátor odesílané zprávy přidělený od VZP ČR. Tento identifikátor konkrétní odesílané zprávy je následně obsažen ve službě avizo a prijemZprav – lze tak podle tohoto elementu korelovat jednotlivé požadavky a odpovědi zasílané do VZP ČR,
- poradiPozadavku – očíslování jednotlivých zpráv v rámci požadavku. Nabývá hodnot od 1 do 5. Koreluje se na id v odpovědi.
- typZpravy – obsahuje název služby, na kterou je zpráva odeslána. (Např.: nastaveniB2BUctu),
- obsahZpravy – obsah zprávy konkrétní služby ve formátu base64. Každá zpráva, která je původně určena pro asynchronní službu, je definována v rámci dokumentace příslušející konkrétní služby,
- stavVyrizeniPozadavku – určuje stav vyřízení požadavku, nabývá hodnot dle následující tabulky.

Příklad vstupu:

```
<odeslaniZpravPozadavek xmlns="http://www.gem.com/b2b/wss/2">
  <typZpravy>nastaveniB2BUctu2</typZpravy>
  <pozadavek poradiPozadavku="1">
```

```

<obsahZpravy>
PD94bWwgdmVyc2lrbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4NCjxuYXN0YXZlbnlCMkJVY3R1MlBvem
FkYXZlayB4bWxucz0iaHR0cDovL3d3dy5nZWlzeXN0ZW0uY3ovQjJCVXBkYXRlLzIuMCI+DQogIDxuYXN0
YXZCMkJLb211bnlrbWwPpg0KICAgIDxldm9kbmlLb25maWdlcmFjZT4NCiAgICAgIDxwcm90b2tvdD5TT0
FQPC9wcm90b2tvdD4NCiAgICAgICA8L3V2b2RuaUtvmZpZ3VyYWNlPg0KICAgIDxzZXpuYWlQcmllhbnljb2
aFpwcmlF2Pg0KICAgICAgPHByaWppbWFuYVpwcmlF2YT4NCiAgICAgICAgPHR5cFpwcmlF2eT5KUKY8L3R
5cFpwcmlF2eT4NCiAgICAgICAgPHN0YXxyUHJpaGxhc2VuaTwvc3Rhdj4NCiAgICAgIDwvcHJpamltYW5hW
nByYXZlbnlrbWwPpg0KICAgIDwvc2V6bmFtUHJpamltYW55Y2hacHJhdj4NCiAgPC9uYXN0YXZCMkJLb211bnlrbWw
Ppg0KPC9uYXN0YXZlbnlCMkJVY3R1MlBvemFkYXZlay4g
</obsahZpravy>
</pozadavek>
</odeslaniZpravPozadavek>

```

Příklad výstupu se zamítnutím operace:

```

<odeslaniZpravOdpoved xmlns="http://www.gem.com/b2b/wss/2">
  <typZpravy>nastaveniB2BUctu2</typZpravy>
  <pozadavek poradipozadavku="1">
    <idPozadavku>23</idPozadavku>
  </pozadavek>
  <stavVyrizeniPozadavku>-8</stavVyrizeniPozadavku>
</odeslaniZpravOdpoved>

```

Příklad výstupu, je-li operace akceptována:

```

<odeslaniZpravOdpoved xmlns="http://www.gem.com/b2b/wss/2">
  <typZpravy>nastaveniB2BUctu2</typZpravy>
  <pozadavek poradipozadavku="1">
    <idPozadavku>23</idPozadavku>
  </pozadavek>
  <stavVyrizeniPozadavku>1</stavVyrizeniPozadavku>
</odeslaniZpravOdpoved>

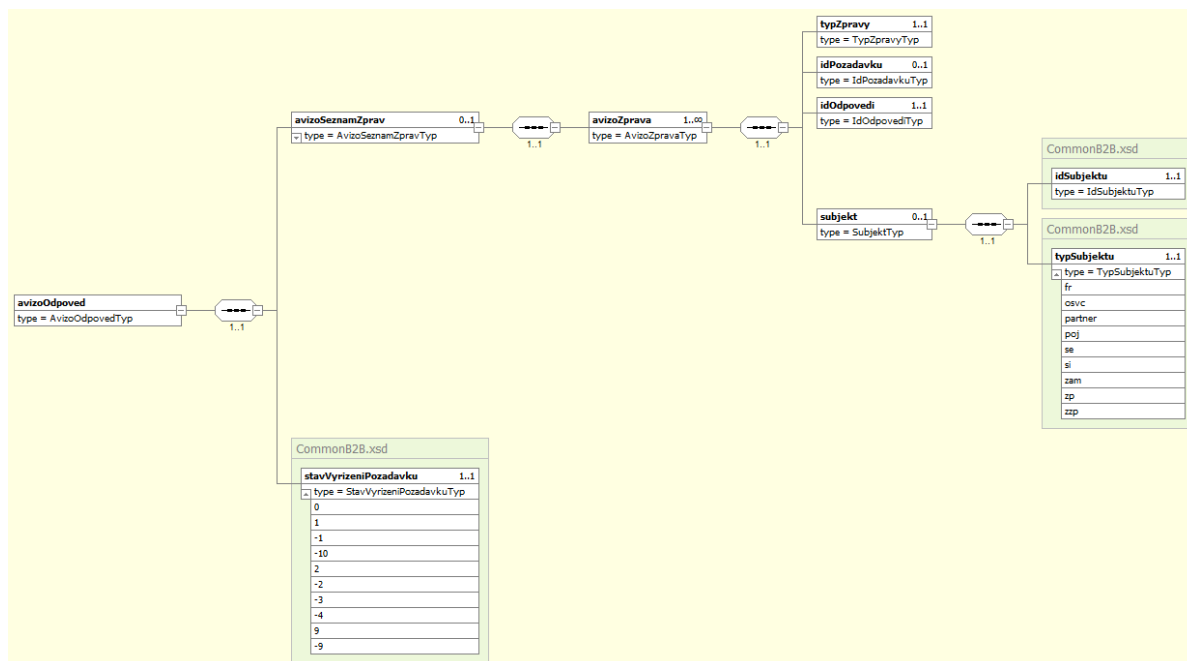
```

1.1.2 Získání seznamu zpráv

Služba vrátí seznam identifikátorů zpráv k vyzvednutí. Nevyžaduje podpis dat a vrací údaje, díky kterým je možné korelovat čekající zprávy s požadavkem a zastupovaným subjektem. Pokud v B2B bráně čeká více zpráv, než je nastaven limit v konfiguraci, bude seznam zkrácen na tento limit a nastaven příznak zkraceno.

