E-Mail Encryption Gateway

Deutsche Telekom Security GmbH | Version 3.0 | 08.2022

What is the Email Encryption Gateway

This document describes the functions of the E-Mail Encryption Gateway (hereinafter referred to as EEGW), which are available to Deutsche Telekom's external communication partner to receive confidential e-mails securely. The EEGW offers the following options for sending and receiving encrypted e-mails:

- by means of a secure WebMail portal
- by means of an encrypted HTML file
- by means of an S/MIME certificate
- by means of a PGP key

What is the Email Encryption Gateway

Secure WebMail-Portal

The external recipient is informed about the delivery of an encrypted e-mail by means of an automatically generated notification by e-mail. With the help of a WebMail portal, the recipient can read all encrypted e-mails delivered to him after successful registration and subsequent authentication.

Encrypted HTML File

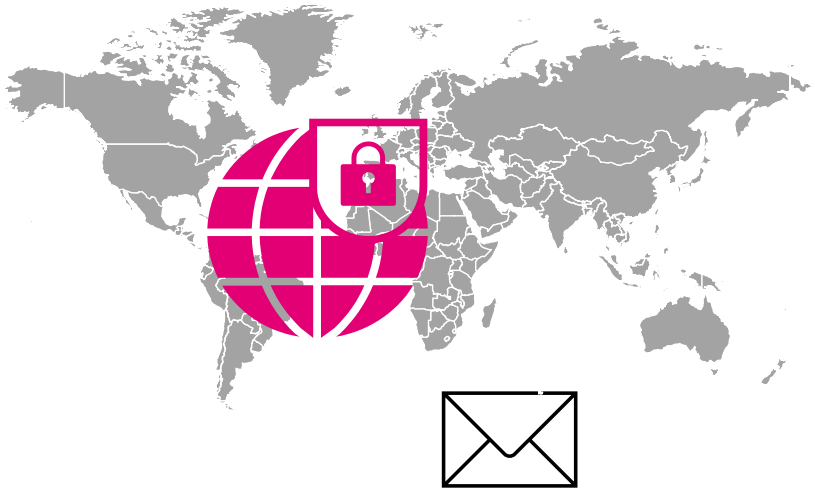
As an alternative to the WebMail portal, the external communication partner can configure the forwarding of the encrypted e-mails addressed to him. The forwarded e-mails, including attachments, are converted into an encrypted HTML document. The HTML document can be decrypted by a password previously specified by him in WebMail. This is referred to as a so-called "Registered Envelope" technology.

S/MIME Certificate or PGP Key

If an external recipient has S/MIME or PGP technology, he can also receive or send e-mails directly encrypted..

01
Use of the WebMail Portal.

The following describes how to register in the WebMail Portal for the first time and how to access delivered e-mails via the EEGW® WebMail interface as well as how to create and return encrypted e-mails

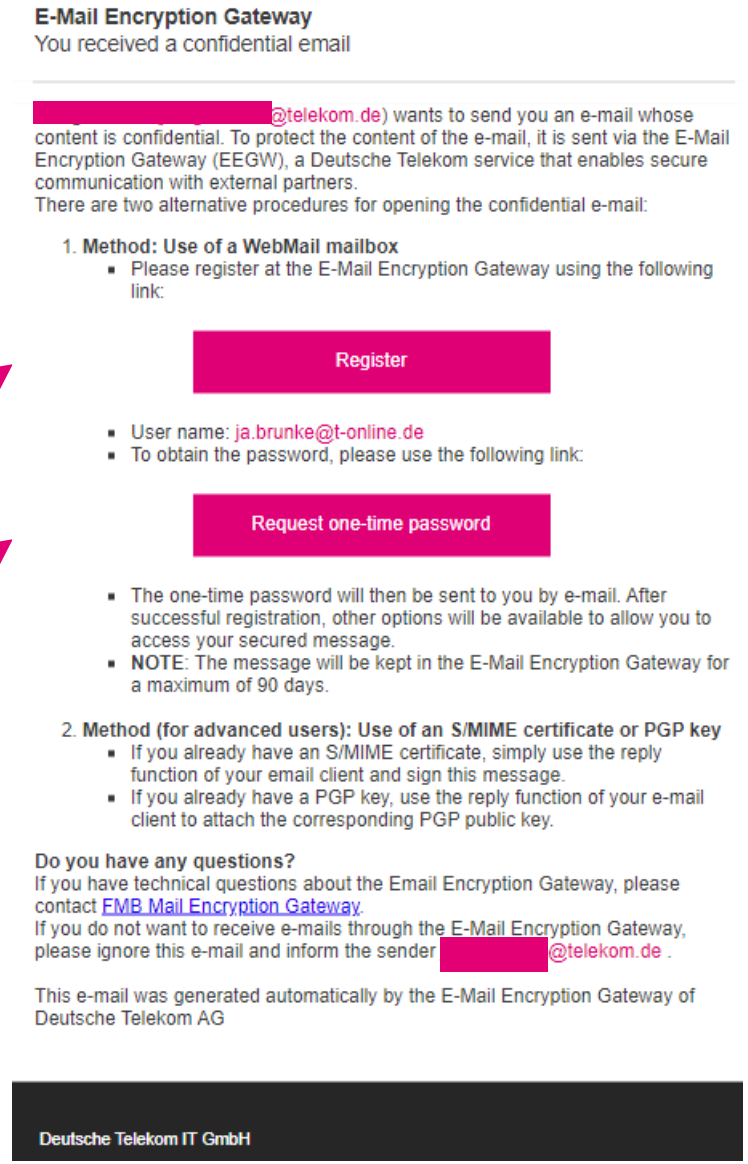


Use of the WebMail Portal

If an external recipient has not yet received an encrypted message from Deutsche Telekom and is therefore not registered on the EEGW, the original mail from an internal sender from the Telekom Group will be retained in the EEGW. Instead, the external recipient automatically receives the notification of the delivery of an encrypted e-mail shown next to it.

