



sedex-Adapter User Manual

Project Name: sedex
Project Number: LZGPR07-00259
Version: 3.0

Status in Process for approval approved to be used

Parties involved	
Author:	Sergey Abagyan
Users:	Business and technical users who partake to sedex: communes, cantons and the BFS

Change Management and approval			
When	Version	Who	Description
10.01.2008	1.0	Sergey Abagyan	Final version
04.02.2008	1.0.2	Sergey Abagyan	Added the property for local DB cleaning
18.04.2008	1.1.3	Thomas Schmidt	Version number changed, Logging Configuration
18.04.2008	1.1.4	Thomas Schmidt	Version number changed, formatting changed
23.09.2008	1.3.0	Thomas Schmidt	Version number changed
03.11.2008	2.0	Thomas Schmidt	Final version 2.0
22.04.2009	2.0.9	Markus Antener	Updated for 2.1
06.07.2009	2.1	Jörg Böhlen	Genehmigung
27.11.2009	2.2	Markus Antener	Added new requirements for firewall
25.02.2011	3.0	Markus Antener	Updated for Adapter 3.0

Table of contents

1	INTRODUCTION	4
1.1	sedex-Adapter	4
1.2	Overview	4
1.3	Adapter Interface	6
1.4	References.....	6
2	INSTALLATION	7
2.1	System requirements	7
2.1.1	Supported Platforms	7
2.1.2	CPU.....	7
2.1.3	RAM	7
2.1.4	Disk Space	7
2.1.5	Maximum Message Size.....	8
2.1.6	Firewall.....	8
2.1.7	Network Speed.....	8
2.2	Delivery Content	9
2.3	Installation Steps	10
2.3.1	Verify Prerequisites.....	10
2.3.2	Extract Adapter Archive	10
2.3.3	Environment Configuration	11
2.3.4	Install JAVA JCE unlimited strength policy files.....	11
2.3.5	Adapter Configuration	11
2.3.6	Logging Configuration.....	13
2.4	Installation Check	13
2.5	Migration Notes	14
3	STARTING THE ADAPTER	15
3.1	Manual Start.....	15
3.2	Automatic Start (Installation as a Service).....	15
3.2.1	UNIX.....	15
3.2.2	Windows.....	16
3.3	Install several Adapter Instances on the same Machine	16
4	ADAPTER CONFIGURATION REFERENCE	18
4.1	Adapter Configuration	18
4.2	Certificate configuration	19
4.2.1	Optional elements	20
4.3	Logging Configuration	21
5	MONITORING	23
6	COMMON PROBLEMS AND SOLUTIONS	24
7	APPENDIX	25

sedex-Adapter User Manual (English)

7.1	Glossary	25
7.2	Receipt Versions	25
7.2.1	Overview	25
7.2.2	Version 1.0.....	25
7.2.3	Version 2.0.....	26

1 Introduction

This document describes the Sedex-Adapter installation and configuration. The Sedex-Adapter is a Java application that is required on end-systems to securely and reliably exchange messages between sedex participants. The end-systems are typically Swiss communes, cantons and federal offices like BFS, ZAS, and Infostar.