K dokumentu je přiloženo XSD schéma: b2bwssadapter2.xsd, CommonB2B.xsd
a WSDL soubor: odeslaniZprav.wsdl.

| |
|--------------------------|
| avizoPozadavek |
| type = AvizoPozadavekTyp |



Název služby: avizo, endpoint WSSAvizo

Typ: synchronní

Konzument: partner v privátní síti, který nemá možnost získat veřejnou IP adresu

Požadavek:

| | | |
|----------------|-------------|---|
| avizoPozadavek | ComplexType | 1 |
|----------------|-------------|---|

Odpověď:

| | | |
|-----------------------|-----------------|-----|
| avizoOdpoved | ComplexType | 1 |
| avizoSeznamZprav | ComplexType | 0-1 |
| zkraceno | Atribut:Boolean | 1 |
| avizoZprava | ComplexType | 1-n |
| typZpravy | String | 1 |
| idPozadavku | String | 0-1 |
| idOdpovedi | String | 1 |
| subjekt | ComplexType | 0-1 |
| idSubjektu | String | 1 |
| typSubjektu | String | 1 |
| stavVyrizeniPozadavku | Enumeration | 1 |

Popis atributů zpráv:

idPozadavku – element obsahuje unikátní identifikátor odesílané zprávy přidělený od VZP ČR. Tento identifikátor odpovídá elementu idPozadavku uvedeném ve službě odesláníZprav a příjemZprav – lze tak podle tohoto elementu korelovat jednotlivé požadavky a odpovědi zasílané do VZP ČR,

idOdpovedi – element obsahuje unikátní identifikátor odpovědi sestavené VZP ČR. Pod tímto identifikátorem se stahují zprávy službou příjemZprav a potvrzuje doručení službou pozvrzeníZprav,

| | |
|-------------------------|--|
| zkraceno – | identifikuje, zda se jedná o kompletní seznam zpráv (false), či je seznam zkrácen (true), |
| typZpravy – | obsahuje název služby, na kterou je zpráva odeslána. (Např.: nastaveniB2BUctu), |
| stavVyřízeníPožadavku – | určuje stav vyřízení požadavku, nabývá hodnot dle tabulky uvedené ke službě odeslaniZprav, |
| idSubjektu – | identifikátor subjektu, |
| typSubjektu – | typ subjektu. |

Příklad vstupu:

```
<avizoPozadavek xmlns="http://www.gem.com/b2b/wss/2" />
```

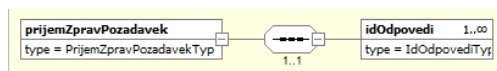
Příklad výstupu:

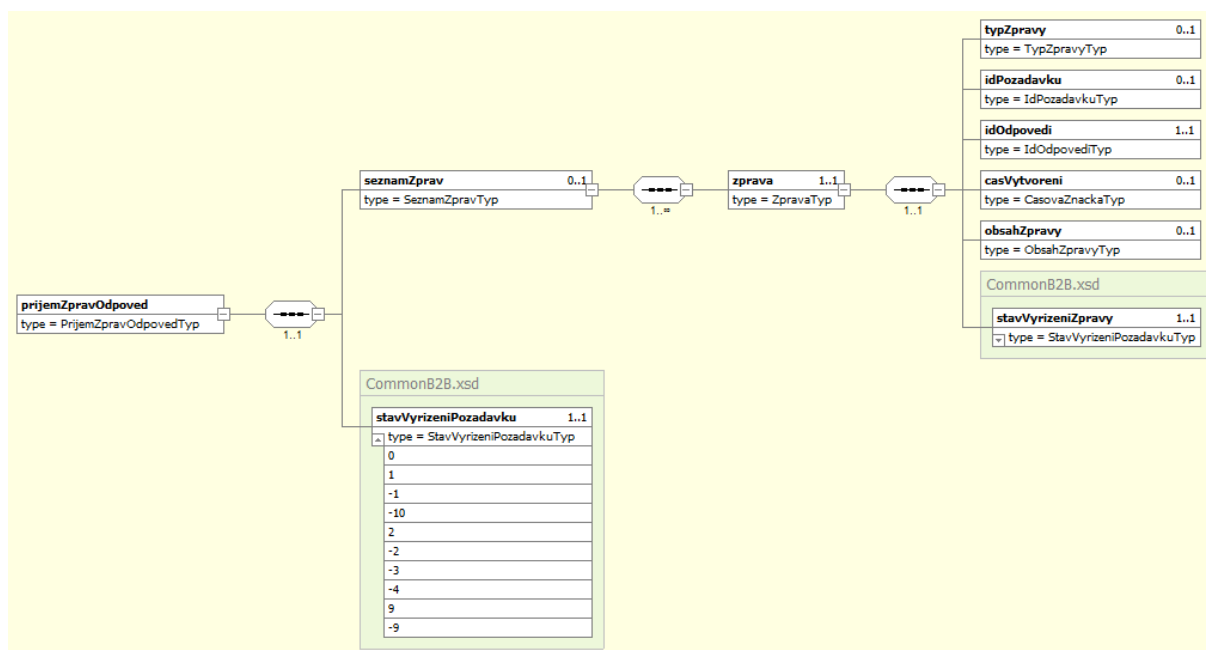
```
<avizoOdpoved xmlns="http://www.gem.com/b2b/wss/2">
  <avizoSeznamZprav zkraceno="false">
    <avizoZprava>
      <typZpravy>nastaveniB2BUctu2</typZpravy>
      <idPozadavku>23</idPozadavku>
      <idOdpovedi>99</idOdpovedi>
    </avizoZprava>
    <avizoZprava>
      <typZpravy>ObecnePodaniB2B</typZpravy>
      <idPozadavku>11</idPozadavku>
      <idOdpovedi>42</idOdpovedi>
    </avizoZprava>
  </avizoSeznamZprav>
  <stavVyřízeníPožadavku>1</stavVyřízeníPožadavku>
</avizoOdpoved>
```

