



Projektname

**sedex**

Projektnummer

**5664**

Dokument

**sedex-Handbuch**

Version

**4.0.1 (25.08.2011)**

Status

in Arbeit

in Prüfung

genehmigt  
zur Nutzung

Angaben aus WORD:

Titel

**sedex-Handbuch**

Speicherdatum

25.08.2011 11:29:00

Datei-Name

sedex\_v4\_0\_1\_hb\_de.doc

Datei-Pfad

Autor(en)

BFS

Kommentar

**Zuständigkeit** (die Verteilung erfolgt entsprechend dem obigen Status bzw. Verwendungszweck):

Bearbeiter/Ersteller:	Rollout sedex
Prüfer/Genehmigung:	Nedim Muratbegovic
Benützer/Anwender:	Software-Lieferanten
zur Information/Kennntnis:	



## Änderungskontrolle

<b>Version</b>	<b>Datum</b>	<b>Name oder Rolle</b>	<b>Bemerkung</b>
1.0	01.10.2007	Igor Metz	Bereinigung für erste Publikation
1.1	22.11.2007	Igor Metz	Versch. Änderungen gemäss Änderungsprotokoll
1.2	07.01.2008	Igor Metz	Versch. Änderungen gemäss Änderungsprotokoll
2.0	01.04.2008	Igor Metz	Versch. Änderungen gemäss Änderungsprotokoll
2.1	18.07.2008	Michel Gentile	Gemäss feedback von Nedim Muratbegovic, Walter Grolimund, Antonio Stoppelli, Ralph Köchli, Igor Metz, Patrick Kummer, Jörg Böhlen
3.0	28.11.2008	Ralph Köchli	Generelle Überarbeitung infolge Ausgliederung RegHarm-Handbuch
3.1	08.07.2009	Ralph Köchli	Versch. Änderungen gemäss Release-Notes
3.2	09.12.2009	Michel Gentile	Versch. Änderungen gemäss Release-Notes
3.3	24.06.2010	Michel Gentile Nadine Pierre	Versch. Änderungen gemäss Release-Notes
4.0	14.04.2011	Michel Gentile Nadine Pierre	Versch. Änderungen gemäss Release-Notes
4.0.1	25.08.2011	Michel Gentile	Versch. Änderungen gemäss Release-Notes

## Genehmigung

<b>Version</b>	<b>Datum</b>	<b>Name oder Rolle</b>	<b>Bemerkung</b>
1.0	01.10.2007	Walter Grolimund	
1.1	22.11.2007	Walter Grolimund	
1.2	09.01.2008	Walter Grolimund	
2.0	02.04.2008	Walter Grolimund	
2.1	18.07.2008	Walter Grolimund	
3.0	28.11.2008	Nedim Muratbegovic	
3.1	08.07.2009	Nedim Muratbegovic	
3.2	09.12.2009	Nedim Muratbegovic	
3.3	24.06.2010	Nedim Muratbegovic	
4.0	14.04.2011	Nedim Muratbegovic	
4.0.1	25.08.2011	Nedim Muratbegovic	

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>7</b>
1.1	Definition von sedex	7
1.2	Zweck des Dokuments	7
1.3	Referenzen	8
1.4	Glossar	9
<b>2</b>	<b>sedex-Architektur</b>	<b>10</b>
2.1	Einleitung	10
2.2	Komponenten der Architektur	11
2.2.1	Gesamtübersicht	11
2.2.2	sedex-Server	12
2.2.3	Teilnehmerverzeichnis	12
2.2.4	sedex-Adapter	12
2.2.5	Webservice-Proxy	13
2.3	Kommunikationsszenarien	13
2.3.1	Übersicht	13
2.3.2	Request / Reply Szenario	13
2.3.3	Publish/Subscribe-Szenario	15
2.4	Anschlussmöglichkeiten an sedex	16
2.4.1	Physischer Anschluss	16
2.4.2	Logischer Anschluss	17
2.4.3	Unabhängigkeit der Meldungsadressierung	19
<b>3</b>	<b>Verwendung von sedex</b>	<b>20</b>
3.1	Schnittstelle zwischen Anwendung und Adapter	20
3.2	Ablauf des Versandes	21
3.3	Namenskonvention	21
3.4	Bereitstellung von Meldungen	22
3.5	Zustände einer Meldung	22
3.6	Inhalt des Umschlags	24
3.7	Inhalt der Quittung	27
3.8	Adressierung	29
3.8.1	Übersicht	29
3.8.2	Bereiche und Organisationseinheiten	29
3.8.3	Funktionscode	30
3.8.4	Beispiele	33
3.9	Fehlerkategorien und Statuscodes	33
3.9.1	Fehlerkategorien	34
3.9.2	Statuscodes	35
3.9.3	Verhalten bei nicht korrektem Umschlag (Status 200)	37
3.9.4	Behandlung von Message ID-Dubletten (Statuscode 201)	38
3.9.5	Verhalten bei Netzwerkfehlern	38
3.9.6	Berechnung des Verfalldatums einer Meldung (Statuscodes 203, 204 und 701)	38
3.10	Technische Sicht der Kommunikation	39
3.10.1	Verzeichnis-Verwaltung	39
3.10.2	Versand einer sedex-Meldung	39
3.10.3	Empfang einer sedex-Meldung	40
3.11	Beispiele	41

3.11.1	Beispiel: Lieferung der Gemeinde Olten an die Statistik	41
3.11.2	Beispiel: Nomenklatur-Update des BFS an interessierte sedex Teilnehmer	44
3.12	Webservice-Proxy	45
3.12.1	Zweck des Webservice-Proxy	45
3.12.2	Funktionsweise des Webservice-Proxy	45
3.12.3	Nachrichtenaustausch	45
3.12.4	Zugriff auf Webservice-Proxy	46
3.12.5	Kompatible Webservices	46
3.13	Aspekte für den Betrieb des sedex-Adapters	47
3.13.1	Aufbewahrungsfristen	47
3.13.2	Versionenhandling des XML-Schemas eCH-0090	47
3.14	sedex-Dienstmeldungen	47
3.15	HPSA	47
3.15.1	Neuheiten	48
3.15.2	Kompatibilität	48
3.15.3	Einstellungen	48
<b>4</b>	<b>Prozesse</b>	<b>50</b>
4.1	Übersicht	50
4.2	Zertifizierung partizipierender Anwendungen	50
4.3	Anmeldung des Teilnehmers	50
4.3.1	Anmeldung vorbereiten	50
4.3.2	Teilnehmer beim BFS anmelden	51
4.4	Installation des sedex-Adapters	51
4.4.1	Anforderungen an Netzwerkkonfiguration	51
4.4.2	Vorbereitung der Netzkonfiguration	51
4.4.3	Installation	55
4.5	Änderung Autorisierungen / Routing	56
4.5.1	Änderungen der Autorisierungen	56
4.5.2	Änderungen Routing	56
4.6	Erneuerung Organisationszertifikat	56
4.6.1	Erneuerungsarten	56
4.6.2	Automatisierte Erneuerung	56
4.6.3	Manuelle Erneuerung	57
4.7	Release Management	57
4.7.1	Support der verschiedenen Versionen	58
4.8	Betrieb	58
4.9	Frequently Asked Questions (FAQ)	58
<b>5</b>	<b>Zuständigkeiten</b>	<b>59</b>
5.1	Service Clientèle des BFS	59
5.1.1	Dienstleistungen	59
5.1.2	Kontakt	59
5.2	Lieferant	59
5.3	Teilnehmer	59
5.4	Fach-Domänen-Koordination	60
5.4.1	Aufgaben	60
5.4.2	Aktuelle Fach-Domänen-Koordinatoren	60
<b>6</b>	<b>Test und Integration</b>	<b>61</b>
6.1	Test-Arten	61

6.1.1	sedex-Tests	61
6.1.2	End-to-End-Tests	61
6.2	Testinstanzen	61
6.3	Testmeldungen	62
6.4	Integration	62
<b>7</b>	<b>Sicherheit</b>	<b>63</b>
7.1	Ausgangslage der Sicherheitsüberlegungen	63
7.2	Systemübersicht sedex	63
7.3	Erwartung an die partizipierenden Anwendungen	64
7.4	Beurteilung der Sicherheitsrisiken für Sender und Empfänger	64
7.5	Komponenten der Sicherheit - Sicherheitszertifikate	64
7.6	Erneuerung der Sicherheitszertifikate	65
7.6.1	Die Problematik der Sicherheitszertifikate-Erneuerung	65
7.6.2	Testzertifikate	65
<b>8</b>	<b>Anhang</b>	<b>66</b>
8.1	XML-Schemas	66
8.1.1	Bereitstellung der XML-Schema-Dateien	66
8.1.2	Verwendung der XML Schemas mit XML Spy	66
8.2	Regeln für XML-Dokumente	69
8.2.1	Kodierung der XML-Dokumente	69
8.2.2	Zeitangaben	70
8.3	Webservice CheckSedex	70
8.3.1	Dienstbeschreibung	70
8.3.2	Einschränkungen	70
8.3.3	Eingabeparameter	71
8.3.4	Antwortparameter	71
8.4	Standard-Prozesse für Ausgabe von Organisationszertifikaten	72
8.4.1	Erstausgabe und manuelle Erneuerung	72
8.4.2	Automatisierte Zertifikatserneuerung	73
8.4.3	Nachteile der manuellen Zertifikatserneuerung	73
8.4.4	Prozedur um das Verfallsdatum zu finden	74

## Abbildungen

Abbildung 1: Schnittstelle zwischen Anwendung und sedex-System	11
Abbildung 2: Gesamtarchitektur sedex	11
Abbildung 3: Erfolgreicher Versand einer Meldung	14
Abbildung 4: Gescheiterter Versand einer Meldung	14
Abbildung 5: Versand einer Meldung an mehrere Empfänger	15
Abbildung 6: Versand einer Publish/Subscribe-Meldung an mehrere Empfänger	15
Abbildung 7: Beispiel mit physischen Teilnehmern	17
Abbildung 8: Beispiel mit logischen Teilnehmern	18
Abbildung 9: Ablauf des Versandes	21
Abbildung 10: Zustände einer Meldung	23
Abbildung 11: Grafische Darstellung des Inhaltsmodells des Umschlags	27
Abbildung 12: Grafische Darstellung des Inhaltsmodells der Quittung	29
Abbildung 13: Schritte des Versandes einer Meldung	40
Abbildung 14: Webservice-Proxy	46
Abbildung 15: sedex-Prozesskette	50
Abbildung 16: Proxy-Einstellungen bei Internet Explorer 7.0	53
Abbildung 17: Beispiel mit der MS-DOS Eingabeaufforderung (Windows), wenn die Verbindung über KOMBV läuft	54
Abbildung 18: Beispiel mit der Bash Eingabeaufforderung (Linux), wenn die Verbindung über das Internet läuft	54
Abbildung 19: Komponenten der sedex-Plattform	63
Abbildung 20: Ordnerstruktur von Altova XMLSpy	68
Abbildung 21: Standard-Prozess für zentrale Ausgabe von Organisationszertifikaten	72
Abbildung 22: Standard-Prozess für die automatische Zertifikatserneuerung	73

# 1 Einführung

## 1.1 Definition von sedex

Der Bund stellt im Rahmen der Harmonisierung der Personenregister des Bundes und der kantonalen bzw. kommunalen Einwohnerregister seit Anfang 2008 eine Plattform für den sicheren Datenaustausch zur Verfügung.

Diese Plattform, genannt sedex (steht für: secure data exchange), ermöglicht einen sicheren Datenaustausch zwischen den Teilnehmern. Die Kommunikation erfolgt asynchron, erlaubt aber im Gegensatz zu herkömmlichen Mailing-Systemen den Austausch sehr grosser und vieler gleichzeitiger Meldungen.

sedex kann für weitere Bereiche genutzt werden, wobei primär e-Government-Anwendungen im Focus stehen.

Für den Anschluss an sedex ist ein Adapter in die partizipierende Anwendung zu integrieren, und die geforderten Sicherheitsforderungen müssen erfüllt werden (Authentifizierung des Teilnehmers, ggf. Zertifizierung der Anwendung).

Ab Version 2.0 enthält der sedex-Adapter auch einen Webservice-Proxy, welcher die Authentifizierung eines sedex-Teilnehmers gegenüber Webservices aufgrund des Organisationszertifikates vornimmt, wodurch für die Webservices die Benutzerverwaltung entfällt.

## 1.2 Zweck des Dokuments

Dieses Dokument beschreibt das sedex-System aus der Sicht der im sedex-Verbund partizipierenden Anwendungen. Es wendet sich primär an die Softwarelieferanten der Anwendungen.

Zielpublikum dieses Dokumentes sind

- Software-Architekten
- Software-Entwickler
- Sicherheitsbeauftragte

Dieses Handbuch gilt als Umsetzungsvorgabe für die SW-Lieferanten, welche ihre Anwendung an sedex anbinden bzw. einzelne Business Use Cases darüber abwickeln wollen. Das Bundesamt für Statistik hat diese Unterlagen in umfangreichen Analyse- und Vernehmlassungsarbeiten erstellt. Künftige Anpassungen und Änderungen können jedoch nicht ausgeschlossen werden.

### 1.3 Referenzen

- [1] OSCI-Transport 1.2, Spezifikation, OSCI Leitstelle, Bremen, 6.6.2002  
[http://www1.osci.de/sixcms/media.php/13/osci\\_spezifikation\\_1\\_2\\_deutsch.pdf](http://www1.osci.de/sixcms/media.php/13/osci_spezifikation_1_2_deutsch.pdf)
- [2] OSCI-Transport 1.2, Entwurfsprinzipien, Sicherheitsziele und -mechanismen, OSCI Leitstelle, Bremen, 6.6.2002  
[http://www1.osci.de/sixcms/media.php/13/osci\\_entwurfsprinzipien\\_1\\_2.2110.pdf](http://www1.osci.de/sixcms/media.php/13/osci_entwurfsprinzipien_1_2.2110.pdf)
- [3] Bundesamt für Statistik:  
Historisiertes Gemeindeverzeichnis der Schweiz. Erläuterungen und Anwendung (15.06.2007)  
<http://www.bfs.admin.ch/bfs/portal/de/index/news/publikationen.html?publicationID=2754>
- [4] Bundesamt für Statistik:  
sedex-Handbuch – Registerharmonisierung. V 3.1 (08.07.2009)  
<http://www.register-stat.admin.ch> > IT-Spezifikationen > sedex
- [5] Bundesamt für Statistik:  
Meldungen der Bundesregister an die Einwohnerregister. V 1.4 (25.08.2011)  
<http://www.register-stat.admin.ch> > IT-Spezifikationen > Datenaustausch zwischen Registern
- [6] Bundesamt für Statistik:  
Erstvergabe der Versichertennummer. Technischer Prozess. V 1.2 (30.09.2008)  
<http://www.register-stat.admin.ch> > IT-Spezifikationen > AHVN13
- [7] Bundesamt für Statistik:  
Spezifikationen für den Meldungstyp eCH-0087 V 1.3 (14.04.2009)  
<http://www.register-stat.admin.ch> > IT-Spezifikationen > EGID/EWID-Zuweisung
- [8] Zentrale Ausgleichsstelle:  
UPI (Unique Personal Identifier) Interface. V 1.4  
<http://www.zas.admin.ch/cdc/cnc3/cdc.php?paqid=33&elid=689&lang=de>
- [9] Bundesamt für Informatik und Telekommunikation:  
sedex Adapter User Manual V 3.0 (25.08.2011)  
<http://www.register-stat.admin.ch> > IT-Spezifikationen > sedex
- [10] Bundesamt für Informatik und Telekommunikation:  
sedex: Webservice-Proxy Benutzerhandbuch V 2.1 (14.04.2011)  
<http://www.register-stat.admin.ch> > IT-Spezifikationen > sedex
- [11] Bundesamt für Statistik:  
sedex-Meldungstypen von Bund und Kantonen, V 1.2 (14.04.2011)  
<http://www.register-stat.admin.ch> > IT-Spezifikationen > sedex
- [12] Bundesamt für Informatik und Telekommunikation:  
Handbuch für EBS-Teilbus-Betreiber, V 0.5 (15.12.2010)
- [13] Bundesamt für Statistik:  
Release-Notes - sedex-Adapter V 3.0 (25.08.2011)  
<http://www.register-stat.admin.ch> > IT-Spezifikationen > sedex

## 1.4 Glossar

Begriff	Bedeutung
Adapter	„Verbindungsstück“ zwischen den im sedex-Verbund partizipierenden Anwendungen und dem sedex-System.
aktiver Teilnehmer	ein <i>Teilnehmer</i> , der Meldungen senden und empfangen kann
Amtsstellenverzeichnis	Verzeichnis der Amtsstellen, welche über sedex erreichbar sind. Das Amtsstellenverzeichnis wird provisorisch vom BFS geführt.
Anwendung	ein im sedex-Verbund partizipierendes Softwaresystem (Registersystem)
BFS	Bundesamt für Statistik
EWR	Einwohnerregister
HPSA	High Performance sedex Adapter (sedex-Adapter 3.0)
inaktiver Teilnehmer	ein <i>Teilnehmer</i> , der jedoch weder Meldungen senden noch empfangen kann
KOMBV/KTV	Kommunikationsnetz der Bundes- und Kantonsverwaltungen
Lieferant	Software-Hersteller resp. dessen Vertreter für die Installation (Vertriebspartner)
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	Synonym für <i>Teilnehmer-ID</i>
Teilnehmer	ein Softwaresystem (z.B. das System einer Amtsstelle), welches über den sedex-Verbund erreichbar ist
Teilnehmer-ID	zur Adressierung von <i>Teilnehmern</i> im sedex-Verbund genutzte „sprechende“ Identifikation; Synonym für <i>Sedex-ID</i> .
Teilnehmerverzeichnis	technisches Verzeichnis, in welchem die über sedex erreichbaren Teilnehmer verzeichnet sind

## 2 sedex-Architektur

### 2.1 Einleitung

Die sedex-Architektur baut auf dem Konzept lose gekoppelter Anwendungen auf, die in einem Verbund über eine Datendrehscheibe asynchrone Meldungen austauschen. Man spricht hier von einer sogenannten „Hub-and-spoke“ (Nabe und Speiche) -Architektur<sup>1</sup>. Als Kommunikationsszenarien stehen

- Request / Reply<sup>2</sup>
- Request ohne Reply
- Publish / Subscribe<sup>3</sup>

zur Verfügung.

Die Basis der sedex-Datendrehscheibe bildet ein nach dem in Deutschland definierten Standard OSCI (siehe [1],[2]) implementierter Intermediär. Der Intermediär ist ein vermittelndes Serversystem, welches den Inhalt der ausgetauschten Meldungen nicht kennt und die vom Gesetzgeber geforderte End-to-End-Sicherheit (Authentifizierung, Zugriffskontrolle, Vertraulichkeit, Datenintegrität, Datenannahme) bietet.

Die über die Datendrehscheibe ausgetauschten Meldungen bestehen aus einem Umschlag und aus Nutzdaten. Der Umschlag ist ein XML-Dokument, welches die für die korrekte Zustellung einer Meldung erforderlichen Adressierungsinformationen enthält. Die Nutzdaten sind in einer Datei enthalten, deren Format vor der verantwortlichen Stelle des entsprechenden Meldungstyps definiert wird.

Die Adressierung der Meldungen im Verbund erfolgt unter Verwendung eines Teilnehmerverzeichnisses. Das sedex-System bildet dabei in Abhängigkeit vom konkreten Geschäftsfall „logische“ Namen (Gemeinde, Amtsstelle) auf die für den sicheren Datentransport erforderlichen Zertifikate ab.

Die Schnittstelle der im Verbund partizipierenden Anwendungen zum sedex-System besteht im Wesentlichen aus zwei Verzeichnissen im Dateisystem. Die Anwendung braucht lediglich die zu versendenden Meldungen als Dateien in einem Verzeichnis bereitzustellen und kann die empfangenen Meldungen wiederum als Dateien aus einem anderen Verzeichnis lesen. Versandquittungen des Systems werden ebenfalls in Form von Dateien bereitgestellt. Den Transport über das sedex-System übernimmt ein Adapter (siehe Abbildung 1: Schnittstelle zwischen Anwendung und sedex-System).

Zusätzlich zur sedex-Kernfunktionalität des sicheren, zuverlässigen und asynchronen Austauschs potentiell grosser Nachrichten unterstützt sedex den synchronen Aufruf von Webservices, welche zur Authentifizierung des Aufrufers sedex-Teilnehmerzertifikate akzeptieren (siehe dazu Kapitel 3.12).

---

<sup>1</sup> Datendrehscheibe = Hub; Anwendungen = Spoke. Siehe auch [http://de.wikipedia.org/wiki/Hub\\_and\\_Spoke](http://de.wikipedia.org/wiki/Hub_and_Spoke)

<sup>2</sup> siehe auch <http://en.wikipedia.org/wiki/Request-response>

<sup>3</sup> siehe auch <http://en.wikipedia.org/wiki/Publish/subscribe>

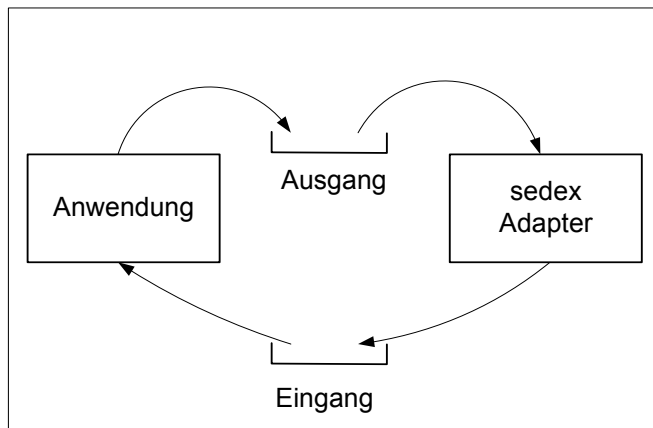


Abbildung 1: Schnittstelle zwischen Anwendung und sedex-System

## 2.2 Komponenten der Architektur

### 2.2.1 Gesamtübersicht

Die folgende Abbildung gibt eine Übersicht über die Gesamtarchitektur von sedex.

