

SDAT - sběr dat



Říjen 2014

**© ZHOTOVITEL Czech s.r.o.**, Všechna práva vyhrazena

Říjen 2014

**© ZHOTOVITEL Czech s.r.o.**, Všechna práva vyhrazena

Říjen 2014

**© ZHOTOVITEL Czech s.r.o.**, Všechna práva vyhrazena

**Technická specifikace SDAT**

**TS-5 Technické informace**

**Technické informace a systémové požadavky**

***Verze: 1.1***

**Identifikace dokumentu**

|  |  |
| --- | --- |
|  |  |
| Název dokumentu: | **Technická specifikace SDAT, TS-5 Technické informace** |
| Verze dokumentu: | **1.1** |
| Projekt:  | **SDAT - sběr dat** |
| Autor: | **NESS Czech s.r.o.**, ČNB |

**Historie dokumentu**

|  |  |  |
| --- | --- | --- |
| **Datum** | **Verze** | **Popis verze a změn oproti verzi předchozí** |
| 2018-05-29 | 0.1 | Úvodní verze dokumentu |
| 2018-10-31 | 0.2 | Drobné úpravy textu podle aktuálního stavu |
| 2019-01-31 | 0.3 | Doplnění informací o testovacím prostředí SDAT |
| 2019-08-27 | 0.4 | Doplnění informací k podepisování (kapitola 3.2.5) |
| 2019-10-16 | 0.5 | Aktualizace kapitoly 5.1 |
| 2020-11-20 | 0.6 | Zrušení SFTP kanálu, odstranění informací o šifrování (nešifruje se) |
| 2021-11-29 | 1.0 | Aktualizace – upraven seznam podporovaných webových prohlížečů |
| 2021-12-14 | 1.1 | Doplnění příkladu volání verze WS (kap. 3.4.2) |

**Obsah**

[1. Přílohy a odkazy na jiné dokumenty 4](#_Toc90367609)

[2. Úvod 5](#_Toc90367610)

[2.1. Účel dokumentu 5](#_Toc90367611)

[3. Základní pravidla komunikace s ČNB 6](#_Toc90367612)

[3.1. Používané standardy 6](#_Toc90367613)

[3.1.1. Znakové sady 6](#_Toc90367614)

[3.1.2. Používání SSL 6](#_Toc90367615)

[3.1.3. Používání komprese 6](#_Toc90367616)

[3.1.4. Podepisování 6](#_Toc90367617)

[3.1.5. Používání otisků souborů 7](#_Toc90367618)

[3.1.6. Standardy webových služeb 7](#_Toc90367619)

[3.2. Požadavky na vyplnění komunikační hlavičky 7](#_Toc90367620)

[3.3. Autentizace 7](#_Toc90367621)

[3.3.1. Autentizace webových služeb 7](#_Toc90367622)

[3.3.2. Autentifikace v aplikaci 7](#_Toc90367623)

[3.4. Změny v rozhraní 7](#_Toc90367624)

[3.4.1. Změny aplikace 7](#_Toc90367625)

[3.4.2. Změny webových služeb 8](#_Toc90367626)

[3.5. Záložní řešení v případě výpadku 9](#_Toc90367627)

[4. Technický popis jednotlivých kanálů 10](#_Toc90367628)

[4.1. Webové služby 10](#_Toc90367629)

[4.2. Webová aplikace 10](#_Toc90367630)

[4.3. Mailová komunikace 10](#_Toc90367631)

[5. Jednotlivá prostředí ČNB 11](#_Toc90367632)

[5.1. Produkční prostředí 11](#_Toc90367633)

[5.1.1. Adresa produkčního prostředí 11](#_Toc90367634)

[5.1.2. Servisní odstávky 11](#_Toc90367635)

[5.1.3. Obsah produkčního prostředí 11](#_Toc90367636)

[5.2. Testovací prostředí 11](#_Toc90367637)

[5.2.1. Adresa testovacího prostředí 11](#_Toc90367638)

[5.2.2. Servisní odstávky 11](#_Toc90367639)

[5.2.3. Obsah testovacího prostředí 11](#_Toc90367640)

