

simply secure

**IncaMail**

**Mailgateway-Integration (MGI)**

Checklist for launch

# Contents

|   |                                    |   |
|---|------------------------------------|---|
| 1 | Introduction.....                  | 3 |
| 2 | Component overview.....            | 3 |
| 3 | Procedure.....                     | 5 |
| 4 | E-mail policy .....                | 6 |
| 5 | Organisation / communication ..... | 6 |
| 6 | Technical checklist .....          | 7 |
| 7 | Next steps.....                    | 8 |
| 8 | Technical explanation.....         | 8 |

# 1 Introduction

With the IncaMail mail gateway integration (MGI or domain integration), your e-mail infrastructure is expanded with the addition of the ability to send and receive secure e-mail messages via the IncaMail service of Swiss Post. For the individual user, delivery via add-ins of the mail client is available. The integration can be carried out for one or more domains.

This document helps you launch IncaMail efficiently and get the best possible use out of it. Launching secure e-mail solutions requires technical and organisational measures. The area of organisational measures comprises e-mail policy, end user and partner communication and the review of the support processes. The technical measures include architecture decisions and the actual connection work.

## 2 Component overview

For the integration, the following components of the mail infrastructure of an organisation are relevant:

| Component                   | Meaning  | Operational requirement   | Technical requirement  |
|-----------------------------|--|---------------------------|--|
| Mail client, e.g. Outlook®  | Is used by the end user for receiving and sending secure IncaMail messages (desktop and/or mobile device).   | Instructions of the users | IncaMail add-in with which the user can send secure IncaMail messages  |
| Browser                     | Is used by the end user for opening encrypted IncaMail SAFE messages (dispatch type "personal" or "registered"). After registration can also be used for access to personal logbook (log). |                           | Current version of one of the various popular browsers   |
| Mail server, e.g. Exchange® | Receives and sends IncaMail messages either directly from and to the IncaMail service or an e-mail gateway   |                           | For IncaMail communication: <ul style="list-style-type: none"><li>- Valid X.509 certificate of a recognised Certification Authority (CA)</li><li>- Support of STARTTLS in SMTP communication via port 25</li><li>- Support of mutual authentication or two-way authentication for TLS encryption (inbound and outbound)</li><li>- Use of MX Lookup</li><li>- Special rules for IncaMail can be compiled as an option, but preferably not for fixed IPs</li></ul> |

| Component              | Meaning  | Operational requirement  | Technical requirement   |
|------------------------|--|--|---|
| Optional: mail gateway | Is switched between mail server and IncaMail service                   | <p>Since the transport encryption does not take place until after the gateway, a sufficiently secure transport encryption has to be ensured between the gateway and the mail server.</p> <p>Hosted gateways are not advisable because then confidential data are decrypted at external companies. Instead the e-mail communication can be directly from the mail server.</p> | <p>For IncaMail communication:</p> <ul style="list-style-type: none"> <li>- Valid X.509 certificate of a recognised Certification Authority (CA)</li> <li>- Support of STARTTLS in SMTP communication via port 25</li> <li>- Support of mutual authentication or two-way authentication for TLS encryption (inbound and outbound)</li> <li>- SwissSign root certificate of the IncaMail server certificate contained in the trust store</li> <li>- Messages with HTML attachments must not be filtered</li> <li>- IncaMail server must not be blocked (→ possible entry in white list)</li> </ul> |
| Firewall               | Enables communication between mail server/gateway and IncaMail service | Decision made in each case for receipt and delivery separately: does the mail server or gateway communicate with the IncaMail service?   | Rules which enable the communication (inbound and outbound) of the mail server with the IncaMail server via port 25 (and possibly exclude other services).  |