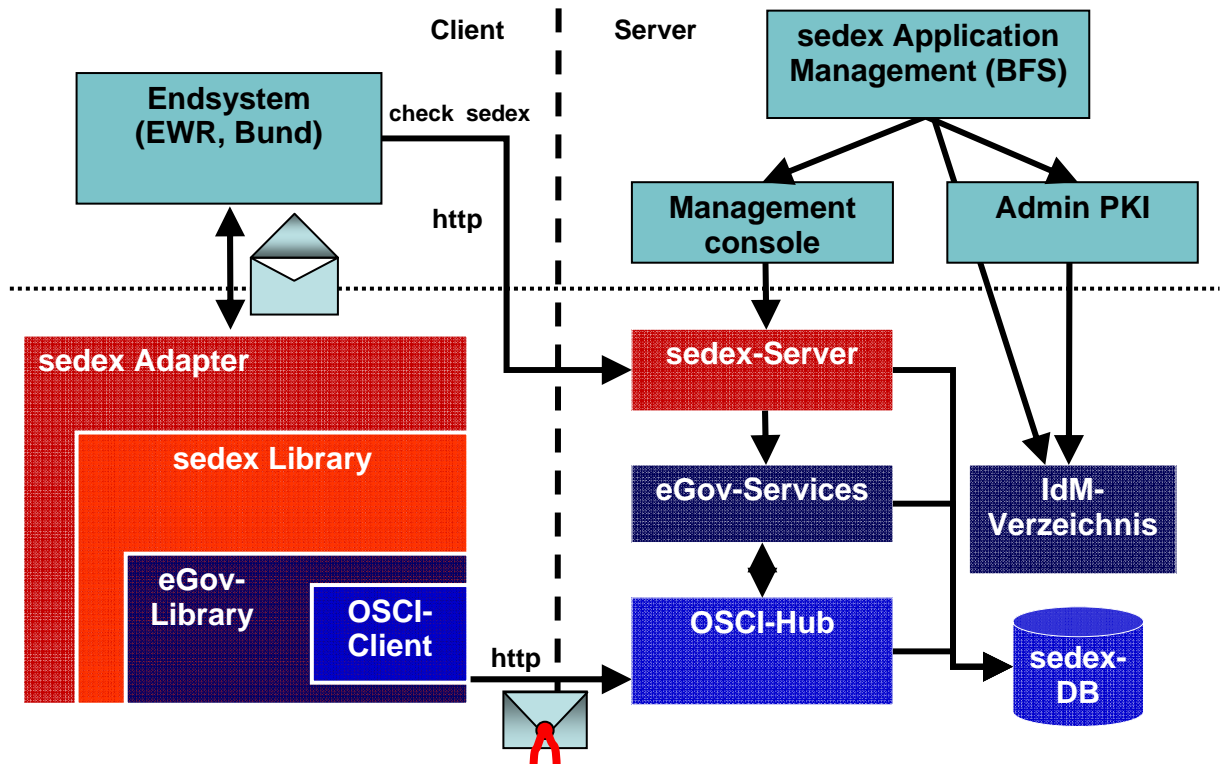
1.1 sedex-Adapter

The sedex-Adapter provides the following functionalities:

- secure transport of sensitive data (International and Swiss standard on data security level 3)
- sender side message encryption for target recipients – only the recipients can decrypt the message)
- message content integrity check through digital signatures
- reliable transport for very large messages (1 GB or higher compressed or uncompressed)
- sending and receiving of messages are indisputable
- audit trail of the message exchange (envelope information only)

1.2 Overview

The figure below gives an overview of the server components:



The server components can be divided into "client side", "server side" and "external systems".

Components on the client side include:

- **Sedex Adapter** includes all the functions that are necessary for a secure and reliable exchange of messages on the client side and can be further divided into:
 - **OSCI-Client** implements the OSCI-Protocol for a secure message exchange based on certificates; it communicates with the OSCI-Hub.
 - **eGov-Library** uses the OSCI-Client and completes it with additional functions such as message segmentation, message publish, public keys lookup, logging, status persistency, status monitoring and alerting.
 - **sedex-Library** makes use of the eGov-Library for a secure and reliable message exchange and completes it with functions such as message envelopes validation, message mapping to the subscription topic, configuration, routing and authorization.
 - **Adapter** is a Java standalone application, which makes use of the sedex-Library and serves as interface between the sedex system and the participant end-systems.
 - **Wrapper**: The Wrapper makes it possible to install a Java application as a Windows Service. For more information about the wrapper visit the wrapper home page¹.

Components on the server side are:

- **OSCI-Hub** (Meldungs-Intermediär) covers the core functions of the server for a secure and reliable message exchange. The OSCI-Hub provides an inbox for each participant who owns a certificate. The OSCI-Client communicates via http with the OSCI-Hub through polling.
- **eGov-Services** (eGov-Dienste) complement the functions of the OSCI-Hub with generic functions like reporting.
- **sedex-Server** includes services for the message transport as well as further modules and interfaces for the participants administration. Its services cover specific functions, particularly authorization and routing.
- **IdM-Directory** (IdM-Verzeichnis): Metadirectory of the system participants that provides interfaces to the data sources.
- **Sedex-Database** is used by the OSCI-Hub, the eGov-Services and the sedex-Server. They use different schemas inside the same physical database.

External systems are:

- **Office directory** (Amtsstellenverzeichnis): The office directory holds data on Swiss communes, cantons and federal offices like BFS, ZAS, Infostar, and so on. For the time being, the Office directory is administered by the BFS (Federal Statistical Office). It will be superseded by the BK (Federal Chancellery) Office directory in the future.
- **Admin PKI** is the BIT (Federal Office for Information Technology and Telecommunication) Certificate Authority that delivers certificates for physical entities (persons) as well as legal entities (organizations).
- **SAP CRM**: sedex “service clientele” or customer care management system, which takes care of the contracts with the sedex- participants, and therefore their authorization and representation.

¹ see <http://wrapper.tanukisoftware.org/doc/english/introduction.html>

- **Endsystems** (Teilnehmersysteme): Endsystems that use the platform for message exchange such as communes, cantons and federal registers.

