DIE POST

einfach sicher

IncaMail
Mailgateway-Integration (MGI)

Einführungscheckliste

Inhaltsverzeichnis

1 Einleitung 3

2 Komponentenübersicht 3

3 Vorgehen 4

4 E-Mail-Policy 6

5 Organisation / Kommunikation 6

6 Technische Checkliste 7

7 Next steps 8

8 Technische Erläuterung 9

1 Einleitung

Mit der IncaMail-Mailgateway-Integration (MGI oder Domänenintegration) wird Ihre E-Mail-Infrastruktur erweitert um die Fähigkeit, sichere E-Mail-Nachrichten über den IncaMail-Dienst der Schweizer Post zu versenden und zu empfangen. Für den einzelnen Anwender steht der Versand über Add-Ins des Mailclients zur Verfügung. Die Integration kann für eine oder mehrere Domänen vorgenommen werden.

Dieses Dokument unterstützt Sie, IncaMail effizient einzuführen und optimal zu nutzen. Das Einführen von sicheren E-Maillösungen bedingt technische und organisatorische Massnahmen. In den Bereich organisatorische Massnahmen fallen E-Mail-Policy, Anpassen der Kommunikationsrichtlinien, Enduser- und Partnerkommunikation und der Review der Supportprozesse. Unter die technische Massnahmen fallen Architekturentscheide und die eigentlichen Anbindungsarbeiten.

2 Komponentenübersicht

Für die Integration sind folgende Komponenten der Mail-Infrastruktur einer Organisation relevant:

Komponente	**Bedeutung**	**Anforderung operativ**	**Anforderung technisch**
Mailclient, z.B. Outlook®	Wird vom Endanwender für den Empfang und Versand von sicheren IncaMail-Nachrichten verwendet (Desktop und/oder Mobilgerät).	Instruktionen der Anwender	IncaMail Add-In, mit welchem der Anwender sichere IncaMail-Nachrichten versenden kann
Browser	Wird vom Endanwender für das Öffnen von verschlüsselten IncaMail-SAFE-Nachrichten verwendet (Versandart „persönlich“ oder „eingeschrieben“). Kann nach Registrierung auch für Zugriff auf persönliches Logbuch (Protokoll) verwendet werden.		Aktuelle Version eines der verschiedenen populären Browser
Mailserver, z.B. Exchange®	Empfängt und versendet IncaMail-Nachrichten entweder direkt von und an den IncaMail-Dienst oder ein E-Mail-Gateway		Für IncaMail-Kommunikation: - Gültiges X.509 Zertifikat einer anerkannten Certification Authority (CA) - Unterstützung von STARTTLS in SMTP-Kommunikation über Port 25 - Unterstützung von Mutual Authentication oder Two-Way-Authentication für TLS-Verschlüsselung (Inbound und Outbound) - Verwendung von MX Lookup

Komponente	Bedeutung	Anforderung operativ	Anforderung technisch
			- Spezielle Regeln für IncaMail können optional erfasst werden, aber möglichst nicht für fixe IPs
Optional: Mail-Gateway	Ist zwischen Mailserver und IncaMail-Dienst geschaltet	Da die Transportverschlüsselung erst ab dem Gateway erfolgt, muss eine hinreichend sichere Transportverschlüsselung zwischen Gateway und Mailserver gewährleistet sein. Von gehosteten Gateways ist abzuraten, da dann vertrauliche Daten bei Externen Unternehmen entschlüsselt werden. Stattdessen kann die IncaMail-Kommunikation direkt vom Mailserver erfolgen.	Für IncaMail-Kommunikation: - Gültiges X.509 Zertifikat einer anerkannten Certification Authority (CA) - Unterstützung von STARTTLS in SMTP-Kommunikation über Port 25 - Unterstützung von Mutual Authentication oder Two-Way-Authentication für TLS-Verschlüsselung (Inbound und Outbound) - SwissSign-Rootzertifikat des IncaMail-Serverzertifikats in Truststore enthalten - Nachrichten mit HTML-Anhängen dürfen nicht gefiltert werden - IncaMail-Server darf nicht gesperrt sein (→ ev. Eintrag in Whitelist)
Firewall	Ermöglicht Kommunikation zwischen Mailserver/Gateway und IncaMail-Dienst	Entscheid getroffen jeweils für Empfang und Versand getrennt: Kommuniziert Mailserver oder Gateway mit IncaMail-Dienst?	Regeln, welche die Kommunikation (ein- und oder ausgehend) des Mailservers mit dem IncaMail-Server über Port 25 ermöglichen (und ggf. andere Dienste ausschliessen).

