B2B rozhraní VZP ČR

Popis rozhraní pro partnery

Obsah

SEZNAM OBRÁZKŮ 4
HISTORIE DOKUMENTU 5
ÚVOD 6
1. PODMÍNKY PRO POSKYTNUTÍ PŘÍSTUPU K B2B ROZHRANÍ 7
1.1 Zřízení přístupu k B2B rozhraní 7
1.2 Certifikáty pro komunikaci s partnery 7
2. SPECIFIKACE ROZHRANÍ PRO PARTNERY 9
2.1 Použité standardy 9
2.1.1 Synchronní komunikace 9
2.1.2 Asynchronní komunikace 10
2.1.3 Standard pro výměnu dat AS2 11
2.1.4 Vlastnosti AS2 protokolu vyžadované VZP ČR 12
2.1.4.1 Struktura AS2 zprávy 12
2.1.4.2 Nastavení asynchronní komunikace AS2 pro VZP ČR 12
2.1.5 Chybové stavy protokolu AS2 13
2.1.6 Kritéria úspěšné asynchronní komunikace 13
2.1.7 Návratové kódy HTTP komunikace v B2B kanálu 14
2.1.7.1 Popis vybraných návratových kódů 14
2.1.8 Řešení nepředpokládaných chybových stavů 16
3. PROVĚŘENÍ PARTNERSKÝCH APLIKACÍ 18
3.1 Prostředí pro simulaci 18
3.2 Rozhraní pro přístup k simulaci 18
3.2.1 Jmenná konvence endpointů pro účely simulace 18
3.3 Produkční prostředí 19
3.3.1 Jmenná konvence produkčních endpointů 19
3.4 Podmínky pro poskytování služeb 20
3.5 Poskytované služby na B2B rozhraní 20
3.5.1 Nastavení B2B účtu 20
3.5.2 Nastavení B2B účtu 2 22
3.6 AS2 Testovací / vzorový požadavek na B2B 24
3.7 AS2 Testovací / vzorová odpověď z B2B 26
4. ČASTO KLADENÉ OTÁZKY 28
5. SEZNAM ZKRATEK 29
6. POUŽITÁ LITERATURA 30

Seznam obrázků

Obrázek 1 – Model synchronní komunikace *9*
Obrázek 2 – Model asynchronní komunikace *11*
Obrázek 3 Rozhraní žurnálu, služba StavCertifikatuB2B *28*

Historie dokumentu

Verze	Datum	Autor	Popis
1.0	6. 8. 2009	HPServices	Založení dokumentu
4.1	9.3.2010	HPServices	Úprava dokumentu a doplnění standardního nastavení parametrů komunikace na B2B bránu
4.2	21.4.2010	HPServices	Doplnění specifikace pro používání B2B služeb, nastaveniB2BUctu,
4.3	19.7.2010	HPServices	Doplnění služby často kladených otázek
4.4	7.9.2010	HPServices	Doplněny informace o nových službách žurnálu B2B
5.0	19. 8. 2011	HPServices	Doplněn úvod, revize
5.1	27.3.2013	HPServices	Rozšířeno o službu NastaveniB2BUctu2
5.2	21.7.2015	HPServices	Popis StavVyrizeniPozadavku pro NastaveniB2BUctu2
5.3	15.6.2016	HPServices	Informace o kontrole certifikátu při použití služby NastaveniB2BUctu2
5.4.	13.4.2018	VZP ČR	Odebrání označení dokumentu jako Příloha č. 1 ke Smlouvě o spolupráci

Úvod

Tento dokument popisuje specifikaci řešení mezi-aplikační komunikace mezi informačním systémem VZP ČR a informačními systémy partnerů. Součástí dokumentu je specifikace komunikačního rozhraní. V rámci komunikačního rozhraní je detailně rozpracován komunikační kanál poskytující vybrané služby partnerům VZP ČR. Dokument je distribuován partnerům VZP ČR, kteří mají zájem komunikovat prostřednictvím B2B kanálu jako **příloha č. 1 smlouvy – „Technické podmínky přístupu na prostředí simulace B2B"**.

VZP ČR poskytuje přístup smluvním partnerům ke svému informačnímu systému. Tento přístup je realizován prostřednictvím B2B brány za využití moderních a otevřených standardů, jejichž popis je uveden dále v dokumentu. B2B brána umožňuje přístup k jednotlivým službám. Rozlišujeme dva typy služeb – synchronní a asynchronní.

Synchronní služby jsou dostupné skrze volání webových služeb protokolem SOAP. Přístup k asynchronním službám je realizován pomocí standardu AS2, který vychází z EDI. Alternativní rozhraní pro menší partnery, jejichž infrastruktura není nepřetržitě připojena k internetu nebo nemá pevnou IP adresu, je popsáno v dokumentu Popis rozhraní pro partnery v privátní síti. VZP ČR jej ale chápe jako nouzové řešení, které s sebou nese kapacitní omezení.

Během registrace partner dokládá smluvní vztah s vybraným subjektem, který hodlá zastupovat v B2B komunikaci. Subjektem může být například zdravotnické zařízení nebo zaměstnavatel. Identifikace subjektu bývá součástí zasílaných zpráv.

Veškerá komunikace probíhá šifrovaně pomocí protokolu SSL za použití klientských certifikátů. Tyto certifikáty jsou dále v textu označovány jako přístupové. Asynchronní zprávy se standardně podepisují podpisovými certifikáty. Během registrace partner předá veřejné klíče těchto certifikátů VZP ČR. Další certifikáty si může přidávat sám pomocí služby nastaveniB2BUctu2.

B2B brána VZP ČR autentizuje uživatele podle jeho přístupového certifikátu. Zároveň dojde i k autorizaci požadavku, kde se ověřuje smluvní vztah k subjektu identifikovanému ve zprávě. Dále zkontroluje, zda partner nepřekračuje smluvenou kapacitu zpráv. V případě překročení této kapacity jsou všechny požadavky zamítnuty do jejího opětovného uvolnění.

VZP ČR vybudovala simulační prostředí pro potřebu tvůrců aplikačního software (ASW) při vývoji a optimalizaci komunikačních modulů navázaných na služby B2B. Přístup do simulačního prostředí je poskytován zdarma na základě vzájemného smluvního vztahu.

1. Podmínky pro poskytnutí přístupu k B2B rozhraní

K tomu, aby bylo možné umožnit partnerovi nebo výrobci ASW přístup k B2B kanálu, musí splnit následující podmínky:

- musí být v odpovídajícím smluvním vztahu s VZP ČR,
- musí mít odpovídající certifikáty pro zajištění bezpečné komunikace s VZP ČR, přesný seznam certifikátů pro jednotlivé partnery je uveden v kapitole 1.2.
- výrobce ASW pro partnery bude dodržovat všechny použité standardy (2.1 Použité standardy)

1.1 Zřízení přístupu k B2B rozhraní

Standardní proces zřízení přístupu partnera k bráně B2B probíhá následujícím procesem:

1. Klient -> VZP ČR — žádost o elektronickou komunikaci
2. VZP ČR-> Klient — poskytnutí informace, vyžádání informací ke smlouvě/dodatku
3. VZP ČR-> Klient — smlouva/dodatek k podpisu
4. Klient <–> VZP ČR — podpis smlouvy/dodatku
5. Klient -> VZP ČR — předání certifikátu (ů) pro přístup a ověření podpisu
6. VZP ČR -> Klient — certifikát VZP ČR k ověření podpisu a komunikace s VZP (podpisový a přístupový certifikát)
7. VZP ČR — zaregistrování certifikátů, povolení přístupu, nastavení zastupování subjektu (ů) zdravotní péče
8. VZP ČR -> Klient — protokol o zaregistrování certifikátu (ů)
9. Klient — ověření elektronické komunikace, v případě asynchronní komunikace nastavení endpointu pro příjem zpráv VZP
10. VZP ČR — případné individuální nastavení přístupu ke službám

1.2 Certifikáty pro komunikaci s partnery

Pro zajištění bezpečné komunikace je vnější komunikace s VZP ČR vždy šifrovaná pomocí SSL. Komunikace na asynchronní služby je opatřena elektronickým podpisem. Každý partner použije přesný výčet povolených certifikátů [3] k ověření totožnosti a podpisu asynchronních zpráv. Platný certifikát je pouze ten, který obsahuje kompletní řetězec certifikátů. Každá komunikující strana zajistí u dohodnuté důvěryhodné autority následující certifikáty:

1. serverový certifikát, vydaný důvěryhodnou autoritou pro příslušný server, se kterým probíhá zabezpečená SSL komunikace (např.: CN=is.nemocnice.cz). Certifikát je vyžadován v případě asynchronní komunikace

2. komerční[1] certifikát, který bude sloužit k identifikaci partnera ve VZP (přístupový certifikát)

3. komerční[1] certifikát [5], u kterého bude privátní klíč sloužit k podepisování odeslaných zpráv a veřejná část bude použita ve VZP ČR k ověření podepsané zprávy,

Veřejná část certifikátů VZP (přístupový i podpisový pro obě prostředí) jsou ke stažení na adrese: [6].

