



sedex: Webservice-Proxy-Benutzerhandbuch

Installation, Konfiguration und Verwendung Webservice-Proxy 5.2

Projektname: Sedex
Projektnummer: LZPSB10-00626
Dokumenten-Version: V4.2

Status	in Arbeit	in Prüfung	genehmigt zur Nutzung
	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Beteiligter Personenkreis	
Autor:	Lorenz Ammon, Thomas Wenger
Genehmigung:	Stefan Leisi
Benützer/Anwender:	Softwarelieferanten, BFS
zur Information/Kenntnis:	

Änderungskontrolle, Prüfung, Genehmigung			
Wann	Version	Wer	Beschreibung
19.11.2008	V0.1	Lorenz Ammon	Initiale Version
30.11.2008	V0.7	Stephan Tschäppät	Proof-Reading / Layout
03.12.2008	V0.8	Lorenz Ammon	Fehlermeldungen in Kapitel ausgegliedert. DTD-Fehlermeldung hinzugefügt.
9.12.2008	V0.9	Lorenz Ammon	„Bekannte Probleme“-Abschnitt hinzugefügt. Druckfehler bei Propertynamen für UPI-Query-Endpunkt korrigiert.
15.01.2009	V1.0	Lorenz Ammon	Proxy-Konfiguration in Abschnitt 2.2.3 angepasst. Kapitel „Bekannte Probleme“ angepasst. Kapitel „Migration von Konfigurationsdateien“ hinzugefügt. Beta-Bemerkung aus Abschnitt „Einführung“ entfernt. Abschnitt 2.2.7 überarbeitet.
18.03.2009	V1.1	Lorenz Ammon	Korrektur des Test-Requests „UPI-Query: getAhvvn“: bisheriger Request war für AHV13-statt AHV11-Abfragen gültig.

Änderungskontrolle, Prüfung, Genehmigung			
Wann	Version	Wer	Beschreibung
18.03.2009	V1.2	Lorenz Ammon	Neu verfügbaren Webservice UPICompare aufgenommen.
07.04.2009	V1.3	Lorenz Ammon	URLs der Dienstbringer-Test-Endpunkte hinzugefügt.
11.06.2009	V1.4	Lorenz Ammon	Anpassungen für neues Release 2.1
25.06.2009	V1.5	Stephan Tschäppät	Proof-Reading / Layout
26.06.2009	V1.6	Jörg Böhlen	Genehmigung
02.07.2009	V1.7	Lorenz Ammon	Anpassungen gemäss Kommentaren/Gespräch Michel Gentile. Dokumentation der Startvariante „Tanuki-Service-Wrapper“ unter Unix.
03.07.2009	V1.8	Jörg Böhlen	Genehmigung
01.12.2009	V1.9	Lorenz Ammon	SOAP-over-OSCI-Ablösung eingepflegt (Release 2.2.0)
04.03.2010	V2.0	Lorenz Ammon	Anpassungen für neues Release 2.2.1. Hinweis zu UPI-Query ab Schema V1.2. Konfigurationsoptionen für Connection-Timeout und „Connections per Host“
14.09.2010	V2.1	Lorenz Ammon	Anpassungen für neues Release 3.0 (Abschnitte „Migration von Konfigurationsdateien“, „Bekannte Probleme“).
14.09.2010	V2.1	Stefan Leisi	Genehmigung
02.12.2011	V3.0	Thomas Wenger	Anpassung an neuen sedex-Client mit Steuerung durch sedex-Controller. Logging umfasst neu ein Technical-Log und ein Access-Log.
08.12.2011	V 3.0	Stefan Leisi	Genehmigung für Release 4.0
01.02.2012	V 3.0.1	Michel Gentile	Änderung der Versionsnummer
15.11.2012	V 3.0.3	Markus Antener	Änderung der Versionsnummer
25.07.2013	V 3.0.4	Michel Gentile	Anpassung der «test»-Endpunkte für den UPI-Webservice.
19.06.2015	V 4.0	Markus Antener	Anpassung an die neue Zertifikatserneuerung durch den Controller, eUmzugCH Webservices
18.10.2016	V 4.1	Markus Antener	Neue URL beim Sasis Webservice
12.04.2017	V 4.2	Markus Antener	Update für Release 5.2.0

Referenzierte Dokumente

[Client]	sedex-Client 5.0.0: Installation and User Manual
[UPI]	UPI (Unique Personal Identifier) Interface
[sedex]	sedex-Handbuch

Begriffe, Abkürzungen

BFS	Bundesamt für Statistik, Neuenburg
DNS	Domain Name System
DTD	Document Type Declaration
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

Begriffe, Abkürzungen	
SOAP	Simple Object Access Protocol
SoapUI	Ein Werkzeug zum Testen von Webservices (http://www.soapui.org)
UPI	Unique Personal Identifier
VM	Virtual Machine
ZAS	Zentrale Ausgleichsstelle

Inhaltsverzeichnis

1	EINFÜHRUNG	7
1.1	Zweck diese Dokuments	7
1.2	Der sedex-Webservice-Proxy	7
2	INSTALLATION UND KONFIGURATION	9
2.1	Installation mit dem Installationsprogramm	9
2.2	Installation ohne Installationsprogramm	9
2.2.1	Ausführungsberechtigungen unter Unix setzen	9
2.2.2	Webservice-Proxy im Controller aktivieren	10
2.2.3	Webservice-Proxy Konfiguration	10
2.2.4	Konfiguration des Webservice-Proxy-Ports	10
2.2.5	Konfiguration eines http-Proxys	10
2.2.6	Konfiguration des sedex-Zertifikats	11
2.2.7	Konfiguration der Dienstbringerzertifikate	11
2.2.8	Konfiguration des Deploy-Mechanismus	12
2.2.9	Konfiguration des Loggings	12
2.3	Servicespezifische Konfigurationsoptionen	13
2.3.1	Konfiguration der Dienstbringer-Endpunkte	13
2.3.2	Connection-Timeout	14
2.3.3	Connections per Host	14
2.4	Spezielle Zugriffsberechtigungen	14
2.4.1	Keystore-Properties	14
2.4.2	Truststore und Truststore-Properties	15
2.4.3	Log-Verzeichnis	15
2.4.4	Deploy-Verzeichnis	15
2.5	Konfiguration des verwendeten Hauptspeichers	15
2.5.1	Konfiguration VM-Speicher	15
2.6	Deinstallation	15
3	BETRIEB	16
3.1	Anforderungen	16
3.1.1	Grundsätzlich gleiche Vorgaben wie Adapter	16
3.1.2	Ports	16
3.1.3	Hauptspeicher	16
3.2	Ausführen des Webservice-Proxys	16
3.3	Logging	17
3.3.1	Webservice-Proxy-Technical-Log	17
3.3.2	Webservice-Proxy-Access-Log	17
3.4	Konfigurationsänderungen nach der Installation	18
4	ZERTIFIKATSERNEUERUNG	19
4.1	Automatisierte Zertifikatserneuerung	19
4.2	Manuelle Zertifikatserneuerung	19
4.2.1	Erneuerung der vertrauenswürdigen Serverzertifikate	19
4.2.2	Erneuerung des sedex-Teilnehmerzertifikats	19

5	HINZUFÜGEN ODER ERNEUERN VON WEBSERVICES	20
5.1	Hinzufügen von neuen Webservices	20
5.2	Erneuern eines bestehenden Webservices	20
6	VERWENDUNG	21
6.1	Verfügbare Webservices, Stand 1.6.2015	21
6.1.1	UPI Query	21
6.1.2	UPI Compare	21
6.1.3	CheckSedex	22
6.1.4	Sedex External Authorisation	22
6.1.5	PlausEx	22
6.1.6	Sasis / VeKa	23
6.1.7	Partnerws / UID	23
6.1.8	Echo	23
7	TESTS UND TEST-REQUESTS	25
7.1	Tests	25
7.1.1	Webservice-Proxy erreichbar?	25
7.1.2	UPI Query erreichbar?	25
7.1.3	UPI Compare erreichbar?	25
7.1.4	CheckSedex erreichbar?	25
7.2	Test-Requests	26
7.2.1	UPI Query: getAhvvn	26
7.2.2	UPI Compare: compareData	26
7.2.3	CheckSedex	27
8	FEHLERBEHEBUNG	28
8.1	SOAP-Fehler	28
8.1.1	"Must not contain a DTD"	28
8.2	Deploy-Probleme	28
8.2.1	Stop-Datei im Deploy-Verzeichnis	28
8.3	Webservice-Proxy nicht erreichbar	29
8.3.1	Webservice-Proxy ohne Fehlermeldung nicht erreichbar	29
9	BEKANNTE PROBLEME	30
9.1	Aktuell vorhandene Probleme	30
9.2	Behobene Probleme	30
9.2.1	Fehlender SOAP-Header verursacht im Debug-Modus eine Exception	30
9.2.2	Lokale Timeouts nach HTTP-Fehlern beim Diensterbringer	30
9.2.3	No route to host	30
9.2.4	The namespace prefix "nsany" was not declared	30
10	MIGRATION VON KONFIGURATIONSDATEIEN	32
10.1	Von Release 4.0 auf 5.0	32
10.2	Von Release 3.0 auf 4.0	32
10.3	Von Release 2.2.1 auf 3.0	32
10.4	Von Release 2.2.0 auf 2.2.1	32

Abbildungen

ABBILDUNG 1: KONZEPT WEBSERVICE-PROXY 8

1 Einführung

1.1 Zweck diese Dokuments

Dieses Dokument vermittelt das notwendige Wissen, um den sedex-Webservice-Proxy auf Stufe Softwarelieferant erfolgreich einzusetzen.

