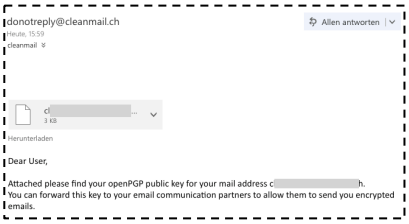
Cleanmail Sign + Encrypt PGP – Kurzanleitung

Schlüsseltausch

Bevor über PGP verschlüsselte Mails ausgetauscht werden können, müssen die Kommunikationspartner ihre öffentlichen Schlüssel austauschen. Dieser Schlüsselaustausch muss nur einmal stattfinden, danach verläuft die Verschlüsselung transparent.

Schlüsseltausch interner Benutzer zu externem Benutzer:
Der interne Benutzer erhält beim Erstellen des PGP-Schlüssels ein Mail mit dem öffentlichen Schlüssel (eine Datei mit der Endung .asc). Diese Datei muss an den externen Benutzer gesendet werden, der ihn dann in sein PGP-Programm aufnehmen muss.



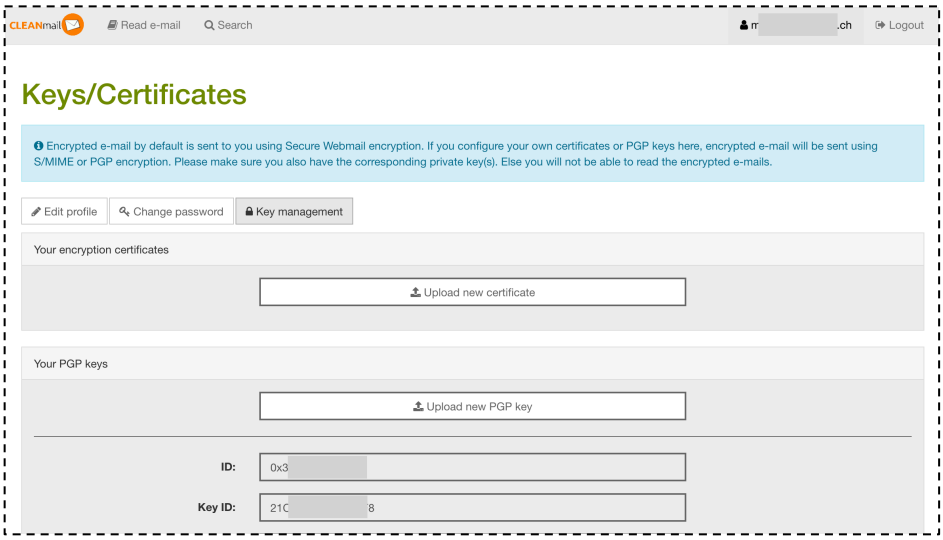
Es ist ratsam, dass die Zustellung des Schlüssels ausserhalb von E-Mail bestätigt wird (zB mit einem kurzen Telefonat).

Schlüsseltausch externer Benutzer zu internem Benutzer: Der öffentliche Schlüssel des externen Benutzers muss auf dem Gateway für die Verschlüsselung hinterlegt werden, im sogenannten GINA-Portal. Das geschieht in zwei Schritten:

Der interne Benutzer schickt dem externen Benutzer eine verschlüsselte neue Nachricht und fügt „[secure]“ in die Subject:-Zeile ein (sonstiger Inhalt ist egal, ratsam ist nur einen kurzen Text einzugeben).

Nun erhält der externe Benutzer eine Nachricht zugesandt, die ihn zum registrieren auf dem GINA-Portal auffordert. Der interne Benutzer erhält eine Nachricht mit dem Passwort, welches der externe Benutzer für die Registrierung benötigt (dieses Passwort kann über einen Klick per SMS an den externen Benutzer geschickt werden).

Nachdem der externe Benutzer die Registrierung im GINA-Portal abgeschlossen hat, muss er seinen öffentlichen Schlüssel hochladen (Klick oben rechts im GINA-Portal auf die Mailadresse, dann unter „Key Management“, „Upload new PGP key“).



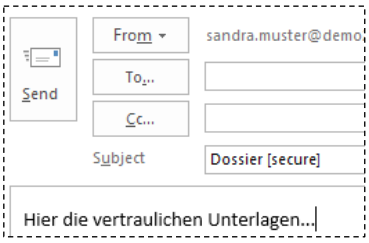
Der externe Benutzer sollte das Passwort zum GINA-Account sicher behandeln, um die Vertraulichkeit der Kommunikation zu gewährleisten.

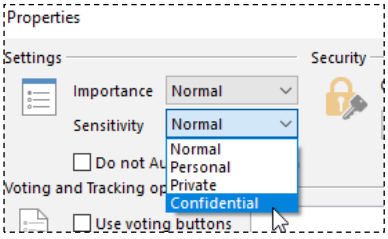
Verschlüsselte Nachricht Senden

Für die meisten Kunden werden Mails automatisch verschlüsselt, nachdem der Schlüsselaustausch erfolgt ist. Die Verschlüsselung kann aber auch explizit angefordert werden:

Um eine Nachricht zu verschlüsseln, fügen Sie dem Subject: das Tag „[secure]“ hinzu. Falls eine Nachricht von aussen entschlüsselt wurde, ist das Tag bereits gesetzt – damit ist sichergestellt, dass auf verschlüsselte Nachrichten ebenfalls mit einer verschlüsselten Nachricht geantwortet wird.

Alternativ kann der interne Benutzer in MS Outlook (oder im Outlook Web Access) die Nachrichtenoption „Vertraulichkeit“ auf „vertraulich“ setzen.





Empfohlene Einstellungen / Nutzungshinweise

Für Mail-/PGP-Programme von externen Benutzern: Aufgrund von verschiedenen Sicherheitsüberlegungen, und um die heute gängigen komplexen Mailformatierungen (HTML, Anhänge) adäquat unterstützen zu können, ist es empfehlenswert die Option „**PGP/MIME**“ statt „Inline PGP“ verwendet werden.

Generell für Subject-Zeilen: Bei der Verschlüsselung wird lediglich der Inhalt einer Nachricht verschlüsselt, nicht aber die sogenannten Header-Zeilen. Die Header-Zeilen beschreiben den Weg, den eine Nachricht genommen hat, Absender, Empfänger, Zeitpunkt und (kritisch!) die Subject-Zeile der Nachricht. Verschiedene PGP-Programme bieten die Möglichkeit, die Subject-Zeile zusätzlich zu verschlüsseln, doch leider gibt es dazu keinen Standard. Es ist daher empfehlenswert, beim Verfassen der Subject-Zeile die dort nicht vorhandene Verschlüsselung zu beachten.