[1] VZP ČR se na základě požadavků komunikujících partnerů rozhodla povolit komunikaci B2B brány i kvalifikovanými certifikáty.

Vzhledem k široké paletě certifikátů je doporučeno, aby výrobce ASW, který bude požadovat přístup k simulační variantě B2B kanálu k prověření vyrobeného ASW, přistupoval s typově stejnou sadou certifikátů jako partner, který bude ASW následně používat. Certifikáty výrobce ASW a reálného partnera jsou odlišeny vlastníkem.

2. Specifikace rozhraní pro partnery

Partneři pro komunikaci prostřednictvím B2B kanálu mají k dispozici dva základní typy rozhraní pro:

- synchronní komunikaci – využitelné pro rychlé ověření aktuálního stavu (např. stav pojištění)
- asynchronní komunikaci – typicky pro požadavky vyžadující manuální zpracování nebo pro předávání většího objemu dat.

2.1 Použité standardy

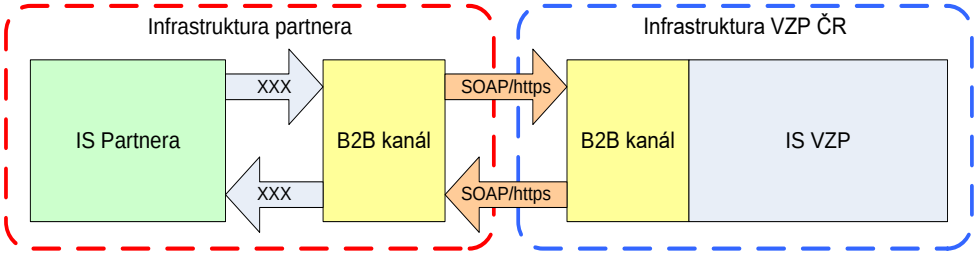
V rámci implementace řešení jsou využívány následující standardy pro komunikaci s partnery:

- **Synchronní komunikace** – standardní webová služba (SOAP [10]), šifrovaný transportní protokol http s použitím klientského certifikátu pro autentifikaci partnera na straně VZP ČR. Součástí popisu služeb je WSDL webové služby [11].
- **Asynchronní komunikace** – standard pro výměnu dat – AS2 **(Applicability Statement 2)** – tento standard je popsán v kapitole 2.1.3.
- **Standard pro formátování dat** – **XML** – V rámci definice vlastních schémat [12] se v jednotlivých případech vychází z již zavedených schémat – např. standard VZP.
- **Komunikace probíhá protokolem HTTP/1.1** – synchronní i asynchronní komunikace mezi partnerem a B2B probíhá metodou POST na úrovni HTTP/1.1 podle standardu, RFC 2616. **Komunikace je vždy zabezpečená pomocí šifrování SSL3.0 a TLS1.0. Komunikace probíhá pouze na standardním portu 443**.
- **Certifikáty** – bránou B2B jsou akceptovány pouze povolené certifikáty VZP ČR [3]. Každý partner musí mít nastavené všechny certifikáty VZP ČR jako důvěryhodné. Certifikáty jsou ke stažení na adrese: [2].

2.1.1 Synchronní komunikace

Při synchronní komunikaci klient webové služby integrovaný do informačního systému partnera VZP ČR vzdáleně volá webovou službu VZP a synchronně zpracuje odpověď.

Synchronní komunikace je zajištěna pomocí rozhraní synchronních webových služeb, které jsou dostupné partnerům VZP ČR přes zabezpečený protokol HTTPS.



Obrázek 1 – Model synchronní komunikace

Pro každou synchronní B2B službu je stanoven limit maximálního počtu volání služby jedním partnerem během daného časového okna. B2B kanál zajistí v případě překročení počtu volaní služby partnerem odmítnutí takového požadavku a zápis této události do auditního logu.

Doporučuje se, aby software partnera posílal na synchronní služby unikátní požadavky s předpokladem unikátní odpovědi. Opakované požadavky, s přihlédnutím k předpokládané četnosti změn v datech, by měly probíhat automaticky na straně softwaru partnera (tj. neměly by být odesílány do VZP).

Autentifikace jednotlivých klientů bude probíhat pomocí klientských certifikátů specifikovaných v kapitole 1.2. bod 2. Klient webové služby (B2B kanál partnera) naváže https spojení s B2B kanálem VZP ČR, který provede autentifikaci podle klientského certifikátu a autorizuje partnera k volání příslušné služby dle jeho role. Pokud nebude klientský certifikát autorizován, služba vrací HTTP chybu 401 – Unauthorized.

Vzhledem k omezenému přístupu ke službám může služba při častějším volání, než je dovoleno, vracet stavový kód 503- Service Unavailable. Pokud je partnerovi vrácen tento stav, je oprávněn volat službu znovu až po uplynutí doby udané parametrem návratové http hlavičky Retry-After, případně po době ne kratší než 1 minuta. Opětovné volání služby je povoleno pouze v případě návratového stavu 503, nikoli v případě výskytu chyb/stavů ostatních.

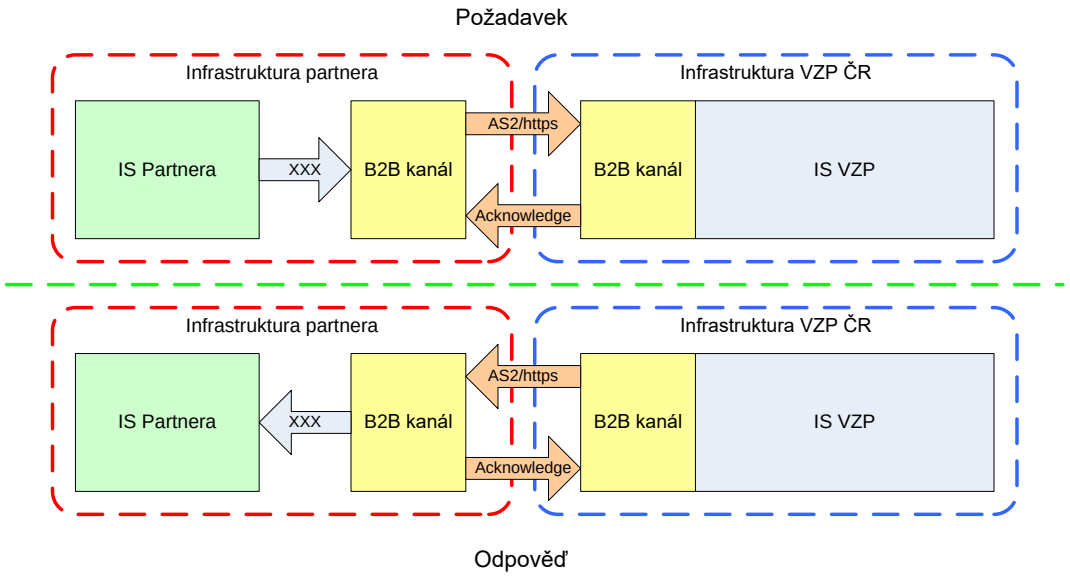
Při implementaci konzumace synchronní služby na straně partnera je doporučeno vzhledem k principu synchronní komunikace brát v úvahu i případ, kdy není služba dostupná z nějakého jiného důvodu než výše uvedené, tj. např. výpadek připojení k internetu na straně partnera nebo chyba v požadavku. Rovněž se předpokládá, že software partnera je připraven zpracovat chyby vzniklé v průběhu komunikace, především SoapException.