With the help of the "**Registrater**" button you get to the WebMail portal page.

Via "**Request one-time password**", the necessary password for the portal will be sent separately by e-mail.



E-Mail Encryption Gateway
You received a confidential email

[redacted]@telekom.de) wants to send you an e-mail whose content is confidential. To protect the content of the e-mail, it is sent via the E-Mail Encryption Gateway (EEGW), a Deutsche Telekom service that enables secure communication with external partners.
There are two alternative procedures for opening the confidential e-mail:

1. **Method: Use of a WebMail mailbox**
   - Please register at the E-Mail Encryption Gateway using the following link:

Register

   - User name: ja.brunke@t-online.de
   - To obtain the password, please use the following link:

Request one-time password

   - The one-time password will then be sent to you by e-mail. After successful registration, other options will be available to allow you to access your secured message.
   - **NOTE**: The message will be kept in the E-Mail Encryption Gateway for a maximum of 90 days.

2. **Method (for advanced users): Use of an S/MIME certificate or PGP key**
   - If you already have an S/MIME certificate, simply use the reply function of your email client and sign this message.
   - If you already have a PGP key, use the reply function of your e-mail client to attach the corresponding PGP public key.

Do you have any questions?
If you have technical questions about the Email Encryption Gateway, please contact FMB Mail Encryption Gateway.
If you do not want to receive e-mails through the E-Mail Encryption Gateway, please ignore this e-mail and inform the sender [redacted]@telekom.de .

This e-mail was generated automatically by the E-Mail Encryption Gateway of Deutsche Telekom AG

Deutsche Telekom IT GmbH

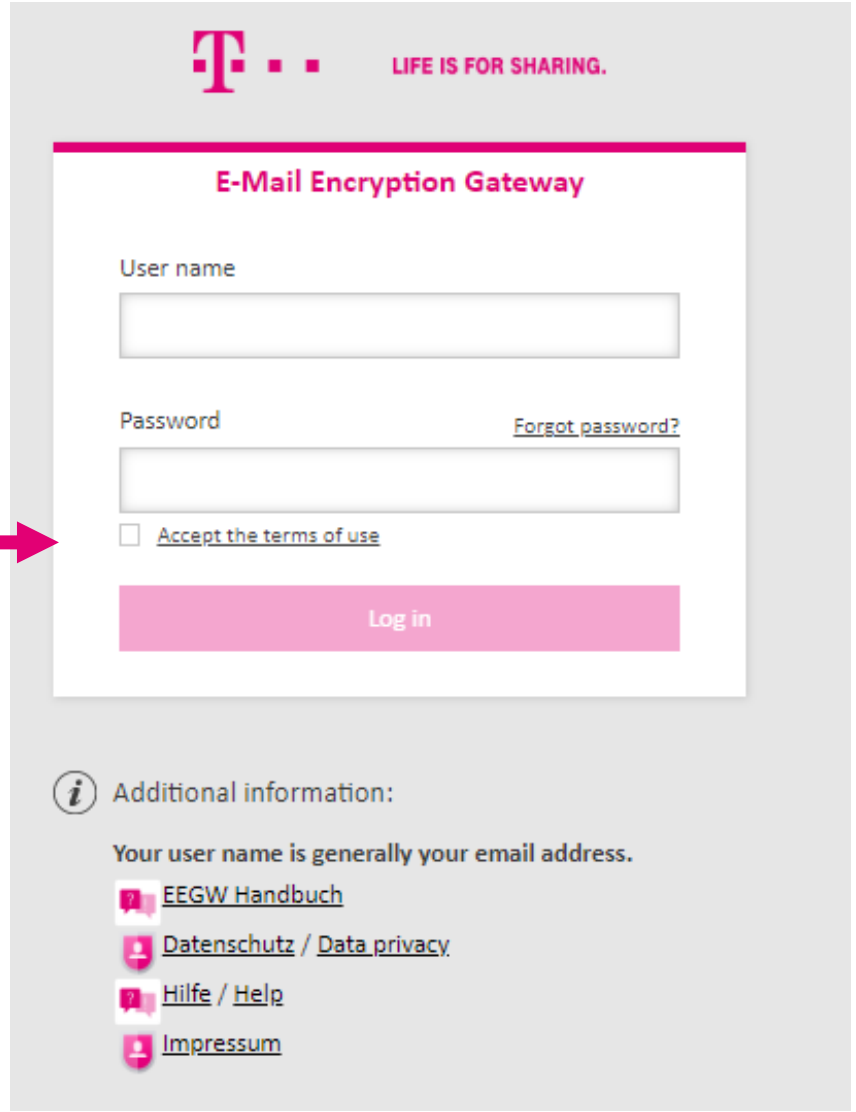
Use of the WebMail Portal

The WebMail portal page can also be accessed via the following URL:

(https://www.mysafemail.telekom.de).

To log in to the WebMail portal, the user name (this is the e-mail address of the recipient) and the password are required.

Please note, the "**Log in**" button will only become active once the “**terms of use**” have been accepted.



