Red Book

eSchKG
Networking

Exchange of Electronic Business
Information in the Domain of Debt
Enforcement and Bankruptcy

MessageHandler: **Version 3.1.1**

Edition: **March 2014**

References

[1]   *Sedex Handbuch Version 4.0.3*, Bundesamt für Statistik, 15.11.2012

[2]   *Open eGov MessageHandler v3.1.1 Technical Documentation*, Glue Software Engineering, 13.03.2013

Table of Contents

About This Document

> **This document addresses integrators and architects responsible for operating software connecting to the eSchKG community network.**

This document is a guide to using MessageHandler v3 in the eSchKG community network. It is a complementary manual to the Sedex user manual [1] and the Open eGov MessageHandler technical documentation [2], both of which are considered mandatory reading along with this document.

> **In this document "MessageHandler v3" is mentioned without specifying the minor version. Actually, we mean the *latest version of the MessageHandler software package having major version 3.***

About eSchKG

The eSchKG standard is a normative framework for the exchange of electronic business information between parties in a debt collection. eSchKG is being published by the Swiss Federal Office of Justice, comprising the following documentation:

- White Book: *Einführung in den eSchKG Standard, Ausgabe März 2014*. An introduction to eSchKG mainly addressing the executive. Available in German, French and Italian;

- Orange Book: *Anleitung für die Mitgliedschaft im eSchKG Verbund, Ausgabe März 2014*. A step-by-step guide to joining the eSchKG community network, including preparatory work and administrative tasks. Available in German, French and Italian.

- Red Book: *eSchKG Networking.* **This document.** A technical guide to connecting an enterprise system to the eSchKG community network. Available in English;

- Blue Book: *Exchange of Electronic Business Information in the Domain of Debt Enforcement and Bankruptcy (Schema Version 2.0.014), Edition March 2014*. An introduction to the architectural principles, data model and high-level protocols. This document comprises two appendices:
  - Appendix 1: *XML Reference*;
  - Appendix 2: *Testbed User Manual.*

  The Blue Book and appendices are available in English.

> **In order to become a full member of the eSchKG network, applicants are required to adhere to the administrative procedures outlined in the Orange Book.**

The full standard specification is available online: www.eschkg.ch

Licensing

The MessageHandler software and all eSchKG specification documents are distributed freely under GNU public license (GPL).

1   Introducing MessageHandler v3

1.1 Before You Start

Before you start, reading the following documentation is highly recommended.

- *Anleitung für die Mitgliedschaft im eSchKG Verbund (Orange Book), Ausgabe März 2014*. How to join the eSchKG community network and obtain your Sedex certificates;

- *Sedex User Manual (Sedex Handbuch), latest version.* A guide to installing and configuring Sedex so you can send and receive Sedex messages;

- *Open eGov MessageHandler v3 Technical Documentation*. MessageHandler v3 was built for a wide variety of community networks. Some of the configuration options are relevant for the eSchKG community network while others are not.

Apart from the above documentation, there is one more thing you need to know.

> When connecting to the eSchKG network community, using your own physical Sedex endpoint (a.k.a. "adapter") is highly recommended.

Using a logical adapter means you'll have to renew your Sedex certificates manually when the time has come.

1.2 Hiding Sedex Complexity From The Application

MessageHandler v3 was designed to ease the integration of enterprise systems with the Sedex network, so applications can rely on a secure message path to peers. Instead of having to re-program your enterprise application so it can deal with the particulars of sending and receiving Sedex messages, all it needs to do is read from and write to the local file system. MessageHandler v3 takes care of the cumbersome tasks associated with sending and receiving Sedex messages without the application even noticing.

> Each time eSchKG messages are to be sent, MessageHandler v3 generates the envelope (`envl_N.xml`) and document file (`data_N.xxx`) required by the Sedex client. Enterprise applications do not have to care about this at all.

1.3 Why Use MessageHandler

Using MessageHandler v3 you take advantage of the following.

- Easy integration of Sedex with the enterprise system;
- Enhanced traffic monitoring and control;
- Allows for transparently applying digital signatures to outgoing PDF documents.