Další možné návratové kódy volání B2B a doporučená reakce ASW jsou popsány v kapitole 2.1.7 Návratové kódy HTTP komunikace.

2.1.2 Asynchronní komunikace

Při asynchronní komunikaci zasílá informační systém partnera podepsanou zprávu VZP nebo VZP zasílá podepsanou zprávu svému partnerovi. Zpráva má pevně stanovenou strukturu a zpravidla obsahuje větší množství informací, jejichž zpracování může být časově náročné. Příjemce zprávy vždy potvrdí zasilateli přijetí. Systém vzájemného potvrzení přijímaných zpráv zajišťuje neodmítnutelnost podání. Pokud je v rámci zpracování zprávy vyžadovaná další komunikace s odesilatelem (např. odeslání výsledků zpracování), je tato navazující komunikace řešena opět asynchronně. V rámci asynchronní komunikace B2B existují následující modely komunikace:

1. **Partner – VZP – Partner**: komunikaci inicializuje partner odesláním požadavku ve zprávě. Na odeslaný požadavek bude partnerovi doručeno potvrzení o přijetí požadavku (MDN). V tento okamžik začne ve VZP ČR kontrola správnosti a zpracování požadavku, na který je po dokončeném zpracování odeslána partnerovi jedna či více odpovědí. Čas na zpracování není předem určen, může trvat několik minut až několik dní. Partner vždy potvrdí každé přijetí odpovědi (zprávy) odesláním potvrzení o přijetí (MDN).
2. **Partner – VZP**: komunikaci inicializuje partner odesláním zprávy. Úspěšné přijetí bude partnerovi vždy potvrzeno odesláním potvrzovací zprávy (MDN).
3. **VZP – Partner – VZP**: komunikaci inicializuje VZP odesláním zprávy partnerovi. Partner takovou zprávu přijme a potvrdí odesláním potvrzovací zprávy (MDN). Asynchronně, v neurčený okamžik, odešle partner odpověď do VZP, která přijetí odpovědi vždy potvrdí.
4. **VZP – Partner**: komunikaci inicializuje VZP odesláním zprávy jednomu nebo více partnerům. Komunikace je používána k rozeslání informačních zpráv určených přesnému výčtu partnerů. Partneři přijetí každé zprávy potvrdí odesláním MDN.



Obrázek 2 – Model asynchronní komunikace

Partneři VZP zasílají při asynchronní komunikaci podepsané zprávy na B2B kanál pomocí transportního protokolu HTTPS. Zprávy budou podepsané certifikátem popsaným v kapitole 1.2 odstavec 3. V informačním systému partnera bude implementována komunikační komponenta zajišťující odesílání podepsaných zpráv (obsahem zprávy jsou XML metadata a dokument zakódovaný v base64) dle standardu AS2 [1] transportním protokolem HTTPS a příjem zpráv stejným protokolem.

Autentifikace jednotlivých klientů probíhá pomocí klientských certifikátů specifikovaných v kapitole 1.2. bod 2. Klient asynchronní služby (B2B kanál partnera) naváže HTTPS spojení s B2B kanálem, který provede autentifikaci podle klientského certifikátu a autorizuje partnera k odeslání zprávy dle jeho role. Pokud nebude klientský certifikát rozeznán nebo není platný, služba vrací chybu 401 – Unauthorized.

Vzhledem k omezenému přístupu ke službám může služba při častějším volání, než je dovoleno, vracet stavový kód 503- Service Unavailable. Pokud je partnerovi vrácen tento stav, je oprávněn volat službu znovu, a to po uplynutí doby udané parametrem návratové http hlavičky Retry-After, případně po době ne kratší než 1 minuta. Opětovné volání služby je povoleno pouze v případě návratového stavu 503, nikoli v případě výskytu chyb/stavů ostatních.

Další možné návratové kódy volání B2B a doporučená reakce ASW jsou popsány v kapitole 2.1.7 Návratové kódy HTTP komunikace.

Asynchronní komunikace probíhá standardně přes protokol AS2. Pokud provozní důvody brání jeho používání, lze použít API specifikované v dokumentu Popis rozhraní pro partnery v privátní síti. Toto API funguje na základě webových služeb, kde si partner stahuje zprávy pomocí pull modelu, na rozdíl od AS2 protokolu, který funguje na bázi push modelu. Rozhraní pro partnery v privátní síti vyžaduje častější komunikaci s B2B bránou VZP ČR, což může při nevhodně nastaveném intervalu komunikace vést k odmítnutí služby.

2.1.3 Standard pro výměnu dat AS2

AS2 (Applicability Statement 2 for Business Data Interchange Using HTTP; RFC 4130 [1]) vychází ze standardu EDIINT (EDI via Internet). Jedná se o standard specifikující proces výměny dat, popisující posílání a příjem dat přes bezpečné připojení. Protokol AS2 umožňuje bezpečně a spolehlivě přenášet data s využitím internetu. Bezpečnosti je dosaženo použitím digitálních certifikátů, šifrováním komunikace mimo VZP ČR a víceúrovňového ověření partnera, se kterým probíhá komunikace. Protokol AS2 je založen na standardu HTTP a zprávách S/MIME. Soubor, který se prostřednictvím protokolu odesílá, je zakódován jako standardní příloha AS2 zprávy. Zpráva přenášená protokolem AS2 je vždy podepsána elektronickým podpisem.

Systémy komunikující přes AS2 požadují potvrzení o doručení zprávy (MDN - Message Disposition Notifications). Po úspěšném ověření podpisu je odesláno oznámení o doručení, které je opět elektronicky podepsané. Oznámení o doručení MDN v B2B nenese žádnou informaci o úspěšnosti přijetí nebo zpracování zprávy v koncových systémech interního informačního systému VZP ČR. Protokol AS2 je v současnosti uznávaným standardem pro komunikaci mezi partnery (B2B), o čemž svědčí jeho implementace ve většině B2B řešení.

AS2 je schopen přenést jakýkoliv typ dat. Vlastní přenos funguje následujícím způsobem:

- data jsou na začátku procesu opatřena elektronickým podpisem (tento podpis nelze v případě použití pro automatizovaný mechanizmus podepisování považovat za kvalifikovaný [7])
- data jsou pomocí HTTPS protokolu přenesena adresátovi
- na straně příjemce je komunikace rozšifrována
- ověření elektronického podpisu zaručuje integritu přenesených dat
- odesilateli je zaslána potvrzující zpráva MDN

Protokol AS2 je specifikován v RFC 4130 uvedeným v dokumentaci [1].

2.1.4 Vlastnosti AS2 protokolu vyžadované VZP ČR

Implementovaný komunikační protokol AS2 v B2B kanálu partnera je specifikován následovně:

- typ zprávy je **Internet EDI MIME Message**
- zpráva AS2 **musí být podepsaná, nesmí byt šifrovaná** (šifruje se v rámci SSL spojení) a nesmí být komprimována (např. Zip, komprimovaný může být pouze obsah zprávy).
- MDN synchronní podepsané
- hašovací algoritmus pouze **SHA1/SHA2**
- obsah zprávy je ve formátu XML (***Content type:application/xml***)

2.1.4.1 Struktura AS2 zprávy

Podle RFC 4130, odstavec 4.2 je definovaných 8 typů správ. B2B kanál používá pouze následující:

- **No encryption, signature**

-RFC2616/2045
-RFC1847 (multipart/signed)
-RFC1767/RFC3023 (application/xml)
-RFC3851 (application/pkcs7-signature)

- **MDN over HTTP, signature**

-RFC2616/2045
-RFC1847 (multipart/signed)
-RFC3798 (message/disposition-notification)
-RFC3851 (application/pkcs7-signature)

2.1.4.2 Nastavení asynchronní komunikace AS2 pro VZP ČR

Konkrétní nastavení protokolu AS2 ve VZP ČR plně respektuje standard AS2 a je specifikováno tímto způsobem:

- Data **jsou** na začátku procesu **opatřena elektronickým podpisem**,
- data **nejsou na úrovni zpráv zašifrována**, šifrovací vrstva je realizována na úrovni pomocí SSL protokolu (HTTPS),
- data **nejsou komprimována,**
- data jsou pomocí HTTP/ HTTPS protokolu přenesena k příjemci,
- na straně příjemce je ověřen elektronický podpis zaručující integritu přenesených dat,
- odesilateli je **synchronně** zaslána podepsaná nebo nepodepsaná potvrzující zpráva (MDN),

- identifikace partnera komunikace **as2-from** bude obsahovat stejnou hodnotu jako používaný podpisový certifikát v položce Předmět (Subject) -> CN.