3 Vorgehen

Auf der Basis unserer Erfahrung schlagen wir Ihnen folgendes Vorgehen vor:

Phase	Ziel	Lieferobjekte	Lead
Planung	Alle notwendigen Entscheidungen sind getroffen und die entsprechenden Massnahmen sind geplant	• Umsetzungsplan • Setup-Dokumenti ausgefüllt an Post retourniert • Setup-Termin	Kunde
Vorbereitung	Alle notwendigen Arbeiten sind erledigt, damit der Setup effizient durchgeführt werden kann.	Technische Massnahmen • SSL-Zertifikat auf MTA (MailTransferAgent: Mailserver oder Gateway) ist bereit für Empfang ***und Versand*** (Mutual Authentication) **Hinweis**: Das verwendete Zertifikat muss von einer anerkannten und bei IncaMail registrierten Zertifizierungsstelle ausgestellt sein. Vorsicht: Exotische CA's werden z.T. nicht anerkannt, ebensowenig abgelaufene oder self-signed Zertifikate. **Im Zweifelsfall anfragen** • Kommunikationsmatrix ist umgesetzt • Mailclient-Add-In-Verteilung ist in SW-Verteilung integriert Organisatorische Massnahmen • E-Mail-Policy ist überprüft und entspricht den neuen Anforderungen Kommunikationsplan - Enduser Kommunikation Partner Kommunikation	Kunde
Setup	Kunde ist an IncaMail angebunden	• Lauffähige Anbindung an IncaMail	POST / Kunde

Phase	Ziel	Lieferobjekte	Lead
Testen	Die Post und der Kunde haben die Gewissheit, dass die Anbindung einwandfrei läuft.	• Versand und Empfang zu internen und externen Kommunikationsadressen funktioniert • Abnahmeprotokolle • Definitive Setup-Dokumentation	POST

4 E-Mail-Policy

Die folgende Checklist unterstützt Sie darin, die richtigen Überlegungen zu machen bezüglich den Fragen wer / was / wie per IncaMail versenden muss / soll / darf.

Fragestellung	Klar	Unklar	To do
4.1 Wer (Stufe, Abteilung, Funktion) setzt IncaMail ein?			
4.2 Welche E-Mails (Inhalt, Geschäftsprozess, Empfänger) müssen via IncaMail versendet werden?			
4.3 Wie müssen sichere (via IncaMail versendete) E-Mails verfasst, aufgebaut, betitelt werden (wie üblich, spezielle Regelung) ?			
4.4 Wie müssen sichere (via IncaMail versendete oder empfangene) E-Mails archiviert werden?			

5 Organisation / Kommunikation

Die folgende Checklist unterstützt Sie darin, sich organisatorisch optimal vorzubereiten.

Fragestellung	Klar	Unklar	To do / Bemerkungen
5.1 Will ich die Standard Bedienungsanleitung von IncaMail nutzen oder möchte ich eine eigene erstellen?			Standard: www.post.ch/incamail-downloads
5.2 Wen kontaktiert der firmeninterne IncaMail Benutzer, wenn er Fragen bezüglich der IncaMail Handhabung hat (1st Level Support)?			• Eigene Supportorganisation • Per E-Mail / Telefon? • Betriebszeiten?
5.3 Wen kontaktiert die IT bei komplexen Fragestellungen (2nd Level Support)?			Help Desk Post IncaMail-Geschäftskundensupport Montag bis Freitag 08.00 – 18.00 business@incamail.ch +41 (0) 848 00 04 15 (ausgenommen allgemeine Feiertage CH)

5.4	Haben Sie Ihre Mitarbeitenden über die Einführung und Nutzung von IncaMail sowie Regelungen gemäss Ziffern 5.1 bis 5.3 informiert?			Anschreiben MA
5.5	Haben Sie Ihre Empfänger informiert, dass sie in Zukunft vertrauliche E-Mails via IncaMail erhalten?			Die Post empfiehlt, die künftigen Empfänger von IncaMail-Nachrichten vorgängig zu informieren und hat dazu eine Empfängeranleitung vorbereitet. Diese kann unter https://www.post.ch/incamail-recipient-info-short heruntergeladen werden.

6 Technische Checkliste

Die folgende Checklist macht Sie auf technische Voraussetzungen aufmerksam. Vergleichen Sie dazu Kapitel 8 Technische Erläuterungen.