There may be other middleware available on the market, doing a similar job.

> To the members of the eSchKG community network, using MessageHandler v3 is highly recommended. It is the only middleware for which ongoing maintenance and support are granted by the Federal Office of Justice.

2   Using MessageHandler v3 with eSchKG

2.1   General Comments

When reading the Sedex User Manual [1] or the Open eGov MessageHandler v3.0 Technical Documentation [2], you may find Sedex address descriptors having prefix `T`, like in `T7-4-2`. As you may be aware, such an address can only be used with the Sedex test network. Don't worry; as a member of the eSchKG network, your Sedex adapter is a fully productive one from the start. Read the documents and examples as if the Sedex address descriptors were productive ones, like `8-AG-13`.

2.2   Mode of Operation

Members of the eSchKG community network use MessageHandler v3 in "native mode".

See also: Open eGov MessageHandler v3 Technical Documentation [2], section 2.3.

2.3   Addressing

Members of the eSchKG community network encode the addressee of a document according to the following file name convention.

`<Sedex-ID>_<original filename>`

Renaming is the responsibility of the enterprise system, not MessageHandler v3.

If you wanted to send `test.xml` to Sedex-ID `7-4-1` which is the eSchKG Testbed, the enterprise application would need to change the file name to `7-4-1_test.xml` prior to moving it to the MessageHandler's OUTBOX. Renaming is the responsibility of the enterprise system.

Once the files are in the OUTBOX, MessageHandler builds the envelope and document files required by Sedex, and forwards them to the Sedex client software. In order to do that, MessageHandler v3 must extract the addressee from the filename first. It does so using an external program or script. For usage in the eSchKG community network, the following Groovy script will do the job.

```groovy
// @param filename - the name of the file to be sent including path
// @return - the resolved Sedex-ID or an empty string
import java.util.regex.Matcher
def String resolve(String filename) {
  Matcher matcher = null;
  if (System.getProperty("os.name").startsWith("Windows") ) {
    matcher = (filename =~ /^.*\\(\S+?)_.*$/)
  } else {
    // could be Unix ...
    matcher = (filename =~ /^.*\/(\S+?)_.*$/)
  }
  if (matcher.matches()) {return matcher.group(1)
  }
  // If all else fails: return empty string
  return ''
}
```

Listing: Groovy script resolving Sedex address from compliant file names

See also: Open eGov MessageHandler v3 Technical Documentation [2], section 4.9.

2.4 Digitally Signing Outgoing Documents

> Collection offices have an obligation to digitally sign outgoing PDF files.

Collection offices can use the signing OUTBOX feature of MessageHandler v3 to do that.

2.4.1 The Signing OUTBOX

MessageHandler v3 allows for digitally signing outgoing PDF documents prior to forwarding them to the Sedex client. Documents are moved to the *Signing Outbox* for pre-processing, rather than the ordinary OUTBOX. After signing, MessageHandler v3 would move the original (unsigned) files to some pre-defined directory (called `processed`, for instance) while signed documents are moved forward to the OUTBOX for sending.
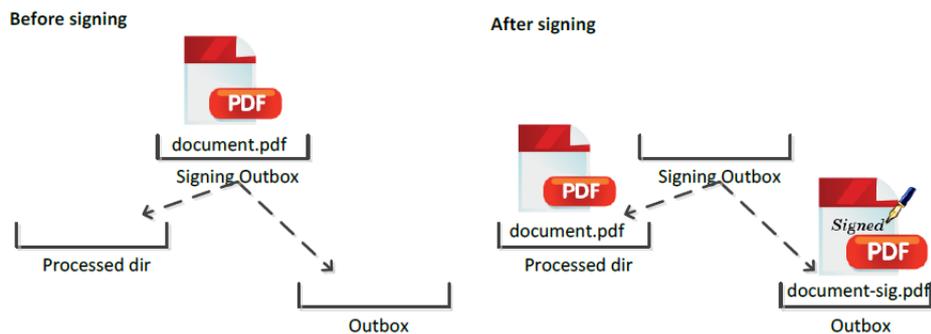

Figure: Signing Outbox Directory

> **Warning:** Do not put any other files but PDF documents to the Signing Outbox.

