



VŠEOBECNÁ
ZDRAVOTNÍ POJIŠŤOVNA
ČESKÉ REPUBLIKY

Alternativní rozhraní VZP Pointu

Určeno pro zaměstnavatele



1 Obsah

1	Obsah	2
2	Úvod	3
2.1	Adresa komunikační brány alternativního rozhraní VZP Pointu	3
3	Autentizace uživatele	3
4	Princip komunikace.....	3
5	Podepisování zpráv	4
5.1	Podporované hešovací funkce pro výtah zprávy	5
6	Rozhraní služeb.....	5
6.1	Odpovědi VZP Pointu	6
6.2	Hromadné oznámení zaměstnavatele	6
6.3	Předání přehledu plateb pojistného zaměstnavatele	6
7	Ukázky XML zpráv.....	7
7.1	Požadavek HOZ.....	7
7.2	Odpověď při úspěchu.....	7
7.3	Odpověď při chybě	8

2 Úvod

Tento dokument popisuje alternativní rozhraní VZP Pointu pro předání vybraných úloh zaměstnavatelů do VZP. Poskytované rozhraní je v plné shodě s rozhraním Portálu ZP a jeho účelem je usnadnění předávání dat.

Integrace SW uživatelů s tímto alternativním rozhraním je tak díky shodě s rozhraním Portálu ZP pouze otázkou konfigurace příslušného SW na straně uživatele.

2.1 Adresa komunikační brány alternativního rozhraní VZP Pointu

Adresa komunikační brány alternativního rozhraní VZP Pointu je:

https://point.vzp.cz/kom_brana.phtml

Poskytované rozhraní je plně v souladu s dokumentací Portálu ZP (*P4ZP_PHP-APP_KOM_TR06.DOC*), která je přílohou tohoto dokumentu. VZP Point nabízí pro zaměstnavatele tyto služby:

- předání hromadného oznámení zaměstnavatele (*Data.Ucel="HOZ"*)
- předání Přehledu plateb pojistného zaměstnavatele (*Data.Ucel="PPPZ"*)

Kompletní dokumentace k Portálu ZP je k dispozici na následující adrese:

<http://www.portalzp.cz/distribuce.ext/>

3 Autentizace uživatele

Autentizace uživatele je realizována prostřednictvím elektronického certifikátu. K podpisu předávaných podání (zpráv) je nutné použít certifikát, který má daný uživatel nastaven ve VZP Pointu.

4 Princip komunikace

Komunikace je realizována prostřednictvím protokolu HTTP/SSL bez použití klientského certifikátu. Klient sestaví a odešle HTTP POST požadavek šifrovaný prostřednictvím SSL, ve kterém předá parametr *request* obsahující XML data zprávy. Odpovědí je pak opět XML dokument.

Adresa komunikační brány VZP Pointu je (viz 2.1) a DTD definice XML, kterou musí veškerá komunikace splňovat, je ve všech případech ve společném souboru uloženém na adrese

http://www.portalzp.cz/portal_kl.dtd

Obsah dokumentu „portal_kl.dtd“:

```
<?xml version="1.0" encoding="ISO-8859-2"?>
<!--
    portal_kl.dtd created 06.10.2003
        last updated 16.03.2015

    Definice DTD pro XML komunikaci z/do komunikační brány klienta Portálu verze 1.6

    Copyright (c) 2003-2015 Asseco Central Europe, a.s.

    Author:
        Jaroslav Brtek, Pavel Koukal, Jiří Kletečka
-->

<!ELEMENT Komunikace (Data, (Podpis | Sms-request | Sms-auth)) >

<!ELEMENT Data          (Prihlaseni, Soubor*)>
<!ATTLIST Data
    Typ          (POZADAVEK |
                  ODPOVED   ) #REQUIRED
    Ucel         (VYU |
                  ORL |
                  HOZ |
                  PPPZ |
                  VERPOJ |
                  VERZZ |
                  PRESMER |
                  SCHRANKA |
                  EXE_FO |
                  EXE_PO |
                  AUTORIZACE |
                  P2_IMPORT |
                  NOVY_CERT ) #REQUIRED
    PZP_IdPodani CDATA          #IMPLIED
    PZP_Chycha   CDATA          #IMPLIED>

<!ELEMENT Prihlaseni    (#PCDATA)>
<!ATTLIST Prihlaseni    UnikatniInfo CDATA          #REQUIRED>

<!ELEMENT Soubor        (#PCDATA)>
<!ATTLIST Soubor
    Jmeno        CDATA          #REQUIRED
    Format       (TEXT |
                  BASE64 |
                  ZIP_BASE64 |
                  GZIP_BASE64 ) #REQUIRED>

<!ELEMENT Podpis        (#PCDATA)>

<!ELEMENT Sms-request   EMPTY>
<!ATTLIST Sms-request
    login        CDATA          #REQUIRED
    password     CDATA          #REQUIRED>

<!ELEMENT Sms-auth      EMPTY>
<!ATTLIST Sms-auth
    login        CDATA          #REQUIRED
    smskod       CDATA          #REQUIRED>
```

