Mail encryption
Desktop

Anwenderdokumentation

Table of Contents

1 Einleitung

1.1 Einführung

Die Verschlüsselung von Daten ist die Anwendung eines Algorithmus, der die Daten derart unleserlich macht, dass nur die Personen, die im Besitz des entsprechenden Schlüssels sind, diese wieder lesbar herstellen können. Verschlüsselte Daten sind damit geschützt vor dem Ausspionieren durch unbefugte Dritte sowie der Veränderung auf dem Transportweg von Sender zu Empfänger.

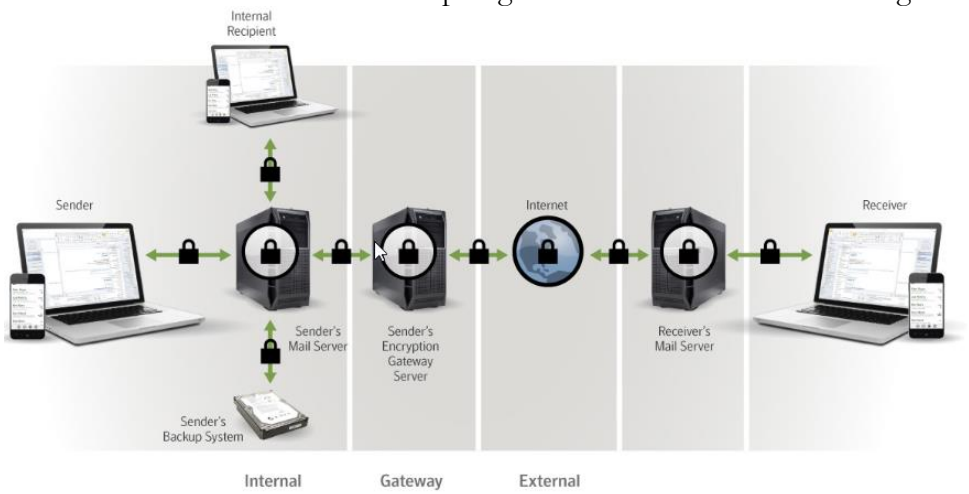
Das von arvato IT support eingesetzte System bietet verschiedene Verschlüsselungsfunktionen:

- Verschlüsselung und Signieren von Emails und Dateien
- Verschlüsselung ganzer Festplatten
- Verschlüsselung von Ordnern auf Serverlaufwerken

Dabei werden standardisierte Algorithmen und Protokolle eingesetzt, die einen Informationsaustausch auch mit externen Anwendern und Unternehmen ermöglichen.

1.2 Funktionsprinzip

Als zu verschlüsseln markierte Nachrichten werden am Desktop verschlüsselt bzw. entschlüsselt und liegen entsprechend gekennzeichnet im Postfach des Benutzers.
E-Mails an interne und externe Empfänger werden verschlüsselt übertragen und gespeichert.



1.3 Verschlüsselung vs. Signatur

Verschlüsselung: Die Nachricht ist nur vom gewünschten Empfänger zu lesen.

Signatur: Die Nachricht wird gegen Veränderungen und Fälschung geschützt.

2 Key Features

- Ende-zu-Ende-Verschlüsselung basierend auf den **Standards** PGP und S/MIME
- Nahtlose Integration in Clients wie Outlook, Lotus Notes, Thunderbird
- automatisiertes und zentrales Schlüsselmanagement
- Verschlüsselung auch an ungesicherte Empfänger möglich (-> Webmessenger)

3 Systemvoraussetzungen

Voraussetzung für den Einsatz von „Mail encryption“ ist ein PC oder Laptop mit Microsoft Windows oder Apple Mac OS Betriebssystem.

4 Schlüssel

Für jeden Anwender wird auf dem zentralen Server ein eindeutiges Schlüsselpaar erzeugt:

Ein Schlüssel, der sogenannte private Schlüssel, wird nur dem Anwender zur Verfügung gestellt und ist von diesem mit einer frei wählbaren *Passphrase* (= Kennwort) zu schützen. Diese *Passphrase* ist jeweils nur einmal pro Anmeldesitzung einzugeben und bleibt dann für den Zeitraum der Anmeldung am PC gespeichert. Im Normalfall sollte diese Passphrase nicht geändert werden.

Der zweite Schlüssel, der öffentliche Schlüssel, wird vom Server in einem Verzeichnis eingetragen und kann von allen anderen Anwendern, auch externen, dort abgerufen werden. Dieser Schlüssel wird von Absendern zum Verschlüsseln von Nachrichten verwendet, die dann nur der private Schlüssel des Empfängers wieder entschlüsseln kann.