1.1.3 Načtení zpráv

Služba vrátí konkrétní zprávu získanou ze seznamu zpráv k vyzvednutí přijatých službou avizo. Služba je implementována, aby umožňovala jednorázové stažení až pěti čekajících zpráv v jediném požadavku. Požadavek nevyžaduje digitální podpis. Služba se nechová atomicky, umožňuje vrátit částečná data, například pokud je v požadavku uvedeno chybné číslo jedné odpovědi. Každá zpráva proto obsahuje element stavVyřízeníZpravy. Element stavVyřízeníPožadavku se vztahuje k požadavku jako celku a obecně nabývá hodnoty 1. Odpověď bude opatřena digitálním podpisem.

K dokumentu je přiloženo XSD schéma: b2bwssadapter2.xsd, CommonB2B.xsd
a WSDL soubor: odeslaniZprav.wsdl.





Název služby: příjemZprav, endpoint WSSPrijemZprav

Typ: synchronní

Konzument: partner v privátní síti, který nemá možnost získat veřejnou IP adresu

Požadavek:

| | | |
|----------------------|-------------|-----|
| prijemZpravPozadavek | ComplexType | 1 |
| idOdpovedi | String | 1-5 |

Odpověď:

| | | |
|-----------------------|-------------|-----|
| prijemZpravOdpoved | ComplexType | 1 |
| seznamZprav | ComplexType | 0-1 |
| zprava | ComplexType | 1-5 |
| typZpravy | String | 0-1 |
| idPozadavku | String | 0-1 |
| idOdpovedi | String | 1 |
| casVytvoreni | DateTime | 0-1 |
| obsahZpravy | Base64 | 0-1 |
| stavVyrizeniZpravy | Enumeration | 1 |
| stavVyrizeniPozadavku | Enumeration | 1 |

Popis atributů zpráv:

- idPozadavku – element obsahuje unikátní identifikátor odesílané zprávy přidělený od VZP ČR. Odpovídá elementu idPozadavku uvedeném ve službě odeslaniZprav a avizo – lze tak podle tohoto elementu korelovat jednotlivé požadavky a odpovědi zasílané do VZP ČR,
- idOdpovedi – element obsahuje unikátní identifikátor odpovědi sestavené VZP ČR. Pod tímto identifikátorem se stahují zprávy službou příjemZprav a potvrzuje doručení službou pozvrzeniZprav,

- typZpravy – obsahuje název služby, na kterou je zpráva odeslána. (Např.: nastaveniB2BUctu),
- stavVyrizeniPozadavku – určuje stav vyřízení požadavku, nabývá hodnot dle tabulky uvedené ke službě odeslaniZprav,
- stavVyrizeniZpravy – určuje stav vyřízení zprávy, nabývá hodnot dle tabulky uvedené ke službě odeslaniZprav,
- obsahZpravy – obsah zprávy konkrétní služby ve formátu base64. Formát zprávy je definován v rámci dokumentace konkrétní služby,
- casVytvoreni – časová značka.

Příklad vstupu:

```
<prijemZpravPozadavek xmlns="http://www.gem.com/b2b/wss/2">
  <idOdpovedi>99</idOdpovedi>
  <idOdpovedi>42</idOdpovedi>
  <idOdpovedi>101</idOdpovedi>
</prijemZpravPozadavek>
```