1.2 Der sedex-Webservice-Proxy

Der sedex-Client besteht aus dem Controller, dem Adapter und dem Webservice-Proxy. Damit der Webservice-Proxy verwendet werden kann, muss er zusammen mit den anderen Komponenten installiert werden. Der Webservice-Proxy kann nicht einzeln installiert werden, da er vom Adapter und dem Controller abhängig ist. Der Controller wiederum ermöglicht die Steuerung und die Überwachung des Adapters und des Webservice-Proxys (Start, Stopp usw.).

Der Webservice-Proxy agiert als Intermediär zwischen einem Webservice-Dienstanbieter und einem Webservice-Benutzer. Durch folgende Merkmale erleichtert der Webservice-Proxy die Arbeit des Benutzers:

- Lokale Replizierung der Webservice-Endpunkte des Dienstanbieters
- Entgegennahme eines HTTP-Aufrufs des Benutzers
- Verschlüsseln des Aufrufs mithilfe des Teilnehmer-Zertifikats
- Verbindung zum gewünschten Dienstanbieter
- Übermittlung der Anfrage via HTTPS an den Dienstanbieter
- Entgegennahme der Antwort des Dienstanbieters via HTTPS
- Entschlüsselung der Antwort
- Weiterleitung der Antwort via HTTP an den Benutzer

Durch der Verarbeitungen, die vom Webservice-Proxy übernommen werden, muss sich der Benutzer nur um die HTTP-Anfragen kümmern. Die ganze Sicherheit (Verschlüsselung und Weiterleitung) wird durch den Webservice-Proxy sichergestellt. Da das Zertifikat des sedex-Teilnehmers verwendet wird, entfällt auch die Übermittlung eines Benutzernamen und eines Passwortes.

Die Abbildung 1 zeigt die Funktionsweise des Webservice-Proxys in einer Übersicht

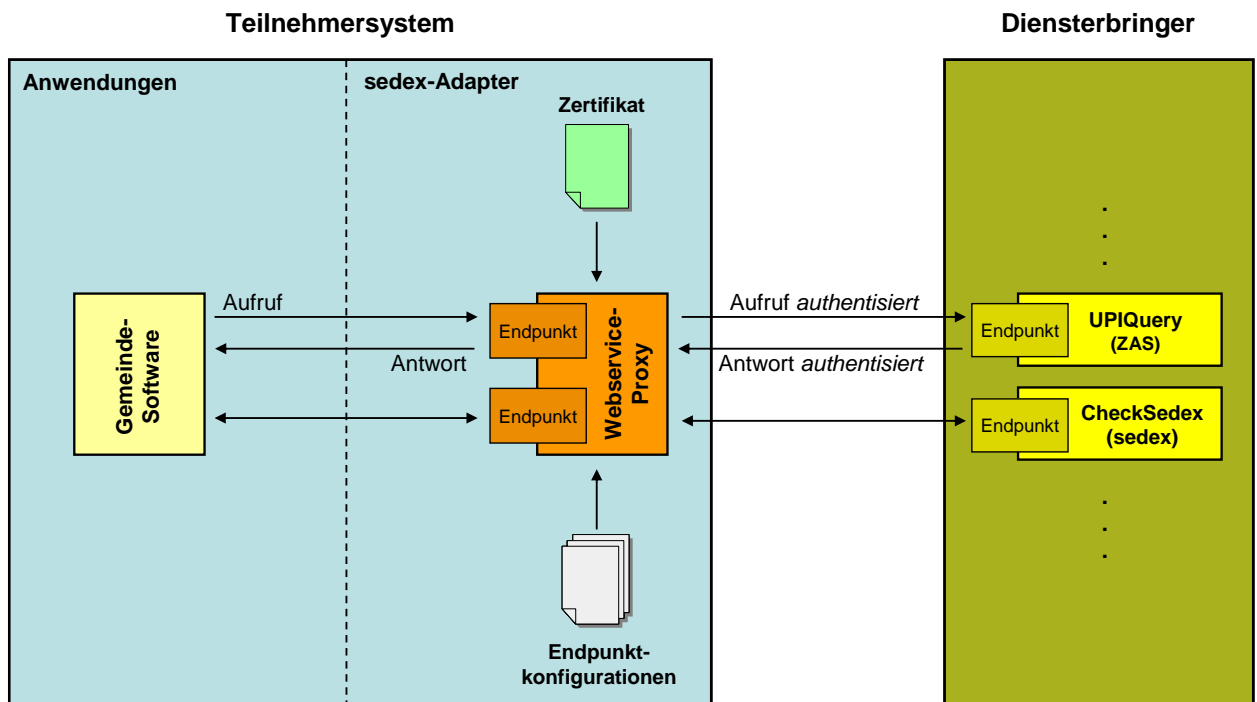


Abbildung 1: Konzept WebService-Proxy

Der Aufruf von Webservices an den lokalen Endpunkten des WebService-Proxys erfolgt ohne Angabe von Sicherheitsmerkmalen wie z. B. Zertifikaten. Da nur physische sedex-Teilnehmer über ein Zertifikat und einen sedex Client verfügen, kann der sedex WebService-Proxy auch nur bei physischen sedex-Teilnehmern zum Einsatz kommen.

Der sedex-WebService-Proxy ist für den Einsatz bei „gewöhnlichen“ sedex-Teilnehmern wie z. B. Einwohnerregister-Ämtern von Gemeinden dimensioniert. Er ist nicht direkt für ein Aufrufvolumen ausgelegt, welches durch den Einsatz bei aggregierenden sedex-Teilnehmern anfallen kann.

Ein solches aggregierendes Szenario wäre z.B. gegeben, wenn der Kanton Bern bestimmte Webservice-Aufrufe seiner Gemeindeverwaltungen einzeln sammeln und die Aufrufe stellvertretend auch wieder einzeln an den eigentlichen Dienstbringer weiterleiten würde. Zur Realisierung dieses Szenarios müsste ein aggregierender Teilnehmer IT-Infrastruktur aufbauen, welche die Webservice-Aufrufe der zu aggregierenden Teilnehmer entgegennimmt und die aufrufenden Teilnehmer anhand irgendwelcher Merkmale identifiziert. Es wird davon ausgegangen, dass in einem solchen aggregierenden Szenario auch die Weiterleitung der gesammelten Webservice-Aufrufe (unter Authentisierung mit dem sedex-Zertifikat des aggregierenden Teilnehmers) mit der dazu aufgebauten IT-Infrastruktur des aggregierenden Teilnehmers realisiert wird.

2 Installation und Konfiguration

Die Installation des sedex-Webservice-Proxy ist Teil der Installation des sedex-Clients.

Dieser kann automatisiert mit dem Installationsprogramm für Windows oder manuell installiert werden (vgl. [Client]). Das Installationsprogramm installiert standardmässig nur den Adapter und den Controller. Wenn der Webservice-Proxy ebenfalls installiert werden soll, ist während der automatisierten Installation die entsprechende Checkbox zu aktivieren.

Soll eine automatisiert installierte sedex-Webservice-Proxy-Installation manuell nachkonfiguriert werden, können die benötigten Informationen dem Abschnitt 2.2 entnommen werden.

2.1 Installation mit dem Installationsprogramm

Wird der sedex-Adapter mit Hilfe des Installationsprogramms für Windows installiert, muss der Anwender während der Installation spezifizieren, auf welchem TCP-Port der Webservice-Proxy seine Dienste anbieten soll. Der Webservice-Proxy-Port muss zwingend angepasst werden, wenn der Default-Port 8080 bereits von einer anderen installierten Anwendung verwendet wird.

Zusätzlich ist sicherzustellen, dass der Webservice-Proxy-Port für eingehende Aufrufe offen ist und dass der Webservice-Proxy über HTTP und HTTPS mit dem Internet kommunizieren kann.

Dies bedingt in der Regel eine passende Konfiguration von vorhandenen Firewalls. So fragt z. B. die Windows-Firewall beim erstmaligen Start des Webservice-Proxys unter Umständen nach, ob Verbindungen mit der Java-VM zugelassen oder blockiert werden sollen. Hier muss der entsprechende Zugriff gewährt werden.