#

# Přílohy a odkazy na jiné dokumenty

|  |  |  |
| --- | --- | --- |
|  | **Název** | **Popis**  |
| 0 | Základní dokument | Popisuje strukturu dokumentace SDAT (tento dokument). |
| 1 | Popis systému | Popisuje základní vlastnosti a architekturu se zaměřením na funkce určené pro externí uživatele. |
| 2 | Metapopis vykazovací povinnosti | Popisuje způsoby, kterými lze získat informace o metodikách vykazování a o vykazovací povinnosti – jak webovými službami, tak přes uživatelské rozhraní webové aplikace. |
| 3 | Vykazování | Popisuje způsoby, kterými lze zaslat Vydání výskytů výkazů podle předepsané vykazovací povinnosti a následně získat informace o stavu jejich zpracování. |
| 4 | Vykazování – specifické případy | Rozcestník na samostatné dokumenty popisující specifické případy či způsoby vykazování. |
| **5** | **Technické informace** | **Popisuje technické náležitosti jednotlivých komunikačních rozhraní (tento dokument).** |
| 6 | Katalog webových služeb | Popisuje webové služby – primární rozhraní pro automatizované vykazování. |
| 7 | Modely metapopisu | Popisuje architekturu systému na úrovni vybraných entitních modelů. |
| 8 | Popis jazyka kontrol | Popisuje jazyk kontrol systému SDAT. |

# Úvod

Tento dokument – Popis systému SDAT, je jedním ze sady dokumentů, které dohromady tvoří Technickou specifikace – kompletní popis systému pro sběr dat pro potřeby externích užiavtelů.

## Účel dokumentu

Účelem tohoto dokumentu je popsat technické informace podstatné pro externí uživatele komunikující se systémem SDAT.

# Základní pravidla komunikace s ČNB

## Používané standardy

### Znakové sady

Pro komunikaci přes webové služby a v zasílaných souborech se používá znaková sada UTF-8.

### Používání SSL

Pro komunikaci je povoleno používat aktuálně pouze TLS1.2 a následující cipher suite﻿:

| **CIPHER SUITE** | **ID** |
| --- | --- |
| TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x00002F |
| TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x000035 |
| TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0x00003C |
| TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 | 0x00003D |

Tyto parametry mohou být v budoucnosti upraveny (ve verzích směrem výše) v reakci na případně odhalené zranitelnosti těchto protokolů.

### Používání komprese

Při použití komprese na binární data zasílaná uvnitř XML bude používán výhradně formát GZIP. Na zasílané soubory je nutné použít formát ZIP nebo GZIP.

### Podepisování

Při zasílání Vstupních zpráv přes webovou aplikaci SDAT bude možné použít komponentu aplikace, která zajistí funkcionalitu pro podpis Vstupní zprávy.

Při podepisování Vstupních zpráv zasíláných přes WS je nutné postupovat podle standardu XAdES, No Container, Detached, BASELINE-B; ve všech případech je podpis aplikován na komprimovaná data vstupní zprávy metodou GZIP Název podepsaného souboru se musí shodovat s obsahem <ReferencniId> Vstupní zprávy dle konvence SDAT\_VYD\_*<ReferencniId>*.gzip (např. SDAT\_VYD\_9898920190827140948547.gzip).

Pro podepsání lze použít jednu z těchto možností

Elektronické podpisy:

1. zaručený elektronický podpis založený na kvalifikovaném certifikátu,
2. kvalifikovaný elektronický podpis.

Elektronické pečeti:

1. zaručená elektronická pečeť založená na kvalifikovaném certifikátu,
2. kvalifikovaná elektronická pečeť.

Pro podepisování protokolů na straně ČNB bude použita zaručená elektronická pečeť; podpis je aplikován způsobem ENVELOPED přímo na XML soubor s protokolem.

### Používání otisků souborů

Pro vytváření otisků souborů je nutné použít algoritmus SHA-256

Otisk se vytváří ze souboru až po jeho komprimaci (pokud je použita).

