

# Datenaustausch über Internet-eMail

(SRM – Secure Report Mailing)

# Inhaltsverzeichnis:

Technische Voraussetzungen zur Teilnahme	2
Ablauf der Anmeldung bzw. Aktualisierung	2
Unterstützte eMailboxen der OeNB für Datenempfang (Produktiv- und Testmodus)	2
Schlüssel und Schlüsseländerungen	2
Ablauf einer Datenübermittlung an die OeNB	2
Ablauf einer Datenübermittlung von der OeNB	3
Konventionen	3
Erklärung der verwendeten Begriffe	5
Quittungen	6

## Technische Voraussetzungen zur Teilnahme

Möglichkeit Internet-eMail Nachrichten mit einer angefügten „verschlüsselten“ Datei senden und empfangen zu können.

Verfügbarkeit des Verschlüsselungsprogramms PGP (Pretty Good Privacy) oder eines kompatiblen Produkts (z.B. das Open Source Produkt GnuPG, [www.gnupg.org](http://www.gnupg.org)) zur Ver- bzw. Entschlüsselung und Signierung der Meldungen.

## Ablauf der Anmeldung bzw. Aktualisierung

- Den Antrag für „Technischer Partner SRM“ finden Sie unter <Link>.
- Übermittlung des ausgefüllten und firmenmäßig gefertigten Teilnahmeantrags an die OeNB. (Per Post oder per eMail an [IT.Meldeverarbeitung@oenb.at](mailto:IT.Meldeverarbeitung@oenb.at))
- Übermittlung einer eMail mit dem public key des „Technischen Partners“ von der im Antrag angegebenen eMailadresse an [IT.Meldeverarbeitung@oenb.at](mailto:IT.Meldeverarbeitung@oenb.at).
- Nach erfolgreicher Registrierung der Daten erhalten Sie ein Bestätigungsmail mit dem public key der OeNB an die im Antrag angegebene eMailadresse für die Übertragung.
- Danach können verschlüsselte und signierte Daten in beide Richtungen übertragen werden.

## Unterstützte eMailboxen der OeNB für Datenempfang (Produktiv- und Testmodus)

- [srm@oenb.at](mailto:srm@oenb.at) (Für produktive Datenübermittlung) Die erste Stelle der 3 bzw. 8-stelligen Meldungsart ist bei zu verarbeitenden Echtdateien immer „D“. Ausnahme: RISK-Meldungen dürfen „T“ und „D“ verwenden.
- [srmtest.schnittstelle@oenb.at](mailto:srmtest.schnittstelle@oenb.at) (Für testweise Datenübermittlung) Die erste Stelle der 3 bzw. 8-stelligen Meldungsart ist bei zu verarbeitenden Testdateien immer „T“.

## Schlüssel und Schlüsseländerungen

Jeder Teilnehmer ist für die sichere Verwahrung des geheimen Teils seines Schlüssels verantwortlich. Wenn sich die Notwendigkeit einer Schlüsseländerung ergibt, ist diese analog zur Anmeldung abzuwickeln. Schlüsseländerungen der OeNB werden nach Ankündigung durchgeführt.

- Schlüsselnamen dürfen keine Umlaute und Strichpunkte enthalten.
- Schlüssel vom Typ DH/DSS und RSA werden akzeptiert. Als Verschlüsselungsalgorithmus sollte AES verwendet werden. Andere Algorithmen bedürfen der Zustimmung der OeNB.
- Die Mindestschlüssellänge sollte mindestens 2048 bit betragen.

## Ablauf einer Datenübermittlung an die OeNB

Verschlüsselung und Signierung der zu versendenden Meldungsdatei. Die Verschlüsselung muss mit dem public key der OeNB erfolgen. Für die Signierung ist der private key, der zum an die OeNB übermittelten public key gehört, zu verwenden.

Versenden der Datei als Anlage an eine der unterstützten eMailadressen. Der Aufbau der eMail muss den u.a. Konventionen entsprechen.

Nach dem Einlangen der Mail in der OeNB und einer anschließenden Formalprüfung wird automatisch eine Quittungsmail an den Sender zurückgeschickt. Diese enthält entweder die Bestätigung der ordnungsgemäßen Entschlüsselung der Meldung oder bei einem Formalfehler einen entsprechenden Fehlertext (siehe ‚Negative Quittungen‘).