4.1 Sekretariatszugriff

Ist ein Zugriff auf die verschlüsselten Daten eines Anwenders durch das Sekretariat (oder einer anderen vertrauenswürdigen Person) notwendig, so muss dem Sekretariat der private Schlüssel des Anwenders übergeben (kopiert) und mit der Passphrase des Anwenders im Sekretariat geschützt werden.

Anmerkung: Ein Signieren von Emails mit dem Schlüssel eines anderen Anwenders ist nicht möglich, da es dem Signaturgesetz (ESiG) widerspricht.

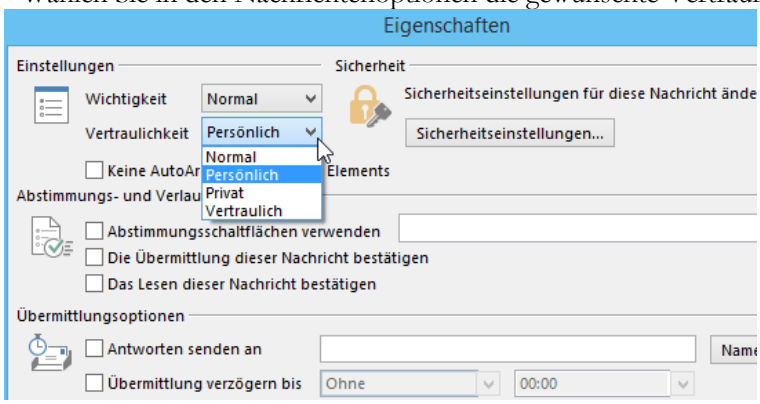
5 Email-Verschlüsselung aus der Perspektive des Absenders

Die Verschlüsselung von Emails ist die Grundfunktion von „Mail encryption“. Die Verschlüsselung einer Email kann vom Anwender durch einen der folgenden Schritte aktiviert werden.
Um eine E-Mail zu signieren bzw. zu verschlüsseln, gibt es folgende Möglichkeiten:

5.1 Vertraulichkeitsoption in Microsoft Outlook

- **Persönlich:** Nachricht wird signiert.
- **Vertraulich:** Nachricht wird signiert und verschlüsselt.

- Erstellen Sie eine neue Nachricht und klicken Sie auf „Optionen“.
- Wählen Sie in den Nachrichtenoptionen die gewünschte Vertraulichkeitsstufe.



5.2 Schlüsselwort in der Betreffzeile

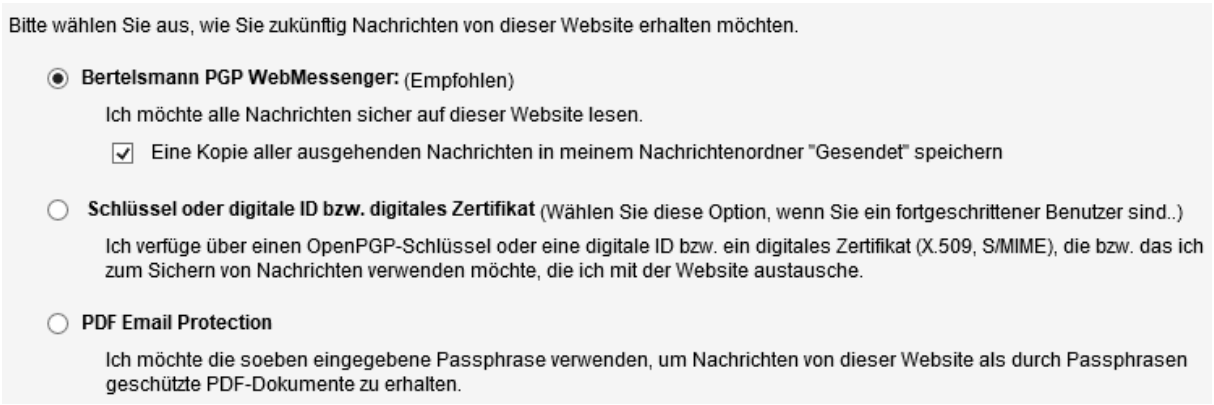
- Die Nachricht wird **signiert**, wenn eines der folgenden Schlüsselwörter bzw. Zeichenketten an beliebiger Stelle in der Betreffzeile auftaucht:
  i. **sign:**
  ii. **[sign]**
- Die Nachricht wird **signiert und verschlüsselt**, wenn eines der folgenden Schlüsselwörter bzw. Zeichenketten an beliebiger Stelle in der Betreffzeile auftaucht:
  i. **pgp**
  ii. **[sign encrypt]**

- Die Nachricht wird **verschlüsselt**, wenn eines der folgenden Schlüsselwörter bzw. Zeichenketten an beliebiger Stelle in der Betreffzeile auftaucht:
  i. **[encrypt]**

6 Email-Verschlüsselung aus der Perspektive des Empfängers

Zunächst versucht das Secure E-Mail Gateway mit verschiedenen Methoden (Key-Cache, PGP Global Directory, Key-Suche bei keys.<zieldomain> und anderen Keyservern) einen Schlüssel/Zertifikat des externen Empfängers zu finden. Wenn ein gültiger Schlüssel oder ein Zertifikat gefunden wurde, wird die Mail verschlüsselt an den externen Empfänger gesendet.

