Office Standardization.
E-Mail Encryption Gateway.

Kurzinformation für externe Kommunikationspartner.

Erleben, was verbindet.

Kurzbeschreibung der Lösung.

Alle Mitarbeiter der Deutschen Telekom können mit Hilfe von TrustMail® E-Mails verschlüsseln und zu jeder beliebigen internen oder externen E-Mail-Adresse senden oder von dort eine verschlüsselte E-Mail empfangen und entschlüsseln. Verschlüsselte E-Mails können darüber hinaus von allen beteiligten Kommunikationspartnern weitergeleitet und verschlüsselt beantwortet werden.

Falls ein externer Kommunikationspartner noch nicht über die S/MIME- bzw. PGP-Technologie verfügt, um E-Mails zu ver- bzw. zu entschlüsseln, so werden ihm die verschlüsselten E-Mails in einer SSL-abgesicherten Webanwendung, die im Folgenden „WebMail“ genannt wird, zur Verfügung gestellt. Über die Zustellung einer verschlüsselten E-Mail wird der externe Kommunikationspartner durch eine automatisiert generierte Benachrichtigung per E-Mail informiert. Mit Hilfe von WebMail kann er nach erfolgreicher Registrierung und nachfolgender Authentifizierung alle ihm zugestellten verschlüsselten E-Mails lesen.

Bei Bedarf kann der externe Kommunikationspartner eine Weiterleitung der an ihn adressierten verschlüsselten E-Mails konfigurieren. Die weitergeleiteten E-Mails werden dabei inklusive Anhängen in verschlüsselte PDF-Dokumente konvertiert, die durch ein zuvor von ihm in WebMail spezifiziertes Passwort entschlüsselt werden können. Man spricht hier von einer sogenannten „PushedPDF“-Technologie.

Falls ein externer Kommunikationspartner bereits über eine Verschlüsselungstechnologie (PGP oder S/MIME) verfügt, so kann er sein Zertifikat bzw. seinen öffentlichen PGP-Schlüssel TrustMail® bekannt machen, damit diese zukünftig von TrustMail® verwendet werden können, um E-Mails basierend auf der entsprechenden Verschlüsselungstechnologie verschlüsseln und direkt zustellen zu können.

Die Verschlüsselung der E-Mail erfolgt dabei nahezu Ende-zu-Ende, d. h., die E-Mail wird bereits im Outlook-Client der Mitarbeiter der Deutschen Telekom verschlüsselt und gegebenenfalls durch den E-Mail Encryption Gateway in Abhängigkeit von den technologischen Gegebenheiten des externen E-Mail-Empfängers z. B. bei einer erforderlichen Umschlüsselung nach PGP umgeschlüsselt.