1.3 Adapter Interface

A file-based interface is used between the EWR system and the sedex-Adapter. The EWR systems have to save the data and the envelope in the outbox directory and have to poll the inbox directory for new data and envelopes.

- Envelope
 - XML format
 - naming convention: envl_XXX.xml
 - must be compliant to the envelope Schema Definition (XSD)
- Reference data
 - XML format
 - naming convention: data_XXX.xml
 - must be compliant to the Schema Definition (XSD) specified in the XML

The base name (XXX in this example) must match. The envelope and reference data files must be placed into the same directory. The Adapter will transfer the data only, if the corresponding envelope is compliant with the XML schema eCH-0090.

The detailed structure of the envelope and interface between EWR system and adapter is specified in [1].

1.4 References

[1] sedex-Handbuch v4.0 (14.04.2011)

[1] Manuel sedex v4.0 (14.04.2011)

2 Installation

The sedex-Adapter is a Java standalone application. It has to be installed in the network zone of the participant, which shall be physically connected to the sedex platform. It can be installed on the same server as the participant system, if that server fulfils the system requirements described below.

The sedex-Adapter is provided in a compressed archive format (ZIP file).

Note: *to make sure that the sedex-Adapter is able to run after the machine is rebooted, it is required to configure it as a service (Windows) or with start script on UNIX.*

2.1 System requirements

2.1.1 Supported Platforms

The sedex-Adapter is a pure Java application. It runs on all platforms supporting Java 1.6.0 or later. However, the sedex-Adapter was only fully tested on the following platforms:

- Windows 2003 Server 64Bit
- Windows XP
- Windows Vista Enterprise (equivalent to Windows Vista Business version)
- SuSE Linux 11.0

2.1.2 CPU

As the sedex-Adapter is not a CPU time consuming application, any CPU capable of running a supported operating system is sufficient.

2.1.3 RAM

There should be at least 256MB of memory available for the sedex-Adapter.

2.1.4 Disk Space

The disc space needed for the sedex-Adapter installation is about 200MB. The disc space needed for the sedex-Adapter at runtime heavily varies depending on the size of sent and received messages, the frequency of sent and received messages, and finally on the time, sent and received messages are kept in their inbox, outbox, or sent messages directory. The following section provides general rules for disc space planning when maintaining a sedex-Adapter. Please note that all values below require a network connection capable of transferring large messages within a reasonable timeframe. For limitations imposed by the network connection, please see chapter 2.1.7 "Network Speed"

Sending messages: during the time when sending a message, approximately 3 times the sum of all concurrently send messages is required. The required disk space is distributed as follows:

- The outbox directory must be capable of holding all messages to send at one time including the envelope files.

- The adapter installation directory must be capable of holding data equal to the size of three times of all messages to send at one time.
Note: if the adapters outbox directory is located within the adapters installation directory, its space requirement must be added resulting in a minimum free space of 4 times equal to the size of all messages to be send at one time.
- The sent messages directory must be capable of holding all messages to send at one time including the envelope files.

Please note that the adapter will remove a sent message from the outbox directory, but will never remove any messages from the sent messages directory. Therefore, the sent messages directory must be capable of holding all ever sent messages until cleaned.

Receiving messages: during the time when receiving a message, approximately 3 times the sum of all concurrently received messages is required. The required disk space is distributed as follows:

- The inbox directory must be capable of holding all messages to receive at one time including the envelope files.
- The adapter installation directory must be capable of holding data equal to the size of 3 times of all messages to send at one time.
Note: if the adapter inbox directory is located within the adapter installation directory, its space requirement must be added resulting in a minimum free space of 4 times equal to the size of all messages to be received at one time.

Please note that the adapter will never remove a received message from the inbox directory. Therefore, the inbox directory must be capable of holding all ever received messages until cleaned.

2.1.5 Maximum Message Size

The maximum size of a single message the adapter can send is currently limited to 10GB.

2.1.6 Firewall

The Sedex Adapter uses the following outgoing connections:

- www.governikus.admin.ch port 80
- www.oscivt-gw.admin.ch port 443
- www.sedex-gw.admin.ch port 443
- www.osciservices-gw.admin.ch port 443

Make sure that these connections are allowed

2.1.7 Network Speed

Sedex needs a connection that can upload **5 Megabytes in 5 Minutes**. Therefore, the **minimum recommended upload speed for sedex is 150 kbit/s**.

Please note that this recommendation assumes that the whole bandwidth of the network connection is available for the adapter. If the adapter has to share the available bandwidth with other applications using networking resources, it might be necessary to increase the capability of the network connection. Otherwise, message transmission using the sedex-Adapter might not be successful.

The following table gives an overview over the amount of time which is required to transfer the payload of a message.