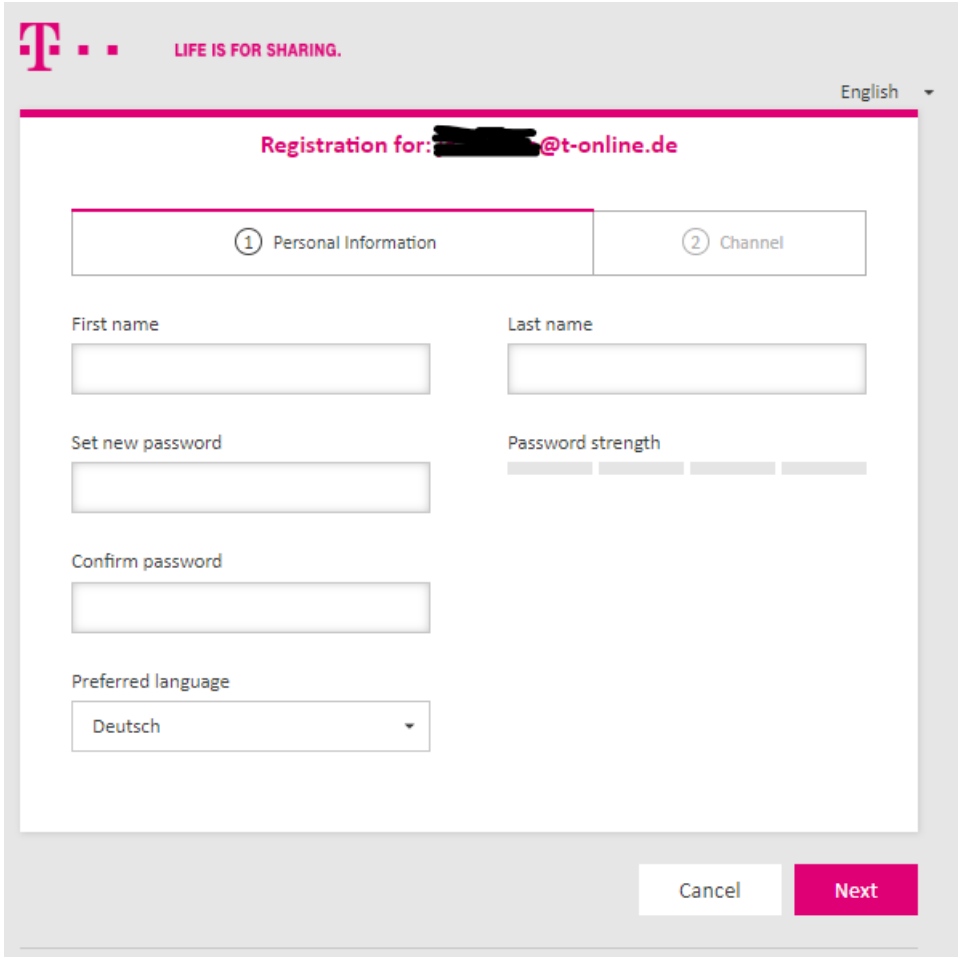
Use of the WebMail Portal

After successful registration, the actual registration takes place and with your name, the assignment of your own secure password and the selection of the preferred language.

On the next page you have to decide whether you want to receive encrypted mails :

a) Would you like to receive it in the WebMail portal

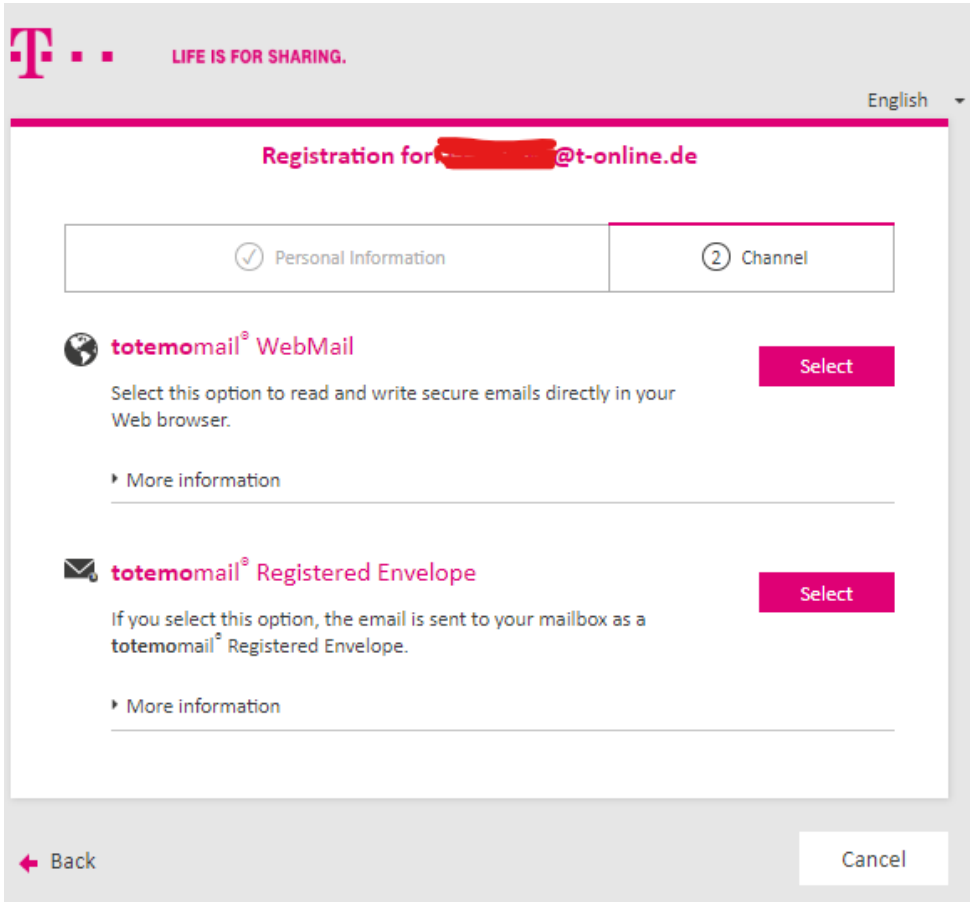
b) Would like to receive it directly as an encrypted HTML document (Registered Envelope)