Takto probíhá komunikace oběma směry. Komunikujícímu partnerovi je znám název protistrany (druhého partnera), kterou je VZP ČR, a název partnera je **VZP**.

Přenášené zprávy jsou v XML formátu, pro přenos dále popisovaných zpráv je v komunikaci nutné nastavit parametr ***Content type:application/xml***.

Každá dále uváděná asynchronní služba popisuje požadavek a odpověď, což jsou dvě zprávy, které budou přeneseny přes bránu B2B VZP ČR. U popisu požadavku a odpovědi je vždy uváděna identifikace zprávy, kterou je nutné nastavit v komunikujícím B2B aplikačním software. Požadavek i odpověď budou vždy obsahovat parametr subject:

subject: <Název služby> + "Pozadavek"
(např.: PrehledUhradZPB2BPozadavek)
subject: <Název služby> + "Odpoved"
(např.: PrehledUhradZPB2BOdpoved)

Pro zprovoznění obousměrné asynchronní komunikace skrze AS2 protokol partner musí odeslat nejdříve konfigurační zprávu na službu Nastavení B2B účtu (viz kapitola 3.5.1)..

2.1.5 Chybové stavy protokolu AS2

Chyby v rámci AS2 protokolu se přenesou zpět k partnerovi přes MDN, pokud je možné MDN vytvořit. Ostatní chyby na úrovni HTTP se přenášejí standardně.

Chyby AS2 protokolu přenášené v rámci MDN jsou následující:

Chyba	Popis chyby
"Failure: **unsupported MIC-algorithms**"	Partner používá nepodporovaný hašovací algoritmus. Postup řešení: kontrola na straně partnera nebo dodavatele ASW a oprava chybné konfigurace ASW
"Error: **authentication-failed**"	B2B brána VZP ČR nedokázala ověřit partnera, tj. pravděpodobně partner na straně VZP ČR neexistuje nebo nebyl zaregistrován správný certifikát ve VZP ČR. Postup řešení: partner zkontroluje platnost svých certifikátů, případně s VZP ČR ověří správnost registrace certifikátů
"Error: **integrity-check-failed**"	Nebylo možné ověřit integritu obsahu správy, kontrolní součet (MIC) nesouhlasí. Postup řešení: pokud došlo k chybě v přenosu zprávy, partner přenos zopakuje, jinak je třeba ověřit podepisovací komponentu ASW.
"Error: **unexpected-processing-error**"	Jiný druh chyby při zpracovaní AS2. Postup řešení: partner se pokusí opakovat jeden přenos této zprávy za hodinu, pokud problém přetrvává, situace vyžaduje řešení problému od dodavatele ASW, případně komunikaci s podporou VZP ČR.

2.1.6 Kritéria úspěšné asynchronní komunikace

Pro komunikaci po AS2 protokolu musí mít partner v síti Internet přístupnou veřejnou doménovou adresu na portu443 (HTTPS), přes kterou bude komunikace probíhat zpět z VZP ČR. Nedoporučuje se používat pouze samotnou IP adresu, ale DNS záznam zejména proto, aby se nestalo, že při změnách v síti partnera nebude již veřejná IP adresa dostupná a partner zapomene včas provést změnu URL endpointu ve VZP ČR. Každá protistrana může být nezávislým iniciátorem komunikace a každá protistrana je nezávislým příjemcem komunikace. Komunikace probíhá přes internet způsobem VZP ←→ PARTNER vždy napřímo mezi partnerem a B2B bránou VZP ČR. V případě VZP ČR je vždy URL adresa pevná (např.: b2b.vzp.cz). Pokud bude mít partner proměnlivou IP adresu, tak si zajistí záznam Dynamické DNS pro komunikaci s konstantním URL. Pouze pro part-

nery, kteří nemají možnost získat veřejnou IP adresu, je zpřístupněna i omezená alternativa komunikace s využitím zabezpečených webových služeb [9] jako nouzové řešení pro „malé partnery“ (např. malé privátní lékařské praxe) – „Partneři v privátní síti“.

Pouze pro tyto partnery je způsob komunikace omezen a upraven na podobu synchronní komunikace s implementací kompletního zabezpečení. Partner v synchronní komunikaci musí implementovat mechanizmus podobný komunikaci asynchronním protokolem AS2. Všechny zprávy budou podepsané a bude probíhat vyzvedávání a odesílání potvrzení obdržení zprávy..

2.1.7 Návratové kódy HTTP komunikace v B2B kanálu

Komunikace v rámci B2B řešení je postavena převážně na HTTP protokolu nebo na jeho nadstavbách (tj. HTTPS, SOAP, AS2 příp. další). Z toho důvodu může B2B při komunikaci s partnerem vracet v principu všechny návratové kódy specifikované pro protokol HTTP (příp. jeho nadstavby). Některé z těchto kódů jsou pro chování B2B specifické a je vhodné, aby na ně partnerský ASW vhodným způsobem reagoval.

Tato kapitola shrnuje vybrané stavy/návratové kódy, upřesňuje jejich důvod vzniku a doporučuje příslušný způsob reakce partnerského ASW.

2.1.7.1 Popis vybraných návratových kódů

HTTP návratové kódy

Kód	Popis	Reakce ASW
401	„Unauthorized“ – použitý certifikát nebyl autorizován k přístupu k požadované službě.	Pokud stav přetrvává, vyžaduje kontaktovat VZP ČR a přidat či změnit přístupový certifikát B2B. ASW nemůže bez vnějšího zásahu administrátora dále přistupovat k požadovaným službám, a je proto nutné tento stav ošetřit ukládáním požadavků na straně ASW do zprovoznění přístupu ke službě.
403	„Forbidden“ – v rámci autorizace je zakázán ke službě přístup pomocí atributu B2B Kategorie.	Stav vyžaduje kontaktovat VZP ČR a požádat o úpravu přístupu ke službě (službám). ASW nemůže bez vnějšího zásahu administrátora dále přistupovat k požadovaným službám, a je proto nutné tento stav ošetřit ukládáním požadavků na straně ASW do zprovoznění přístupu ke službě.
404	„Not found“ – pro zadaný požadavek nebyla nalezena žádná služba.	Pokud partner pečlivě zkontroloval URL (URI) dotazované služby a URI služby je shodné s URL dříve sdělené od VZP ČR, kontaktuje partner VZP ČR. ASW nemůže bez vnějšího zásahu administrátora dále přistupovat k požadovaným službám, a je proto nutné tento stav ošetřit ukládáním požadavků na straně ASW do zprovoznění přístupu ke službě.
503	„Service Unavailable“ – služba je momentálně nedostupná. Odpověď obsahuje HTTP hlavičku „Retry-After“. Tento stav označuje aktuální přílišné vytížení služby.	Počet přístupu ke službám je řízen a upravován podle mohutnosti konkrétního partnera a aktuálního vytížení B2B brány. Pokud partnerský ASW zadá vyšší počet správných požadavků za stanovený čas, než je dovoleno, služba odpoví na požadavek tímto návratovým kódem. Pokud partner

Kód	Popis	Reakce ASW
		odešle řadu chybných požadavků na B2B bránu může být výsledkem rovněž odpověď 503 s uvedením času Retry-After kdy bude akceptován validní požadavek. V případě, že je v odpovědi uvedena HTTP hlavička „Retry-After“ s udáním času v sekundách, může se pokusit partnerský ASW po uplynutí uvedeného počtu sekund o opakovanou komunikaci. Není povoleno přistupovat na B2B bránu za čas kratší než Retry-After, protože bude docházet k neúměrnému přetěžování vstupní části B2B brány. V případě, že odpověď hlavičku „Retry-After“ neobsahuje, pokusí se ASW o opakovanou komunikaci nejdříve za 5 minut. Tento stav je nutné ošetřit ukládáním požadavků na straně ASW do uvolnění přístupu ke službě.
500	„Internal server error“ – služba je momentálně nefunkční.	Tento stav označuje nefunkčnost požadované služby, případně celého hostitelského serveru. Partnerský ASW v takovém případě opakuje svůj požadavek nejdříve za 2 hodiny. Tento stav je nutné ošetřit ukládáním požadavků na straně ASW do zprovoznění přístupu ke službě.

