Dirk Fox

GPGrelay

Die „lokale Poststelle“

Verschlüsselungsgateways oder „virtuelle Poststellen“ haben in vielen Unternehmen und Behörden der Ende-zu-Ende-Verschlüsselung von E-Mails den Rang abgelaufen: Sie sind universeller einsetzbar, zentral konfigurierbar und entlasten den Nutzer. Für mittelständische Unternehmen und unternehmensübergreifende Arbeitsgruppen kann auch das Open Source Tool GPGrelay eine geeignete Alternative sein.

Verschlüsselungsgateways

Die ersten E-Mail-Verschlüsselungslösungen, die auf den Standards PEM (später S/MIME) oder OpenPGP basierten, setzten einen strikten Ende-zu-Ende-Schutz um: Der Sender verschlüsselte die Nachricht vor dem Versand, der Empfänger entschlüsselte sie mit seinem geheimen persönlichen Entschlüsselungsschlüssel. Aus Sicherheitssicht ist dieser Ansatz sinnvoll: Sofern starke kryptographische Algorithmen und hinreichend lange Schlüssel zum Einsatz kommen, hat ein Angreifer keine Möglichkeit, durch Abhören der Übertragungsstrecke an den Inhalt einer Nachricht zu gelangen.

Schon bald zeigte die Praxis zahlreicher PKI-basierter Infrastrukturen, dass Ende-zu-Ende-Verschlüsselungslösungen mit zahlreichen Schwierigkeiten zu kämpfen hatten:

- Die vollständige Nutzerkontrolle über die Verschlüsselung von Nachrichten und die damit einher gehende hohe Transparenz wurde von den Nutzern nicht als Bereicherung, sondern als Belastung empfunden – sodass auf eine Verschlüsselung häufig aus Bequemlichkeit verzichtet wurde.
- Der Erfolg der Verschlüsselungslösung stand und fiel mit der Integration in den jeweils verwendeten E-Mail-Client. Häufig ließ sich eine solche Integration nur durch die Installation von zusätzlicher Software (Plug-In) erreichen – ein erhebliches Hindernis in größeren Unternehmen, da dort meist der Betrieb unterschiedlicher Programmversionen ein automatisches Roll-Out von Plug-Ins erschwert.
- Eingehende verschlüsselte E-Mails ließen sich zwar mit der Entschlüsselungssoftware entschlüsseln, wurden aber „original“ (also verschlüsselt) in den E-Mail-Ordnern abgelegt. Bei jedem erneuten Öffnen der Nachricht war daher eine Entschlüsselung erforderlich. Das verzögerte die E-Mail-Bearbeitung bei intensiver Nutzung der Nachrichtenverschlüsselung – und verhinderte wirksam eine Volltextsuche in E-Mail-Ordnern.

Schließlich barg das Nebeneinander der Standards OpenPGP und S/MIME Konfliktpotential: Gut integrierte und bedienungsfreundliche Lösungen auf dem Client-System setzten in der Regel eine Entscheidung für einen der beiden Verschlüsselungs-Standards voraus.

Konsequenterweise begannen sich daher Alternativen zu einer Ende-zu-Ende-Verschlüsselung durchzusetzen: Verschlüsselungsgateways (auch „virtuelle Poststellen“ genannt), die als „Proxy-E-Mail-Server“ zwischen E-Mail-Server und –Client geschaltet wurden und die Ver- und Entschlüsselung von Nachrichten übernahmen.

Damit ließen sich in der Praxis die meisten praktischen Schwierigkeiten lösen: Verschlüsselungsgateways

- können von jedem E-Mail-Client[1] unabhängig von Version und Betriebssystem und ohne Plug-In direkt genutzt werden,
- unterstützen in der Regel sowohl S/MIME als auch OpenPGP,
- entlasten den Nutzer vom Schlüsselmanagement und der Prüfung von Sperrlisten,
- erlauben die zentrale Freischaltung von (geprüften) Schlüsseln,
- ermöglichen die zentrale Konfiguration und Durchsetzung von Verschlüsselungspolicies (Schlüssellängen, Algorithmen, Empfängergruppen, Zugriff auf Verzeichnisdienste etc.) und
- sorgen für eine unverschlüsselte Speicherung aller Nachrichten im E-Mail-Client des Empfängers.

