



Stefan Podolak, 30.09.2016

sedex Betriebs- / Integrationshandbuch

sedex-Client V5.0

www.sedex.ch

Inhaltsverzeichnis

1	Einführung	3
1.1	Zweck des Dokuments.....	3
2	sedex-Architektur	4
2.1	asynchron.....	5
2.1.1	Konzept.....	5
2.1.2	Ablauf Meldungsaustausch	7
2.2	synchron.....	8
2.2.1	Konzept.....	8
2.2.2	Ablauf Datenaustausch	9
2.3	physischer sedex-Teilnehmer	9
2.4	logischer sedex-Teilnehmer	10
3	Integration des sedex-Client (asynchron)	11
3.1	Funktionsweise	11
3.1.1	Dateischnittstelle	12
3.1.2	Adressierung.....	13
3.1.3	Meldungstypen.....	15
3.1.4	Polling	15
3.1.5	Retry	15
3.2	sedex-Umschlag.....	16
3.2.1	Umschlag - Schema invalid	18
3.2.2	MessageId - Dubletten	19
3.2.3	Meldung - Verfalldatum	19
3.3	sedex-Quittung.....	19
3.3.1	Fehlerkategorien	20
3.3.2	Statuscode	21
3.4	Monitoring	22
3.4.1	Textdatei	23
3.4.2	HTTP	23
4	Integration des Webservice-Proxy (synchron).....	24
4.1	Funktionsweise	24

4.2	Bundle.....	26
4.2.1	Statische URL	26
4.2.2	Dynamische URL	26
4.3	Webservice Checksedex	26
5	Betrieb des sedex-Client.....	28
5.1	Release Management.....	28
5.2	Remote Support Service.....	29
5.3	Client Update	30
5.4	Client Profile	30
5.5	Client Migration	30
5.6	Umgang mit den Zertifikaten	30
5.7	Housekeeping - Datenhaltung.....	31
5.8	eCH-0090 - XML-Schemas	31
5.9	Nachvollziehbarkeit	31
6	Glossar	32
7	Weitergehende Dokumentation	33

1 Einführung

sedex steht für secure data exchange und ist eine Dienstleistung des Bundesamts für Statistik BFS.

Die Plattform ist für den sicheren asynchronen Datenaustausch zwischen Organisationseinheiten konzipiert. In spezifischen Fällen erfolgt auch ein synchroner Datenaustausch. Die Plattform ist hochverfügbar (24/7).

sedex wurde im Rahmen der Modernisierung der Volkszählung 2010 aufgebaut, um die Statistiklieferungen der kommunalen Einwohnerdienste und der Personenregister des Bundes an das BFS sicherzustellen. Da sensitive Daten ausgetauscht werden, musste die Plattform von Beginn an hohen Anforderungen an die Sicherheit sowie Nachvollziehbarkeit genügen. Dazu setzt sedex moderne Verschlüsselungsverfahren sowie Sicherheitszertifikate der Swiss Government PKI ein.

Seit Inbetriebnahme Mitte 2008 hat sich sedex auch Teilnehmern ausserhalb der Registerharmonisierung und der Statistik geöffnet. Heute wird sedex von gut 4600 Organisationseinheiten in über 40 Domänen eingesetzt. Im Jahr 2014 wurden ca. 10 Millionen Meldungen via sedex übermittelt.

sedex fungiert als Postbote und ist vergleichbar mit einem eingeschriebenen Brief.

1.1 Zweck des Dokuments

Dieses Dokument richtet sich an Software-Architekten, Software-Entwickler sowie Betreiber des sedex-Client.

Dieses Handbuch dient als Integrationshilfe für Softwarelieferanten, die ihre Anwendung an sedex anbinden sowie die Betreiber des sedex-Client.

2 sedex-Architektur

Die folgende Abbildung gibt eine Übersicht über die Gesamtarchitektur von sedex. Links sind die Komponenten des sedex-Client ersichtlich. Im Wesentlichen besteht dieser aus den 3 Komponenten: Controller, Adapter und WS-Proxy. Rechts sind die zentralen Server-Komponenten ersichtlich. Über SAM (sedex Administration Management) werden die Aufträge abgewickelt und die Konfiguration der sedex-Plattform erfasst. Mit dem Drittsystem SIS werden die Reportings erstellt.

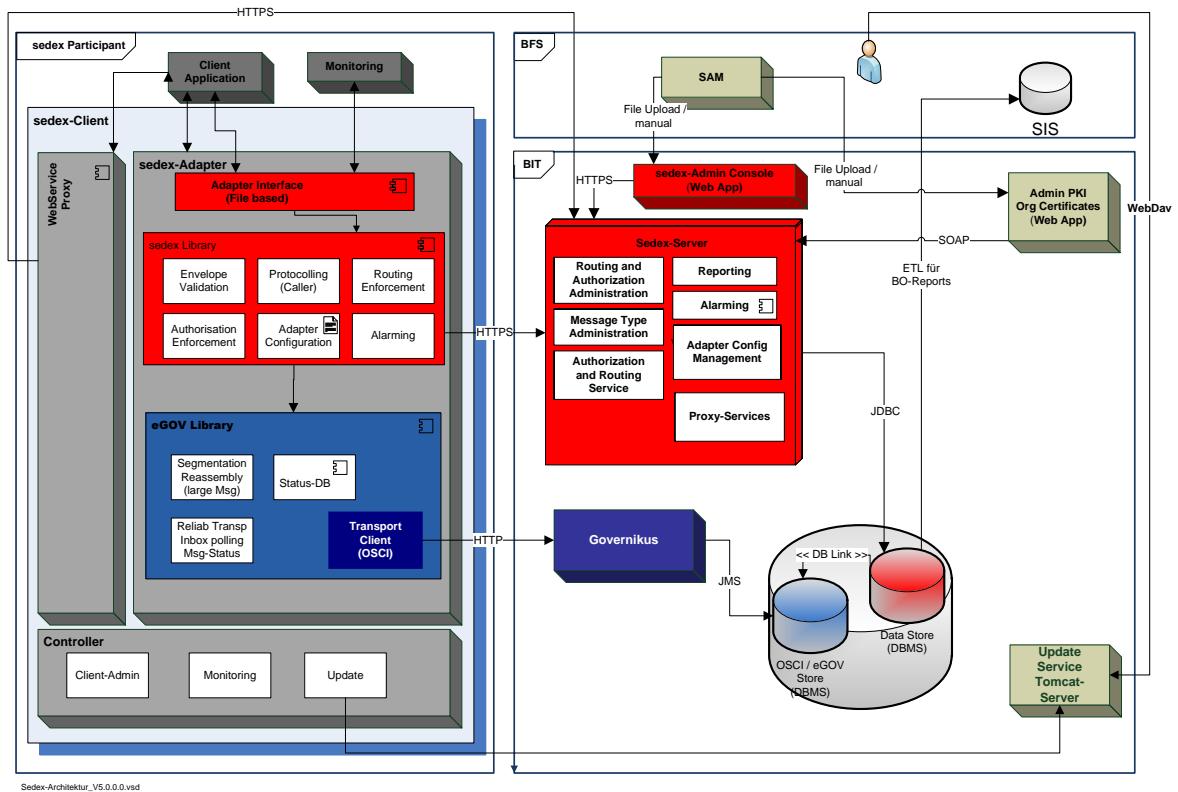


Abbildung 1: Gesamtarchitektur sedex

Die sedex-Clients kommunizieren über den zentralen sedex-Server. Sie werden in der geschützten Infrastruktur des sedex-Teilnehmers installiert. sedex ist ein Client-Server-System.

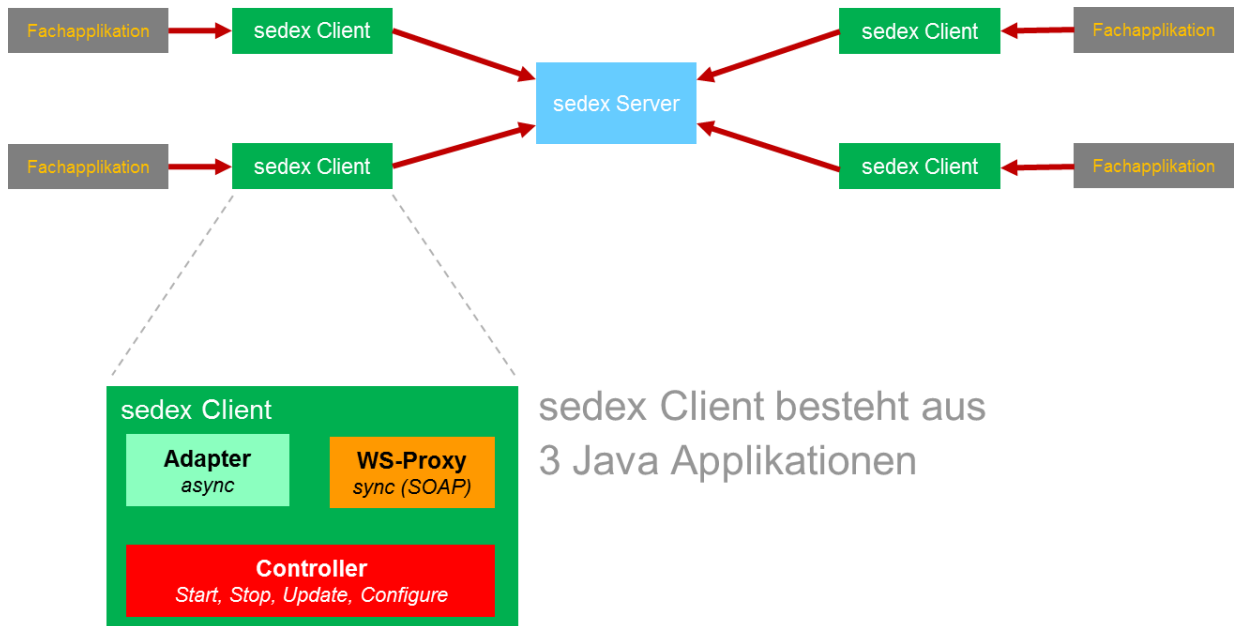


Abbildung 2: Kommunikation zwischen sedex-Client und Server

2.1 asynchron

2.1.1 Konzept

Die sedex-Architektur baut auf dem Konzept lose gekoppelter Anwendungen (Fachanwendung) auf, die in einem Verbund über eine Datendrehscheibe Meldungen austauschen.

Die Basis von sedex bildet der OSCI Standard. Als Kernkomponente wird Governikus als Intermediär eingesetzt. Dieser garantiert die vom Gesetzgeber geforderte Sicherheit (Authentifizierung, Zugriffskontrolle, Vertraulichkeit, Datenintegrität).

Um die Integration für die sedex-Teilnehmer zu vereinfachen und zusätzliche Dienste anzubieten (z.B. automatische Zertifikatserneuerung, Meldungsstückelung, Kompression, Datenverschlüsselung, Monitoring etc.), wurde zusätzlich der sedex-Client entwickelt. Der sedex-Client ist eine JAVA Applikation, die in der geschützten Infrastruktur des jeweiligen sedex-Teilnehmers installiert wird.

