Office Standardization.
E-Mail Encryption Gateway.

A Brief Guide for External Communication Partners.

Life is for sharing.

A Brief Description of the Solution.

All employees of Deutsche Telekom can use the E-Mail Encryption Gateway for either sending e-mails to any internal or external e-mail contacts they desire or for receiving and decrypting encrypted e-mails from those contacts. Encrypted e-mails can also be forwarded to all contacts involved and an encrypted reply can be sent.

If an external contact has no S/MIME or PGP technology for encrypting e-mails, the encrypted e-mails will be made available in an SSL-secure Web application, referred to as "WebMail" below. An automatically generated notification e-mail will inform the external contact that he/she has received an encrypted e-mail. Using WebMail, he/she can then log in and, after authentication, read all of the encrypted e-mails.

If required, the external contact can also configure the settings so that the encrypted e-mails are forwarded. The forwarded e-mails – including attachments – will be converted into encrypted PDF files that can later be decrypted using the password previously specified by him/her in the WebMail application. This is called "PushedPDF" technology.

If an external contact already has an encryption technology (PGP or S/MIME), he/she can inform the E-Mail Encryption Gateway of the appropriate certificate or public PGP key so that the E-Mail Encryption Gateway can use it to encrypt and send e-mails using the corresponding technology in the futue.

The encryption of the e-mails takes place on a nearly end-to-end basis, that is, the e-mails are already encrypted in the Outlook client of the Deutsche Telekom employee and possibly even re-encrypted by the E-Mail Encryption Gateway, depending on the technology used by the external recipient, for example when using the conversion required by PGP.

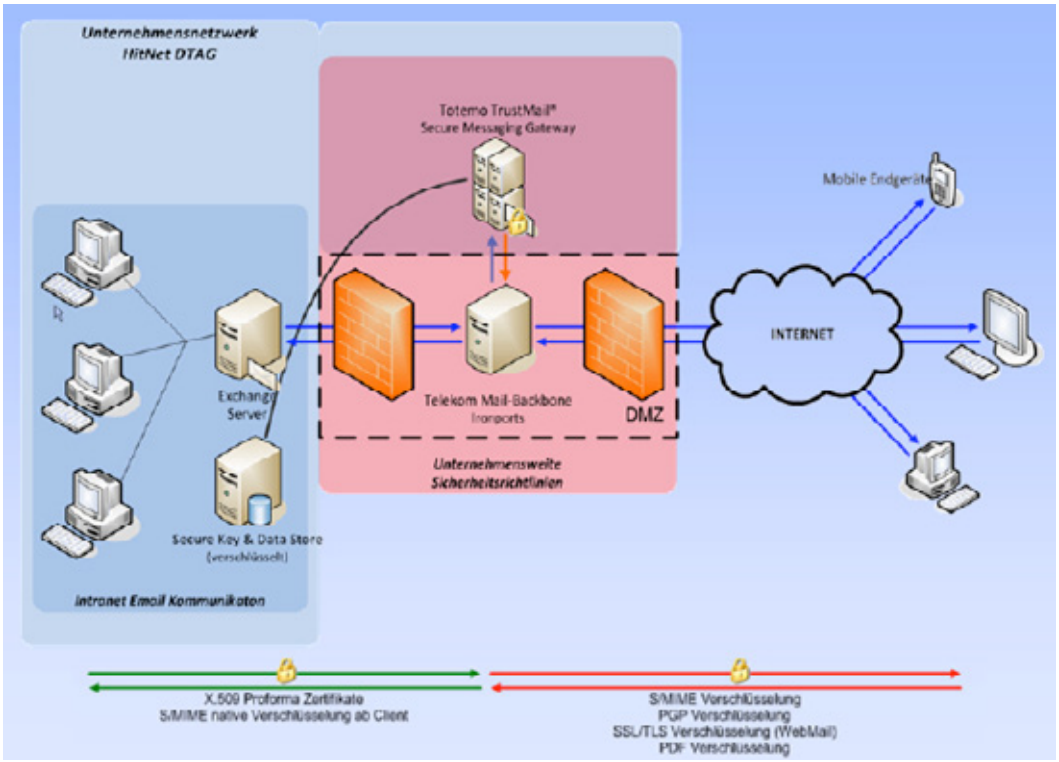

Figure 1: End-to-end encryption of e-mails

All Deutsche Telekom employees can add a signature to their e-mails (with or without encryption) and send them to any internal or external contacts, or they can receive e-mails with signatures from those contacts and even validate digital signatures.

Deutsche Telekom favors the use of S/MIME technology for the encryption and signature of e-mails. To avoid requiring external recipients to migrate from PGP to S/MIME, however, outgoing e-mails from the E-Mail Encryption Gateway can be PGP-encrypted and incoming e-mails can be converted from PGP to S/MIME.

This will ensure a high level of transparency and flexibility for both internal and external communications.

Case 1: S/MIME Certificate or PGP Key Available.

