

Dokumentace pro výrobce SW DIS13 - WS



Státní ústav pro kontrolu léčiv

Hlášení dodávek LP distributory

- Komunikace s úložištěm pomocí webových služeb

DIS13 v. 4.00

20101226

1.	Popis komunikačního rozhraní Hlášení dodávek LP	4
2.	Rozhraní pro zpracování hlášení dodávek LP DIS13	5
2.1.	Komunikační rozhraní	5
2.1.1.	Formát dat	5
2.1.2.	Přístupové body	5
2.2.	Verzování rozhraní	5
2.2.1.	Verze rozhraní	5
2.2.2.	Vystavené rozhraní a aplikační přístupové body pro WS přístup	6
2.2.3.	Verzování	6
2.3.	WS Přístupové body - testovací prostředí	6
2.3.1.	Přístup pomocí VPN	7
2.3.2.	Přístup pomocí SSL	7
2.4.	WS Přístupové body - produkční prostředí	7
2.4.1.	Přístup pomocí VPN	7
2.4.2.	SSL přístup	7
3.	Zabezpečení přístupu a přenosu dat	8
3.1.	Přístup prostřednictvím VPN tunelu	8
3.2.	Přístup prostřednictvím SSL protokolu	8
4.	Autentizace a autorizace	9
4.1.	Nastavené zabezpečení přístupu do úložiště	9
4.2.	Způsob autentizace a autorizace přístupu pro WS	9
4.2.1.	Autentizace pomocí HTTP protokolu	9
4.2.2.	Postup Autentizace pomocí Basic Authentication	9
4.2.3.	Postup Autorizace zaslané SOAP zprávy	9
4.3.	Rozhraní pro přístup k funkcím pro pracoviště distributora	10
4.4.	Konfigurace WS zprávy pro testovací prostředí	10
4.4.1.	Nastavení http hlavičky	10
5.	Funkce rozhraní dostupné pro distributora	12
5.1.	Funkce rozhraní pro Hlášení dodávek LP	12
5.2.	Pomocné funkce rozhraní pro Hlášení dodávek LP	12
5.3.	Základní struktura XML zprávy hlášení	12
5.3.1.	Element Doklad	12
5.3.2.	Element Zprava	12
5.4.	Dokumentace funkcí a zpráv	14

1. POPIS KOMUNIKAČNÍHO ROZHRAŇÍ HLÁŠENÍ DODÁVEK LP

Rozhraní pro předávání strukturovaných hlášení o dodávkách léčivých přípravků subjektům oprávněným k výdeji a distribuujícím subjektům.

Komunikační rozhraní slouží distributorům pro přístup k funkcím umožňujícím:

- **Založit hlášení dodávek**
- **Načíst uložené hlášení dodávek**
- **Změnit uložené hlášení dodávek**
- **Zrušit uložené hlášení dodávek**

Rozhraní je určeno pro pracoviště distributorů (distribuční sklady). Rozhraní využívá vybudované infrastruktury SÚKL a přístupových bodů včetně VPN přístupu pomocí HW routerů a SSL přístupu pomocí certifikátů vydaných SÚKL.

2. ROZHRANÍ PRO ZPRACOVÁNÍ HLÁŠENÍ DODÁVEK LP DIS13

2.1. Komunikační rozhraní

Rozhraní využívá vybudované infrastruktury SÚKL a přístupových bodů včetně VPN přístupu pomocí HW routerů a SSL přístupu pomocí certifikátů vydaných SÚKL.

2.1.1. Formát dat

Data jsou zasílána ve formátu XML na základě XSD a WSDL definice.

2.1.2. Přístupové body

Pro komunikaci jsou dostupné přístupové body pro SOAP.

- WS – webové služby pro zasílání hlášení dodávek

2.2. Verzování rozhraní

Popis řešení verzování komunikačního rozhraní.

2.2.1. Verze rozhraní

Verze rozhraní je definovaná jmenným prostorem v XSD definici a v XML zasílaných zprávách. Každá verze má svůj jednoznačný jmenný prostor.