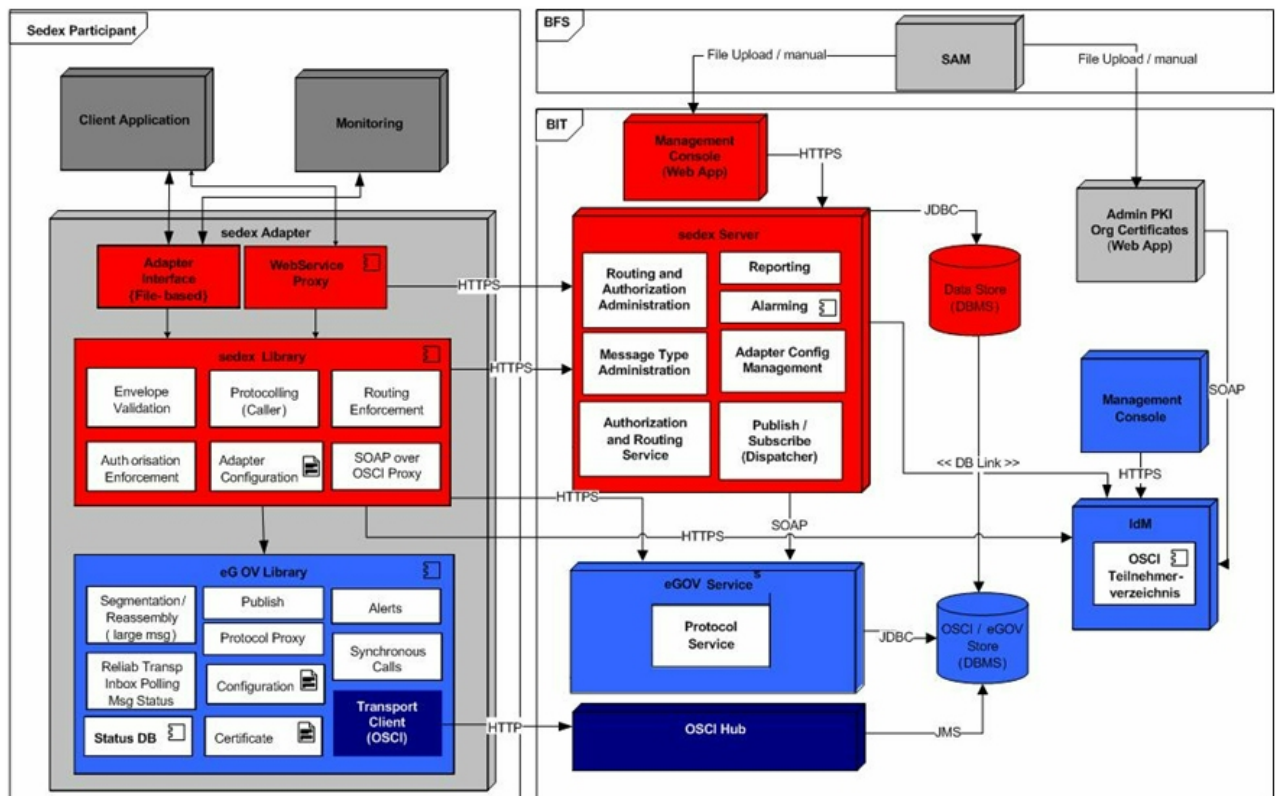


Abbildung 2: Gesamtarchitektur sedex

### 2.2.2 sedex-Server

Der sedex-Server ist im Rahmen der Gesamtarchitektur für die folgenden Aufgaben verantwortlich:

- Bereitstellung der für das Routing der Meldungen erforderlichen Information
- Autorisierung der Zustellung von Meldungen
- zentrale Protokollierung des gesamten Meldungsverkehrs im Verbund
- Bereitstellung des Publish/Subscribe-Mechanismus

### 2.2.3 Teilnehmerverzeichnis

Im Teilnehmerverzeichnis sind alle im sedex-Verbund bekannten Teilnehmer aufgeführt. Im Teilnehmerverzeichnis wird die Information geführt, wer wem wie welche Meldungen senden darf. Teilnehmer können aktiv oder inaktiv sein. Nur aktive Teilnehmer können Meldungen senden und empfangen.

### 2.2.4 sedex-Adapter

Der Adapter funktioniert bidirektional, d.h. er fungiert sowohl als Sender als auch als Empfänger von sedex-Meldungen. Der Adapter versendet und empfängt sowohl Meldungen zwischen den über sedex kommunizierenden Registeranwendungen als auch administrative Meldungen (d.h. Meldungen zwischen den Adaptern bzw. zwischen dem Adapter und anderen Komponenten der sedex-Infrastruktur, wie z.B. dem sedex-Server).

Der Adapter übernimmt in der Architektur die folgenden Aufgaben:

- Überwachung eines Verzeichnisses im Dateisystem, in welches die sendende Anwendung Meldungen hineinschreibt. Sobald der Adapter eine Meldung vorfindet, wird diese versendet.
- Abfrage der für das Routing einer Meldung erforderlichen Information (Zertifikate) beim sedex-Server.
- Versand einer Meldung an die gemäss Routing-Information genannten Empfänger. Die Meldung wird vom Adapter signiert, mit den Zertifikaten der Empfänger verschlüsselt und dann unter Verwendung der OSCI-Bibliothek an den OSCI-Intermediär übermittelt.
- mehrfache Wiederholung des Versandes im Falle technischer Probleme (z.B. Netzwerkstörung).
- Grosse Meldungen werden für den Versand in Segmente zerlegt. Segmente von Meldungen werden beim Empfang wieder zusammengesetzt. Dadurch kann gewährleistet werden, dass bei der Übertragung grosser Meldungen auch dann keine Timeouts entstehen, wenn die Internetanbindung eines Kommunikationspartners über wenig Bandbreite verfügt.
- periodisches Abfragen des Postfaches auf dem OSCI-Intermediär.
- Herunterladen der Meldungen aus dem Postfach. Der Adapter wird dabei eine Triage zwischen administrativen Meldungen der Plattform, sedex-Meldungen mit Nutzdaten und nicht erwarteten Meldungen vornehmen:
- Empfang von Servicemeldungen der Plattform (Receipts).

- Bei Payload-Meldungen wird überprüft, ob die sendende Anwendung berechtigt ist, der empfangenden Anwendung Meldungen zu senden.
- Nicht erwartete Meldungen werden verworfen.
- Empfangene Meldungen mit Nutzdaten werden vom Adapter in ein Verzeichnis im Dateisystem abgelegt, wo sie von der empfangenden Anwendung abgeholt werden.
- Bereitstellung von Versandquittung an die sendende Anwendung.
- zentrale Protokollierung der versendeten und empfangenen Meldungen.
- Der Adapter führt eine eigene (eingebettete) Datenbank, in welcher der Status der einzelnen Meldungen geführt wird. Durch transaktionale Sicherheit kann garantiert werden, dass keine Meldungen verloren gehen.

### 2.2.5 Webservice-Proxy

Der sedex-Webservice-Proxy erlaubt es partizipierenden Anwendungen, bestimmte Webservices zu verwenden, ohne sich selbst gegenüber dem Dienstbringer explizit authentisieren zu müssen oder sich um die Verschlüsselung der Daten kümmern zu müssen. Die Authentisierung und Verschlüsselung erfolgt automatisch durch sedex, unter Verwendung des Organisationszertifikats des Adapters. Dazu repliziert der sedex-Webservice-Proxy die entsprechenden Endpunkte der Dienstbringer clientseitig.

## 2.3 Kommunikationsszenarien

### 2.3.1 Übersicht

Sender und Empfänger sind im sedex-Verbund voneinander vollständig entkoppelt. Die Kommunikation zwischen ihnen läuft über asynchronen Nachrichtenaustausch, wobei das sedex-System die Rolle des Vermittlers übernimmt.

Die Schnittstelle zwischen Anwendung und sedex-System stellen das Eingangs- und das Ausgangsverzeichnis des Adapters dar.

Die sendende Anwendung stellt dem Adapter die zu versendenden Meldungen als Dateien in einem Verzeichnis bereit, von wo aus sie über das sedex-System an den (oder die) vorgesehenen Empfänger transportiert werden. Für die Anwendung bestimmte Meldungen, die der Adapter empfängt, stellt er als Dateien in einem Verzeichnis bereit (siehe Abbildung 1: Schnittstelle zwischen Anwendung und sedex-System).

Der Adapter stellt der sendenden Anwendung für jede versandte Meldung und pro Empfänger dieser Meldung eine Versandquittung in Form einer XML-Datei aus.

Der Webservice-Proxy ermöglicht durch das Anbieten von Webservices zusätzliche Kommunikationsszenarien, welche hier nicht weiter beschrieben werden, da sie nicht zur Kernfunktionalität von sedex gehören.

### 2.3.2 Request / Reply Szenario

Abbildung 3 zeigt den erfolgreichen Versand einer Meldung eines Senders an einen Empfänger. Der in der Abbildung gezeigte einzelne Adapter subsumiert aus der Sicht der Anwendungen das gesamte sedex-System.

Zurzeit ist die Grösse von Meldungen, welche mit diesem Szenario via sedex versandt werden sollen, auf 10 GB limitiert. Sender von Meldungen müssen sich jedoch bewusst sein, dass dies entsprechende Anforderungen an die Hardware von Sender und Empfänger(n) stellt und den Versand bzw. Empfang weiterer Meldungen während dieser Zeit verhindert.

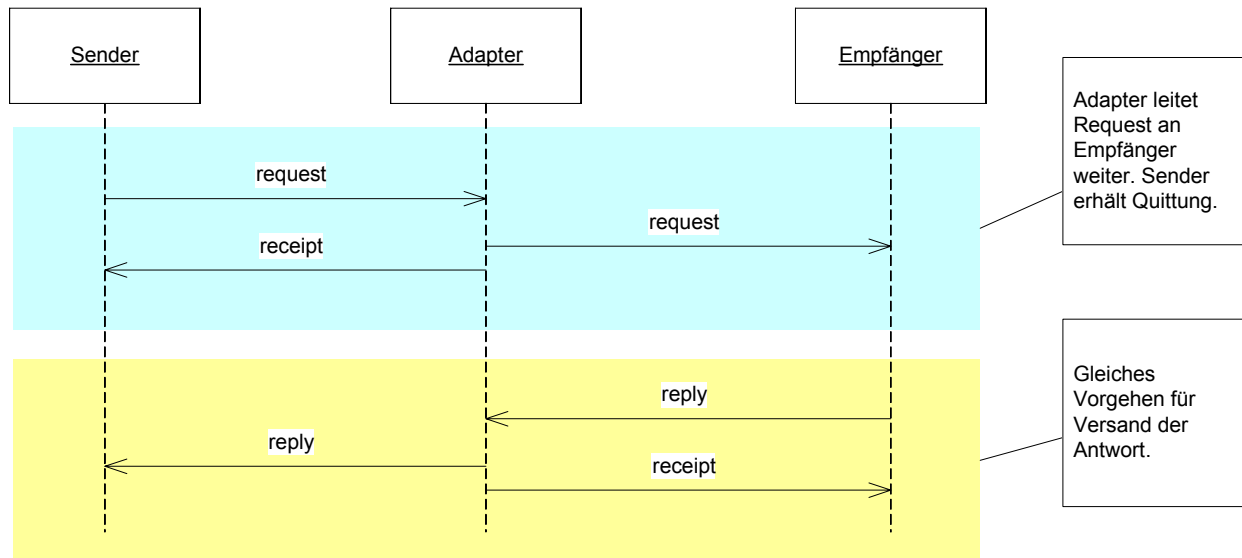


Abbildung 3: Erfolgreicher Versand einer Meldung

Abbildung 4 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.

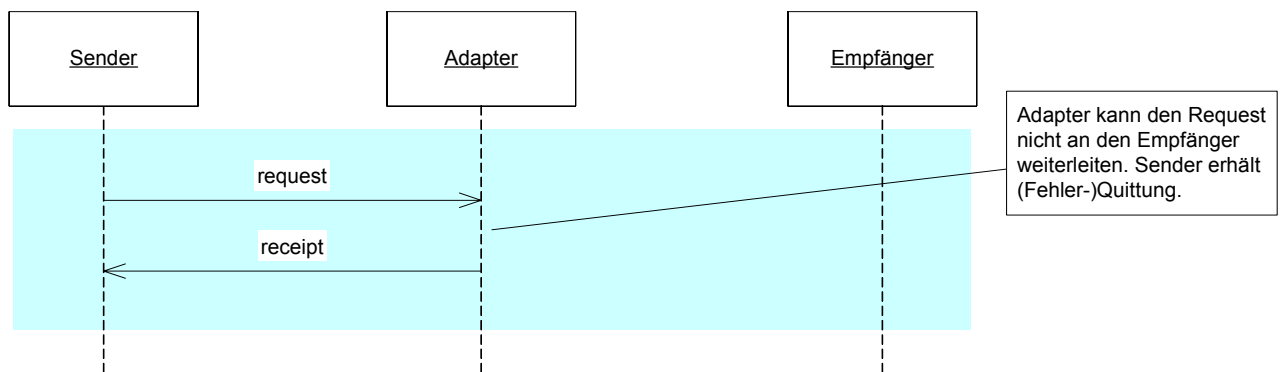


Abbildung 4: Gescheiterter Versand einer Meldung

Abbildung 5 zeigt den Versand einer einzelnen Meldung an zwei Empfänger. Dieses Szenario tritt auf, wenn die sendende Anwendung im Versandumschlag explizit mehrere Empfänger aufführt.

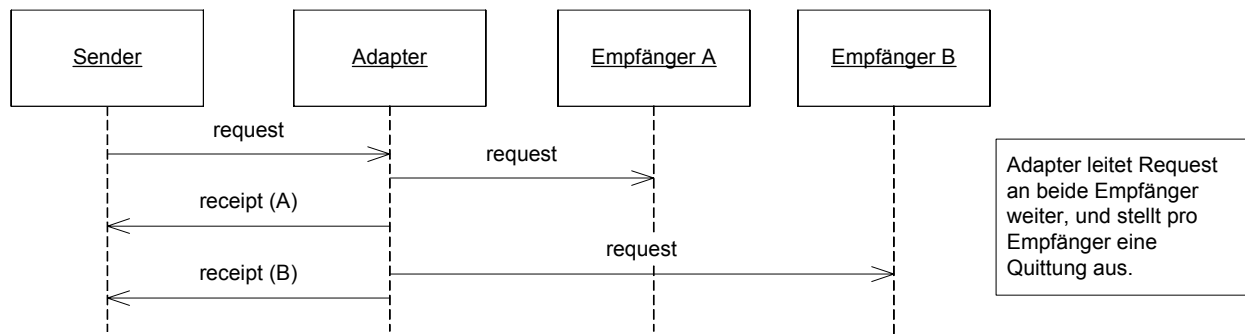


Abbildung 5: Versand einer Meldung an mehrere Empfänger

### 2.3.3 Publish/Subscribe-Szenario

Das Publish/Subscribe-Szenario ermöglicht den Versand einer Meldung an all diejenigen Teilnehmer des sedex-Verbundes, die an diesem Typ von Meldung interessiert sind. Der Sender weiss in diesem Fall nicht, an welche Empfänger seine Meldung letzten Endes ausgeliefert wird.

Aus Sicherheitsgründen sieht sedex - im Unterschied zum klassischen Publish/Subscribe-Szenario - aber keine Möglichkeit vor, dass sich Teilnehmer dynamisch für den Empfang bestimmter Meldungen abonnieren können. Die Abonnie rung (Subskription) erfolgt durch einen administrativen Prozess auf dem Teilnehmerverzeichnis von sedex.

Zurzeit ist die Grösse von Meldungen, welche mit diesem Szenario via sedex versandt werden sollen, auf 100 MB limitiert.

Der Sender („publisher“) einer solchen Meldung adressiert seine Meldung an sedex (/eCH:0090:envelope/recipientId, vgl. Kap. 3.6). Das sedex-System nimmt die Meldung entgegen und bestätigt dem Sender den Empfang mit einer technischen Quittung. Anschliessend wird sedex die Meldung gemäss der Liste der Abonnenten weiter verteilen (siehe Abbildung 6: Versand einer Publish/Subscribe-Meldung an mehrere Empfänger).

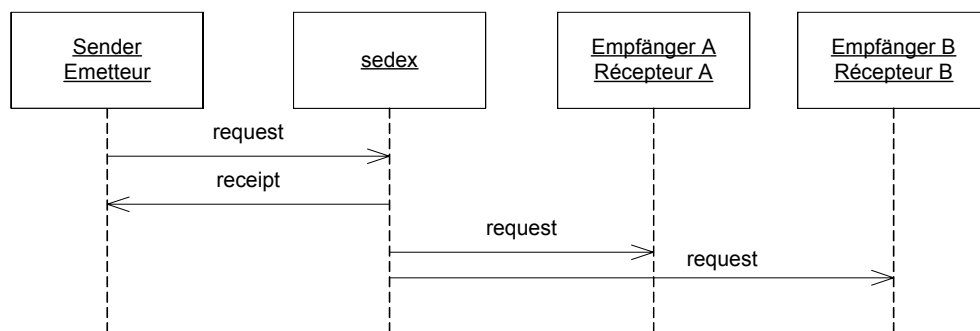


Abbildung 6: Versand einer Publish/Subscribe-Meldung an mehrere Empfänger

Das sedex-System verändert bei der Weiterleitung der vom Sender publizierte Meldung an die Empfänger den Umschlag wie folgt:

- Der Absender im Umschlag (/eCH:0090:envelope/senderId, vgl. Kap. 3.6) wird durch sedex nicht verändert.

- Die Meldungsnummer im Umschlag (/eCH:0090:envelope/messageld, vgl. Kap. 3.6) wird von sedex neu vergeben.
- Der Empfänger im Umschlag (/eCH:0090:envelope/recipientId, vgl. Kap. 3.6) wird durch die sedex-Teilnehmernummer des Empfängers ersetzt.
- Ist der Empfänger der publizierten Meldung direkt an sedex angeschlossen (siehe Kap. 2.4.1), so wird der Umschlag nur die sedex-Teilnehmer-ID dieses Empfängers enthalten.
- Ist der Empfänger der publizierten Meldung indirekt an sedex angeschlossen (siehe Kap. 2.4.2), so wird der Umschlag die sedex-Teilnehmer-IDs aller Empfänger enthalten, die von ihrem direkt angeschlossenen Teilnehmer bedient werden.

## 2.4 Anschlussmöglichkeiten an sedex

Um zwischen verschiedene Systeme und Dienststellen kommunizieren zu können, ist die *sedex-Adapter* Software notwendig. Die sedex-Plattform unterscheidet die sedex-Teilnehmer und den sedex-Adapter. Es ist somit möglich, mit einem einzigen sedex-Adapter mehrere Teilnehmer an das sedex-Netzwerk anzuschliessen.

Es bestehen zwei Möglichkeiten, um einen Teilnehmer (z.B. Einwohnerregister, Betriebsamt, usw.) dem sedex-Netzwerk anzuschliessen :

- Physischer Anschluss
- Logischer Anschluss

Jeder Teilnehmer und jeder Adapter besitzt einen sedex-Identifikator (sedex ID), unabhängig vom gewählten Anschluss. In den meisten Fällen entspricht die sedex ID auch der sedex ID eines Teilnehmers. Ein Teilnehmer besitzt aber nicht unbedingt seinen eigenen Adapter. Die zwei folgenden Kapitel beschreiben ausführlich die möglichen Varianten (physisch/logisch).

### 2.4.1 Physischer Anschluss

Ein physischer Teilnehmer ist ein Teilnehmer, der seinen eigenen Adapter besitzt. In einem solchen Fall entspricht die Teilnehmer sedex ID der Adapter sedex ID (es gibt keinen Unterschied zwischen dem Teilnehmer und dem Adapter, da der Teilnehmer der einzige Benutzer dieses Adapters ist).

Die sedex Teilnehmer 1 und 2 auf folgender Abbildung sind physische Teilnehmer .

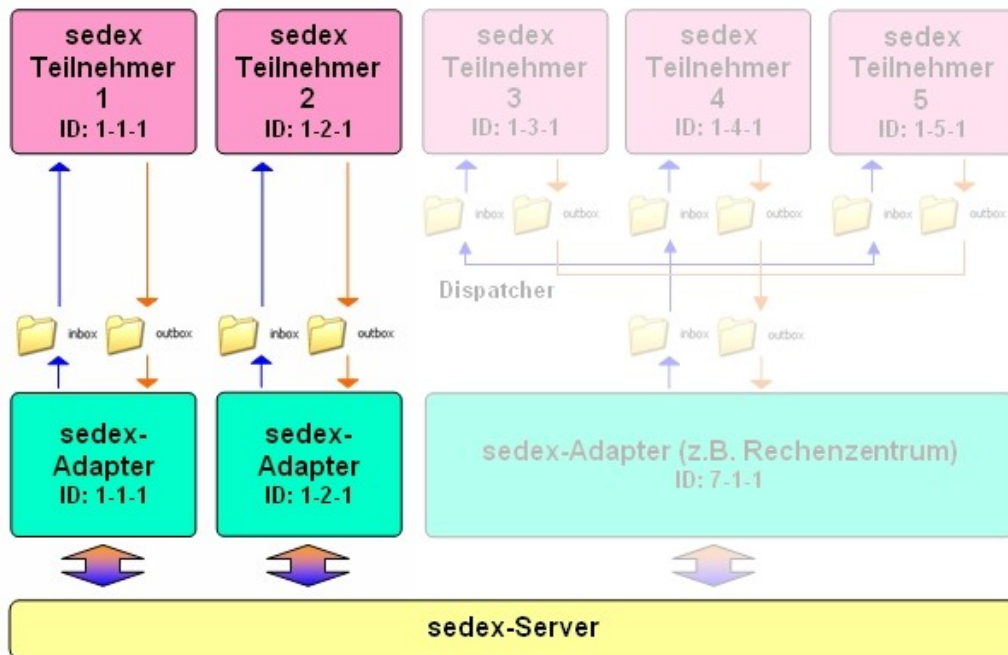


Abbildung 7: Beispiel mit physischen Teilnehmern

Diese Anschlussart empfiehlt sich besonders wenn der anzuschliessende Teilnehmer eine grosse Menge von sedex Meldungen austauscht und wenn die Schutzanforderungen (Sicherheit und Installationsschutz) wichtig sind.

#### 2.4.2 Logischer Anschluss

Ein logischer Teilnehmer ist ein Teilnehmer, der einen von einem Rechenzentrum oder einem Kanton zur Verfügung gestellten generischen Adapter verwendet. In einem solchen Fall entspricht die Teilnehmer sedex ID nicht der Adapter sedex ID (es muss zwischen dem Teilnehmer und dem Adapter unterschieden werden, da mehrere Teilnehmer den gleichen Adapter benutzen könnten).

Für den logischen Anschluss wird der gleiche Adapter verwendet wie für den physischen Anschluss. Es gibt demnach nur einen Eingang (für die zu versendenden Meldungen) und einen Ausgang (für die empfangenen Meldungen) obwohl mehrere logische Teilnehmer diesen adapter verwenden könnten. Die eingehenden und die ausgehenden Meldungen müssen vom Rechenzentrum oder vom Kanton, der den Gemeinschaftsadapter betreibt, bereitgestellt bzw. gesammelt werden. Diese Aufgabe wird in der Regel von einem Programm (Dispatcher) übernommen.

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

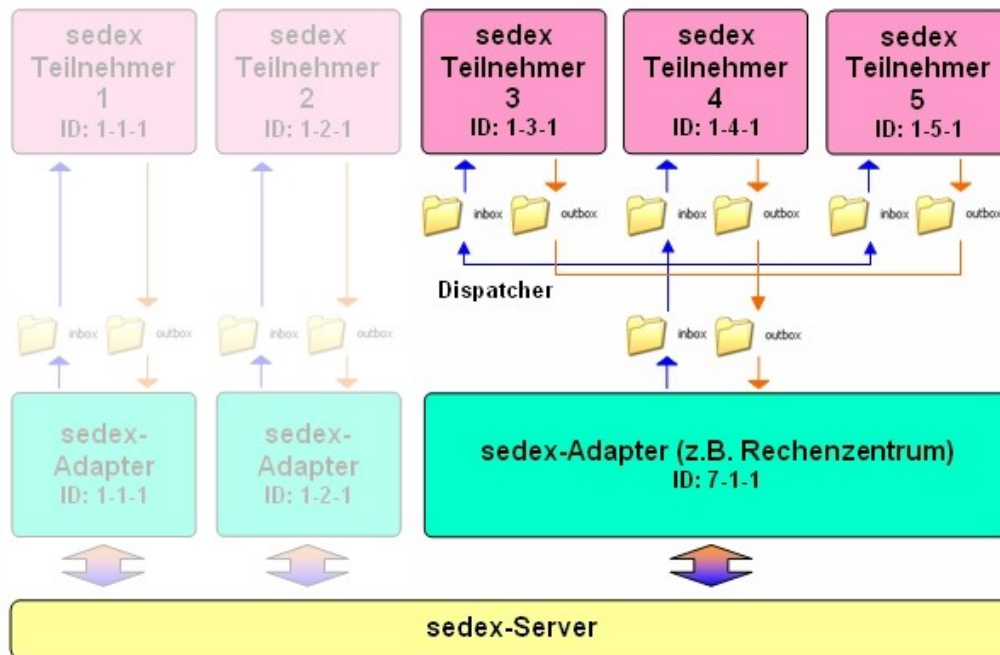


Abbildung 8: Beispiel mit logischen Teilnehmern

Der Dispatcher stellt dem Teilnehmer die eingehenden Nachrichten anhand des im sedex-Umschlag angegebenen Empfängers (Recipient ID) so zu, wie der Postdienst eines Unternehmens die Post anhand der auf den Briefumschlägen angegebenen Namen an die betroffenen Mitarbeitenden verteilt.