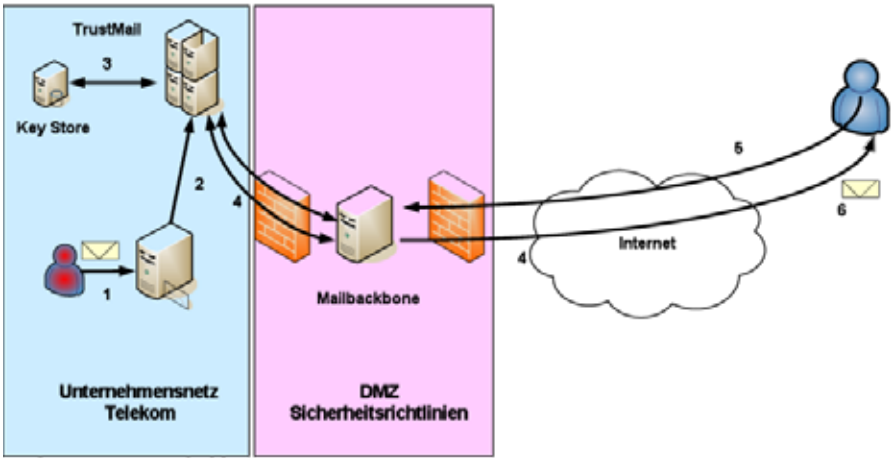

Figure 2: E-mail flow with existing S/MIME or PGP encryption keys

1. A Deutsche Telekom employee sends an external recipient a signed e-mail that is to be encrypted.
2. The e-mail is routed internally to the E-Mail Encryption Gateway.
3. The E-Mail Encryption Gateway verifies whether the external contact is already registered and whether his/her public key (S/MIME or PGP) is available.
4. If no S/MIME certificate or public PGP key is available for the external user, or it cannot be found via the integrated indexing services or key servers, the encrypted e-mail will be temporarily stored in E-Mail Encryption Gateway and the external user will be sent a notification e-mail in the following form.
5. If the recipient already has a S/MIME certificate he/she responds to the e-mail with a S/MIME-signed e-mail. This can be done by activating the “Sign”-Option in for example Microsoft Outlook. If the recipient uses the encryption technology PGP, he/she responds to the e-mail by sending a new e-mail with the public PGP key as an attachement.
6. The E-Mail Encryption Gateway verifies either the S/MIME certificate or the public PGP key as valid and stores the information in its key store.

Case 2: Neither S/MIME Certificate nor PGP Key Available.

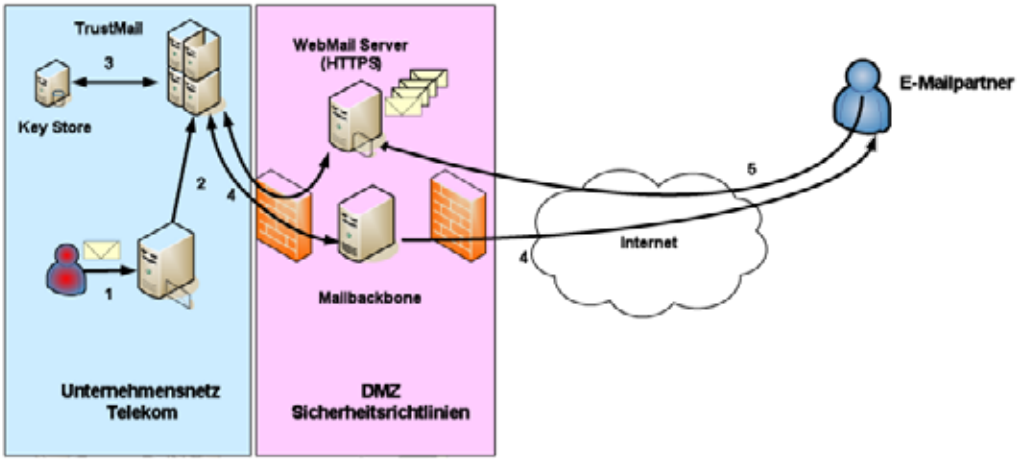

Figure 6: E-mail flow without an S/MIME or PGP key when using WebMail

1. A Deutsche Telekom employee sends an external recipient a (signed) e-mail that is to be encrypted by the E-Mail Encryption Gateway.
2. The e-mail is internally routed to the E-Mail Encryption Gateway.
3. The E-Mail Encryption Gateway verifies whether the external partner is already registered and whether his/her public key is available.
4. If no S/MIME certificate or public PGP key is available for the external contact or it cannot be found via the integrated indexing services or key servers, the encrypted e-mail will be temporarily stored in the E-Mail Encryption Gateway and the external contact will be sent a notification e-mail.
5. Since the external communication partner does not have a S/MIME certificate or a PGP key bundle, he/she can retrieve the encrypted e-mail by registering at WebMail with the information provided in the notification e-mail. This method allows the user to read the message in WebMail or to receive it as an encrypted PDF file.

Office Standardization.
E-Mail Encryption Gateway.
A Brief Guide for Communication Partners.
Version: 01/12/11

Author
Deutsche Telekom AG
Office Standardization program

Contact
Website: http://os.telekom.de
E-Mail: trust@t-systems.com

Life is for sharing.