Seitens der OeNB werden nur signierte und verschlüsselte Dateien akzeptiert. Meldungen gelten nur dann als der OeNB zugestellt, wenn sie in einem gültigen Format von der OeNB empfangen und entschlüsselt werden konnten und dies dem Absender durch die positive Quittung bestätigt wurde.

Mails werden im Normalfall zwischen 0:00 und 24:00 Uhr entgegengenommen. Die Verarbeitung der Meldungen erfolgt zeitlich nach den in der OeNB gegebenen Erfordernissen. Bei technischen Problemen steht zwischen 7:00 und 19:00 Uhr unter der Telefonnummer 01 40420 2777 werktags ein Helpdesk zur Verfügung.

### **Ablauf einer Datenübermittlung von der OeNB**

Die OeNB versendet die mit dem public key des Empfängers verschlüsselten und mit dem privat key der OeNB signierten Daten nach Variante 2 (siehe Konventionen) an die Teilnehmeradresse. Eine Verarbeitung von Empfangsquittungen ist in der OeNB nicht vorgesehen. Falls Daten nicht zum erwarteten Zeitpunkt beim Teilnehmer einlangen, muss eine neuerliche Übertragung angefordert werden (eMail: [IT.Meldeverarbeitung@oenb.at](mailto:IT.Meldeverarbeitung@oenb.at), Telefon 01 40420 2777).

### **Konventionen**

Aus Gründen der Vereinheitlichung und Automatisierung der Meldungsverarbeitung ist die Einhaltung von Konventionen unumgänglich. Die im Folgenden definierten Formatbeschreibungen müssen daher unbedingt eingehalten werden.

- Grundsätzlich wird Groß- und Kleinschreibung nicht unterschieden.
- Die Teilnehmeradresse darf nicht srm@... lauten.
- Um diverse Automatisierungswünsche zu erfüllen sind drei Varianten zur Gestaltung der Mail möglich:

#### **Variante 1**

(kurzer Betreff, langer Attachmentname)

##### **Betreff:**

SRM-<Meldungsgruppe>

##### **Attachmentname 1 ... n**

<Meldungsgruppe><Institutskennzahl>-<Meldeperiode/Meldungsnummer>.  
<Meldungsart>.pgp

##### **Gültige Beispiele:**

Betreff: SRM-M

Attachmentname: M12345-20100300.D23.pgp

Betreff: SRM-Z

Attachmentname: Z12345678-20100300.DZA0KXML.pgp

Betreff: SRM-Z

Attachmentname: Z12345678-00000001.DZL0DZIP.pgp

Betreff: SRM-A

Attachmentname: A12345-20100300.DLQ0DXLS.pgp

## Variante 2

(MeldungsInfo im Betreff, 8+3-stelliger Attachmentname, nur ein Attachment)

### Betreff:

SRM\*<Meldungsgruppe><Institutskennzahl>-<Meldeperiode/  
Meldungsnummer>.<Meldungsart>\*<Dateiname-kurz>

### Attachmentname

<Dateiname-kurz>

### Gültige Beispiele:

Betreff: SRM\*M12345-20100300.D23\*abcdefgh.xxx

Attachmentname: abcdefgh.xxx

Betreff: srm\*Z12345678-20100300.DZA0KXML\*abcd.xxx

Attachmentname: abcd.xxx

Betreff: srm\*Z12345678-00000001.DZL0DZIP\*abcd.xxx

Attachmentname: abcd.xxx

Betreff: srm\*A12345-20100300.DLQ0DXLS\*abcd.xxx

Attachmentname: abcd.xxx

## Variante 3

(Meldungs- und Automatisierungsinfo im Betreff, 8+3-stelliger Attachmentname, nur ein Attachment)

### Betreff:

<Pre>\*SRMA\*<SRM-Release>\*<ID>\*<Meldungsgruppe>  
<Institutskennzahl>-<Meldeperiode/Meldungsnummer>.<Meldungsart>\*<Dateiname-kurz>\*<Post>

### Attachmentname

<Dateiname-kurz>

### Gültige Beispiele:

Betreff:

\*SRMA\*02\*877tbxmd\*M12345-20050300.D23\*877tbxmd.pgp\*xyz

Attachmentname: 877tbxmd.pgp

Betreff:

\*srma\*02\*877tbxmd\*Z12345678-20050300.DZA0KXML\*877tbxmd.pgp\*xyz

Attachmentname: 877tbxmd.pgp

Betreff:

\*srma\*02\*877tbxmd\*Z12345678-00000001.DZL0DZIP\*877tbxmd.pgp\*xyz

Attachmentname: 877tbxmd.pgp

Betreff:

\*srma\*02\*877tbxmd\*A12345-20100300.DLQ0DXLS\*877tbxmd.pgp\*xyz

Attachmentname: 877tbxmd.pgp

## Erklärung der verwendeten Begriffe

### SRM-

Zeichenfolge SRM-

### SRM\*

Zeichenfolge SRM\*

### <Meldungsgruppe>

Ein Buchstabe, der die Meldungsgruppe identifiziert (siehe Tabelle).

### <Institutskennzahl>

8-stellige OeNB-Identnummer, 7-stellige Kennziffer des meldenden Instituts (z.B.: 12345KI) oder 5-stellige Bankleitzahl.

### <Meldeperiode/Meldungsnummer>

Dieses 8-stellige Feld enthält das der Meldung zugeordnete Datum (nicht das Datum der Übertragung) oder eine Meldungsnummer.

Eine Meldeperiode ist in der Form „JJJJMMTT“ einzugeben und dient in erster Linie zur Information bzw. als Identifikationsmerkmal bei allfälligen Rückfragen. Ist eine Meldung keinem Tag oder Monat zuordenbar, ist in den entsprechenden Feldern 00 einzutragen (z.B.: Jahresabschluß 2004 = 20040000).

Wird eine laufende Nummer angegeben, so ist diese mit führenden Nullen einzugeben (z.B.: „00000001“).

### <Meldungsart>

Die Meldungsart kann 3 oder 8-stellig sein.

- Aufbau 3-stellig: *abb*
  - a*: „D“ ... für Meldungsdaten
  - „T“... für Testdaten
  - „Q“ ... für Quittung
  - bb*: Dateityp aus „Tabelle der definierten Meldungen“
- Aufbau 8-stellig: *abb0cddd*
  - a*: „D“ ... für Meldungsdaten
  - „T“... für Testdaten
  - „Q“ ... für Quittung
  - bb*: Dateityp aus „Tabelle der definierten Meldungen“
  - 0*: Zeichen „0“ (Platzhalter für Erweiterung)
  - c*: „K“ ... für Kopfdatei
  - „D“ ... für Datendatei
  - „A“ ... für Acknowledgement Message
  - ddd*: „XML“ ... für XML-Datei
  - „ZIP“ ... für ZIP-Datei
  - „PDF“ ... für PDF-Datei
  - „XLS“ ... für XLS-Datei

### .pgp

Zeichenfolge .pgp

#### <Dateiname-kurz>

Maximal 8 + 3-stelliger Dateiname. Der Dateiname und die Extension sind frei vergebbar. Wichtig ist nur die exakte Übereinstimmung zwischen dem Namen im Betreff und dem Namen des Attachments.

#### <SRM-Release>

Versionskennzeichen (wird von der OeNB nicht ausgewertet).

#### <ID>

8-stellige Ziffern und Buchstabenkombination (keine Sonderzeichen, wird von der OeNB nicht ausgewertet).

#### <Pre>

Beliebige Zeichenfolge aus Buchstaben und Ziffern (keine Sonderzeichen, wird von der OeNB nicht ausgewertet).

#### <Post>

Beliebige Zeichenfolge aus Buchstaben und Ziffern (keine Sonderzeichen, wird von der OeNB nicht ausgewertet).

#### <Code>

4-stelliger Code aus Buchstaben und Ziffern (keine Sonderzeichen).

#### <Text>

Beliebige Zeichenfolge aus Buchstaben und Ziffern (keine Sonderzeichen), die eine Information über den Empfang der Meldung oder einen aufgetretenen Fehler gibt.