Např.:

Verze 4.00.01 `xmlns:dis13=http://www.sukl.cz/dis13/v400r01`

Verze 4.00.02 `xmlns:dis13=http://www.sukl.cz/dis13/v400r02`

Zasílané požadavky na SÚKL jsou zpracovávány podle jmenného prostoru, který určuje přiřazení k verzi.

Např. tento dotaz patří do verze 4.00 revize 01:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<dis13:NacteniHlaseniDodavekDotaz
```

```
  xsi:schemaLocation=http://www.sukl.cz/dis13/v400r01 DIS13_4_00_01.xsd
```

```
  xmlns:dis13="http://www.sukl.cz/dis13/v400r01"
```

```
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
  <dis13:Doklad>
```

```
    <dis13:Distributor>
```

```
      <dis13:KodPracoviste>0000000000</dis13:KodPracoviste>
```

```
    </dis13:Distributor>
```

```
    <dis13:Identifikator>
```

```
      <dis13:ID_Podani>00000000-0000-0000-0000-000000000000</dis13:ID_Podani>
```

```
    </dis13:Identifikator>
```

```
  </dis13:Doklad>
```

```
  <dis13:Zprava>
```

```
    <dis13:ID_Zpravy>00000000-0000-0000-0000-000000000000</dis13:ID_Zpravy>
```

```
    <dis13:VerzeRozhrani>4.00</dis13:VerzeRozhrani>
```

```
    <dis13:DatumCasOdeslaniZpravy>2001-12-17T09:30:47Z</dis13:DatumCasOdeslaniZpravy>
```

```

        <dis13:SW_Klienta>
            <dis13:Vyrobcce>aaaaaa</dis13:Vyrobcce>
            <dis13:Nazev>aaaaaaa</dis13:Nazev>
            <dis13:Verze>aaaaaaa</dis13:Verze>
        </dis13:SW_Klienta>
    </dis13:Zprava>
</dis13:NacteniHlaseniDodavekDotaz>

```

Při vydání nové verze např. 4.00 rev. 02 bude XML vypadat následovně:

```

<?xml version="1.0" encoding="UTF-8"?>
<dis13:NacteniHlaseniDodavekDotaz
    xsi:schemaLocation=http://www.sukl.cz/dis13/v400r01\_DIS13\_4\_00\_02.xsd
    xmlns:dis13="http://www.sukl.cz/dis13/v400r02"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <dis13:Doklad>
        <dis13:Distributor>
            <dis13:KodPracoviste>0000000000</dis13:KodPracoviste>
        </dis13:Distributor>
        <dis13:Identifikator>
            <dis13:ID_Podani>00000000-0000-0000-0000-000000000000</dis13:ID_Podani>
        </dis13:Identifikator>
    </dis13:Doklad>
    <dis13:Zprava>
        <dis13:ID_Zpravy>00000000-0000-0000-0000-000000000000</dis13:ID_Zpravy>
        <dis13:VerzeRozhrani>4.00</dis13:VerzeRozhrani>
        <dis13:DatumCasOdeslaniZpravy>2001-12-17T09:30:47Z</dis13:DatumCasOdeslaniZpravy>
        <dis13:SW_Klienta>
            <dis13:Vyrobcce>aaaaaa</dis13:Vyrobcce>
            <dis13:Nazev>aaaaaaa</dis13:Nazev>
            <dis13:Verze>aaaaaaa</dis13:Verze>
        </dis13:SW_Klienta>
    </dis13:Zprava>
</dis13:NacteniHlaseniDodavekDotaz>

```

2.2.2. Vystavené rozhraní a aplikační přístupové body pro WS přístup

Vystavené aplikační přístupové body WS mají definované URL, které zároveň jednoznačně definuje i verzi rozhraní.

Např.:

Verze 4.00.01: http://test-gtw-ws01.sukl.cz:4560/sst/DIS13_4_00_01?WSDL
 Budoucí verze např. 4.00.02: http://test-gtw-ws01.sukl.cz:4560/sst/DIS13_4_00_02?WSDL atd.

2.2.3. Verzování

Rozhraní je připraveno na vydávání nových verzí s možným přechodným obdobím mezi jednotlivými verzemi. Umožní souběh dvou verzí po definovanou dobu, která bude dle potřeby přibližně v řádech měsíců. Přechod na novou verzi by měl být pro distributory bez větších problémů s nasazováním nových verzí.

2.3. WS Přístupové body - testovací prostředí

Pro vývoj a testování rozhraní pro hlášení dodávek je připraveno testovací prostředí.

Webová služba pro přístup jednoznačně identifikovaného pracoviště distributora k funkcím úložiště pro práci s hlášením dodávek LP.

Služba je dostupná na těchto přístupových bodech:

2.3.1. Přístup pomocí VPN