Use of the WebMail Portal

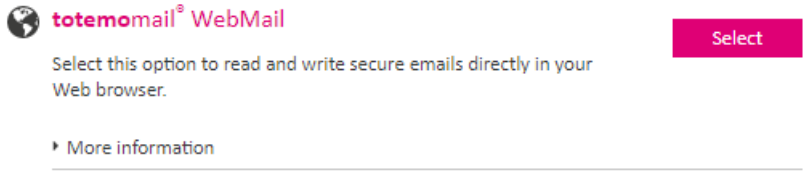
The "**WebMail**" option means that the encrypted e-mails, including any attachments, are not delivered directly to the external communication partner, but can be read via the WebMail portal (comparable to WebMail applications such as GMX or Web.de).

The "**Registered Envelope**" option means that the e-mail stored for him, including any attachments, is converted into an HTML document and encrypted with a password to be specified by him beforehand. This HTML document is sent to the external communication partner by e-mail. All future e-mails that an internal Deutsche Telekom employee sends to this external communication partner will then also be delivered as an encrypted HTML document by direct e-mail.



Functions of the WebMail Portal

To use the WebMail portal, the totemomail WebMail option must be selected.

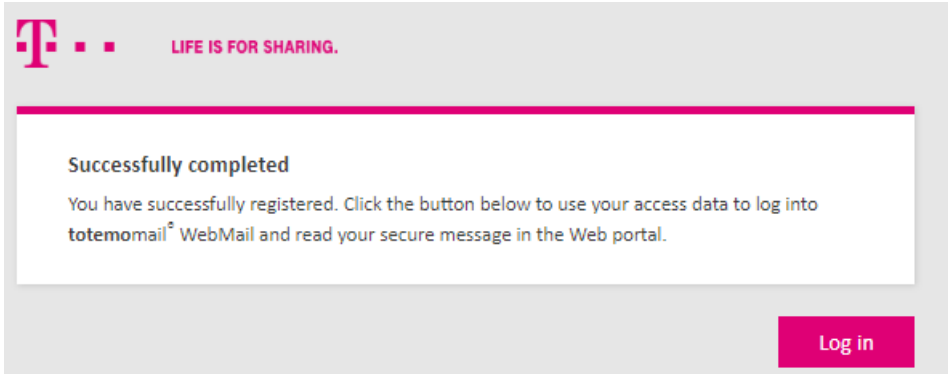


Attention
The use of the WebMail interface requires the activation of Java Script in the web browser.

If your registration is successful, you will receive the message on the right. You have to log in to the WebMail portal again via Login.

User name: <*own e-mail address*>

Password: <*the self-generated password* >



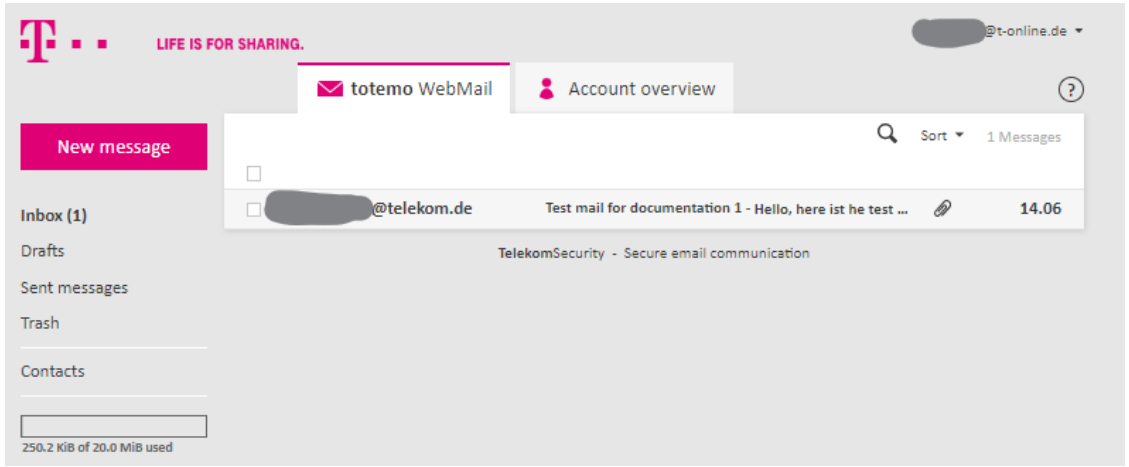
Use of the WebMail Portal

After successful registration, you will be taken to the overview page of the WebMail portal. Via the WebMail user interface, the external recipient can read and reply to his e-mails and send new e-mails as well as delete e-mails.

The selection menu in the left column is easy to understand, i.e. all menu options are self-explanatory.

Reception :

In the inbox, all e-mails sent to the recipient are displayed in the overview.