Příklad výstupu:

```
<prijemZpravOdpoved xmlns="http://www.gem.com/b2b/wss/2">
  <seznamZprav>
    <zprava>
      <typZpravy>nastaveniB2BUctu2</typZpravy>
      <idPozadavku>23</idPozadavku>
      <idOdpovedi>99</idOdpovedi>
      <casVytvoreni>2012-09-18T13:21:51.000+02:00</casVytvoreni>
      <obsahZpravy>
PD94bWwgdMvYc2lrbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4NCjxuc2puYXN0YXZlbmlCMkJKVY3R1Mk
9kcG92ZWQgeGlsbnM6bnM9Imh0dHA6Ly93d3cuZ2Vtc3lzdGVtLmN6L0IyQlVwZGF0ZS8yLjAiPg0KICAg
PG5zOnNlcm5hbVByaWppbWVfueWNoWnByYXY+DQogICAgICA8bnM6cHJpamltYW5hWnByYXZhPg0KICAgIC
AgICA8PG5zOnR5cFpwcmlF2eT5Ob3RpZmlrYWw1T2JzYWw1Q2l2ZWxuaWt1QjJjCPC9uc2p0eXBacHJhdnk+
DQogICAgICA8bnM6c3Rhdlj5QcmlobGFzZW5pPC9uc2pzdGF2Pg0KICAgICA8PC9uc2pwcmlqaW1hbm
FachJHdmE+DQogICAgICA8bnM6cHJpamltYW5hWnByYXZhPg0KICAgICA8PG5zOnR5cFpwcmlF2eT5K
UkY8L25zOnR5cFpwcmlF2eT4NCiAgICA8IDxuc2pzdGF2PlByaWw1bm8L25zOnN0YXY+DQogIC
AgICA8L25zOnByaWppbWVfueWNoWnByYXZhPg0KICAgICA8IDwvbnM6c2V6bmFtUHJpamltYW55Y2hacHJhdj4NCiAg
IDxuc2pzdGF2VnlyaXplbm1Qb3phZGF2a3U+DQogICAgICA8bnM6a29kPjE8L25zOmtvZD4NCiAgIDwvbn
M6c3RhdlZ5cm16ZW5pUG96YWRhdmt1Pg0KPC9uc2puYXN0YXZlbmlCMkJKVY3R1Mk9kcG92ZWQ+
      </obsahZpravy>
      <stavVyrizeniZpravy>1</stavVyrizeniZpravy>
    </zprava>
    <zprava>
      <typZpravy>ObecnePodaniB2B</typZpravy>
      <idPozadavku>11</idPozadavku>
      <idOdpovedi>42</idOdpovedi>
      <casVytvoreni>2012-09-18T11:55:22.000+02:00</casVytvoreni>
      <obsahZpravy>
PG9iZWNUZVBvZGFuaUIyQk9kcG92ZWQgeGlsbnM6bnMwPSJodHRwOi8veGlsbnMuZ2Vtc3lzdGVtLmN6L09
iZWNUZVBvZGFuaUIyQk9kcGlsbnM9Imh0dHA6Ly94bWxucy5nZW1zeXN0ZW0uY3ovT2JlY25lUG9kYW5pQj
JCIj4NCiAgIDxrb3JlbGFiZjZVpwcmlF2eT4zODAwMDRjMmI2YmM8L2tvcmlsYXN0YXZlbmlCMkJKVY3R1Mk
Dp0ZXBh0T2Rwb3ZlZGk+UG9k4W7tIHD4aWTSbGVubjBlbm12YXRlbGkgcG9rYWw1Q2l2ZWxuaWt1QjJjCPC9uc2p0eXBacHJhdnk+
DQogICAgICA8bnM6c3RhdlZ5cm16ZW5pUG96YWRhdmt1PjE8L25zMDpzdGF2VnlyaXplbm1Qb3phZGF2a3U+DQo8L29iZWNUZVBvZGFuaUIyQk9kcG92ZWQ+DQ
o=
      </obsahZpravy>
      <stavVyrizeniZpravy>1</stavVyrizeniZpravy>
    </zprava>
  </seznamZprav>
  <idOdpovedi>101</idOdpovedi>
  <stavVyrizeniZpravy>0</stavVyrizeniZpravy>
</prijemZpravOdpoved>
```

```

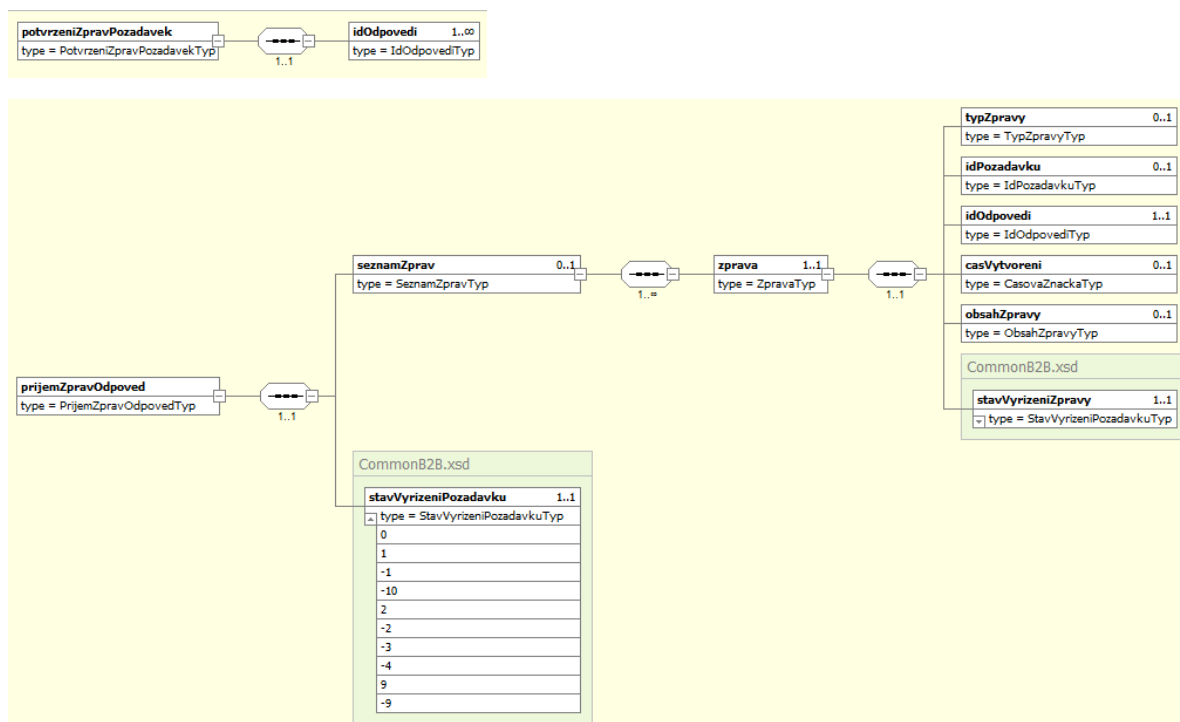
    </seznamZprav>
    <stavVyrizeniPozadavku>1</stavVyrizeniPozadavku>
  </prijemZpravOdpoved>

```

1.1.4 Potvrzení o načtení zpráv

Partner odešle na tuto službu potvrzení o převzetí dat ze služby prijemZprav. Služba umožňuje potvrdit převzetí více zpráv v jednom požadavku. Tímto okamžikem bude zpráva považována za doručenou, přestane se vracet ve službě avizo a nebude brána v potaz při výpočtu omezení pro posílání zpráv. Požadavek nevyžaduje digitální podpis. Služba se chová atomicky, je-li chybný jediný požadavek, je vrácena jeho identifikace v elementu idOdpovedi a celá operace nebude provedena.

K dokumentu je přiloženo XSD schéma: b2bwssadapter2.xsd, CommonB2B.xsd a WSDL soubor: odeslaniZprav.wsdl.