2.2 Installation ohne Installationsprogramm

Wird die manuelle Art der Adapterinstallation verwendet, muss der Webservice-Proxy anschliessend auch manuell konfiguriert werden.

Hinweis: Der Webservice-Proxy setzt eine voll funktionsfähige Installation des Adapters wie in [Client] beschrieben voraus.

/!\ Achtung: Es wird explizit keine Garantie dafür abgegeben, dass die manuellen Konfigurationsmöglichkeiten zwischen Versionen des Webservice-Proxys identisch bleiben. Insbesondere wird davon abgeraten, sich darauf zu verlassen, dass der Webservice-Proxy direkt auf einer Axis2-Distribution aufgebaut ist.

Im Folgenden bezeichnet `ClientDir` das Installationsverzeichnis des sedex-Clients.

2.2.1 Ausführungsberechtigungen unter Unix setzen

Wird der Webservice-Proxy auf einem Unix-System installiert, muss nach der Installation den Skriptdateien das Ausführungsrecht gegeben werden. Dazu sind in einer Shell-Datei folgende Schritte auszuführen:

1. Wechsel in das Verzeichnis `ClientDir/adapter/bin`
2. Ausführen des Befehls: `chmod +x *.sh`
3. Wechsel in das Verzeichnis `ClientDir/adapter/axis2/bin`
4. Ausführen des Befehls: `chmod +x *.sh`

2.2.2 Webservice-Proxy im Controller aktivieren

Damit der Webservice-Proxy zukünftig automatisch vom sedex Controller gestartet werden kann, muss er in der Konfiguration vom sedex Controller aktiviert werden:

Konfigurationsdatei: ClientDir/controller/conf/sedexController.properties

```
wsproxy.enabled=true
```

2.2.3 Webservice-Proxy Konfiguration

Der Pfad, unter welchem der sedex Client installiert ist, muss in der Konfiguration des Webservice-Proxy eingetragen werden:

Konfigurationsdatei: ClientDir/adapter/conf/wsproxy.properties

```
sedex.home=C:/Program Files/SedexClient
```

Es entspricht dem Basisverzeichnis in der ZIP Datei.

Vorsicht: Es ist wichtig, den Pfadseparator "/" zu verwenden, auch auf Windows Installationen.

2.2.4 Konfiguration des Webservice-Proxy-Ports

Der Port, unter welchem der Webservice-Proxy die lokal replizierten Dienste anbietet, wird in der folgenden Konfigurationsdatei spezifiziert:

Konfigurationsdatei: ClientDir/adapter/axis2/conf/axis2.xml

Dort findet sich im XML-Element `transportReceiver` der folgende Konfigurationseintrag:

Konfiguration: `<parameter name="port">8080</parameter>`

Default-Wert für den Webservice-Proxy-Port ist 8080. Es muss darauf geachtet werden, dass der spezifizierte Port nicht bereits von einer anderen Anwendung verwendet wird. Zusätzlich ist sicherzustellen, dass der Webservice-Proxy-Port für eingehende Aufrufe offen ist.

Achtung:

Sollen mehrere Webservice-Proxys auf einem einzigen Host betrieben werden, so müssen diese Webservice-Proxys zwingend auf unterschiedliche Ports konfiguriert werden. Bsp: 8080, 8081, 8082, usw.

2.2.5 Konfiguration eines http-Proxys

Wird der Web-Zugang in der Installationsumgebung des Webservice-Proxys über einen HTTP-Proxy (Web-Proxy) hergestellt, so muss die entsprechende Konfiguration für den HTTP-Zugang in der folgenden Konfigurationsdatei eingetragen werden:

Konfigurationsdatei: ClientDir/adapter/conf/wsproxy.properties

Darin sind die folgenden Properties mit den passenden Angaben anstelle von „proxy.domain.ch“, „8080“, „name“ und „pwd“ zu setzen:

Konfiguration:

```
sedex.wsproxy.webproxy.host=proxy.domain.ch
sedex.wsproxy.webproxy.port=8080
sedex.wsproxy.webproxy.user=name
sedex.wsproxy.webproxy.password=pwd
```

Wird vom Web-Proxy keine Authentisierung mit Benutzername und Passwort verlangt, so sollten die letzten zwei Zeilen gelöscht bzw. mit einem „#“ am Anfang der Zeile auskommentiert werden. Soll kein Web-Proxy verwendet werden, sind alle obigen Zeilen zu löschen bzw. auszukommentieren.

2.2.6 Konfiguration des sedex-Zertifikats

Dem Webservice-Proxy muss der Zugriff auf das sedex-Zertifikat gewährt werden. Dazu müssen Speicherort, Typ und Passwort des zu verwendenden sedex-Zertifikats in einer separaten Keystore-Konfigurationsdatei spezifiziert werden. Diese Keystore-Konfigurationsdatei wird dann in der Webservice-Proxy-Hauptkonfigurationsdatei referenziert.

Angenommen, die Keystore-Konfigurationsdatei ist unter dem folgenden Pfad abgelegt:

Keystore-Konfigurationsdatei: ClientDir/adapter/conf/wsproxykey.properties

Dann sind darin die folgenden Properties mit den passenden Angaben zu setzen:

Konfiguration:

```
sedex.wsproxy.keystore.path=ClientDir/adapter/zertifikate/prod-bit/cert.pl2
sedex.wsproxy.keystore.password=certpwd
sedex.wsproxy.keystore.type=PKCS12
```

In der Webservice-Proxy-Hauptkonfigurationsdatei muss diese Keystore-Konfigurationsdatei dann wie folgt referenziert werden:

Konfigurationsdatei: ClientDir/adapter/conf/wsproxy.properties

Konfiguration:

```
sedex.wsproxy.keystore.properties.path=ClientDir/adapter/conf/wsproxykey.properties
```

2.2.7 Konfiguration der Diensterbringerzertifikate

Die Zertifikate der Diensterbringer, welchen der Webservice-Proxy vertrauen soll, werden in einer Truststore-Datei gepflegt. Dazu müssen dem Webservice-Proxy Speicherort, Typ, Passwort und Versionsnummer der Truststore-Datei bekannt gemacht werden. Der Speicherort des Truststores muss wie folgt spezifiziert werden:

Konfigurationsdatei: ClientDir/adapter/conf/wsproxy.properties

Konfiguration (alles auf nur einer Zeile):

```
sedex.wsproxy.serviceclient.ssl.truststore.path=
    ClientDir/adapter/zertifikate/prod-bit/wsproxytrust.jks
```

Typ, Passwort und Versionsnummer des Truststores werden dann wie folgt spezifiziert:

Konfigurationsdatei:

ClientDir/adapter/zertifikate/prod-bit/wsproxytrust.jks.properties

Konfiguration:

```
sedex.wsproxy.truststore.password=trustme
sedex.wsproxy.truststore.version=versionnr
sedex.wsproxy.truststore.type=JKS
```

Zur spezifizierten Truststore-Datei wsproxytrust.jks gibt es also im selben Verzeichnis eine Properties-Datei wsproxytrust.jks.properties, welche die zugehörige eigentliche Truststore-Datei beschreibt. **Fehlt zu einem Truststore die passende Properties-Datei, wird der Webservice-Proxy diese Truststore-Datei nicht verwenden können.** Truststores werden vom sedex-Betreiber immer in Form von zwei solchen zueinander passenden Dateien

ausgeliefert. Das Versionsproperty wird vom sedex-Betreiber definiert und darf nicht eigenhändig angepasst werden.

2.2.8 Konfiguration des Deploy-Mechanismus

Der Webservice-Proxy implementiert einen Deploy-Mechanismus, der es dem sedex-Adapter erlaubt, einen laufenden Webservice-Proxy mit Updates zu versorgen. Solche Updates sind Dateien, welche der Webservice-Proxy in einem speziellen Deploy-Verzeichnis entgegennimmt und nach gewissen Vorgaben bei sich installiert. Die Installation eines Updates kann den Neustart des Webservice-Proxys auslösen. Deshalb kann für einen Webservice-Proxy die Installation von Updates auf einen bestimmten Zeitraum eingeschränkt werden. Momentan unterstützt der Webservice-Proxy über den Deploy-Mechanismus die automatisierte Installation neuer Truststores und neuer sedex-Zertifikate. Die Konfiguration des Deploy-Mechanismus wird im Folgenden kurz erläutert.

Das Deploy-Verzeichnis, in welchem der Webservice-Proxy nach Updates sucht, wird wie folgt konfiguriert:

Konfigurationsdatei: `ClientDir/adapter/conf/wsproxy.properties`

Konfiguration:

```
sedex.wsproxy.server.deploydir.path=ClientDir/adapter/deploy
```

!/\ Achtung: Der Webservice-Proxy wird von „seinem“ zugehörigen sedex-Adapter nur Updates erhalten, wenn in der Adapterkonfiguration [client] als Zielverzeichnis für die vom Adapter auszuliefernden Updates das gleiche Deploy-Verzeichnis wie beim Webservice-Proxy konfiguriert ist!