In particular, you must not write any XML files to it. Outgoing XML files (eSchKG messages) must always go to the normal MessageHandler's OUTBOX.

2.4.2 Signature Conventions

For usage in the eSchKG community network, the signature applied by MessageHandler v3 must adhere to a common layout convention specifying the position of the visible signature on the PDF file. The position and size of the signature are as follows:

- Always sign on page 1;
- Position: x = 110 mm from left edge, y = 270 mm from upper edge;
- Size of signature box: width = 75 mm, height = 15 mm

2.4.3 Signature Profile

In order to adhere to the signature conventions, a *signature profile* must be created telling MessageHandler v3 the position of the signature in a document. The following is a sample signature profile suitable for signing PDF documents like default summons and others by the collection offices (**bold text** indicates configuration information that must be used exactly as shown).

```
typeOfSignature = signature
visibleSignature = true
location = Bern
reason =
contact = name@your-company.ch
backgroundImage =
leftPos = 110
```

```
topPos = 270
boxWidth = 75
boxHeight = 15
signOn = 0
enableTimestamping = false
tsaurl = http://tsa.swisssign.net, http://tsa-t01.admin.ch/rfc3161
tsauser =
tsapassword =
```

Listing: Signature profile compliant with eSchKG conventions

Parameter	Remarks	Convention
typeOfSignature	The kind of signature to be produced	**MUST BE** signature
visibleSignature	Prints a signature box in the PDF	**MUST BE** true
location	The signer's domicile	
reason	A text specifying the signing action	
contact	A person's email address	
backgroundImage	A picture displaying in the signature's background	
leftPos	Position from left (x) in mm	**MUST BE** 110
topPos	Position from top (y) in mm	**MUST BE** 270
boxWidth	Width of the signature box in mm	**MUST BE** 75
boxHeight	Height of the signature box in mm	**MUST BE** 15
signOn		**MUST BE** 0
enableTimestamping	true, if you want the signature timestamped	**MUST BE** false
tsaurl	The URL of a timestamp authority	
tsauser	User name for the timestamp service	
tsapassword	The password for the timestamp service	

Listing: Parameters of the signature profile

In the download file for MessageHandler v3 you can find a sample signature profile in `<installation-dir>/conf/signing/signature.properties`

According to the sample configuration file in `<installation-dir>/conf/config.xml` MessageHandler v3 uses a file called `signature.properties` as the signature profile specification. Feel free to override the location of the signature profile.

2.4.4   Digital Certificate for Signing

When configuring the signing feature of MessageHandler v3, users can specify the certificate and other parameters freely. However, users of the eSchKG community network have no freedom when it comes to specifying the signing certificate.

> Users of the eSchKG community network MUST configure the signing feature such that it uses the certificate of the Sedex client software for signing.

In the MessageHandler v3 configuration file `config.xml`, the `<signingOutbox>` tag is used to specify the location of the Signing Outbox as well as the digital signature certificate. For the eSchKG community network, specify the location of the Sedex client certificate configuration using `<certificateConfigFile>` as shown below.

```
<nativeApp participantId="7-4-1" >     <!-- your own local sedexId -->
    <outbox dirPath="mh3outbox" msgType="10301">
        <recipientIdResolver filePath=
        "C:\SedexAdapter\mh3\conf\recipientIdResolver.groovy" method="resolve"/>
        <signingOutbox dirPath="mh3signOutbox"
        processedDir="C:\SedexAdapter\mh3\runtime\mh3signOutbox\processed"
        signingProfilePath="C:\SedexAdapter\mh3\conf\signing\signature.properties">
            <certificateConfigFile
            filePath="C:\SedexAdapter\conf\certificateConfiguration.xml"/>
        </signingOutbox>
    </outbox>
    <inbox dirPath="mh3inbox" msgTypes="10301"/>
</nativeApp>
```

Listing: Configuring the Signing Outbox in the eSchKG community network

The good news is that the certificate renewal process of Sedex has an immediate effect on the Signing Outbox. There is no need for the system administrator to change or renew neither the configuration of MessageHandler v3 nor the signature certificate.