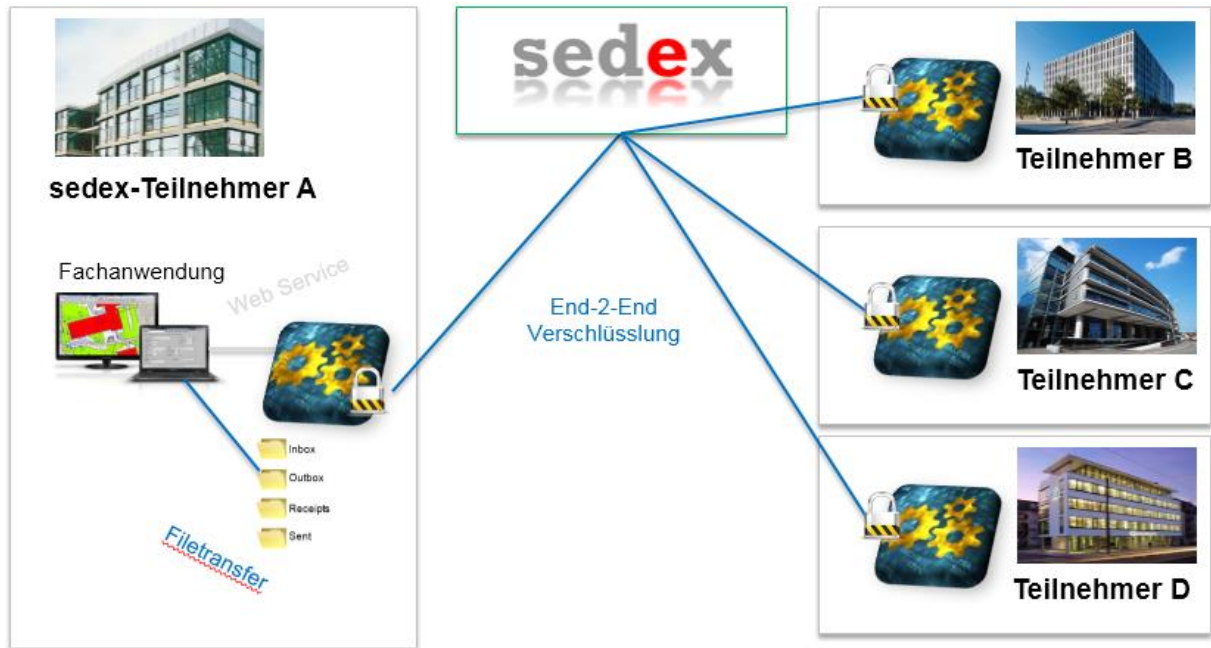


Abbildung 3: Schnittstelle zwischen Anwendung und sedex-System

Die Schnittstelle der Fachanwendungen zum sedex-Client besteht im Wesentlichen aus Verzeichnissen im Dateisystem (z.B. In- und Outbox). Versandquittungen des Systems werden in Form einer XML-Datei bereitgestellt.

2.1.2 Ablauf Meldungsaustausch

Sender und Empfänger sind technisch vollständig voneinander entkoppelt. Die Kommunikation zwischen ihnen läuft über einen asynchronen Meldungaustausch, wobei sedex die Rolle des Vermittlers übernimmt.

Die sendende Anwendung stellt dem Adapter die zu versendenden Meldungen als Dateien in einem Verzeichnis bereit, von wo aus sie über sedex an den vorgesehenen Empfänger transportiert werden. Die Grösse der Meldungen ist auf 10 GB limitiert.

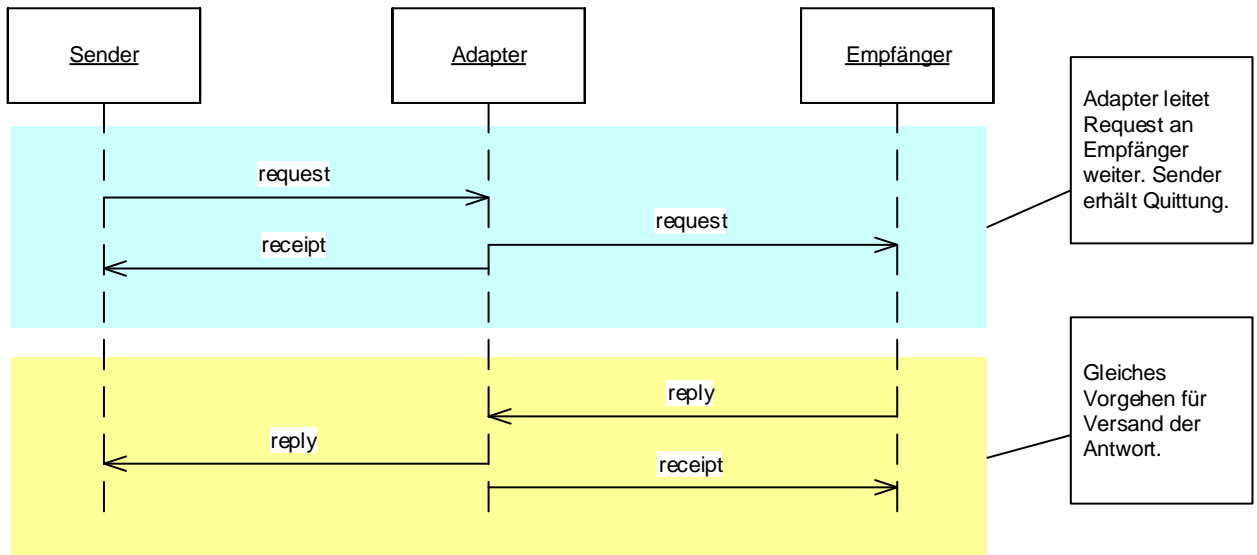


Abbildung 4: Erfolgreicher Versand einer Meldung

Die nachfolgende Grafik zeigt den gescheiterten Versand einer Meldung. Die Ursache dafür kann in einem formalen Fehler der sendenden Anwendung (z.B. falsche Adressierung im Umschlag) oder in einem technischen Problem (z.B. Netzwerkproblem) liegen. Die sendende Anwendung erhält in der Quittung entsprechende Hinweise auf die Fehlerursache.

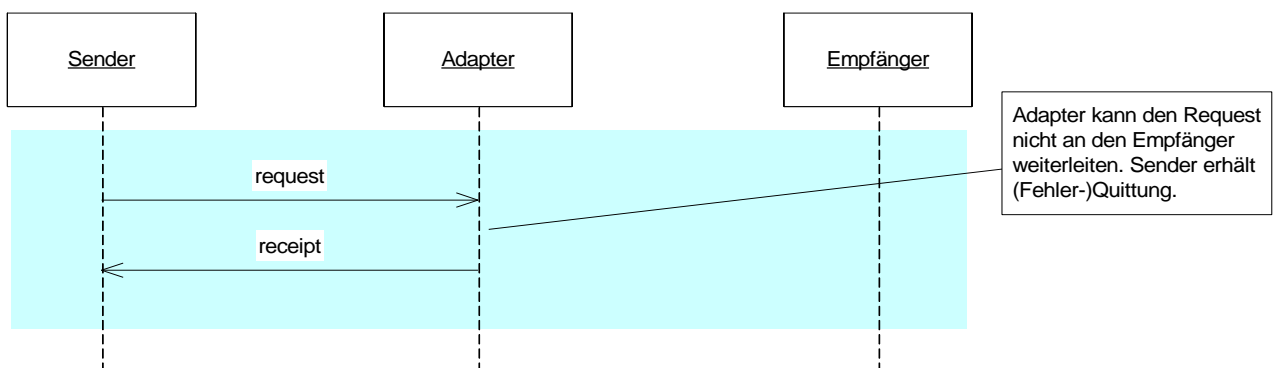


Abbildung 5: Gescheiterter Versand einer Meldung

Die nachfolgende Grafik zeigt den Versand einer einzelnen Meldung an zwei Empfänger. Dieses Szenario tritt auf, wenn die sendende Anwendung im Versandumschlag mehrere Empfänger aufführt. Der Adapter erstellt pro Empfänger eine Versandquittung.

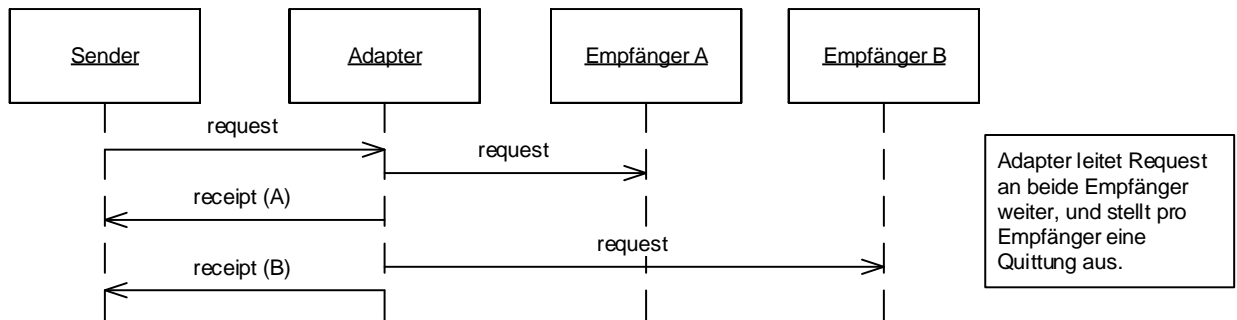


Abbildung 6: Versand einer Meldung an mehrere Empfänger

2.2 synchron

2.2.1 Konzept

Der sedex-Client ermöglicht auch die synchrone Kommunikation mit angebotenen Web-Services. Die aktuelle Liste der angebotenen Web Services finden Sie auf unserer Webseite: www.sedex.ch / synchron. Für die Verschlüsselung sowie Authentifizierung werden die bestehenden Credential vom sedex-Client verwendet.

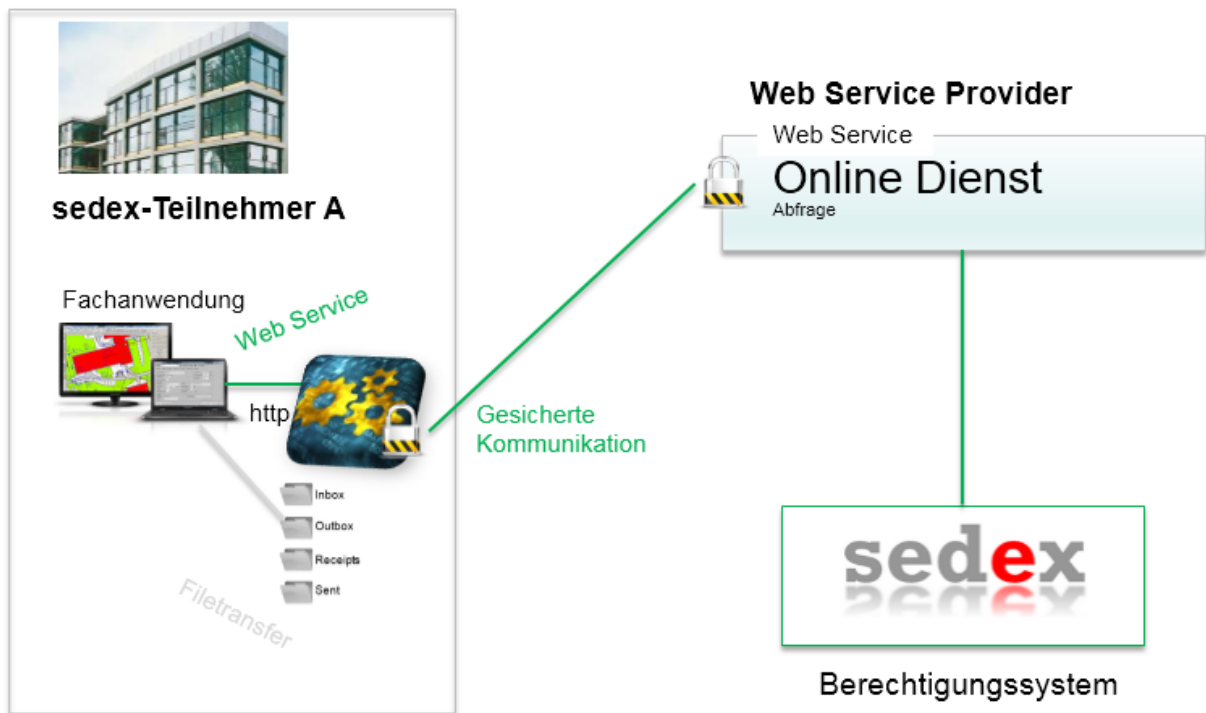


Abbildung 7: Konzept synchrone Kommunikation

Der Web-Service Provider kann einen sedex-Client einsetzen muss aber nicht. Für die Berechtigungen der sedex-Teilnehmer kann der Web Service Provider auf das Berechtigungssystem von sedex zurückgreifen. Dadurch kann dieser die Benutzerverwaltung vereinfachen oder gar ganz weglassen. Das Berechtigungssystem steht ebenfalls als Web Service im sedex-Client zur Verfügung.

2.2.2 Ablauf Datenaustausch

Konsument und Provider sind technisch vollständig voneinander entkoppelt. Die Kommunikation zwischen ihnen erfolgt via sedex-Client des Web Service Konsumenten.

