LA POSTE

simple et sûr

IncaMail
Intégration de passerelle e-mail (MGI)

Check-list d'introduction

Sommaire

1 Introduction

Avec l'intégration de passerelle e-mail IncaMail (MGI ou intégration de domaine), votre infrastructure e-mail est étendue par la capacité d'envoyer et recevoir des messages e-mail sécurisés via le service IncaMail de la Poste Suisse. L'utilisateur individuel dispose de l'expédition via des add-ins du client mail. L'intégration peut être effectuée pour un ou plusieurs domaines.

Ce document vous aide à mettre en place IncaMail efficacement et à l'utiliser de manière optimale. L'introduction de solutions e-mail sécurisées suppose des mesures techniques et organisationnelles. Le domaine des mesures organisationnelles comprend la politique d'e-mail, la communication avec l'utilisateur final et avec le partenaire 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 d'une organisation sont importants pour l'intégration.

Composant	**Signification**	**Exigence opérationnelle**	**Exigence technique**
Client mail, par ex. Outlook®	Utilisé par l'utilisateur final pour la réception et l'envoi de messages IncaMail sécurisés (appareil fixe ou mobile).	Instructions des utilisateurs	Add-in IncaMail permettant à l'utilisateur d'envoyer des messages IncaMail sécurisés
Application IncaMail	Application pour la lecture et l'envoi de messages IncaMail sur appareils mobiles Android et iOS	Instruction des utilisateurs	Application gratuite installée
Navigateur	Utilisé par l'utilisateur final pour ouvrir des messages cryptés IncaMail SAFE (mode d'expédition «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
Serveur mail, par ex. Exchange®	Reçoit et envoie des messages IncaMail soit directement du et vers le service IncaMail ou une passerelle e-mail		Pour la communication IncaMail: - 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-

Composant	Signification	Exigence opérationnelle	Exigence technique
			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: - 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	• Plan de mise en œuvre • Documentation de mise en place • Date de mise en place	Client
Préparation	Toutes les mesures nécessaires sont terminées afin que la mise en place puisse être effectuée efficacement.	Mesures techniques • Le certificat SSL sur MTA (MailTransferAgent: serveur mail ou passerelle) est prêt pour la réception et l'***expédition*** (mutual authentification) **Note:** le certificat utilisé doit provenir d'un service de certification reconnu figurant sur la liste trust de Mozilla: https://wiki.mozilla.org/CA:IncludedCAs • Attention: certains CA exotiques ne sont pas reconnus, pas plus que les certificats périmés ou self-signed. Demander dans le douteLa matrice de communication est mise en œuvre • Diffusion de Add-in intégrée dans la diffusion du logiciel Mesures organisationnelles • La politique e-mail a été vérifiée et est conforme aux nouvelles exigences Plan de communication • communication utilisateur final • communication partenaire	Client

Phase	Objectif	Objets de livraison	Lead
Mise en place	Le client est relié à IncaMail	• Liaison viable à IncaMail	POSTE / Client
Test	La Poste et le client ont la certitude que la liaison fonctionne sans défaut.	• L'envoi et la réception vers des adresses de communication internes et externes fonctionnent • Procès-verbaux de réception • Documentation de mise en place définitive	POSTE

4 Politique d'e-mail

La check-list ci-après vous aide à faire les bonnes réflexions concernant les questions qui doit / devrait / peut envoyer quoi et comment par IncaMail.

Questionnement		Clair	Pas clair	À faire
4.1	Qui (niveau, service, fonction) utilise IncaMail?			
4.2	Quels e-mails (contenu, processus opérationnel, destinataires) faut-il envoyer via IncaMail?			
4.3	Comment les e-mails sécurisés (envoyés via IncaMail) doivent-ils être rédigés, mis en page, intitulés (comme d'habitude, règlement spécifique)?			
4.4	Comment doit-on archiver des e-mails sûrs (envoyés ou reçus via IncaMail)?			

5 Organisation / communication

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

Questionnement		Clair	Pas clair	À faire / remarques
5.1	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
5.2	À qui s'adresse l'utilisateur lorsqu'il a des questions concernant la manipulation d'IncaMail (1st Level Support)?			• Organisation d'assistance interne • Par e-mail / téléphone? • Heures de fonctionnement?

5.3	À qui s'adresse l'IT pour les questionnements complexes (2nd Level Support)?			Helpdesk de la Poste Assistance pour client professionnels IncaMail Lundi à vendredi, 8 à 18h business@incamail.ch +41 (0) 848 00 04 15 (sauf jours fériés généraux)
5.4	Avez-vous informé vos collaborateurs des règlements et de l'utilisation d'IncaMail selon les chiffres 5.1 à 5.3?			Courrier aux collaborateurs
5.5	Avez-vous informé vos destinataires qu'ils recevront à l'avenir des e-mails confidentiels via IncaMail?			La Poste recommande d'informer au préalable les futurs destinataires de messages IncaMail et a préparé à ce sujet des instructions pour destinataires. Celles-ci peuvent être téléchargées sur www.poste.ch/incamail-recipient-info et adaptées à vos besoins. Une version courte est disponible sur www.poste.ch/incamail-recipient-info-short.