Weder das BFS noch das BIT stellt einen Dispatcher bereit. Rechenzentren und Kantone, die einen solchen Dienst anbieten möchten, können eine massgeschneiderte Lösung entwickeln oder eine auf dem Markt erhältliche Lösung erwerben.

Der Betreiber des sedex-Adapters haftet für die Datensicherheit zwischen den logischen Teilnehmern und dem sedex-Adapter und sorgt dafür, dass ein Teilnehmer A nicht auf die von einem Teilnehmer B gesendeten oder empfangenen Daten zugreifen kann.

Diese Anschlussart empfiehlt sich besonders für Rechenzentren, die einen sedex-Anschluss anbieten möchten, ohne gleich mehrere sedex-Adapter zu betreiben. Die so an sedex angeschlossenen Teilnehmer tauschen in der Regel nur wenige sedex-Meldungen aus.

### 2.4.3 Unabhängigkeit der Meldungsadressierung

Zu beachten ist, dass die Art des Anschlusses eines Teilnehmers keinen Einfluss auf die Adressierung von Meldungen hat: Die *senderId* und/oder *recipientId* im Umschlag (siehe Kap. 3.6) sind gegebenenfalls logische Teilnehmer. Die Routing-Regeln des sedex-Servers stellen sicher, dass die Meldungen an den korrekten Teilnehmer geleitet werden. Ein sendender Teilnehmer muss demzufolge nicht wissen, ob der Empfänger ein physischer (direkt angeschlossen) Teilnehmer oder ein logischer (indirekt über ein Rechenzentrum oder einen Kanton angeschlossener) Teilnehmer ist.

## 3 Verwendung von sedex

### 3.1 Schnittstelle zwischen Anwendung und Adapter

Sendende und empfangende Anwendung, nachfolgend „Sender“ und „Empfänger“ genannt, sind im sedex-Verbund voneinander vollständig entkoppelt. Die Kommunikation zwischen ihnen läuft über asynchronen Meldungs austausch, wobei das sedex-System die Rolle des Vermittlers übernimmt.

Die Schnittstelle der im Verbund partizipierenden Registersysteme zum sedex-System besteht im wesentlichen aus zwei Verzeichnissen im Dateisystem, über welche Dateien ausgetauscht werden. Das Registersystem braucht lediglich die zu versendenden Meldungen als Dateien in einem Verzeichnis bereitzustellen und kann die empfangenen Meldungen wiederum als Dateien aus einem anderen Verzeichnis lesen.

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

Den Transport über das sedex-System übernimmt ein Adapter (siehe Abbildung 1: Schnittstelle zwischen Anwendung und sedex-System).

Eine *Meldung* besteht immer aus *zwei* Dateien:

- einer *Umschlagsdatei*  
Die Umschlagsdatei ist ein XML-Dokument, welches dem XML-Schema eCH-0090.xsd entspricht und ein Element /eCH-0090:envelope enthält. Der sedex-Adapter prüft den Inhalt des Umschlags auf syntaktische (d.h. XML-Schema) und semantische Korrektheit (z.B. korrekte Adressen u.ä.).
- einer *Nutzdatendatei*  
Die Nutzdatendatei kann Daten beliebigen Typs enthalten. Der sedex-Adapter nimmt keine Prüfung des Inhalts der Nutzdatendatei vor. Es ist Aufgabe des Senders, die Korrektheit des Inhaltes zu garantieren bzw. die Aufgabe des Empfängers, den Inhalt vor der Verarbeitung auf seine Korrektheit 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.

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 Adapter 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.

## 3.2 Ablauf des Versandes

Genereller Ablauf des Versandes einer Meldung:

- Der Sender übergibt seine Meldung, bestehend aus einem Umschlag und einer Nutzdatei, dem Adapter zum Versand. Die Anwendung stellt die Dateien im Ausgangsverzeichnis des Adapters bereit.
- Der Adapter versucht die Zustellung der Meldung.
- Sobald der sendende Adapter die Meldung weitergeleitet hat, wird er die beiden Dateien in das Verzeichnis der verschickten Meldungen verschieben.
- Nach erfolgreicher oder gescheiterter Zustellung stellt der Adapter dem Sender pro Empfänger, der im Umschlag explizit aufgeführt war, eine Quittungsdatei aus.
- Ab der Adapterversion 2.0 kann dieser auch während des Zustellungsprozesses Quittungen für Statusupdates und Warnungen ausstellen
- Die Anwendung wertet die Quittung aus.

Sendet der Empfänger dem Sender eine Antwort zurück, so funktioniert der obige Ablauf identisch, aber mit verkehrten Rollen. Die in Abbildung 9 gezeigten Adapter subsumieren aus der Sicht der Anwendungen das gesamte sedex-System.

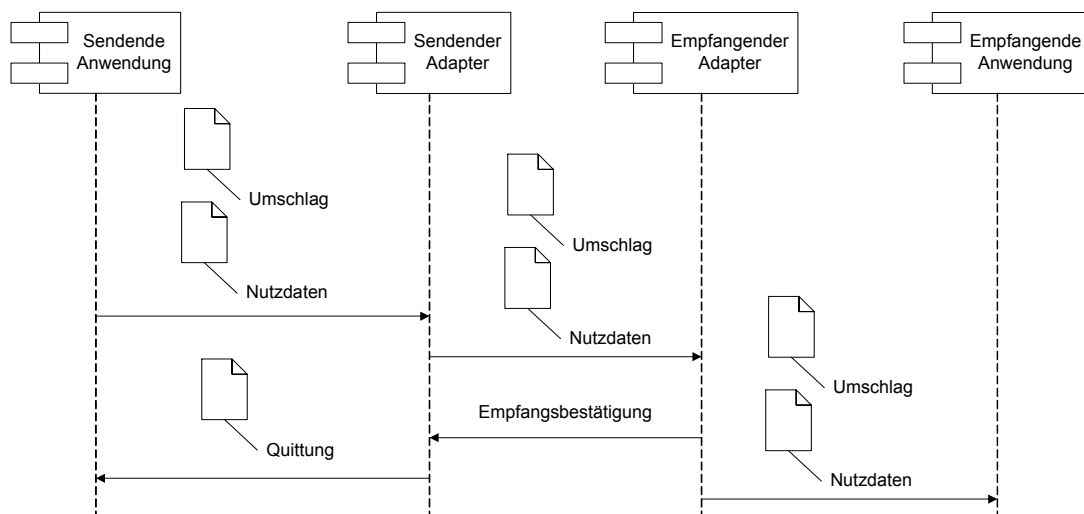


Abbildung 9: Ablauf des Versandes

## 3.3 Namenskonvention

Der sendende Adapter erwartet die folgenden Dateien:

- Den Umschlag als Datei `envl_N.xml`
- Die Nutzdaten als Datei `data_N.xxx`

„N“ ist ein von der Anwendung erzeugter eindeutiger Namenssuffix. Die Korrelation von Umschlag zu Nutzdaten erfolgt durch die Verwendung der gleichen Suffixe. Zum Beispiel bilden die Dateien „envl\_4711.xml“ und „data\_4711.zip“ eine Meldung, weil sie den gleichen Suffix „4711“ enthalten. Die Namen der Dateien haben für den Adapter ausser für die Korrelation von Umschlag und Nutzdaten keinerlei Bedeutung. Die Anwendung ist frei, die Namenssuffixe nach eigenem Gutdünken zu vergeben. Wir empfehlen, als Namenssuffix die *messaged* aus dem Umschlag zu nutzen.

„xxx“ bezeichnet eine beliebige Dateierweiterung (Extension), welchen den Dateityp (XML, Zip, PDF etc.) bezeichnet. Der Adapter leitet aus der Dateierweiterung den Dateityp her.

Der sendende Adapter stellt die Versandquittung als Datei mit Namen „receipt\_\_ID\_MY.xml“ im Quittungsverzeichnis bereit. „M“ ist die *MessageId* und „Y“ ist eine vom Adapter vergebene eindeutige Sequenznummer. Der Adapter erstellt eine Versandquittung pro im Umschlag explizit aufgeführten Empfänger, an den er eine Meldung verschickt. D.h. sind im Umschlag zwei Empfänger aufgeführt, erhält der Sender zwei Versandquittungen.

Der empfangende Adapter erstellt die folgenden Dateien, wenn er eine Meldung empfängt:

- den Umschlag als Datei „envl\_M.xml“
- die Nutzdaten als Datei „data\_M.xxx“

Bei "M" handelt es sich um einen vom empfangenden Adapter erzeugten, eindeutigen alphanumerischen Code. Die Korrelation von Umschlag zu Nutzdaten erfolgt durch die Verwendung desselben alphanumerischen Sequenzcodes.

Die Dateinamen bleiben beim Transport **nicht erhalten**. Einzig die Dateierweiterung der Nutzdaten, welchen den Dateityp bezeichnet, wird erhalten. Benötigt eine Anwendung aus irgendeinem Grund die Erhaltung eines bestimmten Dateinamens, so muss sie die Originaldatei in eine Zip-Datei verpacken und dann die Zip-Datei versenden.

### 3.4 Bereitstellung von Meldungen

Eine Meldung gilt dann als für den Versand (Sender an sendenden Adapter) bzw. für die Verarbeitung (empfangender Adapter an Empfänger) bereitgestellt, wenn im entsprechenden Verzeichnis die Umschlagsdatei angelegt ist.

Folgende plattform-unabhängige Strategie ist zu verwenden, um race conditions zu vermeiden:

- Erstelle die Nutzdatendatei im entsprechenden Verzeichnis gemäss Namenskonvention und schreibe die Daten hinein.
- Erstelle die Umschlagsdatei im entsprechenden Verzeichnis als temporäre Datei mit einem Namen, der nicht mit dem Namen des Umschlags gemäss Namenskonvention übereinstimmt (z.B. „tmp<processid>.xml“). Schreibe die Daten des Umschlags in die Datei.
- Benenne die Umschlagsdatei gemäss Namenskonvention um.

### 3.5 Zustände einer Meldung

Die Statechart in Abbildung 10 zeigt die Zustände, die eine sedex-Meldung aus der Sicht des sendenden Adapters durchläuft. Dabei wird der Zustand jeweils pro einzelnen Empfänger angesehen, an den die Meldung geschickt wurde.

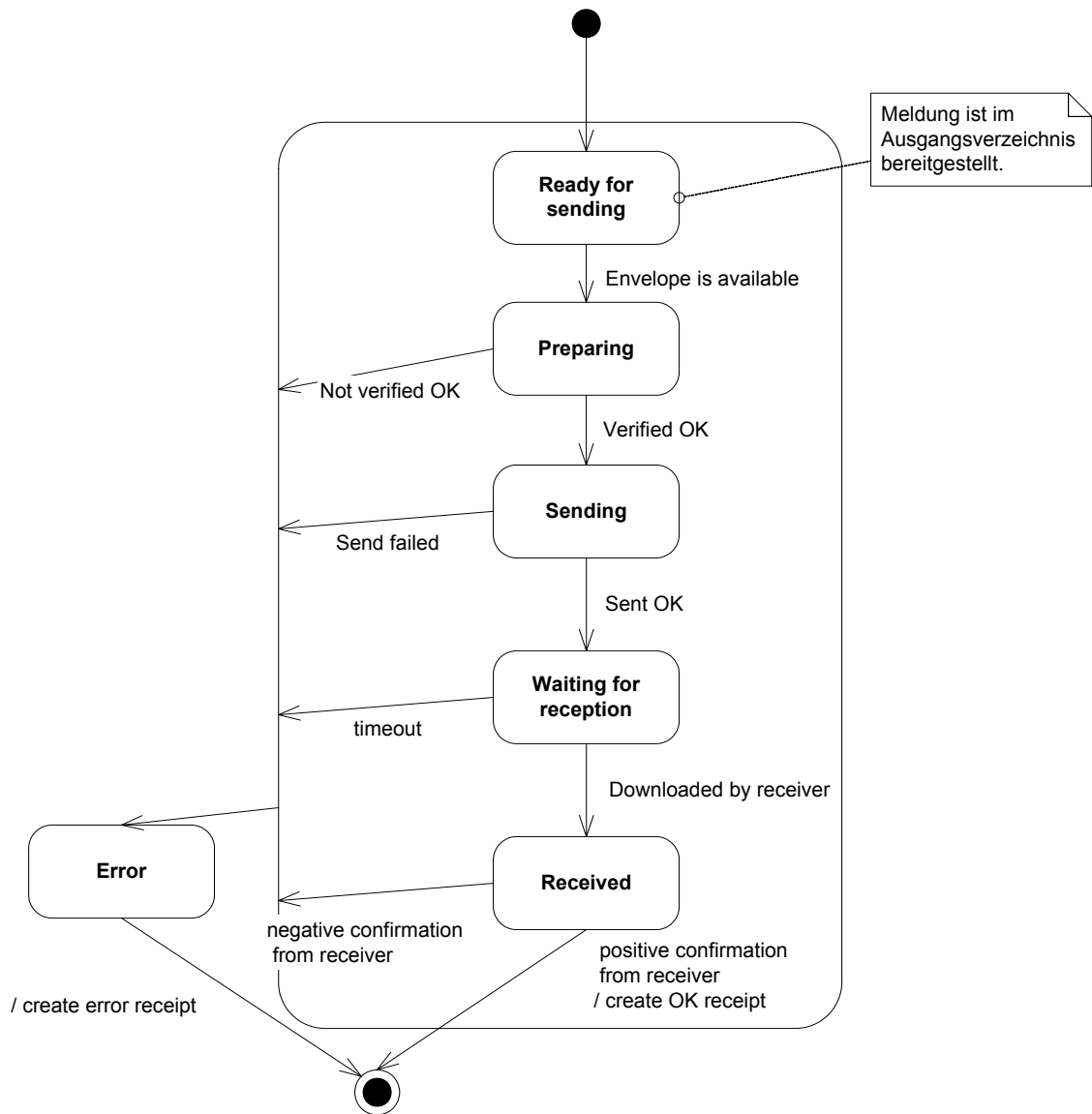


Abbildung 10: Zustände einer Meldung

### 3.6 Inhalt des Umschlags

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

Element-Name	Bedeutung	Typ	oblig.	Anzahl
message ID	<p><b>Sendende Anwendung</b> Diese ID wird von der sendenden Anwendung vergeben. Die Message ID muss in diesem Kontext eindeutig sein. Sie dient der sendenden Anwendung dazu, eine Meldung und eine Antwort auf diese Meldung zu korrelieren. Wenn sich mehrere Anwendungen denselben Adapter teilen, muss die Vergabe der Message ID zwischen den Anwendungen per Konvention geregelt werden (Range).</p> <p>Die Eindeutigkeit des Paares (Sender ID/Message ID) muss von der sendenden Anwendung verwaltet werden.</p> <p><b>sedex-Adapter</b> Im Kontext des sedex-Systems ist das Paar (Sender ID, Message ID) nicht immer eindeutig (siehe Kapitel 3.9.4).</p>	<p>String, der diesem regulären Ausdruck entspricht:  ([a-zA-Z]   [0-9]   -){1,36}</p> <p>d.h. Zeichenkette mit max 36 Zeichen, die Ziffern, Buchstaben oder Bindestriche enthalten kann. Die Zeichenkette ist lang genug, um eine UUID (vgl. RFC 4122) einen 64 Bit Integer oder eine Art von Schlüssel darzustellen.</p> <p>Bsp: f81d4fae-7dec-11d0-a765-00a0c91e6bf6</p>	ja	1
messageType	<p>Meldungstyp. Der Meldungstyp definiert die Funktion eines Datenpakets. Der Wertebereich ist in Nummerierungsbereiche unterteilt, die einer bestimmten Fachdomäne zugeordnet sind.</p> <p>Die Bedeutung der einzelnen Meldungstypen ist in [11] beschrieben. Der Meldungstyp definiert zusammen mit der Meldungsklasse (messageClass) implizit, welcher Art (Datentyp bzw. XML-Schema) die Nutzdaten der Meldung sind. Der Meldungstyp ist zusammen mit senderId und recipientId für das Routing der Meldung relevant.</p>	[0 .. 2699999] (Teilmenge von xs:int)	ja	1

Element-Name	Bedeutung	Typ	oblig.	Anzahl
messageClass	<p>Meldungsklasse. Definiert innerhalb eines Meldungstyps die Bedeutung der Meldung. Die folgenden Werte sind vordefiniert:</p> <ul style="list-style-type: none"> <li>• 0 = Message. Kennzeichnung der initialen Meldung.</li> <li>• 1 = Response. Kennzeichnet die Antwort auf eine Meldung.</li> <li>• 2 = Receipt. Kennzeichnet eine applikatorische Quittung (Empfangsbestätigung), welche eine empfangende Anwendung der sendenden Anwendung schickt. 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.</li> <li>• 3 = Error. Information von einer empfangenden an die sendende Anwendung, dass ihre Meldung nicht verarbeitet werden konnte.</li> <li>• 10 = reserviert für den Validierungsservice Kann bei Meldungstyp 99 für Teillieferungen verwendet werden (siehe [4])</li> <li>• 4-9 + 11 - maxint: reserviert für spätere Erweiterungen.</li> </ul>	xs:int	ja	1
referenceMessageld	Dieses Element wird von einer Anwendung gesetzt, wenn sie einer anderen Anwendung eine Antwort oder eine Fehlermeldung auf eine Meldung sendet. 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	nein	1
senderId	Absender der Meldung. Bezeichnet eindeutig die Amtsstelle, welche die Meldung sendet.	String. Aufgebaut gemäss Kap. 3.8	ja	1

Element-Name	Bedeutung	Typ	oblig.	Anzahl
recipientId	Empfänger der Meldung. Bezeichnet eindeutig die Amtsstelle, welche die Meldung empfangen soll.	String. Aufgebaut gemäss Kap. 3.8	ja	>0
eventDate	Ereignisdatum. Datum, an dem das Ereignis, auf welches sich die Nutzdaten beziehen, geschah. Das Ereignisdatum kann von der empfangenden Anwendung als Bestandteil der Nutzdaten (z.B. Wegzug, Zuzug, Stichtag Datenlieferung für die Statistik etc.) betrachtet werden.	xsd:dateTime	ja	1
messageDate	Versanddatum. Datum (Zeitstempel), an dem die sendende Anwendung die Meldung dem Adapter in den Ausgangsorder gelegt hat.	xsd:dateTime	ja	1
Loopback	Markiert die Meldung als eine Loopbackmeldung. Als Loopbackmeldung bezeichnen wir eine Meldung, die der empfangende Adapter für den Empfang wie eine herkömmliche Meldung behandelt (d.h. ggf. die Berechtigung des Sender prüft), sie aber nicht der empfangenden Anwendung zur Verarbeitung weiterleitet. Wird auch im produktiven Betrieb für Tests benötigt.	Leeres Inhaltsmodell mit einem Attribut ‚authorize‘. Das Attribut definiert, ob die sedex-Berechtigungsprüfung für diese Loopback-Meldung geprüft werden soll. Wird der Wert auf „true“ gesetzt, so kann die Meldung verwendet werden, um zu prüfen, ob ein Sender einem Empfänger eine Meldung eines bestimmten Typs senden darf. Wird der Wert auf „false“ gesetzt, so kann die Meldung für einen reinen Verbindungstest zwischen Adaptern verwendet werden (Ping).	nein	1
testData	Kann von einer sendenden Anwendung für Testzwecke verwendet werden, um den empfangenden Simulator zu steuern. Die Semantik der übergebenen Werte ist Sache des empfangenden Simulators.	Namen/Werte Paar	nein	>0

Das folgende XML-Dokument ist ein Beispiel eines Umschlags:

```
<?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>

```

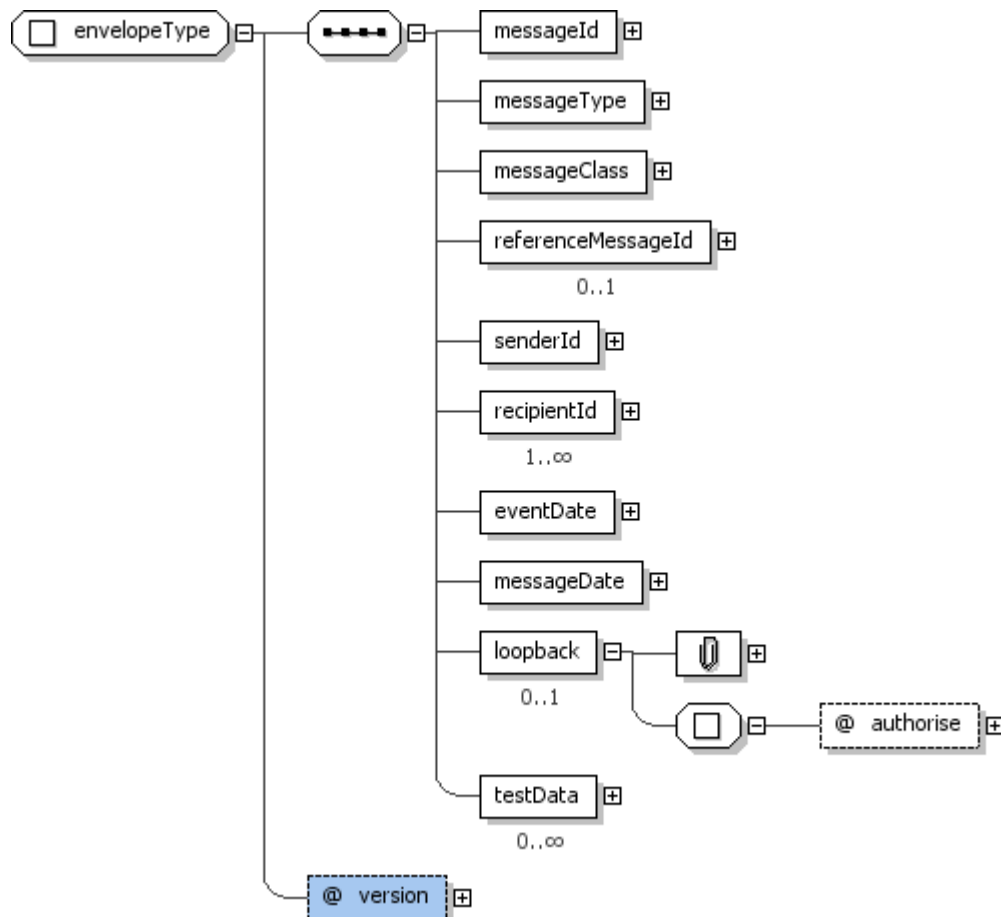


Abbildung 11: Grafische Darstellung des Inhaltsmodells des Umschlags

### 3.7 Inhalt der Quittung

Die Quittung wird vom Adapter pro Empfänger einer Meldung ausgestellt, d.h. sendet der Sender eine Meldung an zwei Empfänger, so bekommt er zwei Quittungen. Ausnahme: bei Publish/Subscribe wird nur eine einzige Quittung erstellt, welche den erfolgreichen Empfang durch das Sedex System signalisiert.