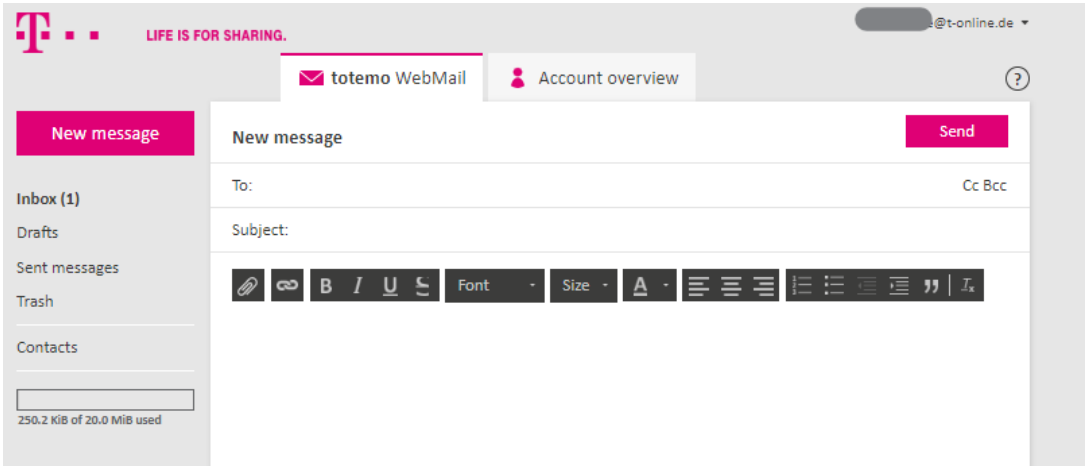


Dispatch :

Via the menu item "**New message**" an e-mail can be securely sent to an internal employee.

Attention:

It is not possible to send to e-mail addresses of external domains.



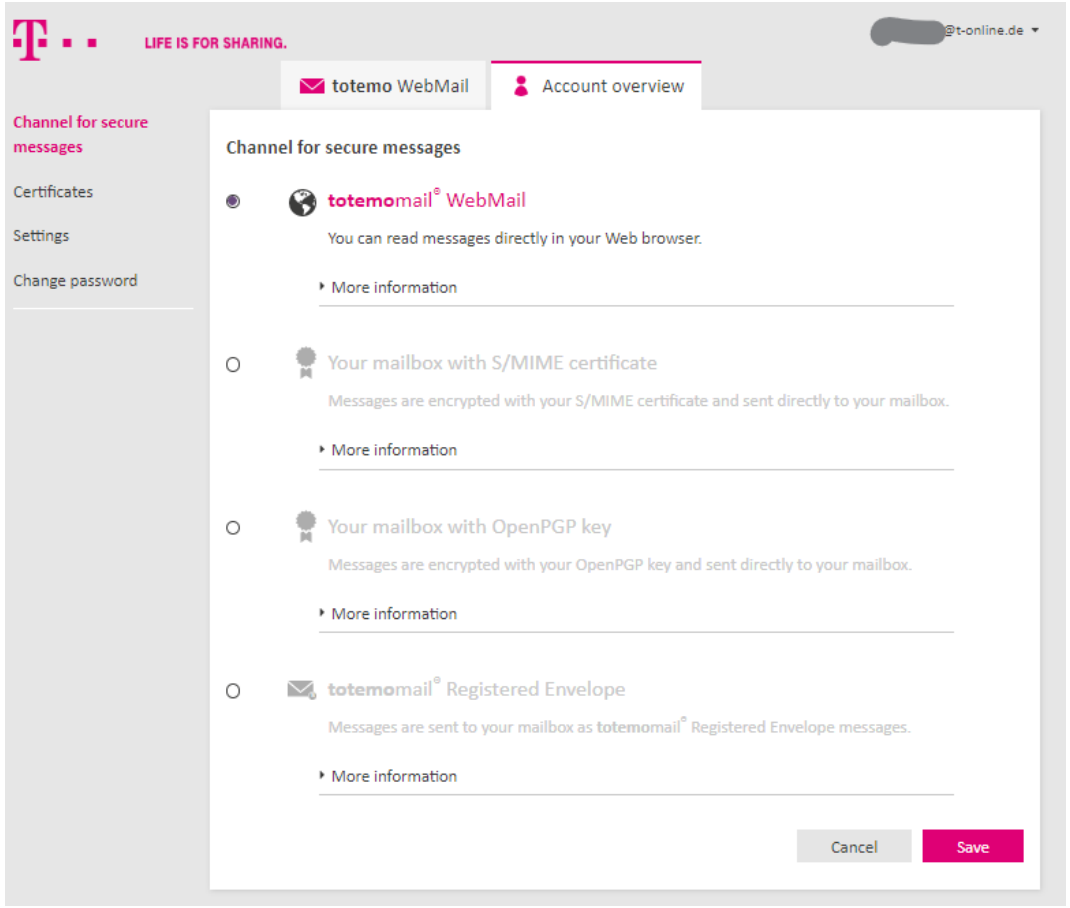
Account overview of the WebMail portal

Individual configurations of the recipient can be carried out in the account overview.