Die konsumierende Anwendung eröffnet einen SOAP Request (REST ist in Planung) mit der gewünschten Methode. Der WS-Proxy des sedex-Client spiegelt den Web-Service des Web-Service Providers im lokalen Netz wieder. Pro Web-Service steht eine eindeutige URL zur Verfügung. Die konsumierende Fachanwendung kann so alle angebotenen Web-Services einheitlich einbinden.

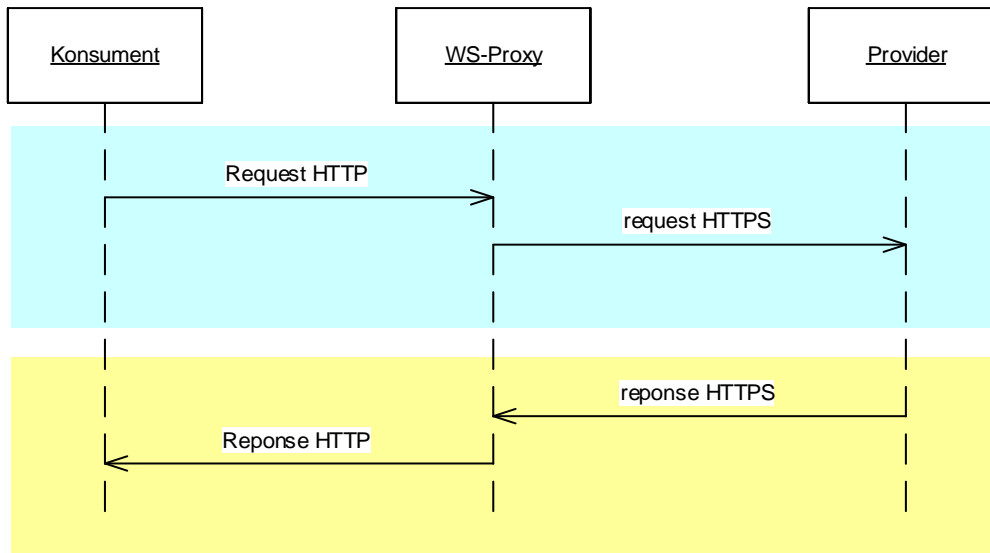


Abbildung 8: Ablauf Datenaustausch

2.3 physischer sedex-Teilnehmer

Ein physischer Teilnehmer entspricht einer Installation des sedex-Client auf einem Rechner mit entsprechender sedex-ID. In nachfolgender Abbildung sind die sedex-Teilnehmer 1 und 2 physische Teilnehmer.

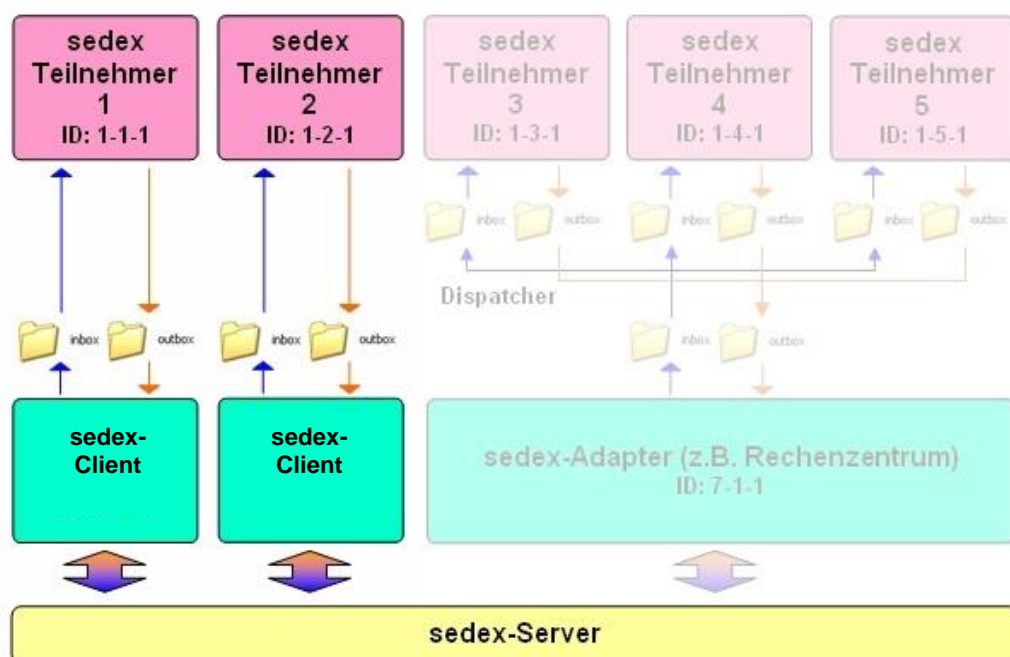


Abbildung 9: Beispiel mit physischen Teilnehmern

Diese Anschlussart empfiehlt sich insbesondere dann, wenn der anzuschliessende Teilnehmer eine grosse Menge an sedex-Meldungen austauscht, und wenn die Datenschutzanforderungen hoch sind.

2.4 logischer sedex-Teilnehmer

Eine Installation des sedex-Client ermöglicht mehrere Teilnehmer zu bedienen. Diese Möglichkeit wurde insbesondere für den Betrieb in Rechenzentren geschaffen. Hierzu wurden sogenannte logische sedex-Teilnehmer geschaffen.

Die logischen sedex-Teilnehmer teilen sich eine gemeinsame In- und Outbox und das elektronische Zertifikat.

Der übergeordnete physische sedex-Teilnehmer fungiert als Router und ist nicht direkt adressierbar.

Dies macht es erforderlich, dass der Betreiber des sedex-Client eine Feinverteilung der Meldungen sicherstellt. Diese Aufgabe wird in der Regel von einem Programm (Dispatcher) wahrgenommen. Der Betreiber des sedex-Client haftet für den Datenschutz zwischen den logischen Teilnehmern und ergreift angemessene Massnahmen.

Die Art des Anschlusses eines Teilnehmers hat keinen Einfluss auf die Adressierung von Meldungen: Ein sendender Teilnehmer muss nicht wissen, ob es sich beim Empfänger um einen physischen oder logischen Teilnehmer handelt.

Die sedex-Teilnehmer 3, 4 und 5 in nachfolgender Abbildung sind logische Teilnehmer. Die Pfeile zwischen den sedex-Teilnehmern und dem Adapter stellen den Dispatcher dar.

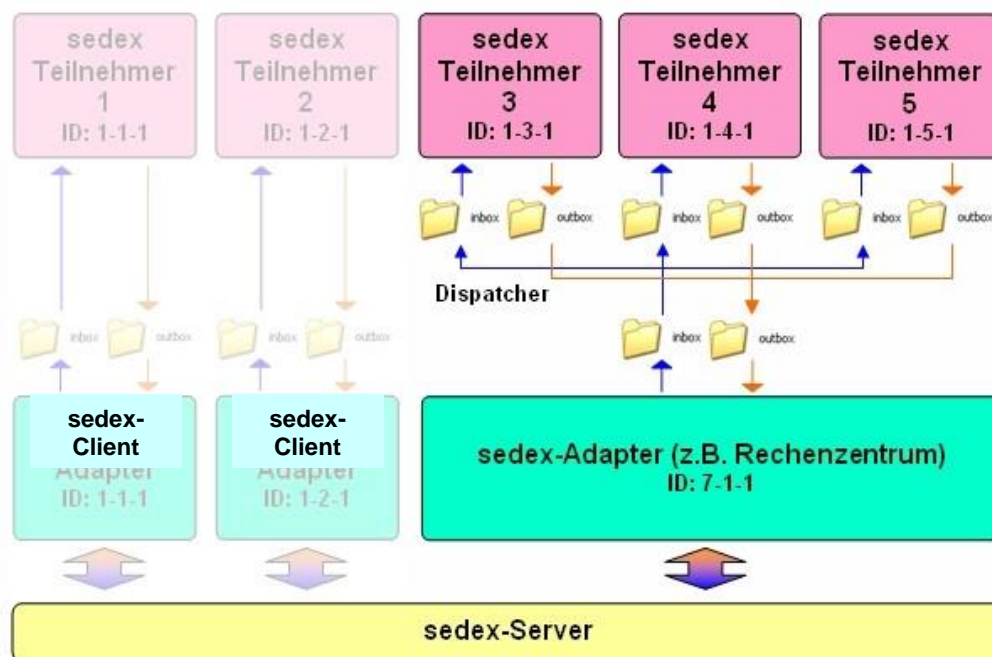


Abbildung 10: Beispiel mit logischen Teilnehmern

Der Dispatcher ist vergleichbar mit der internen Hauspost. Sowohl das BFS als auch das BIT bieten keinen solchen Dispatcher an. In Zusammenarbeit mit Partnern wurden solche Werkzeuge geschaffen. Bei Interesse geben wir Ihnen gerne Auskunft.

3 Integration des sedex-Client (asynchron)

Nachfolgend sind die wesentlichen Elemente beschrieben, um den sedex-Client entweder in eine bestehende Infrastruktur zu integrieren oder einer Fachanwendung zu ermöglichen, via sedex mit einer anderen Fachanwendung Meldungen auszutauschen.

3.1 Funktionsweise

Versand einer Meldung

Um Fehlverhalten zu vermeiden, ist darauf zu achten, dass zunächst die Nutzdatendatei und erst danach die Umschlagsdatei in der Outbox erstellt werden.

Beim Versand einer Meldung arbeitet der sedex-Client die folgende Reihenfolge ab:

1. Der Adapter überwacht die Outbox in Intervallen (Polling). Sobald der Adapter den Umschlag erkannt hat, wird die Meldung verarbeitet. Der Adapter validiert den Umschlag anhand des XML-Schemas und speichert die Meldung im Verzeichnis `sedextempmessage`.
2. Verbindung mit dem sedex-Server, zur Kontrolle der Daten der Teilnehmer (aktive Teilnehmer, Zertifikat, Autorisierung usw.).
3. Die Dateien der Meldung werden für den Versand in ein temporäres Verzeichnis verschoben und gegebenenfalls in Segmente zerlegt (Meldung > 5 MB).
4. Die Meldung wird vom sedex-Client signiert, mit dem Zertifikat des Empfängers verschlüsselt und an den sedex-Server übermittelt.
5. Die Dateien der Meldung werden ins Verzeichnis *processed* verschoben, unabhängig davon, ob der Versand erfolgreich war.
6. Sobald der Empfänger die Meldung heruntergeladen hat, erzeugt der Adapter eine technische Quittung pro Empfänger mit dem Versandstatus. Diese Quittung wird der sendenden Anwendung über das Verzeichnis *receipts* zur Verfügung gestellt.

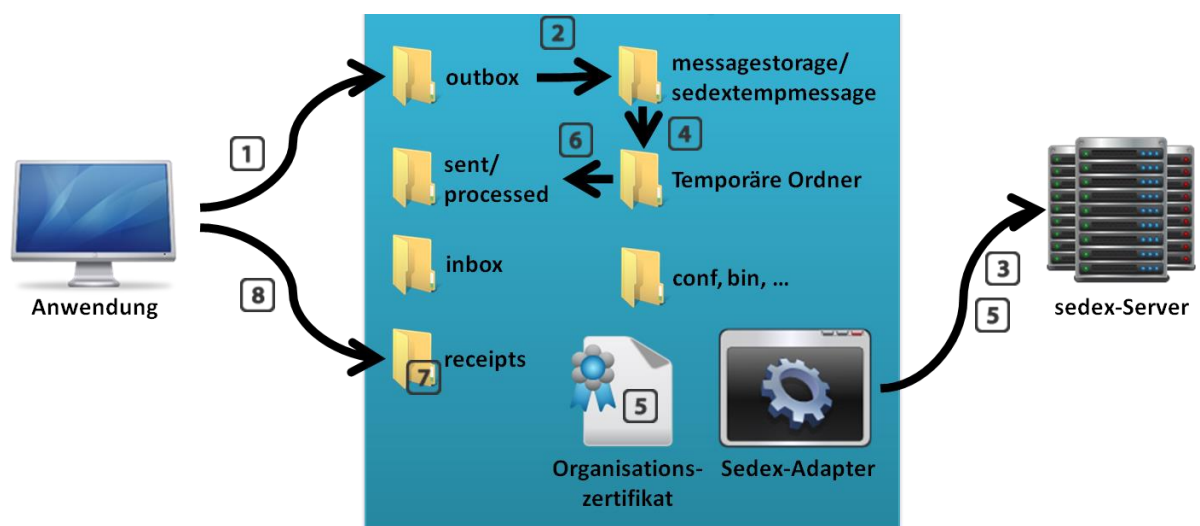


Abbildung 11: Sendeprozess

Empfangen einer Meldung

Beim Empfang einer Meldung arbeitet der sedex-Client die folgende Reihenfolge ab:

- 1) Der sedex-Client verbindet sich mit dem sedex-Server (Polling), prüft das Postfach auf dem sedex-Server und lädt alle bereitliegenden Meldungen herunter.
- 2) Teilweiser Download der Meldung ins temporäre Verzeichnis.
- 3) Sicherheitskontrollen (Signatur, Verschlüsselung, Autorisierung).
- 4) Fortsetzung des Downloads ins temporäre Verzeichnis.
- 5) Sobald die Datei entschlüsselt ist, wird sie in den Inbox-Ordner verschoben.
- 6) Der Status der Meldung wird auf dem Server aktualisiert und eine technische Quittung wird an den Sender geschickt.