Testovací prostředí pro přístup přes SOAP a webové služby je nakonfigurováno na:

serveru: test-gtw-ws01.sukl.cz – 195.113.95.103
portu: 4560
URL: http://test-gtw-ws01.sukl.cz:4560/sst/DIS13_4_00_01?WSDL

2.3.2. Přístup pomocí SSL

Testovací prostředí pro přístup přes SOAP a webové služby je nakonfigurováno na:

serveru: test-gtw-ssl-ws01.sukl.cz – 195.113.95.45
portu: 4660
URL: https://test-gtw-ssl-ws01.sukl.cz:4660/sst/DIS13_4_00_01_SSL?WSDL

2.4. WS Přístupové body - produkční prostředí

Provozní prostředí.

Webová služba pro přístup jednoznačně identifikovaného pracoviště distributora k funkcím úložiště pro práci s hlášením dodávek LP.

Služba je dostupná na těchto přístupových bodech:

2.4.1. Přístup pomocí VPN

Produkční prostředí pro přístup přes SOAP a webové služby je nakonfigurováno na:

serveru: s-gtw-ws01.sukl.cz – 195.113.95.83
portu: 4560
URL: http://s-gtw-ws01.sukl.cz:4560/sst/DIS13_4_00_01?WSDL

2.4.2. SSL přístup

Produkční prostředí pro přístup přes SOAP a webové služby je nakonfigurováno na:

serveru: s-gtw-ssl-ws01.sukl.cz – 195.113.95.46
portu: 4660
URL: http://s-gtw-ssl-ws01.sukl.cz:4660/sst/DIS13_4_00_01_SSL?WSDL

3. ZABEZPEČENÍ PŘÍSTUPU A PŘENOSU DAT

Zasílání hlášení dodávek léčivých přípravků je prováděno prostřednictvím zabezpečeného spojení vytvořeného nad veřejnou datovou sítí (Internet). Zasílání je možné uskutečnit prostřednictvím jedné z následujících metod zabezpečeného přístupu.

3.1. Přístup prostřednictvím VPN tunelu

K zabezpečení poskytovaných údajů během přenosu je mezi přístupovým bodem (distributorem) a SÚKL vytvořen VPN tunel pro zajištění šifrovaného přenosu dat. VPN tunel mezi přístupovým bodem (distributorem) a SÚKL bude zabezpečen pomocí protokolu IPsec (IP security, specifikovaný v RFC 4308) v tunel módu s podporou IKEv2 (Internet Key Exchange specifikovaný v RFC 4306).

Pro komunikaci s VPN serverem (úložištěm) jsou podporovány následující vlastnosti IPsec tunelu:

- Podpora kryptovacích mechanismů dle RFC 4305
- Podpora PKI (Public Key Infrastructure) ověřování pomocí certifikátů X.509 v3
- VPN klient musí podporovat komunikaci na VPN server (úložiště) prostřednictvím UDP protokolu dle RFC 3948 „UDP Encapsulation of IPsec ESP Packets“