Ostatní návratové kódy

Protokol	Popis	Reakce ASW
TCP/IP	„Connection refused“/“Connection timeout“ – připojení k B2B bráně není dostupné, brána není funkční nebo přenos trval dlouhou dobu	Vzhledem k tomu, že nelze v tomto stavu přesně určit, kde na cestě od partnera k B2B bráně vznikl problém, aplikace by prvně měla doporučit obsluze prověřit lokální (na straně partnera/uživatele) připojení k internetu a povolené komunikaci na porty 443. V případě, že je lokální připojení k internetu v pořádku, aplikace se chová shodně, jako pro HTTP návratový kód 500 (viz výše). Tento stav je nutné ošetřit ukládáním požadavků na straně ASW do zprovoznění přístupu ke službě.
SSL	Chyba sestavení SSL kanálu – Chyba je na straně partnerského ASW v případě, že není umožněn přístup k přístupovému certifikátu.	Použitím síťových nástrojů pro analýzu síťové komunikace lze zjistit případné problémy v sestavování SSL komunikačního kanálu mezi partnerem a B2B VZP ČR. V případě, že je přístup k certifikátu v rámci ASW partnera plně funkční a problém je na straně B2B brány, opakuje ASW svůj požadavek po 4 hodinách. Tento stav je nutné ošetřit ukládáním požadavků na straně ASW do zprovoznění přístupu ke službě.

Protokol	Popis	Reakce ASW
SOAP	- odpověď neodpovídá datovému rozhraní očekávanému na partnerské ASW - požadavek neodpovídá datovému rozhraní očekávanému na serveru	partnerský ASW nemá k dispozici aktuálně platné rozhraní požadované služby. Stav vyžaduje kontaktovat VZP ČR a vyžádat si aktuální rozhraní konkrétní služby. ASW nemůže bez vnějšího zásahu administrátora ASW dále přistupovat k požadovaným službám, a je proto nutné tento stav ošetřit ukládáním požadavků na straně ASW do zprovoznění přístupu ke službě.

Další doporučené reakce partnerského ASW se již řídí rozhraním konkrétních služeb a jsou v rámci těchto služeb specifikovány.

2.1.8 Řešení nepředpokládaných chybových stavů

Komunikace B2B kanálem lze realizovat pouze vyrobeným ASW, který tuto komunikaci podporuje. VZP není výrobcem a není dodavatelem softwaru pro partnery. VZP nabízí služby, na které se partnerský ASW připojí.
Výrobce softwaru bude podporovat vlastní produkt dodaný partnerovi. Partner bude řešit rozdíly mezi očekávanou a skutečnou funkčností s dodavatelem softwaru. Partner, který využívá software ke komunikaci B2B kanálem, nemá možnost zjistit, kde skutečně chyba nastala. Je nutné, aby se koncový partner s problémy s používaným software obracel na dodavatele SW, nikoliv na VZP ČR.
Při vzniku chyby, kterou zjistí partner, se poradí s výrobcem používaného produktu v rámci jeho klientské podpory. Výrobce ve vlastním zájmu zkontroluje, zda chyba není v jeho produktu. Pokud je zjištěn rozdíl mezi specifikovanou a testovanou funkčnosti B2B kanálu, má výrobce možnost kontaktovat podporu B2B ve VZP ČR.

Před začátkem komunikace s podporou VZP ČR je potřeba mít připraveny následující informace:

- přesný popis partnera nebo zastupovaného subjektu,
- přesný popis očekávaného chování ASW a B2B kanálu (včetně velikosti přenášených dat),
- přesný popis nestandardního chování ASW a B2B kanálu,
- popis připojení (včetně rychlosti) k síti internet,
- popis nastavení firewall partnera, důraz je kladen na povolení SSL komunikace,
- seznam používaných a akceptovaných certifikátů,
- popis nastaveného URI pro komunikaci s VZP,
- popis a provedenou validaci odesílaných XML dat vůči definovanému XSD – XML data musí být validní,
- pokud je hlášen problém s dostupností služeb, je nutné znát název služeb, které nejsou dostupné.

Podpora VZP může vyžádat (pro porovnání) následující doplnění informací:

- záznam síťové komunikace na straně partnera,
- další informace týkající se síťové komunikace, které jsou potřeba k vyřešení nestandardního stavu.

Na základě dodaných informací bude výrobce ASW a VZP ČR provádět analýzu případného nestandardního stavu.
Partner se potenciálně může setkat s problémy, které nevyřeší VZP ČR ani dodavatel ASW, například:

- nefunguje síť na straně partnera - nutno řešit s poskytovatelem internetového připojení,
- bylo partnerovi změněno nastavení na firewalu, nefunguje například SSL na portu 443,
- rychlost připojení partnera k internetu kolísá nebo je nízká,
- počítač partnera je nakažen virem, který blokuje komunikaci do sítě,
- případně další neznámé chyby, které mohou nastat v průběhu komunikace.

3. Prověření partnerských aplikací

Pro účely prověření správné funkčnosti partnerské komunikace bude zveřejněno simulační B2B rozhraní, které bude partnerům ve standardním B2B rozhraní poskytovat pouze simulační data. Toto simulační rozhraní bude využito k prověření vyvinutého ASW a partnerského B2B rozhraní.

V rámci přípravy procesu ověřování ASW daného partnera musí být splněny následující kroky:

- Partner obdrží dokumentaci B2B rozhraní.
- Partner si zřídí svůj testovací přístupový a podpisový certifikát a předá jej VZP ČR.
- Operátor simulačního prostředí zavede příslušný záznam do simulační instance B2B kanálu.
- Partner zahájí proces prověřování rozhraní.

3.1 Prostředí pro simulaci

Toto prostředí je určeno pro vývojové týmy, které připravily software pro partnery VZP. Prostředí bude spuštěno oproti produkčnímu s omezeným rozsahem zdrojů. Účelem simulačního prostředí je zpřístupnit partnerům vyvíjejícím software podobné prostředí produkčnímu pro zajištění kvality vyrobeného ASW zejména z pohledu integračních testů. Toto prostředí bude umožňovat přístup k simulačním datům všech služeb přístupných přes B2B kanál.

3.2 Rozhraní pro přístup k simulaci

Simulační rozhraní budou vyvěšena na adresách oddělených od produkčního rozhraní. V následující podkapitole je popis sestavení URL služby.

3.2.1 Jmenná konvence endpointů pro účely simulace

Volané endpointy služeb pro simulaci B2B budou ASW sestaveny podle definovaného pravidla. Pro synchronní služby i asynchronní služby se bude používat následující endpoint:

https://simu.b2b.vzp.cz/B2BProxy/HttpProxy/SIMU*NazevSluzby*

„NazevSluzby“ bude vždy nahrazen konkrétním názvem volané služby, např.: PrehledUhradZPB2B. Doplňující informace nastavení URI vztahující se k žurnálu komunikace jsou uvedeny v dokumentu [12].

VZP si vyhrazuje právo individuálně změnit partnerovi název služby nebo endpointu po předchozím oznámení výrobci ASW. Výrobce ASW je povinen tuto změnu akceptovat a bezodkladně aktualizovat klientovi ověřený ASW s uvedenou změnou.

3.3 Produkční prostředí

3.3.1 Jmenná konvence produkčních endpointů

Volané endpointy produkčních služeb pro partnery VZP budou ASW sestaveny podle definovaného pravidla. Pro synchronní i asynchronní služby se bude používat stejný endpoint:

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

„NazevSluzby“ bude vždy nahrazen konkrétním názvem volané služby, např.: PrehledUhradZPB2B. Doplňující informace nastavení uri vztahující se k žurnálu komunikace jsou uvedeny v dokumentu [12].

Odchozí komunikace bude z uvedeného endpointu **b2b.vzp.cz**.