Die Quittung enthält die folgenden Elemente:

Element-Name	Bedeutung	Typ	oblig.	Anzahl
eventDate	Zeitpunkt des Ereignisses, welches zu der Quittung führt. Z.B. Zeitpunkt, wann die Meldung beim empfangenden Adapter angekommen ist oder wann der Übermittlungsfehler aufgetreten ist.	xsd:dateTime	ja	1
statusCode	Status der Meldung: OK oder Fehlercode	Aufzählung auf Basis von xsd:int Mögliche Werte siehe Kap. 3.9	ja	1
statusInfo	Infotext zum Statuscode. Enthält allfällige weitere Informationen, die für den Systemmenschen interessant sein könnten.	xsd:string, maxlength=255 Mögliche Werte siehe Kap. 3.9	ja	1
messageId	ID der Meldung, auf die sich die Quittung bezieht	gleich wie in Umschlag	ja	1
messageType	Meldetyp der Meldung, auf die sich die Quittung bezieht	gleich wie in Umschlag	ja	1
messageClass	Meldungsklasse der Meldung, auf die sich die Quittung bezieht	gleich wie in Umschlag	ja	1
senderId	Absender der Meldung, auf die sich die Quittung bezieht	gleich wie in Umschlag	ja	1
recipientId	Empfänger der Meldung, auf die sich die Quittung bezieht	Gleich wie in Umschlag. Beachte: in der Quittung erscheint immer die recipientId, wie sie im Umschlag angegeben wurde. Dies auch dann, wenn der Adapter die Meldung in Folge der Routing-Regeln an einen anderen Empfänger (z.B. eine zentrale kantonale Plattform) gesendet hat.	ja	1

Das folgende XML-Dokument zeigt ein Beispiel einer Versandquittung zu der Meldung, die mit dem Umschlag aus dem vorhergehenden Kapitel verschickt wurde und beim Empfänger angekommen ist.

```
<?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>
```

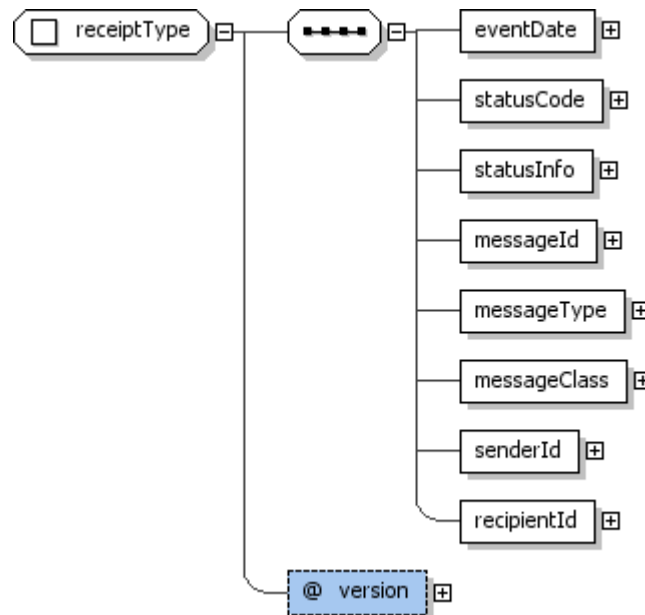


Abbildung 12: Grafische Darstellung des Inhaltsmodells der Quittung

## 3.8 Adressierung

### 3.8.1 Übersicht

Teilnehmer im sedex-Verbund sind zum Beispiel Systeme der Amtsstellen von Gemeinden, Kantonen und des Bundes. Teilnehmer im sedex-Verbund sind durch eine eindeutige ID gekennzeichnet. Um den teilnehmenden Systemen die Adressierung der Teilnehmer im Verbund zu vereinfachen, definiert sedex eine einfach aufgebaute logische Teilnehmer-ID. Das sedex-System bildet diese Teilnehmer-ID unter Verwendung des sedex-Teilnehmerverzeichnisses auf den konkreten Teilnehmer sowie das ihm zugewiesene Zertifikat ab.

Die Teilnehmer-ID ist eine Zeichenkette<sup>4</sup>, die wie folgt aufgebaut ist:

Teilnehmer-ID ::= <bereich> "-" <organisationseinheit> "-" <funktionscode>.

### 3.8.2 Bereiche und Organisationseinheiten

Die Bereichsnummer definiert einen „Namensraum“ im Adressbereich von sedex. Innerhalb eines Bereiches können einzelne Organisationseinheiten und Funktionen innerhalb dieser Organisationseinheiten adressiert werden.

<sup>4</sup> Aktuell ist die Länge der Teilnehmer-ID aus technischen Gründen auf 20 Zeichen beschränkt. In Zukunft wird diese Beschränkung aber voraussichtlich fallen.

Bereich	Bedeutung	Wertebereich für die Organisationseinheit
0	sedex Für das sedex-System reservierter Bereich. Dient der Adressierung der sedex-eigenen Dienste.	Einziger möglicher Wert: sedex
1	Gemeinde Bezeichnet eine Gemeinde.	Zulässige Werte sind die BFS-Nummern der politischen Gemeinden gemäss [3], z.B. 351 für Bern.
2	Kanton Bezeichnet einen Kanton.	Zulässige Werte sind die zweistelligen Kantonskürzel gemäss [3], z.B. SO für Solothurn.
3	Bund Bezeichnet eine Bundesstelle oder eine Applikation des Bundes.	Einziger möglicher Wert: CH
4	EBS-TV. Bezeichnet Event Bus Schweiz.	Der Wertebereich ist gemäss [12], Kapitel 1.3.8 festgelegt und enthält zwei Informationen : Teilbus-Identifikator und Teilnehmer-Identifikator.
5	Bezirk Bezeichnet einen Bezirk eines Kantons.	Zulässige Werte sind die BFS-Nummern der Bezirke gemäss [3].
6	Sozialversicherungsunternehmen Bezeichnet eine AHV Ausgleichskasse oder eine IV-Stelle.	Vom Bundesamt für Sozialversicherung (BSV) an Ausgleichskassen/Zweigstellen, IV-Stellen, EL-Stellen, Militär und Mitinteressierte vergebene 6-stellige Nummer.
7	Privatunternehmen Bezeichnet ein privatrechtliches Unternehmen.	Zulässige Werte sind die vom BFS den an sedex teilnehmenden Firmen zugeordneten, nicht sprechenden Nummern, z.B. 1 für TI Informatique.
8	eSchKG Bezeichnet die Betreibungsämter und Gläubiger die an den eSchKG-Verbund gehören.	Zulässige Werte sind die zweistelligen Kantonskürzel gemäss [3], z.B. SO für Solothurn.
9	reserviert	

Im sedex-Teilnehmerverzeichnis können ausgezeichnete Teilnehmer definiert werden, die nur zu Testzwecken dienen. Die ID dieser Teilnehmer wird mit einem Präfix „T“ versehen. Testteilnehmer können nur mit anderen Testteilnehmern kommunizieren.

### 3.8.3 Funktionscode

Der Funktionscode bezeichnet die Geschäftsfunktion, die ein teilnehmendes System wahrnimmt. Die Geschäftsfunktionen, bzw. ihre Codes, sind pro Bereich definiert, d.h., dass die gleichen Funktionscodes in unterschiedlichen Bereichen unterschiedliche Geschäftsfunktionen bezeichnen können. Aktuell sind die nachfolgenden Funktionscodes zugeteilt:

### 3.8.3.1 Bereich System

Bereich	Funktionscode	Geschäftsfunktion / Bedeutung
0	0	Das sedex-System
0	1	Das sedex-Monitoring-System

Im Bereich 0 (sedex) werden vom BFS weitere Nummern ausschliesslich für Bedürfnisse des sedex-Systems vergeben.

### 3.8.3.2 Bereich Gemeinde

Bereich	Funktionscode	Geschäftsfunktion / Bedeutung
1	1	Einwohnerregister (EWR)
1	2	Informatik
1	3	Statistik
1	4	-
1	5	Steuerverwaltung
1	6	Bürger- bzw. Bürgergemeinde
1	7	-
1	8	Gläubiger

Der Nummernbereich > 5 ist für gemeindeübergreifende Funktionen reserviert. Die Nummern werden vom BFS vergeben.

### 3.8.3.3 Bereich Kanton

Bereich	Funktionscode	Geschäftsfunktion / Bedeutung
2	1	Einwohnerregister (EWR)
2	2	Informatik
2	3	Statistik
2	4	Handelsregister
2	5	Steuerverwaltung
2	6	-
2	7	Militärverwaltung
2	8	Gläubiger

Bereich	Funktionscode	Geschäftsfunktion / Bedeutung
2	9	Betreibungsamt

Im Bereich 2 (Kanton) sind die folgenden Nummernbereiche reserviert:

- Der Nummerbereich 1000 - 26999 ist für spätere Erweiterungen durch die einzelnen Kantone reserviert. Die Nummerierung ist analog zum Meldungstyp, d.h. der Präfix entspricht der BFS-Nummer des Kantons. Beispiel: über den Nummernbereich 1000 - 1999 kann der Kanton Zürich für seine eigenen Bedürfnisse frei verfügen.

#### 3.8.3.4 Bereich Bund

Bereich	Funktionscode	Geschäftsfunktion / Bedeutung
3	1	Bundesamt für Statistik
3	2	Bundesamt für Statistik (nur amtsinterne Verwendung)
3	3	ZAS UPI DB DMZ
3	4	InfoStar
3	5	ZEMIS
3	6	ORDIPRO
3	7	VERA
3	8 - 17	Bundesamt für Statistik (nur amtsinterne Verwendung)

Die Nummernbereiche sind für die Geschäftsfunktionen des Bundes reserviert. Die Nummern werden vom BFS vergeben. Die Nummern werden „historisiert“, d.h. eine einmal vergebene Nummer wird nach deren Freigabe (z.B. Ablösung der entsprechenden Anwendung) nicht wieder verwendet.

#### 3.8.3.5 Bereich Bezirk

Bereich	Funktionscode	Geschäftsfunktion / Bedeutung
5	1	Betreibungsamt

### 3.8.3.6 Bereich Privatunternehmen

Bereich	Funktionscode	Geschäftsfunktion / Bedeutung
7	1	1. sedex-Adapter
7	2	2. sedex-Adapter
7	N	n. sedex-Adapter

Im Bereich 7 (Privatfirmen) werden mit dem Funktionscode die sedex-Adapter einer Firma durchnummeriert. Die Nummerierung erfolgt durch das BFS und ist nicht-sprechend. Weitere Funktionscodes werden vom BFS angelegt, wenn Firmen mehr als zwei Adapter einsetzen wollen.

### 3.8.3.7 Bereich Sozialversicherungsunternehmen

Im Bereich 6 (Sozialversicherungsunternehmen) wird der Funktionscode nach dem gleichen Prinzip wie bei Privatfirmen (Bereich 7, siehe Kapitel 3.8.3.6) angewandt.

### 3.8.3.8 Bereich eSchKG

Im Bereich 8 (eSchKG) wird der Funktionscode nach dem gleichen Prinzip wie bei Privatfirmen (Bereich 7, siehe Kapitel 3.8.3.6) angewandt.

### 3.8.4 Beispiele

- 0-sedex-0 bezeichnet das sedex-System selbst.
- 1-351-1 bezeichnet das EWR der politischen Gemeinde Bern.
- 1-351-6 bezeichnet das EWR der Burgergemeinde Bern
- 2-SO-1 bezeichnet das EWR des Kantons Solothurn.
- 2-GL-2 bezeichnet die Dienststelle Informatik des Kantons Glarus.
- 3-CH-5 bezeichnet das Zentrale Migrationsinformationssystem (ZEMIS) des EJPD.
- T3-CH-1 bezeichnet die Testinstanz des Bundesamtes für Statistik.
- 7-1-1 bezeichnet den 1. sedex-Adapter der Firma TI Informatique.
- 8-TG-1 bezeichnet das erste, an sedex angeschlossene Betriebsamt des Kantons Thurgau.

## 3.9 Fehlerkategorien und Statuscodes

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.

Eine Anwendung muss auch mit ihr noch unbekanntem Codes umgehen können, indem sie diese entweder gemäss ihrer Kategorie behandelt oder eventuell ignoriert (abhängig von ihrer Kategorie, z.B. für Informationen / Warnungen).

### 3.9.1 Fehlerkategorien

Die Statuscodes, die bei der Übermittlung auftreten können, lassen sich wie folgt kategorisieren:

Kategorie	Subkategorie	Statuscodes	Erläuterung
<b>Erfolg</b>	Bsp: eine Nachricht ist erfolgreich übermittelt worden.	100 - 199	Bestätigungen der erfolgreichen Übermittlung <b>Verhalten:</b> Anwender benachrichtigen
<b>Permanenter Fehler</b>	<b>Message Error</b> Bsp: der Umschlag einer Nachricht ist ungültig.	200 - 299	Ein Problem mit der Meldung oder der Autorisierung selber liegt vor. Ein erneuter Sendeversuch ohne Veränderung der Gegebenheiten wird wieder zum selben Fehler führen.
	<b>Authorisation Error</b> Bsp: ein Empfänger aus dem Envelope ist nicht autorisiert.	300 - 399	<b>Verhalten:</b> vor einem erneuten Senden das Problem beheben bzw. den Anwender informieren.
<b>Temporärer Fehler</b>	<b>Transport Error</b> Bsp: der Autorisierungsserver steht momentan nicht zur Verfügung.	400 - 499	Auf der Transportebene oder bei den Adaptern ist ein Problem aufgetreten. <b>Verhalten:</b> Meldung nach einer Wartezeit nochmals senden.
	<b>Adapter Error</b> Bsp: dem Adapter steht nicht genügend Speicherplatz zur Verfügung.	500 - 599	
<b>Information</b>	<b>Update</b> 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. <b>Verhalten:</b> die Information kann ausgewertet oder ignoriert werden.

Kategorie	Subkategorie	Statuscodes	Erläuterung
	<b>Warning</b> Bsp: der Empfänger hat nur noch wenige Tage Zeit, um die Meldung herunter zu laden.	700 - 799	Zu einer versendeten Meldung liegt eine Warnung vor. <b>Verhalten:</b> die Warnung kann ausgewertet oder ignoriert werden.

### 3.9.2 Statuscodes

Die folgenden Statuscodes sind für die Quittung definiert:

Subkategorie	Wert	zugehörige Meldung	Bedeutung	Quelle <sup>5</sup>	Seit <sup>6</sup>
Success	100	Message correct transmitted	Meldung ist korrekt und vollständig übermittelt worden.	EA	1.0
Message Error	200	Invalid envelope syntax	Der Umschlag entspricht nicht dem erwarteten XML-Schema für Umschläge bzw. liegt in einer nicht erwarteten Version vor. Siehe auch Kap. 3.9.1.	SA EA	1.0
	201	Duplicate message ID	Der Umschlag enthält eine Meldungs-ID, die der Adapter in seiner Status-Datenbank schon führt (siehe Kapitel 3.9.4).	SA	1.0
	202	No payload found	Eine sedex-Meldung besteht immer aus zwei Dateien: Umschlag und Nutzdaten (siehe Kap. 3.1). Die sendende Anwendung hat nur einen Umschlag, aber keine Nutzdaten bereitgestellt.	SA	1.0
	203	Message too old to send	Message Date im Umschlag ist älter als 30 Tage.	SA	2.0
	204	Message expired	Der Empfänger hat die Meldung nicht innerhalb des von sedex geforderten Zeitraumes von einem Monat abgeholt.	SA	2.0
Authorisation Error	300	Unknown sender id %s	Die im Umschlag angegebene senderId ist im sedex-TV nicht bekannt.	SA	1.0

<sup>5</sup> Als Quelle wird der Adapter bezeichnet. SA = sender Adapter, EA = empfangender Adapter

<sup>6</sup> Der Statuscode wurde mit folgendem Adapter-Release eingeführt

Subkategorie	Wert	zugehörige Meldung	Bedeutung	Quelle <sup>5</sup>	Seit <sup>6</sup>
	301	Unknown recipient id %s	Die im Umschlag angegebene recipientId ist im sedex-TV nicht bekannt.	SA	1.0
	302	Unknown physical sender id %s	Die im Adapter konfigurierte ID des Adapters ist im sedex-TV nicht bekannt (kann nur bei zentralisierten Infrastrukturen auftreten).	SA	1.0
	303	Invalid message type %s	Der im Umschlag aufgeführte Meldungstyp ist nicht bekannt.	SA	1.0
	304	Invalid message class %s	Die im Umschlag aufgeführte Meldungsklasse ist nicht bekannt.	SA	1.0
	310	Not allowed to send	Dieser Absender darf diese Meldung nicht senden.	SA	1.0
	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	1.0
	312	User certificate not valid	Das Zertifikat des Teilnehmers ist entweder annulliert worden, oder es ist ungültig.	SA	1.0
	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	2.0
	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 die erlaubte Grösse für diesen MessageType.	SA	2.0
Transport Error	400	Network error	Allgemeines Netzwerkproblem	SA	1.0
	401	OSCI hub not reachable	Keine Verbindung zum OSCI-Intermediär möglich	SA	1.0
	402	Directory not reachable	Die sedex-Liste ist nicht erreichbar.	SA	1.0

Subkategorie	Wert	zugehörige Meldung	Bedeutung	Quelle <sup>5</sup>	Seit <sup>6</sup>
	403	Logging service not reachable	Das sedex-Logging ist nicht erreichbar.	SA	1.0
	404	Authorisation service not reachable	Der Autorisierungsservice von sedex ist nicht verfügbar	SA	2.0
Adapter Error	500	Internal error: %s	Der Adapter kann die Daten nicht senden, weil ein interner Fehler aufgetreten ist. Weitere Informationen stehen angefügt (%s ersetzen). Details zum Fehler sind dem Log des Adapters zu entnehmen.	SA	1.0
	501	Error during receiving	Beim Empfangen der Meldung ist ein Fehler aufgetreten, der Empfänger konnte die Meldung nicht rekonstruieren.	EA	2.0
Partial Success	601	Message successfully sent	Die Meldung wurde erfolgreich dem Intermediär übergeben. <sup>7</sup>	SA	2.0
Warning	701	Message expires soon	Der empfangende Adapter hat nur noch 7 Tage Zeit, die Meldung vom Intermediär herunterzuladen.	SA	2.0

### 3.9.3 Verhalten bei nicht korrektem Umschlag (Status 200)

Übergibt die sendende Anwendung dem Adapter einen syntaktisch nicht korrekten Umschlag (d.h. der Umschlag kann nicht gegen das Schema eCH-0090 validiert werden -> Statuscode 200), so ist der Adapter unter Umständen nicht in der Lage, allfällig darin enthaltene Informationen über Absender, Empfänger etc. zu extrahieren.

Dies gilt auch für empfangene Meldungen, wenn deren Umschlagsdatei nicht mit der Schema-Version des empfangenden Adapters kompatibel ist.

Der Adapter wird in diesem Fall unabhängig von der Anzahl der im Umschlag aufgeführten Empfänger eine einzige Versandquittung ausstellen, die nachstehende Werte enthält.

Wenn immer möglich, wird der Adapter versuchen, die *messageId* zu erkennen, um die Fehleranalyse zu vereinfachen. Ist dies nicht möglich, wird der Filename der Umschlagsdatei im Element „statusInfo“ mitgegeben.

<sup>7</sup> Diese Quittung, die das erfolgreiche Senden der Meldung an den sedex-Server bestätigt, ist konfigurierbar, aber defaultmässig ausgeschaltet.

Die Quittung für einen Status „200“ enthält somit folgende Elemente:

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

### 3.9.4 Behandlung von Message ID-Dubletten (Statuscode 201)

Der sedex-Adapter garantiert die Eindeutigkeit der Message ID bis zur Meldungankunft beim Empfänger. Der Adapter speichert alle mit dem sedex-Umschlag verbundenen Informationen bis zur Ankunft der Meldung. Solange diese Nachricht gespeichert ist, ist keine andere Nachricht mit der selben Message ID für die Sendung akzeptiert und wird eine Quittung mit dem code 201 erzeugen.

Nach der generierten technischen Quittung (für die gesandte Meldung) ist es möglich, eine weitere Nachricht mit dem gleichen Identifikator zu senden. Diese neue Sendung ist nur möglich nach dem Ausführen des geplanten Jobs, der alle 5 Minuten die interne Adapter-Datenbank leert.

### 3.9.5 Verhalten bei Netzwerkfehlern

Tritt ein Netzwerkfehler auf, so wird der Adapter für die Dauer der im Adapter konfigurierten Retry Periode wiederholt versuchen, die Meldung zu versenden. Erst nach Ablauf dieser Periode wird er eine Versandquittung mit Fehlerstatus der Kategorie „Network“ ausstellen.

Tritt im Adapter ein interner Fehler auf, so wird er diesen sofort mit einer Versandquittung mit Fehlerstatus „500“ melden.

### 3.9.6 Berechnung des Verfalldatums einer Meldung (Statuscodes 203, 204 und 701)

Meldungen müssen innerhalb eines Monats vom empfangenden Adapter abgeholt werden. Massgebend ist das Element /eCH-0090:envelope/messageDate, unabhängig davon, ob dieses dem tatsächlichen Zeitpunkt des Versands entspricht bzw. entsprochen hatte.

sedex macht aus diesem Grund folgende Validierungen:

- Beim Versand der Meldung: *messageDate* darf nicht kleiner als aktueller Zeitpunkt minus 30 Tage sein → Statuscode „203 Message too old to send“ an sendenden Adapter.
- Auf dem Server: *messageDate* gleich aktueller Zeitpunkt minus 30 Tage plus 7 Tage → Statuscode „701 Message expires soon“ an sendenden Adapter.
- Auf dem Server: *messageDate* gleich aktueller Zeitpunkt minus 30 Tage → Statuscode „204 message expired“ an sendenden Adapter.

Der Statuscode „701“ ist als Warnung an den Sender zu verstehen und gibt ihm die Möglichkeit, beim Empfänger allenfalls zu intervenieren, damit dieser die Meldung noch abholen bzw. den Betrieb seines Adapter noch überprüfen kann.

Erhält der Sender nach dem Versand den Statuscode „204“ (anstelle „100“), kann die Meldung vom Empfänger endgültig nicht mehr heruntergeladen werden. Gegebenenfalls muss der Geschäftsfall in der partizipierenden Anwendung erneut angestossen werden.

## 3.10 Technische Sicht der Kommunikation

### 3.10.1 Verzeichnis-Verwaltung

Die Installation des sedex-Adapters erfordert die Erstellung mehrerer Verzeichnisse. Nur vier Verzeichnisse sind spezifisch für den Meldungs austausch (Versand-Empfang) und die Verwaltung der Quittungen vorgesehen:

- outbox (zu versendende Meldungen)
- inbox (empfangene Meldungen)
- sent (bearbeitete Meldungen)
- receipts (sedex-Quittungen)

Die anderen, für den Betrieb des sedex-Adapters erstellten Verzeichnisse (temporary folders, conf, bin usw.), sind für die sendende Anwendung nicht wichtig. Der Inhalt dieser Verzeichnisse hat aber bei der Installation, dem Aufstarten und Herunterfahren, den Updates usw. des Adapters eine wichtige Bedeutung.

### 3.10.2 Versand einer sedex-Meldung

Beim Versand einer sedex-Meldung führt der sedex-Adapter die einzelnen Aufgaben in folgender Reihenfolge durch:

1. Alle 30 Sekunden, Polling (periodisches Abfragen) des Outbox-Verzeichnisses im Dateisystem, in welches die sendende Anwendung die zu versendenden Meldungen einschreibt
2. Sobald der Adapter eine Meldung (Umschlag und Payload) vorfindet, wird der Umschlag geöffnet und gegen das XML-Schema validiert.
3. Verbindung mit dem sedex-Server zur Überprüfung der Nutzdaten (aktive Teilnehmer, Zertifikat, Autorisierung, Routing-Regeln usw.)

4. Die Dateien der Meldung werden verschoben:
  - a) in die temporären Adapter-Verzeichnisse zum Versand
  - b) in das Sent-Verzeichnis zur Archivierung
5. Die Meldung wird vom Adapter signiert, mit dem Zertifikat des Empfängers verschlüsselt und an den sedex-Server übermittelt.
6. Sobald der Empfänger die Meldung heruntergeladen hat, stellt der Adapter eine technische Quittung mit dem Versandstatus aus. Diese Quittung wird der sendenden Anwendung über das Receipts-Verzeichnis zur Verfügung gestellt.