- **Channel for secure messages :**
- Here, the transmission type of the e-mail can be redefined. Depending on your wishes or availability, the receiver can choose one of the available channels:

- WebMail	Delivery of the mail in the WebMail portal
- S/MIME Zertifikat	Delivery of the e-mail directly and S/MIME encrypted
- PGP	Delivery of the e-mail directly and PGP encrypted
- Registered Envelope	Delivery of the mail as an encrypted HTML document

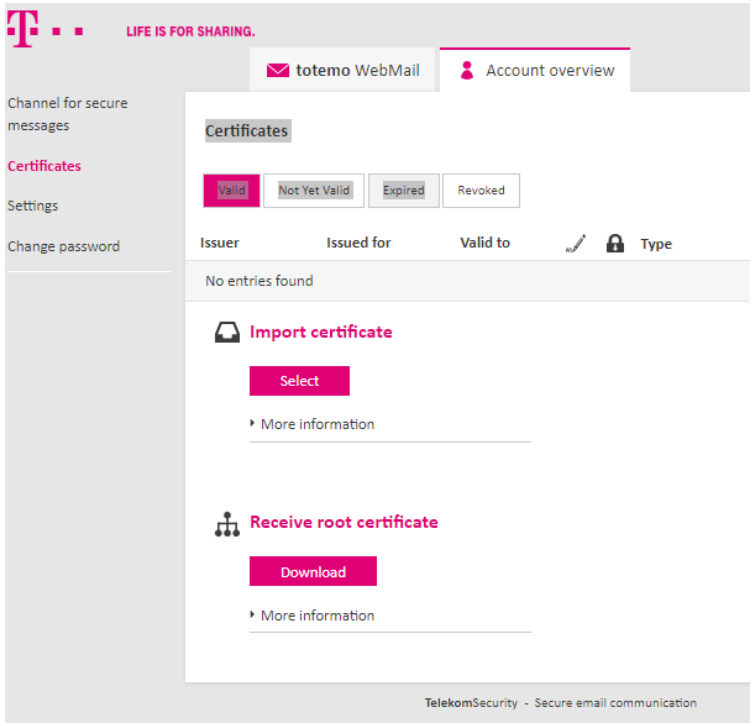
Attention
The selection of S/MIME certificate or PGP requires that an S/MIME certificate or PGP key has been provided in the WebMail interface.



Account overview of the WebMail portal

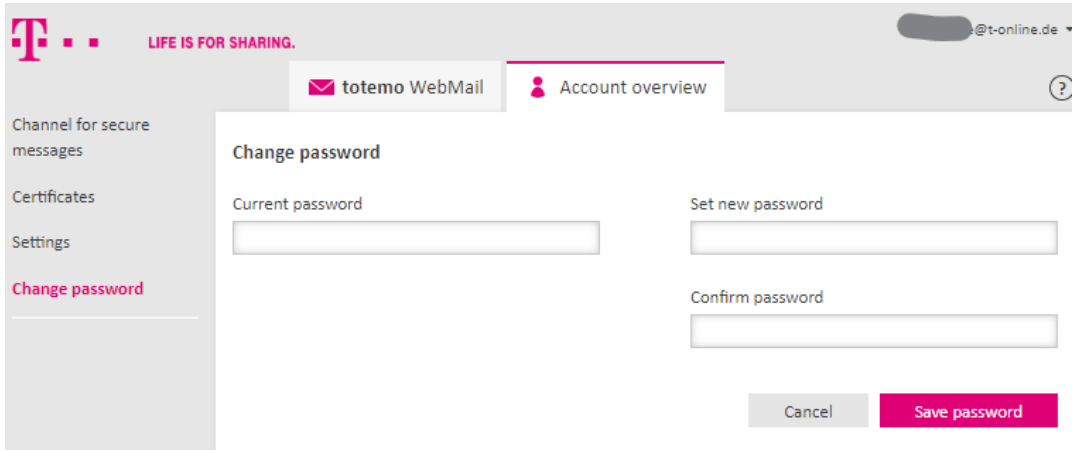
Certificates

In order to receive certificate- or PGP-encrypted e-mails directly, either a valid S/MIME certificate or a PGP key must be stored. The "**Select**" function can be used to upload a certificate or key to the EEGW.



Password:

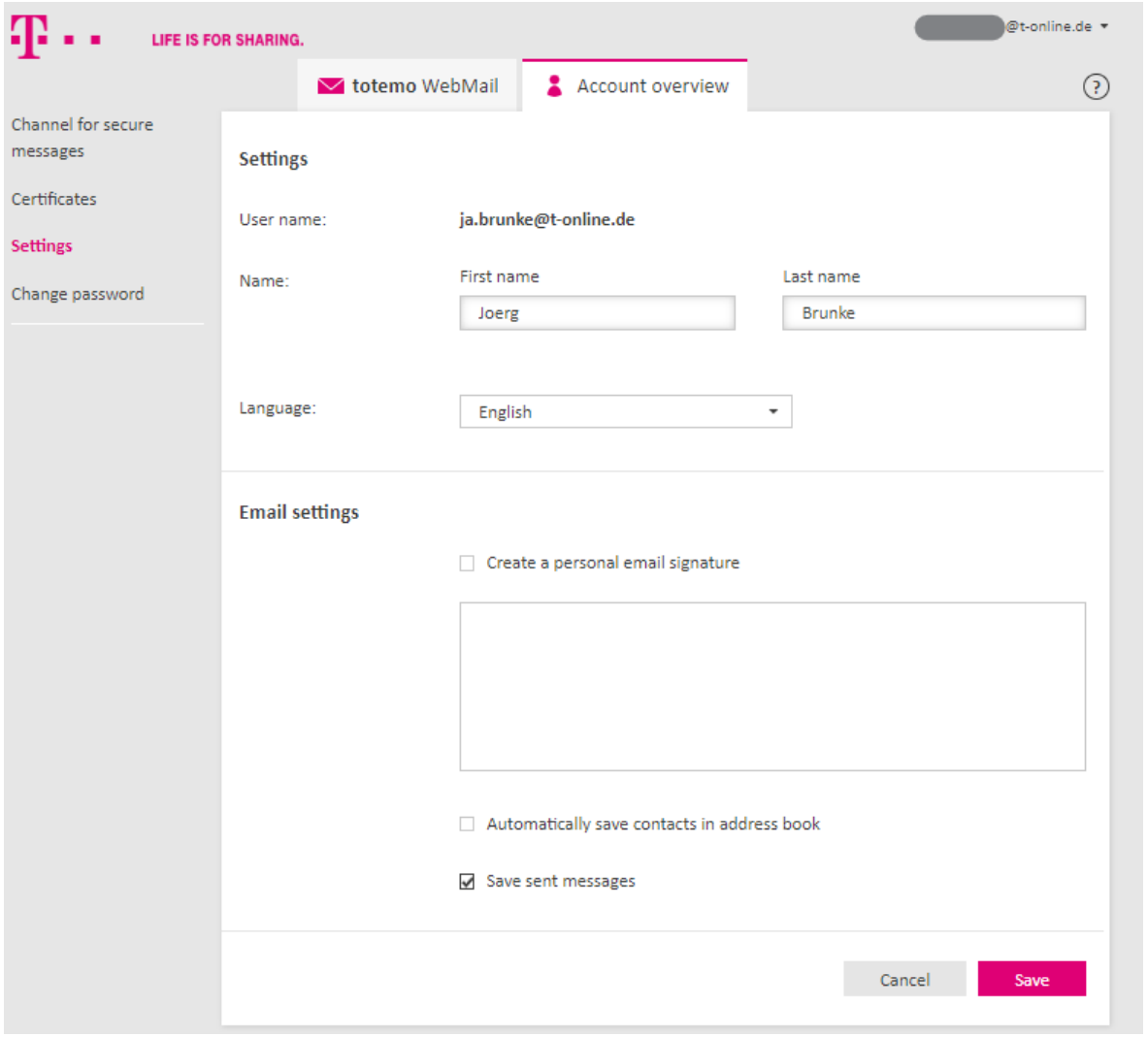
A new password can be set via the selection item "**Change password**".