3.1.1 Dateischnittstelle

Die Fachanwendung legt die zu versendenden Meldungen als Dateien im Verzeichnis „Outbox“ bereit und kann die empfangenen Meldungen als Datei aus dem Verzeichnis „Inbox“ lesen.

Versandquittungen («technische Quittungen») des Systems werden ebenfalls in Form von Dateien bereitgestellt. Die Versandquittungen werden in das Verzeichnis „Receipts“ gestellt.

Eine Meldung besteht immer aus zwei Dateien:

Umschlagsdatei

Die Umschlagsdatei ist ein XML-Dokument, welches dem XML-Schema eCH-0090.xsd entspricht und ein Element /eCH-0090:envelope enthält. Der sedex-Client prüft den Inhalt des Umschlags auf syntaktische (d.h. XML-Schema) und semantische Korrektheit (z.B. korrekte Adressen). Für den Umschlag kann nur die Version 1.0 des XML-Schemas eCH-0090 verwendet werden.

Nutzdatendatei

Die Nutzdatendatei kann Daten beliebigen Typs enthalten. Der sedex-Client nimmt keine Prüfung des Inhalts der Nutzdatendatei vor. Es ist Aufgabe des Senders bzw. des Empfängers, die Korrektheit des Inhaltes zu prüfen. Möchte eine Anwendung in einer einzelnen Meldung mehrere Dateien transportieren, so kann sie diese in einer Zip-Datei oder einem anderen Datencontainer zusammenfassen. Welcher Art der Container ist, ist zwischen den Anwendungen zu vereinbaren, die Daten austauschen. Die Quittung bezieht sich immer auf die Meldung.

Eine *Versandquittung* (oder kurz „Quittung“) ist ein XML-Dokument, welches dem XML-Schema eCH-0090-1-0.xsd bzw. eCH-0090-2-0.xsd entspricht und ein Element /eCH-0090:receipt enthält. Die Versandquittung gibt darüber Auskunft, ob eine Meldung beim sedex-Client des Empfängers angekommen ist bzw. ob allenfalls ein Übermittlungsfehler aufgetreten ist. Die Quittung ist keine Bestätigung dafür, dass der Empfänger die Meldung auch verarbeitet hat. Zu diesem Zweck müssen die Anwendungen eigene fachliche Quittungen vereinbaren.

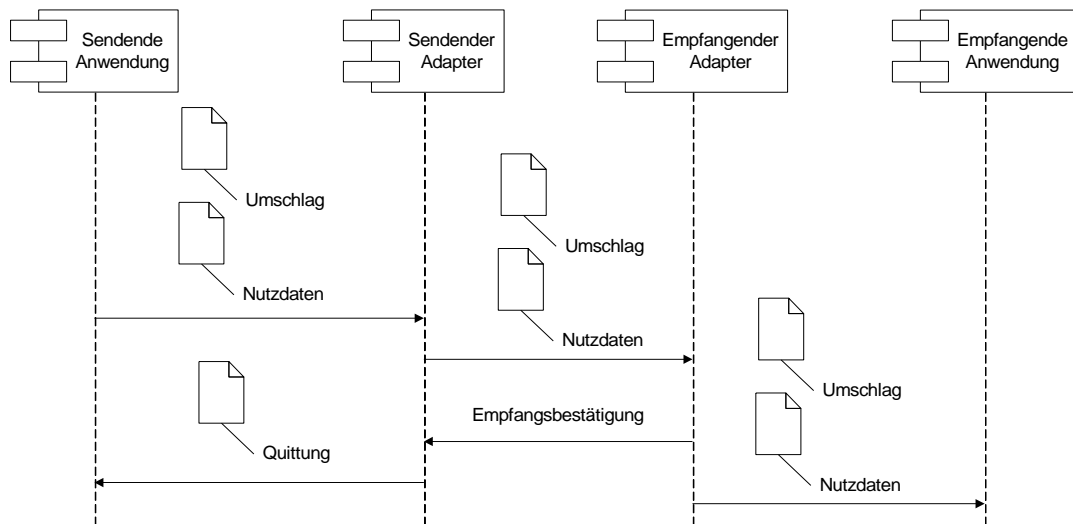


Abbildung 12: Ablauf des Versands

Namenskonvention

Um die Nutzdatei und den Umschlag zusammen zu führen, wurde die folgende Namenskonvention getroffen:

- Der Umschlag als Datei envl_N.xml
- Die Nutzdaten als Datei data_N.xxx

«N» ist ein von der Anwendung erzeugtes eindeutiges Attribut. Zum Beispiel bilden die Dateien «envl_4711.xml» und «data_4711.zip» eine Meldung. Es können beliebige Namensuffixe vergeben werden. Die Namen der Dateien haben für den sedex-Client ansonsten keinerlei Bedeutung. Wir empfehlen, als Namenssuffix die messageld aus dem Umschlag zu nutzen.

«xxx» bezeichnet eine beliebige Dateierweiterung (Extension), welche den Dateityp (XML, ZIP, PDF, usw.) bezeichnet.

Der sendende sedex-Client stellt die Versandquittung als Datei mit Namen «receipt_ID_M_Y.xml» im Quittungsverzeichnis bereit. «M» ist die messageld und «Y» ist eine vom sedex-Client vergebene eindeutige Sequenznummer.

Der empfangende sedex-Client erstellt die folgenden Dateien:

- die Nutzdaten als Datei «data_M.xxx»
- der Umschlag als Datei «envl_M.xml»

Bei «M» handelt es sich um einen vom empfangenden sedex-Client erzeugten, eindeutigen alphanumerischen Code. Die Dateinamen bleiben beim Transport **nicht erhalten**. Einzig die Dateierweiterung (Dateityp) der Nutzdaten bleibt unverändert. Wird die Erhaltung eines bestimmten Dateinamens benötigt, kann die Originaldatei in eine Zip-Datei verpackt und versendet werden.

3.1.2 Adressierung

Alle sedex-Teilnehmer sind durch eine eindeutige ID gekennzeichnet. Die aktuelle Liste finden Sie auf unserer Website www.sedex.ch / synchron.

Bis Ende 2014 wurden die IDs der Teilnehmer nach verschiedenen Kriterien strukturiert und zahlreiche Nummernbereiche waren reserviert. Dadurch erschwerte sich jedoch die Handhabung merklich, insbesondere bei Zentralisierungsprojekten oder Splittungen, sodass seit dem

01.01.2015 der Prozess zur Vergabe der Teilnehmer-ID für unsere Kunden vereinfacht wurde. Neue IDs werden seitdem zufällig vergeben und sind nicht sprechend.

Bestehende sedex-IDs werden nicht umbenannt.

Um den Fusionsprozess zu unterstützen, bleiben einige Bereiche von obiger Regelung ausgenommen:

Bereich		Bedeutung	Wertebereich für die Organisationseinheit
1		Bezeichnet eine Gemeinde	<p>Zulässige Werte sind die BFS-Nummern der politischen Gemeinden, z.B. 351 für Bern.</p> <p>Beispiel Stadt Bern: 1-351-1</p> <p>Bei jedem weiteren adressierbaren Teilnehmer derselben Gemeinde wird die letzte Nummer inkrementell erhöht.</p> <p>Beispiel: 1-351-2, 1-351-3, 1-351-4,</p>
4		Neue vergebene sedex-Teilnehmer	<p>4-xxxxxx-x</p> <p>Beispiel : 4-143281-9</p>
6		<p>Sozialversicherungsunternehmen</p> <p>Bezeichnet eine AHV-Ausgleichskasse oder eine IV-Stelle.</p>	<p>Vom Bundesamt für Sozialversicherung (BSV) an Ausgleichskassen/Zweigstellen, IV-Stellen, EL-Stellen, Militär und Mitinteressierte vergebene 6-stellige Nummer.</p> <p>Beispiel Ausgleichskasse Uri: 6-148281-2</p>
T		Bezeichnet einen Test-Teilnehmer.	<p>Die ID wird mit einem Präfix «T» versehen. Testteilnehmer können ausschliesslich untereinander kommunizieren, nicht aber mit produktiven Teilnehmern.</p> <p>Beispiel Stadt Bern: T1-351-1</p> <p>Beispiel Ausgleichskasse Uri: T6-148281-2</p>
9		Reserviert für Teilbusse	<p>Dieser Bereich steht Teilbussen zur Bewirtschaftung ihrer internen Teilnehmer zur Verfügung. Bei sedex sind diese nicht registriert. Diese Teilnehmer können nur im internen Teilbus erreicht werden. Eine Kommunikation via sedex ist nicht möglich.</p> <p>Es ist zu beachten: In diesem Nummernbereich existieren bereits wenige sedex-Teilnehmer. Es werden jedoch von sedex keine neuen sedex-IDs vergeben.</p>

3.1.3 Meldungstypen

Alle Meldungen sind durch einen eindeutigen Meldungstyp gekennzeichnet. Die aktuelle Liste entnehmen Sie bitte unserer Website www.sedex.ch / synchron.

Definition sedex-Meldungstyp: Jede Domäne definiert ihre eigenen sedex-Meldungstypen. Ein Meldungstyp entspricht einem Geschäftsfall, der zwischen den sedex-Teilnehmern abgewickelt wird. Jede sedex-Meldung wird einem Meldungstyp zugeordnet. Dies erfolgt durch den Eintrag der entsprechenden Nummer im sedex-Umschlag (Couvert), auch „envelope“ genannt.

Jeder sedex-Teilnehmer ist für bestimmte Meldungstypen autorisiert. Eine Meldung kann zwischen zwei Teilnehmern ausgetauscht werden, wenn der Sender und der Empfänger für den jeweiligen Meldungstyp autorisiert sind. Welche dies sind, bestimmt der jeweilige Domänenvertreter (Owner des Meldungstyps).

Bis Ende 2014 wurden die IDs der Teilnehmer nach verschiedenen Kriterien strukturiert und zahlreiche Nummernbereiche waren reserviert. Dadurch erschwerte sich jedoch die Handhabung merklich, sodass seit dem 01.01.2015 der Prozess zur Vergabe der Teilnehmer-ID für unsere Kunden vereinfacht wurde. Neue Nummern werden seither, beginnend bei 1000, fortlaufend nummeriert und sind nicht sprechend.

3.1.4 Polling

Der sedex-Client fragt den sedex-Server periodisch an, ob Meldungen zum Download bereitstehen. Diesen Vorgang nennt man Polling. Die Dauer zwischen zwei Verbindungen wird mit dem Polling-Intervall festgelegt. Um den Meldungs austausch weiter zu beschleunigen, wurde die Möglichkeit für eine Web-Socket-Verbindung geschaffen. Ob diese etabliert werden kann, hängt von den Regeln der Netzwerkkomponenten ab.

Web-Socket	Zeitraum	Polling-Intervall
nicht etabliert	07:00 – 18:59	5 Minuten
	19:00 – 06:59	15 Minuten
etabliert		ohne Verzögerung

Anmerkung: Das Intervall zwischen zwei Abfragen ist auf die Gesamtheit der Anwender und auf eine optimale Leistung des sedex-Servers abgestimmt. Nehmen Sie bitte vor einer Änderung Kontakt mit dem sedex-Support auf.

