

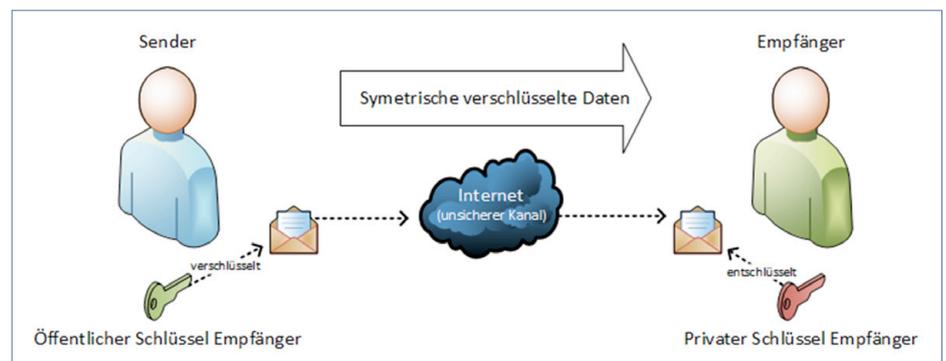
E-Mail-Verschlüsselung und Methoden zur sicheren Mail-Kommunikation mit der R+V Betriebskrankenkasse

Einleitung

Diese Kurzanleitung wendet sich an Mitarbeiter in der IT von Kunden und Partnern der R+V Betriebskrankenkasse. Es werden technische Möglichkeiten aufgelistet, nach welchen Verfahren eine beiderseitige verschlüsselte E-Mail-Kommunikation ermöglicht werden kann

Hybride Verschlüsselung

Das Prinzip der hybriden Verschlüsselung basiert auf einem privaten und öffentlichen Schlüssel. Um jemandem eine verschlüsselte E-Mail zu senden werden der öffentliche Schlüssel des Empfängers sowie der eigene private Schlüssel benötigt.



Mögliche Verfahren

» S/MIME

Das S/MIME-Verfahren basiert auf dem Prinzip der hybriden Verschlüsselung. Dafür werden X.509 Zertifikate benötigt. Das Mailgateway der R+V BKK signiert jede (auch unverschlüsselte) ausgehende E-Mail automatisch. Diese Signierung enthält den öffentlichen Schlüssel und wird in der Regel als Dateianhang mit den Namen „smime.p7s“ ersichtlich.

Bei allen eingehenden E-Mails wird geprüft ob die E-Mail signiert wurde und damit ein öffentlicher S/MIME Schlüssel angehängt ist. Falls dies der Fall ist, wird geprüft ob der Schlüssel von einer vertrauten Zertifizierungsstelle ausgestellt ist. Ist dies erfolgreich, wird der Schlüssel auf dem Mailgateway gespeichert und der Absenderadresse zugeordnet.

Bei jeder ausgehenden E-Mail wird geprüft ob für den Empfänger ein öffentlicher S/MIME Schlüssel auf dem Mailgateway vorliegt. Ist dies der Fall wird die E-Mail automatisch per S/MIME verschlüsselt gesendet.

Hinweis:

Jede verschlüsselte E-Mail wird seitens der R+V BKK im Namen des Absenders **info@ruv-bkk.de** verschlüsselt. Dies kann ggf. beim Empfänger in der E-Mail-Applikation, wie z. B. Outlook, zu Problemen führen.

☎ 0611 99909-0

Weitere Informationen im Internet
www.ruv-bkk.de
Fan werden auf Facebook!
www.facebook.com/ruvbkk





© Fotolia – MH

» Zertifizierungsstellen

Bei S/MIME wird das verwendete Zertifikat (enthält den privaten bzw. öffentlichen Schlüssel) von einer Zertifizierungsstelle ausgestellt. Dies kann entweder eine private oder eine öffentliche Zertifizierungsstelle sein. Bei öffentlichen Zertifizierungsstellen ist in der Regel keine Anpassung notwendig, da diese in den meisten Systemen (Windows, Linux, Android, iOS) bereits als vertraute Stammzertifizierungsstelle hinterlegt ist. Bei eigenen (privaten) Zertifizierungsstellen müssen diese bei der Gegenstelle händisch als vertraute Stammzertifizierungsstelle hinterlegt werden.

Die R+V BKK verwendet ein Zertifikat von einer öffentlichen Zertifizierungsstelle (GlobalSign).

