

simple et sûr

IncaMail

Enterprise Application Integration MGI

Check-list d'introduction

Sommaire

1	Introduction.....	3
2	Aperçu des composants	3
3	Démarche.....	5
4	Organisation / communication	6
5	Check-list technique	7
6	Étapes suivantes	8
7	Explication technique	8

1 Introduction

Avec l'intégration de passerelle e-mail IncaMail (MGI ou intégration de domaine), votre système ERP (par ex. module RH pour l'envoi de documents de salaire) est étendu par la capacité d'envoyer et recevoir des messages e-mail sécurisés via le service IncaMail de la Poste Suisse.

Ce document vous aide à mettre en place IncaMail efficacement et à l'utiliser de manière optimale. L'introduction de cette intégration suppose des mesures techniques et organisationnelles. Le domaine des mesures organisationnelles comprend la politique d'e-mail et la communication avec l'utilisateur final et la revue des processus de soutien. Les mesures techniques comprennent les choix d'architecture et les travaux de connexion proprement dits.

2 Aperçu des composants

Les composants suivants de l'infrastructure mail de votre organisation sont importants pour l'intégration:

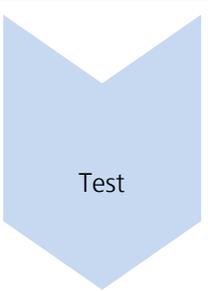
Composant	Signification	Exigence opérationnelle	Exigence technique
Logiciel ERP avec module d'interface IncaMail	Envoie des messages via IncaMail, par ex. des documents de salaire	Installation et configuration par le partenaire de logiciel ERP	Doit pouvoir envoyer des messages e-mail via le serveur mail
Client mail, par ex. Outlook®	Utilisé par l'utilisateur final pour la réception de messages IncaMail sécurisés (appareil fixe ou mobile).	Instructions des utilisateurs	Client mail standard (par ex. Outlook, GMail, Apple Mail etc.)
Navigateur	Utilisé par l'utilisateur final pour ouvrir des messages cryptés IncaMail SAFE (mode «personnel» ou «recommandé»). Peut aussi être utilisé pour l'accès au journal personnel (protocole après l'enregistrement).		Version actuelle de l'un des différents navigateurs populaires

Composant	Signification	Exigence opérationnelle	Exigence technique
Serveur mail, par ex. Exchange®	Reçoit et envoie des messages IncaMail soit directement du et vers le service IncaMail ou une passerelle e-mail	Inscription du domaine d'expédition et du certificat de serveur SSL utilisé auprès d'IncaMail	Pour la communication IncaMail: <ul style="list-style-type: none"> - Certificat X.509 valable avec une Certification Authority (CA) reconnue - Prise en charge de STARTTLS en communication SMTP via port 25 - Prise en charge de Mutual Authentication ou de Two-Way-Authentication pour le cryptage TLS (Inbound et Outbound) - Utilisation de MX Lookup - Des règles spéciales pour Incamail peuvent être saisies en option, mais pas pour des IP fixes si possible
En option: Passerelle e-mail	Établie entre le serveur mail et le service IncaMail	Comme le cryptage de transport se fait seulement à partir de la passerelle, il faut qu'un cryptage de transport suffisamment sûr soit garanti entre la passerelle et le serveur mail. Nous déconseillons les passerelles hébergées, car des données confidentielles sont alors décryptées auprès d'entreprises externes. Au lieu de cela, la communication IncaMail peut être effectuée directement du serveur mail.	Pour la communication IncaMail: <ul style="list-style-type: none"> - Certificat X.509 valable avec une Certification Authority (CA) reconnue - Prise en charge de STARTTLS en communication SMTP via port 25 - Prise en charge de Mutual Authentication ou de Two-Way-Authentication pour le cryptage TLS (Inbound et Outbound) - Les messages avec des pièces jointes HTML ne doivent pas être filtrés - Les messages avec pièces jointes HTML ne doivent pas être filtrés - Le serveur IncaMail ne doit pas être bloqué (→ év. entrée dans whitelist)
Firewall	Permet la communication entre passerelle/serveur mail et service IncaMail	Choix de séparer la réception et l'envoi: Est-ce le serveur mail ou la passerelle communique avec le service IncaMail?	Règles permettant la communication (entrante ou sortante du serveur mail) avec le serveur IncaMail via port 25 (et excluant éventuellement d'autres services).