Název služby: potvrzeniZpravPozadavek, endpoint WSSPotvrzeniZprav

Konzument: partner v privátní síti, který nemá možnost získat veřejnou adresu

Typ: synchronní

Požadavek:

| | | |
|-------------------------|-------------|-----|
| potvrzeniZpravPozadavek | ComplexType | 1 |
| idOdpovedi | String | 1-n |

Odpověď:

| | | |
|-----------------------|-------------|-----|
| potvrzeniZpravOdpoved | ComplexType | 1 |
| idOdpovedi | String | 0-1 |
| stavVyrizeniPozadavku | Enumeration | 1 |

Popis atributů zpráv:

- idOdpovedi – potvrzeniZpravPozadavek: element obsahuje unikátní identifikátor odpovědi sestavené VZP ČR. Pod tímto identifikátorem se potvrzuje přijetí zprávy službou příjemZprav,
- idOdpovedi – potvrzeniZpravOdpoved: v případě chyby odkazuje na první nevalidní požadavek
- stavVyřízeníPozadavku – určuje stav vyřízení požadavku, nabývá hodnot dle tabulky uvedené ke službě odeslaniZprav.

Příklad vstupu 1:

```
<potvrzeniZpravPozadavek xmlns="http://www.gem.com/b2b/wss/2">
  <idOdpovedi>42</idOdpovedi>
  <idOdpovedi>99</idOdpovedi>
  <idOdpovedi>101</idOdpovedi>
</potvrzeniZpravPozadavek>
```

Příklad výstupu 1:

```
<potvrzeniZpravOpoved xmlns="http://www.gem.com/b2b/wss/2">
  <idOdpovedi>101</idOdpovedi>
  <stavVyřízeníPozadavku>0</stavVyřízeníPozadavku>
</potvrzeniZpravOpoved>
```

Příklad vstupu 2:

```
<potvrzeniZpravPozadavek xmlns="http://www.gem.com/b2b/wss/2">
  <idOdpovedi>42</idOdpovedi>
  <idOdpovedi>99</idOdpovedi>
</potvrzeniZpravPozadavek>
```

Příklad výstupu 2:

```
<potvrzeniZpravOpoved xmlns="http://www.gem.com/b2b/wss/2">
  <stavVyřízeníPozadavku>1</stavVyřízeníPozadavku>
</potvrzeniZpravOpoved>
```

1.2 Stav vyřízení požadavku

V rozhraní jsou používány společné stavy vyřízení požadavku. Jejich přehled je uveden v následující tabulce.

| Kód | Popis |
|-----|--|
| 0 | Data nenalezena |
| 1 | Nalezen jeden záznam nebo obecná návratová hodnota OK |
| 2 | Požadavek byl úspěšně přijat, zpracování bude pokračovat, očekávejte další odpověď |
| 9 | Nalezeno více záznamů |
| -1 | Technická chyba |
| -2 | Chyba vstupních dat |
| -3 | Role nemá oprávnění odesílat data |
| -4 | Duplicitní identifikace požadavku |
| -8 | Překročen limit nepřevzatých zpráv |
| -9 | Služba přijala požadavek, který bude zpracován později |
| -10 | Zpráva je určena pro jiné prostředí |

1.3 SOAP Message Security

Podle standardu SOAP Message Security se vkládá element <Security> do SOAP header standardní SOAP Envelope. Uvnitř je umístěn element <SignedInfo>, který v elementu <DigestValue> obsahuje SHA256 otisk celé SOAP zprávy, která je definována referencí. Následuje element <SignatureValue>, který nese vlastní elektronický podpis obsahu elementu <SignedInfo>. Na konci je připojena unikátní identifikace vydavatele certifikátu a sériové číslo certifikátu odesílatele v elementu <KeyInfo>. Alternativně je možné vložit podepisovací certifikát ve formátu X.509 do elementu <BinarySecurityToken> a referencovat jej v rámci elementu <KeyInfo>. Pro doplňující informace je dostupná dokumentace [8], [9].

Ukázkový obsah uvádí Obrázek 2:

```
<?xml version="1.0" encoding="UTF-8" standalone="1" ?>
<soapenv:Envelope xmlns:ns="http://www.gem.com/b2b/wss/2" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
      <ds:Signature Id="SIG-A8393EED5B5789D8E1143431564744314" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces PrefixList="ns soapenv" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </ds:CanonicalizationMethod>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
          <ds:Reference URI="#id-E22B85398311DA9B6F143351140586610">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces PrefixList="ns" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256" />
            <ds:DigestValue>eQCwulRLA4cfYmfgPLFSr+67drJeLxLqNw5irh0i6Zg=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>KB9YDc7eWnW2r2GEJWtvAYVTeYj189hs0+AfFMKR++EUy3+Qs4Ug6iVMDtAypgika/OxIUX24yMg ko7ibS4H65FAG6S</ds:SignatureValue>
        <ds:KeyInfo Id="KI-A8393EED5B5789D8E1143431564744112">
          <wsse:SecurityTokenReference wsu:Id="STR-A8393EED5B5789D8E1143431564744213">
            <ds:X509Data>
              <ds:X509IssuerSerial>
                <ds:X509IssuerName>OU=I.CA - Provider of Certification Services,O=První certifikační autorita,</ds:X509IssuerName>
                <ds:X509SerialNumber>2064677</ds:X509SerialNumber>
              </ds:X509IssuerSerial>
            </ds:X509Data>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
      <wsu:Timestamp wsu:Id="TS-A8393EED5B5789D8E1143431564743410">
        <wsu:Created>2015-06-14T21:00:47.434Z</wsu:Created>
        <wsu:Expires>2015-06-14T21:05:47.434Z</wsu:Expires>
      </wsu:Timestamp>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body wsu:Id="id-E22B85398311DA9B6F143351140586610" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
    <ns:odeslaniZpravPozadavek>
      <ns:typZpravy>SestavaPrehledUhradZPB2B</ns:typZpravy>
      <!--1 ox more repetitions:-->
      <ns:pozadavek poradiPozadavku="1">
        <ns:obsahZpravy>PG5zMtPpZXXN0YXZhUHJlaGx1ZFVocmFkWBkMkQJb3phZGF2ZWsgG1sbnM6bnMxPSJodHRwOi8v eG1sbnMuZ2Vtc3lzdG</ns:obsahZpravy>
      </ns:pozadavek>
    </ns:odeslaniZpravPozadavek>
  </soapenv:Body>
</soapenv:Envelope>
```