Komunikace na službu VratEndpoint je pro zachování kompatibility s partnery dostupná. Nepředpokládá se další podpora nebo rozšíření této služby. Nově připravovaný ASW by neměl na tuto službu přistupovat.

VZP ČR si vyhrazuje právo individuálně změnit partnerovi název služby nebo endpointu po předchozím oznámení výrobci ASW. Výrobce ASW je povinen tuto změnu akceptovat a bezodkladně aktualizovat klientovi ověřený ASW s uvedenou změnou.

3.4 Podmínky pro poskytování služeb

Aplikace B2B umožňuje partnerům komunikovat s VZP pomocí zpráv a taktéž získávat potřebná data k tomuto účelu poskytována. Všichni partneři komunikují stejným B2B kanálem podle dohodnutých pravidel. Pro zajištění komunikace všech partnerů současně je každý partner povinen dohodnutá pravidla dodržovat a nepřekračovat individuálně přiřazené parametry. Pouze tímto způsobem je možné zajistit spravedlivý přístup všech komunikujících partnerů k přiřazeným službám.

Vzhledem k tomu, že se jedná o optimální nastavení parametrů komunikace všech partnerů, určuje nastavení parametrů komunikace B2B kanálem VZP. V závislosti na počtu komunikujících partnerů je VZP oprávněna provést korekce nastavení povolených přístupů tak, aby zachovala stejnou kvalitu služeb pro každého komunikujícího partnera a nedocházelo k vzájemnému omezování. Nastavené parametry komunikace jsou každému partnerovi definovány individuálně tak, aby partner mohl ihned začít komunikovat a svou aktivitou neomezil ostatní partnery a vnitřní systémy. Případné požadavky na změny v nastavení parametrů komunikace ze strany partnera budou posouzeny a po důkladné analýze vlivů požadovaného nastavení na ostatní partnery a vnitřní aplikace VZP rozhodne o dalším postupu.

Parametrem komunikace partnera s B2B bránou je B2B Kategorie, kterou určí VZP při zavádění partnera do vnitřních systémů. B2B Kategorie dovoluje partnerovi početné využití služby podle vzájemně dohodnutých kritérií. V případě, kdy partner obdrží odpověď od B2B brány s chybou 503, znamená to, že se pokusil odesílat požadavky rychleji, že partner překročil možnosti přiřazené B2B kategorie. V hlavičce HTTP komunikace partner obdrží odpověď „Retry-After“ s udáním času v sekundách, který předepisuje partnerovi, kdy může začít opětovně komunikovat. Není povoleno přistupovat na B2B bránu za čas kratší než Retry-After, protože bude docházet k neúměrnému přetěžování vstupní části B2B brány. Tento stav je nutné ošetřit ukládáním požadavků na straně ASW do uvolnění přístupu ke službě. Další kódy komunikace popisuje kapitola 2.1.7.1.

Odpovědi na asynchronní požadavky B2B brány se obvykle pohybují v rozsahu minut až dní. Rychlost vyřízení odpovědi vždy závisí na aktuálním vytížení provozních systémů, procesu zpracování zprávy a typu zprávy. U některých typů zpráv dochází k řadě kontrol, které prověřují opodstatněnost a oprávněnost předané žádosti a nelze očekávat, že veškeré akce budou provedeny během krátké doby. Další typy zpracovávání mohou souviset s uzávěrkou v rámci konkrétního období a rovněž zde může být očekávána odpověď až po provedení návazných akcí.

U všech parametrů se předpokládá, že partner odesílá požadavky na stabilní doménová jména B2B definovaná v kapitole 3.3.1 a nikoliv pouze na příslušející IP adresu, která se může změnit. Odesílání zpráv na relevantní IP adresu není dovoleno.

3.5 Poskytované služby na B2B rozhraní

B2B brána VZP ČR nabízí obecnou konfigurační asynchronní službu **Update B2B účtu** ve starší a novější verzi**.** Služby umožňují partnerům nastavit a změnit některé parametry svého B2B účtu vedeného u VZP ČR. Jedná se především o certifikáty, URL endpointu partnera, nabízené/objednané služby. Tyto služby používají všichni partneři, komunikující asynchronními službami, zejména pak ti komunikující AS2 protokolem pro konfiguraci endpointu pro příjem odpovědí. Bez správně nastaveného endpointu pro příjem zpráv nebude možné využívat služby pro asynchronní komunikaci.

Další služby jsou popsány v přiložených dokumentech. Součástí dokumentace jsou XSD schémata přesně popisující formát vstupních a výstupních dat každé služby.

3.5.1 Nastavení B2B účtu

Tato asynchronní služba slouží partnerům pro nastavení a změnu parametrů B2B kanálu (certifikáty, URL endpointu partnera). Partnerovi umožňuje nastavovat úvodní konfiguraci v případě AS2 protokolu 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 objednánu. 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. Dokud nebude zadáno validní URI, B2B brána nemůže doručit žádnou odpověď na požadavek ani jinou zprávu.

Služba je již zastaralá a zůstává zde pouze ke zpětné kompatibilitě. V kapitole 3.5.2 je popsána nová služba NastaveniB2BUctu2, která slouží ke stejnému účelu a rozšiřuje možnosti stávající služby.

Název služby: nastaveniB2BUctu

Konzument: Každý partner komunikující asynchronními službami

Typ služby: asynchronní

Požadavek:

nastaveniB2BUctuPozadavek	Complex	1		
nastavB2Bkomunikaci	Complex	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		
doplnekZpravy	String	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:

nastaveniB2BUctuOdpoved	Complex	1	
seznamPrijimanychZprav	Complex	0-1	
prijimanaZprava	Complex	1-n	
typZpravy	String	1	
doplnekZpravy	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:

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,

doplnekZpravy – rozlišovací parametr k typu objednané zprávy je definovaný pro každou objednávanou zprávu,

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 – Element se již nadále nepoužívá. V odpovědích server nevrací element seznamPrijimanychZprav.

3.5.2 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 objednánu. 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. Dokud nebude zadáno validní URI, B2B brána nemůže doručit žádnou odpověď na požadavek ani jinou zprávu.

Při aktualizaci certifikátu pomocí této služby dochází k jeho kontrole. Požadavky na certifikát jsou následující:

- certifikát musí být platný,
- byl vydán certifikační autoritou, která je na seznamu povolených autorit VZP ČR,
- prodloužit lze pouze certifikát, který obsahuje stejný „subject“ a „issuer“, jako platný certifikát již zavedený ve VZP ČR.

Pokud certifikát tyto podmínky nesplňuje, služba vrátí stavVyrizeniPozadavku **-2**.

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 – Technická chyba IS VZP (dříve 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 vracen stav: NeniOpravneni.