Fragestellung		**Klar**	**Unklar**	**To do / Bemerkungen**
6.1	Mit welchen Infrastrukturkomponenten (MTA: Mailserver, Mailgateway) soll die Anbindung realisiert werden? Empfang und Versand können dabei unterschiedlich erfolgen. • Beherrscht diese TLS-Verschlüsselung mittels STARTTLS über Port 25 mit beidseitiger Authentifizierung mittels X.509-Zertifikaten? • Ist ein gültiges Zertifikat für Empfang und Versand installiert? • Ist das Setzen von Routingregeln erforderlich und falls ja, ist es möglich? • Ist das IncaMail-Rootzertifikat („SwissSign Server Gold CA 2014 - G22") im Truststore des Mail-Gateways enthalten (bei aktuellen Windows, Linux und OSX-Versionen ist das sowieso der Fall)?				
6.2	Ist dieser MTA schon für die Verwendung von TLS eingerichtet? (Zertifikat / Konfiguration)			
6.3	Welches Routingverfahren soll umgesetzt werden (Domain based, Content based)?			
6.4	Muss die Netzwerkkommunikationsmatrize angepasst werden? • SMTP von MTA →im.post.ch (194.41.147.13 (gw1.incamail.com) oder 194.41.147.14 (gw2.incamail.com))			Siehe technische Erläuterungen Kapitel 8

6.5 Falls Sie Outlook, Lotus Notes, Mozilla Thunderbird oder GroupWise einsetzen, wie werden Sie das entsprechende IncaMail Add-in den Benutzern zur Verfügung stellen?			Download Add-in: www.post.ch/incamail-downloads
6.6 Wie und an wen soll das Add-In verteilt werden?			
6.7 Muss das Monitoring angepasst werden? • Überwachung der Logs auf Zustellungsfehler bezüglich IncaMail E-Mails • Überwachen von Mailqueues			
6.8 Ist die IncaMail-Domain in Ihre White-list aufgenommen?			Sofern die IncaMail-Domain nicht in die White-list aufgenommen wurde, kann es zu Verzögerungen und/oder Ablehnungen beim Empfangen von IncaMail-Nachrichten führen.

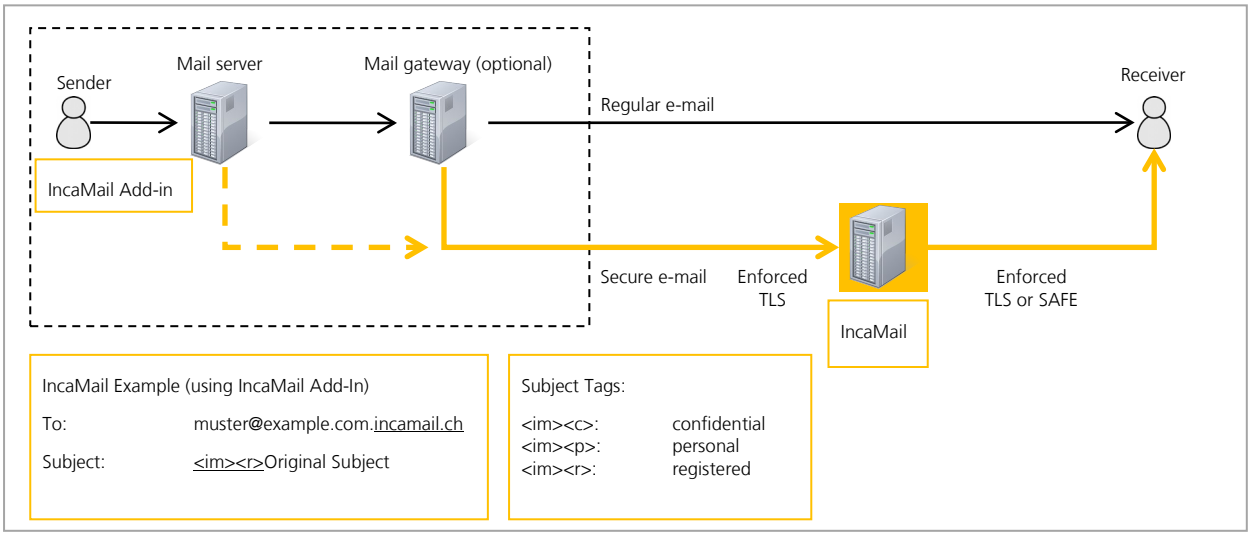
7 Next steps

Die folgende Checklist zeigt auf, welches die nächsten Schritte gegenüber der Post sind.

Nächste Schritte	**Klar**	**Unklar**	**To do**
7.1 "Setup Documentation" ausfüllen			
7.2 „Setup-Documentation" retournieren			Die „Setup-Documentation" ist der Antwort auf die WelcomeMail als Anhang beizufügen.
7.3 Aufschalttermin abstimmen			Der in der „Setup-Documentation" gewünschte Termin wird durch den Post Helpdesk bestätigt oder gemeinsam ein neuer Termin gesucht.