5 Podepisování zpráv

Elektronicky podepisované jsou všechny předávané zprávy a mechanismus podepisování je zvolen co nejjednodušší. XML zprávy obsahují element Podpis, jenž obsahuje podpis dat obsažených v elementu Data (včetně XML tagů). Vlastní podpis slouží pouze k ověření autenticity předávaných dat v elementu Data a je realizován ve formátu PKCS#7 a data podpisu již nesmějí z kapacitních důvodů obsahovat podepisovaná data ani certifikáty. Obě komunikující strany musejí znát své certifikáty navzájem.

5.1 Podporované hešovací funkce pro výtah zprávy

Při podpisu zprávy je třeba použít jednocestnou hešovací funkci (one-way hash function) pro vytvoření výťahu ze zprávy (message digest).

Název hešovací funkce	Popis
MD5	Jednocestný kryptovací algoritmus Message Digest 5
SHA-1	„Secure Hash Algorithm“ s délkou 160bit
SHA-256	„Secure Hash Algorithm“, tedy varianta SHA-2 s délkou 256bit
SHA-384	„Secure Hash Algorithm“, tedy varianta SHA-2 s délkou 384bit
SHA-512	„Secure Hash Algorithm“, tedy varianta SHA-2 s délkou 512bit

Tabulka 1 - Podporované hešovací funkce

V případě, že je použita nepodporovaná hešovací funkce, vrací alternativní rozhraní následující chybové hlášení, kde {0} představuje celý název nepodporované funkce a {1} pak kód Oid.

Nepodporovaný požadavek: Nepodporovaná hešovací funkce {0} ({1})

6 Rozhraní služeb

Služby Portálu ZP jsou realizovány prostřednictvím XML zpráv, které mají následující strukturu:

Název a umístění elementu	Datový typ	Multiplicita	Popis
Komunikace	ComplexType	1	Kořenový element
Data	ComplexType	1	Předávaná data
Typ	String	1	Typ zprávy (např. POZADAVEK, ODPOVED)
Ucel	String	1	Účel zprávy (HOZ, PPPZ)
Prihlaseni	ComplexType	0-1	Informace o uživateli (pouze pokud Typ=POZADAVEK)
UnikatniInfo	String	1	Unikátní identifikace podání daného uživatele (certifikátu)
Soubor	ComplexType	1-n	Předávaný soubor
Jmeno	String	1	Název předávaného souboru
Format	String	1	Formát dat souboru (např. BASE64, TEXT)
Podpis	String	1	Elektronický podpis podání

6.1 Odpovědi VZP Pointu

Odpovědi na požadavky jsou klientům předávány ve formě souborů následovně:

- v případě přijetí podání bez chyb obsahuje odpověď soubor *protocol.log* s informacemi o založení podání ve VZP Pointu, jako je číslo, čas a název podání
- v případě nepřijetí ze závažného důvodu, jako je např. chybný certifikát, obsahuje podání soubor *error.log* s popisem chyby
- veškerý obsah souboru *error.log* je v plain/text
- kódová stránka není definována, vracena je vždy taková kódová stránka, ve které je poslán požadavek. Pokud není kódová stránka zjištěna, je kódována v *UTF-8*.