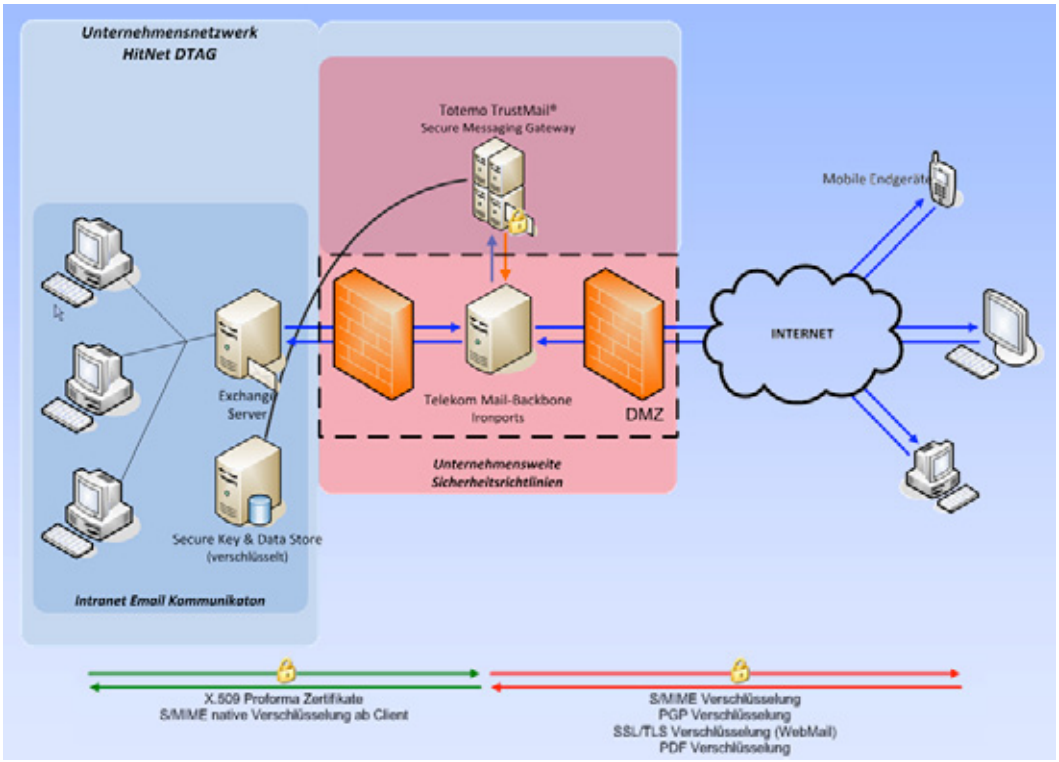

Abbildung 1: Ende-zu-Ende-Verschlüsselung von E-Mails

Alle Mitarbeiter der Deutschen Telekom können E-Mails signieren (mit und ohne Verschlüsselung) und zu jeder beliebigen internen oder externen E-Mail-Adresse senden oder signierte E-Mails von dort empfangen und eine eventuell angefügte digitale Signatur verifizieren.

Die Deutsche Telekom favorisiert die Verwendung von S/MIME für die Verschlüsselung und Signierung von E-Mails. Um externe Kommunikationspartner nicht zu verpflichten, von PGP auf S/MIME zu migrieren, kann TrustMail® ausgehende E-Mails nach PGP umschlüsseln bzw. eingehende PGP-verschlüsselte E-Mails nach S/MIME umschlüsseln.

Damit ist eine hochgradige Transparenz und Flexibilität sowohl auf interner als auch auf externer Kommunikationsseite gewährleistet.

Fall 1: S/MIME-Zertifikat oder PGP-Schlüssel vorhanden.

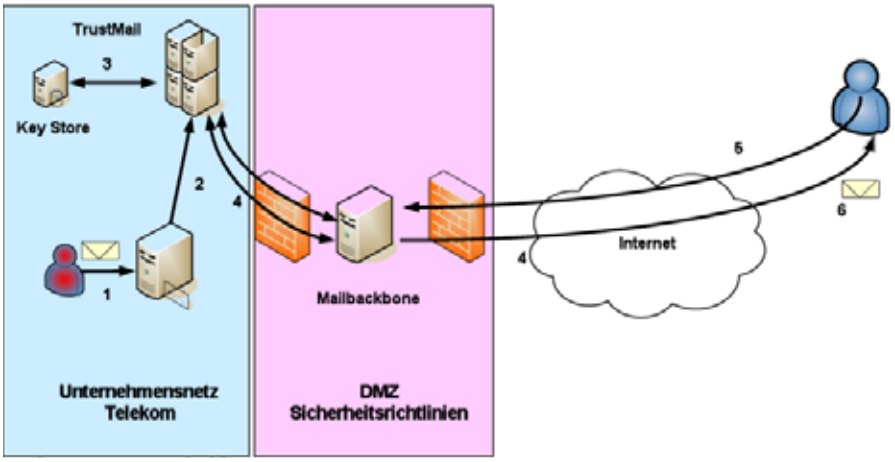

Abbildung 2: Mailfluss bei bereits verfügbarem S/MIME- oder PGP-Schlüssel für Verschlüsselung