- Podpora navázat tunel přes NAT/PAT (Network Address Translation/Port Network Address Translation), kde je požadována podpora RFC 3715 „IPsec-Network Address Translation (NAT) Compatibility Requirements“ a RFC 3947 „Negotiation of NAT-Traversal in the IKE“

Distributorům bude pro tento účel doporučeno vybavení zabezpečovací technologie ze strany SÚKL, na vytvoření VPN spojení. VPN tunel neslouží k zajištění připojení distributora do Internetu.

3.2. Přístup prostřednictvím SSL protokolu

K zabezpečení poskytovaných údajů během přenosu je mezi přístupovým bodem (distributorem) a SÚKL vytvořeno zabezpečené spojení prostřednictvím SSL protokolu.

Pro komunikaci s SSL serverem (úložištěm) jsou podporovány následující vlastnosti SSL protokolu

- Podpora SSL Version 3.0, Transport Layer Security (TLS) Version 1.0. RFC 2246
- Podpora PKI (Public Key Infrastructure) ověřování pomocí certifikátů X.509 v3

Podpora kryptovacích mechanismů dle RFC 3268

4. AUTENTIZACE A AUTORIZACE

4.1. Nastavené zabezpečení přístupu do úložiště

Přístup do úložiště SÚKL je kromě VPN nebo SSL přístupu dále zabezpečen na úrovni volání jednotlivých funkcí úložiště pro hlášení dodávek LP.

Při každém volání funkce je prováděna

- **autentizace přistupujícího** - ověření, že ten kdo zasílá požadavek je opravdu ten, za koho se vydává (pracoviště distributora) - jméno/heslo
 - o vyhledání identity v systému pro správu identit v příslušné skupině
 - o ověření znalosti hesla
- **autorizace přistupujícího** – kontrola oprávnění přístupu - ověření, že autentizovaný odesílatel má právo volat příslušnou funkci a zároveň zasílá data za konkrétní pracoviště, za které je může zasílat
 - o ověření práva přístupu autentizovaného uživatele k volané funkci
 - o ověření, že autentizovaný uživatel zasílá data za své pracoviště

V případě, že zasláný požadavek nebude autentizován nebo autorizován, bude vrácena FAULT odpověď s kódem chyby. Nebude možné dále pokračovat ve zpracování dat požadavku. Požadavek bude po zažurnálování odmítnut.