3.1.5 Retry

Verbindungsfehler (z.B. Netzwerkfehler) sind in der Regel temporäre Fehler. Tritt ein solcher Fehler auf, wird der sedex-Client für die Dauer der konfigurierten Retry-Periode (Default 12 Stunden) wiederholt versuchen, die Meldung zu versenden. Erst nach Ablauf dieser Periode wird er eine Versandquittung mit Fehlerstatus dem Absender erstellt.

3.2 sedex-Umschlag

Der Umschlag einer sedex-Meldung enthält gemäss XML-Schema eCH-0090 die folgenden Elemente:

Element-Name	Bedeutung	Typ	Anzahl
messageld [zwingend]	Sendende Anwendung Diese ID wird von der sendenden Anwendung vergeben. Die messageld muss eindeutig sein. Sie dient dazu, eine Meldung und eine Antwort zu korrelieren. Wenn sich mehrere Anwendungen denselben sedex-Client teilen, muss die Vergabe der messageld zwischen den Anwendungen per Konvention geregelt werden. Hinweis: Es kann die UUID (vgl. RFC 4122) eingesetzt werden.	([a-zA-Z] [0-9] -){1,36} max. 36 Zeichen, kann Ziffern Buchstaben oder Bindestriche enthalten. Bsp: f81d4fae-7dec-11d0-a765-00a0c91e6bf6	1
messageType [zwingend]	Der Meldungstyp entspricht der Use Case Funktion der Meldung. Der Meldungstyp ist zusammen mit der senderId und der recipientId für das Routing der Meldung relevant.	[0 .. 26999999] (Teilmenge von xs:int)	1
messageClass [zwingend]	Die Meldungsklasse definiert innerhalb eines Meldungstyps die Bedeutung der Meldung. Die folgenden Werte sind vordefiniert: <ul style="list-style-type: none"> • 0 = Message. Kennzeichnung der initialen Meldung. • 1 = Response. Kennzeichnet die Antwort auf eine Meldung. • 2 = Receipt. Kennzeichnet eine applikatorische Quittung (Empfangsbestätigung. Eine solche Quittung wird ggf. geschickt, wenn bis zur Lieferung einer Antwort ein längerer Zeitraum vergehen kann oder wenn der Empfänger gar keine Antwort senden wird. • 3 = Error. Information von einer empfangenden an die sendende Anwendung, dass ihre Meldung nicht verarbeitet werden konnte. • 4-9 + 11 - maxint: reserviert. 	xs:int	1

Element-Name	Bedeutung	Typ	Anzahl
referencemessageld [fakultativ]	Dieses Element wird gesetzt, wenn eine Antwort oder eine Fehlermeldung erfolgt. Das Element enthält die ID der ursprünglich gesendeten Meldung. Muss gesetzt werden, wenn messageClass = 1 (Response), = 2 (Receipt) oder = 3 (Error) ist.	gleich wie messageld	1
senderId [zwingend]	Bezeichnet den sedex-Teilnehmer, der die Meldung gesendet hat.	String	1
recipientId [zwingend]	Bezeichnet den sedex-Teilnehmer, der die Meldung erhalten soll.	String	>0
eventDate [zwingend]	Datum an dem das Ereignis, auf welches sich die Nutzdaten beziehen, geschah.	xsd:dateTime	1
messageDate [zwingend]	Datum (Zeitstempel), wann die Meldung in die Inbox geschrieben wurde.	xsd:dateTime	1
Loopback [fakultativ]	Mit Loopback kann geprüft werden, ob der adressierte sedex-Teilnehmer die Meldung empfangen könnte. Der sendende sedex-Client verarbeitet die Meldung, der adressierte Empfänger erhält aber nichts. «true» die Autorisierungen (Meldungstyp, Zertifikat) werden geprüft «false» die Erreichbarkeit des Empfängers wird geprüft. Vergleichbar mit dem DOS Befehl ping.	Attribut 'authorise' «true» / «false»	0,1
testData [fakultativ]	Dieses XML-Element erlaubt, eine unbeschränkte Anzahl Testparameter mit beliebigen Ausprägungen mitzugeben. Die Parameter und ihre möglichen Ausprägungen müssen vom Fachbereichs-Koordinator definiert werden.	Namen/Werte Paar	>=0

Alle Zeitangaben in XML-Dokumenten (XML-Schema-Datentypen xs:datetime und xs:time) müssen Angaben über die Zeitzone enthalten, also entweder in der Form «hh:mm:ssZ» oder in der Form «hh:mm:ss(+|-)hh:mm» vorliegen. Fehlt die Angabe der Zeitzone, so sind die Zeitangaben nicht vollständig determiniert.

Beispiel eines Umschlags (XML-Dokument):

```
<?xml version="1.0" encoding="UTF-8"?>
<envelope xmlns="http://www.ech.ch/xmlns/eCH-0090/1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ech.ch/xmlns/eCH-0090/1 http://www.ech.ch/xmlns/eCH-
0090/1/eCH-0090-1-0.xsd"
  version="1.0">
  <messageId>62fdee70d9ea77646f6e8686a3f9332e</messageId>
  <messageType>99</messageType>
  <messageClass>0</messageClass>
  <senderId>1-351-1</senderId>
  <recipientId>3-CH-1</recipientId>
  <eventDate>2007-01-01T00:00:00</eventDate>
  <messageDate>2007-09-06T14:13:51</messageDate>
</envelope>
```

3.2.1 Umschlag - Schema invalid

Übergibt die sendende Anwendung dem sedex-Client einen nicht schemavaliden Umschlag (eCH-0090), so ist der sedex-Client unter Umständen nicht in der Lage, darin enthaltene Informationen über Absender, Empfänger etc. zu extrahieren. Der sedex-Client wird in diesem Fall eine Versandquittung ausstellen, die nachstehende Werte enthält.

Wann immer möglich, wird der sedex-Client versuchen, die *messageId* zu erkennen. Ist dies nicht möglich, wird der Filename der Umschlagsdatei im Element «statusInfo» mitgeliefert.

Die Quittung für einen Status «200» enthält folgende Elemente:

Elementname	Wert	Bedingung
eventDate	Aktuelles Datum/Zeit	
statusCode	200	
statusInfo	Invalid envelope syntax	messageId <> 0
	Invalid envelope syntax found in file %f	messageId = 0
messageId	0	messageId in envelope nicht gefunden
	<> 0	messageId in envelope gefunden
messageType	0	
messageClass	0	
senderId	0-sedex-0	
recipientId	0-sedex-0	

3.2.2 Messageld - Dubletten

Der sedex-Client garantiert die Eindeutigkeit der *messageld*. Er speichert die mit dem sedex-Umschlag verbundenen Informationen bis zur Ankunft der Meldung. Bis dahin wird jede weitere Nachricht mit derselben *messageld* mit dem Fehlercode 201 quittiert.

Wir empfehlen nur eindeutige *messagelds* einzusetzen.

3.2.3 Meldung - Verfalldatum

Meldungen müssen innerhalb von 30 Tagen dem adressierten sedex-Client übermittelt werden können. Massgebend ist das Element */eCH-0090:envelope/messageDate*, unabhängig davon, ob dieses dem tatsächlichen Zeitpunkt des Versands entspricht bzw. entsprochen hat. Nach Ablauf des „*messageDates*“ wird die Meldung auf dem sedex-Server vernichtet.

sedex nimmt folgende Validierungen vor:

- Beim Versand der Meldung: *messageDate* darf nicht kleiner als der aktuelle Zeitpunkt minus 30 Tage sein → Statuscode «203 Message too old to send» an sendenden sedex-Client.
- Auf dem Server: *messageDate* gleich aktueller Zeitpunkt minus 23 Tage → Statuscode «701 Message expires soon» an sendenden sedex-Client.
- Auf dem Server: *messageDate* gleich aktueller Zeitpunkt minus 30 Tage → Statuscode «204 message expired» an sendenden sedex-Client.

Der Statuscode «701» ist als Warnung an den Sender zu verstehen. Allenfalls kann beim Empfänger interveniert werden.

Erhält der Sender nach dem Versand den Statuscode «204» (anstelle «100»), kann die Meldung vom Empfänger endgültig nicht mehr heruntergeladen werden.

3.3 sedex-Quittung

Jede Meldung wird quittiert. Die Quittung enthält die folgenden Elemente:

Element-Name	Bedeutung	Typ	Anzahl
<i>eventDate</i> [zwingend]	Zeitpunkt, wann die Meldung beim empfangenden sedex-Client angekommen ist, oder wann der Übermittlungsfehler aufgetreten ist.	xsd:dateTime	1
<i>statusCode</i> [zwingend]	Status der Meldung.	Aufzählung auf Basis von xsd:in OK oder Fehlercode	1
<i>statusInfo</i> [zwingend]	Infotext zum Statuscode. Enthält allfällige weitere Informationen.	xsd:string, maxlength=255	1
<i>messageld</i> [zwingend]	ID der Meldung, auf die sich die Quittung bezieht.	gleich wie im Umschlag	1
<i>messageType</i> [zwingend]	Meldetyp der Meldung, auf den sich die Quittung bezieht.	gleich wie im Umschlag	1
<i>messageClass</i> [zwingend]	Meldungsklasse der Meldung, auf die sich die Quittung bezieht.	gleich wie im Umschlag	1
<i>senderId</i> [zwingend]	Absender der Meldung, auf den sich die Quittung bezieht.	gleich wie im Umschlag	1

Element-Name	Bedeutung	Typ	Anzahl
recipientId [zwingend]	Empfänger der Meldung, auf den sich die Quittung bezieht. Im Falle einer Routing-Regel (z.B. Weiterleitung an eine kantonale Plattform) wird dennoch der Original Empfänger ausgegeben.	gleich wie im Umschlag	1

Das folgende XML-Dokument zeigt ein Beispiel einer Quittung als „Antwort“ auf vorhergehendes Beispiel einer Meldung:

```
<?xml version="1.0" encoding="UTF-8"?>
<receipt xmlns="http://www.ech.ch/xmlns/eCH-0090/2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ech.ch/xmlns/eCH-0090/2 http://www.ech.ch/xmlns/eCH-0090/1/eCH-0090-2-0.xsd"
  version="2.0">
  <eventDate>2008-10-16T14:13:51Z</eventDate>
  <statusCode>100</statusCode>
  <statusInfo>Message correct transmitted</statusInfo>
  <messageId>62fdee70d9ea77646f6e8686a3f9332e</messageId>
  <messageType>94</messageType>
  <messageClass>0</messageClass>
  <senderId>1-351-1</senderId>
  <recipientId>3-CH-1</recipientId>
</receipt>
```

3.3.1 Fehlerkategorien

Die verschiedenen Statuscodes werden in Kategorien und Subkategorien gegliedert. Die Kategorien sind so aufgebaut, dass die aufrufende Applikation bereits anhand der Kategorie eines Codes entscheiden kann, wie sie grundsätzlich reagieren soll. Beispielsweise kann bei einem Statuscode der Kategorie *temporärer Fehler* nach einer gewissen Zeit ein erneuter Sendeversuch gestartet werden.

Typ	Beschreibung	Bereich	Hinweis
Permanenter Fehler	Message Error Bsp: Der Umschlag einer Nachricht ist ungültig.	200 - 299	Ein Problem mit der Meldung oder der Autorisierung liegt vor. Ein erneuter Sendeversuch, ohne Veränderung der Gegebenheiten, wird denselben Fehler auslösen.
	Authorisation Error Bsp: Ein Empfänger aus dem envelope ist nicht autorisiert.	300 - 399	
Temporärer Fehler	Transport Error Bsp: Der Autorisierungsserver steht momentan nicht zur Verfügung.	400 - 499	Auf der Transportebene oder bei den Adaptern ist ein Problem aufgetreten. Verhalten: Meldung nach einer Wartezeit nochmals senden.
	Adapter Error Bsp: Dem sedex-Client steht nicht genügend Speicherplatz zur Verfügung.	500 - 599	

Information	Update Bsp: Eine Meldung wurde erfolgreich an den Server versendet.	600 - 699	Zu einer versendeten Meldung liegen Fortschrittsinformationen vor, die Meldung ist jedoch noch nicht erfolgreich zugestellt. Verhalten: Die Information kann ausgewertet oder ignoriert werden.
	Warning Bsp: Der Empfänger hat nur noch wenige Tage Zeit, um die Meldung herunterzuladen.	700 - 799	Zu einer versendeten Meldung liegt eine Warnung vor. Verhalten: Die Warnung kann ausgewertet oder ignoriert werden.