#### <Timestamp>

JJJJ/MM/TT hh:mm

Die Zeichen "-", ".", "\*" im Betreff bzw. dem Dateinamen sind zur automatisierten Weiterverarbeitung der Meldung unbedingt erforderlich. Andere Sonderzeichen und Umlaute sind nicht erlaubt.

### Quittungen

Wenn eine Nachricht dem SRM-Service zugeordnet werden kann, wird für jede Meldung automatisch eine Quittung erstellt und an den Sender normalerweise innerhalb weniger Minuten zurückgeschickt. Quittungen haben folgendes Format:

#### **Aufbau des Betreff:**

Antw: <Ursprünglicher Betreff des Senders> (in der Meldungsart wird das erste Zeichen durch Q ersetzt)

#### **Aufbau der Mitteilung:**

OeNB/SRM

<Code>: <Text>

Ihre Meldung: <Betreff der an die OeNB gesandten Mail>

In OeNB eingelangt: <Timestamp>

<Post>

#### Details:

- Inhalt <Code> (4-stellig):

<a><b><c><n>: <Meldungstext>

<a> A ... Aktion

E ... Fehler

I ... Information

<b> S ... SRM

<c> 1 ... Mailformat Variante 1

2 ... Mailformat Variante 2

3 ... Mailformat Variante 3

A ... Attachment

D ... Entschlüsseln

M ... Mail

<n> lfd. Nummer

- Inhalt <Text>:

*Positive Quittungen*

AS10 Attachment <Attachmentname> empfangen und entschlüsselt

AS20 Attachment <Attachmentname> empfangen und entschlüsselt

AS30 Attachment <Attachmentname> empfangen und entschlüsselt

*Negative Quittungen (Fehlermeldungen)*

ESA1 Kein Attachment gefunden

ESA2 Mehr als ein Attachment nicht erlaubt

ESA3 Attachment fehlerhaft oder nicht vorhanden

ESD1 <file>id Fehler beim Entschlüsseln <error>

ESD2 Fehler beim Entschlüsseln: Attachment ist nicht korrekt signiert

ES11 Fehlerh. Betr: Meldungsgruppe konnte nicht erkannt werden

ES12 Fehlerh. Att: Meldungsgruppe konnte nicht erkannt werden

ES13 Fehler: Meldungsgruppe im Betreff und im Attachment sind nicht gleich

ES14 Fehlerh. Att: Bindestrich konnte nicht an einer gültigen Position erkannt werden

ES15 Fehler: Institutskenzahl <InstKZ> für die Meldeadresse nicht zulässig

ES16 Fehlerh. Att: Punkt konnte nicht an einer gültigen Stelle erkannt werden

ES17 Fehlerh. Att: Meldungsart konnte nicht erkannt werden

ES1B Fehlerh. Att: Meldungsart passt nicht zur Meldungsgruppe

ES1C Fehlerh. Att: Meldungsart ist für Meldungen an die OeNB nicht vorgesehen

ES18 Fehlerh. Att: Extension PGP konnte nicht an einer gültigen Stelle erkannt werden

ES19 Fehlerh. Att: Ungültige Länge des Dateinamens

ES1A Fehlerh. Att: Meldeperiode nicht numerisch / Meldeperiode hat mehr oder weniger als 8 Zeichen

ES1G Fehlerh. Att: Meldungsart hat nicht 3 oder 8 Stellen

ES1H Fehlerh. Att: Vierte Stelle der Meldungsart ist nicht '0'

ES1I Fehlerh. Att: Fünfte Stelle der Meldungsart ist nicht 'K','D' oder 'A'

ES1J Fehlerh. Att: Filetyp in Meldungsart ist nicht 'XML' oder 'ZIP'