Die Abbildung 13 zeigt die beschriebenen Schritte :

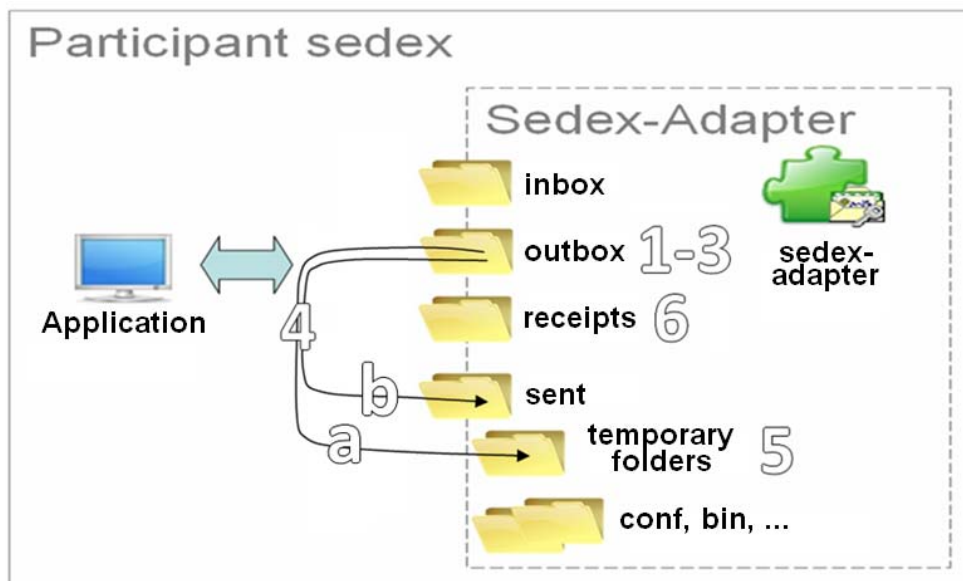


Abbildung 13: Schritte des Versandes einer Meldung

### 3.10.3 Empfang einer sedex-Meldung

Beim Empfang einer sedex-Meldung führt der sedex-Adapter die einzelnen Aufgaben in folgender Reihenfolge durch:

1. Überwachung der inbox auf dem sedex-Server (alle 5 Minuten)
2. Teil-Download der Meldung in das temporary folders-Verzeichnis heruntergeladen
3. Sicherheitskontrollen (Signatur, Verschlüsselung, Autorisierung)
4. Fortsetzung des Downloads in das temporary folders-Verzeichnis
5. Sobald die Datei entschlüsselt wurde, wird sie in das inbox-Verzeichnis verschoben.
6. Der Status der Meldung wird auf dem sedex-Server aktualisiert und dem Empfänger eine technische Quittung ausgestellt.

## 3.11 Beispiele

Dieser Abschnitt zeigt Beispiele von sedex-Umschlägen und Quittung anhand konkreter Use Cases. Aus Platzgründen wurden in den Beispielen die Referenzen auf die XML-Schema-Dateien (xsi:schemaLocation) weggelassen. Die Sequenzdiagramme für diese Beispiele befinden sich in [4].

### 3.11.1 Beispiel: Lieferung der Gemeinde Olten an die Statistik

Im folgenden Beispiel liefert die Gemeinde Olten (sedex ID: 1-2581-1) am 21.01.2011 mit Stichdatum 31.12.2010 Statistikdaten an das BFS (sedex ID: 3-CH-1).

Meldung 1: Lieferung Gesamtbestand von Olten an BFS (*eventDate* bezeichnet das Stichdatum der Lieferung, *messageDate* bezeichnet den Zeitpunkt der Erstellung der Meldung an das BFS):

```
<?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"
  version="1.0">
  <messageId>550e8400-e29b-11d4-a716-446655440000</messageId>
  <messageType>99</messageType>
  <messageClass>0</messageClass>
  <senderId>1-2581-1</senderId>
  <recipientId>3-CH-1</recipientId>
  <eventDate>2010-12-31T00:00:00</eventDate>
  <messageDate>2011-01-21T12:34:56</messageDate>
</envelope>
```

Quittung zu Meldung 1 (ausgestellt vom sedex-Adapter der Gemeinde Olten; *eventDate* bezeichnet den Zeitpunkt der Auslieferung der Meldung an das BFS):

```
<?xml version="1.0" encoding="UTF-8"?>
<receipt xmlns="http://www.ech.ch/xmlns/eCH-0090/1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  version="1.0">
  <eventDate>2011-01-21T12:45:00Z</eventDate>
  <statusCode>100</statusCode>
  <statusInfo>Message correct transmitted</statusInfo>
  <messageId>550e8400-e29b-11d4-a716-446655440000</messageId>
  <messageType>99</messageType>
  <messageClass>0</messageClass>
  <senderId>1-2581-1</senderId>
  <recipientId>3-CH-1</recipientId>
</receipt>
```

Meldung 2: Fachliche Quittung von BFS an Gemeinde Olten:

```
<?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"
  version="1.0">
  <messageId>13</messageId>
  <messageType>99</messageType>
  <messageClass>2</messageClass>
  <referenceMessageId>550e8400-e29b-11d4-a716-446655440000</referenceMessageId>
  <senderId>3-CH-1</senderId>
  <recipientId>1-2581-1</recipientId>
```

```
<eventDate>2010-12-31T00:00:00</eventDate>  
<messageDate>2011-01-21T13:00:00</messageDate>  
</envelope>
```

**Quittung zu Meldung 2 (erstellt vom Adapter des BFS):**

```
<?xml version="1.0" encoding="UTF-8"?>
<receipt xmlns="http://www.ech.ch/xmlns/eCH-0090/1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  version="1.0">
  <eventDate>2011-01-21T13:15:00Z</eventDate>
  <statusCode>100</statusCode>
  <statusInfo>Message correct transmitted</statusInfo>
  <messageId>13</messageId>
  <messageType>99</messageType>
  <messageClass>2</messageClass>
  <senderId>3-CH-1</senderId>
  <recipientId>1-2581-1</recipientId>
</receipt>
```

**Meldung 3: Antwort des BFS an die Gemeinde Olten:**

```
<?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"
  version="1.0">
  <messageId>48</messageId>
  <messageType>99</messageType>
  <messageClass>1</messageClass>
  <referenceMessageId>550e8400-e29b-11d4-a716-446655440000</referenceMessageId>
  <senderId>3-CH-1</senderId>
  <recipientId>1-2581-1</recipientId>
  <eventDate>2010-12-31T00:00:00</eventDate>
  <messageDate>2011-01-22T06:00:00</messageDate>
</envelope>
```

**Quittung zu Meldung 3 (erstellt vom Adapter des BFS):**

```
<?xml version="1.0" encoding="UTF-8"?>
<receipt xmlns="http://www.ech.ch/xmlns/eCH-0090/1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  version="1.0">
  <eventDate>2011-01-22T14:13:02Z</eventDate>
  <statusCode>100</statusCode>
  <statusInfo>Message correct transmitted</statusInfo>
  <messageId>48</messageId>
  <messageType>99</messageType>
  <messageClass>1</messageClass>
  <senderId>3-CH-1</senderId>
  <recipientId>1-2581-1</recipientId>
</receipt>
```

### 3.11.2 Beispiel: Nomenklatur-Update des BFS an interessierte sedex Teilnehmer

Dieses Beispiel illustriert das Publish/Subscribe-Szenario anhand der Publikation des Updates der Nomenklatur „Historisiertes Gemeindeverzeichnis“ durch das BFS.

Umschlag zur Meldung vom BFS an sedex zwecks Publikation:

```
<?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"
  version="1.0">
  <messageId>51</messageId>
  <messageType>71</messageType>
  <messageClass>0</messageClass>
  <senderId>3-CH-1</senderId>
  <recipientId>0-sedex-0</recipientId>
  <eventDate>2008-02-01T00:00:00</eventDate>
  <messageDate>2008-01-01T06:00:00</messageDate>
</envelope>
```

Der Adapter des BFS bestätigt dem BFS den Empfang der Meldung durch das sedex-System:

```
<?xml version="1.0" encoding="UTF-8"?>
<receipt xmlns="http://www.ech.ch/xmlns/eCH-0090/1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  version="1.0">
  <eventDate>2008-01-01T12:15:00Z</eventDate>
  <statusCode>100</statusCode>
  <statusInfo>Message correct transmitted</statusInfo>
  <messageId>51</messageId>
  <messageType>71</messageType>
  <messageClass>0</messageClass>
  <senderId>3-CH-1</senderId>
  <recipientId>0-sedex-0</recipientId>
</receipt>
```

Der Umschlag zu der vom sedex-System weitergeleiteten Meldung, wie er bei einer fiktiven, direkt an sedex angeschlossenen, Gemeinde mit sedex-Teilnehmer-ID 1-9999-1 ankommt.

```
<?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"
  version="1.0">
  <messageId>b9d29749-2e72-4e0b-b08a-c3c4fc773312</messageId>
  <messageType>71</messageType>
  <messageClass>0</messageClass>
  <senderId>3-CH-1</senderId>
  <recipientId>1-9999-1</recipientId>
  <eventDate>2008-02-01T00:00:00</eventDate>
  <messageDate>2008-01-01T06:00:00</messageDate>
</envelope>
```

Der Umschlag zu der vom sedex-System weitergeleiteten Meldung, wie er bei einer indirekt an sedex angeschlossenen Gemeinde ankommt. Die fiktive Gemeinde mit sedex-Teilnehmer-ID 1-9900-1 wird zusammen mit der fiktiven Gemeinde 1-9901-1 vom gleichen physischen sedex Teilnehmer bedient.

```
<?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"
  version="1.0">
  <messageId>d2f0489e-8d0c-4fe7-a15e-69c63081c37d</messageId>
  <messageType>71</messageType>
  <messageClass>0</messageClass>
  <senderId>3-CH-1</senderId>
  <recipientId>1-9900-1</recipientId>
  <recipientId>1-9901-1</recipientId>
  <eventDate>2008-02-01T00:00:00</eventDate>
  <messageDate>2008-01-01T06:00:00</messageDate>
</envelope>
```

## 3.12 Webservice-Proxy

### 3.12.1 Zweck des Webservice-Proxy

Partizipierende Anwendungen können Webservices verwenden, ohne sich selbst gegenüber dem Dienstbringer explizit authentisieren oder sich um die Verschlüsselung der Daten kümmern zu müssen. Die Authentisierung und Verschlüsselung erfolgt automatisch durch sedex, unter Verwendung des Organisationszertifikats des Adapters. Dazu bietet sedex einen Webservice-Proxy an, welcher die Endpunkte der Dienstbringer clientseitig repliziert.

### 3.12.2 Funktionsweise des Webservice-Proxy

Der Webservice-Proxy nimmt auf der sedex-Clientseite Webservice-Aufrufe für bestimmte Endpunkte entgegen, authentisiert und verschlüsselt diese je nach Vorgabe und leitet die Aufrufe an die Endpunkte der eigentlichen Dienstbringer weiter. Die Antworten der Dienstbringer werden vom Webservice-Proxy bei Bedarf authentifiziert und entschlüsselt und an den ursprünglichen Aufrufer weitergegeben. Die Abbildung 14 stellt diesen Ablauf schematisch dar.

### 3.12.3 Nachrichtenaustausch

Der Nachrichtenaustausch, welcher über den Webservice-Proxy geführt wird, ist synchron. Für den asynchronen Nachrichtenaustausch steht der Adapter zur Verfügung.

Der Webservice-Proxy nimmt auf einer Nachricht, welche an einen seiner Endpunkte gerichtet wird, keine Transformationen ausser der verlangten Verschlüsselung/Signierung vor, d.h. Nachrichten werden inhaltlich 1:1 an den Dienstbringer weitergeleitet. Dasselbe gilt analog für die Rückantwort des Dienstbringers.

Der Webservice-Proxy nimmt keine Autorisierung vor. Dies ist alleinige Sache der Dienstbringer. Es werden allerdings nur Services vom Webservice-Proxy unterstützt, welche das Organisationszertifikat des sedex-Adapters als Autorisierungsmerkmal akzeptieren.

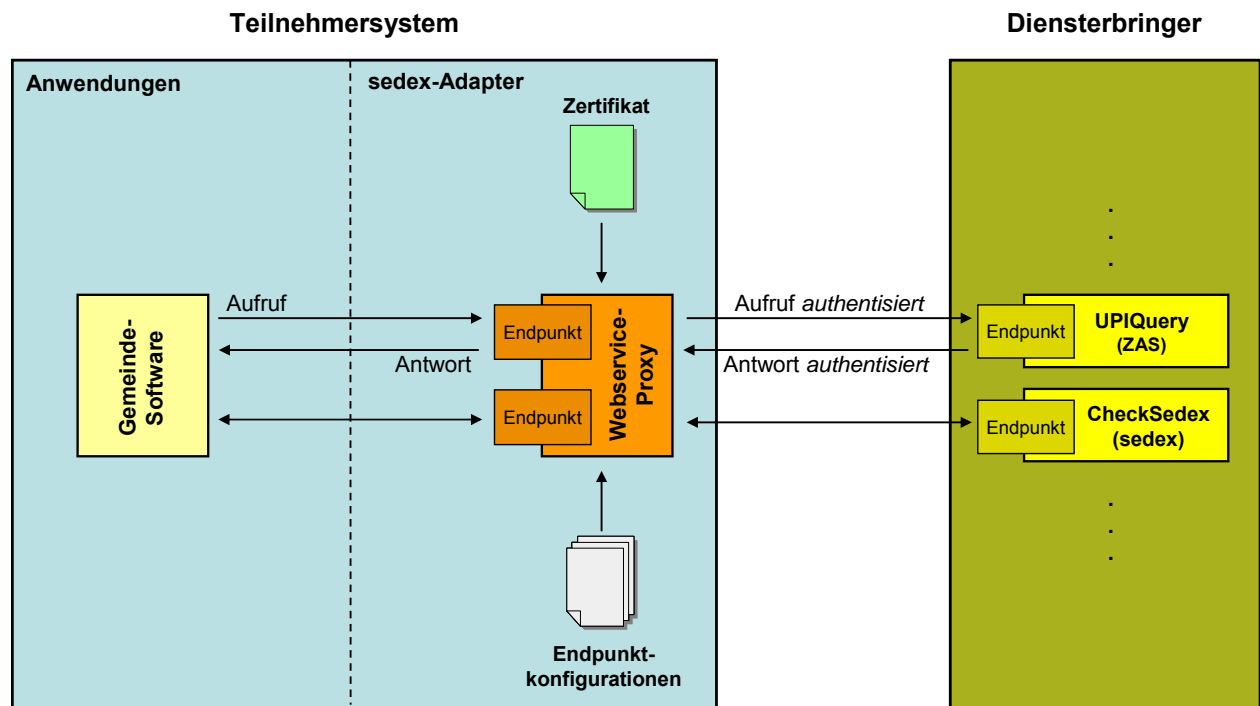


Abbildung 14: Webservice-Proxy

### 3.12.4 Zugriff auf Webservice-Proxy

Der Webservice-Proxy identifiziert den Aufrufer nicht anhand der sedexID. Der Aufruf kann somit grundsätzlich von jedem Computer aus erfolgen, der den Webservice-Proxy erreichen kann. Es ist Sache von dessen Betreiber, sicherzustellen, dass er nur von den Stellen erreicht werden kann, welche auch berechtigt sind, die Webservices aufzurufen.

Je nach Volumen der Service-Aufrufe kann die Kapazität des Servers, auf dem Webservice-Proxy und sedex-Adapter installiert sind, nicht ausreichen. In dem Fall ist für den Webservice-Proxy ein dedizierter Server vorzusehen.

### 3.12.5 Kompatible Webservices

Die nachstehenden Webservices akzeptieren die Authentisierung mittels Organisationszertifikat:

Webservice	Dokumentation
CheckSedex	siehe Kapitel 8.3
UPI query service	siehe [8]
UPI compare service	siehe [8]

Der sedex-Webservice-Proxy bietet prinzipiell nur Dienste an, welche unter Verwendung des Zertifikats des sedex-Teilnehmers auch direkt aufgerufen werden könnten. Welche Webservice-Endpunkte der Proxy auf der Clientseite zur Verfügung stellt und wie er diese an welche Dienstbringer weiterleitet, ist Teil der Webservice-Proxy-Konfiguration.

## 3.13 Aspekte für den Betrieb des sedex-Adapters

### 3.13.1 Aufbewahrungsfristen

Für Meldungen und Quittungen, welche vom sedex-Adapter empfangen bzw. von diesem versandt wurden, besteht keine Aufbewahrungsfrist.

Wenn für Daten, welche via sedex übermittelt werden, Aufbewahrungsvorschriften existieren, so sind diese von der partizipierenden Anwendung entsprechend aufzubewahren.

Der Adapter löscht weder die Meldungen (Verzeichnis *inbox*, *outbox* und *sent*) noch die technischen Quittungen (Verzeichnis *receipts*). Es ist der partizipierenden Anwendung überlassen, diese Daten nach einem für die Anwendung nützlichen Prinzip zu löschen (z.B. periodisch aufgrund des Alters oder nach Erledigung Geschäftsfall).

Die Logfiles werden überschrieben, sobald die maximale Anzahl Logfiles erreicht ist (rollover-Prinzip). Die Protokollierung durch den sedex-Server ist davon jedoch nicht betroffen.

### 3.13.2 Versionenhandling des XML-Schemas eCH-0090

Umschläge und technische Quittung werden aufgrund des XML-Schemas eCH-0090 gebildet. Eine partizipierende Anwendung 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

Das BFS wird Fristen festlegen, bis wann die Verwendung der alten Schema-Version erlaubt ist.

Um bei Einführung neuer Statuscodes allfällige Anpassungen in der partizipierenden Anwendung zu einem späteren Zeitpunkt machen zu können, kann in der Adapter-Konfiguration die Adapter-Version definiert werden, nach welcher Version des XML-Schemas die Quittung zu erstellen ist.

Umschläge (/eCH-0090:envelope) werden weiterhin mit der Version 1.0 von eCH-0090 gebildet.

## 3.14 sedex-Dienstnachrichten

Für die Kommunikation mit den Adaptern selbst kann das BFS als Betreiber der sedex-Plattform Dienstnachrichten einsetzen. Einsatzgebiete von sedex-Dienstnachrichten sind:

- automatisierte Erneuerung der Organisationszertifikate (siehe Kapitel 4.6)
- automatisierte Erneuerung des WS-Proxy-Truststores

Dienstnachrichten werden an ein separates Verzeichnis geliefert und werden vom Adapter selbst konsumiert. Die Autorisierung für den Empfang der Dienstnachrichten nimmt die sedex-Administration selbständig vor.

Die korrekte Verarbeitung der Dienstnachrichten wird von der sedex-Administration überwacht, die im Problemfall mit dem Teilnehmer Kontakt aufnimmt, sofern ein manueller Eingriff nötig ist.

## 3.15 HPSA

2009 haben einige Teilnehmer (z.B. Infostar) darauf hingewiesen, dass bestimmte Use Cases den Austausch von mehreren Tausend Meldungen pro Tag erfordern. Das BFS hat deshalb beschlos-

sen, für die besonderen Bedürfnisse grosser Benutzer einen leistungsstärkeren Adapter bereitzustellen. Der Entscheid wurde in zwei Phasen umgesetzt:

- Version 2.2.0: Optimierungen für mehr Performance, ohne grundlegende Änderungen am sedex-Adapter
- Version 3.0 (HPSA): grundlegende Optimierung mit einigen umfassenden Änderungen für deutlich mehr Performance

Die Version 2.2.0 wurde im Dezember 2009 veröffentlicht. und deckt einen Grossteil der Performancebedürfnisse ab. Die Version 3.0, auch HPSA (High Performance Sedex Adapter) genannt, wurde im April 2011 veröffentlicht und deckt sämtliche Performancebedürfnisse der einzelnen Teilnehmer (z.B. Infostar).

### 3.15.1 Neuheiten

Neu in der Version 3.0 ist vor allem das je nach Meldungsgrösse unterschiedliche Sendeverhalten. Meldungen mit weniger als 100 KB werden im Schnellverfahren (Fast Lane) bearbeitet, für Meldungen mit bis zu 10 GB ist der langsame Weg (Slow Lane) vorgesehen.

Dieses Verhalten ist besonders für kantonale Plattformen und Bundesregister interessant, wo eine grosse Anzahl kleiner Dateien ausgetauscht werden.

### 3.15.2 Kompatibilität

Die früheren Versionen sind nur teilweise mit der Version 3.0 kompatibel.

#### Nutzung

Da die Verzeichnisse und die Spezifikationen der Schnittstelle gleich bleiben, ist die Kompatibilität bei der Nutzung gewährleistet. Der Meldungsverkehr (Inbox, Outbox, Sent, Receipts) bleibt demnach unverändert.

#### Installation

Bei der Installation ist die Kompatibilität hingegen nicht gewährleistet, da die interne Datenbank und die Konfigurationsdateien des Adapters geändert wurden. Es ist deshalb wichtig, vor der Installation der neuen Version das Organisationszertifikat und das entsprechende Passwort sowie das Inbox-, Sent- und Receipts-Verzeichnis zu speichern. Das genaue Vorgehen der Migration zur Version 3.0 wird im Installationshandbuch und den Release Notes des sedex-Adapters beschrieben.

### 3.15.3 Einstellungen

Die Version 3.0 kann vom einfachen Desktop bis zum Hochleistungsserver auf allen Plattformen verwendet werden. Damit die Kapazitäten der Maschine, auf der der Adapter installiert werden soll, optimal genutzt werden können, stehen vier verschiedene Profile mit einer unterschiedlichen Anzahl paralleler Prozesse und gleichzeitiger Verbindungen zum sedex-Server zur Verfügung.

Die Wahl des Profils beeinflusst die Performance des sedex-Adapters in beträchtlicher Weise. Die Leistung kann auch erhöht werden, indem der grösstmögliche Arbeitsspeicher (RAM), der für die Java Virtual Machine verwendet werden darf, erhöht wird.

Bei der Wahl des Profils ist die Umgebung des Adapters massgebend:

- Merkmale der Maschine (CPU, RAM, Speicherplatz)

- Netzwerk (Datenkapazität Intranet/Internet, Präsenz einer Firewall usw.)

In der folgenden Tabelle sind die Merkmale der verschiedenen Profile zusammengefasst:

	<b>small *</b>	<b>medium</b>	<b>large</b>	<b>x-large</b>
Verbindungen zum sedex-Server	1	2	4	8
Parallele Prozesse (Threads)	2	3	5	7

\* Standardprofil

Nähere Angaben zu den Optimierungsmöglichkeiten können den Dokumenten [9] und [13] entnommen werden. Der Service Clientèle des BFS ([4], Kapitel 2.2.1) steht für Erläuterungen zu Profiländerungen ebenfalls zur Verfügung

## 4 Prozesse

### 4.1 Übersicht

Der Anschluss einer Anwendung und/oder eines Teilnehmers an sedex kann in die Phasen Entwicklung, Einführung und Betrieb unterteilt werden.

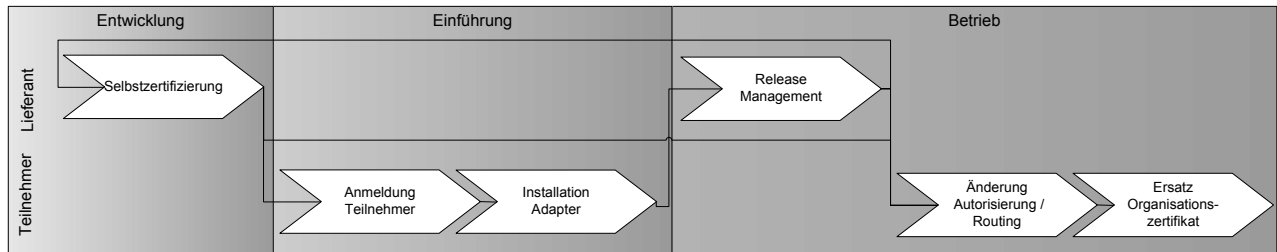


Abbildung 15: sedex-Prozesskette

### 4.2 Zertifizierung partizipierender Anwendungen

Der Fachgebietskoordinator kann verlangen, dass eine Anwendung vor dem Anschluss des ersten Teilnehmers, der sie einsetzt, zertifiziert wird.