3 Démarche

Sur la base de notre expérience, nous proposons la démarche suivante:

Phase	Objectif	Objets de livraison	Lead
Planification	Toutes les décisions nécessaires sont prises et les mesures correspondantes sont planifiées	<ul style="list-style-type: none"> Plan de mise en œuvre Prise de contact avec le partenaire de logiciels, Document de mise en place rempli et retourné à la Poste Date de mise en place 	Client
Préparation	Toutes les mesures nécessaires sont terminées afin que la mise en place puisse être effectuée efficacement.	<p>Mesures techniques</p> <ul style="list-style-type: none"> Le certificat SSL sur MTA (MailTransferAgent: serveur mail ou passerelle) est prêt pour la réception et l'expédition (Mutual Authentication). Remarque: le certificat utilisé doit être émis par une autorité de certification reconnue et enregistrée dans IncaMail. Attention: des certificats «exotiques» ne sont parfois par reconnus, tout comme des certificats ayant expiré ou auto-signés. En cas de doute, contactez-nous. Le paramétrage nécessaire dans le logiciel RH est fait <p>Mesures organisationnelles</p> <ul style="list-style-type: none"> La politique e-mail a été vérifiée et est conforme aux nouvelles exigences. Plan de de communication pour communication avec les collaborateurs 	Client
Mise-en-Place	Le client est relié à IncaMail	<ul style="list-style-type: none"> Liaison viable à IncaMail 	POSTE / Client

Phase	Objectif	Objets de livraison	Lead
 Test	La Poste, comme le client, a la certitude que la liaison fonctionne sans défaut.	<ul style="list-style-type: none"> • Procès-verbaux de réception • Documentation de mise en place 	POSTE

4 Organisation / communication

La check-list ci-après vous aide à préparer votre organisation de manière optimale.

Questionnement	Clair	Pas clair	À faire / remarques
4.1 Est-ce que je veux me servir de la notice d'utilisation standard d'IncaMail ou rédiger la mienne?			Standard www.poste.ch/incamail-downloads
4.2 À qui s'adresse l'émetteur du décompte de salaire lorsqu'il a des questions concernant la manipulation d'IncaMail dans la solution RH (1 st Level Support)?			Réponse: - Organisation d'assistance interne - Par e-mail / téléphone? - Heures de fonctionnement? - Partenaire de prise en charge
4.3 À qui s'adresse l'IT pour les questionnements complexes (2nd Level Support)?			Réponse: Lundi à vendredi 08 – 18h business@incamail.ch +41 (0) 848 00 04 15 (sauf jours fériés généraux CH)
4.4 À qui s'adresse le destinataire du décompte de salaire concernant la manipulation d'IncaMail?			Réponse: www.post.ch/incamail-contact
4.5 La Poste recommande d'informer au préalable les futurs destinataires de documents personnels via IncaMail et de les inviter à s'inscrire gratuitement. Avez-vous informé vos destinataires qu'ils recevront à l'avenir des e-mails confidentiels via IncaMail?			La Poste a préparé à cet effet des instructions pour destinataires. Celles-ci peuvent être téléchargées sous https://www.poste.ch/incamail-recipient-info-short .

5 Check-list technique

La check-list suivante vous sensibilise aux conditions techniques. À ce sujet voir le chapitre 6 explications techniques.