Network speed / message size	150 kbit/s	300 kbit/s	1'000 kbit/s	10'000 kbit/s
5 MB	4,5 minutes *	2,3 minutes *	36 seconds *	3,6 seconds *
50 MB	44,5 minutes *	22,3 minutes *	6,6 minutes *	36 seconds *
500 MB	7,4 hours *	3,7 hours *	1,2 hours *	6,7 minutes *
1000 MB	14,8 hours *	7,4 hours *	2,3 hours *	13,4 minutes *

Table 1: Payload transfer times

* These values are only transmit times for the payload of a message. You must consider that a real sedex Message has some overhead which may extend the real transmit time especially for small messages.

2.2 Delivery Content

The sedex-Adapter software is delivered as a ZIP file that has to be extracted to the target installation directory. The folder structure looks as follows:

sedexAdapter.zip:

Directory	Description
/axis2	Webservice Proxy files
/bin	Scripts to manually start and stop the sedex-Adapter: start.bat/stop.bat start.sh/stop.sh
/conf	Configuration files: sedexAdapter.properties – sedex-Adapter properties file log4j.xml – logging properties file wrapper.conf – configuration for installing adapter as Windows service certificateConfiguration.xml – configuration of Credentials (Certificate and Password)
/deploy	Deploy directory for Webservice Proxy
/eGovTmp	This directory is auto created on the first start of the adapter. Used as a temporary directory for eGov-Library.
/h2db	Database for eGov-Library
/inbox	Default "inboxDir" location.
/internalmessages	Directory for sending and receiving internal messages. This directory is managed by the adapter itself.
/jce	Java Cryptography Extension Policy files for Unlimited Strength. Provided for sun and ibm based java runtime environment.
/lib	Contains all required libraries
/logs	Contains all logs
/messagestorage	Default messagestorage location. Used by the adapter to manage registered outgoing messages.

/outbox	Default "outboxDir" location.
/receipts	Default "receiptsDir" location.
/schema	All schemas used by the adapter. This Directory contains also the eCH0090 schema which is used for sedex messages.
/sent	Sent messages will be put here. Please note that this directory will keep all sent messages by the adapter. This might result in a full filesystem if messages are not frequently removed from the sent directory.
/zertifikate	Private Keys and Certificates needed to communicate with OSCI server

2.3 Installation Steps

To install the adapter, run the following steps:

1. verify prerequisites
2. extract adapter archive
3. environment configuration
4. adapter configuration
5. installation check

Please see for the following chapters for a description of each topic.

2.3.1 Verify Prerequisites

Java 6 must be installed on the target machine. It is possible to install and configure the sedex-Adapter without Java, but to run the adapter, Java must be installed.

2.3.2 Extract Adapter Archive

The sedex-Adapter is shipped as a ZIP file. To install the adapter, extract the ZIP file into a directory of your choice. The ZIP archive contains a top-level directory called "SedexAdapter_<version>", so there is no need to create a separate adapter top-level directory before extracting the archive.

Additional steps on UNIX:

When installing on UNIX, some additional steps are necessary after extracting the archive:

1. Change into the directory <SEDEX_HOME>/bin.
2. Change the file type of the start/stop scripts from Dos to UNIX, for example by using the dos2unix program:

```
dos2unix start.sh  
dos2unix stop.sh
```

If dos2unix is not available on your system, install the appropriate package or use any other command capable of converting the file format from DOS to UNIX.

3. Change the permissions of the start/stop scripts:

```
chmod +x start.sh stop.sh
```

2.3.3 Environment Configuration

The following system environment variables must be set:

- JAVA_HOME – location of JRE 6.0x

To setup this variable in your current shell, you run the following commands:

Windows

```
set JAVA_HOME=C:\Program Files\Java\jre1.6.0_09
```

UNIX (depends of shell script, this example is for bash)

```
export JAVA_HOME=/usr/java/jre1.6.0_09
```

Usually, the JAVA_HOME variable is set either as a system variable on Windows, or is set during login on UNIX by adding the variable assignment to a shell startup script, for example ~/.profile.

2.3.4 Install JAVA JCE unlimited strength policy files

Due to import control restrictions, the version of JCE policy files that are bundled in the JRE(TM) 6 environment allows "strong" but limited cryptography to be used. Sedex needs to have the "Unlimited Strength Java(TM) Cryptography Extension Policy Files" installed in your local java runtime environment (Java installation).

The sedex package contains these policy files for Sun based and IBM Java VMs. The files are located in:

- <adapter-home>\jce\sun (e.g. c:\sedex\jce\sun)
- <adapter-home>\jce\ibm (e.g. /opt/sedex/jce/ibm)

To install it, simply copy all *.jar files contained in the corresponding folder above into the following directory of your runtime environment (overwrite the same existing files):

- <JRE>\lib\security
(e.g. c:\program files\java\jre6\lib\security or /usr/java/jdk1.6/bin/lib/security)

Those policy files can also be downloaded directly from the Sun or the IBM homepage.