Form und Gegenstand der Zertifizierung sind Sache des Fachgebietskoordinators und sind in dessen Dokumentationen zum Anschluss der Anwendung an sedex nachzulesen.

Für den Bereich der Registerharmonisierung hat die Sektion POP des BFS die Form der Selbstzertifizierung gewählt; deren Gegenstand in [4] enthalten ist.

Jeder Koordinator kann entscheiden, ob er für seinen Bereich eine Zertifizierung oder eine Selbstzertifizierung verlangen will.

### 4.3 Anmeldung des Teilnehmers

Voraussetzung für die Teilnahme an sedex ist, dass der Lieferant der partizipierenden Anwendung diese für den Einsatz mit sedex zertifiziert hat (siehe Kapitel 4.2).

#### 4.3.1 Anmeldung vorbereiten

Der künftige Teilnehmer und sein SW-Lieferant sammeln die für die Anmeldung erforderlichen Informationen:

- Name und e-Mail-Adresse des Teilnehmers
- Art und Name der Anwendung, mit der die sedex-Meldungen erstellt werden sollen (z.B. Zivilstandsregister, Infostar)
- Anschlussart an sedex (direkt oder indirekt, vgl. Kapitel 2.4)
- bei indirektem Anschluss: Name des Defaultempfängers
- bei direktem Anschluss: Zustellform des Organisationszertifikates (vgl. Kapitel 8.4)
- Anschlusstermin

- Name und e-Mail-Adresse der mit dem Anschluss betrauten Person

#### 4.3.2 Teilnehmer beim BFS anmelden

Der künftige Teilnehmer oder sein SW-Lieferant melden den bzw. die neuen Teilnehmer via den Fachbereichsordinator beim Service Clientèle des BFS an:

Die Meldung ist telefonisch oder via e-Mail möglich:

- Telefon: 0800 866 700
- E-Mail: harm@bfs.admin.ch

Die Anmeldung hat zwei Wochen vor dem erwünschten Anschlusstermin zu erfolgen. Bei späterem Eingang kann nicht gewährleistet werden, dass der Anschluss termingerecht bereit steht.

### 4.4 Installation des sedex-Adapters

Die nachstehenden Ausführungen sind nur für direkt an sedex angeschlossene Teilnehmer relevant.

#### 4.4.1 Anforderungen an Netzwerkkonfiguration

##### 4.4.1.1 Proxy-Server

Sofern die lokalen Gegebenheiten den Verkehr mit dem sedex-Server via einem oder mehreren Proxy-Server(n) erfordert, sind die entsprechenden Adapter-Einstellungen im Abschnitt „URL's and connection points“ des Files „sedexAdapter.properties“ vorzunehmen.

##### 4.4.1.2 Router

Sofern die lokalen Gegebenheiten dies erfordern bzw. sinnvoll erscheinen lassen, kann der Datenverkehr über ein kantonales Netz und/oder KOMBV/KTV geleitet werden.

Die Sicherheitsmerkmale von sedex lassen jedoch den Datenaustausch via Internet zu.

##### 4.4.1.3 Firewall

In der Firewall müssen die Ports 80 (http) und 443 (https) für abgehende Verbindungen offen sein. Als Minimalanforderung ist dies für java.exe zuzulassen.

Da sedex nie eine Verbindung zu einem empfangenden Adapter aufbaut, müssen keine Ports für eingehenden Verkehr geöffnet werden.

#### 4.4.2 Vorbereitung der Netzkonfiguration

##### 4.4.2.1 Überprüfung der Verbindung zum sedex-Server (sedex-Adapter < V2.2)

Geben Sie im Webbrowser der Maschine, auf dem der Adapter installiert werden soll, folgende URL ein (vgl. „OSCI Connection URL“ in der Datei sedexAdapter.properties):

<http://www.governikus.admin.ch/osci-manager-entry/externalentry>

Sofern auf der angezeigten Seite die Meldung

I don't speak GET - Send POST to URL - -

erscheint, kann der sedex-Server vom Adapter erreicht werden.

#### 4.4.2.2 Überprüfung der Verbindung zum sedex-Adapter (≥ V2.2)

Mit den älteren Versionen verkehrten alle notwendigen Mitteilungen zwischen den sedex-Adapter und den Server über SOAP-over-OSCI. Was den Adapter anbelangt, musste nur die Adresse des OSCI-Servers ([www.governikus.admin.ch](http://www.governikus.admin.ch), port 80, siehe Kapitel 4.4.2.1) erreichbar sein.

Die Einführung von SOAP-over-HTTPS bedeutet, dass folgende Adressen für den Adapter (≥ v2.2) erreichbar sein müssen :

- [www.governikus.admin.ch](http://www.governikus.admin.ch) (port 80)
- [www.oscity-gw.admin.ch](http://www.oscity-gw.admin.ch) (port 443)
- [www.sedex-gw.admin.ch](http://www.sedex-gw.admin.ch) (port 443)
- [www.osciseservices-gw.admin.ch](http://www.osciseservices-gw.admin.ch) (port 443)

Die Erreichbarkeit kann nicht Mithilfe eines Browsers überprüft werden. Die Netzwerkkomponenten (wie Proxy, DNS Server, Router, Firewall) der sedex-Teilnehmer müssen im Falle Anschlussproblemen diesbezüglich konfiguriert.

Mehr Informationen können im Dokument [9] entnommen werden.

#### 4.4.2.3 Ermittlung Proxy-Server

Sofern der Zugriff aufs Internet bzw. KOMBV-KTV über einen Proxy-Server erfolgen soll, benötigen Sie folgende Informationen:

- URL des Proxy-Servers (z.B. myhost.at.com)
- Port, über den der Proxy-Server erreicht werden kann (z.B. 8080 oder 8088)

Klären Sie im Weiteren ab, ob der Zugriff frei ist oder ein spezielles Logon erforderlich ist. In letzterem Fall benötigen Sie folgende weitere Informationen:

- User-Identifikation
- Passwort

Diese Angaben erhalten Sie von Netzwerkverantwortlichen; sie müssen in der Adapter-Konfigurationsdatei eingetragen werden.

URL und Port können auch selbst ermittelt werden:

- Starten Sie den Browser (z.B. Windows Internet Explorer oder Firefox). Die nachstehende Beschreibung bezieht sich auf den Internet Explorer 7.0.
- Wählen Sie „Extras - Internetoptionen - Verbindungen - LAN-Einstellungen“
- Prüfen Sie die Einträge im folgenden Fenster:

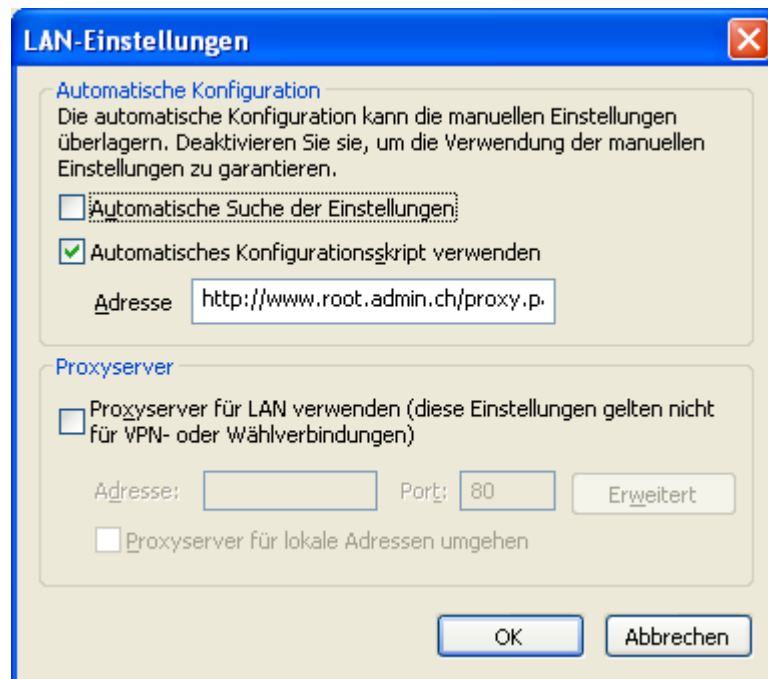


Abbildung 16: Proxy-Einstellungen bei Internet Explorer 7.0

- Ist die Checkbox unter „Proxyserver“ aktiviert, sind Adresse und Port gemäss den Angaben an dieser Stelle massgebend und in die Adapter-Konfiguration einzutragen.
- Ist die Checkbox „Automatisches Konfigurationsskript verwenden“ aktiviert, editieren Sie die angegebene Datei (z.B. mit Wordpad) und prüfen, welche Regeln für die IP-Adresse des sedex-Servers (siehe Kapitel 4.4.2.5) gelten.
- Ist keine Checkbox aktiviert, erfolgt der Zugriff aufs Internet direkt (ohne Proxy-Server).

#### 4.4.2.4 Routing definieren

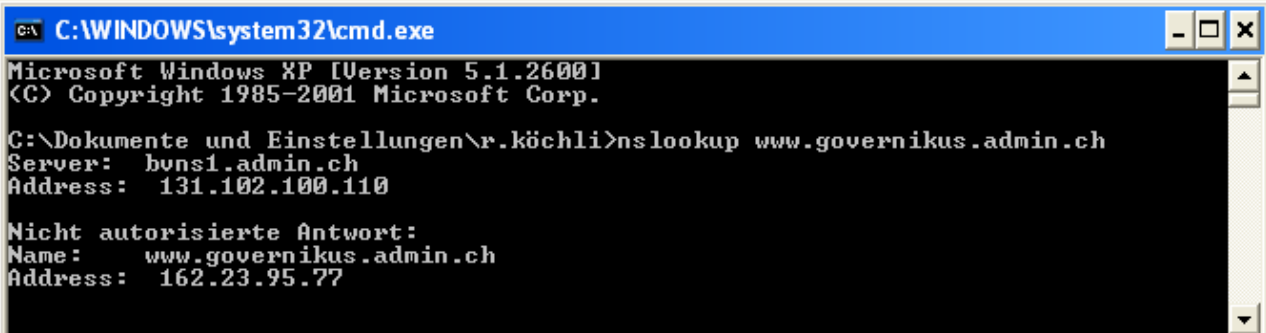
Klären Sie mit den kommunalen bzw. kantonalen Netzwerkverantwortlichen, auf welchem Weg der sedex-Server erreicht werden soll:

- Kann bzw. darf der sedex-Server via Internet erreicht werden?
- Muss der sedex-Server via einen (kantonalen) Proxy-Server erreicht werden?
- Muss bzw. soll der sedex-Server via KOMBV/KTV erreicht werden?

#### 4.4.2.5 Überprüfung Netzwerkkonfiguration

Um sicherzustellen, ob aufgrund der getroffene Entscheidung im Kapitel 4.4.2.4 überhaupt Änderungen in der Netzwerkeinstellung nötig sind, kann man die IP-Adresse der sedex-Server-URL anfragen:

- Starten Sie das Command-Prompt.
- Geben Sie den Befehl `nslookup www.governikus.admin.ch` ein.

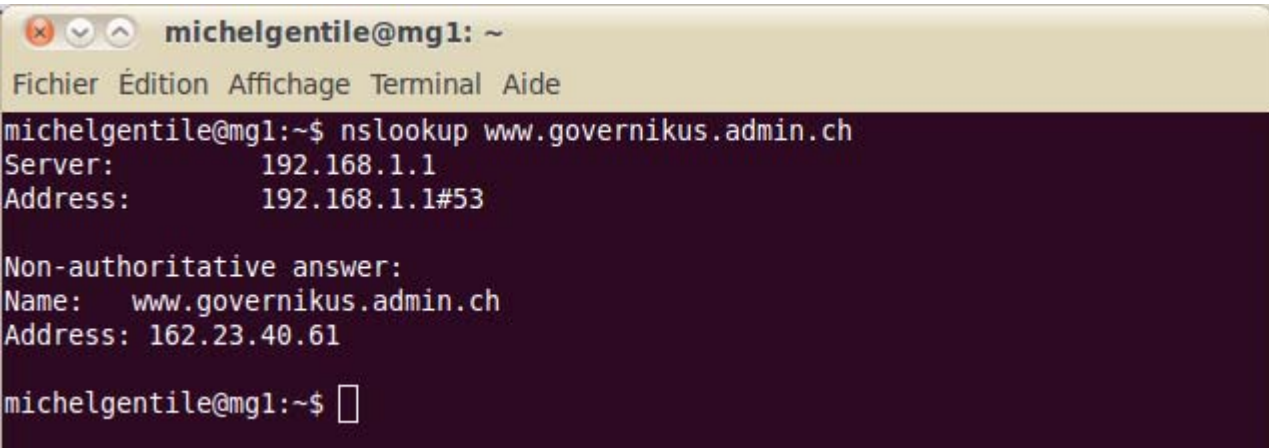


```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Dokumente und Einstellungen\r.köchli>nslookup www.governikus.admin.ch
Server:      huns1.admin.ch
Address:     131.102.100.110

Nicht autorisierte Antwort:
Name:       www.governikus.admin.ch
Address:    162.23.95.77
```

Abbildung 17: Beispiel mit der MS-DOS Eingabeaufforderung (Windows), wenn die Verbindung über KOMBV läuft



```
michelgentile@mg1: ~
Fichier  Édition  Affichage  Terminal  Aide

michelgentile@mg1:~$ nslookup www.governikus.admin.ch
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
Name:       www.governikus.admin.ch
Address:    162.23.40.61

michelgentile@mg1:~$
```

Abbildung 18: Beispiel mit der Bash Eingabeaufforderung (Linux), wenn die Verbindung über das Internet läuft

Bei Linux kann man diesen Befehl als normaler Benutzer ausführen.

Aufgrund des Ergebnisses kann dann ermittelt werden, über welches Netz die Kommunikation erfolgt:

- IP-Adresse 162.23.95.77: Verbindung über KOMBV
- IP-Adresse 162.23.40.61: Verbindung über das Internet

Gegebenenfalls ist der DNS-Server anzupassen (siehe Kapitel 4.4.2.6).

#### 4.4.2.6 DNS-Konfiguration veranlassen

Sofern der sedex-Server nicht direkt, d.h. via Internet, sondern über ein kantonales und/oder interkantonales Netz (KOMBV/KTV) erreicht werden soll, ist bei den Verantwortlichen des entsprechenden Netzes das dazu erforderliche Routing in Auftrag zu geben.

Dazu müssen folgende Angaben geliefert werden:

- IP-Adresse, von der aus auf den sedex-Server zugegriffen werden soll (entweder Client, auf dem der Adapter installiert ist, oder Proxy-Server)
- IP-Adresse des sedex-Servers. Diese ist abhängig vom Zugriffspfad. Die DNS ist deshalb in dem Netz aufzulösen, über das der sedex-Server angesprochen werden soll (siehe Kapitel 4.4.2.5).

Dies ist auch für sämtliche Server der Dienste vorzunehmen, die über den Webservice-Proxy aufgerufen werden sollen.

#### 4.4.2.7 Port freischalten

Klären Sie bei den Netzwerkverantwortlichen, ob die Ports 80 (http) und 443 (https) für ausgehende Verbindungen freigeschaltet sind (siehe Kapitel 4.4.1.3).

### 4.4.3 Installation

Bei direkten (physischen) Teilnehmern ist ein sedex-Adapter zu installieren. Zuständig ist die jeweilige IT-Supportorganisation des Teilnehmers.

Mit Vorteil erfolgt die Installation des Adapters gleichzeitig mit der für sedex zertifizierten Version der partizipierenden Anwendung.

#### 4.4.3.1 Systemanforderung

Die massgebende Systemanforderung ist im Installationshandbuch des Adapters [9] beschrieben, der sich auf der BFS Internetseite befindet. Die nachstehenden Abschnitte unterstreichen die wichtigsten Punkte.

Für eine optimale Performance, empfehlen wir einen Rechner, der mit einem „Dual-Core“ Prozessor ausgerüstet ist. Weiter sollte mindestens 512MB Arbeitsspeicher (RAM) für den sedex Adapter verfügbar sein. Der sedex Adapter erfordert die Java-Version 1.6 (die Version 1.5 wird nicht mehr unterstützt).

Mit der Version 3.0 (HPSA) des sedex-Adapters kann zudem zwischen mehreren Benutzerprofilen gewählt werden. Somit sind abhängig vom gewählten Profil verschiedene Mindestanforderungen möglich. Nähere Informationen zur Version 3.0 des sedex-Adapters (HSPA) sind in Kapitel 3.15 zu finden.

#### 4.4.3.2 Berechtigungen

Während des Betriebs muss der sedex-Adapter an verschiedenen Stellen der sedex-Installation auf Dateien zugreifen, sowie Dateien lesen und schreiben können. Das Verzeichnis des sedex-Adapters, sowie alle Unterverzeichnisse müssen deshalb für den sedex-Adapter uneingeschränkt zugänglich sein. Ausserhalb seiner Baumstruktur benötigt der Adapter hingegen keinen anderen Zugriff.

In den Windows-Systemen muss dazu die Berechtigung „Vollzugriff“ und in den Unix/Linux-Systemen das Recht „rwx“ festgelegt werden. Der sedex-Adapter benötigt kein Schreibrecht für andere Systemverzeichnisse.

Wird der Adapter als Anwendung gestartet (script bin/start.bat oder bin/start.sh), müssen die vorgenannten Rechte für den Benutzer festgelegt werden, der den Adapter verwendet. Wird der Adapter als Windows-Dienst oder Unix/Linux Deamon gestartet, müssen die gleichen Rechte auf den „System“- (Windows) oder „Root“ (Unix/Linux)-Benutzer angewendet werden.

## 4.5 Änderung Autorisierungen / Routing

Änderungen der autorisierten Meldungstypen und/oder der Routingregeln bestehender Teilnehmer sind von diesem selbst oder dem Lieferanten seiner partizipierenden Anwendung an den Service Clientèle des BFS zu richten (siehe [4], Kapitel 2.2.1).

### 4.5.1 Änderungen der Autorisierungen

Es müssen nur Meldungstypen gemeldet werden, welche der Teilnehmer zusätzlich zur Selbstzertifizierung des Lieferanten seiner Anwendungs-SW möchte, bzw. Meldungstypen von dieser, welche er nicht möchte.

Meldungstypen, welche vom Lieferanten der Erneuerung der Selbstzertifizierung hinzugefügt werden, müssen nicht von jedem Teilnehmer separat beantragt werden. Der Service Clientèle des BFS wird dafür besorgt sein, dass die bereits autorisierten Kunden des Lieferanten für die neuen Meldungstypen autorisiert werden. Je nach Anzahl betroffener Teilnehmer wird der Service Clientèle mit dem Lieferanten den Zeitpunkt, bis zu dem die Mutationen gemacht sein müssen, vereinbaren.

### 4.5.2 Änderungen Routing

Teilnehmer, welche neu indirekt an sedex angeschlossen werden wollen, müssen den Namen des Defaultempfängers nennen. Ohne anderslautende Instruktion wird das Organisationszertifikat 1 Monat nach dem Umstellungsdatum revoziert.

Teilnehmer, welche neu direkt an sedex angeschlossen werden wollen, müssen die Zustellform des Organisationszertifikates melden (vgl. Kapitel 8.4).

## 4.6 Erneuerung Organisationszertifikat

### 4.6.1 Erneuerungsarten

Die Organisationszertifikate haben eine Gültigkeitsdauer von drei Jahren. Grundsätzlich erfolgt die Erneuerung **automatisch** (siehe Kapitel 4.6.2).

Im Falle einer Testinstanz (z.B. T3-CH-1), muss die Erneuerung **manuell gemacht werden** (siehe Kapitel 4.6.3).

Aufgrund der Nachteile des manuellen Erneuerungsprozesses (vgl. Kapitel 8.4.3) empfiehlt das BFS, von der automatisierten Zertifikatserneuerung Gebrauch zu machen.

### 4.6.2 Automatisierte Erneuerung

Der Adapter löst den Erneuerungsprozess zwischen 60 und 90 Tagen vor dem Verfallsdatum selbständig aus. Der Prozess kann aus planerischen Gründen auch von sedex-Administratoren (d.h. dem BFS) ausgelöst werden.

Der automatisierte Erneuerungsprozess ist im Kapitel 8.4.2 beschrieben. Der einzige manuelle Eingriff muss durch die sedex Administratoren bestätigt werden.

Das BFS überwacht die korrekte Installation der neuen Zertifikate und nimmt gegebenenfalls mit dem Teilnehmer (es kann sich auch um den Lieferanten oder den Betreiber handeln) Kontakt auf.

Voraussetzung für eine automatisierte Zertifikatserneuerung ist sedex-Adapter-Version 2.1 oder höher.

### 4.6.3 Manuelle Erneuerung

Die manuelle Erneuerung entspricht grundsätzlich derjenigen der erstmaligen Installation des Organisationszertifikates (Prozess siehe Kapitel 8.4.1).

Das neue Zertifikat muss beim Service Clientèle beantragt werden (Dokument 4, Kapitel 2.2.1). In der Regel liefert das BFS dem Teilnehmer das Zertifikat und das Passwort. Wenn das Zertifikat einem Lieferanten oder einem Betreiber geliefert werden muss, ist es notwendig, bei der Bestellung die E-Mail Adresse für die Lieferung anzugeben.

Für die Installation des Zertifikates ist der Teilnehmer zuständig. Die manuelle Installation erfordert einen anschliessenden Neustart des Adapters.

Die Periode zwischen der Bestellung des neuen Zertifikates beim Service Clientèle und der Installation muss so kurz wie möglich gehalten werden, um Verschlüsselungsprobleme beim Übergang vom alten zum neuen Zertifikat zu vermeiden.

Das BFS empfiehlt also genügend Zeit zu reservieren, um die Bestellung und Installation des neuen Zertifikates in einmal zu erledigen.

## 4.7 Release Management

Die Weiterentwicklung der sedex Plattform und damit verbunden die Anpassungen des sedex-Adapters verlaufen in definierten Schritten. Jährlich ist mit einem bis maximal zwei Releases zu rechnen.

Die mit einer neuen Adapter-Version einhergehenden Änderungen und Neuerungen werden vom BFS in Release Notes angekündigt. Die Release Notes werden zusammen mit diesem Handbuch publiziert.

Gleichzeitig mit der Publikation einer neuen Adapter-Version werden auch dieses Handbuch sowie das Installationsmanual aktualisiert.

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 Adapter-Versionen wird in den Release Notes beschrieben.

Wir empfehlen jedoch, bei Update einer partizipierenden Anwendung jeweils auch die aktuelle sedex-Adapter-Version zu installieren.

Den Adapter ist jeweils auf dem Website des BFS<sup>8</sup> zum Download zur Verfügung gestellt. Zusätzlich informiert diese Website<sup>9</sup> auch über die nächsten Aktualisierungen. Die Aktualisierungsliste beinhaltet insbesondere auch die Planung der Veröffentlichung von IT-Komponenten, von Nomenklaturen, von Validierungsregeln etc...

<sup>8</sup> <http://www.register-stat.admin.ch> > IT-Spezifikationen > sedex

<sup>9</sup> <http://www.register-stat.admin.ch> > IT-Spezifikationen > Release Management

#### 4.7.1 Support der verschiedenen Versionen

Das Ende des Supports erfolgt in zwei Schritten. Der vollständige Support endet normalerweise 18 Monate nach der Veröffentlichung. Nach dieser Zeit ist der Support eingeschränkt : Bei einer Funktionsstörung wird nachgesucht, aber das Problem wird dem Bundesamt für Informatik und Telekommunikation (BIT) nicht weitergeleitet um gelöst zu werden. Dieser reduzierte Support endet meistens 24 Monate nach der Veröffentlichung. Nach dieser Zeit gibt es gar keinen Support mehr.