3.6 AS2 Testovací / vzorový požadavek na B2B

Požadavek odesílaný protokolem AS2 obsahuje custom xml data, která splňují standard RFC 4130 [1]. Následující příklad uvádí **požadavek** a **odpověď**, v rámci jedné „session“, sledované na síťové úrovni. Synchronní odpověď, ve vzorovém požadavku, obsahuje podepsané MDN.

```
POST /gem-as2-web/HttpReceiver HTTP/1.1
AS2-Version: 1.1
mime-version: 1.0
recipient-address: http://app06h:7001/gem-as2-web/HttpReceiver
message-id: <AS2-1238659827527-12@SIMPARTNER_VZP>
as2-from: SIMPARTNER
as2-to: VZP
subject: PrehledUhradZPB2BPozadavek
from: as2@company.com
connection: close, TE
date: Thu, 02 Apr 2009 10:10:27 CEST
Content-Type:  multipart/signed; protocol="application/pkcs7-signature"; micalg=sha1;  boundary="----=_Part_53_2776593.1238659827527"
disposition-notification-to: http://192.168.3.43/_as2/HttpReceiver
disposition-notification-options: signed-receipt-protocol=optional, pkcs7-signature; signed-receipt-micalg=optional, sha1, md5
content-disposition: attachment; filename="smime.p7m"
User-Agent: gem_test_AS2
Host: app06h:7001
Expect: 100-continue
Content-Length: 5075

HTTP/1.1 100 Continue

------=_Part_53_2776593.1238659827527
Content-Type: application/xml
Content-Transfer-Encoding: binary
Content-Disposition: attachment; filename=TC01_platneRC.xml
<ns1:sestavaPrehledUhradZPB2BPozadavek xmlns:ns1="http://xmlns.gemsystem.cz/B2B/sestavaPrehledUhradZP">
   <ns1:idZpravy>72237</ns1:idZpravy>
   <ns1:sestavaPUZPPozadavek>
      <ns1:rodneCislo>8045095907</ns1:rodneCislo>
      <ns1:od>
         <ns1:mesic>1</ns1:mesic>
         <ns1:rok>2008</ns1:rok>
      </ns1:od>
      <ns1:do>
         <ns1:mesic>3</ns1:mesic>
         <ns1:rok>2008</ns1:rok>
      </ns1:do>
      <ns1:filtr>
         <ns1:lazne>Ano</ns1:lazne>
         <ns1:ozdravovny>Ano</ns1:ozdravovny>
         <ns1:zahranicniPlatby>Ano</ns1:zahranicniPlatby>
         <ns1:kapitace>Ano</ns1:kapitace>
      </ns1:filtr>
      <ns1:typSestavy>PDef</ns1:typSestavy>
   </ns1:sestavaPUZPPozadavek>
</ns1:sestavaPrehledUhradZPB2BPozadavek>
```

```
------=_Part_53_2776593.1238659827527
Content-Type: application/pkcs7-signature; name=smime.p7s; smime-type=signed-data
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIAwggSbMIID
…
h1SDjANMhYB24aaU25gHE7G/zMBxuVTaQEnrWoM+iZCiWZ06KyLhWcTbf74Ooa8rnViBmuwgT4ZI
PIKkl5RWcGrGiR2yjRxr9wAAAAAAAA==
------=_Part_53_2776593.1238659827527--

HTTP/1.1 200 OK
Connection: close
Date: Thu, 02 Apr 2009 08:10:30 GMT
Server: GEM System AS2
Content-Length: 7491
Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg=sha1;  boundary="----=_Part_14_33119478.1238659830566"
AS2-To: SIMPARTNER
Subject: Message Delivery Notification
From: as2@company.com
AS2-Version: 1.1
Mime-Version: 1.0
AS2-From: VZP
X-Powered-By: Servlet/2.5 JSP/2.1
Message-ID: <GEM_AS2-1238659830527-8@VZP_SIMPARTNER>

------=_Part_14_33119478.1238659830566
Content-Type: multipart/report; report-type=disposition-notification;  boundary="----=_Part_13_31624232.1238659830532"

------=_Part_13_31624232.1238659830532
Content-Type: text/plain
Content-Transfer-Encoding: 7bit
The AS2 message has been received.

------=_Part_13_31624232.1238659830532
Content-Type: message/disposition-notification
Content-Transfer-Encoding: 7bit
Reporting-UA: GEM System AS2
Original-Recipient: rfc822; VZP
Final-Recipient: rfc822; VZP
Original-Message-ID: <AS2-1238659827527-12@SIMPARTNER_VZP>
Disposition: automatic-action/MDN-sent-automatically; processed
Received-Content-MIC: MDFtygobAlqBUDBKhn9Lp95NbpA=, sha1

------=_Part_13_31624232.1238659830532--

------=_Part_14_33119478.1238659830566
Content-Type: application/pkcs7-signature; name=smime.p7s; smime-type=signed-data
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIAwggW6MIIE
oqADAgECAgoZIx+NAAEAAdM5MA0GCSqGSIb3DQEBBQUAMGkxGzAZBgkqhkiG9w0BCQEWDHN1YkNB
…
QHZ6cC5jejELMAkGA1UEBhMCQ1oxDDAKBgNVBAoTA1ZaUDEPMA0GA1UECxMGQ0EtVzNLMR4wHAYD
VQQDExVWWlAgQ1IgU3Vib3JkaW5hdGUgQ0EwHhcNMDkwMzMxMTEzMTE5WhcNMTEwMzMxMTEzMTE5
sCwmvHPQIZXT84JaaUgK1wt4jjjCmgiyX6++ntBvmeCrXJElVpyOZipP9EOBUsuHLQIVqRHF7Tjw
kyArPRRR+akAAAAAAAA=
------=_Part_14_33119478.1238659830566--
```

3.7 AS2 Testovací / vzorová odpověď z B2B

POST /mec_as2/HttpReceiver HTTP/1.1
AS2-Version: 1.1
mime-version: 1.0
recipient-address: http://192.168.3.43:8088/_as2/HttpReceiver
message-id: <GEM_AS2-1238675091343-17@VZP_SIMPARTNER>
as2-from: VZP
as2-to: SIMPARTNER
subject: PrehledUhradZPB2BOdpoved
from: sender@gemsystem.cz
connection: close, TE
date: Thu, 02 Apr 2009 14:24:51 CEST
Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg=sha1; boundary="----=_Part_27_18547941.1238675091376"
disposition-notification-to: http://localhost:7001/gem-as2-web/HttpReceiver
disposition-notification-options: signed-receipt-protocol=optional, pkcs7-signature; signed-receipt-micalg=optional, sha1, md5
content-disposition: attachment; filename="smime.p7m"
User-Agent: AS2 1.0 build 0 - http://www.gemsystem.cz
Host: 192.168.3.43:8088
Expect: 100-continue
Content-Length: 28175

HTTP/1.1 100 Continue

------=_Part_27_18547941.1238675091376
Content-Type: application/xml
Content-Transfer-Encoding: binary
Content-Disposition: attachment; filename=data.raw
<sestavaPrehledUhradZPB2BOdpoved xmlns="http://xmlns.gemsystem.cz/B2B/sestavaPrehledUhradZP">
  <stavVyrizeniPozadavku>
    <kod>1</kod>
    <popis/>
  </stavVyrizeniPozadavku>
  <korelaceZpravy>72237</korelaceZpravy>
  <idPozadavkuSestavy>X20090105000215</idPozadavkuSestavy>
  <dokument>
    <nazev>PrehledUhrad-xO34fjd039090D3mdkjcd.pdf</nazev>
    <mime>application/pdf</mime>
    <obsah>JVBERi0xLjQNJeLjz9MNCjEgMCBvYmoNPDwvQ3JlYXRpb25EYXRlIChEOjIwMDkwMzAzMDkzNjQ3
KS9Nb2REYXRlICgpL1Byb2R1Y2VyIChQREYgQ29tcGxldGUgdmVyc2lvbiAzLjUuMS4xKS9UaXRs
ZSAoTWljcm9zb2Z0IFdvcmQgLSBEb2t1bWVudDMpPj4NZW5kb2JqDTIgMCBvYmoNPDwvUGFnZXMg
MyAwIFIvVHlwZSAvQ2F0YWxvZy9WZXJzaW9uIC8xLjQ+Pg1lbmRvYmoNMyAwIG9iag08PC9Db3Vu
dCAxL0tpZHMgWzQgMCBSXS9UeXBlIC9QYWdlcz4+DWVuZG9iag00IDAgb2JqDTw8L0NvbnRlbnRz
IDkgMCBSL01lZGlhQm94IFswIDAgNTk1LjIgODQxLjkyXS9QYXJlbnQgMyAwIFIvUmVzb3VyY2Vz
…
PDF převedeno do BASE64
…
MDAwMCBuDQowMDAwMDAxNzk4IDAwMDAwIG4NCjAwMDAwMTQ5NDggMDAwMDAgbg0KMDAwMDAxNDk3
NyAwMDAwMCBuDQp0cmFpbGVyDTw8L0luZm8gMSAwIFIvUm9vdCAyIDAgUi9TaXplIDEwPj4Nc3Rh
cnR4cmVmDTE1MTM0DSUlRU9GCg==</obsah>
  </dokument>
</sestavaPrehledUhradZPB2BOdpoved>
------=_Part_27_18547941.1238675091376
Content-Type: application/pkcs7-signature; name=smime.p7s; smime-type=signed-data
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIAwggW6MIIE
oqADAgECAgoZIx+NAAEAAdM5MA0GCSqGSIb3DQEBBQUAMGkxGzAZBgkqhkiG9w0BCQEWDHN1YkNB