Obrázek 2 Digitálně podepsaná SOAP zpráva

```
<soapenv:Envelope xmlns:ns="http://www.gem.com/b2b/wss/2" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">  
  <soapenv:Header>  
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.xsd">  
      <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.xsd#Base64" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.X509v3">  
        <wsu:Id="X509-A8393EED5B5789D8E1143431624235916">MIIEpDCCA4yGwIBAglIDH4ElMAOGCSqGSIb3DQEBBCwUAMIGRMsCQCgYDVQGEJwJT      </wsse:BinarySecurityToken>  
      <ds:Signature Id="SIG-A8393EED5B5789D8E1143431624239019" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  
        <ds:SignedInfo>  
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">  
            <ec:InclusiveNamespaces PrefixList="ns soapenv" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />  
          </ds:CanonicalizationMethod>  
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />  
          <ds:Reference URI="#id-E22B85398311DA9B6F143351140586610">  
            <ds:Transforms>  
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">  
                <ec:InclusiveNamespaces PrefixList="ns" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />  
              </ds:Transform>  
            </ds:Transforms>  
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256" />  
            <ds:DigestValue=eQCWuRLA4cfYmfGPLFSr+67drJeLxLqNw5irh0i6Zg</ds:DigestValue>  
          </ds:Reference>  
        </ds:SignedInfo>  
        <ds:SignatureValue=KB9YDc7eWnW2r2GEjWtvAYVTeYj189hs0+AfmFKR++EUy3+Qs4Ug6iVMDtAppgika/OxIUX24ylMg ko7ibS4H65FAG6S</ds:SignatureValue>  
        <ds:KeyInfo Id="KI-A8393EED5B5789D8E1143431624236017">  
          <wsse:SecurityTokenReference wsu:Id="STR-A8393EED5B5789D8E1143431624236018">  
            <wsse:Reference URI="#X509-A8393EED5B5789D8E1143431624235916">  
              <wsse:ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.X509v3" />  
            </wsse:SecurityTokenReference>  
          </ds:KeyInfo>  
        </ds:Signature>  
        <wsu:Timestamp wsu:Id="TS-A8393EED5B5789D8E1143431624234915">  
          <wsu:Created>2015-06-14T21:10:42.349Z</wsu:Created>  
          <wsu:Expires>2015-06-14T21:15:42.349Z</wsu:Expires>  
        </wsu:Timestamp>  
      </wsse:Security>  
    </soapenv:Header>  
    <soapenv:Body wsu:Id="id-E22B85398311DA9B6F143351140586610" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.xsd">  
      <ns:odeslaniZpravPozadavek>  
        <ns:typ2pravyy>SestavaPrehledUhraďZPB2B</ns:typ2pravyy>  
        <!--1 or more repetitions-->  
        <ns:pozadavek poradiPozadavku="1">  
          <ns:obsahZpravyy>PG5zMTpzZXNOYXZhUHJlTGx1ZFVocmFkWlBMcKJQb3phZGF2ZWsgG1sbnM6bnMxPSJodHRwOi8v eG1sbnMuZ2Vtc3lzdGVzLnRlcw==</ns:obsahZpravyy>  
        </ns:pozadavek>  
      </ns:odeslaniZpravPozadavek>  
    </soapenv:Body>  
  </soapenv:Envelope>
```

Obrázek 3 Digitální podpis používající BinarySecurityToken

B2B používá následující algoritmy digitálních podpisů XML:

Tabulka 1 Významné standardy používané v rámci SOAP Message Security

| Parametr | Hodnota |
|------------------------|---|
| CanonicalizationMethod | Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" |
| SignatureMethod | Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" |
| Transform | Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" |
| DigestMethod | Algorithm="http://www.w3.org/2001/04/xmlenc#sha256 " |

1.4 Service endpoint ve WSDL

V příložených WSDL [11] souborech není uvedeno URL (endpoint) služby, ač WSDL obsahuje XML [12] element address [10] s atributem location. Hodnota atributu location dodaných WSDL je „*** SERVICE END-POINT LOCATION ***“ zejména proto, aby se zabránilo použití nevhodných URL služeb. Pro potřeby partnerů, vyvíjejících klientskou stranu těchto služeb, buď není nutné hodnotu atributu location nahrazovat skutečným URL (v běžně používaných vývojových nástrojích a vyrobených software je skutečné URL služby uloženo v konfiguraci, nikoliv ve WSDL potřebném pro vygenerování komunikující části klienta služby), nebo si atribut location doplní pro potřeby vývoje a testování sám partner záměnou za skutečná URL pro konkrétní prostředí.

Endpoint pro simulační prostředí:

`https://simu.b2b.vzp.cz/B2BProxy/HttpProxy/SIMUNazevSluzby`

Endpoint pro produkční prostředí:

`https://prod.b2b.vzp.cz/B2BProxy/HttpProxy/NazevSluzby`

„NazevSluzby“ bude vždy nahrazen konkrétním názvem volané služby, např.: WSSAvizo. Výsledný endpoint pro simulační prostředí bude: **`https://simu.b2b.vzp.cz/B2BProxy/HttpProxy/SIMUWSSAvizo`**.

1.4.1 Chybové výstupy

Kromě stavu VyrizeniPozadavku uvedených v kapitole 1.2, jsou chybové výstupy řešeny pomocí standardních prostředků WS - pomocí tagu Fault. Většina webových frameworků je schopna tyto chyby zpracovat automaticky a převést je na lokální výjimku.

