

## 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.

<u>Schlüsseltausch interner Benutzer zu externem Benutzer</u>: 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.

(donotreply@cleanmail.ch I <sup>tenen</sup> t559 I <sup>denmail V</sup>	Allen antworten
Herunterladen Dear User,	
Attached please find your openPGP public key for your mail address c You can forward this key to your email communication partners to allow th emails.	h. em to send you encrypted

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

<u>Schlüsseltausch externer Benutzer zu internem Benutzer</u>: 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).

Secure e-i	nail pas	sword	
You have for the fir possible of the pass able to read the cor	st time sent an word below eith ntent of the mes	encrypted e-ma her by phone, S ssage.	ail to MS
When initially readi reminder question ( mails we send him.	ng the encrypte for password re	d e-mail, the re ecovery). This n	cipi ew (
Recipient			
Date: Wed			
Date: Wed Subject: t			
Date: Wed Subject: t			
Date: Wed Subject: t Password			



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").

EANmail	🛢 Read e-mail	Q Search						<b>≜</b> m	.ch	🕩 Logout
Keys/	'Certific	ates								
Encrypted S/MIME or F	d e-mail by default is PGP encryption. Plea	sent to you ase make sur	using Secure Webmai re you also have the c	il encryption. If yo orresponding priv	u configure your c ate key(s). Else yo	own certificates or PGP k ou will not be able to read	eys here, enci I the encrypte	rypted e-mail w d e-mails.	ill be sent usi	ng
<ul> <li>Edit profile</li> <li>Your encryp</li> </ul>	e & Change pas	sword	Key management							
				ᆂ Uplo	ad new certificate					
Your PGP ke	eys									
				ᆂ Upic	oad new PGP key					
		ID:	0x3							
		Key ID:	21C	8						

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.

Ŧ <b></b>	To	
<u>S</u> end	10	
	<u>C</u> c	
	S <u>u</u> bject	Dossier [secure]

Propert	ies			
Settings				Security -
:	Importance	Normal	$\sim$	
	Sensitivity	Normal	~	- 6
Voting a	Do not Au	Normal Personal Private		
A	Use voting	Confidential buttons	6	



## Empfohlene Einstellungen / Nutzungshinweise

<u>Für Mail-/PGP-Programme von externen Benutzern</u>: 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.

<u>Generell für Subject-Zeilen</u>: 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.