Debeka Versichern und Bausparen

Anleitung zur E-Mail-Verschlüsselung für Kommunikationspartner der Debeka

Stand: 31. Mai 2017 (Version 1.02)

Kontakt / Fragen bitte per E-Mail an: securemail@debeka.de

Inhalt

1 Zusammenfassung

Die Debeka setzt ein E-Mail-Verschlüsselungs-Gateway ein, um vertrauliche E-Mails mit ihren Geschäftspartnern und öffentlichen Stellen verschlüsselt auszutauschen.

Dieses E-Mail-Verschlüsselungs-Gateway wird **nicht** für die E-Mail-Kommunikation mit Mitgliedern, Kunden bzw. Interessenten benutzt. Sollten Sie Fragen zu Versicherungs- oder Finanzierungsprodukten der Debeka haben, wenden Sie sich bitte an Ihren zuständigen Außendienst-Mitarbeiter bzw. nehmen Sie über die Ansprechpartner-Suche auf dem Internetauftritt der Debeka (http://www.debeka.de) Kontakt zu einem Ansprechpartner auf.

Das E-Mail-Verschlüsselungs-Gateway der Debeka unterstützt folgende Arten von verschlüsselter E-Mail-Kommunikation:

- S/MIME-basierte E-Mail-Verschlüsselung (Einzelpersonen bzw. Domänen)
- PGP- bzw. GPG-basierte E-Mail-Verschlüsselung (Einzelpersonen bzw. Domänen)

Nehmen Sie bitte Kontakt mit Ihrem IT-Service auf, um das für Sie am besten geeignete Verschlüsselungsverfahren auszuwählen und einrichten zu lassen.

Die Debeka präferiert die S/MIME-basierte E-Mail-Verschlüsselung mit kommerziellen S/MIME-Zertifikaten.

2 Unterstütze Verschlüsselungsverfahren

2.1 S/MIME-basierte E-Mail-Verschlüsselung (Einzelpersonen)

Voraussetzungen:

- Ihr E-Mail-Programm unterstützt S/MIME-basierte E-Mail-Verschlüsselung.
- Sie besitzen ein S/MIME-Zertifikat und den zugehörigen privaten Schlüssel.

Konsultieren Sie bitte die Online-Hilfe Ihres E-Mail-Programms bzw. die Herstellerseiten, um Informationen zur Verwaltung von S/MIME-Zertifikaten und zur Nutzung von S/MIME-Verschlüsselung zu erhalten.

Um per S/MIME verschlüsselte E-Mails empfangen oder signierte E-Mails senden zu können, benötigen Sie selbst ein S/MIME-Zertifikat und den zugehörigen privaten Schlüssel. Diese können von einem Zertifizierungsdiensteanbieter (Certificate Authority) bzw. Trustcenter bezogen werden.

Falls Ihr IT-Service eine eigene PKI-Infrastruktur betreibt, können diese Zertifikate ebenfalls verwendet werden. Senden Sie in diesem Fall bitte Ihre S/MIME Root CA mit Ihren Kontaktdaten an die E-Mail-Adresse securemail@debeka.de bzw. nennen Sie eine Internetadresse, unter der Ihre X.509 Root CA heruntergeladen werden kann. Ein Mitarbeiter der Debeka wird anschließend mit Ihnen bzw. Ihrem IT-Service Kontakt aufnehmen, um den Fingerprint des Zertifikates abzugleichen.

2.2 PGP/GPG-basierte Verschlüsselung (Einzelpersonen)

Voraussetzungen:

- Ihr E-Mail-Programm unterstützt PGP- bzw. GPG-basierte E-Mail-Verschlüsselung bzw. Sie benutzen ein Plugin für Ihr E-Mail-Programm oder ein Zusatzprogramm.
- Sie besitzen einen öffentlichen PGP-Schlüssel und den zugehörigen privaten Schlüssel.

PGP- bzw. GPG-Schlüssel können von Ihnen selbst bzw. von Ihrem IT-Service erstellt werden. Achten Sie bitte darauf, vor Ablauf Ihres PGP- bzw. GPG-Schlüssels ein neues Schlüsselpaar zu generieren bzw. anzufordern und der Debeka den neuen öffentlichen Schlüssel per signierter E-Mail zu übermitteln.

2.3 S/MIME- oder PGP/GPG-Domänenschlüssel

Falls Ihr IT-Service eine Gateway-basierte E-Mail-Verschlüsselung mit einem S/MIME oder PGP/GPG-Domänenzertifikat bzw. -schlüssel nutzt, können diese Zertifikate bzw. Schlüssel ebenfalls verwendet werden. Senden Sie in diesem Fall bitte Ihr S/MIME bzw. PGP/GPG-Domänenschlüssel mit Ihrem Kontaktdaten an die E-Mail-Adresse securemail@debeka.de bzw. nennen Sie eine Internetadresse, unter der ihr Domänenzertifikat bzw. -schlüssel heruntergeladen werden kann. Ein Mitarbeiter der Debeka wird anschließend mit Ihnen bzw. Ihrem IT-Service Kontakt aufnehmen, um den Fingerprint des Zertifikates bzw. Schlüssels abzugleichen. Des Weiteren wir Ihnen der Debeka IT-Service den Debeka-Domänenschlüssel (S/MIME oder PGP/GPG) zur Verfügung stellen.