Auch mit dem zwischengeschalteten Verschlüsselungsgateway kann die Übermittlung auf der Teilstrecke zwischen E-Mail-Client und Gateway verschlüsselt erfolgen, indem die Verbindung mit dem TLS/SSL-Protokoll geschützt wird. Bleiben zwei Nachteile: Der Entzug der Benutzerkontrolle und die zentrale Speicherung der geheimen Signier- und Entschlüsselungsschlüssel.

Die meisten Verschlüsselungsgateways kompensieren den Kontrollverlust des Benutzers über die Nachrichtenverschlüsselung durch Kommandos in der Betreff-Zeile einer E-Mail: Darüber kann der Sender einer Nachricht die Verschlüsselung und Signatur durch das Gateway erzwingen oder verhindern. Eingehende ver-

Dirk Fox

Geschäftsführer der Secorvo Security Consulting GmbH und Herausgeber der DuD.
E-Mail: dirk.fox@secorvo.de

1 Einschließlich PDAs und Smartphones, sofern sie über ein Standardprotokoll (POP3 oder IMAP) auf den E-Mail-Server zugreifen.

Abb.: Konfiguration Relay-Server

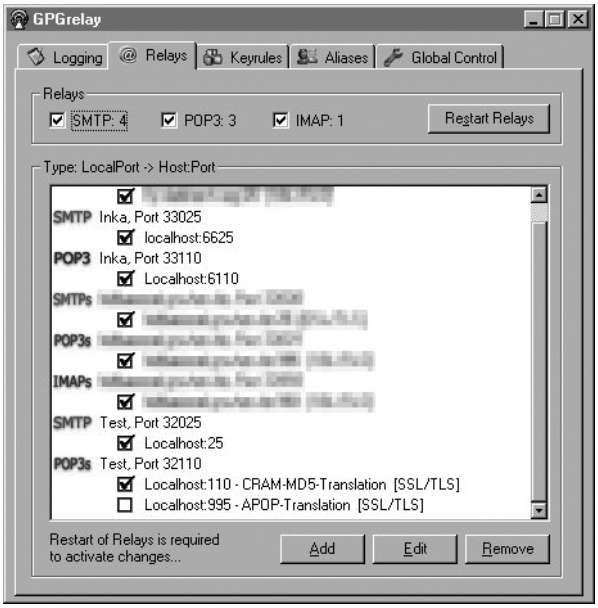


Abb.: Konfiguration der Relay-Server

schlüsselte oder signierte E-Mails werden nach der Entschlüsselung bzw. Signaturprüfung mit einem entsprechenden Vermerk versehen.

Die zentrale Speicherung geheimer Schlüssel im Gateway erfordert zwar geeignete Maßnahmen zum Schutz vor Missbrauch, verhindert aber zugleich den Verlust von Schlüsseln z. B. bei einem Wechsel oder einer Neuinstallation eines Client-Systems.

GPGrelay

Für viele kleine mittelständische Unternehmen oder unternehmensübergreifende Arbeitsgruppen, die eine benutzerfreundliche Lösung zur E-Mail-Verschlüsselung suchen, sind Installation und Betrieb eines Verschlüsselungsgateways jedoch zu aufwändig. In solchen Fällen stellt die Open-Source-Lösung GPGrelay eine elegante Alternative dar.

GPGrelay basiert auf der vom Bundeswirtschaftsministerium geförderten Entwicklung GNU Privacy Guard (GNUPG)[2] – einer Kommandozeilen basierten freien Open-Source-Implementierung des OpenPGP-Standards.

GPGrelay vereinfacht die Nutzung von GNUPG zur E-Mail-Verschlüsselung. Mit der Programmierung in C++ begann Andreas John im Jahr 2001. Die aktuelle, englischsprachige Version v0.959 für Microsoft Windows wurde am 31.03.2005 herausgegeben und kann bpsw. unter Sourceforge.net heruntergeladen werden.[3] Mit nur 646 kByte ist sie bestechend klein.