Der Webservice-Proxy kann angewiesen werden, Updates aus dem Deploy-Verzeichnis nur innerhalb bestimmter Stunden des Tages zu installieren. Die entsprechenden Vorgaben können wie folgt gemacht werden:

Konfigurationsdatei: `ClientDir/adapter/conf/wsproxy.properties`

Konfiguration:

```
sedex.wsproxy.server.deployhours.start=startingHour  
sedex.wsproxy.server.deployhours.start=endingHour
```

Der Webservice-Proxy wird Updates an jedem Tag zwischen den Stunden «startingHour» und «endingHour» installieren. Mit `startingHour=0` und `endingHour=23` wird keine Einschränkung gemacht und Updates können während des ganzen Tags installiert werden. Mit `startingHour=1` und `endingHour=3` werden Updates nur in den Nachtstunden zwischen 01:00 und 03:59 vorgenommen.

Innerhalb der für Updates zugelassenen Stunden überprüft der Webservice-Proxy das Deploy-Verzeichnis periodisch (alle 5 Minuten) nach Updates.

2.2.9 Konfiguration des Loggings

Der sedex-Webservice-Proxy führt zwei Log-Dateien:

- eine *Technical-Log-Datei*, in welcher aufgetretene Fehler, Warnungen und Informationen zur Konfiguration des Webservice-Proxys während des Betriebs aufgezeichnet werden,
- und eine *Access-Log-Datei*, in welcher alle über den Webservice-Proxy erfolgten Webservice-Aufrufe protokolliert werden.

Die Konfiguration der beiden Logs wird in der Logback-Konfigurationsdatei vorgenommen:

Konfigurationsdatei: `ClientDir/adapter/conf/wsproxy-logback.xml`

Hier muss eingetragen werden, in welche Dateien der sedex-Webservice-Proxy Log-Einträge schreiben soll. Da der Webservice-Proxy rollende Logs in mehreren Dateien führt, muss er im Verzeichnis der angegebenen Log-Dateien das Recht haben, neue Dateien anzulegen und in diese zu schreiben.

Konfiguration Technical-Log-Datei:

```
<appender name="wsproxy-technical" class="ch.qos.logback.core.rolling.RollingFileAppender">
    <File>ClientDir/logs/wsproxy/wsproxy-technical.log</File>
    [...]
</appender>
```

Konfiguration Access-Log-Datei:

```
<appender name="wsproxy-access" class="ch.qos.logback.core.rolling.RollingFileAppender">
    <File>ClientDir/logs/wsproxy/wsproxy-access.log</File>
    [...]
</appender>
```

Eine weitere interessante, aber fakultative Anpassung legt das Log-Level für die eigentlichen Webservice-Proxy-Klassen auf eines der Log-Levels `ERROR`, `INFO`, `WARN` oder `DEBUG` fest. Am meisten Informationen werden dabei auf dem `DEBUG`-Level ausgegeben, am wenigsten auf dem `ERROR`-Level. Für den produktiven Einsatz sollte `INFO` gewählt werden.

Konfiguration Log-Level der Technical-Log-Datei:

```
<logger name="ch.admin.bit.sedex.wsproxy" level="INFO" />
```

Konfiguration Log-Level der Access-Log-Datei:

Im Access-Log erfolgen alle Einträge auf dem Level `INFO`. Das Access-Log kann also beispielsweise abgestellt werden, indem einfach der Log-Level für dieses Log auf die Stufe `ERROR` angehoben wird.

```
<logger name="WSProxyAccessLogfile" level="INFO" additivity="false">
    <appender-ref ref="wsproxy-access" />
</logger>
```

2.3 Servicespezifische Konfigurationsoptionen

Einige Konfigurationsoptionen können spezifisch pro angebotenen Service konfiguriert werden. Diese Optionen werden im Folgenden kurz beschrieben.

2.3.1 Konfiguration der Diensterbringer-Endpunkte

Die Endpunkte der jeweiligen Diensterbringer hinter einem lokalen Webservice-Proxy-Endpunkt können in der folgenden Konfigurationsdatei konfiguriert werden:

Konfigurationsdatei: `ClientDir/adapter/conf/wsproxy.properties`

Für jeden replizierten Webservice können dort die entsprechenden Properties gesetzt werden. Wird für einen bestimmten Webservice kein Eintrag vorgenommen, wird als Default automatisch die produktive Standardadresse des Diensterbringers gewählt. Während der Entwick-

lungsphase und für Tests wird empfohlen, die von den Dienstbringern zur Verfügung gestellten Testinstanzen der Dienste zu verwenden. Dazu müssen die untenstehenden Konfigurationsanpassungen vorgenommen werden. Für den produktiven Betrieb wird hingegen empfohlen, keine expliziten Konfigurationen der Dienstbringer-Endpunkte vorzunehmen.

Konfiguration UPIQuery-Webservice (alles auf nur einer Zeile):

```
sedex.wsproxy.UPIQueryService.target.endpoint.url=  
https://wupi-test.zas.admin.ch/wupi_cc/UPIQueryService
```

Konfiguration UPICompare-Webservice (alles auf nur einer Zeile):

```
sedex.wsproxy.UPICompareService.target.endpoint.url=  
https://wupi-test.zas.admin.ch/wupic_cc/UPICompareService
```

2.3.2 Connection-Timeout

Über das Connection-Timeout kann in Millisekunden festgelegt werden, wie lange der Webservice-Proxy auf eine Antwort vom Dienstbringer warten soll. Eine explizite Konfiguration des Connection-Timeouts wird nur empfohlen, falls im produktiven Betrieb Probleme auftreten.

Konfigurationsdatei: ClientDir/adapter/conf/wsproxy.properties

Konfiguration: `sedex.wsproxy.servicename.timeout=60000`

servicename kann UPICompareService (60000), UPIQueryService (360000) oder CheckSedexWebService (60000) sein. Werden die entsprechenden Konfigurationen nicht vorgenommen, werden die Default-Werte in den Klammern verwendet.

2.3.3 Connections per Host

Mit der Konfigurationsoption „Connections per Host“ kann die maximale Anzahl Verbindungen vorgegeben werden, welche der Webservice-Proxy gleichzeitig pro Service zu einem Dienstbringer-Server öffnen darf. Eine explizite Konfiguration der „Connections per Host“ wird nur empfohlen, falls im produktiven Betrieb Probleme auftreten.

Konfigurationsdatei: ClientDir/adapter/conf/wsproxy.properties

Konfiguration: `sedex.wsproxy.servicename.connections.perhost.default=5`

servicename kann UPICompareService (5), UPIQueryService (10) oder CheckSedexWebService (5) sein. Werden die entsprechenden Konfigurationen nicht vorgenommen, werden die Default-Werte in den Klammern verwendet.

2.4 Spezielle Zugriffsberechtigungen

Der Webservice-Proxy benötigt prinzipiell auf alle Dateien und Verzeichnissen innerhalb seines Installationsverzeichnisses Lesezugriff. Zusätzlich benötigt der Webservice-Proxy auf gewissen Dateien und Verzeichnissen spezielle weitere Zugriffsberechtigungen. Diese werden im Folgenden aufgelistet:

2.4.1 Keystore-Properties

Der Webservice-Proxy muss während eines Updates die Keystore-Properties-Datei aus Abschnitt 2.2.6 ersetzen können.

2.4.2 Truststore und Truststore-Properties

Der Webservice-Proxy muss die Truststore- und die Truststore-Properties-Datei aus Abschnitt 2.2.7 ersetzen können. Zusätzlich muss er für Backup-Zwecke im Verzeichnis des Truststores neue Dateien erzeugen und diese beschreiben können.

2.4.3 Log-Verzeichnis

Der Webservice-Proxy muss im Log-Verzeichnis bzw. in den Log-Verzeichnissen aus Abschnitt 2.2.9 Dateien anlegen und diese beschreiben können.

2.4.4 Deploy-Verzeichnis

Der Webservice-Proxy muss im Deploy-Verzeichnis aus Abschnitt 2.2.8 eine Datei anlegen und Update-Dateien löschen können. Ausserdem muss er den Verzeichnisisinhalt des Deploy-Verzeichnisses abfragen können.

2.5 Konfiguration des verwendeten Hauptspeichers

Bei Bedarf kann mit der gebotenen Vorsicht der von der Java-VM für den Webservice-Proxy allozierte minimale und maximale Speicher angepasst werden.

2.5.1 Konfiguration VM-Speicher

Die Java-VM des Webservice-Proxy wird vom sedex-Controller über die Startup-Skripts des Webservice-Proxys gestartet:

Konfigurationsdatei Windows:

```
ClientDir/adapter/bin/wsproxy-start.bat
```

Konfigurationsdatei Unix:

```
ClientDir/adapter/bin/wsproxy-start.sh
```

Entsprechend können die Speichereinstellungen sowie weitere Startparameter für die VM in diesen Skripts als Java-Optionen konfiguriert werden:

Konfiguration: `JAVA_OPTS=-Xms128M -Xmx256M [weitere Optionen]`

Hinweis: Bei der Konfiguration dieser beiden Parameter ist darauf zu achten, dass die weiteren konfigurierten Java-Optionen nicht geändert oder gelöscht werden!