2.4 SMTP-Transportverschlüsselung (TLS)

Auch bei der Verschlüsselung von E-Mails mit S/MIME und PGP/GPG werden die Metadaten jeder E-Mail unverschlüsselt zwischen den beteiligten E-Mail-Servern übertragen. Dazu gehören Absender, Empfänger, E-Mail-Betreff und weitere Metadaten jeder E-Mail.

Sofern der Mailserver der Gegenstelle TLS (Transport Layer Security) unterstützt, versenden und empfangen die E-Mail-Gateways der Debeka E-Mails standardmäßig transportverschlüsselt (opportunistic TLS). Wenn die Gegenstelle TLS nicht unterstützt, werden die E-Mail-Metadaten ohne Transportverschlüsselung übertragen.

In Einzelfällen ist die Konfiguration von erzwungener Transportverschlüsselung möglich (mandatory TLS), um zu verhindern, dass E-Mails ohne Transportverschlüsselung ausgetauscht werden. Sollten Sie Bedarf an mandatory TLS haben, wenden Sie sich bitte per E-Mail an securemail@debeka.de.

Für den Austausch von sensiblen bzw. personenbezogenen Daten per E-Mail setzt die Debeka weder opportunistic noch mandatory TLS ein, sondern eines der o.g. S/MIME oder PGP/GPG-Verfahren.

3 E-Mail-Austausch mit der Debeka

3.1 Woher bekomme ich das Zertifikat bzw. den Schlüssel meines Kontaktes bei der Debeka?

Dazu gibt es folgende Möglichkeiten (Tabelle 1):

Tabelle 1. Möglichkeiten zum Bezug der Zertifikate bzw. Schlüssel von Debeka-Mitarbeitern.

Verfahren	Erhalt des Schlüssels eines Debeka-Mitarbeiters
S/MIME (Einzelpersonen)	Möglichkeit 1: Bitten Sie Ihre Debeka-Kontaktperson Ihnen eine signierte E-Mail zuzuschicken. In den meisten Fällen wird Ihr E-Mail-Programm beim Empfang einer signierten E-Mail das S/MIME-Zertifikat bzw. den PGP/GPG-Schlüssel des Debeka Kontaktes automatisch importieren.
	Möglichkeit 2: Geben Sie die E-Mail-Adresse Ihres Kontaktes bei der Debeka in das Suchformular auf folgender Seite ein: https://www.globaltrustpoint.com. Diese Seite wird von der deutschen

	Firma Zertificon betrieben. Dort können Sie die gültigen S/MIME-Zertifikate von Debeka Mitarbeitern herunterladen und anschließend in Ihr E-Mail-Programm importieren.
S/MIME (Domänenschlüssel)	Fordern Sie das Debeka-Domänenzertifikat (S/MIME- oder PGP/GPG) bitte per E-Mail bei securemail@debeka.de an.
PGP/GPG (Domänenschlüssel)	

Wenden Sie sich bitte ggf. an Ihren IT-Service, um die Debeka-Zertifikate bzw. Schlüssel zu importieren.

Unter Umständen besitzt Ihre Debeka-Kontaktperson noch kein Zertifikat bzw. keinen Schlüssel. In diesem Fall muss Ihr Debeka-Kontakt zuvor Debeka-intern ein Zertifikat bzw. einen Schlüssel beantragen.

3.2 Ich habe von einem Debeka-Mitarbeiter eine E-Mail mit einem Link auf http://securemail.debeka.de bekommen

In diesem Fall hat ein Debeka-Mitarbeiter Ihnen eine vertrauliche E-Mail zugeschickt, ohne dass er ein S/MIME-Zertifikat bzw. einen PGP/GPG-Schlüssel von Ihnen hatte. Folgen Sie bitte den Anweisungen in der E-Mail, um die Nachricht auf dem WebMail-Portal der Debeka lesen zu können. Der Debeka-Mitarbeiter wird Ihnen per Telefon, Fax oder Brief ein Kennwort nennen, mit dem Sie sich auf dem WebMail-Portal registrieren und die E-Mail lesen können. Sie können die E-Mail dort auch beantworten.

Um zukünftig eine direkte Kommunikation per verschlüsselter E-Mail ohne Umweg über das WebMail-Portal zu ermöglichen, sollten Sie sich ein S/MIME-Zertifikat oder einen PGP-Schlüssel besorgen (siehe Abschnitt 2.1–2.3) und den zugehörigen öffentlichen Schlüssel per signierter E-Mail an eine ihrer Kontaktpersonen bei der Debeka schicken. Weil ihr öffentlicher Schlüssel zentral verwaltet wird, genügt es, wenn Sie ihn an eine Debeka-Kontaktperson schicken. Alle anderen Debeka-Mitarbeiter können ihren Schlüssel dann zur E-Mail-Verschlüsselung nutzen.