2.4.5 Specifying the Signing OUTBOX Digital Certificate with a Logical Adapter

Transparently signing outgoing PDF documents is a novel feature of MessageHandler v3. The software allows using any digital certificate for which a PKCS #12 description exists. However, users of the eSchKG community network use the Sedex client certificate, as outlined earlier (see 2.4.4 above).

For eSchKG users running their own physical Sedex adapter, there's nothing more to say. But those running a logical Sedex adapter have got some more work to do.

To those using a logical Sedex adapter: **CHECK THIS OUT!**

When using the Signing Outbox feature of MessageHandler v3, you must use the digital certificate of your logical Sedex adapter.

As digital signatures are used to identify the signing party, using the physical Sedex adapter's certificates would not work, as they identify a different party, not you.

In a nutshell, if you run a logical Sedex adapter and intend to use the Signing Outbox feature of MessageHandler v3, you must do the following:

1. Install the digital certificate of your logical Sedex adapter in a separate location from the physical Sedex adapter certificates. (You probably did not install this one, yet);

2. When configuring the Signing Outbox, specify the logical adapter's certificate as the signature certificate (see 2.4.4 above);

Doing so ensures your organisation is the originator of a digitally signed PDF document. Yet, you will continue using the physical adapter and its certificates for Sedex messaging.

Now that you use two different digital certificates, do not forget that one of them gets renewed automatically while the other will not.

Users of a logical Sedex adapter benefit from the certificate renewal process only as far as Sedex messaging is concerned. **Logical Sedex adapter certificates used for the Signing Outbox will need to be renewed manually.**

Repeat: Users of the eSchKG community network are encouraged to use a physical Sedex adapter of their own.

2.5 Event Logging and Traffic Monitoring

MessageHandler v3 keeps a monitoring log for each outgoing message. See the Open eGov MessageHandler v3 Technical Documentation [2], section 2.7, Protocol, for details.

Inspecting log files is a cumbersome and tricky task. In order to make things easier, MessageHandler v3 comes with a monitoring interface so traffic can be controlled from the enterprise application or console. If you intend to exercise control over eSchKG traffic by the enterprise application, you'll find this new feature very useful.

> It is highly recommended that applications exercise some kind of monitoring and control over eSchKG traffic. Enterprise applications shall be capable of responding to network issues timely and reliably.

See also: Open eGov MessageHandler v3 Technical Documentation [2], section 5.

2.6 Operational Issues

2.6.1 File System Access Rights

Experience shows that in the early stages of configuration and testing, a great number of issues are simply due to insufficient access rights preventing files from being written to, or moved away from a specific directory.

> Make sure the user account running MessageHandler v3 is granted the appropriate access rights to launch services and scripts and to store and remove documents around in the file system where Sedex and MessageHandler directories reside.

2.6.2 Renewal of Sedex Client and MessageHandler Software

Sedex Client software is maintained and published by the Swiss Federal Statistical Office, while MessageHandler v3 software is maintained and published by the Federal Office of Justice. Whenever a new version of either software suite is released, those registered as a technical contact are notified so they can download and re-install the software. Note that by the time of this writing, updating the Sedex Client and MessageHandler v3 software suites are a manual task.

2.6.3 Renewal of the Sedex Client Certificate

The Sedex client is responsible for sending and receiving messages from and to the Sedex Server securely, which is why they are encrypted/decrypted using public key infrastructure technology (PKI). As mentioned above, the Sedex client is unable to renew itself as a software suite, but it does renew the Sedex client's PKI information, including the private key and the digital certificate. **Note that it can do so only with a physical adapter, not a logical one.**

Note that, when using a logical Sedex adapter, the Sedex messages you send are being encrypted and signed using the common physical adapter and its certificates. This you must understand when using the Signing Outbox feature in an eSchKG context.

2.6.4 eSchKG Member Directory

Although this is not a particular MessageHandler v3 issue, the following is worth mentioning.

> The eSchKG member directory is published on the Internet and distributed to the members using the SN message by the Federal Office of Justice.