GPGrelay wird auf dem Client-System installiert und stellt einen „lokalen E-Mail-Proxy" zur Verfügung. Entsprechend konfiguriert wird GPGrelay zwischen E-Mail-Client und –Server geschaltet und übernimmt die Ver- und Entschlüsselung sowie die Signierung und Signaturprüfung von E-Mail-Nachrichten.

Damit bietet GPGrelay drei Vorteile eines Verschlüsselungsgateways auch ohne die Installation eines separaten Proxy-Servers:

- es kann – unter Microsoft Windows – von jedem E-Mail-Client und ohne Plug-In direkt genutzt werden,
- es entlastet den Nutzer weitgehend vom Schlüsselmanagement und
- es sorgt für die unverschlüsselte Speicherung aller Nachrichten im E-Mail-Client des Empfängers.

Wie bei einem „ausgewachsenen" Verschlüsselungsgateway können auch in GPGrelay sowohl Verschlüsselungsprofile für bestimmte Empfänger und Empfängergruppen angelegt als auch durch Kommandos in der Betreff-Zeile der E-Mail die Nachrichtenverschlüsselung gesteuert werden.

Anders als die meisten Verschlüsselungsgateways unterstützt GPGrelay allerdings nur den Standard OpenPGP (RFC 2440).[4] Je nach Konfiguration werden die verschlüsselten Nachrichten als PGP-kompatible Verschlüsselungsblöcke im Text verschickt oder Standard-konform als PGP-MIME-Nachricht (RFC 2015, 3156)[5] codiert. Damit auch Nachrichtenanhänge automatisch entschlüsselt werden, muss das format PGP-MIME gewählt werden. Damit sind die Nachrichten kompatibel zu PGP-verschlüsselten E-Mails; S/MIME-Nachrichten kann GPGrelay jedoch nicht verarbeiten.

Installation und Konfiguration

Voraussetzung für die Installation von GPGrelay ist ein bereits installiertes GNU Privacy Guard (GNUPG), der deutschen Open-Source-Implementierung für Erzeugung und Management von PGP-Schlüsseln, in Version 1.4.1 oder höher. Sofern die Pfade richtig eingestellt sind, lädt GPGrelay beim Starten die von GNUPG verwalteten Schlüssel aus dem Schlüsselring. Ist dieser Schlüsselring leer, wird automatisch die Erzeugung eines Schlüsselpaares gestartet.[6]

2 http://www.gnupg.org

3 http://gpgrelay.sourceforge.net

4 http://www.ietf.org/rfc/rfc2440.txt

5 http://www.ietf.org/rfc/rfc2015.txt, http://www.ietf.org/rfc/rfc3156.txt

6 Auch die Schlüssel eines PGP-Schlüsselrings lassen sich nutzen. Dazu müssen diese zuvor manuell in GNUPG importiert werden.