Version	Veröffentlichung	Ende des vollständigen Supports	Ende des reduzierten Supports
2.1.0	Juli 2009	30.06.2011	31.12.2011
2.2.0	Dezember 2009	30.06.2011	31.12.2011
2.2.1	Juni 2010	31.12.2011	30.06.2012
2.2.2	Oktober 2010	30.06.2012	31.12.2012
3.0 (HPSA)	April 2011	30.09.2012	31.03.2013

#### 4.8 Betrieb

Das Bundesamt für Statistik (BFS) hat am 15. Januar 2008 die sedex Plattform in Betrieb gesetzt. Das BFS hat dem Bundesamt für Informatik und Technologie (BIT) das Mandat für den Teil sedexbetrieb erteilt. In diesem Zusammenhang wurde zwischen dem BFS (Auftragnehmer) und dem BIT (Leistungserbringer) eine SLA (Service Level Agreement) betreffend sedexbetrieb erstellt. Dies sind die wichtigsten Punkte:

<b>Verfügbarkeit des Systems</b>	99.8%
<b>Servicezeit</b>	Montag bis Freitag, von 06.00 bis 20.00 Uhr
<b>Störungsbehebungszeit</b>	5 Stunden

Informationen über die vorgesehenen Wartungsfenster, über festgestellte Unterbrüche sowie der aktuelle Stand des Systems, sind auf der BFS Internetseite<sup>10</sup> verfügbar.

#### 4.9 Frequently Asked Questions (FAQ)

Eine FAQ-Liste (Häufig gestellte Fragen)<sup>11</sup> wurde auf der Internet-Seite des BFS publiziert und wird regelmässig aktualisiert.

Bei Problemen, empfehlen wir Ihnen, auf der online Dokumentation nachzuschlagen bevor Sie sich an den Service-Clientèle des BFS wenden.

<sup>10</sup> <http://www.registre-stat.admin.ch> > sedex > Betrieb

<sup>11</sup> <http://www.registre-stat.admin.ch> > FAQ sedex

## 5 Zuständigkeiten

### 5.1 Service Clientèle des BFS

#### 5.1.1 Dienstleistungen

Das BFS betreibt einen Kunden-Helpdesk (nachfolgend „Service Clientèle“ genannt), der als Anlaufstelle für folgende Aufgaben dient:

- Anmeldung neuer Teilnehmer, Autorisierungs- und Routing-Änderungen bestehender Teilnehmer
- Fragen zum Betriebszustand von sedex bzw. dem Status einzelner Meldungen
- Anträge für Änderungen oder Erweiterungen der sedex-Funktionalität

Der Service Clientèle wird Anfragen, die er nicht selbst erledigen kann, an die zuständige Stelle weitergeben (z.B. sedex Rollout Management).

#### 5.1.2 Kontakt

- Telefon: 0800 866 700
- E-Mail: [harm@bfs.admin.ch](mailto:harm@bfs.admin.ch)
- Web: [www.register-stat.admin.ch](http://www.register-stat.admin.ch) > Contact
- FAQ: [www.register-stat.admin.ch](http://www.register-stat.admin.ch) > FAQ sedex

### 5.2 Lieferant

Der Lieferant einer an sedex partizipierenden Anwendung ist für folgende Punkte verantwortlich:

- Entwicklung, Test und Unterhalt der Funktionalität der über sedex abgewickelten Use Cases gemäss den entsprechenden Spezifikationen
- Entwicklung, Test und Unterhalt der Schnittstelle zwischen Anwendung und sedex-Adapter gemäss diesem Handbuch
- Planung und Umsetzung des Rollouts der Anwendungsversion bei den Kunden, welche für die Nutzung der über sedex abzuwickelnden Use Cases erforderlich ist, gegebenenfalls in Zusammenarbeit mit einer externen Vertriebsorganisation
- Schulung und Helpdesk der Kunden bei der Nutzung der über sedex abzuwickelnden Use Cases, gegebenenfalls in Zusammenarbeit mit einer externen Vertriebsorganisation

### 5.3 Teilnehmer

Der (künftige) sedex-Teilnehmer ist für folgende Punkte verantwortlich:

- Wahl der Anschlussart an sedex (direkt oder indirekt, vgl. Kapitel 2.4)
- Anmeldung an sedex
- Organisationszertifikat Anforderung

- Bestellung der Anwendungsversion, welche für die Nutzung neuer, über sedex abzuwickelnder Use Cases erforderlich ist

Diese Aufgaben können an den Lieferanten bzw. dessen Vertriebspartner delegiert werden. In jedem Fall empfiehlt sich aber eine Absprache der Aktivitäten mit dem Lieferanten, zumal die Teilnehmer den sedex-Anschluss i.d.R. über eine Fachanwendung nutzen werden.

## 5.4 Fach-Domänen-Koordination

Als „Fach-Domäne“ bezeichnen wir einen thematisch klar definierten Anwendungsbereich, der einzelne seiner Funktionen über sedex abwickeln will.

### 5.4.1 Aufgaben

- Antrag zur Teilnahme an sedex-Steuerungsausschuss
- Dokumentation und Publikation der über sedex abzuwickelnden Use Cases
- Information der tangierten Lieferanten und potentiellen sedex-Teilnehmer über die über sedex abzuwickelnden Use Cases
- Koordination der für die Umsetzung der sedex-Use Cases erforderlichen Aktivitäten

### 5.4.2 Aktuelle Fach-Domänen-Koordinatoren

Fach-Domäne	Koordinationsstelle
Einwohnerkontrolle	BFS, Registerharmonisierung
AHVN13	BFS, Registerharmonisierung
Handelsregister	BJ, Direktionsbereich Privatrecht
eSCHKG	BJ, Direktionsbereich Zentrale Dienste
eAHV/IV	BSV, Bereich Organisation + RW AHV/IV
SSK	Schweiz. Steuerektoren-Konferenz
ASA 2011	BLW, Bundesamt für Landwirtschaft
ASTRA-VU	ASTRA, Bundesamt für Strassen

## 6 Test und Integration

### 6.1 Test-Arten

#### 6.1.1 sedex-Tests

Das BFS bietet Lieferanten unabhängig vom Meldungstyp die Möglichkeit zu testen, ob die Anwendung

- die Meldungen syntaktisch korrekt aufbaut;
- der Umschlag korrekt aufgebaut ist;
- eine Nutzdatendatei vorhanden ist;
- die Meldung dem sedex-Adapter korrekt übergeben kann, bzw. von sedex entgegennehmen kann;
- die vom BFS erfassten Autorisierungs- und Routing-Regeln korrekt sind.

Dabei steht die Kommunikation zwischen zwei sedex-Adaptoren im Vordergrund. Die Schnittstelle zur partizipierenden Anwendung muss nicht verfügbar sein, ebenso spielt der Inhalt der Nutzdaten-Datei keine Rolle.

Die Besonderheiten bei der Aufbereitung der Umschlagsdatei sind in Kapitel 6.3 beschrieben.

#### 6.1.2 End-to-End-Tests

Sofern vom Fachgebiets-Koordinator vorgesehen, können auch Tests zwischen partizipierenden End-Systemen durchgeführt werden. Grundsätzlich ist dies wie folgt möglich:

- Versand bzw. Empfang normaler sedex-Meldungen durch spezielle Test-Instanzen
- Versand bzw. Empfang spezieller sedex-Test-Meldungen durch normale Instanzen

In welcher Form E2E-Tests durchzuführen sind, wird vom Fachgebiets-Koordinator festgelegt.

Es empfiehlt sich, diese Test-Möglichkeiten im Hinblick auf eine allfällige (Selbst)-Zertifizierung der Anwendung zu nutzen (siehe Kapitel 4.2).

### 6.2 Testinstanzen

Für Tests, welche mit speziellen Testinstanzen durchgeführt werden sollen, sind die erforderlichen Testinstanzen beim Service Clientèle des BFS zu beantragen.

Grundsätzlich sind die gleichen Angaben erforderlich wie bei der Anmeldung eines normalen sedex-Teilnehmers (vgl. Kapitel 4.3). Die für die Tests erforderlichen Autorisierungen und Routingregeln sind gegebenenfalls zu präzisieren.

Zu beachten ist, dass sedex den Meldungs austausch zwischen Test- und normalen Instanzen nicht zulässt. Für einen Testcase sind somit mindestens zwei Test-Instanzen nötig.

### 6.3 Testmeldungen

Reine sedex-Tests (vgl. Kapitel 6.1.1) sind auf zwei Arten möglich:

	Meldung an Sender	Loopback-Meldung
Besonderheit Umschlag	recipientID = senderID	Element loopback/authorise true oder false (siehe Kapitel 3.6)
Besonderheit Meldung	Meldung wird in eigene Inbox gestellt.	Meldung wird an Empfänger gesendet, von dessen Adapter aber vernichtet.
Zweck	Überprüfung Adapterkonfiguration	<ul style="list-style-type: none"> <li>• Authorise = „true“: Überprüfung Autorisierung und Routing</li> <li>• Authorise = „false“: Verbindungstest zwischen Adaptern</li> </ul>
Voraussetzung	<ul style="list-style-type: none"> <li>• sedexID des Senders muss aktiv sein</li> <li>• Sender muss autorisiert sein für Meldungstyp</li> </ul>	<ul style="list-style-type: none"> <li>• sedexID von Sender und Empfänger müssen aktiv sein</li> <li>• Authorise = „true“: Sender und Empfänger müssen autorisiert sein für Meldungstyp</li> </ul>

Für E2E-Tests (vgl. Kapitel 6.1.2), welche mit speziellen Test-Instanzen durchgeführt werden (sender ID / recipient ID = T...), unterscheidet sich die Umschlagsdatei mit Ausnahme von Sender und Empfängeridentifikation von normalen Meldungen nicht.

Werden normale Instanzen für die E2E-Tests genutzt, ist die Umschlagsdatei mit dem XML-Element /eCH-0090:envelope/testData zu ergänzen (siehe Kapitel 3.6).

Das XML-Schema des Umschlags erlaubt, eine unbeschränkte Anzahl Testparameter mit beliebigen Ausprägungen mitzugeben. Die Parameter und ihre möglichen Ausprägungen müssen vom Fachbereichs-Koordinator definiert werden.

### 6.4 Integration

Die Ausbreitung der Anwendungen im produktiven Umfeld, d.h. Installation bei Kunden, darf vom Lieferanten erst vorgenommen werden, wenn er den Selbstzertifizierungsprozess erfolgreich abgeschlossen hat (siehe Kap. 4.2).

## 7 Sicherheit

### 7.1 Ausgangslage der Sicherheitsüberlegungen

Die Sicherheit der zu übertragenden Daten wird bei sedex gross geschrieben. Die wichtigsten Anforderungen sind Vertraulichkeit, Integrität und gesicherte Herkunft (Authentizität), welche während der gesamten Übermittlung vom Sender bis zum Empfänger (end-to-end) sichergestellt sein müssen, auch wenn die Daten über ungeschützte Netzwerke verschickt werden.

### 7.2 Systemübersicht sedex

Bei der Kommunikation über die sedex-Plattform arbeiten folgende Komponenten zusammen:

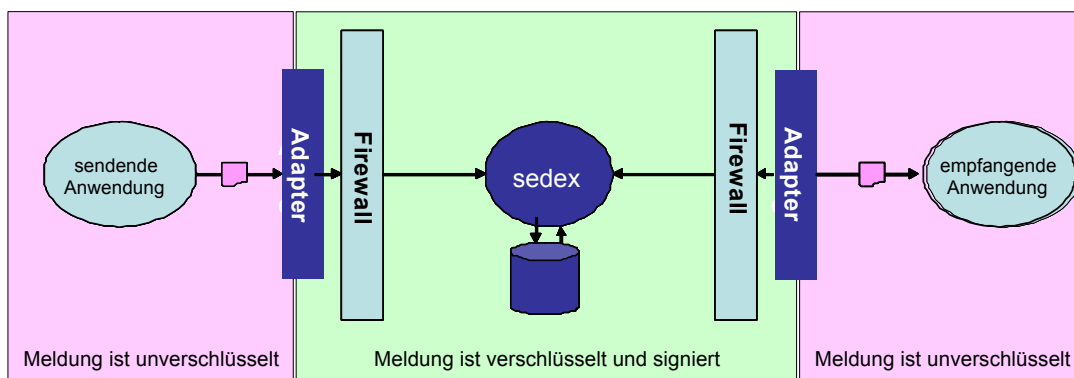


Abbildung 19: Komponenten der sedex-Plattform

Die Übertragung einer Meldung geschieht asynchron:

1. Die sendende Anwendung schreibt die zu übertragenden Daten in das lokale Filesystem.
2. Der Adapter des Senders nimmt die Datei, signiert sie mit seinem privaten Schlüssel, verschlüsselt die Nutzdaten mit dem öffentlichen Schlüssel des Empfängers und sendet sie an sedex. sedex legt die erhaltenen Daten, so wie sie sind, also verschlüsselt, bei sich ab.
3. Der Adapter des Empfängers überprüft in regelmässigen Abständen, ob bei sedex für ihn Meldungen vorhanden sind. Wenn dies der Fall ist, holt er sie ab.
4. Der Adapter des Empfängers entschlüsselt die Daten mit dem privaten Schlüssel des Empfängers, prüft die Signatur des Senders und legt die empfangene Meldung als Datei im Filesystem ab.
5. Die empfangene Meldung kann auf der Seite des Empfängers vor der Verarbeitung durch die empfangende Anwendung weiter geprüft werden (z.B. Virenskan u.a.).
6. Die empfangende Anwendung liest die Datei bei sich ein und prüft sie auf Konformität mit einem XML-Schema.

Für die Zusammenarbeit mit sedex sind auf Seite von Sender und Empfänger folgende Bedingungen zu erfüllen:

- Installation des Adapters
- Installation des Organisationszertifikats (X509.v3)
- Es muss ein elektronischer Kommunikationskanal (TCP/IP; http, https) vorhanden sein, über den sie mit sedex kommunizieren können.
- In der Firewall müssen die Ports 80 (http) und 443 (https) für abgehende Verbindungen offen sein. Da sedex nie eine Verbindung zu einem empfangenden Adapter aufbaut, müssen keine Ports für eingehenden Verkehr geöffnet werden.

Unabhängig von sedex sind natürlich für die lokalen Umgebungen die dafür adäquaten Sicherheitsvorkehrungen zu treffen (vgl. Kap. 7.3).

Hinweis: Das sedex-System nutzt für den eigentlichen Datenaustausch das Produkt „Governikus“ der Firma Bremen Online Services. Dieses Produkt ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) der deutschen Bundesregierung auf Sicherheit überprüft worden ist.

### 7.3 Erwartung an die partizipierenden Anwendungen

Folgende Anforderungen an die Betriebssicherheit müssen von den Software-Lieferanten umgesetzt werden:

- Die Software muss den sedex-Adapter gemäss den Vorgaben in diesem Handbuch verwenden. Es dürfen keine Umgehungslösungen implementiert werden, welche die Datensicherheit gefährden könnten.
- Die Rechner, auf welchen die Software installiert wird, müssen einen erhöhten Grundschutz aufweisen. Dazu gehören:
  - ein automatisch aktualisierter Virenschutz
  - sofortige Aktualisierung der Installation, falls Sicherheitslücken bekannt werden
  - Zugriff nur für Personen, welche diesen für die Ausübung ihrer Funktion brauchen
  - Abschalten von nicht benötigten Diensten des Betriebssystems
  - Einschränkung des Netzwerkzugriffs auf die für den Betrieb verwendeten Protokolle. Dies betrifft insbesondere den Zugriff von Netzwerken aus, welche nicht direkt in der Verantwortung der betreffenden Organisation liegen.

### 7.4 Beurteilung der Sicherheitsrisiken für Sender und Empfänger

Ist durch das Informatikstrategieorgan Bund (ISB) erstellt worden. Die Resultate (sedex-ISB-Sicherheit.PDF) sind unter

<http://www.bfs.admin.ch/bfs/portal/fr/index/news/00/00/12/01.parsys.65996.downloadList.69123.DownloadFile.tmp/sedexisbsicherheit.pdf> verfügbar.

### 7.5 Komponenten der Sicherheit - Sicherheitszertifikate

Die Datensicherheit auf dem Transportweg wird von sedex mit Hilfe der Public-Key-Technologie unter Verwendung der Organisationszertifikate von der AdminPKI gewährleistet (siehe auch

<http://www.pki.admin.ch>). Von entscheidender Bedeutung für den Schutz der verarbeiteten Daten ist aber auch die Absicherung der Rechner, auf welchen die Daten für den Versand vorbereitet werden. Erstens liegen die Daten hier ungeschützt vor, und zweitens werden die Geheimelemente (Private Key) für den kryptographischen Schutz ebenfalls auf diesen Rechnern installiert und können durch unbefugten Zugriff kompromittiert werden.

## 7.6 Erneuerung der Sicherheitszertifikate

### 7.6.1 Die Problematik der Sicherheitszertifikate-Erneuerung

Die Sedex Plattform braucht mehrere Sorten von Zertifikaten. Die Sedex Sicherheitszertifikate (Server und Adapter) sind 3 Jahre gültig. Die zuvor verteilten Zertifikate laufen demnächst ab. In diesem Dokument werden nur zwei Sorten Zertifikate behandelt, die von diesem Verfallsdatum und der automatischen Erneuerungsfunktionalität direkt betroffen sind :

1. Das Organisationszertifikat des Sedex-Adapters
2. Das Transportzertifikat des Sedex-Servers.

Ohne gültiges Zertifikat ist es unmöglich, eine Nachricht über die Sedex Plattform zu senden.

#### 7.6.1.1 Organisationszertifikat des Sedex-Adapters

Dieses Zertifikat ist auf der Client-Maschine installiert und wird vom Sedex-Adapter benutzt. Es wird für die Signierung und die Verschlüsselung der vom physischen Teilnehmer gesendeten und empfangenen Daten benutzt. Diese Art von Zertifikat wird vom BFS ausgestellt sobald ein neuer physischer Teilnehmer erstellt und erstmals konfiguriert wird.

### 7.6.2 Testzertifikate

Die Funktionalität der automatischen Zertifikaterneuerung wurde für die Test-Teilnehmer (Sedex Id, die mit einem TX-XXX-X beginnen) nicht implementiert. Diese Art von Zertifikat, die auch 3 Jahre gültig ist, muss manuell und in Zusammenarbeit mit dem BFS erneuert werden.

Dafür muss die verantwortliche Person des Zertifikates 60 Tage vor dem Zertifikatsablauf eine Erneuerungsanfrage an das BFS machen (Kundendienst der Registerharmonisierung: [harm@bfs.admin.ch](mailto:harm@bfs.admin.ch)). Das Verfallsdatum kann von der verantwortlichen Person des Zertifikates problemlos gefunden werden (siehe Anhang 8.4.4).

Ohne Erneuerungsantrag des Testzertifikates an den Kundendienst wird das BFS das Zertifikat nicht erneuern. Dieses Zertifikat ist nach dem Verfallsdatum nicht mehr verwendbar.

## 8 Anhang

### 8.1 XML-Schemas

#### 8.1.1 Bereitstellung der XML-Schema-Dateien

Das BFS stellt die XML-Schema-Dateien für sedex-Umschlag und technische Quittung sowie alle im Zusammenhang mit der Registerharmonisierung relevanten Schemas auf ihrer [Webseite](#) zum Download bereit. Die ZIP Datei enthält eine vordefinierte Verzeichnisstruktur mit den XML Schema Dateien sowie einen XML Katalog gemäss dem Standard OASIS XML Catalogs v1.0<sup>12</sup>.

Wenn der von Ihnen eingesetzte XML Parser über einen XML Entity Resolver verfügt, der gemäss OASIS XML Catalogs v1.0 arbeitet, so kann der XML Parsers angewiesen werden, die in den XML Schema Dateien referenzierten (nicht existierenden!) URL im lokalen Dateisystem aufzulösen. Wenn Ihr XML Parser OASIS XML Catalogs v1.0 nicht unterstützt, werden Sie die Referenzen händisch anpassen müssen. Sie finden Referenzen der folgenden Art:

```
<xs:import namespace="http://www.ech.ch/xml ns/eCH-0006/2"
  schemaLocation="http://www.ech.ch/xml ns/eCH-0006/2/eCH-0006-2-0.xsd" />
```

Von folgende XML Parsern bzw. Tools wissen wir, dass sie OASIS XML Catalogs v1.1 unterstützen:

- Xerces/J ab Version 2.7 (siehe <http://xerces.apache.org/xerces2-j/faq-xcatalogs.html>)
- XMLSpy ab Version 2007 (siehe Kap. 8.1.2)
- oXygen XML Editor (<http://www.oxygenxml.com/>) ab Version 6
- StylusStudio (<http://stylusstudio.com/>)
- jEdit Editor (<http://www.jedit.org/>)

Beachten Sie, dass Sie für den produktiven Betrieb Ihrer Applikationen, die mit XML Dateien arbeiten, welche eCH Schemata verwenden, ein analoges Verfahren verwenden müssen. Beachten Sie hierzu die Kommentare in der Datei ech-catalog.xml, welche sich in der Zip Datei mit den XML Schemata befindet.

Für das Microsoft .NET Framework muss vermutlich ein eigener XML Resolver geschrieben werden (siehe Dokumentation der Klasse System.Xml.XmlUriResolver).

#### 8.1.2 Verwendung der XML Schemas mit XML Spy

Die folgende Anleitung erklärt, wie XML Spy konfiguriert werden muss, um damit mit den XML Schemas von eCH für sedex korrekt umgehen zu können.

Das "Problem" besteht darin, dass in den eCH Schemata andere eCH Schemata importiert werden müssen. Die dazu verwendeten Import-Anwendungen enthalten URL wie diesen:

```
<xs:import namespace="http://www.ech.ch/xml ns/eCH-0006/2"
  schemaLocation="http://www.ech.ch/xml ns/eCH-0006/2/eCH-0006-2-0.xsd" />
```

Siehe <sup>12</sup> <http://www.oasis-open.org/committees/download.php/14809/xml-catalogs.html>

Da dieser URL auf der Website des Vereins eCH (noch) nicht existiert, muss XML Spy angewiesen werden, solche Schemata nicht über das Web, sondern von der lokalen Festplatte zu holen. Dies geschieht durch eine so genannte XML-Katalog-Definition gemäss dem Standard OASIS XML Catalogs v1.0.

Um den XML Katalog unter XML Spy einzurichten, gehen Sie wie folgt vor:

- Öffnen Sie das Verzeichnis, in welchem auf Ihrem Computer XML Spy installiert ist. Dieses Verzeichnis heisst bei einer deutschen Installation von Windows und XML Spy 2008 C:\Programme\Altova\XMLSpy2008
- Speichern Sie die Zip Datei mit den Sedex XML Schemas, die Sie von der Website des BFS geholt haben, im Verzeichnis C:\Programme\Altova\XMLSpy2008\Schemas. Entpacken Sie den Inhalt der Zip Datei, und nennen Sie das resultierende Verzeichnis in sedex um. Das Verzeichnis sollte dann so aussehen:

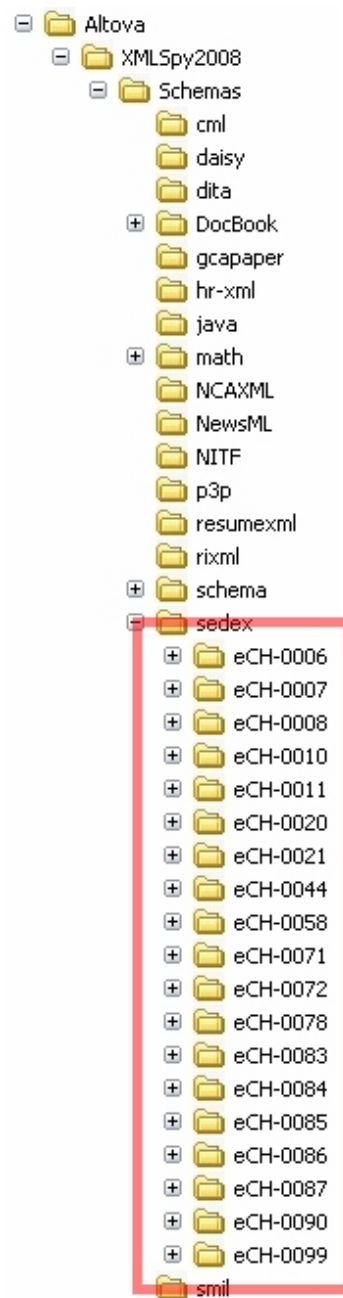


Abbildung 20: Ordnerstruktur von Altova XMLSpy

- Öffnen Sie mit XML Spy die Datei C:\Programme\Altova\XMLSpy2008\CustomCatalog.xml und ersetzen Sie den Inhalt mit dem folgenden Text:

```
<catalog xmlns="urn:oasis:names:tc:entity:xmlns:xml:catalog" prefer="public">
  <rewriteSystem systemIdStartString="http://www.ech.ch/xml ns/"
    rewritePrefix="schemas/sedex/" />
</catalog>
```

- Öffnen Sie mit XML Spy die Datei C:\Programme\Altova\XMLSpy2008\RootCatalog.xml und ersetzen Sie gegebenenfalls den Inhalt mit dem folgenden Text:

```
<catalog xmlns="urn:oasis:names:tc:entity:xmlns:xml:catalog"
  xmlns:spy="http://www.altova.com/catalog_ext"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:entity:xmlns:xml:catalog
  Catalog.xsd">
  <nextCatalog catalog="CustomCatalog.xml" />
  <nextCatalog catalog="CoreCatalog.xml" />
</catalog>
```

- Starten Sie XML Spy neu auf.