The member directory is available in two formats, Microsoft Excel and CSV. See the eSchKG homepage on www.eschkg.ch and the specification of the *SN Sequence* in the Blue Book.

2.7   MessageHandler Configuration Examples on the Web

As a novelty, MessageHandler v3 comes with a variety of typical configuration examples in www.e-service.admin.ch/wiki/display/openegovdoc/Online+supplement.

You are highly encouraged to consult this site; the example library was developed after years of experience of solving configuration issues with MessageHandler and Sedex.

2.8   MessageHandler INBOX and OUTBOX

At the time of writing, the installation instructions in the Open eGov MessageHandler v3 Technical Documentation [2] are missing the point when the INBOX and OUTBOX directories have to be created. Don't forget to create those directories; they can be located anywhere (see example directories below).
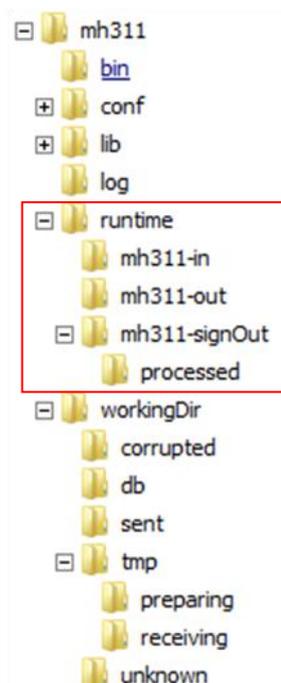

Figure: Example INBOX (mh311-in) and OUTBOX (mh311-out / mh311-signOut)

Annex: MessageHandler Configuration Overview

The following sample configuration is to demonstrate some typical configuration options for use within the eSchKG community network.

```
1  <config xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
2   xsi:schemaLocation="http://msghandler.suis.admin.ch/xmlns/config config.xsd"
3   xmlns="http://msghandler.suis.admin.ch/xmlns/config" version="3.1">
4
5  <sedexAdapter>
6     <participantId>7-4-1</participantId>
7     <inboxDir>C:\SedexAdapter\inbox</inboxDir>
8     <outboxDir>C:\SedexAdapter\outbox</outboxDir>
9     <receiptDir>C:\SedexAdapter\receipts</receiptDir>
10    <sentDir>C:\SedexAdapter\sent</sentDir>
11 </sedexAdapter>
12
13 <messageHandler>
14    <workingDir dirPath="C:\SedexAdapter\mh\workingDir"/>
15    <baseDir dirPath="C:\SedexAdapter\mh\runtime"/>
16    <sedexInboxDirCheck cron="0/30 * * * * ?" />
17    <sedexReceiptDirCheck cron="0/30 * * * * ?" />
18    <defaultOutboxCheck cron="0/30 * * * * ?" />
19    <webserviceInterface host="localhost" port="18080"/>
20    <statusDatabase dirPath="C:\SedexAdapter\mh\workingDir\db"
21    dataHoldTimeInDays="2" resend="true"/>
22 </messageHandler>
23
24 <nativeApp participantId="7-4-1"> <!-- die lokale sedexId -->
25    <outbox dirPath="mh-out" msgType="10301">
26      <recipientIdResolver
27        filePath="C:\SedexAdapter\mh\conf\recipientIdResolver.groovy"
28        method="resolve"/>
29      <signingOutbox dirPath="mh-signOut"
30        processedDir="C:\SedexAdapter\mh\runtime\mh-signOut\processed"
31        signingProfilePath="C:\SedexAdapter\mh\conf\signing\signature.properties">
32        <certificateConfigFile
33          filePath="C:\SedexAdapter\conf\certificateConfiguration.xml"/>
34      </signingOutbox>
35    </outbox>
36    <inbox dirPath="mh-in" msgTypes="10301"/>
37 </nativeApp>
38 </config>
```

Listing: Typical configuration options for the eSchKG community network

6	`participantId` is the address of your Sedex client (adapter)
19	`port` can be chosen arbitrarily
24	`participantId` is the address of your Sedex client (adapter)
25	Always use `10301` for attribute `msgType`
36	Always use `10301` for attribute `msgTypes`