4.2. Způsob autentizace a autorizace přístupu pro WS

4.2.1. Autentizace pomocí HTTP protokolu

- **HTTP Basic access authentication**
 - o *Basic Authentication* je založena na tom, že uživatel zašle svůj login a heslo, jež jsou zakódovány ve formě base64 a vloženy do hlavičky http protokolu.
 - o Neposkytuje žádné zabezpečení proti odposlechu hesla po cestě. Nezbytným předpokladem použití tohoto způsobu je zabezpečené spojení mezi klientem a serverem např. pomocí VPN tunelu nebo SSL spojení. Tento předpoklad je splněn. Není možné přistupovat nezabezpečeným kanálem, pouze VPN tunelem nebo SSL spojením.
 - o Tento mechanismus autentizace je nejsnáze implementovatelný.

4.2.2. Postup Autentizace pomocí Basic Authentication

- SW vytvoří SOAP zprávu a do hlavičky HTTP vloží atribut **Authorization** a hodnotu „**BASIC řetězec Basic64(jméno:heslo)**”
- SW odešle zprávu na příslušné URL
- Úložiště SÚKL provede autentizaci. V případě že jméno/heslo nesouhlasí, je vrácen FAULT. V případě, že autentizace proběhla, je požadavek předán k dalšímu zpracování a následné autorizaci

4.2.3. Postup Autorizace zasláné SOAP zprávy

- po úspěšné autentizaci provede server
 - o ověření práva přístupu autentizovaného uživatele k volané funkci
 - o porovnání autentizovaného uživatele s údaji v zasláné datové zprávě

- pokud uživatel nemá právo funkci volat, nebo nesouhlasí autentizační údaje s údaji v datové zprávě, je vrácena zpráva s FAULT odpovědí. V případě že autorizace proběhla, je požadavek předán k dalšímu zpracování.

4.3. Rozhraní pro přístup k funkcím pro pracoviště distributora

Autentizace a autorizace:

V komunikačním rozhraní pro přístup pracoviště distributora pro práci s funkcemi je jako identifikátor pracoviště použit kód pracoviště přidělený SÚKL. Tento identifikátor je použitý pro ověření identity pracoviště a ověření, že uživatel zasílá data za pracoviště, za které má právo data zasílat. Kód pracoviště použitý pro autentizaci se musí rovnat kódu pracoviště v XML datové zprávě.

Autentizace přistupujícího pracoviště je prováděna při každém volání funkce pro pracoviště. Autentizace je prováděna ověřením předaného jména pracoviště a hesla v systému pro správu identit SÚKL.