Abb.: Generelle Einstellungen

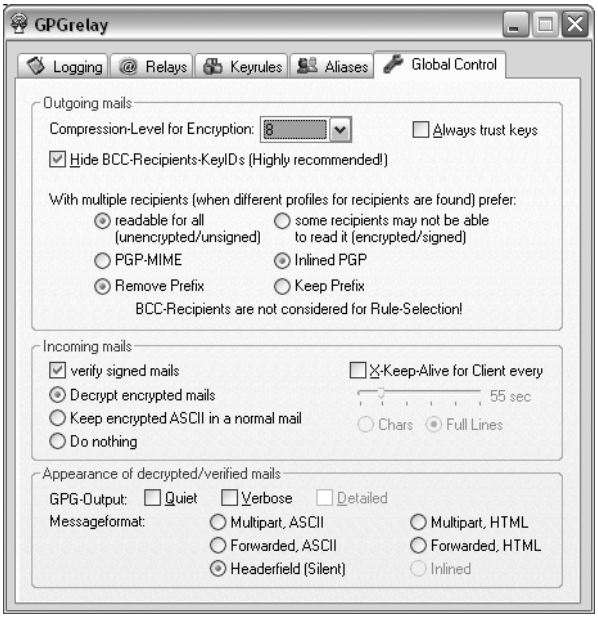
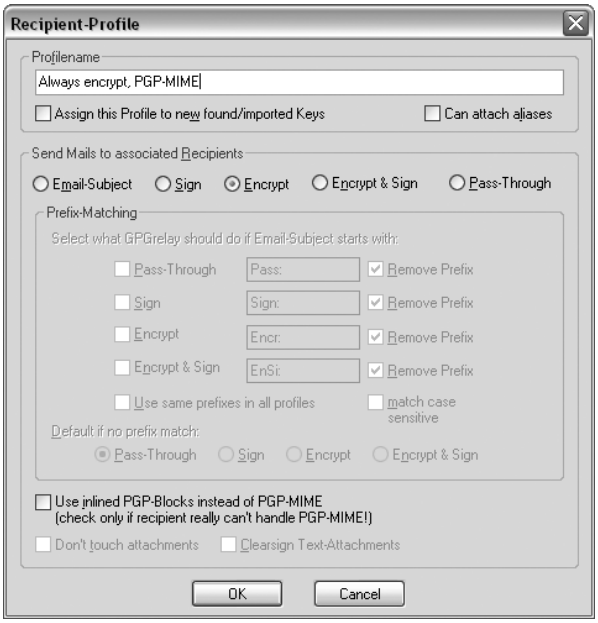


Abb.: Konfiguration eines Profils



GPGrelay kann mit unterschiedlichen POP3-, SMTP- und IMAP-Servern verbunden werden. Damit ermöglicht GPGrelay eine elegante Zusammenführung von E-Mails unterschiedlicher E-Mail-Server (Freemailer, Webmaster-Accounts, ...) in einem E-Mail-Client.

Dazu müssen Relays für alle SMTP-, POP3- und IMAP-Server konfiguriert werden, mit denen GPGrelay verbunden werden soll („Relays“, siehe Abb.):

- Vergabe eines logischen Namens
- Festlegung des lokalen Ports
- Eintrag des E-Mail-Servers und des dort genutzten Ports
- Ggf. Auswahl von SSL/TLS zur Verschlüsselung der Verbindung zum E-Mail-Server.

Im E-Mail-Client werden die dort eingetragenen E-Mal-Server jeweils durch Localhost (127.0.0.1) ersetzt.

Unter den Relay-Servern müssen mindestens ein POP3- und ein SMTP-Server sein, sofern GPGrelay ein- und ausgehende E-Mails ver- und entschlüsseln soll. Die gewünschten aktiven Relay-Server werden über ein Kontrollkästchen ausgewählt und beim Starten von GPGrelay automatisch initialisiert. Nach jeder Konfigurationsanpassung müssen die Änderungen mit „Restart Relays“ aktiviert werden.

Im Anschluss an die Konfiguration der Relay-Server können unter „Global Control“ einige Grundeinstellungen vorgenommen werden. Dort lassen sich z. B. der Kompressionslevel, das Format der OpenPGP-E-Mails und die Art der Markierung entschlüsselter E-Mails auswählen.