1. Ein Mitarbeiter der Deutschen Telekom sendet eine (signierte) E-Mail, die verschlüsselt werden soll, an einen externen Kommunikationspartner.
2. Die E-Mail wird intern an TrustMail® geroutet.
3. TrustMail® prüft, ob der externe Kommunikationspartner bereits registriert ist und sein öffentlicher Schlüssel (S/MIME oder PGP) entsprechend verfügbar ist.
4. Wenn kein S/MIME-Zertifikat oder öffentlicher PGP-Schlüssel des externen Kommunikationspartners verfügbar ist oder über angebundene externe Verzeichnisdienste bzw. Key Server gefunden werden kann, wird die verschlüsselte E-Maill in TrustMail® zwischengespeichert und dem externen Kommunikationspartner eine Benachrichtigung zugesendet.
5. Falls der externe Kommunikationspartner bereits über ein S/MIME-Zertifikat für E-Mail-Verschlüsselung und -Signierung verfügt, antwortet er auf die o. a. Mail mit einer S/MIME-signierten E-Mail. Verwendet der externe Kommunikationspartner z. B. Microsoft Outlook, so ist dies einfach durch Aktivierung der entsprechenden Schaltfläche für Signatur möglich. Falls der externe Kommunikationspartner bereits PGP-Verschlüsselung im Einsatz hat, so antwortet er auf diese E-Mail und hängt dabei seinen öffentlichen PGP-Schlüssel als Attachment an.
6. TrustMail® überprüft das erhaltene Schlüsselmaterial auf Gültigkeit und speichert den öffentlichen Schlüssel (S/MIME oder PGP) in seinem Key Store.

Fall 2: Weder S/MIME-Zertifikat noch PGP-Schlüssel vorhanden.

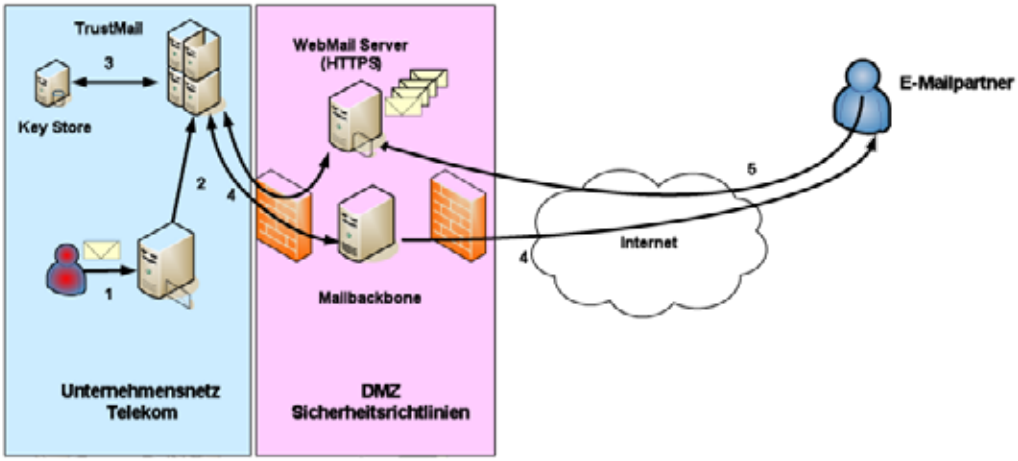

Abbildung 6: Mailfluss bei nicht vorhandenem S/MIME- oder PGP-Schlüssel und Verwendung von WebMail

1. Ein Mitarbeiter der Deutschen Telekom sendet eine (signierte) E-Mail, die durch TrustMail® verschlüsselt werden soll, an einen externen Kommunikationspartner.
2. Die E-Mail wird intern an TrustMail® geroutet.
3. TrustMail® prüft, ob der externe Kommunikationspartner bereits registriert ist und sein öffentlicher Schlüssel entsprechend verfügbar ist.
4. Wenn kein S/MIME-Zertifikat oder öffentlicher PGP-Schlüssel des externen Kommunikationspartners verfügbar ist oder über angebundene externe Verzeichnisdienste bzw. Key Server gefunden werden kann, wird die E-Mail in TrustMail® zwischengespeichert und dem externen Kommunikationspartner eine Benachrichtigung zugesendet.
5. Da der externe Kommunikationspartner noch kein eigenes S/MIME-Zertifikat oder PGP-Schlüsselpaar für E-Mail-Verschlüsselung bzw. -Signierung besitzt, bietet sich für ihn der Zugriff auf die verschlüsselte E-Mail per WebMail oder in Form einer direkten Zusendung einer verschlüsselten PDF-Datei per E-Mail an. Dazu registriert sich der externe Kommunikationspartner SSL-geschützt in WebMail mit Hilfe der in der Benachrichtigung angegebenen URL.

Office Standardization.
E-Mail Encryption Gateway.
Kurzinformation für externe Kommunikationspartner.
Stand: 12.01.2011

Herausgeber
Deutsche Telekom AG
Programm Office Standardization

Kontakt
Internet: http://os.telekom.de
E-Mail: trust@t-systems.com

Erleben, was verbindet.