2.3.5 Adapter Configuration

As soon as the sedex-Adapter is extracted, you need to configure the file
<SEDEX_HOME>/conf/sedexAdapter.properties.

While the chapter 4.1 "Adapter Configuration" describes all configuration values, the following paragraph provides the list of setting values, which **must** be set for the adapter to run. More options can be set if necessary. Most notably, you must configure the proxy settings if your adapter sits behind a proxy server.

Variable	Description
sedex_home	Directory, where the sedex-Adapter is installed. This is the directory, where the ZIP file was extracted including the top-level directory in the ZIP file. For example "c:/software/SedexAdapter_1.1"

	It is important to use the “/” sign as a path separator, even on Windows.
adapterSedexId	The adapter Sedex-ID
receiptConfiguration	<p>Configures the receipt version. Defines the used error codes and xml namespace for generated receipts. By default, the newest configuration is activated.</p> <p>For Backward compatibility, older version can also be configured. Possible values are: V2_0, V1_0. See chapter 7.2 for Details.</p> <p>Please note that this only refers to the receipt. The schema for the envelope files is independent of this option.</p>

Further, you need to configure the path and password to your private certificate. For this, the following xml file has to be edited:

<SEDEX_HOME>/conf/certificateConfiguration.xml

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

<certificateConfiguration
xmlns="http://www.sedex.ch/xmlns/certificateConfiguration/1/0">

  <privateCertificate>

    <location> (1) </location>

    <password> (2) </password>

  </privateCertificate>

  <transportCertificate>

    <location>${SEDEX_HOME}/zertifikate/prod-bit/AdminCA-CD-
T01.cer</location>

  </transportCertificate>

  [...]

</certificateConfiguration>
```

- (1) Insert the path to the location where you have put your private certificate between <location> and </location>.

You can use \${SEDEX_HOME} to specify a path relative to sedex_home, but you can also use an absolute path.

e.g. <location>\${SEDEX_HOME}/zertifikate/prod-bit/T501.p12</location>

(2) Insert your password between `<password>` and `</password>`

e.g. `<password>myPassword123</password>`

2.3.6 Logging Configuration

The file `<SEDEX_HOME>/conf/log4j.xml` can be edited before starting the adapter. A possible change is related to the “sedex-logfile” appender tag, where the inner `<param>` tag with the value attribute currently set to “./logs/sedexAdapter.log” can be changed according to your preferred path and logfile name.

2.4 Installation Check

To verify a correct installation and configuration, the adapter can be started and a test message can be send.

To start the adapter, run the steps described in chapter “Starting the Adapter”, section “Manual Start”. When configured correctly, the adapter starts up and polls for inbound/outbound messages. In case of an error, the adapter will terminate with an error message. Most often, this leads to a wrong configuration. Please see chapter “Common Problems and Solutions” for common configuration mistakes.

After the adapter has successfully started, a test message can be send. To send a test message, create two text files with a text editor:

1. `data_test.txt`
In this file, simply enter some text. This file contains the data to be transferred.
2. `envl_test.xml`
In this envelope file, enter the metadata for the message. A typical envelope file looks like follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<eCH-0090:envelope version="1.0" xmlns:eCH-
0090="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 eCH-
0090-1-0.xsd ">
<eCH-0090:messageId>TestMessageId</eCH-0090:messageId>
<eCH-0090:messageType>94</eCH-0090:messageType>
<eCH-0090:messageClass>0</eCH-0090:messageClass>
<eCH-0090:senderId>Your Sedex ID here</eCH-0090:senderId>
<eCH-0090:recipientId>Your Sedex ID here</eCH-
0090:recipientId>
<eCH-0090:eventDate>2008-02-06T13:30:00</eCH-0090:eventDate>
<eCH-0090:messageDate>2008-02-06T13:30:00</eCH-
0090:messageDate>
</eCH-0090:envelope>
```

Please note that you must replace the string “Your Sedex ID here” with the sedex-ID you have placed in the configuration file. Further, you may have to amend the “messageType” and “messageClass” entity values to match the allowed message types for your sedex-ID.

Finally, copy or save the files into the sedex-Adapter outbox directory. If the sedex-Adapter is configured correctly, sedex will send the message, and as the message recipient is the sending adapter itself, the send message will appear in your adapter inbox directory. While the adapter is sending the message, you can monitor the adapter log file to see its progress or detect possible errors.