Questionnement	Clair	Pas clair	À faire / remarque
5.1 Avec quels composants d'infrastructure (MTA, serveur mail, passerelle mail), liaison doit-elle être réalisée? La réception et l'envoi peuvent se faire de manière différente. <ul style="list-style-type: none"> • Maîtrise-t-elle le cryptage TLS à l'aide de STARTTLS via port 25 avec authentification mutuelle via des certificats X.509? • Un certificat valable est-il installé pour la réception et l'envoi? • Faut-il poser des règles de routage et, si oui, est-ce possible? • Le certificat racine IncaMail («SwissSign Server Gold CA 2014 - G22») est-il contenu dans le truststore de la passerelle mail (de toute façon, c'est le cas pour les versions actuelles de Windows, Linux et OSX)? 			
5.2 Ce MTA est-il déjà paramétré pour l'utilisation de TLS? (certificat / configuration)			
5.3 Quel procédé de routage doit être mis en œuvre (à base de domaine, à base de contenu)?			
5.4 La matrice de communication réseau doit-elle être adaptée? <ul style="list-style-type: none"> • SMTP de MTA → im.post.ch (194.41.147.13 (gw1.incamail.com) ou 194.41.147.14 			Voir explications techniques au chapitre 6
5.5 Le monitoring doit-il être adapté? <ul style="list-style-type: none"> • Surveillance des logs pour la détection d'erreurs d'expédition concernant les e-mails IncaMail. • Surveillance des files d'attente d'email 			
5.6 Option: le domaine IncaMail im.post.ch a-t-il été ajouté à la white-list de votre serveur mail?			Les messages système d'IncaMail sont envoyés à l'adresse de l'expéditeur. Ceux-ci peuvent être retardés si votre serveur e-mail (ou votre passerelle e-mail) pratiquent le «greylisting» et retardent artificiellement les messages d'expéditeurs inconnus.

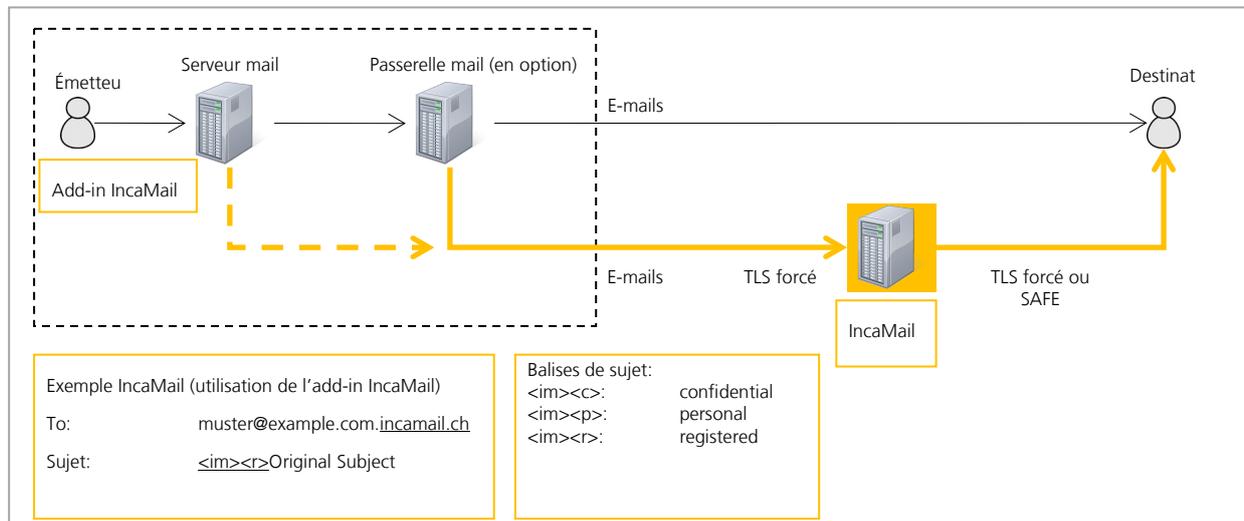
6 Étapes suivantes

La check-list ci-après montre quelles sont les étapes suivantes vis-à-vis de la Poste.

Étapes suivantes	Clair	Pas clair	À faire
6.1 Remplir la «documentation de mise en place»			
6.2 Retourner la «documentation de mise en place»			Joindre «documentation de mise en place» en annexe à la réponse au mail de bienvenue.
6.3 Déterminer la date de mise en ligne			Le helpdesk de la Poste confirme le délai souhaité dans la documentation de mise en place ou en trouve un nouveau en concertation.