3.3.2 Statuscode

Die folgenden Statuscodes sind für die Quittung definiert:

Sub-kategorie	Wert	zugehörige Meldung	Bedeutung	Quelle ¹
Success	100	Message correct transmitted	Meldung ist korrekt und vollständig übermittelt worden.	EA
Message Error	200	Invalid envelope syntax	Der Umschlag entspricht nicht dem erwarteten XML-Schema für Umschläge bzw. liegt in einer nicht erwarteten Version vor.	SA EA
	201	Duplicate messageld	Der Umschlag enthält eine Meldungslid, die der Adapter in seiner Status-Datenbank schon führt.	SA
	202	No payload found	Eine sedex-Meldung besteht immer aus zwei Dateien: Umschlag und Nutzdaten. Die sendende Anwendung hat nur einen Umschlag, aber keine Nutzdaten bereitgestellt.	SA
	203	Message too old to send	essageDate im Umschlag ist älter als 30 Tage.	SA
	204	Message expired	Der Empfänger hat die Meldung nicht innerhalb des von sedex geforderten Zeitraums von einem Monat abgeholt.	SA
Autorisation Error	300	Unknown senderId %s	Die im Umschlag angegebene senderId ist im sedex-TV nicht bekannt.	SA
	301	Unknown recipientId %s	Die im Umschlag angegebene recipientId ist im sedex-TV nicht bekannt.	SA
	302	Unknown physical senderId %s	Die im Adapter konfigurierte ID des Adapters ist im sedex-TV nicht bekannt (kann nur bei zentralisierten Infrastrukturen auftreten).	SA
	303	Invalid message Type %s	Der im Umschlag aufgeführte Meldungstyp ist nicht bekannt.	SA
	304	Invalid message Class %s	Die im Umschlag aufgeführte Meldungsklasse ist nicht bekannt.	SA
	310	Not allowed to send	Dieser Absender darf diese Meldung nicht senden.	SA

¹ Als Quelle wird der Adapter bezeichnet. SA = sendender Adapter, EA = empfangender Adapter

Sub-kategorie	Wert	zugehörige Meldung	Bedeutung	Quelle ¹
	311	Not allowed to receive	Dieser Empfänger darf diese Meldung nicht empfangen. Kann auch auftreten, wenn nach Versand, aber vor Empfang durch EA, Routing oder Autorisierung des Empfängers geändert wurde.	SA EA
	312	User certificate not valid	Das Zertifikat des Teilnehmers ist entweder annulliert worden oder es ist ungültig.	SA
	313	Other recipients are not allowed to receive	Die Meldung kann nicht an den Empfänger gesendet werden, da andere Empfänger im selben Umschlag nicht autorisiert sind.	SA
	320	<i>Message expired</i>	<i>Ab Adapter-Version 2.0 durch 204 ersetzt. Bedeutung siehe dort.</i>	SA
	330	Message size exceeds limit	Die Meldung überschreitet für diesen messageType die erlaubte Grösse.	SA
Transport Error	400	Network error	Allgemeines Netzwerkproblem	SA
	401	OSCI hub not reachable	Keine Verbindung zum OSCI-Intermediär möglich.	SA
	402	Directory not reachable	Die sedex-Liste ist nicht erreichbar.	SA
	403	Logging service not reachable	Das sedex-Logging ist nicht erreichbar.	SA
	404	Authorisation service not reachable	Der Autorisierungsservice von sedex ist nicht verfügbar.	SA
Adapter Error	500	Internal error: „Text“	Der sedex-Client kann die Daten nicht senden, weil ein interner Fehler aufgetreten ist. Details zum Fehler sind dem Log des Adapters zu entnehmen.	SA
	501	Error during receiving	Beim Empfangen der Meldung ist ein Fehler aufgetreten, der Empfänger konnte die Meldung nicht rekonstruieren.	EA
Partial Success	601	Message sucessfully sent	Die Meldung wurde erfolgreich dem Intermediär übergeben.	SA
Warning	701	Message expires soon	Der empfangende Adapter hat nur noch 7 Tage Zeit, die Meldung vom Intermediär herunterzuladen.	SA

3.4 Monitoring

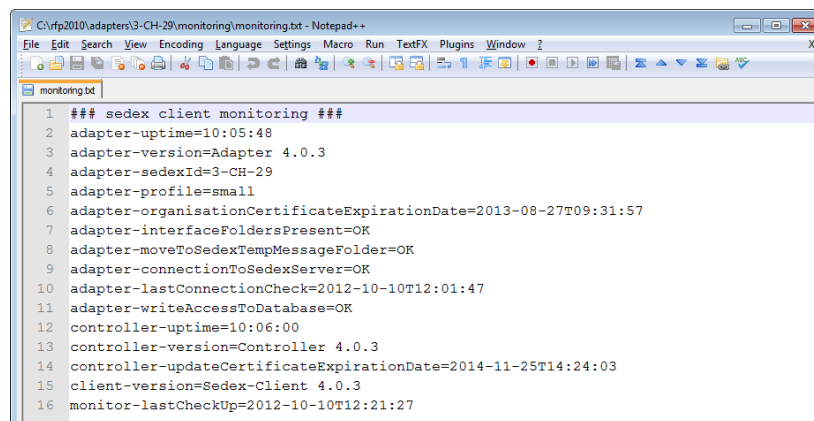
Das Monitoring des sedex-Clients erlaubt die folgenden Aspekte:

- Version des Adapters
- Version des WS-Proxy
- Version des Controllers
- sedex-ID der Installation
- Konfiguriertes Profil des Adapters
- Verfallsdatum des Organisationszertifikats
- Verfallsdatum des Update-Zertifikats

- Konfiguration der Schnittstellenordner
- Verbindung mit dem sedex-Sever
- Version von jedem AAR-Archiv
- Version des Truststores des WS-Proxy
- Betriebsdauer des Adapters
- Betriebsdauer des WS-Proxy
- Betriebsdauer des Controllers
- Hash-Werte des Installationsverzeichnisses sowie des Rechners

3.4.1 Textdatei

Die Monitoring-Datei wird in 5-Minuten-Intervallen vom sedex-Controller generiert. Es ist eine Datei im Textformat, welche die oben aufgeführten Informationen umfasst. Die Datei monitoring.txt befindet sich im Verzeichnis „Monitoring“.



```

1  ### sedex client monitoring ###
2  adapter-uptime=10:05:48
3  adapter-version=Adapter 4.0.3
4  adapter-sedexId=3-CH-29
5  adapter-profile=small
6  adapter-organisationCertificateExpirationDate=2013-08-27T09:31:57
7  adapter-interfaceFoldersPresent=OK
8  adapter-moveToSedexTempMessageFolder=OK
9  adapter-connectionToSedexServer=OK
10 adapter-lastConnectionCheck=2012-10-10T12:01:47
11 adapter-writeAccessToDatabase=OK
12 controller-uptime=10:06:00
13 controller-version=Controller 4.0.3
14 controller-updateCertificateExpirationDate=2014-11-25T14:24:03
15 client-version=Sedex-Client 4.0.3
16 monitor-lastCheckUp=2012-10-10T12:21:27

```

Abbildung 13: Ansicht der Monitoring-Datei

In der Standardeinstellung ist die Erzeugung der Monitoring-Datei aktiviert. Es ist möglich, das Monitoring zu deaktivieren oder auch den Speicherort der Datei und das Überprüfungsintervall mithilfe der entsprechenden Parameter in der Konfigurationsdatei des sedex-Client festzulegen.

3.4.2 HTTP

Über den http-Aufruf kann eine Verbindung mit dem http-Service hergestellt werden, der vom sedex-Controller über den Port 8000 bereitgestellt wird. Die Antwort erfolgt im Textformat und umfasst die oben aufgeführten Informationen. Zur Verwendung des HTTP-Aufrufs muss folgende URL verwendet werden:

http://[host]:[port]/monitoring (z.B. <http://localhost:8000/monitoring>).

In der Standardeinstellung ist der HTTP-Server des Monitorings aktiviert. Es ist möglich, das Monitoring zu deaktivieren oder auch den Port und das Überprüfungsintervall mithilfe der entsprechenden Parameter in der Konfigurationsdatei des sedex-Client festzulegen.

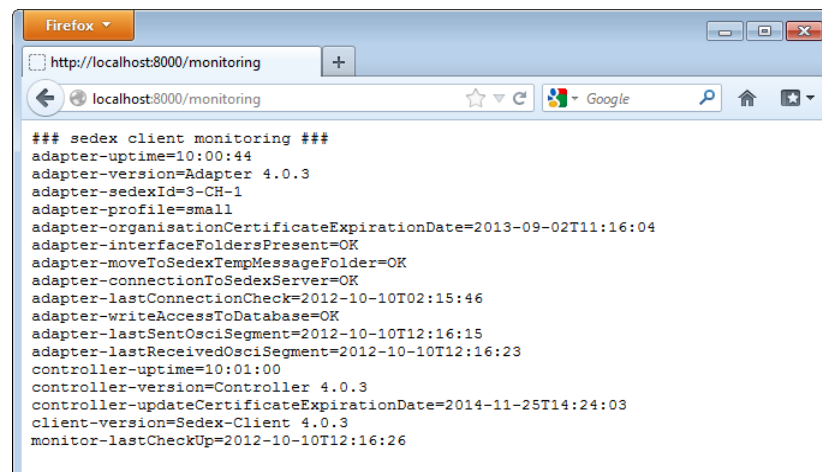


Abbildung 14: Ansicht der Antwort des HTTP-Aufrufs

4 Integration des Webservice-Proxy (synchron)

Nachfolgend sind die wesentlichen Elemente beschrieben, um den Webservice-Proxy (nachfolgend als WS-Proxy bezeichnet) in eine bestehende Infrastruktur zu integrieren oder einer Fachanwendung zu ermöglichen via sedex mit einem Webservice Provider zu kommunizieren.

Der sedex-Client besteht aus mehreren Komponenten. Die Komponente WS-Proxy wickelt den synchronen Datenaustausch ab. Der WS-Proxy spiegelt die Endpunkte der angebotenen Dienstleister im lokalen Netz des sedex-Teilnehmers. Die aktuelle Liste finden Sie auf unserer Website www.sedex.ch / synchron.

Analog zum synchronen Verfahren werden keine Veränderungen am Dateninhalt vorgenommen. Die Authentisierung, Verschlüsselung und Signatur erfolgt durch den sedex-Client unter Verwendung des Organisationszertifikats. Die Autorisierung erfolgt durch den Dienstleistungserbringer. Dieser kann das Berechtigungssystem von sedex anbinden.

4.1 Funktionsweise

Der WS-Proxy nimmt auf Seiten des sedex-Client Webservice-Aufrufe entgegen. Die Aufrufe werden authentisiert, verschlüsselt und an die Endpunkte des gewünschten Dienstbringers weitergereicht. Die Antwort des Dienstbringers wird vom WS-Proxy authentifiziert, entschlüsselt und an den ursprünglichen lokalen Aufrufer zurückgereicht.

Die nachfolgende Abbildung stellt diesen Ablauf schematisch dar.