Kann kein Schlüsselmaterial gefunden werden, erhält der externe Empfänger zunächst eine Benachrichtigung über den Erhalt einer verschlüsselten Nachricht. Im selben Moment erhält der Absender ein Initial-Passwort für den externen Empfänger, sofern für den externen Empfänger noch kein PGP-Webmessenger existiert.
Dieses Passwort muss der Absender dem Empfänger wenn möglich persönlich oder telefonisch mitteilen. Mit diesem Passwort kann der externe Empfänger den PGP WebMessenger einmalig öffnen und sich ein eigenes Kennwort vergeben. Nach der Eingabe eines neuen Passwortes muss sich der externe Empfänger für eine der unten genannten Methoden entscheiden:



6.1 „Mail encryption“ WebMessenger

Wird eine Email verschlüsselt an einen Empfänger verschickt und der zentrale Server kann keinen Schlüssel für diesen Empfänger finden, so wird die Nachricht über den sogenannten *WebMessenger* zur Verfügung gestellt. Der Absender der Nachricht bekommt dazu ein Zugangskennwort vom zentralen Server geschickt sollte es sich um die erste Kommunikation eines „Mail encryption“-Benutzers mit diesem externen Kontakt handeln. Dieses Kennwort sollte dem Empfänger über eine andere Methode z.B. telefonisch übermittlet werden. Der Empfänger bekommt zeitgleich vom zentralen Server eine unverschlüsselte Nachricht mit dem Internet-Link zum „Mail encryption“ WebMessenger zugestellt.

Nachdem sich der Empfänger mit seinem Zugangskennwort am *WebMessenger* angemeldet hat, kann er die verschlüsselte Nachricht über eine SSL-verschlüsselte Internetverbindung lesen.

Schlüssel oder digitale ID
Er hat darüber hinaus die Möglichkeit, dem System mitzuteilen, ob er über eine eigene Verschlüsselungslösung verfügt. Ist dies der Fall, kann er seinen öffentlichen Schlüssel hochladen. Der zentrale Server speichert diesen Schlüssel und wird ab diesem Zeitpunkt verschlüsselte Emails direkt in das Postfach des Empfängers zustellen.

PDF Messenger
Sofern der Empfänger den kostenlosen Adobe Acrobat Reader installiert hat, kann er sich mit dieser Option alle Nachrichten incl. Anhänge als verschlüsseltes PDF-Dokument senden lassen, welches mit dem bei der Registrierung vergebenen Kennwort zu öffnen ist.

7 Festplattenverschlüsselung

Bei Diebstahl oder Verlust von Laptops sind mittels der Verschlüsselung der kompletten Festplatte die darauf gespeicherten Daten gegen unbefugten Zugriff geschützt. Der Anwender wählt dazu eine weitere *Passphrase* aus, die beim Systemstart einzugeben ist und den Start des Betriebssystems ermöglicht. Diese *Passphrase* sollte ergänzt werden durch ein zweites, dem PC-Support generell bekanntes, Kennwort.

8 PGPZip

Die Funktion *PGPZip* ermöglicht das Erstellen einer verschlüsselten oder signierten ZIP-Datei. Damit ist die Übertragung von verschlüsselten Daten auf anderen Medien als Email (CD/DVD, etc.) möglich.

9 Fileserver-Verschlüsselung

Mittels der Funktion *NetShare* kann ein beliebiges Verzeichnis auf Serverlaufwerken verschlüsselt werden. Damit ist der Zugriff nur noch für einen ausgewählten Anwenderkreis möglich. Administratoren haben zwar technischen Zugriff auf die Dateien (z.B. um diese zu sichern und Backups zu erstellen), können die Inhalte aber nicht mehr einsehen.

10 Download Client

Die aktuell provisionierte Client-Version ist über die folgenden Links verfügbar.

Evtl. wird Ihnen aber auch über den UHD per Software-Depot dieses Software-Paket zur Verfügung gestellt, sollten Sie über keine Admin-Rechte auf Ihrem Endgerät verfügen.

- Windows 64bit:
  https://secure.servicemail24.de/~pgp/PGPDesktop64_de-DE.msi
  https://secure.servicemail24.de/~pgp/PGPDesktop64_en-US.msi

- Windows 32bit:
  https://secure.servicemail24.de/~pgp/PGPDesktop_de-DE.msi
  https://secure.servicemail24.de/~pgp/PGPDesktop_en-US.msi

- OSX:
  https://secure.servicemail24.de/~pgp/PGPDesktop.tar.gz