Příklad chybového výstupu:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Server</faultcode>
      <faultstring>InvalidSecurity</faultstring>
      <detail/>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>
```

1.5 Poskytované služby na B2B rozhraní

Partner v privátní síti připraví požadavek podle popisu této služby, obsah požadavku vloží do elementu payload a odešle podle popisu pomocí synchronní služby Odeslání zpráv. Obdobným způsobem přijme i odpověď.

1.5.1 Nastavení B2B účtu

Tato asynchronní služba slouží partnerům pro nastavení a změnu parametrů B2B kanálu (certifikáty, nabízené služby). Partnerovi umožňuje nastavovat úvodní konfiguraci, objednávat přijímané zprávy a aktualizovat B2B certifikát. V odpovědi na nastavení (případně při prázdném požadavku) služba vrací seznam zpráv, které si partner může objednat, a rovněž, zda má tuto zprávu již objednanu. Objednání přijímaných zpráv umožňuje přihlášení partnera k pravidelnému zasílání zvolené zprávy. Seznam zpráv k objednáání bude uveden v odpovědi služby v elementu seznam přijímaných zpráv včetně aktuálního stavu. **Nastavení úvodní konfigurace není pro Partnery v privátní síti povinné.** Služba umožňuje pro danou registraci ve VZP ČR změnit typ komunikace v případě potřeby.

Název služby: nastaveniB2BUctu

Typ služby: asynchronní

Konzument: Každý partner komunikující asynchronními službami

Požadavek:

| | | |
|---------------------------|---------|-----|
| nastaveniB2BUctuPozadavek | Complex | 1 |
| nastavB2Bkomunikaci | Complex | 0-1 |

| | | | |
|--------------------------|---------|-----|----------------------|
| uvodniKonfigurace | Complex | 0-1 | SOAP |
| protokol | Enum | 1 | |
| seznamPrijimanychZprav | Complex | 0-1 | |
| prijimanaZprava | Complex | 0-n | |
| typZpravy | String | 1 | Prihlaseni/Odhlaseni |
| doplněkZpravy | String | 0-1 | |
| stav | Enum | 1 | |
| aktualizujB2BCertifikat | Complex | 0-1 | |
| zmenaLDAP | Complex | 0-1 | |
| uid | String | 1 | |
| novyPristupovyCertifikat | Base64 | 0-1 | |
| novyPodpisovyCertifikat | Base64 | 0-1 | |

Odpověď:

| | | |
|-------------------------|---------|-----|
| nastaveniB2BUctuOdpoved | Complex | 1 |
| seznamPrijimanychZprav | Complex | 0-1 |
| prijimanaZprava | Complex | 1-n |
| typZpravy | String | 1 |
| doplněkZpravy | String | 1 |
| stav | String | 0-1 |
| stavVyrizeniPozadavku | Enum | 1 |

Popis návratových kódů odpovědi (v XSD bez českých znaků):

- „-3 – Nejsou oprávnění pro realizaci části požadavku“
- „-1 – Chybné vstupní parametry služby“
- „0 – Služba přijala prázdný požadavek“
- „1 – Nastavení služby proběhlo úspěšně“

Popis atributů zpráv:

- uvodniKonfigurace – pro partnery v privátní síti se vyplňuje pouze subelement protokol konstantní hodnotou SOAP,
- protokol – zvolený komunikační protokol pro výměnu dat s VZP, aktuálně je podporován SOAP,
- typZpravy – název objednaných zpráv resp. služeb,
- doplněkZpravy – rozlišovací parametr k typu objednané zprávy je definovaný pro každou objednanou zprávu,
- uid – přihlašovací jméno definované v aplikaci spolupracujících subjektu v rámci procesu naparování uživatele a povolení B2B komunikace,
- novyPristupovyCertifikat – aktualizace přístupového certifikátu v době platnosti aktuálního certifikátu kterému se blíží čas vypršení. Obdobný význam má element novyPodpisovyCertifikat,
- seznamPrijimanychZprav.stav – v rámci požadavku je stav definován: Prihlaseni/Odhlaseni. V rámci odpovědi se stav může změnit v závislosti na oprávněních k objednávané službě. V případě, že se bude jednat o službu, na kterou nemá partner oprávnění, bude vrácen stav: NeniOpraveni.

1.5.2 Nastavení B2B účtu 2

Tato asynchronní služba slouží partnerům pro nastavení a změnu parametrů B2B kanálu (certifikáty, URL endpointu partnera, odebírané služby). Partnerovi umožňuje nastavovat úvodní konfiguraci v případě AS2 protokolu, objednávat přijímané zprávy a aktualizovat B2B certifikát. V odpovědi na nastavení (případně při prázdném požadavku) služba vrací seznam zpráv, které si partner může objednat, a rovněž, zda má tuto zprávu již objednanu. Objednání přijímaných zpráv umožňuje přihlášení partnera k pravidelnému zasílání zvolené zprávy. Seznam zpráv k objednání bude uveden v odpovědi služby v elementu seznam přijímaných zpráv včetně aktuálního stavu objednání. **Nastavení úvodní konfigurace není pro Partnery v privátní síti povinné.** Služba umožňuje pro danou registraci ve VZP ČR změnit typ komunikace v případě potřeby.

Název služby: nastaveniB2BUctu2

Konzument: Každý partner komunikující asynchronními službami

Typ služby: asynchronní

Požadavek:

| | | | |
|----------------------------|---------|-----|----------------------|
| nastaveniB2BUctu2Pozadavek | Complex | 1 | |
| nastavB2Bkomunikaci | Complex | 0-1 | |
| partnerUid | String | 0-1 | |
| uvodniKonfigurace | Complex | 0-1 | |
| protokol | Enum | 1 | AS2 |
| URI | String | 0-1 | |