Abb.: Einstellung des Schlüsselprofils

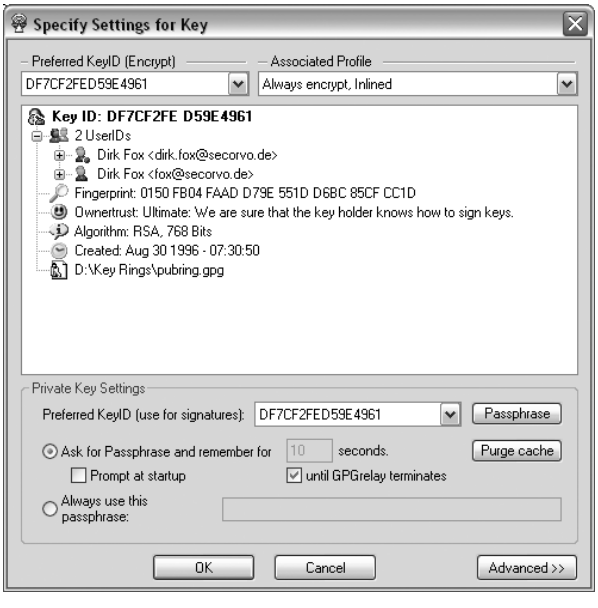
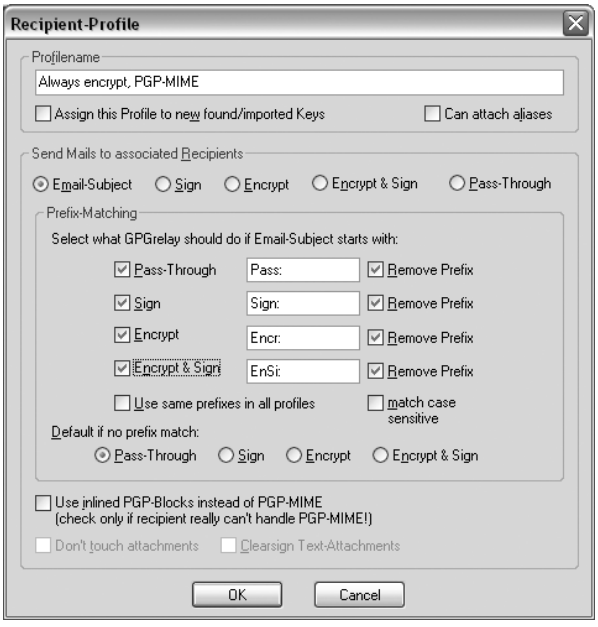


Abb.: Präfixkommando-Konfiguration



Wichtig für den Empfang von E-Mails mit umfangreichen Anhängen ist die Option „X-Keep-Alive for Client“, die die regelmäßige Aussendung von „Kontakt“-Paketen an den E-Mail-Client veranlasst. Damit lässt sich ein vorzeitiger Timeoff des E-Mail-Clients verhindern.

Profile

Die Behandlung ausgehender E-Mails an bekannte Empfängeradressen wird in Profilen konfiguriert. Dazu sind mehrere Profile vorgegeben; es lassen sich jedoch weitere eigene anlegen.

Anschließend werden die aus GNUPG importierten Schlüssel einem Profil zugeordnet. Das geht elegant durch Verschieben des Schlüssels mit der Maus. Eines der Profile kann als Standard-Profil ausgewählt werden; neue Schlüssel werden dann automatisch zunächst diesem Profil zugeordnet.

Zusätzlich lassen sich für jeden Schlüssel weitere Festlegungen treffen, z. B. ein spezifischer Umgang mit der Passphrase beim Entschlüsseln einer für diesen Schlüssel verschlüsselten Nachricht (siehe Abb.).

Client-Kontrolle

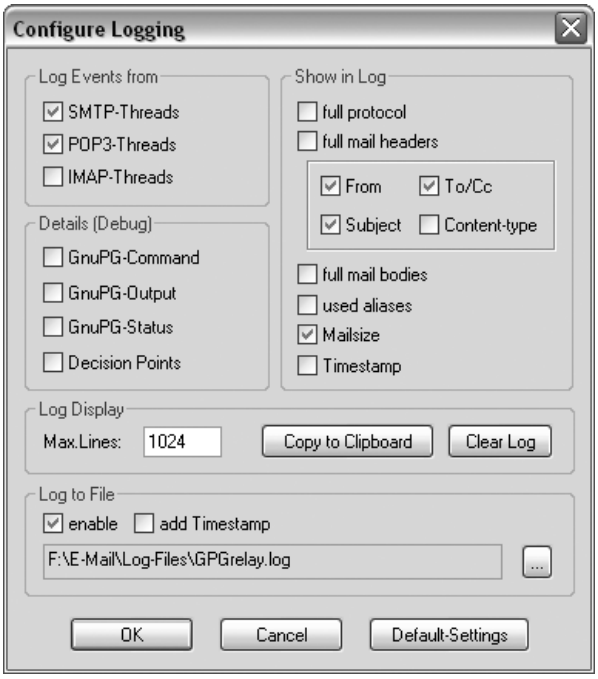
Wie bei „ausgewachsenen“ Verschlüsselungsgateways kann der Umgang mit ausgehenden E-Mail-Nachrichten auch bei GPGrelay vom E-Mail-Client aus gezielt gesteuert werden. Dazu lassen sich in den Profilen von GPGrelay Präfix-Kommandos für die Subject-Zeile ausgehender E-Mails einstellen, mit denen der Sender die Verschlüsselung, die unverschlüsselte Versendung oder das Signieren einer E-Mail auch abweichend vom vorgegebenen Profil erzwingen kann.