### Standardy webových služeb

Webové služby jsou založeny na následujících standardech

- použití WSDL 1.1,

- použití SOAP 1.1,

- použití SOAP/HTTP binding (komunikační protokol mezi systémy je HTTP),

- použití soapAction pro všechny operace (nad požadavek WS-I Basic Profile 1.1),

- pro přenos binárních dat použití MTOM/XOP (nad požadavek WS-I Basic Profile 1.1),

- XSD schéma pro popis katalogů, jednotný katalog pro společné struktury,

- zabezpečení webových služeb pomocí komunikační vrstvy (nepoužívá se WS-Security, XML-Signature a XML-Encryption, atd.),

- formátování Document / Literal Wrapped.

## Požadavky na vyplnění komunikační hlavičky

V hlavičce každého volání WS musí být povinně vyplněny následující údaje:

ID žádosti (uuid)

OsobaKod

CasZadosti

## Autentizace

### Autentizace webových služeb

* Pro autentizaci u všech webových služeb (zasílání dat, informace o zpracování i metodické informace) bude používán komerční serverový certifikát.
* Tyto certifikáty musí být registrovány v SDAT.
* ČNB akceptuje certifikáty vydané kvalifikovaným poskytovatelem služeb vytvářejících důvěru ve smyslu článku 3 bodu 20 Nařízení eIDAS, který je uveden na důvěryhodném seznamu Ministerstva vnitra dle § 13 odst. 3 Zákona o službách vytvářejících důvěru pro elektronické transakce.
* Pokud bude autentizace neúspěšná, bude navázání spojení odmítnuto.

### Autentifikace v aplikaci

* Pro autentifikaci v aplikaci bude využito přihlášení pomocí uživatelského jména + hesla

## Změny v rozhraní

### Změny aplikace

Aplikace je verzována  a informace o verzi a datu nasazení je v aplikaci dostupná po najetí kurzorem na logo systému.



### Změny webových služeb

Změny v rozhraní budou v maximální možné míře realizovány jako zpětně kompatibilní, tj. nebudou vynucovat změny na straně Osob.

Pokud to bude nezbytné může Česká národní banka provést i **zpětně nekompatibilní změny** v definovaných datových, komunikačních a bezpečnostních rozhraních, které však budou vyhlášeny v případě změn:

* **datového rozhraní** nejméně **devět měsíců** před začátkem jejich využívání,
* **komunikačního či bezpečnostního rozhraní** v předstihu nejméně **dvanácti měsíců**.

Jedná se o změny vyvolané potřebou zvýšení využitelnosti systému, zvýšení jeho kvality, sjednocení s dalšími řešeními ve finančním sektoru, státní správě či EU a v souladu s rozvojem informačních technologií nebo vývojem standardů

Pro jednotlivé typy změn bude verzováno webových služeb realizováno takto:

1. **Minoritní změny**, které nemění definici rozhraní, jenom logiku zpracování (např. opravu chyby). Pro tyto účely slouží atribut <VerzeSluzby> ve všech schématech (dokumentech XSD). Úvodní hodnota tohoto atributu je „1.0.0“. Při minoritních změnách se mění hodnota atributu na poslední pozici (tedy další verze je „1.0.1“). Služby jsou nadále vystaveny na stejném rozhraní (URL adresa). Starší SOAP dokumenty jsou nadále validní.
2. **Kompatibilní změny**, které mění jak definici rozhraní, tak logiku zpracování. Tyto změny jsou zpětně kompatibilní (např. přidání nepovinného atributu nebo elementu s minOccurs=“0“). Pro tyto účely slouží atribut <VerzeSluzby> ve všech schématech (dokumentech XSD). Úvodní hodnota tohoto atributu je „1.0.0“. Při kompatibilních změnách se mění hodnota atributu na předposlední pozici (tedy další verze je „1.1.0“). Služby jsou nadále vystaveny na stejném rozhraní (URL adresa). Starší SOAP dokumenty jsou nadále validní.
3. **Nekompatibilní (majoritní změny)**. Tato situace vede ke změně webové služby, resp. k vytvoření nové služby. Pro tyto účely slouží formát jmenného prostoru ve všech schématech (dokumentech XSD). Příkladem je schéma společných typů, jež je „urn:cz:cnb:sdat:schemas:ObjektyTypy:v1“. Při těchto změnách se mění jmený prostor, číslo na konci URN (tedy další verze této služby bude mít jmenný prostor „urn:cz:cnb:sdat:schemas:ObjektyTypy:v2“). Současně se mění výše uvedený atribut version na první pozici (tedy další verze je „2.0.0“). Služby jsou vystaveny na jiném rozhraní (URL adresa) a předpokládá se po omezenou dobu souběh provozu obou verzí webových služeb.

