Secure E-Mail Communication with Deutsche Telekom AG.

Things worth knowing about the E-Mail Encryption Gateway.

What is the E-Mail Encryption Gateway?

Deutsche Telekom AG securely exchanges confidential and encrypted e-mails with the help of the E-Mail Encryption Gateway (EEGW). As the security of e-mail communication does not depend on the communication partner's encryption technologies, the EEGW represents one of the most innovative secure messaging solutions.

Who is an "external" communications partner?

E-mail recipients are considered external communication partners if their e-mail account does not end on either *.telekom.de or *.t-systems.com.

Requirements for receiving encrypted e-mails from Deutsche Telekom.

To be able to receive encrypted e-mails from Deutsche Telekom employees, the external communication partner must be familar with the EEGW or made aware through a registration procedure. The procedure is automatically initiated the first time a Telkom employee sends an encrypted e-mail to the external communication partner.

First time delivery of encrypted e-mail.

If a Telekom employee sends an encrypted e-mail to an external communication partner for the first time, the recipient receives a message that an encrypted e-mail is queued for delivery. Depending on the type of encryption technology available at the recipient's end, the following options are available:

- **The recipient uses PGP encryption:**
  The external communication partner sends an e-mail containing his public PGP key to trust@t-systems.com.
- **The recipient uses S/MIME certificates:**
  The external communication partner sends a signed e-mail to trust@t-systems.com.
- **The recipient uses neither PGP encryption nor S/MIME certificates:**
  The external communication partner registers with the EEGW website by
  - Establishing a password and security question for accessing the website and
  - Selecting a delivery method – encrypted e-mails can be accessed via the website or delivered via e-mail with the encrypted mail sent as PDF-attachment.

Repeated delivery of encrypted e-mail.

In this case, the recipient is already familiar with the E-Mail Encryption Gateway.

- **The recipient uses PGP encryption or S/MIME certificates:**
  The encrypted e-mail is delivered directly.
- **No use of PGP encryption or S/MIME certificates at recipient's end:**
  Depending on the EEGW settings, the e-mail will either be delivered as an encrypted PDF attachment or is available for access at the website.

Further information on the E-Mail Encryption Gateway is available at **www.telesec.de/eegw**.
Questions and inquiries may also be addressed to **trust@t-systems.com**.

Life is for sharing.