2.5 Migration Notes

When updating to a new version of the Sedex Adapter, you have to extract the archive to a new directory and do the configuration again. For safety reasons it is advisable to backup the old files if you want to reuse the same directory.

When you run the Sedex Adapter as a Windows Service, the service should be stopped (using Windows Service Management) and deregistered (using the script `UninstallWindowsService.bat` shipped with the Sedex Adapter) before installing the new version. Also, when updating an existing installation, please make sure to configure the same Window Service Name as for the existing installation.

3 Starting the Adapter

3.1 Manual Start

The sedex-Adapter can be started / stopped by running the following commands in the <sedex_home>/bin folder from within a command line:

Windows:

- <sedex_home>\bin\start.bat - to start the adapter
- <sedex_home>\bin\stop.bat - to stop the adapter

UNIX:

- <sedex_home>/bin/start.sh - to start the adapter
- <sedex_home>/bin/stop.sh - to stop the adapter

Important: please set first the configuration described in chapter “Configuration”.

3.2 Automatic Start (Installation as a Service)

3.2.1 UNIX

Overview

The Adapter is distributed with a service wrapper from Tanuki Software. This wrapper allows the sedex adapter to be run as a detached daemon process.

The Wrapper supports many operating Systems. The adapter provides binaries for the following systems:

- Linux ppc / x86 / x86 64
- AIX ppc 32 / ppc 64
- OSX ppc / universal
- Solaris Sparc 32 / Sparc 64 / x86

If your system is not in this list, check <http://wrapper.tanukisoftware.org> to download additional modules.

Prepare the wrapper

Before you can start, you have to change permission for start script and the appropriate unix wrapper:

```
chmod +x sedexAdapterWrapper.sh

chmod +x libwrapper-linux-x86.so    (please choose the appropriate
file)
```

Start the wrapper

Start the wrapper by executing script using the start command.

```
Adapterdir/bin/sedexAdapterWrapper.sh start
```

To stop the application rerun the script using the stop command.

```
Adapterdir/bin/sedexAdapterWrapper.sh stop
```

To check the current status, run the script using the status command.

```
Adapterdir/bin/sedexAdapterWrapper.sh status
```

To start the wrapper with console output just use the command

```
Adapterdir/bin/sedexAdapterWrapper.sh console
```

Integrate the wrapper

To start the adapter automatically at boot time, just add the wrapper to your etc/init. For more info about the wrapper visit <http://wrapper.tanukisoftware.org/>

3.2.2 Windows

If you want to start the adapter automatically (for example after reboot), run InstallAsService.bat to install the sedex-Adapter as a service. To uninstall it use the script UninstallWindowsService.bat.

You can also reconfigure the service installation settings using <sedex_home>/conf/wrapper.conf. For more information about starting a java program as a Windows service, see <http://wrapper.tanukisoftware.org/>.

Note: you have to configure the adapter before installing it as service. Don't forget to configure conf/log4j.xml as the path to the log file must be absolute when used as Windows service.

3.3 Install several Adapter Instances on the same Machine

You can install as many adapters on the same machine as you want. To install a new one adapter you just have to unzip the provided sedex_adapter.zip in a different directory and configure it anew.

When installing it under Windows as a service, each instance requires a separate service name. The service name is defined in the <sedex_home>/conf/wrapper.conf file. To set a

sedex-Adapter User Manual (English)

new service name, edit this file with a text editor and change the values of the following two configuration entries from "SedexAdapter" to a different name:

```
wrapper.nts-service.name=SedexAdapter  
wrapper.nts-service.displayname=SedexAdapter
```

For example:

```
wrapper.nts-service.name=SedexAdapter2  
wrapper.nts-service.displayname=SedexAdapter2
```

4 Adapter Configuration Reference

4.1 Adapter Configuration

Property	Description	Default Value
Basic Configuration		
sedex_home	Directory, where sedex-Adapter is installed. For example c:/sedex_adapter. It is important to use the "/" sign as a path separator, even on Windows.	n/a
sendingSentToServerMsg	If set to true, generate a receipt for each recipient after successfully sending a message to the server.	false
inboxDir	Location of received and already decrypted files for EWR applications. The EWR applications will read the files from this directory.	\${sedex_home}/inbox
outboxDir	Directory for files waiting for encryption and transmission. The EWR applications will place those files here.	\${sedex_home}/outbox
sentItemsDir	Sent messages will be saved here	\${sedex_home}/sent
receiptDir	Location of receipts for EWR applications. The EWR applications will read the files from this directory. If not set, the default location "<sedex_home >/receipt" is used.	\${sedex_home}/receipt
receiptConfiguration	For Backward compatibility, older version can also be configured. Possible values are: V2_0, V1_0. See chapter 7.2 for Details.	V2_0
Configuration of credentials		
adapterSedexId	Adapter sedex-ID	n/a
Proxy		
ch.admin.bit.egov.egovlib.transport.osci.TransportFactoryImpl.proxy.host	Proxy host <i>Note: you should not use Erreur ! Référence de lien hypertexte non valide. in proxy host, it must looks like: <code>myproxy.server.ch</code></i>	n/a, by default is not used