8 Technische Erläuterung

Unter folgendem Video finden Sie die Animation, welche Sie in die Funktionsweise und Integration von IncaMail einführt. →Video



8.1 E-Mail-Fluss Outbound

Im Folgenden wird ein möglicher Outbound-Mailfluss beschrieben:

(1) Endbenutzer will eine IncaMail E-Mail versenden

(2) Mit Hilfe des Add-ins wird die E-Mail entsprechend vorbereitet (Subject wird im Fall eines vertraulichen E-Mails mit "<im><c>" ergänzt und Empfänger-Adresse wird um die Domainsuffix ".incamail.ch" erweitert)

(3) Der interne Mail-Server nimmt diese IncaMail E-Mail entgegen und gibt sie dem Mailgateway weiter

(4) Der Mailgateway hat die Aufgabe E-Mails an die richtigen Mailserver weiter zuleiten (Routing), im Falle von IncaMail E-Mails unter Verwendung des TSL/SSL (STARTTLS)-Protokolls an die IncaMail-Plattform.

a. Die Bestimmung des korrekten IncaMail-Mailservers erfolgt standardmässig über eine DNS-Abfrage (MX Lookup).
b. Alternativ dazu kann sie über Routing-Regeln erfolgen. Dabei gibt es folgende Varianten:

i. Routing-Regel: *.incamail.ch --> im.post.ch (falls statisch: 194.41.147.13 / 194.41.147.14)

ii. Alternative Routing-Regel: Subject enthält "<im>" --> im.post.ch (falls statisch: 194.41.147.13 / 194.41.147.14)
WICHTIG: Es wird davon abgeraten, statische IPs zu verwenden, da diese generell ändern können!

(5) Die IncaMail Plattform nimmt die IncaMail E-Mail entgegen, sofern der sendende Mailgateway sich korrekt durch sein SSL Zertifikat authentifiziert hat. Dafür muss er Mutual Authentication beherrschen, bei welchem Client und Server ihre Zertifikate zeigen müssen.

(6) Die IncaMail Plattform leitet das IncaMail-E-Mail an den Empfänger weiter, gemäss der gewählten Anschlussart.

8.2 E-Mail Fluss Inbound

Im Folgenden wird ein möglicher Inbound-E-Mailfluss beschrieben:

(1) IncaMail Plattform sendet E-Mail über TLS/SSL an den Mailgateway. Die IP-Adresse des Mailgateways wird entweder über ein MX-Lookup im DNS ermittelt oder als statische IP oder statischer Hostname hinterlegt. Diese Methode bestimmen Sie mit den Angaben im Setup-Dokument.

(2) Mailgateway nimmt E-Mail entgegen

(3) Mailgateway prüft dieses auf Schadsoftware (Ausnahme: Eingeschriebene E-Mails, welche einen SAFE-Anhang haben)

(4) Mailgateway leitet die IncaMail E-Mail an den internen Mailserver weiter

(5) Mailclient holt die IncaMail E-Mail vom Mailserver ab

(6) Endbenutzer öffnet die IncaMail E-Mail

(7) Fall Einschreiben:

   a. Endbenutzer öffnet das Attachement

   b. Endbenutzer klickt „Öffnen“, dabei wird das verschlüsseltes Mail im SAFE-Format zum Entschlüsseln über HTTPS an die IncaMail-Plattform übertragen

8.3 Einfacher Anbindungstests

Der Outbound-E-Mail-Fluss kann ohne Add-in wie folgt getestet werden:

Empfänger: Verwenden Sie eine beliebige externe E-Mail-Adresse, an welche Sie die Endung „.incamail.ch“ anhängen, z.B. hans.muster.2543@gmail.com .

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

Bodytext: Dies ist ein Test, ob die Routing-Regel funktioniert…

8.4 Prüfen, ob Ihr Rechner das korrekte IncaMail-Plattform Zertifikat erkennt und Lesen der Zertifikatsinformationen

IDS, IPS und andere Systeme können sich zwischen Ihren Rechner und der IncaMail-Plattform schalten. In diesem Fall sieht Ihr Rechner bei der Kommunikation mit dem IncaMail-Server ein Zertifikat, welches nicht der IncaMail-Plattform zugeordnet werden kann.

Um das zu überprüfen, können Sie OpenSSL verwenden (ggf. zuerst installieren). Damit können Sie das Zertifikat zuerst herunterladen und dann inspizieren.

Herunterladen des Zertifikats:

openssl s_client –connect gw1.incamail.com:25 –starttls smtp >zertifikat.pem

Danach befindet sich das Zertifikat in der Datei „zertifikat.pem“. Sie können es nun analysieren mit einem Online-Decoder, z.B.

https://www.sslchecker.com/certdecoder

Verifizieren Sie, dass unter Subject/Organization „Post CH AG“ steht, oder noch besser, vergleichen Sie den Fingerprint (SHA-1) mit demjenigen in der Setup-Doku.