Mail encryption Gateway

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.

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 Gateway verschlüsselt bzw. entschlüsselt und entsprechend gekennzeichnet im Postfach des Benutzers abgelegt. Mail an interne Empfänger wird unverschlüsselt gesendet.

1.3 Verschlüsselung vs. Signatur

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

Signatur: Die Nachricht wird gegen Veränderungen und Fälschung geschützt.

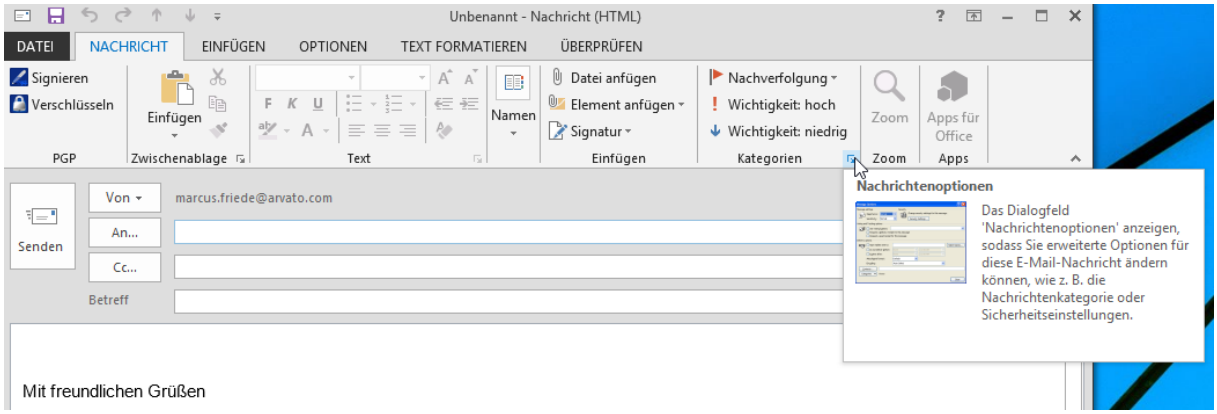
2 Aus der Perspektive des Absenders

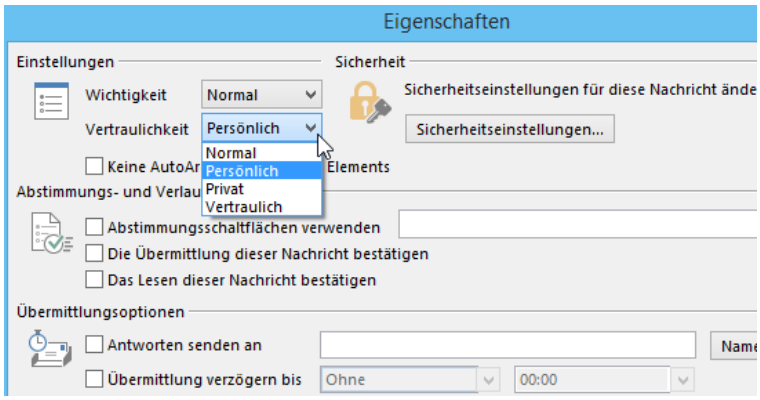
2.1 Eine verschlüsselte und/oder signierte E-Mail versenden

Um eine E-Mail zu signieren bzw. zu verschlüsseln, gibt es folgende Möglichkeiten:

1. Vertraulichkeitsoption in Microsoft Outlook
    a. **Persönlich:** Nachricht wird signiert.
    b. **Vertraulich:** Nachricht wird signiert und verschlüsselt.

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





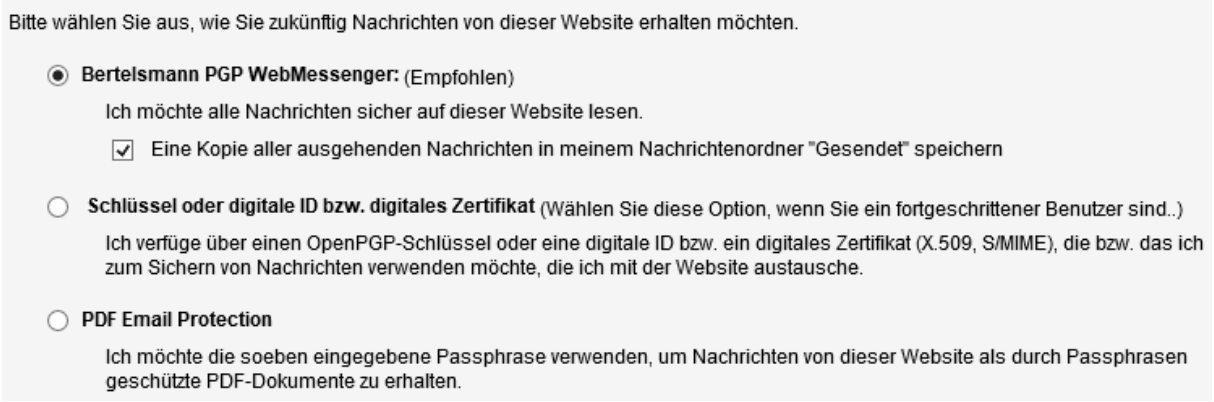
2. Schlüsselwort in der Betreffzeile
    a. Die Nachricht wird signiert, wenn eines der folgenden Schlüsselwörter an beliebiger Stelle in der Betreffzeile auftaucht:
        i. **sign:**
        ii. **[sign]**
    b. Die Nachricht wird signiert und verschlüsselt, wenn eines der folgenden Schlüsselwörter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

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

3 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:



3.1 „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.