### 3 Procedure

Based on our experience, we suggest the following procedure for you:

| Phase  | Target   | Delivered objects   | Lead            |
|--|--|---|-----------------|
|  <p>Planning</p>    | All necessary decisions are taken and the corresponding measures are planned     | <ul style="list-style-type: none"> <li>• Implementation plan</li> <li>• Setup documentation filled in and returned to Swiss Post</li> <li>• Setup deadline</li> </ul>   | Customer        |
|  <p>Preparation</p> | All necessary work has been done so that the setup can be performed efficiently. | <p>Technical measures</p> <ul style="list-style-type: none"> <li>• SSL certificate on MTA (MailTransferAgent: mail server or gateway) is ready for receipt and delivery (mutual authentication).</li> </ul> <p><b>Note:</b> the certificate used must be issued by a recognized certification authority registered with IncaMail. Caution: some foreign CAs might not be recognized; this also applies to expired or self-signed certificates. <b>If in doubt, ask.</b></p> <ul style="list-style-type: none"> <li>• Communication matrix is implemented</li> <li>• Mail client add-in distribution is integrated in software distribution</li> </ul> <p>Organisational measures</p> <ul style="list-style-type: none"> <li>• E-mail policy is checked and corresponds with the new requirements</li> </ul> <p>Communication plan</p> <ul style="list-style-type: none"> <li>• End user communication</li> <li>• Partner communication</li> </ul> | Customer        |
|  <p>Setup</p>     | Customer is connected to IncaMail  | <ul style="list-style-type: none"> <li>• Executable connection to</li> </ul>  | POST / Customer |

|         |  |  |      |
|---------|--|--|------|
| Testing | Swiss Post and the customer can be certain that the connection is running perfectly. | <ul style="list-style-type: none"> <li>• Delivery and receipt works for internal and external communication addresses</li> <li>• Acceptance protocols</li> <li>• Definitive setup documentation</li> </ul> | POST |
|---------|--|--|------|

## 4 E-mail policy

The following checklist helps you make the right considerations with regard to the questions of who / what / how must / will / may send/be sent via IncaMail.

| Question  | Clear | Unclear | To do |
|---|-------|---------|-------|
| <b>4.1</b> Who (level, department, function) uses IncaMail?   |       |         |       |
| <b>4.2</b> Which e-mails (content, business process, recipients) must be sent via IncaMail?                           |       |         |       |
| <b>4.3</b> How must secure e-mails (sent via IncaMail) be written, structured, titled (as usual, special regulation)? |       |         |       |
| <b>4.4</b> How must secure e-mails (sent or received via IncaMail) be archived?                                       |       |         |       |

## 5 Organisation / communication

The following checklist helps you ideally prepare in organisational terms.

| Question   | Clear | Unclear | To do / comments   |
|--|-------|---------|--|
| <b>5.1</b> Do I want to use the standard IncaMail instruction manual or do I want to create my own?                                  |       |         | Standard:<br><a href="http://www.swisspost.ch/incamail-downloads">www.swisspost.ch/incamail-downloads</a>  |
| <b>5.2</b> Whom do IncaMail users within the company contact if they have questions about how to use IncaMail (1st level support)?   |       |         | <ul style="list-style-type: none"> <li>• Own support organisation</li> <li>• By e-mail /telephone?</li> <li>• Operating hours?</li> </ul>  |
| <b>5.3</b> Whom does IT contact for complex questions (2 <sup>nd</sup> level support)?   |       |         | Post Help Desk<br>IncaMail business customer support<br>Monday to Friday<br>8.00 am – 6.00 pm<br><a href="mailto:business@incamail.ch">business@incamail.ch</a><br>+41 (0) 848 00 04 15 (except general holidays in Switzerland) |
| <b>5.4</b> Have you informed your employees about the introduction and use of IncaMail and also regulations according to 5.1 to 5.3? |       |         | Write to employees   |
| <b>5.5</b> Have you informed your recipients that they will receive confidential e-mails via IncaMail in the future?                 |       |         | Swiss Post recommends informing future recipients of IncaMail messages in advance and has prepared instructions  |

|  |  |  |  |
|--|--|--|--|
|  |  |  | for recipients here. This can be downloaded below<br><a href="https://www.swisspost.ch/incamail-recipient-info-short">https://www.swisspost.ch/incamail-recipient-info-short</a> . |
|--|--|--|--|

## 6 Technical checklist

The following checklist draws your attention to technical requirements. See chapter 8 “Technical explanation” for comparison.