Voreingestellt sind die Präfixe „Pass:“ (durchlassen), „Sign:“ (signieren), „Encr:“ (verschlüsseln) und „EnSi:“ (für „Encrypt & Sign“). Diese Präfixe können für alle Profile einheitlich oder auch jeweils unterschiedlich gewählt werden.

Das Präfix wird vor Weiterversand der E-Mail an den E-Mail-Server auf Wunsch wieder aus der Subject-Zeile der E-Mail entfernt (siehe Abb.).

Ob eine E-Mail-Nachricht tatsächlich verschlüsselt versendet wurde, lässt sich auch durch Nutzung der Protokollierungsfunktion überprüfen. Diese lässt sich unter „Logging“ detailliert konfigurieren (Schaltfläche „Config“, siehe Abb.). Im Log-Fenster werden alle Log-Einträge seit dem letzten Start von GPGrelay angezeigt.

Abb.: Konfiguration der Log-Datei



Unter den generellen Konfigurationseinstellungen („Global Control“, s. o.) kann festgelegt werden, wie das Ergebnis einer Signaturprüfung oder der Entschlüsselung einer zugestellten Nachricht dokumentiert werden soll. Alternativen sind eine mehrteilige Nachricht mit einer Status-Meldung und der Original-E-Mail als Anhang oder eine zusätzliche Status-Zeile im Kopf der E-Mail:

```
X-GPGrelay-Received:
from mein-mailserver.de
by GPGrelay (GPGrelay v0.959,
„Mein-Mailserver“) with POP3s
```

Zusatzfunktionen

GPGrelay bietet einige ergänzende Funktionen, die über einen Klick mit der rechten Maustaste auf das GPGrelay-Icon in der Taskleiste genutzt werden können:

- den Import von PGP-Schlüsseln direkt aus dem Zwischenspeicher (Clipboard),
- die Verschlüsselung und Entschlüsselung des Clipboard-Inhalts,
- das Management von UserIDs zu einem bestimmten Schlüssel und
- die Erzeugung von Schlüsselpaaren.

Vor- und Nachteile

GPGrelay macht die Verschlüsselung von Nachrichten für den Benutzer vollständig transparent – sie läuft automatisch im Hintergrund. Lediglich für die Entschlüsselung und das Signieren von Nachrichten öffnet sich ein Fenster für die Eingabe der passenden Passphrase. Das macht die Lösung sehr bequem; wer viele Kontakte hat, mit denen er verschlüsselt kommuniziert, wird GPGrelay zu schätzen wissen.

Je nach Perspektive ist dieser Vorteil jedoch auch ein gewichtiger Nachteil, denn die vollständige Transparenz der Abläufe erschwert es in der Praxis, einen Konfigurationsfehler zu bemerken wie z. B. den unverschlüsselten Versand einer Nachricht aufgrund einer irrtümlichen Zuordnung des Empfängerschlüssels zum falschen Profil.

Für größere Unternehmen ist die Lösung zudem wenig geeignet, weil das Fehlen einer zentralen Konfigurationskonsole kundige Nutzer für die Erstkonfiguration erfordert. Auch die fehlende S/MIME-Fähigkeit beschränkt die Einsatzmöglichkeiten erheblich.

Stabilität, Durchdachtheit und umfangreiche Konfigurationsmöglichkeiten machen GPGrelay jedoch zu einem sehr leistungsfähigen und professionellen Verschlüsselungstool für kleinere Unternehmen und Gruppen.