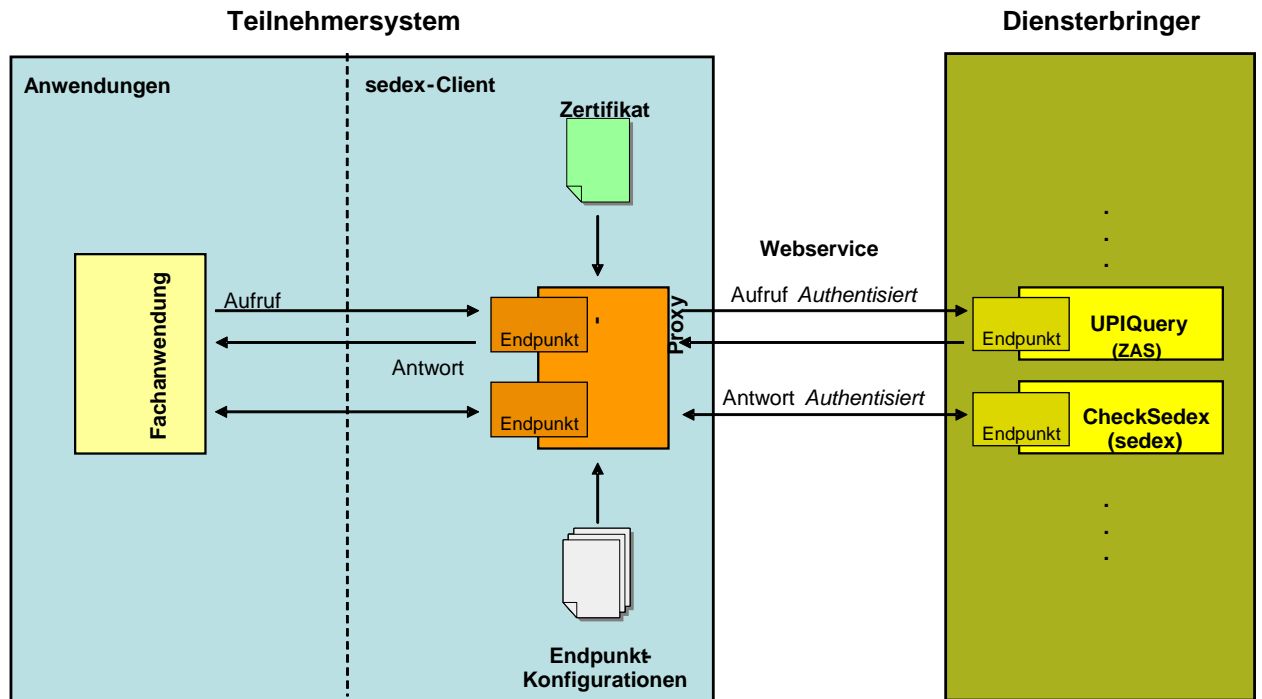


Abbildung 15: WS-Proxy

Der Aufruf kann grundsätzlich von jedem Rechner im lokalen Netz erfolgen. Es liegt in der Verantwortung des Betreibers sicherzustellen, dass ein Aufruf nur von den berechtigten Stellen erfolgen kann.

4.2 Bundle

Die Fachanwendungen können die angebotenen Webservices einheitlich integrieren.

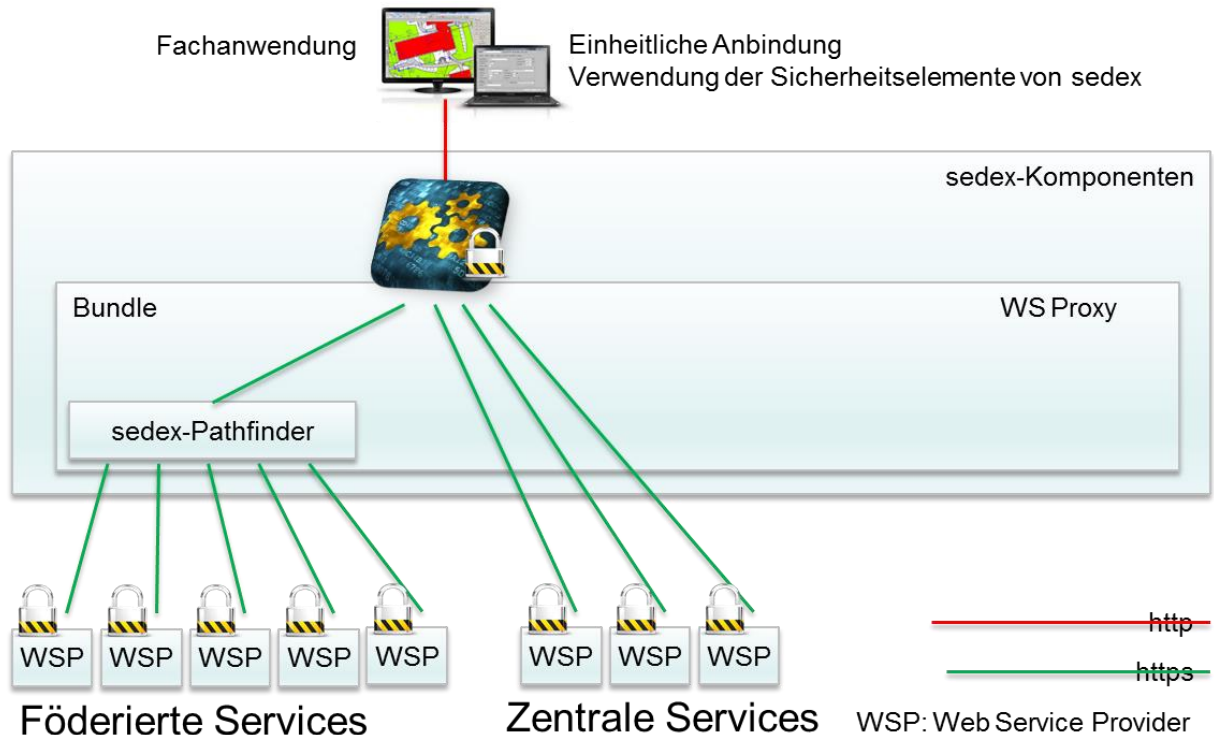


Abbildung 16: Bundle

4.2.1 Statische URL

Hierbei handelt es sich um Webservices, die zentral unter einer URL im WEB angeboten werden. Beispiele: Checksedex oder UPI der ZAS. Der WS Proxy verbindet die beiden Endpunkte.

4.2.2 Dynamische URL

Hierbei handelt es sich um verteilte Webservices (föderiert), wie die Webservices zur Personenidentifikation, die im Projekt A1.12 eUmzugCH verwendet werden. Der WS-Proxy verbindet anhand von Informationen mit der richtigen URL. Zum Beispiel wird im SAOP Request angegeben, mit welcher politischen Gemeinde eine Onlineverbindung aufgebaut werden soll. Der WS-Proxy baut dann anhand einer internen Routing Table eine Verbindung zu der richtigen URL / Port auf.

4.3 Webservice Checksedex

Checksedex ist ein vom WS-Proxy angebotener Webservice. Der Provider ist hierbei der sedex-Server selber. Der Dienst «Checksedex» prüft die wesentlichen Elemente des Meldungsumschlags:

- sedex-IDs von Absender und Empfänger sind korrekt
- Sender und Empfänger sind aktive sedex-Teilnehmer
- Sender und Empfänger haben gültige Zertifikate
- Der Absender ist autorisiert, Meldungen dieses Typs zu versenden

- Der Empfänger ist autorisiert, Meldungen dieses Typs zu empfangen
- Grösse der Nutzdatendatei übersteigt maximal zulässiges Limit (optionale Prüfung)

Die technische Beschreibung der Parameter:

Attributname	Typ	Mandatory	Beschreibung
Sender	sedex-ID	ja	ID des Absenders
AdapterID	sedex-ID	ja	ID des sedex-Client (des physischen Senders), der die Meldungen abschicken soll
MessageType	Numerisch	ja	Meldungstyp
MessageClass	Numerisch	ja	Meldungsklasse
MessageSize	Numerisch	nein	Grösse der Nutzdatendatei in Anzahl Bytes
Recipients	Liste von sedex-IDs	ja	Liste der Adressaten (auf dem Umschlag)

Antwortparameter:

Attributname	Typ	Beschreibung
Result	numerisch	0: YES (= Meldung ist gültig und autorisiert) 1: NO (= Meldung kann nicht geschickt werden, Grund siehe ErrorCode)
ErrorCode	numerisch	100: (OK - no error) 300: Unknown senderId %s 301: Unknown recipientId %s ** 302: Unknown physical senderId %s 303: Invalid messageType %s 304: Invalid messageClass %s 310: Not allowed to send 311: Not allowed to receive ** 312: User certificate not valid ** 330: Message size exceeds limit ** 999: Other (Details im Attribut ErrorMessage) ** Für Resultat pro Empfänger siehe RecipientAuthResult
ErrorMessage	string	Fehlermeldung, falls der ErrorCode > 0 ist
RecipientAuthResult	RecipientAuthResult[]	Liste mit dem Autorisierungs-Resultat für jeden einzelnen Empfänger. Nur vorhanden, wenn ErrorCode 301, 311, 312 oder 330 ist.

Typ RecipientAuthResult:

Attributname	Typ	Beschreibung
RecipientsedexId	string	sedex-ID für die das Resultat gilt
RecipientResult	numerisch	0: YES (= Empfänger ist autorisiert) 1: NO (= Meldung kann nicht an diesen Empfänger geschickt werden, Grund siehe RecipientErrorCode)
RecipientErrorCode	numerisch	100: (OK - no error) 301: Unknown recipientId %s 311: Not allowed to receive 312: User certificate not valid 330: Message size exceeds limit
RecipientErrorMessage	string	Fehlermeldung, falls der RecipientErrorCode > 0 ist

5 Betrieb des sedex-Client

5.1 Release Management

Jährlich ist mit einem bis maximal zwei Releases zu rechnen.

Der aktuelle sedex-Client steht jeweils auf der Website www.sedex.ch / Download zur Verfügung.

Die neuen Versionen sind abwärtskompatibel bis mindestens zur jeweiligen aktuellen n.0-Version. Zum Beispiel 4.9 ist kompatibel mit 4.0 aber nicht mit 3.9. Die Kompatibilität der verschiedenen Client-Versionen wird im jeweiligen Release Notes beschrieben.

Der Meldungsaustausch ist zwischen allen Versionen möglich:

Version des sedex-Client	Veröffentlichung	Ende des Supports	Ausserbetriebnahme
2.2.1	Juni 2010	30.06.2012	31.03.2016
2.2.2	Oktober 2010	31.12.2012	31.03.2016
3.0	April 2011	31.12.2013	31.03.2016
4.0.3	November 2012	31.12.2014	31.03.2016
4.0.4	Juli 2013	30.06.2015	31.03.2016
5.0	15. Juni 2015	30.09.2017	30.09.2017

Nach Ablauf „Ende des Supports“ betreibt der sedex-Support selber diese Client-Version mehr. Allfällige Probleme können unter Umständen nicht nachgestellt (reproduziert) werden. Sollte sich nicht innert nützlicher Frist eine Lösung abzeichnen, wird für die weitere Abklärung zunächst ein Update auf die aktuelle Version des sedex-Client vorausgesetzt. Bei Release Wechsel der sedex-Server wird diese Client-Version unter Umständen nicht mehr vollumfänglich getestet.

Nach Ablauf „Ausserbetriebnahme“ muss der sedex-Client zwingend auf die aktuellste Version gehoben werden. Die ausser Betrieb genommenen sedex-Clients funktionieren nicht mehr.

5.2 Remote Support Service

Der sedex-Support kann mittels Remote-Befehl genau festgelegte und begrenzte Aktionen vom sedex-Client vornehmen lassen:

- automatisierte Erneuerung des Organisationszertifikats
- automatisierte Erneuerung des WS-Proxy Truststores (Zertifikate)
- Stoppen / Starten / Neustarten des sedex-Client
- automatisiertes Update des Client
- Anfrage / Lieferung der Konfigurations- und Logdateien
- Aktualisierung der Routinginformationen für die Webservices (ab 2016)

Die so erteilten Remote-Befehle werden protokolliert und vom sedex-Support aktiv überwacht. Sollten sich Unregelmässigkeiten ergeben, ergreift der sedex-Support angemessene Massnahmen.

Es handelt sich dabei in keinem Fall um einen eigentlichen Fernzugriff (RDP, SSH, Telnet, VNC, usw.), sondern um ein definiertes Set an sedex internen Befehlen. Einzig der sedex-Support kann diese Befehle erfassen.