Account overview of the WebMail portal

Settings:

Personal data can be changed in the settings, such as the name or the language used by the WebMail portal. You can choose between German, English, Italian or French. Furthermore, it is possible to create your own signature and save the contacts used in your own address book. If "**Enable sent messages**" is selected, the data will be saved under "Sent messages".

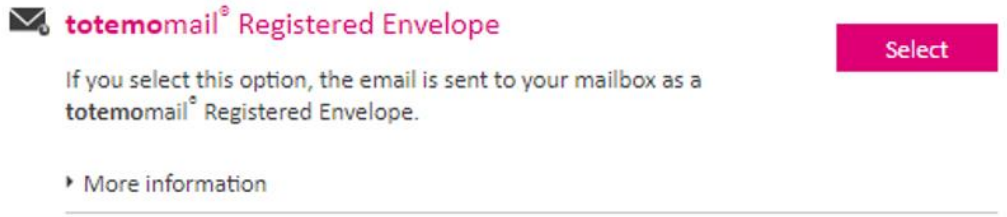


02
Use of Registered Envelope

In the following, the receipt and sending of e-mails with the help of Registered Envelope (HTML file) is described.

Use of Registered Envelope

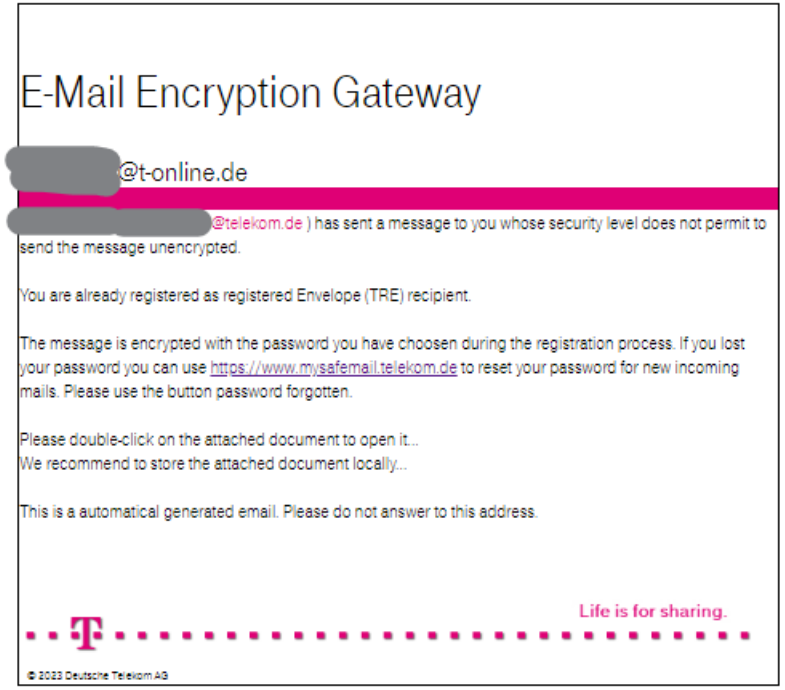
When registering for the first time (see above), the recipient must select the "**Registered Enevelope**" option.



If a Deutsche Telekom employee sends an e-mail to be secured to a "Registered Envelope" recipient, the recipient receives a notification from the EEGW by e-mail, which now contains the original e-mail as an HTML-encrypted attachment.

The encrypted HTML document containing the delivered e-mail can only be opened on the receiving side with the password previously specified by the recipient.

It is recommended to save the encrypted HTML file contained in the attachment of the mail locally and then open it with a browser.