2.6 Deinstallation

Der Webservice-Proxy ist Teil des sedex-Clients und wird mit diesem installiert. Deshalb wird der Webservice-Proxy auch wieder zusammen mit dem Client deinstalliert (vgl. [Client]).

3 Betrieb

Im Folgenden bezeichnet `ClientDir/adapter` das Installationsverzeichnis des sedex-Clients.

3.1 Anforderungen

3.1.1 Grundsätzlich gleiche Vorgaben wie Adapter

Der sedex-Webservice-Proxy ist Teil des sedex-Clients und stellt grundsätzlich dieselben Anforderungen wie dieser (vgl. [Client]). Zusätzliche Anforderungen des Webservice-Proxys werden im Folgenden kurz aufgelistet.

3.1.2 Ports

Eingehend

Der Port, unter welchem der Webservice-Proxy lokal replizierte Dienste anbietet, muss für eingehende Verbindungen offen sein. Default-Wert für den Webservice-Proxy-Port ist 8080.

Ausgehend

Der Webservice-Proxy tätigt Aufrufe zu den eigentlichen Dienstbringern über HTTPS (Port 443). Deshalb müssen für den Webservice-Proxy ausgehende Verbindungen über dieses Protokoll (Port) erlaubt sein und mindestens die Server der eigentlichen Dienstbringer (vgl. Abschnitt 6) erreichbar sein.

3.1.3 Hauptspeicher

Der sedex-Webservice-Proxy läuft in einer eigenen Java-VM. Der Speicher, welchen der Webservice-Proxy verwendet, muss deshalb zum Speicher, welcher vom sedex-Controller und vom sedex-Adapter benötigt wird, hinzugerechnet werden. Der sedex-Webservice-Proxy konfiguriert der Speicher (Heap) der Java-VM wie folgt:

- *minimal* allozierter Heap: 128 MB
- *maximal* allozierbarer Heap: 256 MB

Bei Bedarf können diese Defaults angepasst werden (vgl. Abschnitt 2.5).

3.2 Ausführen des Webservice-Proxys

Der Webservice-Proxy wird nicht direkt gestartet, sondern vom sedex-Controller gestartet, gestoppt und überwacht. Eine Anleitung zur Ausführung des sedex-Controllers findet sich in [Client].

Hinweise:

- Es ist nicht vorgesehen, dass der Webservice-Proxy direkt, d. h. ohne Zuhilfenahme des sedex-Controllers, gestartet oder gestoppt wird.
- Falls der Webservice-Proxy ohne Fehler startet, aber nach dem Start trotzdem nicht erreichbar ist, sollte die Konfiguration des Webservice-Proxy-Ports überprüft werden (vgl. Kapitel 2.2.2). Es ist sicherzustellen, dass ein gültiger und freier Port eingetragen ist.

3.3 Logging

Der Webservice-Proxy führt zwei unterschiedliche Log-Dateien:

- das Technical-Log
- das Access-Log

Die folgenden Abschnitte gehen getrennt auf die beiden Log-Dateien ein.

3.3.1 Webservice-Proxy-Technical-Log

Der sedex-Webservice-Proxy führt eine Technical-Log-Datei, in welcher aufgetretene Fehler, Warnungen und Informationen zur Konfiguration des Webservice-Proxys während des Betriebs aufgezeichnet werden. Das Log wird per Default rollend in folgender Datei geführt:

Log-Datei: ClientDir/logs/wsproxy/wsproxy-technical.log

Die Konfiguration des Loggings ist in Abschnitt 2.2.9 beschrieben.

3.3.2 Webservice-Proxy-Access-Log

Der sedex-Webservice-Proxy führt eine Access-Log-Datei, in welcher die über den Proxy abgewickelten Webservice-Aufrufe protokolliert werden. Das Log wird per Default rollend in folgender Datei geführt:

Log-Datei: ClientDir/logs/wsproxy/wsproxy-access.log

Die Konfiguration des Loggings ist in Abschnitt 2.2.9 beschrieben.

Format des Access-Log

Die Einträge des Access-Logs bestehen aus durch mindestens zehn mittels Leerzeichen separierten Feldern:

Feld	Beschreibung
date	Datum des Eintrags im Format ISO 8601: YYYY-MM-DD Bsp: 2004-07-11
time	Uhrzeit des Eintrags im Format ISO 8601: hh:mm:ss.f Bsp: 16:43:16.234
duration	Dauer des Aufrufs (Round Trip Time) in Millisekunden. Bsp: 129
client	IP-Adresse des aufrufenden Clients. Bsp: 192.128.30.22
result-code	Resultats-Code (eine Zeichenkette). Bsp: OK Standardantwort für erfolgreiche Aufrufe. Fault_HTTP_Get_Not_Allowed SOAP-Fault mit Hinweis auf Typ des Faults.
req-bytes	Anzahl Bytes des SOAP-Requests.
rsp-bytes	Anzahl Bytes der SOAP-Response.
req-endpoint	Endpunkt (URL) des Diensterbringers. Hinweis: Allfällige Leerzeichen werden durch Underscores („_“) ersetzt.
req-method	Name der Webservice-Methode, welche im Request aufgerufen wird.
orig-req	Endpunkt (URL) auf dem WS-Proxy. Hinweis: Allfällige Leerzeichen werden durch Underscores („_“) ersetzt.

optional fields	Künftige weitere Felder werden hier angefügt werden.
--------------------	--

3.4 Konfigurationsänderungen nach der Installation

Änderungen an der Konfiguration des Webservice-Proxys nach der Installation können analog den Beschreibungen in Abschnitt 2.2 vorgenommen werden. Alle Änderungen an den beschriebenen Konfigurationsdateien bedingen einen Neustart des Webservice-Proxys via sedex-Controller.

4 Zertifikatserneuerung

4.1 Automatisierte Zertifikatserneuerung

Der Webservice-Proxy kann seine Zertifikate nicht selbständig erneuern. Über seinen Deploy-Mechanismus bietet der Webservice-Proxy aber ein Verfahren an, das es erlaubt, von aussen sowohl seinen Truststore als auch das für die sichere Kommunikation verwendete sedex-Teilnehmerzertifikat zu ersetzen. Dieser Deploy-Mechanismus wird sowohl vom sedex-Adapter wie auch vom sedex-Controller verwendet.

Immer wenn ein sedex-Controller sein sedex-Teilnehmer-Zertifikat erneuert, versorgt er auch seinen zugehörigen Webservice-Proxy damit. Zudem kann ein sedex-Adapter neue Truststore-Dateien empfangen und diese ins Deploy-Verzeichnis seines zugehörigen Webservice-Proxys zur Installation ausliefern. Der Webservice-Proxy wird also letztlich von seinem Adapter und Controller mit Updates versorgt.

4.2 Manuelle Zertifikatserneuerung

4.2.1 Erneuerung der vertrauenswürdigen Serverzertifikate

Beim Hinzufügen von zusätzlichen Webservices (oder aus anderen Gründen) kann es notwendig werden, die Liste der vertrauenswürdigen Server-Zertifikate zu erneuern. Dazu wird vom sedex-Betreiber ein entsprechender neuer Truststore zur Verfügung gestellt. Dieser Truststore besteht aus zwei Dateien, z. B. `truststore.jks` und `truststore.jks.properties`. Diese zwei Dateien müssen gemeinsam in einem vom Webservice-Proxy zugreifbaren Verzeichnis abgelegt werden und der Speicherort der Dateien muss in der Webservice-Proxy-Konfiguration, wie in Abschnitt 2.2.7 beschrieben, spezifiziert werden. Wenn die Dateien des alten Truststores direkt mit den Dateien des neuen Truststores überschrieben werden, ist keine Anpassung der Webservice-Proxy-Konfigurationsdatei notwendig. Um ersetzte Truststore-Dateien bzw. eine angepasste Konfiguration anzuwenden, muss der Webservice-Proxy gestoppt und neu gestartet werden.

4.2.2 Erneuerung des sedex-Teilnehmerzertifikats

Das sedex-Teilnehmer-Zertifikat wird zusammen mit dem sedex-Adapter installiert und vom Webservice-Proxy nur referenziert. Für die Erneuerung dieses Zertifikats wird deshalb auf [Client] verwiesen. Nach der Erneuerung des Teilnehmer-Zertifikats muss die Webservice-Proxy-Konfiguration wie in Abschnitt 2.2.6 beschrieben an die Verwendung des neuen Zertifikats angepasst werden. Um die angepasste Konfiguration anzuwenden, muss der Webservice-Proxy gestoppt und neu gestartet werden.