6.2 Hromadné oznámení zaměstnavatele

Hromadné oznámení zaměstnavatele probíhá tak, že klientský systém předá prostřednictvím HTTP POST požadavku XML zprávu, kde atribut Data.Ucel="HOZ" a v atributu Data.Soubor je obsaženo samotné hlášení ve formátu DR souboru.

Odpověď je kódována v Base64, pro zobrazení obsahu je potřeba provést dekodování Base64.

6.3 Předání přehledu plateb pojistného zaměstnavatele

Předání přehledu o platbě zaměstnavatele probíhá tak, že klientský systém předá prostřednictvím HTTP POST požadavku XML zprávu, kde atribut Data.Ucel="PPPZ" a v atributu Data.Soubor je obsažen soubor s přehledem v DR formátu.

V případě této služby je chování identické jako v případě vyúčtování.

7 Ukázky XML zpráv

V této kapitole jsou uvedeny příklady zpráv pro HOZ (hromadné oznámení zaměstnavatele). Požadavky pro PPPZ jsou v principu formátované stejným způsobem.

7.1 Požadavek HOZ

Případ požadavku typu HOZ v kódování ibm852 (CP852, OEM 852 (Latin II), MS-DOS Latin 2). Ve formátu TEXT.

```
<?xml version="1.0" encoding="ibm852"?>
<Komunikace>
<Data Typ="POZADAVEK" Ucel="HOZ">
<Prihlaseni UnikatniInfo="123456789">Přihlašovací text v souladu s normou SN ETSI TS 101
456.</Prihlaseni>
<Soubor Jmeno="00028894.00" Format="TEXT">00209464461 Abel Jaroslav
30092015Rudé armády 5144 Horní Dunajovice 65185
</Soubor>
</Data>
<Podpis>-----BEGIN PKCS7-----
MIICIAIJKoZiHvcNAQcCoIICETCCAg0CAQExCzAJBgUrDgMCGGUAMAsGCSqGSIb3DQEHAQCAeww
ggHoAgEBMGYwXzELMAKGA1UEBhMCQ1oxLDAqBgNVBAoMI8SMZXNrw6EgcG/FoXRhLCBzLnAuIFtJ
xIwGNDcxMTQ050DNDMSiWIAyDVQQDEx1Qb3N0U2lnbnVtIFF1YWxpZm1lZCBDSQSAyAgMdkR4wCQYF
Kw4DAHoFAKBdMBGCSqGSIb3DQEJAzELBgqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTE2MDIx
MjExMTg0NlowIwYJKoZIhvcNAQkEMRYEFFwldpGFA7j6gd6I2TYb+5GkKRHFMA0GCSqGSIb3DQEB
AQUABIIBAEB+o/22i0huS0s4N614baTC1LsyWnh9KEmfoiithMUjN0ru0ztmegjroodaA1boNDyU
iTn0vOI27W4IusrKwH7TMSxHPvU5Zk26MRXqi0QDyG00wvq0JD75QSGLoii+Wu4tWGONJ7NxXiF0
ZV1UAJtBnWuV6rIuIZtE4jIzCKN3r4cCtXVRMIW0Sd2tr/JWmDzrV41g4WpVxqS4zQuG+ThgvxIn
tBNEORn3sz6Z6EEpNkmYwxiHqyTfdcmQmcgqwyqHdS1/JHSJYp05B5jwRXDjiJ41LBuSeQyZBEf
rSYHuMj3y/JDbuRjSwgRP1XuA+/jMUtoEuCF1LhDFHYrM1Y=
-----END PKCS7-----
</Podpis>
</Komunikace>
```

