Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Red Book

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

eSchKG
Networking

MessageHandler Version 3.3.1

Edition September 2017

About eSchKG

The eSchKG standard is a normative framework for the exchange of electronic business information among the parties in a debt collection. eSchKG is published by the Swiss Federal Office of Justice in a comprehensive series of documents.

- White Book: *Einführung in den eSchKG Standard, Ausgabe September 2017*. An introduction to eSchKG mainly addressing the executive. Available in German, French and Italian;

- Orange Book: *Anleitung für die Mitgliedschaft im eSchKG Verbund, Ausgabe September 2017*. A step-by-step guide to becoming a member of the eSchKG community network. Available in German, French and Italian;

- Green Book: *Prozesshandbuch und Best Practice, Ausgabe September 2017*. Explains the key concepts of eSchKG, providing recommendations and guidelines for best practice. Available in German, French and Italian;

- Red Book (this document): *eSchKG Networking, Edition September 2017*. A technical guide to connecting an enterprise information system to the eSchKG community network. Available in English;

- Blue Book: *Technical Specification, Edition September 2017*. An introduction to the architectural principles, data model and message patterns. The XML data model is specified in the appendix, *XML Reference*. The Blue Book and appendix are available in English.

About The Red Book

This document addresses programmers and integrators of eSchKG software as well as operators of sedex and MessageHandler.

References

[1]   *sedex Betriebs- / Integrationshandbuch*
Bundesamt für Statistik, 3. Juni 2016
www.sedex.ch

[2]   *Open eGov MessageHandler v3.3 Technical Documentation*
Glue Software Engineering
www.e-service.admin.ch/wiki/display/openegovdoc/MessageHandler

Changes with regard to previous versions of the Red Book

The contents of this book are the same as in the edition of August 2015. The book's title was changed to maintain consistency across the eSchKG documentation suite.

Further Information on the Web

The full documentation of the eSchKG standard is published on the web: *www.eschkg.ch*.

Table of Contents

About This Document

This document addresses integrators responsible for operating software connecting the eSchKG community network.

This document is a guide to using MessageHandler v3.3 in the eSchKG community network. It is a complementary manual to the sedex User Manual [1] and the Open eGov Message-Handler v3.3 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 among the parties in a debt collection. eSchKG is published by the Federal Office of Justice in a comprehensive series of documents.

- White Book: *Einführung in den eSchKG Standard, Ausgabe März 2017*. 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 2017*. A step-by-step guide to joining the eSchKG community network. Available in German, French and Italian;

- Green Book: *Prozesshandbuch und Best Practice, Ausgabe März 2017*. Explains the key concepts of eSchKG, and provides for recommendations and best practice guidelines. Available in German, French and Italian;

- Red Book: *eSchKG Networking, Edition March 2017*. **This document.** A technical guide to connecting an enterprise information system to the eSchKG community network. Available in English;

- Blue Book: *Technical Specification, Edition March 2017*. An introduction to the architectural principles, data model and high-level protocols. The XML data model is specified in the appendix: *XML Reference*.

  The Blue Book and appendix 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 v3.3

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 2017.* How to join the eSchKG community network and obtain your sedex certificates;

- *sedex User Manual [1], latest version.* A guide to installing and configuring sedex so you can send and receive sedex messages;

- *Open eGov MessageHandler v3.3 Technical Documentation [2].* MessageHandler v3.3 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 joining the eSchKG network community, use a separate sedex adapter dedicated exclusively to sedex message Id 10301 (which is "eSchKG Verbund").

1.2   Hiding sedex Complexity From The Application

MessageHandler v3.3 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 v3.3 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 v3.3 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 v3.3 you take advantage of the following.

- Easy integration of sedex with the enterprise system;
- Enhanced traffic monitoring and control;
- Allows for easily applying digital signatures to outgoing PDF documents (collection offices only).

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

> To the members of the eSchKG community network, using MessageHandler v3.3 is highly recommended. It is the only middleware for which ongoing maintenance and support are provided by the Federal Office of Justice.