Pro funkce hlášení dodávek LP je **autentizační řetězec pro pracoviště distributora**:

Kód pracoviště: XXXXXXXXXX
Heslo: XXXXXXXXXX

Kód pracoviště je přidělený SÚKL

HTTP dotaz musí mít nastavený atribut Authorization pro BASIC autentizaci:

NAME	VALUE	TYPE
Authorization	BASIC base64(účet uživatele:heslo)	String

Kde base64(účet uživatele: heslo)

je : base64(XXXXXXXXXX:XXXXXXXXXX) = eHh4eHh4eHh4eHg6eHh4eHh4eHh4eA==

potom je atribut Authorization = „BASIC eHh4eHh4eHh4eHg6eHh4eHh4eHh4eA==“

Autorizace je prováděna při každém volání funkcí pro přístup pracoviště distributora pro práci s funkcemi. Autorizace ověřuje, že zasílající pracoviště volá funkce pod svým kódem pracoviště. Porovnává se autentizační kód pracoviště z http hlavičky a kód pracoviště v těle zprávy.

4.4. Konfigurace WS zprávy pro testovací prostředí

Příklad konfigurace volání WS funkcí pro pracoviště s kódem 00000029001

4.4.1. Nastavení http hlavičky

HTTP dotaz musí mít nastavený atributu Authorization pro BASIC autentizaci:

NAME	VALUE	TYPE
Authorization	BASIC base64(účet pracoviště: heslo)	String

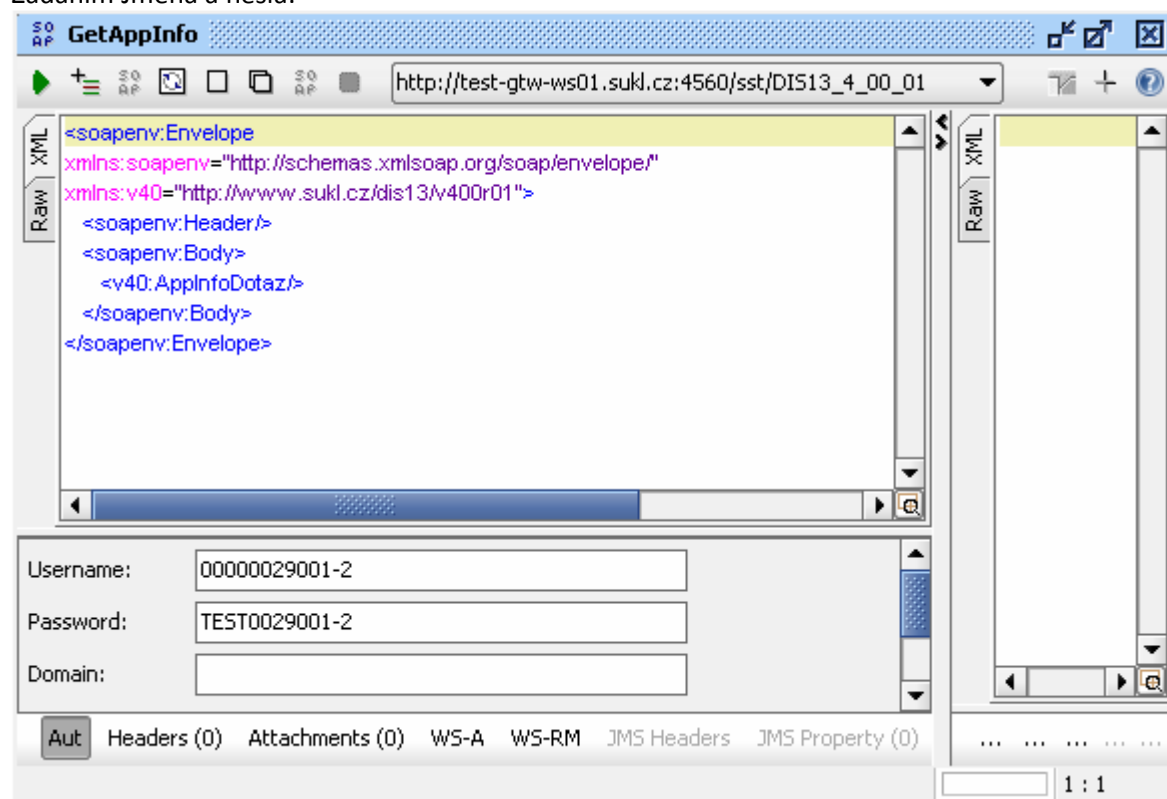
Kde base64(účet pracoviště: heslo)

je např.: base64(00000029001-2:TEST0029001-2) = MDAwMDAwMjkwMDEtMjpURVNUMDAyOTAwMS0y

potom je atribut **Authorization = BASIC MDAwMDAwMjkwMDEtMjpURVNUMDAyOTAwMS0y**

Pro testování funkcí je možné použít volně dostupnou aplikaci soapUI. V soapUI projektu je možné zadat jméno a heslo následovně:

Zadáním Jména a hesla:



5. FUNKCE ROZHRAŇÍ DOSTUPNÉ PRO DISTRIBUTORA

5.1. Funkce rozhraní pro Hlášení dodávek LP

Dostupné funkce pro zasílání Hlášení dodávek LP. Slouží pro komunikaci SW distributora úložištěm SÚKL.

- **ZalozitHlaseniDodavek** - Funkce pro založení hlášení dodávek LP
- **ZmenitHlaseniDodavek** – Funkce pro změnu uloženého hlášení dodávek LP
- **ZrusitHlaseniDodavek** - Funkce pro označení uloženého hlášení dodávek za zrušené
- **NacistHlaseniDodavek_4_00** - Funkce pro načtení uloženého hlášení dodávek uloženého ve verzi 4.00