5 Hinzufügen oder Erneuern von Webservices

Im Folgenden bezeichnet `ClientDir` das Installationsverzeichnis des sedex-Clients.

5.1 Hinzufügen von neuen Webservices

Neue, zusätzliche Webservices, die der Webservice-Proxy unterstützen soll, werden als Webservice-Archive, deren Namen dem Muster „*.aar“ entsprechen, verteilt.

Die Installation eines solchen Webservice-Archivs wird dadurch vorgenommen, dass die entsprechende Archivdatei einfach in das folgende Verzeichnis kopiert wird:

Installationsverzeichnis: `ClientDir/adapter/axis2/repository/services`

Eventuell müssen beim Hinzufügen eines neuen Webservices auch Konfigurationsdateien und/oder die Liste der vertrauenswürdigen Server-Zertifikate angepasst werden (vgl. Abschnitt 2.2.7).

Ein Neustart des Webservice-Proxys nach Hinzufügen eines neuen Webservices ist nur notwendig, wenn gleichzeitig auch noch Konfigurationsdateien oder die Liste der vertrauenswürdigen Server-Zertifikate angepasst wurden.

5.2 Erneuern eines bestehenden Webservices

Zur Erneuerung eines bestehenden Webservices wird eine neuere Version des entsprechenden, bereits installierten Webservice-Archives verteilt. Die Erneuerung wird dadurch vorgenommen, dass die entsprechende Webservice-Archiv-Datei einfach im folgenden Verzeichnis überschrieben wird:

Installationsverzeichnis: `ClientDir/adapter/axis2/repository/services`

Ein Neustart des Webservice-Proxys nach Erneuerung eines bestehenden Webservices ist nur notwendig, wenn gleichzeitig auch noch Konfigurationsdateien oder die Liste der vertrauenswürdigen Server-Zertifikate angepasst wurden (vgl. Abschnitt 2.2.7).

6 Verwendung

6.1 Verfügbare Webservices, Stand 1.6.2015

Im Folgenden bezeichnet `wsproxyhost` die IP-Adresse oder den DNS-Host-Eintrag (symbolischer Name) des Rechners, auf dem der Webservice-Proxy installiert ist, und `wsproxyport` den Port, auf dem der Webservice-Proxy seine Dienste anbietet.

6.1.1 UPI Query

Für Online-Abfragen bei der ZAS steht das „UPI Query“-Interface zur Verfügung. Die Dokumentation dieses Interfaces ist in [UPI] beschrieben. Dieser Webservice ist auch direkt bei der ZAS verfügbar (vgl. unten). Damit der Webservice-Proxy das UPI-Query-Interface erfolgreich zur Verfügung stellen kann, muss er über HTTPS auf den entsprechenden Server der ZAS zugreifen können.

Mit der Schema-Version 1.2 von UPI Query kam unter anderem die Operation „getCancelledAndInactiveAhvvn“ hinzu. Aufrufe dieser Operation dauern zum Teil auch für Abfragen über wenige Tage bereits sehr lange (einige Minuten). Deshalb wurden für UPI Query die Konfigurationsoptionen „Connection-Timeout“ und „Connections per Host“ speziell festgelegt (vgl. Abschnitte 2.3.2 und 2.3.3).

Endpunkt-URL	<code>http://wsproxyhost:wsproxyport/wsproxy/services/UP- IQueryService</code>
WSDL-URL	<code>http://wsproxyhost:wsproxyport/wsproxy/services/UP- IQueryService?wsdl</code>

Ein direkter Zugriff auf den UPI-Query-Webservice der ZAS ist unter Verwendung des sedex-Zertifikats unter den folgenden Endpunkten möglich:

Produktion: `https://wupi.zas.admin.ch/wupi_cc/UPIQueryService`
(`https://wupi.zas.admin.ch/wupi_cc/UPIQueryService?wsdl`)

Test: `https://wupi-test.zas.admin.ch/wupi_cc/UPIQueryService`
(`https://wupi-test.zas.admin.ch/wupi_cc/UPIQueryService?wsdl`)

6.1.2 UPI Compare

Für vergleichende Online-Abfragen bei der ZAS steht das „UPI Compare“-Interface zur Verfügung. Die Dokumentation dieses Interfaces ist in [UPI] beschrieben. Dieser Webservice ist auch direkt bei der ZAS verfügbar (vgl. unten). Damit der Webservice-Proxy das UPI-Compare-Interface erfolgreich zur Verfügung stellen kann, muss er über HTTPS auf den entsprechenden Server der ZAS zugreifen können.

Endpunkt-URL	<code>http://wsproxyhost:wsproxyport/wsproxy/services/UPICo- mpareService</code>
WSDL-URL	<code>http://wsproxyhost:wsproxyport/wsproxy/services/UPICo- mpareService?wsdl</code>

Ein direkter Zugriff auf den UPI-Compare-Webservice der ZAS ist unter Verwendung des sedex-Zertifikats unter den folgenden Endpunkten möglich:

Produktion: https://wupi.zas.admin.ch/wupic_cc/UICompareService
(https://wupi.zas.admin.ch/wupic_cc/UICompareService?wsdl)

Test: https://wupi-test.zas.admin.ch/wupic_cc/UICompareService
(https://wupi-test.zas.admin.ch/wupic_cc/UICompareService?wsdl)

6.1.3 CheckSedex

Für Abfragen zur Verfügbarkeit und zu Einsatzmöglichkeiten von sedex steht das CheckSedex-Interface bereit. Die Dokumentation dieses Interfaces ist in [sedex] beschrieben. Dieser Webservice ist auch direkt über das sedex-Webservice-Gateway verfügbar (vgl. unten). Damit der Webservice-Proxy das CheckSedex-Interface erfolgreich zur Verfügung stellen kann, muss er über HTTPS auf den sedex-Webservice-Gateway zugreifen können.

Endpoint-URL	http://wsproxyhost:wsproxyport/wsproxy/services/CheckSedexWebService
WSDL-URL	http://wsproxyhost:wsproxyport/wsproxy/services/CheckSedexWebService?wsdl

Ein direkter Zugriff auf den CheckSedex-Webservice von sedex ist unter Verwendung des sedex-Zertifikats unter dem folgenden Endpunkt möglich:

Produktion: <https://sedex-service.admin.ch/sedex-runtime-ws/CheckSedexWebService>
(<https://sedex-service.admin.ch/sedex-runtime-ws/CheckSedexWebService?wsdl>)

6.1.4 Sedex External Authorisation

Für Abfragen zur Autorisierung von externen asynchronen Webservices, die über die sedex Infrastruktur angeboten werden, steht das ExternalAuth-Interface bereit. Die Dokumentation dieses Interfaces ist in [extAuth] beschrieben.

Endpoint-URL	http://wsproxyhost:wsproxyport/wsproxy/services/sedexExternalAuthorisationService
WSDL-URL	http://wsproxyhost:wsproxyport/wsproxy/services/sedexExternalAuthorisationService?wsdl

Ein direkter Zugriff auf den External-Authorisation-Webservice von sedex ist unter Verwendung des sedex-Zertifikats unter dem folgenden Endpunkt möglich:

Produktion: <https://sedex-service.admin.ch/sedexExternalServices/sedexExternalAuthorisationService>
(<https://sedex-service.admin.ch/sedexExternalServices/sedexExternalAuthorisationService?wsdl>)

6.1.5 PlausEx

Für Abfragen in Zusammenhang mit eUmzugCH steht der PlausEx Webservice bereit.

Endpunkt-URL	http://wsproxyhost:wsproxyport/wsproxy/services/SHSWebService
WSDL-URL	http://wsproxyhost:wsproxyport/wsproxy/services/SHSWebService?wsdl

Ein direkter Zugriff auf den PlausEx-Webservice ist unter Verwendung des sedex-Zertifikats unter dem folgenden Endpunkt möglich:

Produktion: <http://cd009339.adb.intra.admin.ch/PlausExWebservice/PlausExWebservice.asmx>

(<http://cd009339.adb.intra.admin.ch/PlausExWebservice/PlausExWebservice.asmx?wsdl>)

6.1.6 Sasis / VeKa

Für Abfragen in Zusammenhang mit eUmzugCH steht der Sasis Webservice bereit.

Endpunkt-URL	http://wsproxyhost:wsproxyport/wsproxy/services/VeKa_Query
WSDL-URL	http://wsproxyhost:wsproxyport/wsproxy/services/VeKa_Query?wsdl

Ein direkter Zugriff auf den PlausEx-Webservice ist unter Verwendung des sedex-Zertifikats unter dem folgenden Endpunkt möglich:

Produktion: https://www.versichertenkarte.ch/queryws_1_0/VeKa_Query_1_0.asmx

(https://www.versichertenkarte.ch/queryws_1_0/VeKa_Query_1_0.asmx?wsdl)

6.1.7 Partnerws / UID

Für Abfragen in Zusammenhang mit eUmzugCH steht der UID Webservice bereit.