QHZ6cC5jejELMAkGA1UEBhMCQ1oxDDAKBgNVBAoTA1ZaUDEPMA0GA1UECxMGQ0EtVzNLMR4wHAYD
VQQDExVWWlAgQ1IgU3Vib3JkaW5hdGUgQ0EwHhcNMDkwMzMxMTEzMTE5WhcNMTEwMzMxMTEzMTE5
WjBnMQswCQYDVQQGEwJDWjEOMAwGA1UECBMFUHJhaGExDjAMBgNVBAcTBVByYWhhMQwwCgYDVQQK
…
IwYJKoZIhvcNAQkEMRYEFB2yMzi4Def0os2qZPWX6biLBLdbMDQGCSqGSIb3DQEJDzEnMCUwCgYI
KoZIhvcNAwcwDgYIKoZIhvcNAwICAgCAMAcGBSsOAwIHMA0GCSqGSIb3DQEBAQUABIGAXWqoB0pQ
Uw5SVhjR+iSB4bJqaTmDAXq3g9GIa3aW8kfisn27rcaSctH0Q+CwRX0BdgSgQYTcjg6nY7wSU1zh
oXWWslDcKuXaLrczD6zha7XC/qafgrRKEZ1gfRwJIC5q3TUtxmt5//pi/nHBgQOSSf+X2NRH9OYr
tcj118g5sFYAAAAAAAA=
------=_Part_27_18547941.1238675091376—
HTTP/1.1 200 OK
AS2-From: SIMPARTNER
Server: m-e-c as2
MIME-Version: 1.0
Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg=sha1; boundary="----=_Part_10_24749257.1238675088685"
Date: Thu, 02 Apr 2009 14:24:48 CEST
Subject: Message Delivery Notification
AS2-Version: 1.1
Content-Length: 4955
From: sender@as2server.com
Message-ID: <as2-1238675088685-1@SIMPARTNER_VZP>
AS2-To: VZP
Connection: close

------=_Part_10_24749257.1238675088685
Content-Type: multipart/report; report-type=disposition-notification;
.boundary="----=_Part_7_6254292.1238675088685"

------=_Part_7_6254292.1238675088685
Content-Type: text/plain
Content-Transfer-Encoding: 7bit

The AS2 message has been received. Thank you for exchanging AS2 messages.

------=_Part_7_6254292.1238675088685
Content-Type: message/disposition-notification
Content-Transfer-Encoding: 7bit

Reporting-UA: gem_test_AS2
Original-Recipient: rfc822; SIMPARTNER
Final-Recipient: rfc822; SIMPARTNER
Original-Message-ID: <GEM_AS2-1238675091343-17@VZP_SIMPARTNER>
Disposition: automatic-action/MDN-sent-automatically; processed
Received-Content-MIC: HbIzOLgN5/Sizapk9ZfpuIsEt1s=, sha1

------=_Part_7_6254292.1238675088685--

------=_Part_10_24749257.1238675088685
Content-Type: application/pkcs7-signature; name=smime.p7s; smime-type=signed-data
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

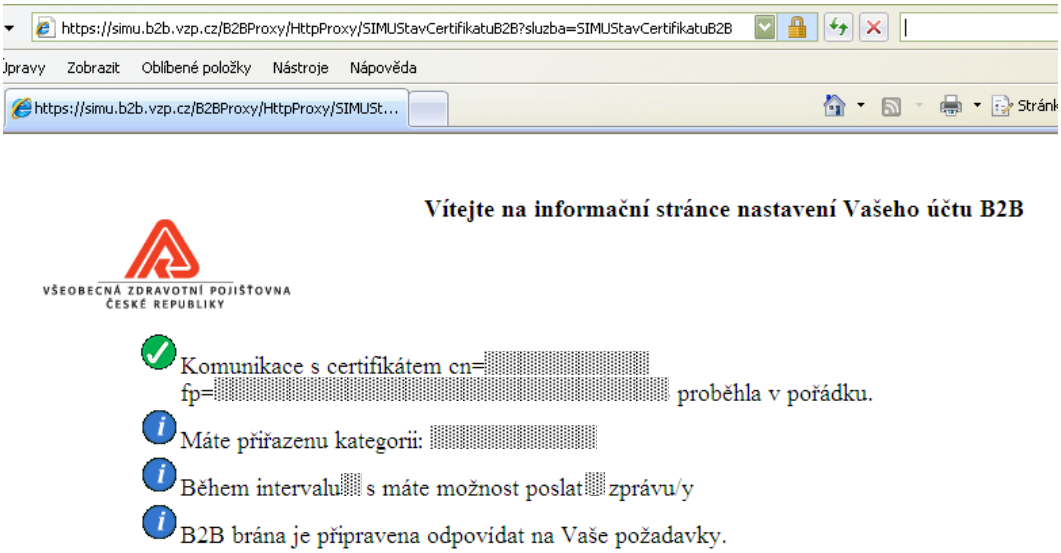
MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIAwggSbMIID
g6ADAgECAgQAnc0VMA0GCSqGSIb3DQEBBQUAMGgxCzAJBgNVBAYTAkNaMSowKAYDVQQDDCFJLkNB
IC0gUXVhbGlmaWVkIHJvb3QgY2VydGlmaWNhdGUxLTArBgNVBAoMJFBydm7DrSBjZXJ0aWZpa2HE
…
mOrxukvmjfknijk51Sx6wcD4Z7T5s3KqiXjokeophXjpEtTbWxfdSqONgqKmw6HO7wOlyPbrM4kl
MmeUo92/J0Iqknp1T0nXbwAAAAAAAA==
------=_Part_10_24749257.1238675088685—

4. Často kladené otázky

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

1. Nefunguje brána B2B určena k simulaci vyvinutého ASW

   Prověřte, jestli je přístupné rozhraní synchronní služby v prohlížeči (certifikáty se do prohlížeče musí naimportovat vč. certifikátů VZP [2] a [3]). Informace získáte i pomocí služby SIMUStavCertifikatuB2B, kterou ukazuje Obrázek 3.



Obrázek 3 Rozhraní žurnálu, služba StavCertifikatuB2B

Pokud se podobná stránka partnerovi nezobrazí:

nemá partner certifikáty VZP [2] a [3] ve svém systému zavedené jako důvěryhodné

Řešení: partner si zajistí, aby důvěřoval všem potřebným certifikátům [2].

nebo nemůže přistupovat na uvedený endpoint, protože nemá povolený firewall,

Řešení: partner si zajistí povolení komunikace na fw. pro port 443

nebo neproběhlo úspěšné párování certifikátu ve VZP

Řešení: partner dohodne s VZP prověření procesu párování certifikátu. Parametr CN uvnitř VZP se musí shodovat s parametrem certifikátu CN. Certifikáty musí být na obou stranách správné.

5. Seznam zkratek

Pojem	Význam pojmu
AS2	Application Statement 2 – protokol používaný v B2B řešeních
ASW	Aplikační software určený pro partnery, vyrobený dodavatelem software pro partnery VZP
B2B	Business to Business
DB	Databáze
EDI	Sada standardů pro elektronickou výměnu dat
HP	Hewlett-Packard s.r.o.
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.
HW	Hardware
IS VZP ČR	Informační systém VZP ČR
MDN	Message Delivery Notification – potvrzení o příjmu zprávy posílané AS2 protokolem
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“.
S/MIME	Rozšíření standardu MIME pro posílání elektronické pošty o kryptografické funkce
SSL	Secure Socket Layer. Jedná se o šifrovací vrstvu pracující na principu symetrické kryptografie (jeden symetrický klíč).
SW	Software
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
VZP nebo VZP ČR	Všeobecná zdravotní pojišťovna České republiky
XML	Značkovací jazyk používaný pro výměnu dat.
XMLDSig	Standard podepisování XML struktur, XML dat.

6. 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-kanal/podporovane-certifikaty
[4] Kvalifikovaný certifikát: http://www.ica.cz/Kvalifikovany-certifikat
[5] Komerční certifikát: http://www.ica.cz/Komercni-certifikat
[6] Veřejná část přístupového a podpisového certifikátu VZP:
https://www.vzp.cz/e-vzp/informace-pro-sw-firmy/b2b-komunikace/certifikaty-vzp
[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/xmldsig-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