Falls Sie die Sedex Schemata lieber in einer gemeinsamen Ablage hinterlegen möchten, statt in einem lokalen Verzeichnis, so können Sie dies auch tun. Nehmen wir an, die gemeinsame Ablage befindet sich unter P:\projekte\P2007-B34\schemas\sedex, so müssen Sie den Inhalt der Datei CustomCatalog.xml wie folgt definieren:

```
<catalog xmlns="urn:oasis:names:tc:entity:xmlns:xml:catalog" prefer="public">
  <rewriteSystem systemIdStartString="http://www.ech.ch/xml ns/"
    rewritePrefix="file:///P:/projekte/P2007-B34/schemas/sedex/" />
</catalog>
```

## 8.2 Regeln für XML-Dokumente

### 8.2.1 Kodierung der XML-Dokumente

Als Kodierung für alle ausgetauschten XML-Dokumente sollte gemäss den Empfehlungen des eCH-Standards eCH-0018 (XML Best Practices) UTF-8 verwendet werden. Ist die verwendete Codierung nicht UTF-8, so muss die entsprechende „encoding“-Deklaration in der XML-Deklaration angegeben werden. Des zusätzlichen Datenvolumens wegen (jedes Zeichen braucht 2 Bytes!) ist auf die Verwendung von UTF-16 für die Kodierung zu verzichten.

### 8.2.2 Zeitangaben

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 „hh:mm:ss(+|-)hh:mm“ vorliegen. Fehlt die Angabe der Zeitzone, so sind die Zeitangaben nicht vollständig determiniert.

Wir empfehlen, Zeit- und Datumsangaben immer in UTC vorzunehmen.

## 8.3 Webservice CheckSedex

Wenn ein Teilnehmer eine Meldung an eine andere Amtsstelle schicken möchte, weiss er nicht, ob er die Meldung über sedex schicken darf oder ob er für diese Meldung einen anderen Kanal wählen muss, z.B. Briefpost. Deshalb besteht die Möglichkeit, vor dem Versand einer Meldung im Webservice CheckSedex nachzusehen.

### 8.3.1 Dienstbeschreibung

Der Dienst „CheckSedex“ prüft die wesentlichen Elemente des Meldungsumschlags (Absender, Meldetyp, Meldeklasse, Empfänger) gegenüber dem Teilnehmerverzeichnis von sedex und führt eine Autorisierungsprüfung durch.

Aus folgenden Gründen ist es möglich, dass der Teilnehmer die Meldung nicht über sedex schicken darf:

- Der Sender oder einer der Empfänger ist nicht als Teilnehmer von sedex aktiviert.
- Der Absender im Umschlag ist nicht autorisiert, Meldungen dieses Typs zu schicken (Senderautorisierung).
- Ein Empfänger im Umschlag ist nicht autorisiert, Meldungen dieses Typs zu empfangen (Empfängerautorisierung).
- Der sendende Adapter (physischer Sender) ist nicht autorisiert, Meldungen dieses Typs für diesen Sender zu schicken (Senderautorisierung).
- Einer der Empfänger hat kein gültiges Zertifikat, mit dem man die Nachricht für ihn verschlüsseln kann.
- Fehler im Umschlag: Absender, Adapter-ID, Meldetyp oder Empfänger ist falsch.
- Grösse der Nutzdatendatei übersteigt maximal zulässige Limite (Optionale Prüfung).

Die Adapter-ID wird benötigt, weil bestimmte Autorisierungsregeln auch die Identität des Adapters verwenden, welcher die Meldung schickt, das heisst die Identität des physischen Senders.

### 8.3.2 Einschränkungen

Dieser Webservice kann für alle Meldungen, die via sedex gesendet werden, verwendet werden. Er wird aber hauptsächlich für einen Austausch zwischen Gemeinden gebraucht und im allgemeinen wenn der Teilnehmerkreis wächst (z.B. für Umzugsmeldungen zwischen den Einwohnerregistern).

Bei der Antwort stützt sich der Webservice nur auf die für einen Teilnehmer autorisierten Meldungstypen. Die von den Teilnehmern unterstützten XML Schema-Versionen werden also nicht betrachtet.

### 8.3.3 Eingabeparameter

Attributname	Typ	Mandatory	Beschreibung
Sender	sedex-ID	ja	ID des Absenders (Absender im Umschlag)
AdapterID	sedex-ID	ja	ID des sedex-Adapters (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 (im Umschlag)

### 8.3.4 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 sender id %s 301: Unknown recipient id %s ** 302: Unknown physical sender id %s 303: Invalid message type %s 304: Invalid message class %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)

Attributname	Typ	Beschreibung
RecipientErrorCode	numerisch	100: (OK - no error) 301: Unknown recipient id %s 311: Not allowed to receive 312: User certificate not valid 330: Message size exceeds limit
RecipientErrorMessage	string	Fehlermeldung, falls der RecipientErrorCode > 0 ist

Die Bedeutung der einzelnen Fehlercodes kann Abschnitt 3.9.2 entnommen werden.

## 8.4 Standard-Prozesse für Ausgabe von Organisationszertifikaten

### 8.4.1 Erstausgabe und manuelle Erneuerung

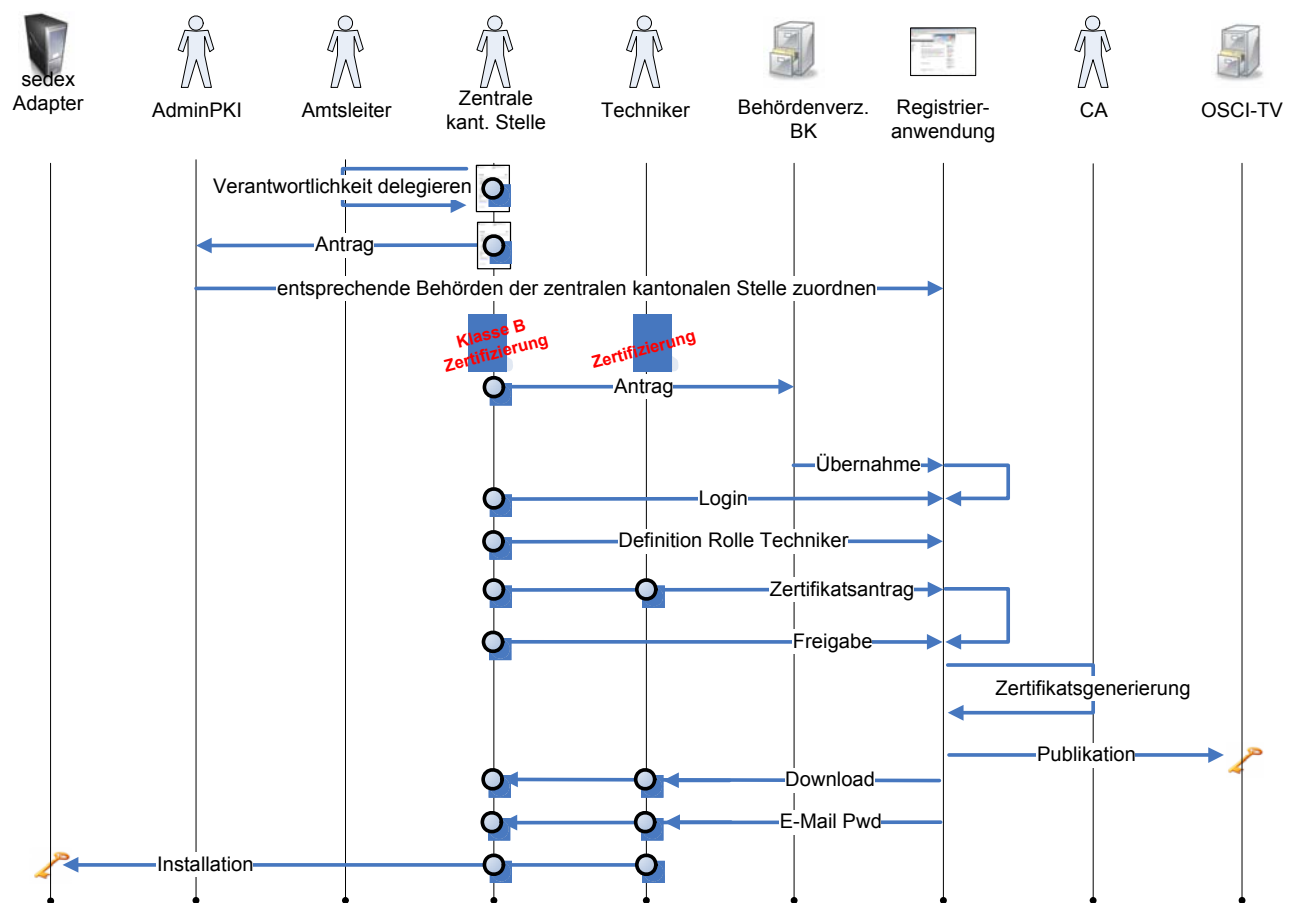


Abbildung 21: Standard-Prozess für zentrale Ausgabe von Organisationszertifikaten

## 8.4.2 Automatisierte Zertifikatserneuerung

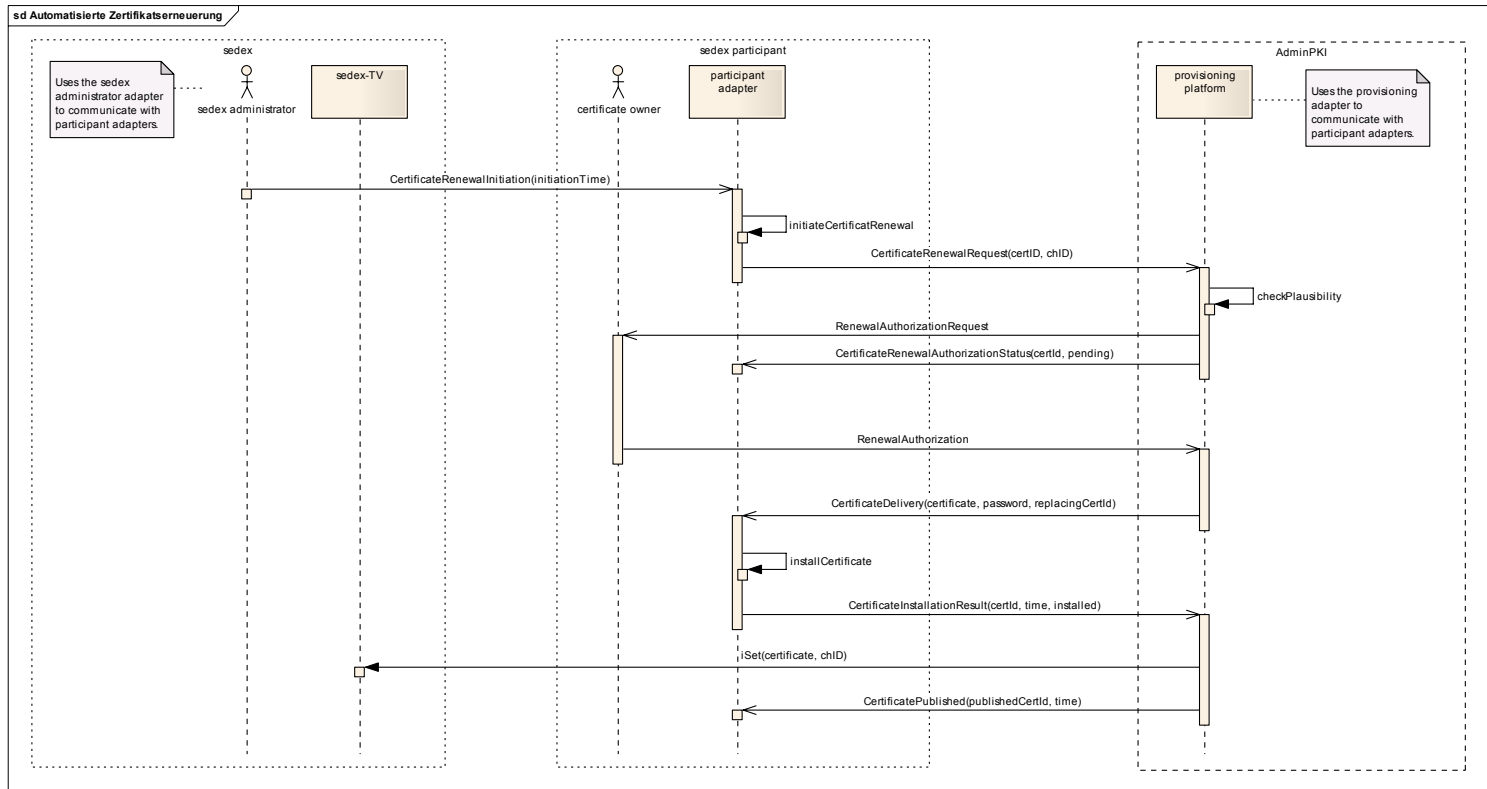


Abbildung 22: Standard-Prozess für die automatische Zertifikatserneuerung

## 8.4.3 Nachteile der manuellen Zertifikatserneuerung

- Prozess wird nicht systemgesteuert ausgelöst, sondern muss vom sedex-Teilnehmer initiiert werden.
- Der Transport des Organisationszertifikats von der Ausgabeapplikation von Admin PKI zum sedex-Teilnehmer ist aufwändig, zeitintensiv und teuer.
- Der Public Key wird unmittelbar nach der Bestellung, nicht nach der Installation des neuen Zertifikats, publiziert. Meldungen, welche in dieser Zeit an den Teilnehmer gesandt werden, können nicht heruntergeladen werden.
- Die manuelle Zertifikatserneuerung erfordert einen Neustart des Adapters.

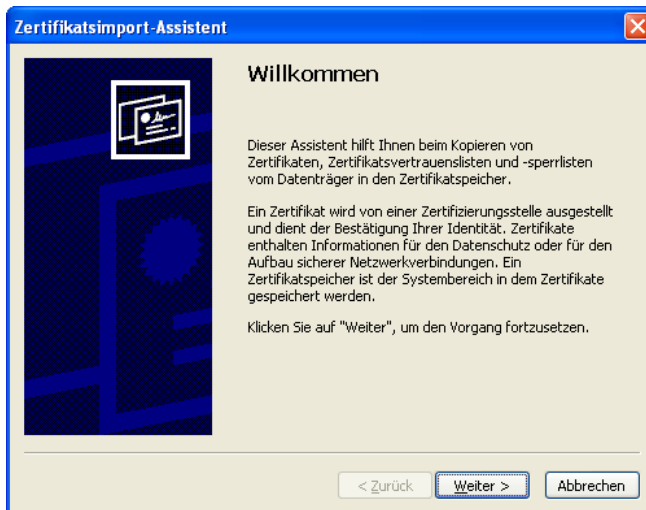
#### 8.4.4 Prozedur um das Verfallsdatum zu finden

1



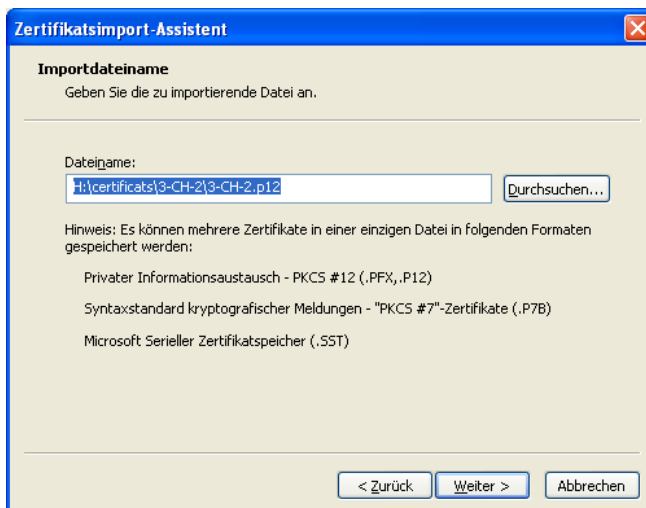
Im **Windows Explorer**, Doppelklick auf das Zertifikat mit dem gesuchten Verfallsdatum.

2



Einführungsbildschirm.  
Auf **Weiter** klicken

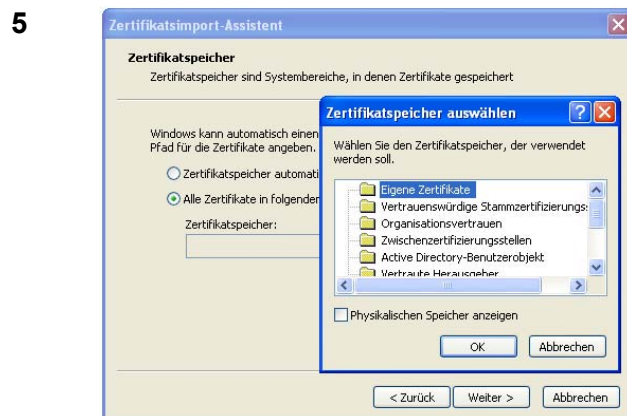
3



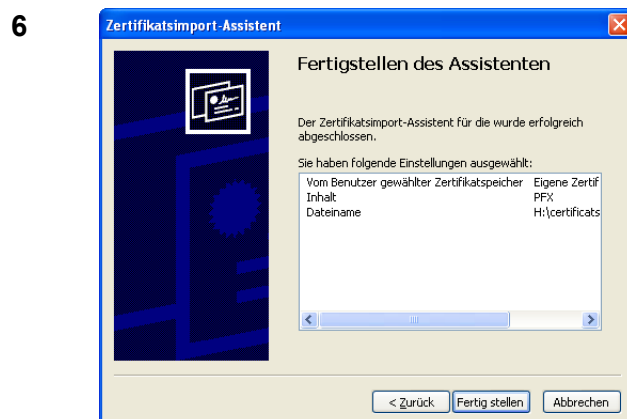
Das gewählte Zertifikat ist standardmässig angezeigt.  
Auf **Weiter** klicken.



Das Kennwort des Organisationszertifikates eingeben  
(in der conf/password.txt oder conf/certificateConfiguration.xml Datei definiert).  
Auf **Weiter** klicken.



Auf **Durchsuchen** klicken und « **Eigene Zertifikate** » wählen.  
Auf **Weiter** klicken.



Auf **Fertig stellen** klicken.

7

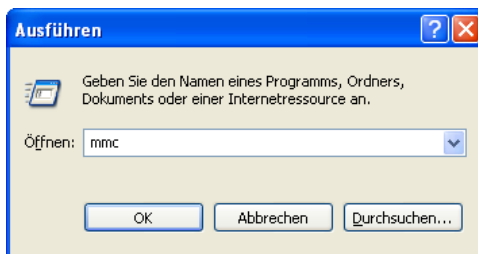


Auf **OK** klicken.

8

 → **Ausführen**

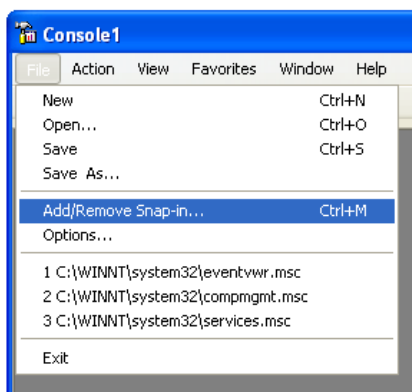
9



"mmc" eingeben.

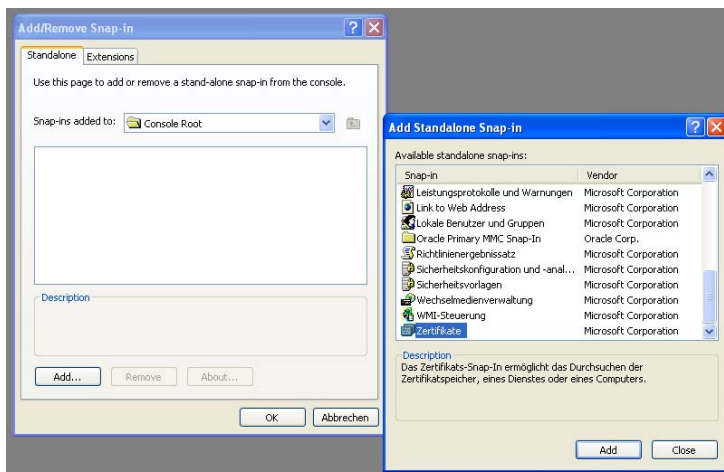
Auf **OK** klicken.

10



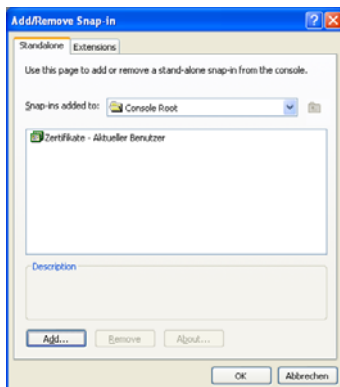
Auf **File** klicken und **Add/Remove Snap-in** wählen.

11



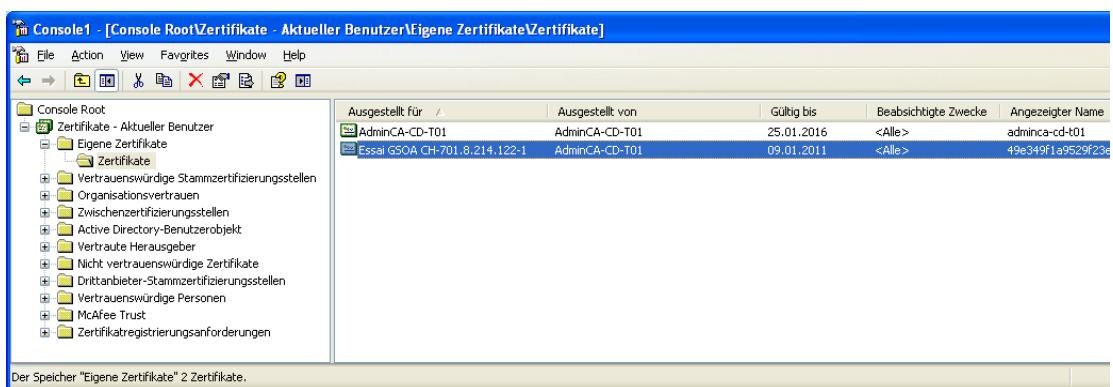
Auf **Add** klicken und den Snap-in « **Zertifikate** » wählen.  
Auf **Add** dann **Close** klicken.

12



Die Wahl des Snap-in mit **OK** bestätigen.

13



Das Zertifikat und dessen Verfallsdatum erscheinen unter

- ↳ Zertifikate – Aktueller Benutzer
  - ↳ Eigene Zertifikate
    - ↳ Zertifikate