Nachfolgend die Liste der verfügbaren Befehle:

Befehl	Beschreibung
getconfig	Mit diesem Befehl werden alle Konfigurationsdateien des sedex-Client an den sedex-Server gesendet
getlogs	Mit diesem Befehl werden alle Logdateien des sedex-Client an den sedex-Server gesendet. Jede Komponente des sedex-Client (Controller, Adapter und WS-Proxy) erzeugt mindestens eine Logdatei.
start	Mit diesem Befehl wird der sedex-Adapter und/oder sedex-WS-Proxy gestartet.
stop	Mit diesem Befehl wird der sedex-Adapter und/oder sedex-WS-Proxy beendet.
update	Mit diesem Befehl wird der sedex-Client angewiesen, auf dem sedex-Server eine signierte Updateinstallation herunterzuladen und zu installieren.
Trust-store	Mit diesem Befehl wird dem sedex-Client eine aktualisierte Datei mit den erforderlichen Sicherheitszertifikaten vom sedex-Client installiert. Diese Zertifikate müssen in regelmässigen Abständen erneuert werden.

Die sedex-Client kommunizieren über sogenannte Dienstmeldungen.

Dienstmeldungen werden in einem separaten Verzeichnis verwaltet und vom sedex-Client selbst konsumiert.

Die korrekte Verarbeitung der Dienstmeldungen wird vom sedex-Support überwacht. Bei Problemen wird mit dem sedex-Teilnehmer Kontakt aufgenommen.

5.3 Client Update

Der sedex-Support verteilt in regelmässigen Abständen die aktuelle Client-Version an die installierten sedex-Client. Dem sedex-Client wird dabei via sedex-Meldungen der Auftrag erteilt, ein signiertes Update vom sedex-Server herunterzuladen und ein Update durchzuführen. Sollte das Update fehlschlagen, erfolgt vom sedex-Client ein Rollback.

Der Betreiber des sedex-Client kann durch Konfiguration den Updatemechanismus unterbinden. Allerdings verpflichtet er sich dann, mindestens einmal jährlich die aktuellste Version zu installieren.

5.4 Client Profile

Um die sedex-Teilnehmer optimal zu unterstützen, stehen vier verschiedene Client Profile mit unterschiedlicher Anzahl gleichzeitiger Verbindungen zum sedex-Server zur Verfügung. Dadurch wird der Meldungsdurchsatz gesteuert. Die Profile „large“ und „x-large“ sind grösseren Organisationen mit einem massiven Meldungsaufkommen vorbehalten und werden nur bei Bedarf gewährt. Die Hardware muss entsprechend leistungsfähig sein.

Vor einer Änderung des Profils kontaktieren Sie bitte den sedex-Support.

	small *	medium	large	x-large
Verbindungen zum sedex-Server	1x	2x	4x	8x
Parallele Prozesse (Threads)	2x	3x	5x	7x
Reinigungsskript (Clearing Job)	15 min.	30 min.	45 min.	60 min.

* Standardprofil

5.5 Client Migration

Der sedex-Support überwacht die sedex-Client und ergreift allenfalls bei Unregelmässigkeiten entsprechende Massnahmen. Um bei Umstellungsarbeiten eventuelle Fehlalarme zu vermeiden, werden die Betreiber gebeten, geplante Migrationen dem sedex-Support zu melden. Darunter fallen der Austausch des Servers, Wechsel der virtuellen Maschine, Wechsel des Betreibers des sedex-Client.

5.6 Umgang mit den Zertifikaten

Das elektronische Zertifikat des sedex-Client besteht aus einem public- sowie private key. Beide werden bei der Installation lokal generiert. Der private key ist nur in der lokalen Installation vorhanden und kann bei einem eventuellen Verlust von niemandem wieder hergestellt werden.

Beim sedex-Support kann ein neues Zertifikat beantragt werden. Sollten auf dem sedex-Server zu diesem Zeitpunkt nicht abgeholte Meldungen sein, können diese nicht mehr dechiffriert werden.

Der sedex-Support löst in regelmässigen Abständen die Erneuerung der Zertifikate aus.

Wir empfehlen daher, ein angemessenes Backup sicherzustellen.

Die Zertifikate sind elementare Sicherheitselemente von sedex. Diese identifizieren die sedex-Teilnehmer und dienen der Ver- und Entschlüsselung der eigenen Meldungen. Entsprechend

sind die Zertifikate vor unbefugtem Zugriff zu schützen. Ein Verdacht auf Missbrauch ist umgehend dem sedex-Support zu melden. Bei selbstverschuldetem Missbrauch wird jegliche Haftung abgelehnt.

Die Zertifikate für die sedex-Teilnehmer werden bei der Swiss Admin PKI bezogen und unterliegen einem definierten Verwendungszweck. Die Verwendung ausserhalb des sedex-Client ist durch den sedex-Support zu genehmigen. Bei anderweitiger Verwendung wird jegliche Haftung abgelehnt. Es besteht kein Anspruch auf Support.

5.7 Housekeeping - Datenhaltung

Der sedex-Client ist nicht als Archiv für Meldungen und Quittungen vorgesehen.

Für den robusten Betrieb des sedex-Client und allenfalls einfacheres Fehlerhandling, sollten nicht mehr benötigte Meldungen aus der Verzeichnisstruktur des sedex-Client gelöscht werden. Sollten Aufbewahrungsvorschriften existieren, sind deren Einhaltung vom Betreiber des sedex-Client oder der Fachanwendung mit entsprechend geeigneten Werkzeugen sicherzustellen.

Der sedex-Client löscht weder die Meldungen (Verzeichnis *inbox*, *outbox* und *processed*) noch die technischen Quittungen (Verzeichnis *receipts*). Eine periodische Löschung kann jedoch nur für das Verzeichnis *processed* im sedex-Client konfiguriert werden.

Die Logfiles werden überschrieben, sobald die maximale Grösse erreicht ist (rollover-Prinzip). Die Protokollierung auf dem sedex-Server ist davon nicht betroffen.

5.8 eCH-0090 - XML-Schemas

Das BFS ist Owner des Standards eCH-0090. Der Owner legt die Fristen fest, bis wann die Verwendung der alten Schema-Version möglich ist. Der Standard unterliegt dem Release-Management der eCH-Fachgruppe Meldewesen. Die Publikation erfolgt bei eCH www.ech.ch.

Umschläge und technische Quittungen werden aufgrund des XML-Schemas eCH-0090 gebildet. Eine Fachanwendung sollte in der Lage sein, Umschläge mehrerer XML-Schema-Versionen verarbeiten zu können. Zu beachten ist, dass bei Major Releases (2.0, 3.0,...) der Namespace der URL ändert, z.B. «xmlns:eCH-0090=http://www.eCH.ch/xmlns/eCH-0090/2» für eCH-0090 Version 2.0.

In der Konfiguration des sedex-Client wird definiert, in welcher Version des XML-Schemas die Quittung erstellt wird.

Umschläge (/eCH-0090:envelope) müssen weiterhin mit der Version 1.0 von eCH-0090 gebildet werden. Die Quittungen werden hingegen standardmässig gemäss Version 2.0 von eCH-0090 erzeugt.

Die Schemas sind unter der folgenden Adresse downloadbar: <http://www.ech.ch/xmlns>.

5.9 Nachvollziehbarkeit

Der Versand von Meldungen ist transaktionsbasiert. Jede Transaktion wird auf vom sedex-Server protokolliert und dient als Verbindungsnachweis. Die Verbindungsnachweise werden mindestens 10 Jahre aufbewahrt.

Vor- und nachgelagerte Transportsysteme sind angehalten, die MeldungsId im Umschlag eCH-0090 zu speichern

6 Glossar

Begriff	Bedeutung
sedex-Adapter	Stellt den asynchronen Datenaustausch mit dem sedex-Server sicher. Altes Synonym für den sedex-Client.
sedex-Server	Zentraler Intermediär. Übernimmt das Routing der Meldungen, Autorisierung, zentrale Protokollierung des gesamten Meldungsverkehrs. Verbindungsnachweis.
aktiver Teilnehmer	Ein Teilnehmer, der Meldungen senden und empfangen kann
Anwendung	Ein im sedex-Verbund partizipierendes Softwaresystem (Registersystem)
BFS	Bundesamt für Statistik
sedex-Client	Der Begriff sedex-Client wird ab Version 4.0 für die komplette Installation verwendet. Der sedex-Client bezeichnet die gesamte Installation, bestehend aus sedex-Controller, sedex-Adapter und sedex-WS-Proxy.
ClientDir	Das Installationsverzeichnis des sedex-Clients
sedex-Controller	Ab Version 4.0 verfügt der sedex-Client über den Controller. Dieser übernimmt das Monitoring der Komponenten des sedex-Client und das Wiederaufstarten der Komponenten, wenn diese unerwartet beendet werden. Ausserdem ermöglicht dieser Fernabfragen der Log- und Konfigurationsdaten, Aktualisierung der sedex-Komponenten und periodische Zustandsmeldung beim sedex-Server.
EWR	Einwohnerregister
HPSA	High Performance sedex-Adapter (sedex-Client 3.0)
Inaktiver Teilnehmer	Ein <i>Teilnehmer</i> , der jedoch weder Meldungen senden noch empfangen kann
Kardinalität	Bezogen auf eine präzise Logdatei, bezeichnet die Kardinalität die Anzahl Einträge, die in diese Datei geschrieben werden müssen.
KOMBV/KTV	Kommunikationsnetz der Bundes- und Kantonsverwaltungen
Log	Protokolldatei, die vom sedex-Client geschrieben wird
Logischer Teilnehmer	Ein im <i>Teilnehmerverzeichnis</i> von sedex verzeichneter <i>Teilnehmer</i> , der weder über einen sedex-Adapter noch ein eigenes Zertifikat verfügt. Ein für einen logischen Teilnehmer verantwortlicher <i>physischer Teilnehmer</i> übernimmt die Aufgabe, Meldungen von und für diesen <i>Teilnehmer</i> zu versenden.
Physischer Teilnehmer	Ein im <i>Teilnehmerverzeichnis</i> von sedex verzeichneter <i>Teilnehmer</i> , der über einen sedex-Adapter und ein Zertifikat verfügt
sedex-ID	Eindeutige Identifikation eines sedex-Teilnehmers. Synonym für <i>Teilnehmer-ID</i>
sedex-Teilnehmer	Ein Softwaresystem (z.B. das System einer Amtsstelle), welches über den sedex-Verbund erreichbar ist
Teilnehmerverzeichnis	Im Teilnehmerverzeichnis sind alle sedex-Teilnehmer, public key, Autorisierungen etc... aufgeführt. Dieses ermöglicht die eindeutige Adressierung der sedex-Teilnehmer.
WS-Proxy	Der Webservice-Proxy erlaubt partizipierenden Anwendungen, Webservices zu verwenden, ohne selbst die erforderlichen Sicherheitselemente des Providers zu integrieren oder die Verschlüsselung der Daten umzusetzen.
Wrapper	Benötigte Software, um den sedex-Client als Windows-Dienst zu starten.

Begriff	Bedeutung
WebSocket	Das WebSocket-Protokoll ist ein auf TCP basierendes Netzwerkprotokoll, das entworfen wurde, um eine bidirektionale Verbindung zwischen einer Webanwendung und einem WebSocket-Server bzw. einem Webserver, der auch WebSockets unterstützt, herzustellen. (Quelle: Wikipedia)

7 Weitergehende Dokumentation

Wir bieten diverse Dokumente an, die laufend aktualisiert werden.

Beachten Sie dazu unseren Download Bereich www.sedex.ch. Sie finden dort alle öffentlich einsehbaren Dokumente. Bei weitergehenden Bedürfnissen kontaktieren Sie bitte unseren sedex-Support.

Abbildung 1: Gesamtarchitektur sedex	4
Abbildung 2: Kommunikation zwischen sedex-Client und Server	5
Abbildung 3: Schnittstelle zwischen Anwendung und sedex-System	6
Abbildung 4: Erfolgreicher Versand einer Meldung	7
Abbildung 5: Gescheiterter Versand einer Meldung	7
Abbildung 6: Versand einer Meldung an mehrere Empfänger	8
Abbildung 7: Konzept synchrone Kommunikation	8
Abbildung 8: Ablauf Datenaustausch	9
Abbildung 9: Beispiel mit physischen Teilnehmern	9
Abbildung 10: Beispiel mit logischen Teilnehmern	10
Abbildung 11: Sendeprozess	11
Abbildung 12: Ablauf des Versands	13
Abbildung 13: Ansicht der Monitoring-Datei	23
Abbildung 14: Ansicht der Antwort des HTTP-Aufrufs	24
Abbildung 15: WS-Proxy	25
Abbildung 16: Bundle	26