| Question  | Clear | Unclear | To do / comments   |
|---|-------|---------|--|
| <p><b>6.1</b> With which infrastructure components (MTA: mail server, mail gateway) will the connection be made? Receipt and delivery can be done in different ways here.</p> <ul style="list-style-type: none"> <li>• Does this have TLS capability using STARTTLS via port 25 with two-sided authentication using X.509 certificates?</li> <li>• Is a valid certificate for receipt and delivery installed?</li> <li>• Is it necessary to set routing rules and, if so, is this possible?</li> <li>• Is the IncaMail root certificate (“SwissSign Server Gold CA 2014 - G22”) contained in the trust store of the mail gateway (with current Windows, Linux and OSX versions this is the case anyway)?</li> </ul> |       |         |  |
| <b>6.2</b> Is this MTA already set up for the use of TLS ? (certificate /configuration)   |       |         |  |
| <b>6.3</b> Which routing procedure will be carried out (domain-based, content-based)?   |       |         |  |
| <p><b>6.4</b> Does the network communication matrix have to be adapted?</p> <ul style="list-style-type: none"> <li>• SMTP from MTA →im.post.ch</li> </ul>   |       |         | See Technical explanation, chapter 8.  |
| <b>6.5</b> If you use Outlook, Lotus Notes or GroupWise, how will you make the corresponding IncaMail addin available to users?   |       |         | Download add-in:<br><a href="http://www.swisspost.ch/incamail-downloads">www.swisspost.ch/incamail-downloads</a> |
| <b>6.6</b> How and to whom will the add-in be distributed?  |       |         |  |

|  |  |  |  |
|--|--|--|--|
| <p><b>6.7</b> Does the monitoring have to be adapted?</p> <ul style="list-style-type: none"> <li>Monitoring of logs for delivery errors regarding IncaMail e-mails</li> <li>Monitoring of mail queues</li> </ul> |  |  |  |
| <p><b>6.8</b> Is the IncaMail infrastructure included in your white list?</p>  |  |  | <p>If the IncaMail infrastructure has not been included in the white list, there may be delays and/or rejections when receiving IncaMail messages.</p> |

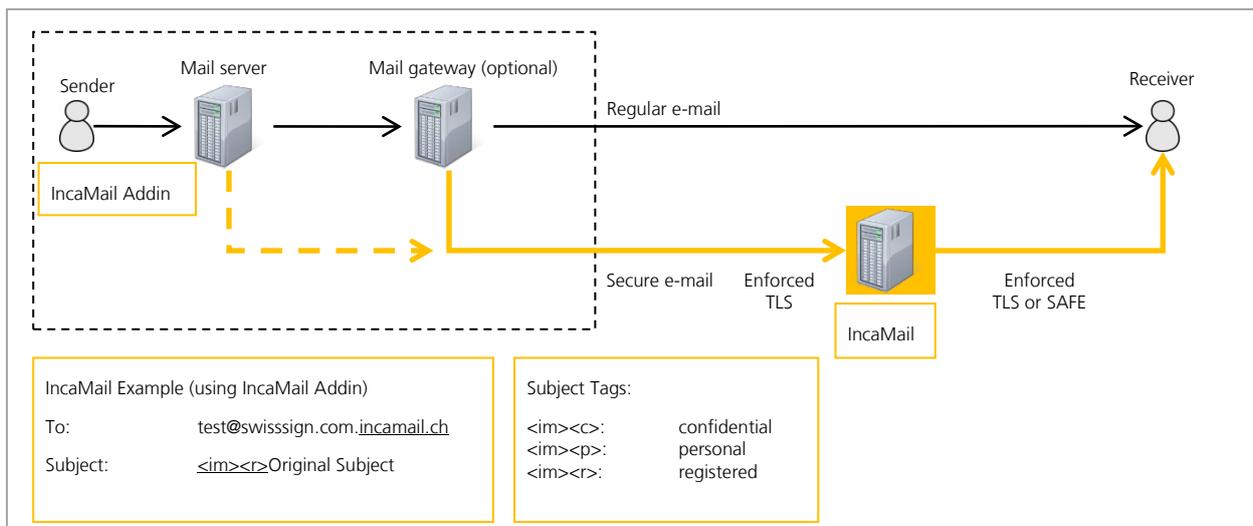
## 7 Next steps

The following checklist shows what are the next steps in relation to Swiss Post.