7.2 Odpověď při úspěchu

Při úspěšném provedení je v rámci *protocol.log* je vrácena informace o založení nového podání.

```
<?xml version="1.0" encoding="ibm852"?>
<Komunikace>
<Data Typ="ODPOVED" Ucel="HOZ" PZP_IdPodani="2498" PZP_Chyba="0">
<Soubor Jmeno="protocol.log"
Format="BASE64">WmUgc291Ym9ydSAnMDAwMjg4OTQ0MDAnIGJ5bG8gemFsb6d1bm8gcG9koG6hIDI0OTggKEhyb21hZG6CI
G96bqBtZW6hIHphbdhZdG5hdmF0ZWx1KQ0K</Soubor>
</Data>
<Podpis>-----BEGIN PKCS7-----
MIIBpwYJKoZIhvcNAQcCoIIBmDCCAQCAQExCzAJBgUrDgMCGGUAMAsGCSqGSIb3DQEHAQCAwMw
ggFvAgEBMG4wYDELMakGA1UEBhMCQ1oxNzA1BgNVBAoTL1ZzZW9iZWNUYSB6ZHJhdm90bmkgcG9q
aXN0b3ZuYSB0ZDZXRZSByZXB1Ymtpa3kxGDAWBgNVBAMTD1ZaUC1JbnRyYW5ldC1DQ0QIKFwMSQAB
AA10fDAJBgUrDgMCGGUAAoF0wGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHAQACBgkqhkiG9w0BCQUx
DxcNMTYwMjEjYmTEODQ0W4jAjbGkqhkiG9w0BCQXxGgQUuSuTiL/GeqcxK6rMcrzwgz8m0AwwDQYJ
KoZIhvcNAQEBBQAEgYAMNZcbspiik1EB0jyRbiINlyd0pGf2RHbWY+uCl6yGP30LOx/UXSSybgG4
esNyAUTx0vGwxQQ+6z0H4B8ZI8AeKpyfMAUkhKWgKNNpcREEYDINGC3P05SXPqvZehdZp08YqGA1
1UMSsz5zSjXMoHND9GyYILhZJ10fJ1tKLeoPteQ==
-----END PKCS7-----
</Podpis>
</Komunikace>
```

7.3 Odpověď při chybě

Po zanesení chyby do souboru v požadavku dojde k vrácení následujícího hlášení v rámci *error.log*.

Chyba zpracování souboru: Chybný formát vstupního souboru (00028894.00).

```
<?xml version="1.0" encoding="ibm852"?>
<Komunikace>
<Data Typ="ODPOVED" Ucel="H0Z" PZP_Chyba="ERR">
<Soubor Jmeno="error.log"
Format="BASE64">Q2h5YmEgenByYWVndqBuoSBzb3Vib3J1OiBDaHlibuwgZm9ybaB0IHZzdHVwbqFobyBzb3Vib3J1ICgwM
DAyODg5NC4wMCku</Soubor>
</Data>
<Podpis>-----BEGIN PKCS7-----
MIIBpwYJKoZIhvcNAQcCoIIBmDCCAQQCAQExCzAJBgUrDgMCGGUAMAsGCSqGSIb3DQEHAQGCAXMw
ggFvAgEBMG4wYDELMAkGA1UEBhMCQ1oxNzA1BgNVBAoTL1ZzZW9iZWNUYSB6ZHJhdm90bmkgcG9q
aXN0b3ZuYSBDZXNrZSByZXB1Ymtpa3kxGDAWBgNVBAMTD1ZaUC1JbnRyYW5ldC1DQIQKFiwmSQAB
AA10fDAJBgUrDgMCGGUAAoF0wGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHAQACBgkqhkiG9w0BCQUx
DxcNMTYwMjEyMTE1NjU0WjAjbGkqhkiG9w0BCQQxFgQU8Ff10uhqdMi6kwhheDXbbCbqh14wDQYJ
KoZIhvcNAQEBBQAEgYACgxGoarQs+X1XT8JJtu5dR+7Z1nfnSGW0HRwJfP/rDDToLbY/zJbQrJ4A
PXE5fJBoDo6EYG3hEywfSMcCwD0hIjeEf+ZMNQqbJ9uATbsYLxwkm6BceqSHH8p3wxqUBMaSprM+
ky0s3X6/GvqCOPaRYvozSv3MA18tz20cj0gXew==
-----END PKCS7-----
</Podpis>
</Komunikace>
```