Obdobně se tato pravidla aplikují na verzování XSD, které nepopisují přímo obsah webových služeb, ale strukturu dokumentů obsažených ve webových službách v binární komprimované podobě.

Na úrovni SOAP dokumentů (vyměňovaných dat webových služeb) je rovněž element version, který je možno kontrolovat vůči podporovaným verzím ze strany aplikační logiky webových služeb. Osoby při vyvolání služby plní tento atribut poslední jimi používanou hodnotou verze XSD dokumentu. Systém SDAT kontroluje tuto verzi a v případě, že detekuje nekompatibilní hodnotu (např. sám podporuje verze XSD 1.1.0 a výš, ale v dokumentu je verze 1.0.1), může odmítnout zpracování dotazu/žádosti se statusem „NEPLATNÁ VERZE“. Pokud detekuje různou ale kompatibilní hodnotu, zpracování provede a posílá zpátky status „STARŠÍ VERZE“.

Příklad pro CtiUdajeOsoby

Od verze 1.87.5 jsou pro určité informační služby podporovány verze:

* 1.0.0 – původní výstup služeb
* 1.1.0 – rozšířený výstupu služeb o nové elementy

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:urn="urn:cz:cnb:sdat:schemas:CtiUdajeOsoby:v1">

 <soapenv:Header/>

 <soapenv:Body>

 <urn:CtiUdajeOsobyRequest>

 <ZadostInfo>

 <CasZadosti>${=new Date().format("yyyy-MM-dd'T'HH:mm:ss.SSS")}</CasZadosti>

 <ZadostId>${=UUID.randomUUID()}</ZadostId>

 **<VerzeZadosti>1.0.0</VerzeZadosti>**

 <OsobaKod>9999</OsobaKod>

 </ZadostInfo>

 <Dotaz>

 <!--Optional:-->

 <OsobaKod>9999</OsobaKod>

 </Dotaz>

 </urn:CtiUdajeOsobyRequest>

 </soapenv:Body>

</soapenv:Envelope>

Výstup neobsahuje elementy <XbrlId>, <Iso20022Id>. Pro uvedené elementy je nutné volání s verzí

<VerzeZadosti>**1.1.0**</VerzeZadosti>

## Záložní řešení v případě výpadku

1. Náhradním způsobem pro předání Vstupní zprávy s Vydání výskytu výkazu je fyzický nosič dat nebo zabezpečená elektronická pošta. Náhradní způsob je možno použít po dohodě s Českou národní bankou, a to výhradně po nezbytně dlouhou dobu v případě výpadku technických komunikačních prostředků.
2. Náhradním způsobem pro předávání metodických informací (metapopisu) je předání souborů na fyzickém nosiči dat nebo prostřednictvím elektronické pošty, a to výhradně v případě, že hrozí nebezpečí prodlení.
3. Náhradním způsobem předávání protokolu o zpracování Vstupní zprávy a protokolu o zpracování Vydání výskytu výkazu je neformalizované oznámení výsledku zpracování pracovníkem České národní banky a to telefonem nebo prostřednictvím elektronické pošty.
4. Náhradním způsobem pro předávání Upomínky 1. a 2. stupně je v případě potřeby neformalizované upomenutí pracovníkem České národní banky prostřednictvím telefonu nebo e-mailovou zprávou. V případě Upomínky 3. Stupně je to datová schránka.