Property	Description	Default Value
<code>ch.admin.bit.egov.egovlib.transport.osci.TransportFactoryImpl.proxy.port</code>	Proxy port	n/a, by default is not used
<code>ch.admin.bit.egov.egovlib.transport.osci.TransportFactoryImpl.proxy.user</code>	Proxy user. You can also use proxy without a user/password	n/a, by default is not used
<code>ch.admin.bit.egov.egovlib.transport.osci.TransportFactoryImpl.proxy.password</code>	Proxy password. You can also use proxy without a user/password	n/a, by default is not used
Cleanup		
<code>cleanSentFilesOlderThan</code>	Clean sent messages which are older than the number of days specified (use -1 to disable automatic message deletion)	-1

4.2 Certificate configuration

The configuration for certificates and private keys is located in an external xml-file, in `conf/certificateConfiguration.xml`. The file has the following structure:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<certificateConfiguration xmlns="http://www.sedex.ch/xmlns/certificateConfiguration/1/0">
  <privateCertificate>
    <location>(location)</location>
    <password>(password)</password>
  </privateCertificate>
  <transportCertificate>
    <location>${SEDEX_HOME}/zertifikate/prod-bit/AdminCA-CD-T01.cer</location>
  </transportCertificate>
  <webserviceTruststore>
    <location>${SEDEX_HOME}/zertifikate/prod-bit/adaptertrust.jks</location>
    <password>trustme</password>
    <truststoretype>JKS</truststoretype>
  </webserviceTruststore>
</certificateConfiguration>
```

The field `location` has to point to a valid p12 keystore containing the private key, the field `password` holds the appropriate password to the keystore.

An Adapter is able to handle more than one certificate:

```
[...]  
<privateCertificate>  
  <location>(location 1)</location>  
  <password>(password 1)</password>  
</privateCertificate>  
<privateCertificate>  
  <location>(location 2)</location>  
  <password>(password 2)</password>  
</privateCertificate>  
[...]
```

4.2.1 Optional elements

The following elements are optional and mostly set by the adapter itself.

- **Restriction:** This element is mostly likely set by in the automatic certificate renewal.

```
[...]  
<privateCertificate>  
  <location>(location)</location>  
  <password>(password)</password>  
  <restriction>READONLY</restriction>  
</privateCertificate>  
[...]
```

Possible restrictions are:

Restriction Type	Impact
READONLY	This certificate cannot be used for sending messages, only for receiving
DISABLED	This certificate cannot be used at all

- **Optional Info:** When the adapter updates the certificate configuration, it also adds the optional element **optionalInfo** for informational purposes

```
<privateCertificate>
  <location>(location)</location>
  <password>(password)</password>
  <optionalInfo>
    <issuer>CN=vAdminCA-CD-T01,OU=Certification[...]</issuer>
    <serial>4545</serial>
    <expirydate>2012-06-19T13:34:50.000+02:00</expirydate>
  </optionalInfo>
</privateCertificate>
```

4.3 Logging Configuration

Logging in sedex-Adapter based on [Log4j](#), a powerful log manager that supports the Commons Logging Interface.

Your logging configuration file is located in `<sedex_home>/conf/log4j.xml` file, and look something like this:

Default console appender, used to write log direct in console

```
<appender name="stdout" class="org.apache.log4j.ConsoleAppender">
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern"
      value="%d{ABSOLUTE} %5p %c{1}:%L - %m%n" />
  </layout>
</appender>
```

This appender write the logs in rolling files

```
<!-- Properties for file appender, we use rolling file -->
<appender name="sedex-logfile"
  class="org.apache.log4j.RollingFileAppender">
  <!-- Where to write log files -->
  <param name="file"
value="c:/Temp/SedexAdapter_0.9.4/logs/sedex-adapter.log" />
  <!-- After restart we add new log to last file -->
  <param name="Append" value="true" />
  <!-- each file has maximal size 10MB-->
  <param name="MaxFileSize" value="10MB"/>
  <!-- we write 5 files, then logger will be "rolled" -->
  <param name="maxBackupIndex" value="5"/>
  <!-- used layout -->
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern"
      value="%d{ISO8601} %-5p [%t] %c: %m%n" />
  </layout>
</appender>
```

sedex-Adapter User Manual (English)