Bitte stellen Sie sicher, dass dies auch in Ihren Systemen der Fall ist. Sie finden die von uns verwendeten Zertifikate zum Überprüfen und Importieren unter:
<https://www.ruv-bkk.de/zertifikate>

Wenn Sie Ihre Zertifikate von einer eigenen Zertifizierungsstelle ausstellen lassen, senden Sie uns bitte Ihr Stammzertifikat und die ggf. notwendigen Zwischenzertifikate an: **EMailVerschluesselung@ruv-bkk.de**

Zusammenfassung

1. Wenn Sie eine eigene Zertifizierungsstelle verwenden, senden Sie uns Ihr Stammzertifikat.
2. Hängen Sie einfach ihren öffentlichen Schlüssel an E-Mails an die R+V BKK an. Wenn dies passiert ist, erhalten Sie automatisch verschlüsselte Nachrichten von uns.
Wenn Sie ihr Zertifikat erneuern, hängen sie einfach den aktualisierten öffentlichen Schlüssel an. Unser Mailgateway aktualisiert dies auf unserer Seite automatisch.
3. Prüfen Sie ob Ihr System dem von uns verwendete Schlüssel bzw. Zertifikat vertraut. Importieren Sie ggf. die oben beschriebenen Stammzertifizierungsstellen

» PGP

Das PGP-Verfahren basiert ebenfalls auf dem Prinzip der hybriden Verschlüsselung. Allerdings ist es aufgrund von anderen Schlüsselformaten nicht mit S/MIME kompatibel. Der Unterschied liegt daran dass bei PGP die Schlüssel nicht von einer Zertifizierungsstelle ausgestellt und überprüft werden.

Das bevorzugte Verfahren seitens der R+V BKK ist die S/MIME Verschlüsselung. Daher wird aktuell der öffentliche PGP Schlüssel von uns nicht automatisch angehängt. Sollten Sie die PGP Verschlüsselung wünschen, können wir dies für Ihre Domain aktivieren.

Bei allen eingehenden E-Mails wird geprüft ob ein öffentlicher PGP Schlüssel angehängt ist. Falls dies der Fall ist, wird der Schlüssel auf dem Mailgateway gespeichert. Da bei PGP die Echtheit nicht über eine dritte Partei (Zertifizierungsstelle) validiert werden kann, müssen wir die Schlüssel händisch freigeben. Bitte senden Sie uns dazu eine E-Mail an:

EMailVerschluesselung@ruv-bkk.de

Bei jeder ausgehenden E-Mail wird geprüft ob für den Empfänger ein öffentlicher PGP Schlüssel auf dem Mailgateway vorliegt. Ist dies der Fall wird die E-Mail automatisch PGP verschlüsselt gesendet.

 **0611 99909-0**

Weitere Informationen im Internet
www.ruv-bkk.de
Fan werden auf Facebook!
www.facebook.com/ruvbkk 



© Fotolia – MH

Zusammenfassung

1. Wenn Sie PGP für Ihre Domain oder E-Mail Adresse verwenden möchten, hängen Sie uns einfach bei jeder E-Mail Ihren öffentlichen PGP Schlüssel an. Senden Sie uns eine E-Mail an **EMailVerschluesselung@ruv-bkk.de** mit dem Wunsch PGP für Sie zu aktivieren. Wir senden Ihnen anschließend bei jeder E-Mail unseren öffentlichen Schlüssel im Anhang mit.

» PDF-Verschlüsselung

Sollte keine Verschlüsselung über S/MIME oder PGP möglich sein, wird als Notlösung die PDF-Verschlüsselung verwendet.

In diesem Fall wird der eigentliche Inhalt der von uns versendeten E-Mail durch unser Mailgateway in ein passwortverschlüsseltes PDF Dokument umgewandelt. Anschließend wird geprüft ob der Empfänger ein Passwort auf unserem Mail-Gateway hinterlegt hat. Wenn ja, wird die E-Mail automatisch mit dem verschlüsselten PDF-Anhang versendet. Wenn nicht, wird der Empfänger per E-Mail automatisch informiert. Dort ist beschrieben wie der Empfänger sich auf dem Mailgateway ein Kennwort hinterlegen kann. Das Kennwort wird verwendet um damit das verschlüsselte PDF zu öffnen. Ist dies getan wird die zuvor angehaltene E-Mail dem Empfänger mit dem verschlüsselten PDF zugestellt.

 **0611 99909-0**

Weitere Informationen im Internet
www.ruv-bkk.de
Fan werden auf Facebook!
www.facebook.com/ruvbkk 