ES1K Fehlerh. Att: Meldungsart hat nicht 8 Stellen

ES21 Fehlerh. Betr: Meldungsgruppe konnte nicht erkannt werden

ES22 Fehlerh. Betr: Dateiname konnte nicht erkannt werden

ES2D Fehlerh. Betr: Dateiname hat mehr als 8 Zeichen

- ES2E Fehlerh. Betr: Extension des Dateinamens konnte nicht erkannt werden
- ES2F Fehlerh. Betr: Extension des Dateinamens hat mehr als 3 Zeichen
- ES23 Fehler: Dateiname im Betreff und im Attachment sind nicht gleich
- ES24 Fehlerh. Betr: Bindestrich konnte nicht an einer gültigen Position erkannt werden
- ES25 Fehler: Institutskenzahl <InstKZ> für die Meldeadresse nicht zulässig
- ES26 Fehlerh. Betr: Punkt konnte nicht an einer gültigen Stelle erkannt werden
- ES27 Fehlerh. Betr: Meldungsart konnte nicht erkannt werden
- ES2B Fehlerh. Betr: Meldungsart passt nicht zur Meldungsgruppe
- ES2C Fehlerh. Att: Meldungsart ist für Meldungen an die OeNB nicht vorgesehen
- ES28 Fehlerh. Betr: Stern konnte nicht an einer gültigen Stelle erkannt werden
- ES2A Fehlerh. Att: Meldeperiode nicht numerisch / Meldeperiode hat mehr oder weniger als 8 Zeichen
- ES2G Fehlerh. Att: Meldungsart hat nicht 3 oder 8 Stellen
- ES2H Fehlerh. Att: Vierte Stelle der Meldungsart ist nicht '0'
- ES2I Fehlerh. Att: Fünfte Stelle der Meldungsart ist nicht 'K','D' oder 'A'
- ES2J Fehlerh. Att: Filetyp in Meldungsart ist nicht 'XML' oder 'ZIP'
- ES2K Fehlerh. Att: Meldungsart hat nicht 8 Stellen
- ES31 Fehlerh. Betr: Meldungsgruppe konnte nicht erkannt werden
- ES32 Fehlerh. Betr: Dateiname konnte nicht erkannt werden
- ES3D Fehlerh. Betr: Dateiname hat mehr als 8 Zeichen
- ES3E Fehlerh. Betr: Extension des Dateinamens konnte nicht erkannt werden
- ES3F Fehlerh. Betr: Extension des Dateinamens hat mehr als 3 Zeichen
- ES33 Fehler: Dateiname im Betreff und im Attachment sind nicht gleich
- ES34 Fehlerh. Betr: Bindestrich konnte nicht an einer gültigen Position erkannt werden
- ES35 Fehler: Institutskenzahl <InstKZ> für die Meldeadresse nicht zulässig
- ES36 Fehlerh. Betr: Punkt konnte nicht an einer gültigen Stelle erkannt werden
- ES37 Fehlerh. Betr: Meldungsart konnte nicht erkannt werden
- ES3B Fehlerh. Betr: Meldungsart passt nicht zur Meldungsgruppe
- ES3C Fehlerh. Att: Meldungsart ist für Meldungen an die OeNB nicht vorgesehen
- ES38 Fehlerh. Betr: Stern konnte nicht an einer gültigen Stelle erkannt werden
- ES3A Fehlerh. Att: Meldeperiode nicht numerisch / Meldeperiode hat mehr oder weniger als 8 Zeichen
- ES3G Fehlerh. Att: Meldungsart hat nicht 3 oder 8 Stellen
- ES3H Fehlerh. Att: Vierte Stelle der Meldungsart ist nicht '0'
- ES3I Fehlerh. Att: Fünfte Stelle der Meldungsart ist nicht 'K','D' oder 'A'
- ES3J Fehlerh. Att: Filetyp in Meldungsart ist nicht 'XML' oder 'ZIP'
- ES3K Fehlerh. Att: Meldungsart hat nicht 8 Stellen
- ESA1 Kein Attachment gefunden
- ESA2 Mehr als ein Attachment nicht erlaubt
- ESD1 Fehler beim Entschlüsseln: <PGP Fehlermeldung>
- ESD2 Fehler beim Entschlüsseln: Attachment ist nicht korrekt signiert
- ESD3 Signatur <Signatur> passt nicht zur Institutskenzahl

*Quittung zur Information*

ISM4 Nicht automatisiert verarbeitbare SRM-Nachricht

- Inhalt <Timestamp>:  
Tag und Uhrzeit im Format: JJJJ/MM/TT hh:mm
- Inhalt <Post>:  
Allgemeine Informationen zum SRM-Service in Textform mit einer variablen Anzahl von Zeilen.