Endpunkt-URL	http://wsproxyhost:wsproxyport/wsproxy/services/PartnerServices
WSDL-URL	http://wsproxyhost:wsproxyport/wsproxy/services/PartnerServices?wsdl

Ein direkter Zugriff auf den PlausEx-Webservice ist unter Verwendung des sedex-Zertifikats unter dem folgenden Endpunkt möglich:

Produktion: <https://www.uid-wse.admin.ch/V3.0/PartnerServices.svc>

(<https://www.uid-wse.admin.ch/V3.0/PartnerServices.svc?wsdl>)

6.1.8 Echo

Der Echo-Webservice bietet eine simple Möglichkeit, zu testen, ob der Webservice-Proxy verfügbar ist. Wie sein Name erwarten lässt, wiederholt der Echo-Webservice in seiner Antwort einfach die an ihn gestellte Anfrage, versieht diese allerdings zusätzlich noch mit einem Zeit-

stempel. Dieser Webservice ist nur über den Webservice-Proxy verfügbar und für Entwicklungs- und Testzwecke gedacht. Software im produktiven Einsatz sollte nicht von der Existenz oder Funktionalität des Echo-Webservices abhängen. Es wird keine Garantie gegeben, dass der Echo-Webservice in späteren Versionen des Webservice-Proxys noch in exakt derselben Form oder überhaupt verfügbar sein wird.

SOAP 1.1 Endpunkt-URL	<code>http://wsproxyhost:wsproxyport /wsproxy/services/echows.echowsHttpSoap11Endpoint</code>
SOAP 1.2 Endpunkt-URL	<code>http://wsproxyhost:wsproxyport /wsproxy/services/echows.echowsHttpSoap12Endpoint</code>
WSDL-URL	<code>http://wsproxyhost:wsproxyport/wsproxy/services/echows?wsdl</code>

7 Tests und Test-Requests

7.1 Tests

Im Folgenden bezeichnet `wsproxyhost` die IP-Adresse oder den DNS-Host-Eintrag (symbolischer Name) des Rechners, auf dem der Webservice-Proxy installiert ist, und `wsproxyport` den Port, auf dem der Webservice-Proxy seine Dienste anbietet.

7.1.1 Webservice-Proxy erreichbar?

Um herauszufinden, ob von einem Rechner aus der Webservice-Proxy unter dem konfigurierten Port erreichbar ist, kann vom untersuchten Rechner aus mit einem Webbrowser die folgende URL aufgerufen werden:

```
http://wsproxyhost:wsproxyport/wsproxy/services/echoes?wsdl
```

Ist der Webservice-Proxy erreichbar, erscheint im Browser eine Webseite, welche das WSDL-Dokument zum echo-Webservice enthält. Dieses Dokument beschreibt die vom Webservice angebotenen Operationen.

7.1.2 UPI Query erreichbar?

Um herauszufinden, ob es dem Webservice-Proxy möglich ist, den UPI-Query-Webservice aufzurufen, kann mit einem Webbrowser vom Rechner, auf dem der Webservice-Proxy installiert ist, die folgende URL aufgerufen werden:

```
https://wupi.zas.admin.ch/wupi_cc/UPIQueryService
```

Damit der Zugriff auf diese URL möglich ist, muss das sedex-Zertifikat zuvor in den verwendeten Webbrowser importiert werden. Beim Aufruf der obigen URL werden dann das sedex-Zertifikat abgefragt und eine Webseite angezeigt, welche unter anderem den folgende Satz enthält: „Hello! This is an Axis2 Web Service!“

7.1.3 UPI Compare erreichbar?

Um herauszufinden, ob es dem Webservice-Proxy möglich ist, den UPI-Compare-Webservice aufzurufen, kann mit einem Webbrowser vom Rechner, auf dem der Webservice-Proxy installiert ist, die folgende URL aufgerufen werden:

```
https://wupi.zas.admin.ch/wupic_cc/UPICompareService
```

Damit der Zugriff auf diese URL möglich ist, muss das sedex-Zertifikat zuvor in den verwendeten Webbrowser importiert werden. Beim Aufruf der obigen URL werden dann das sedex-Zertifikat abgefragt und eine Webseite angezeigt, welche unter anderem den folgende Satz enthält: „Hello! This is an Axis2 Web Service!“

7.1.4 CheckSedex erreichbar?

Um herauszufinden, ob es dem Webservice-Proxy möglich ist, den CheckSedex-Webservice aufzurufen, kann mit einem Webbrowser vom Rechner, auf dem der Webservice-Proxy installiert ist, die folgende URL aufgerufen werden:

```
https://sedex-service.admin.ch/sedex-runtime-ws/CheckSedexWebService
```

Damit der Zugriff auf diese URL möglich ist, muss das sedex-Zertifikat zuvor in den verwendeten Webbrowser importiert werden. Beim Aufruf der obigen URL werden dann das sedex-Zertifikat abgefragt und eine Webseite angezeigt, welche unter anderem den folgende Satz enthält: „Welcome to the ... homepage“.

7.2 Test-Requests

Im Folgenden werden SOAP-Requests aufgeführt, die zum Testen der Verfügbarkeit des Webservice-Proxys und der dahinterliegenden Diensteanbieter verwendet werden können. Die Requests können z. B. mit Hilfe des frei erhältlichen Programms „SoapUI“ (www.soapui.org) an die entsprechenden Webservice-Proxy-Endpunkte geschickt werden.

7.2.1 UPI Query: getAhvvn

Im folgenden Request ist AHV-Nummer durch eine gültige AHV-11-Nummer zu ersetzen.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
                  xmlns:ns="http://www.ech.ch/xmlns/eCH-0085/1"
                  xmlns:ns1="http://www.ech.ch/xmlns/eCH-0044/1">
  <soapenv:Header/>
  <soapenv:Body>
    <ns:getAhvvnRequest>
      <ns:personIdentification>
        <ns:localPersonId>
          <ns1:personIdCategory>CH.AHV</ns1:personIdCategory>
          <ns1:personId>AHV-Nummer</ns1:personId>
        </ns:localPersonId>
      </ns:personIdentification>
    </ns:getAhvvnRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

7.2.2 UPI Compare: compareData

Der folgende Request vergleicht die Daten „Name“, „Vorname“, Geburtsdatum „yyyy-mm-dd“, Nationalität „0“ (Schweiz) und Geschlecht „1“ (männlich) vom Zeitpunkt „Exportdatum“ mit den Daten, welche unter „Versichertennummer“ bei ZAS gespeichert sind.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
                  xmlns:ns="http://www.ech.ch/xmlns/eCH-0086/1"
                  xmlns:ns1="http://www.ech.ch/xmlns/eCH-0044/1"
                  xmlns:ns2="http://www.ech.ch/xmlns/eCH-0084/1">
  <soapenv:Header/>
  <soapenv:Body>
    <ns:compareDataRequest>
      <ns:exportDate>Exportdatum</ns:exportDate>
      <ns:dataToCompare>
        <ns:ahvvn>Versichertennummer</ns:ahvvn>
        <ns:firstNames>Vorname</ns:firstNames>
        <ns:officialName>Nachname</ns:officialName>
        <ns:sex>1</ns:sex>
        <ns:dateOfBirth>
```

```
        <ns1:yearMonthDay>yyyy-mm-dd</ns1:yearMonthDay>
    </ns:dateOfBirth>
    <ns:nationality>
        <ns:nationalityStatus>0</ns:nationalityStatus>
    </ns:nationality>
</ns:dataToCompare>
</ns:compareDataRequest>
</soapenv:Body>
</soapenv:Envelope>
```

7.2.3 CheckSedex

Im folgenden Request ist `sedexId` durch eine gültige sedex-Id zu ersetzen.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/en-
velope/" xmlns:v1="http://sedex.admin.ch/checkSedexSchema/V1">
    <soapenv:Header/>
    <soapenv:Body>
        <v1:checkSedexReq>
            <senderSedexId>sedexId</senderSedexId>
            <physicalSenderSedexId>sedexId</physicalSenderSedexId>
            <messageType>99</messageType>
            <messageClass>0</messageClass>
            <recipientSedexId>sedexId</recipientSedexId>
        </v1:checkSedexReq>
    </soapenv:Body>
</soapenv:Envelope>
```

8 Fehlerbehebung

8.1 SOAP-Fehler

Tritt während des Bearbeitens eines Webservice-Aufrufes beim Webservice-Proxy oder beim eigentlichen Dienstbringer ein Fehler auf, so gibt der Webservice-Proxy wenn immer möglich einen SOAP-Fehler zurück. Falls der Dienstbringer selbst auf einen Aufruf mit einem SOAP-Fehler geantwortet hat, so wird dieser genau so auch vom Webservice-Proxy zurückgegeben. Eigene SOAP-Fehler erzeugt der Webservice-Proxy nur, wenn beim Aufruf des eigentlichen Dienstbringer etwas schief geht. Solche Fehler werden auch in das Log (vgl. Abschnitt 3.3.1) geschrieben. Die folgenden Abschnitte zeigen mögliche Ursachen für bestimmte SOAP-Fehler auf.