# Technický popis jednotlivých kanálů

Pro komunikaci Osob s ČNB je možná využít následující komunikační kanály

## Webové služby

Webové služby jsou základním způsobem komunikace, jak pro předkládání výkazů, tak pro získávání informací. Jsou dostupné pouze pro registrované osoby. Webové služby využívají protokol SOAP s využitím HTTPS jako transportního protokolu. Služby jsou synchronní. Detailní popis jednotlivých služeb je uveden v dokumentu TS\_6\_KatalogWebovychSluzeb.

Veškerá komunikace se systémem SDAT je možná pouze s využitím SSL s využitím podporovaných standardů. Pro navázání spojení při volání webových služeb je nutné použít registrovaný certifikát.

## Webová aplikace

Webová aplikace je alternativním komunikačním kanálem, který nabízí funkčnost v obdobném rozsahujako kanál webových služeb. Je dostupná pro registrované i neregistrované (jen část funkčnosti) Osoby, část informací týkající se prezentace metodických informací je dostupná veřejně.

Oproti webovým službám umožňuje navíc i správu údajů o Osobách, uživatelích a jejich oprávnění.

Je dostupná přes standardní protokol https s využitím SSL/TLS certifikátu na straně ČNB.

Aplikace je optimalizována pro prohlížeče::

Microsoft Edge

Mozilla Firefox – od verze 56

Google Chrome – od verze 61

Testování probíhá na verzích aktuálních v době testování.

Patrně budou fungovat i jiné prohlížeče a jiné verze, ale bez záruky správného rozmístění ovládacích prvků.

## Mailová komunikace

Pro některé typy komunikace je jako komunikační kanál (pouze výstupní) využita standardní mailová komunikace. Tento kanál je používán zejména při správě uživatelů a při zasílání protokolů.

Maily jsou zasílány z domény cnb.cz ve formátu HTML a nejsou šifrované ani podepsané, mohou ovšem obsahovat přílohy opatřené elektronickou pečetí.

# Jednotlivá prostředí ČNB

Externím uživatelům jsou zpřístupněna produkční a testovací prostředí.

## Produkční prostředí

### Adresa produkčního prostředí

* Webová aplikace - <https://sdat.cnb.cz/sdat_ext/>
* Webové služby - <https://sdat.cnb.cz/sdat_ws/> (adresa pro volání webové služby Soap POST requesty - ne přístup prohlížečem)

### Servisní odstávky

Zpravidla každé pondělí probíhá v odpoledních hodinách technická odstávka systému - důvodem je nasazování nových verzí.

### Obsah produkčního prostředí

Zprovozněné moduly externího portálu:

* prezentace metodických informací (veřejná část),
* správa Osoby a uživatelských účtů (neveřejná část - řízený přístup),
* prezentace vykazovacích povinností (neveřejná část - řízený přístup),
* informační webové služby (řízený přístup).

Dostupné metodické informace:

* migrované platné metodiky ze systému MtS od roku 2016
* výkazy vytvořené na základě XBRL taxonomií EBA (platné od roku 2018) a EIOPA (platné od roku 2017).

## Testovací prostředí

Testovací prostředí systému SDAT bude trvale dostupné jako funkční kopie produkčního prostředí, určená zejména pro testování klientského SW a předprodukční testování metodik.

### Adresa testovacího prostředí

* Webová aplikace - <https://sdatt.cnb.cz/sdat_ext/>
* Webové služby - <https://sdatt.cnb.cz/sdat_ws/> (adresa pro volání webové služby Soap POST requesty - ne přístup prohlížečem)

### Servisní odstávky

Zpravidla v pondělí probíhá v odpoledních hodinách technická odstávka systému - důvodem je nasazování nových verzí.

### Obsah testovacího prostředí

Zprovozněné moduly externího portálu:

* prezentace metodických informací (veřejná část),
* správa Osoby a uživatelských účtů (neveřejná část - řízený přístup),
* prezentace vykazovacích povinností (neveřejná část - řízený přístup),
* informační webové služby (řízený přístup).

Dostupné metodické informace:

* migrované platné metodiky ze systému MtS od roku 2016
* výkazy vytvořené na základě XBRL taxonomií EBA (platné od roku 2018) a EIOPA (platné od roku 2017).