- **NacistSeznamHlaseniDodavek_4_00** - Funkce pro načtení seznamu uložených hlášení dodávek uložených ve verzi 4.00

5.2. Pomocné funkce rozhraní pro Hlášení dodávek LP

Pro práci s funkcemi Hlášení dodávek LP jsou dostupné další pomocné funkce.

- **GetAppInfo** – Funkce pro ověření funkčnosti rozhraní, která zároveň umožní načtení čísla aktuální verze rozhraní a vrátí aktuální datum a čas na serveru SÚKL
- **NacistVerzeDIS13** – Funkce pro načtení seznamu dostupných verzí rozhraní Hlášení dodávek LP
- **NacistCiselnikChyb** – Funkce pro načtení aktuálního číselníku chyb pro práci s rozhraním Hlášení dodávek LP
- **AppPing** – Funkce aplikační Ping pro ověření zasílání správného data, času a verze rozhraní
- **NacistVerziDokladu** – Funkce pro načtení verze uloženého Hlášení dodávek LP

5.3. Základní struktura XML zprávy hlášení

Každá zpráva se skládá ze dvou základních elementů Doklad a Zpráva.

5.3.1. Element Doklad

Pod elementem Doklad jsou přenášena samotná data Hlášení včetně identifikace distributora.

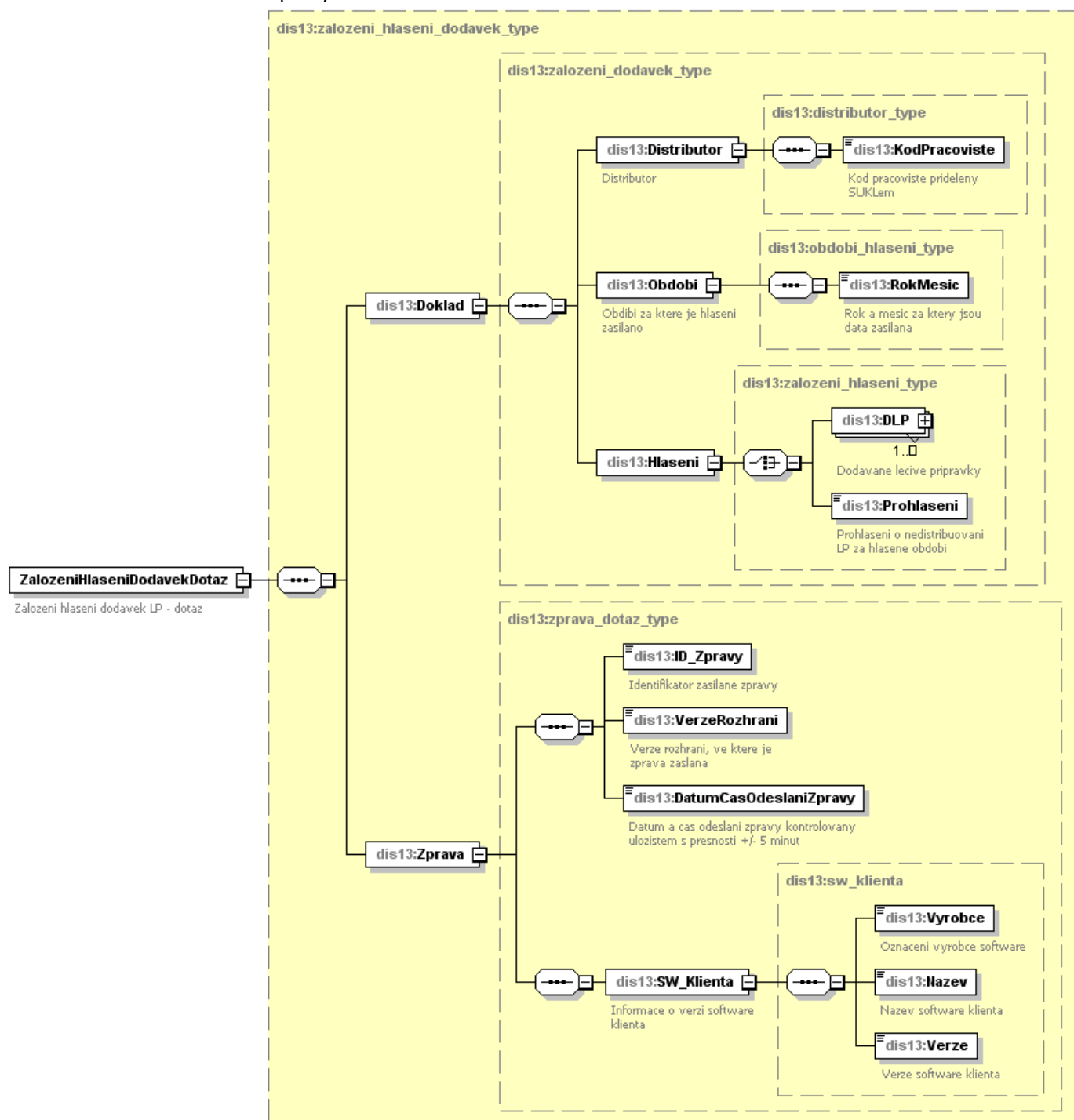
Jednoznačný identifikátor dokladu „ID_Dokladu“ generuje a vrací úložiště na základě zaslaného nového hlášení. Jako hodnota je použit vygenerovaný GUID/UUID podle závazných pravidel publikovaných v RFC 4122 (viz <http://www.ietf.org/>).

5.3.2. Element Zprava

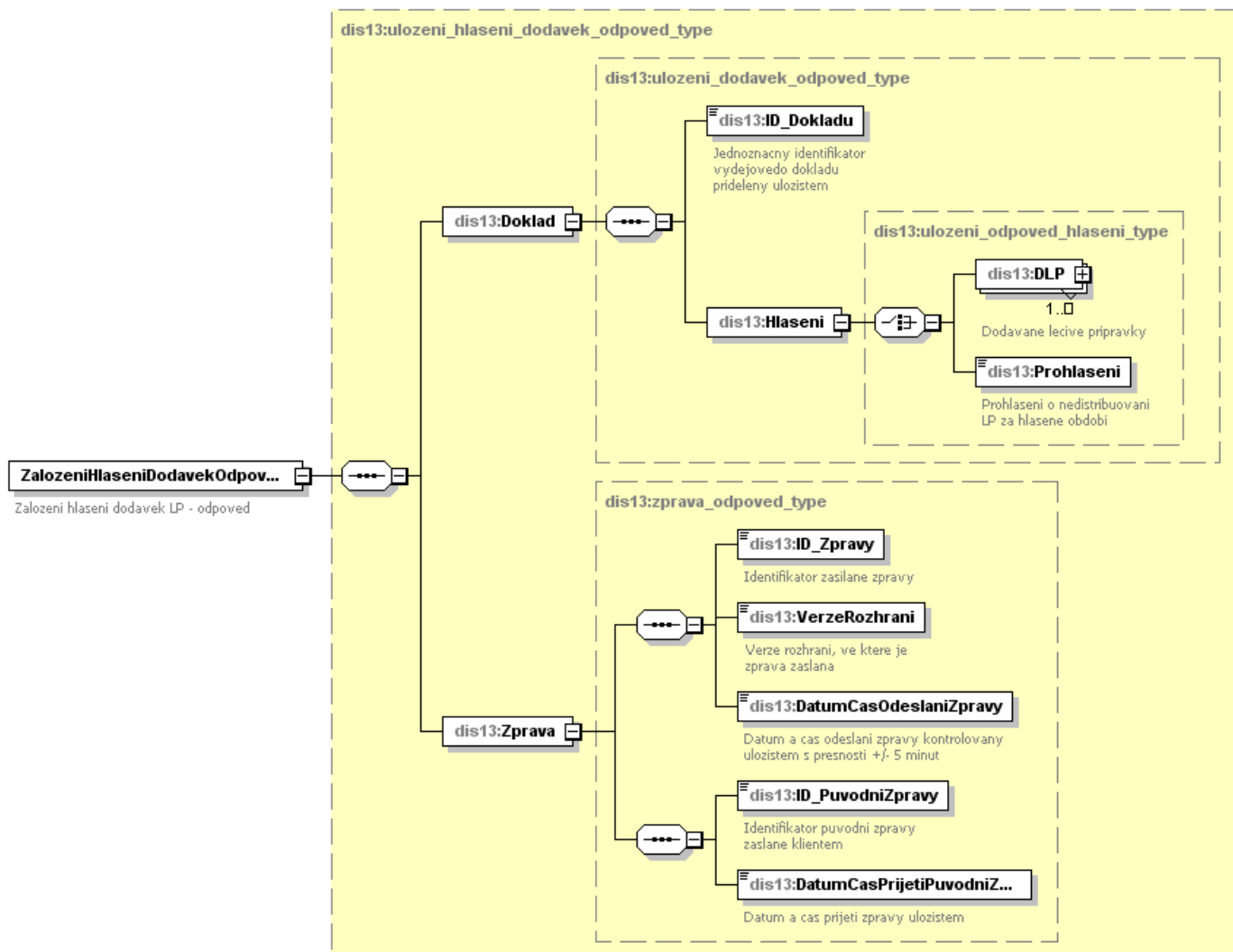
Pod elementem Zprava jsou přenášena pomocná data zprávy včetně její jednoznačné identifikace.

Jednoznačný identifikátor zprávy „ID_Zpravy“ generuje odesílatel (SW klient) při každém volání funkce. Jako hodnota je použit vygenerovaný GUID/UUID podle závazných pravidel publikovaných v RFC 4122 (viz <http://www.ietf.org/>).

Obr.: Základní struktura XML zprávy dotazu



Obr.: Základní struktura XML zprávy odpovědi



5.4. Dokumentace funkcí a zpráv

Dokumentace funkcí rozhraní a jednotlivých zpráv je dostupná v dokumentaci ve složce „Definice položek - hlášení dodávek léčivých přípravků HTML“

Složka „DOC-WSDL-DIS13_4_00“

– dokumentace WSDL rozhraní

Složka „DOC-XSD-DIS13_4_00“

- dokumentace XSD definice zpráv

Složka „DOC-XSD-FAULTDETAIL“

- dokumentace FAULT odpovědi