2   Using MessageHandler v3.3 with eSchKG

2.1   General Comments

When reading the sedex User Manual [1] or the Open eGov MessageHandler v3.3 Technical Documentation [2], you may find sedex address descriptors having the prefix `T`, like in `T7-4-2`. As you may be aware, such an address can only be used within 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 v3.3 in "native mode".

See also: Open eGov MessageHandler v3.3 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.

If you wanted to send `test.xml` to, say, sedex-ID `7-4-1`, 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 of the file 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.

```
// @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 v3.3 Technical Documentation [2], section 4.9.

2.4 Digitally Signing Outgoing Documents

> Collection offices SHALL digitally sign outgoing PDF files using the built-in signing feature of MessageHandler. Creditors MUST NOT use the feature.

2.4.1 The Signing OUTBOX

MessageHandler v3.3 allows for digitally signing outgoing PDF documents prior to forwarding them to the sedex client. To do so, files are moved to the *Signing OUTBOX* instead of the regular OUTBOX. After signing, MessageHandler v3 would move the original (unsigned) files to some pre-defined directory (called `processed`, for instance) while the signed documents are forwarded to the OUTBOX for sending.
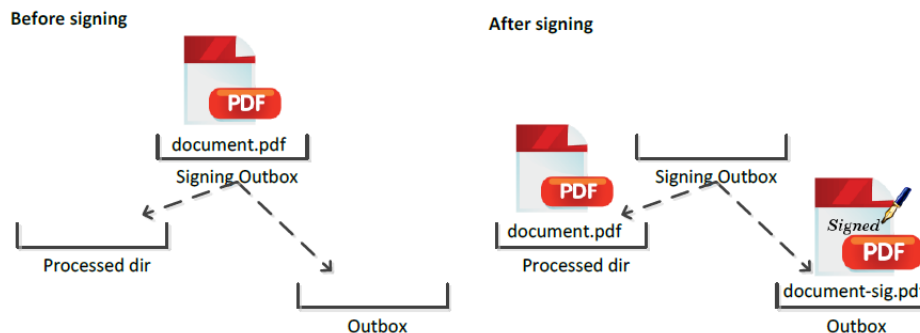

Figure: Signing Outbox Directory

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

In particular, you must not write any XML files to the Signing OUTBOX. Outgoing XML files (eSchKG messages) must always go to the ordinary OUTBOX of MessageHandler.

2.4.2 Signature Conventions

For usage in the eSchKG community network, the signature applied by MessageHandler v3.3 must adhere to a common layout convention specifying the position of the visible signature on the PDF document. 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 v3.3 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 type 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	Adds a timestamp to the signature	**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 v3.3 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 v3.3, users have to specify the digital signing certificate and other parameters. The digital signing certificate is issued to the collection offices by the Federal Office of Justice. It is especially dedicated to the digital signature of eSchKG documents.

The signing feature MUST be configured such that only the signing certificate provided by the Federal Office of Justice is used. The Sedex client certificate MUST NOT be used for the signing feature.

In the configuration file `config.xml`, the `<signingOutbox>` tag is used to specify the details of the digital signature certificate. See below for a sample specification of the `<nativeApp>` element.