| seznamPrijimanychZprav | Complex | 0-1 | |
| prijimanaZprava | Complex | 0-n | |
| typZpravy | String | 1 | |
| subjekt | Complex | 0-1 | |
| id | Enum | 1 | |
| typ | Enum | 1 | |
| stav | Enum | 1 | Prihlaseni/Odhlaseni |
| aktualizujB2BCertifikat | Complex | 0-1 | |
| zmenaLDAP | Complex | 0-1 | |
| uid | String | 1 | |
| novyPristupovyCertifikat | Base64 | 0-1 | |
| novyPodpisovyCertifikat | Base64 | 0-1 | |

Odpověď:

| | | |
|--------------------------|---------|-----|
| nastaveniB2BUctu2Odpoved | Complex | 1 |
| seznamPrijimanychZprav | Complex | 0-1 |
| prijimanaZprava | Complex | 1-n |
| typZpravy | String | 1 |
| subjekt | Complex | 1 |
| id | String | 1 |
| typ | Enum | 1 |
| stav | String | 0-1 |
| stavVyrizeniPozadavku | Enum | 1 |

Popis návratových kódů odpovědi (v XSD bez českých znaků):

- „-2 – Chyba vstupních dat“
- „-1 – Chybné vstupní parametry služby“
- „0 – Služba přijala prázdný požadavek“
- „1 – Nastavení služby proběhlo úspěšně“

Popis atributů zpráv:

| | |
|-------------------------------|--|
| protokol – | zvolený komunikační protokol pro výměnu dat s VZP, aktuálně je podporován AS2 a SOAP, |
| URI – | kompletní adresa endpointu (jen standardní https port), na kterou budou odesílány asynchronní odpovědi z VZP, |
| typZpravy – | název objednané zprávy, |
| subjekt – | specifikace subjektu, pro který je objednávaný typ zprávy, |
| uid – | unikátní identifikátor přidělený od VZP v rámci procesu registrace k B2B bráně VZP ČR, |
| novyPristupovyCertifikat – | aktualizace přístupového certifikátu v době platnosti aktuálního certifikátu, kterému se blíží čas vypršení. Obdobný význam má element novyPodpisovyCertifikat. |
| seznamPrijimanychZprav.stav – | v rámci požadavku je stav definován: Prihlaseni/Odhlaseni. V rámci odpovědi se stav může změnit v závislosti na oprávněních k objednávané službě. V případě, že se bude jednat o službu, na kterou nemá partner oprávnění, bude vrácen stav: NeniOpraveni. |

2. Často kladené otázky

Tato kapitola popisuje nejčastější dotazy partnerů, které jsou spojeny se simulačním a produkčním prostředím.

1. Odeslaná zpráva byla odmítnuta s chybou "Timestamp could not be validated".

WS-Policy ve WSDL služeb pro partnery v privátní síti vyžaduje přítomnost elementu wsu:Timestamp v odesílané zprávě. Hodnota podelementu wsu:Created nesmí být větší než aktuální čas na B2B bráně VZP ČR. Pokud má partner na počítači čas v budoucnosti, požadavek bude odmítnut touto chybou. Systém dokáže tolerovat až pětiminutový časový rozdíl. Doporučujeme používat synchronizaci času pomocí NTP protokolu.

3. Seznam zkratek

| Pojem | Význam pojmu |
|--------|---|
| HTTP | Hypertext Transfer Protocol. Jedná se o transportní protokol, který slouží ke komunikaci mezi klientem a serverem. |
| HTTPS | Protokol HTTP zabezpečený pomocí šifrovací vrstvy SSL. |
| SOAP | „Simple Object Access Protocol“ – Standardní protokol pro komunikaci mezi systémy a aplikacemi. Jeden ze základních kamenů webových služeb. Někdy interpretována jako „Service Oriented Architecture Protocol“. |
| SSL | Secure Socket Layer. Jedná se o šifrovací vrstvu pracující na principu symetrické kryptografie (jeden symetrický klíč). |
| SW | Software |
| VZP | Všeobecná zdravotní pojišťovna ČR |
| VZP ČR | Všeobecná zdravotní pojišťovna České republiky |
| XML | Značkovací jazyk používaný pro výměnu dat. |
| XMLSig | Standard podepisování XML struktur, XML dat. |

4. Použitá literatura

- [1] AS2 for Business Data Interchange Using HTTP; RFC 4130, <http://www.rfc-editor.org/rfc/rfc4130.txt>, <http://www.ietf.org/rfc/rfc4130.txt>.
- [2] Kořenové certifikáty certifikačních autorit:
<http://www.ica.cz/Korenove-certifikaty>
http://www.postsignum.cz/certifikaty_autorit.html
- [3] Popis akceptovaných certifikátů: <http://www.vzp.cz/e-komunikace/b2b-komunikace/podporovane-certifikaty>
- [4] Kvalifikovaný certifikát: <http://www.ica.cz/cz/menu/12/produkty-a-sluzby/zadost-o-certifikat/x2-kvalifikovany-certifikat/>
- [5] Komerční certifikát: <http://www.ica.cz/cz/menu/15/produkty-a-sluzby/zadost-o-certifikat/x5-komerčni-certifikat/>
- [6] Veřejná část přístupového a podpisového certifikátu VZP:
<http://www.vzp.cz/uploads/document/pristup-b2b-prod.zip>
<http://www.vzp.cz/uploads/document/podpis-b2b-prod.zip>
<http://www.vzp.cz/uploads/document/podpis-b2b-simu.zip>
<http://www.vzp.cz/uploads/document/pristup-b2b-simu.zip>
- [7] Informace pro uživatele ke kvalifikovaným certifikátům, MVCR
<http://www.mvcr.cz/clanek/informace-k-pouzivani-kvalifikovanych-certifikatu-pro-elektronicky-podpis-a-zaroven-pro-autentizaci-a-sifrovani.aspx#cara>
- [8] XMLSig varianta „enveloped“ <http://www.w3.org/TR/xmlsig-core/>
- [9] WS-Security <http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>
- [10] W3C SOAP standard: <http://www.w3.org/TR/soap/>
- [11] W3C WSDL standard: <http://www.w3.org/TR/wsdl>
- [12] W3C XML Schéma: <http://www.w3.org/XML/Schema>