8.1.1 "Must not contain a DTD"

Fehlermeldung:

SOAP message MUST NOT contain a Document Type Declaration (DTD)

Ursache:

Diese Fehlermeldung wird erzeugt, wenn der beim Dienstbringer aufgerufene Webservice nicht wie erwartet mit einer SOAP-Nachricht antwortet, sondern mit einer HTML-Seite (welche eine DTD enthält). Typischerweise steht auf einer solchen HTML-Seite eine Fehlermeldung des Web-/App-Servers, auf dem der aufgerufenen Webservice installiert ist. Die HTML-Seite könnte z. B. melden, dass der aufgerufene Webservice nicht zur Verfügung steht oder der Aufrufer nicht autorisiert ist, den Webservice zu verwenden. Um die HTML-Seite mit der Fehlermeldung einzusehen, kann der betroffene Webservice-Endpunkt des Dienstanbieters direkt z. B. mit SoapUI oder einem Webbrowser unter Verwendung des sedex-Zertifikats aufgerufen werden.

8.2 Deploy-Probleme

8.2.1 Stop-Datei im Deploy-Verzeichnis

Unter gewissen Umständen schreibt der Webservice-Proxy eine `deploy.stop`-Datei in das Deploy-Verzeichnis. Solange diese Datei im Deploy-Verzeichnis vorhanden ist, ist der Deploy-Mechanismus des Webservice-Proxys blockiert. Um den Mechanismus zu deblockieren, muss die Datei `deploy.stop` gelöscht werden. Zuvor sollte aber die Ursache behoben werden, welche zur Erzeugung der Stop-Datei geführt hat.

Der Webservice-Proxy erzeugt eine Stop-Datei immer dann, wenn er nach der Verarbeitung einer Update-Datei im Deploy-Verzeichnis die Update-Datei nicht aus dem Deploy-Verzeichnis löschen konnte. Die Anwesenheit der Stop-Datei stellt in diesem Fall sicher, dass bei der nächsten periodischen Prüfung des Deploy-Verzeichnisses die bereits verarbeitete Update-Datei nicht nochmals verarbeitet wird.

Die Ursache für das Vorhandensein einer Stop-Datei ist also im Allgemeinen ein Berechtigungsproblem. Der Webservice-Proxy muss die Berechtigung haben, eine Update-Datei, welche der sedex-Adapter in das Deploy-Verzeichnis geschrieben hat, wieder aus dem Deploy-Verzeichnis zu entfernen. Vor dem Löschen einer Stop-Datei sollten also immer die Berechtigungen auf dem Deploy-Verzeichnis überprüft und evtl. angepasst werden.

8.3 Webservice-Proxy nicht erreichbar

8.3.1 Webservice-Proxy ohne Fehlermeldung nicht erreichbar

Falls der Webservice-Proxy ohne Fehlermeldung startet, aber trotzdem nicht erreichbar ist, sollte als erstes die Port-Konfiguration aus dem Abschnitt 2.2.2 überprüft werden. Hier muss unbedingt ein gültiger und freier Port spezifiziert werden. Der Default-Port ist 8080.

9 Bekannte Probleme

Die nachstehenden „bekannten Probleme“ beziehen sich ausschliesslich auf den Webservice-Proxy, nicht aber auf den sedex-Controller bzw. den sedex-Adapter.

9.1 Aktuell vorhandene Probleme

Zurzeit sind im Webservice-Proxy-Release 5.0 keine Probleme bekannt.

9.2 Behobene Probleme

9.2.1 Fehlender SOAP-Header verursacht im Debug-Modus eine Exception

Betrifft: Alle Webservice-Proxy-Releases \leq Version 2.2.1.

Wird der Webservice-Proxy im Debug-Modus betrieben, was nicht Default ist, verursacht ein im SOAP-Aufruf fehlender SOAP-Header eine Exception im Webservice-Proxy und der aufgerufene Webservice wird nicht ausgeführt. Weitere Aufrufe mit SOAP-Header werden jedoch ausgeführt.

9.2.2 Lokale Timeouts nach HTTP-Fehlern beim Diensterbringer

Betrifft: Webservice-Proxy-Release 2.2.0

Beantwortet der Server eines Diensterbringers mehrere Anfragen des Webservice-Proxys mit einem HTTP-Fehler, so führt dies i. Allg. dazu, dass der betroffene Dienst über den Webservice-Proxy für unbestimmte Zeit nicht mehr zur Verfügung steht. In diesem Fall wird jede weitere Anfrage für diesen Dienst vom Webservice-Proxy nur noch mit einem Timeout-SOAP-Fehler beantwortet. Ein Neustart des Webservice-Proxys behebt das Problem. Ursache ist ein Bug in Axis 1.5.1, welcher dazu führt, dass bei HTTP-Fehlern Verbindungen nicht mehr freigegeben werden und deshalb plötzlich keine neuen Verbindungen zum Diensterbringer-Server mehr aufgebaut werden können.

9.2.3 No route to host

Betrifft: Webservice-Proxy-Release 1.0 und 1.0.1

Es wurde in einer Umgebung, in welcher der Webservice-Proxy auf Linux hinter einem Web-Proxy betrieben wurde, beobachtet, dass der UPI-Query-Webservice des Webservice-Proxys keine Verbindung zum Server der ZAS aufbauen konnte und immer den SOAP-Fehler „No route to host“ zurückgab. Unter Windows trat das Problem in derselben Umgebung hingegen nicht auf.

9.2.4 The namespace prefix "nsany" was not declared

Betrifft: Webservice-Proxy Release 1.0 und 1.0.1

Bestimmte korrekt formulierte SOAP-Requests für den UPI-Query-Webservice werden zur Zeit vom Webservice-Proxy nicht korrekt weitergeleitet. Das Problem tritt im Zusammenhang mit Namespaces auf, welche nicht mit dem Namespace des Request-Elements übereinstimmen, und zwar immer dann, wenn Elemente dieses Namespaces in Sequenz aufeinanderfolgen. In diesem Fall ist im weitergeleiteten SOAP-Request nur der Namespace des ersten Elements korrekt referenziert, was im Fehler "The namespace prefix 'nsany' was not declared" resultiert.

Das folgende Beispiel zeigt ein Beispiel für einen solchen Request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://www.ech.ch/xmlns/eCH-0085/1"
xmlns:ns1="http://www.ech.ch/xmlns/eCH-0044/1">
  <soapenv:Header/>
  <soapenv:Body>
    <ns:getAhvvnRequest>
      <ns:personIdentification>
        <ns:localPersonId>
          <ns1:personIdCategory>CH.AHV</ns1:personIdCategory>
          <ns1:personId>000.00.000.000</ns1:personId>
        </ns:localPersonId>
      </ns:personIdentification>
    </ns:getAhvvnRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Das Problem wird hier durch die Sequenz der Elemente `<ns1:personIdCategory>` und `<ns1:personId>` ausgelöst.

10 Migration von Konfigurationsdateien

Im Folgenden bezeichnet `ClientDir` das Installationsverzeichnis des sedex-Clients.

10.1 Von Release 4.0 auf 5.0

Beim Wechsel zu Release 5.0 wird für das Logging neu Logback anstelle von Log4j eingesetzt. Die bestehende Logging-Konfiguration kann deshalb nicht wiederverwendet werden.

10.2 Von Release 3.0 auf 4.0

Mit dem Release 4.0 des sedex-Clients wird eine ganz neue Programmkomponente *sedex-Controller* eingeführt. Der sedex-Controller steuert u.a. den sedex-Adapter und den sedex-Webservice-Proxy. Als Folge dieser Umstellung weisen sowohl der sedex-Client als Ganzes als auch der Webservice-Proxy im Speziellen eine neue Konfigurationsdatei-Struktur auf.

Aufgrund der zahlreichen Änderungen wird empfohlen, den sedex-Client 4.0 neu zu installieren und die generierten Konfigurationsdateien anzupassen, ohne bestehende Konfigurationsdateien älterer Webservice-Proxys direkt weiterzuverwenden.

Änderungen:

- Umstellung der Log4J-Konfiguration von einer Java-Property-Datei (`AdapterDir/wsproxylog4j.properties`) auf eine XML-Datei (`ClientDir/adapter/conf/wsproxylog4j.xml`).
- Webservice Proxy befindet sich nun im Ordner `ClientDir/adapter/axis2`.

10.3 Von Release 2.2.1 auf 3.0

Für eine Migration von Release 2.2.1 zu Release 3.0 müssen keine Veränderungen an Konfigurationsdateien vorgenommen werden.

10.4 Von Release 2.2.0 auf 2.2.1

Für eine Migration von Release 2.2.0 zu Release 2.2.1 müssen keine Veränderungen an Konfigurationsdateien vorgenommen werden.