```
<nativeApp participantId="7-4-1">        <!-- your sedex id -->
  <outbox dirPath="Outbox" msgType="10301">
    <recipientIdResolver filePath="C:/mh3/conf/Resolver.groovy" method="resolve"/>
    <signingOutbox dirPath="signing-outbox" signingProfilePath=
    "C:/mh3/conf/signing/signature.properties">
      <certificate filePath="C:/mh3/conf/signing/7-4-1_209A4626D7F383A4.p12"
      password="8H2xf$1?3" />        <!-- your certificate password -->
    </signingOutbox>
  </outbox>
  <inbox dirPath="inbox" msgTypes="10301"/>
</nativeApp>
```

Listing: Signing outbox configuration in config.xml

As opposed to the early years of eSchKG, the sedex client certificate is no longer involved in the digital signature process whatsoever. As a consequence, the certificate renewal process of sedex has no effect on the digital signing certificate. Generally, the sedex client certificate and the signing certificate each have their own distinct life cycles.

2.5 Event Logging and Traffic Monitoring

MessageHandler v3.3 keeps a monitoring log for each outgoing message. See the Open eGov MessageHandler v3.3 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 v3.3 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 intense monitoring and control over eSchKG traffic. Enterprise applications shall be capable of responding to network issues timely and reliably.

See also: Open eGov MessageHandler v3.3 Technical Documentation [2], section 5.

2.6 Operational Issues

2.6.1 File System Access Permissions

Experience shows that in the early stages of configuration and testing, a great number of issues have to do with insufficient access permissions preventing files from being written to or moved away from a specific location in the file system.

> Make sure the user account running MessageHandler v3.3 is granted the appropriate access rights to launch services and scripts and to store and remove documents around in the file system in which Sedex and MessageHandler directories reside.

2.6.2   Renewal of sedex Client and MessageHandler Software

The sedex client is maintained and published by the Swiss Federal Statistical Office, while MessageHandler v3.3 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 for eSchKG affairs are notified to download and re-install the software.

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 and signed using public key infrastructure technology (PKI). While the sedex client software does not renew automatically, the PKI information does, which includes the private key and digital certificate – they get updated automatically and remotely under the control of the Federal Statistical Office.

Note that, when using a logical sedex adapter, the sedex messages you send are encrypted and signed using the digital certificate of the physical adapter rather than the logical one.

2.7   MessageHandler Configuration Examples on the Web

As a novelty, MessageHandler v3.3 comes with a variety of typical configuration examples for download at 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 v3.3 Technical Documentation [2] are missing instructions on when to create the INBOX and OUTBOX directories. Don't forget to create those directories; they can be located anywhere (see example directories below).
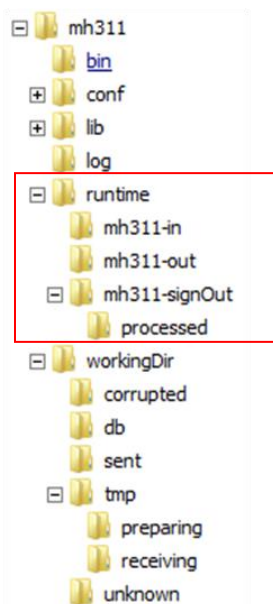

Figure: Example INBOX (mh311-in) and OUTBOX (mh311-out / mh311-signOut)

Appendix: MessageHandler Configuration Overview

The following sample configuration demonstrates 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>       <!-- your sedex id -->
7    <inboxDir>C:/sedex5/inbox</inboxDir>
8    <outboxDir>C:/sedex5/outbox</outboxDir>
9    <receiptDir>C:/sedex5/receipts</receiptDir>
10   <sentDir>C:/sedex5/sent</sentDir>
11 </sedexAdapter>
12
13 <messageHandler>
14   <workingDir dirPath="C:/mh3/workingDir"/>
15   <baseDir dirPath="C:/mh3/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:/mh3/workingDir/db"
21   dataHoldTimeInDays="2" resend="true"/>
22 </messageHandler>
23
24 <nativeApp participantId="7-4-1">  <!-- your sedex id -->
25   <outbox dirPath="mh3-out" msgType="10301">
26     <recipientIdResolver
27       filePath="C:/mh3/conf/Resolver.groovy" method="resolve" />
28     <signingOutbox dirPath="mh3-signOut"
29       signingProfilePath="C:/mh3/conf/signing/signature.properties">
30       <certificate filePath="C:/mh3/conf/signing/7-4-1_209A4626D7F383A4.p12"
31       password="8H2xf$1?3" />        <!-- your certificate password -->
32     </signingOutbox>
33   </outbox>
34   <inbox dirPath="mh3-in" msgTypes="10301"/>
35 </nativeApp>
36 </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`
30	`filePath`: location of the p12-file obtained by the Federal Office of Justice
31	`password`: private key password obtained by the Federal Office of Justice
34	Always use `10301` for attribute `msgTypes`