| Next steps                                      | Clear | Unclear | To do   |
|---|-------|---------|---|
| <p><b>7.1</b> Fill in "setup documentation"</p> |       |         |   |
| <p><b>7.2</b> Return "setup documentation"</p>  |       |         | <p>The "setup documentation" has to be enclosed as an attachment in the reply to the welcome mail.</p>                        |
| <p><b>7.3</b> Agree activation date</p>         |       |         | <p>The desired date in the "setup documentation" is confirmed by the Post Help Desk or a new date is looked for together.</p> |

## 8 Technical explanation

In the following video you will find the animation which introduces you to the functionality and integration of IncaMail. →[Video](#)



## 8.1 Outbound e-mail flow

In the following a possible outbound mail flow is described:

- (1) End user wants to send an IncaMail e-mail
- (2) With the help of the addin the e-mail is prepared accordingly (if it is a confidential e-mail, subject will have "<im><c>" added and the recipient address will be extended with the domain suffix ".incamail.ch")
- (3) The internal mail server receives this IncaMail e-mail and passes it onto the mail gateway
- (4) The mail gateway has the task of forwarding e-mails to the right mail servers (routing), with IncaMail e-mails this is with use of the TLS/SSL (STARTTLS) protocol to the IncaMail platform.
  - a. The correct IncaMail mail server is determined as standard via DNS query (MX Lookup).
  - b. Alternatively this can be carried out via routing rules. There are the following variants here:
    - i. Routing rule: \*.incamail.ch --> im.post.ch (if static: 194.41.147.13 / 194.41.147.14)
    - ii. Alternative routing rule: Subject contains "<im>" --> im.post.ch (if static: 194.41.147.13 / 194.41.147.14)

IMPORTANT: It is not advised to use static IPs because these can change in general!

- (5) The IncaMail platform receives the IncaMail e-mail if the sending mail gateway has been correctly authenticated with its SSL Certificate. For this it must be capable of mutual authentication, with which the client and server have to show their certificates.
- (6) The IncaMail platform forwards the IncaMail e-mail to the recipient according to the selected connection type.

## 8.2 Inbound e-mail flow

In the following a possible inbound e-mail flow is described:

- (1) IncaMail platform sends e-mail via TLS/SSL to the mail gateway. The IP address of the mail gateway is either determined via MX Lookup in the DNS or is stored as a static IP or static host name. You determine this method with the information in the setup document.
- (2) Mail gateway receives e-mail
- (3) Mail gateway checks this for malware (exception: registered e-mails which have a SAFE attachment)
- (4) Mail gateway forwards the IncaMail e-mail to the internal mail server
- (5) Mail client retrieves the IncaMail e-mail from the mail server
- (6) End user opens the IncaMail e-mail
- (7) For registered:
  - a. End user opens the attachment
  - b. End user clicks on "Open", here the encrypted mail is sent in SAFE format to the IncaMail platform to be decrypted via HTTPS

## 8.3 Simple connection tests

The outbound e-mail flow can be tested without a Add-in as follows:

Recipient: [Use any external e-mail address to which you attach the ending ".incamail.ch", e.g. joe.public.2543@gmail.com.](mailto:joe.public.2543@gmail.com)

Subject: <im><c> Test mail outbound to IncaMail

Body text: This is a test to see if the routing rule works...

## 8.4 Check if your computer recognises the correct IncaMail platform certificate and read certificate details

IDS, IPS and other systems can interpose between your computer and the IncaMail platform. In this case, the certificate which is visible in the communication with the IncaMail server is not assigned to IncaMail IncaMail and the Swiss Post.

Use OpenSSL to verify this (install if necessary). It can download and inspect the server's certificate to verify this.

Download certificate:

Until Nov. 2015:

```
openssl s_client -connect mx1.post.ch:25 -starttls smtp >mycert.pem
```

From Dez. 2015:

```
openssl s_client -connect gw1.incaemail.com:25 -starttls smtp >mycert.pem
```

The certificate is downloaded to the file "mycert.pem". It can be analyzed with an online-decoder, e.g.

<https://www.sslchecker.com/certdecoder>

Verify the entry "Subject/Organization": It should have the content "Post CH AG". Alternatively compare the fingerprint (SHA-1) with the one listed in the setup documentation for IncaMail.