6 Check-list technique

La check-list suivante vous sensibilise aux conditions techniques. À ce sujet voir le chapitre 8 Explications techniques.

Questionnement	**Clair**	**Pas clair**	**À faire / remarques**
6.1 Avec quels composants d'infrastructure (MTA: serveur mail, passerelle mail) la connexion doit-elle être réalisée? La réception et l'envoi peuvent se faire de manière différente. • Maîtrise-t-elle le cryptage TLS à laide 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)?**?			
6.2 Ce MTA est-il déjà paramétré pour l'utilisation de TLS? (certificat / configuration)			

6.3	Quel est le procédé de routage à mettre en place (à base de domaine, à base de contenu)?			
6.4	La matrice de communication réseau doit-elle être adaptée? • SMTP de MTA →im.post.ch (194.41.147.13 (gw1.incamail.com) ou 194.41.147.14 (gw2.incamail.com))			Voir explications techniques au chapitre 8
6.5	Si vous utilisez Outlook, Lotus Notes ou GroupWise, comment mettrez-vous l'add-in IncaMail correspondant à disposition des utilisateurs?			Add-in à télécharger: www.poste.ch/incamail-downloads ➔ Pour les services de terminal / Citrix, veuillez observer les indications dans le ReadMe du paquet de téléchargement de l'add-in.
6.6	Comment et à qui faut-il distribuer l'add-in?			
6.7	Le monitoring doit-il être adapté? • Surveillance des logs pour la détection d'erreurs d'expédition concernant les e-mails IncaMail. • Surveillance des files d'attente d email			
6.8	L'infrastructure IncaMail a-t-elle été ajoutée à votre white-list?			Si l'infrastructure IncaMail n'a pas été ajoutée à la white-list, cela peut entraîner des retards et/ou des rejets lors de la réception de messages IncaMail.

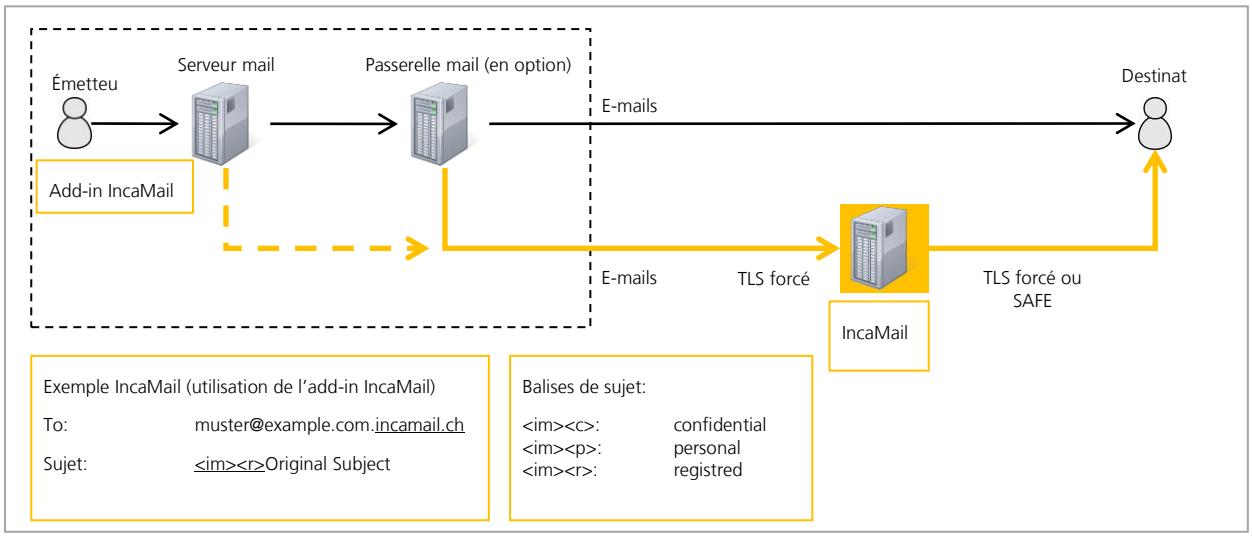
7 Étapes suivantes

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

Étapes suivantes		**Clair**	**Pas clair**	**À faire**
7.1	Remplir la «documentation de mise en place»			
7.2	Retourner la «documentation de mise en place»			Joindre «documentation de mise en place» en annexe à la réponse au mail de bienvenue.
7.3	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.

8 Explication technique

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



8.1 Flux des e-mails sortants

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

(1) L'utilisateur final veut envoyer un e-mail IncaMail

(2) L'e-mail est préparé en conséquence à l'aide de l'add-in (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 les 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)
ii. 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!

(5) La plateforme IncaMail transmet l'e-mail IncaMail au destinataire conformément au mode de connexion choisi.

8.2 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 place.

(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.

8.3 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 au choix à laquelle vous ajoutez „.incamail.ch", par ex. 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.

8.4 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 ce trouve dans la documentation "IncaMail Setup".