```
<!-- logger for sedex classes -->
<category name="ch.admin.bit.sedex">
  <!-- logging level -->
  <level value="INFO" />
  <!-- used appenders -->
  <appender-ref ref="sedex-logfile" />
  <appender-ref ref="stdout" />
</category>
<!-- logger for eGovLib classes -->
<category name="ch.admin.bit.egov">
  <!-- logging level -->
  <level value="INFO" />
  <!-- used appenders -->
  <appender-ref ref="sedex-logfile" />
  <appender-ref ref="stdout" />
</category>
<!-- root logger -->
<root>
  <level value="ERROR" />
</root>
```

5 Monitoring

The sedex-Adapter can be monitored like any other standard process or registered service. When registered and run as a service on Windows, the Windows Computer Management Console can be used to check or change the status of the adapter.

The adapter itself does not provide any further monitoring services by itself.

6 Common Problems and Solutions

The following section describes some often encountered problems and how to fix them.

1. The Adapter cannot restart after a crash.

Solution: please check and delete (if exist) the file `<sedex_home>/adapter.lock`

2. Message in logfile:
Could not start engine: JCE is not installed properly.

Solution:

Install the jce policy files in your local vm as described in chapter 2.3.4: Install JAVA JCE unlimited strength policy files

3. Message in logfile:
java.lang.SecurityException: Invalid Password or invalid private certificate

Solution: open `<sedex_home>/conf/certificateConfiguration.xml` and check the password and location to the private certificate

4. Message in logfile:
Could not find private key file in <[...]>

Solution: open `<sedex_home>/conf/certificateConfiguration.xml` and fix the path the private certificate

5. A message was not received; instead a receipt containing the text "Not allowed to send" arrived at the sender.

Solution: check if the configured sedex-ID is allowed to send messages.

6. A message was sent by the adapter but was not received. No receipt arrived, no error was written in the adapters log file.

Solution: the receiving adapter might be down or not responsive. (Re-)start the receiving adapter.

7 Appendix

7.1 Glossary

Term	Definition
BFS	Federal Statistical Office
CA	Certificate Authority
Keystore	A keystore is a database of keys. Private keys in a keystore have a certificate chain associated with them, which authenticates the corresponding public key. A keystore also contains certificates from trusted entities.
Meta-directory	Identity management component used to harmonize two different directories by mapping the meta-data together
PKI	Public Key Infrastructure which implements an independent trusted third-party which vouches for the real identity of IKT users
public key certificate	You can think of a public key certificate as the digital equivalent of a passport.

7.2 Receipt Versions

7.2.1 Overview

New Releases may contain new Message Codes and may use a different xml namespace that requires changes in the application. To offer backward compatibility, the adapter can be configured to use an old message error schema with old message error codes.

7.2.2 Version 1.0

Since: Adapter 1.0

Receipt xml namespace: eCH0090/1

Configuration setting: receiptConfiguration = V1_0

Full list of Codes:

Code	Remark
100	Message correct transmitted
200	Invalid Envelope Syntax
201	Duplicate Message ID
202	No payload found
300	Unknown sender id
301	Unknown recipient id
302	Unknown physical sender id
303	Invalid message type
304	Invalid message class

Code	Remark
310	Not allowed to send
311	Not allowed to receive
312	User certificate not valid
320	Message expired
400	Network error
401	OSCI hub not reachable
402	Directory not reachable
403	Logging service not reachable
500	Internal error

7.2.3 Version 2.0

Since: Adapter 2.0

Receipt xml namespace: eCH0090/2

Configuration setting: receiptConfiguration = V2_0

New Codes since version 1.0:

Code	Remark
203	Message too old to send
204	Message expired
313	Other recipients are not allowed to receive
330	Message size exceeds limit
404	Authorisation service not reachable
501	Error during receiving
601	Message successfully sent
701	Message expires soon

Deprecated Codes since 1.0:

Code	Remark
320	Changed to Code 204 Message expired

Full list of Codes:

Code	Remark
100	Message correct transmitted
200	Invalid Envelope Syntax
201	Duplicate Message ID
202	No payload found
203	Message too old to send
204	Message expired

sedex-Adapter User Manual (English)

Code	Remark
300	Unknown sender id
301	Unknown recipient id
302	Unknown physical sender id
303	Invalid message type
304	Invalid message class
310	Not allowed to send
311	Not allowed to receive
312	User certificate not valid
313	Other recipients are not allowed to receive
330	Message size exceeds limit
400	Network error
401	OSCI hub not reachable
402	Directory not reachable
403	Logging service not reachable
404	Authorisation service not reachable
500	Internal error
501	Error during Receiving
601	Message successfully sent
701	Message expires soon