7 Explication technique

Dans la vidéo ci-après vous trouverez l'animation qui vous initie au fonctionnement et à l'intégration d'IncaMail.
→ [Vidéo](#)



7.1 Flux des e-mails sortants

Un flux possible pour les e-mails sortants est décrit ci-après:

- (1) La solution RH veut envoyer des documents personnels à l'aide d'IncaMail.
- (2) L'e-mail est préparé en conséquence à l'aide de l'intégration de logiciel (dans le cas d'un e-mail confidentiel, le sujet est complété par «<im><c>» et l'adresse du destinataire est rallongée du suffixe de domaine «.incamail.ch»)
- (3) Le serveur mail interne reçoit les e-mails IncaMail et les transmet à la passerelle mail

- (4) La tâche de la passerelle mail consiste à transférer les e-mails aux bons serveurs mail (routage), dans le cas des e-mails IncaMail en utilisant des protocoles TSL/SSL (STARTTLS) en direction de la plateforme IncaMail.
 - a. L'identification du serveur IncaMail correct se fait en standard via une requête DNS (MX Lookup).
 - b. Alternativement, ceci peut se faire par des règles de routage. Actuellement, il existe les variantes suivantes:
 - i. Règle de routage: *.incamail.ch --> im.post.ch (si statique: 194.41.147.13 / 194.41.147.14)
- (5) Règle de routage alternative: Le sujet contient "<im>" --> im.post.ch (si statique: 194.41.147.13 / 194.41.147.14)
IMPORTANT: Il est déconseillé d'utiliser des IP statiques car celles-ci peuvent généralement changer!
La plateforme IncaMail reçoit l'e-mails IncaMail si la passerelle e-mail émettrice s'est authentifiée correctement. Pour cela, il doit maîtriser Mutual Authentication où le client et le serveur doivent montrer leurs certificats.
- (6) La plateforme IncaMail transmet l'e-mail IncaMail au destinataire conformément au mode de connexion choisi. Pour cela, elle doit maîtriser Mutual Authentication, où le client et le serveur doivent montrer leurs certificats

7.2 Flux d'e-mails entrants

Un flux possible pour les e-mails entrants est décrit ci-après:

- (1) La plateforme IncaMail envoie un e-mail à la passerelle mail via TSL/SSL L'adresse IP de la passerelle mail est soit déterminée via un MX-Lookup dans le DNS ou enregistrée comme IP statique ou nom d'hôte statique. Vous choisissez cette méthode avec les indications dans le document de mise en placeSSL
- (2) La passerelle e-mail reçoit l'e-mail
- (3) La passerelle e-mail vérifie s'il contient des logiciels malveillants (exception: e-mails recommandés ayant une annexe SAFE)
- (4) La passerelle mail transmet l'e-mail IncaMail au serveur mail interne
- (5) Le client mail récupère l'e-mail IncaMail du serveur mail
- (6) L'utilisateur final ouvre l'e-mail IncaMail
- (7) Dans le cas d'un recommandé:
 - a. L'utilisateur final ouvre la pièce jointe
 - b. L'utilisateur final clique «Ouvrir», le mail crypté au format SAFE étant transmis via HTTPS à la plateforme IncaMail pour le décryptage.

7.3 Test de liaison simple

Le flux d'e-mails sortants peut être testé sans Add-in de la manière suivante:

Destinataire: [Utilisez une adresse e-mail externe quelconque à laquelle vous ajoutez le suffixe «.incamail.ch», par ex. hans.muster.2543@gmail.com](mailto:hans.muster.2543@gmail.com) 

Concerne: <im><c> Test-Mail outbound to IncaMail

Bodytext: ceci est un test pour vérifier si la règle de routage fonctionne.

7.4 Vérifier si l'ordinateur reconnaît correctement le certificat de la plateforme IncaMail et inspecte les détails du certificat

IDS, IPS et d'autres systèmes peuvent se placer entre votre ordinateur et la plateforme IncaMail. Vous pouvez le constater au vu de certificats qui ne peuvent pas être attribués à la plateforme IncaMail et à la Poste Suisse.

Vous pouvez contrôler cela à l'aide de OpenSSL. Cet logiciel est capable de télécharger le certificat du serveur et de l'inspecter pour vérifier les détails.

Télécharger le certificat:

Jusqu'au Nov. 2015:

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

Après Dec. 2015:

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

Le certificat est enregistré comme "mycert.pem". Il peut être analysé à l'aide d'un décodeur online :

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

Vérifiez "Subject/Organisation": Le contenu devrait être "Post CH AG". Vous pouvez aussi comparer le fingerprint (SHA-1) avec celui qui se trouve dans la documentation "IncaMail Setup".