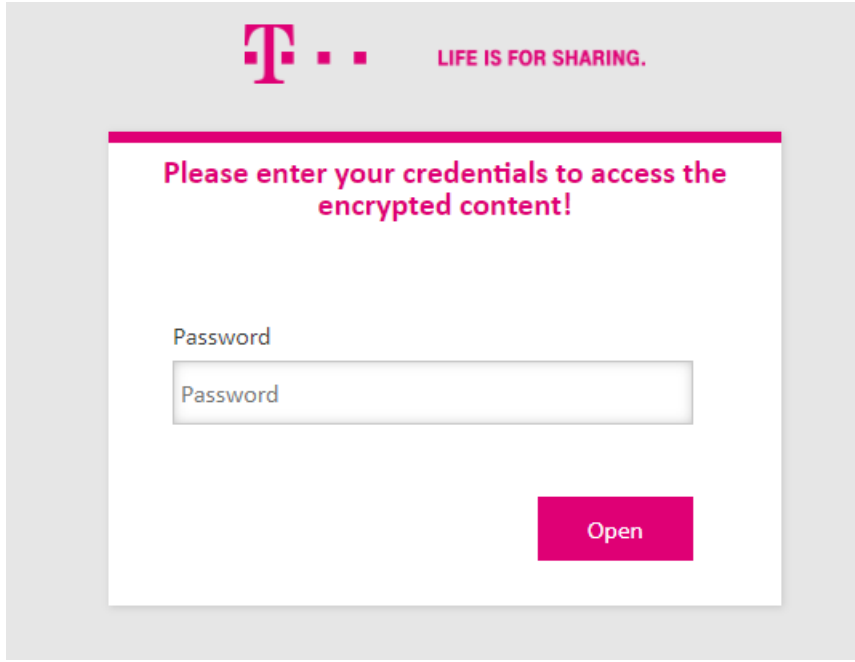


Use of Registered Envelope

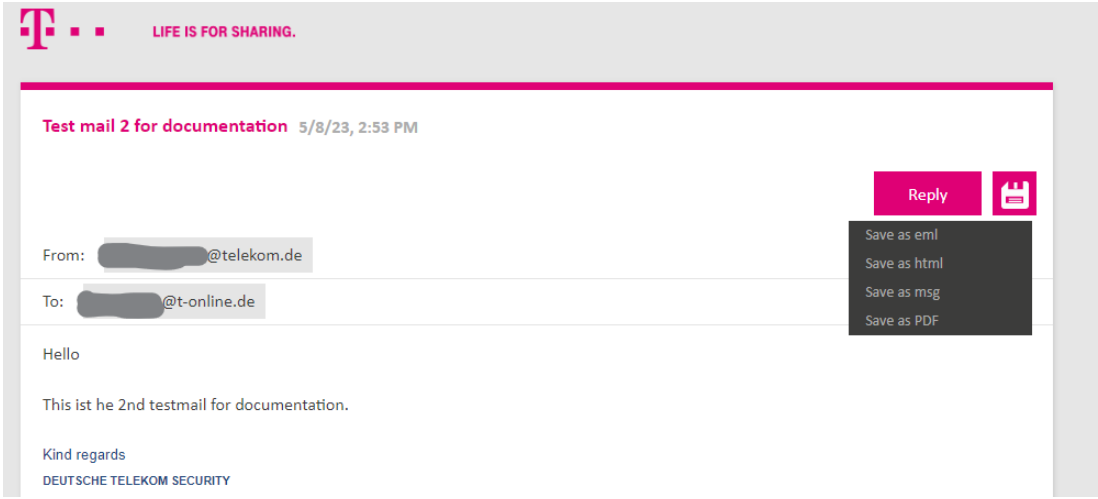
Before the browser can open the file, it is necessary to enter the password previously set during registration. Only after validation of the password can the browser open the file. For validation, an Internet connection with Deutsche Telekom's EEGW is always mandatory.

Attention

The use requires the activation of Java Script in the web browser.



After entering the password, the mail opens in the browser window. Under the floppy disk symbol there are various options for saving the mail locally.

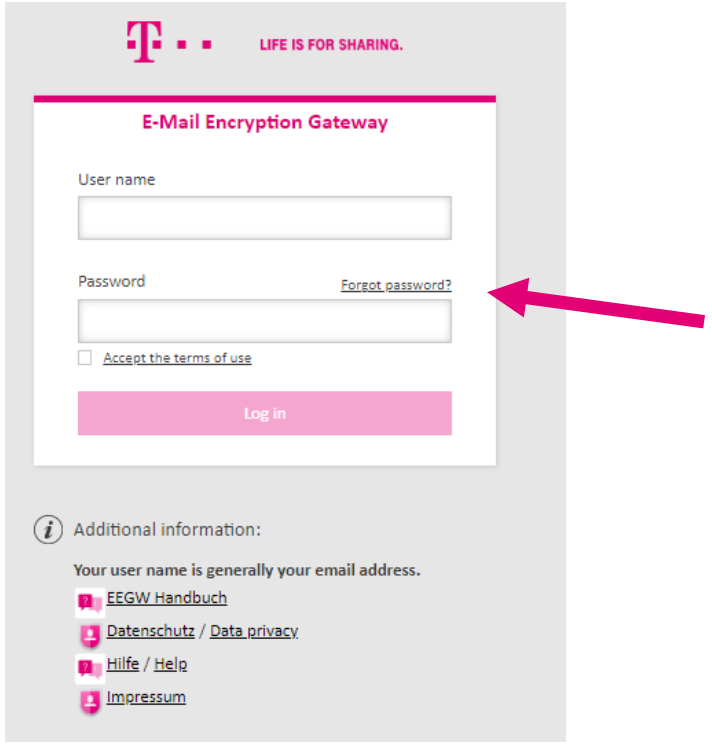


Password forgotten

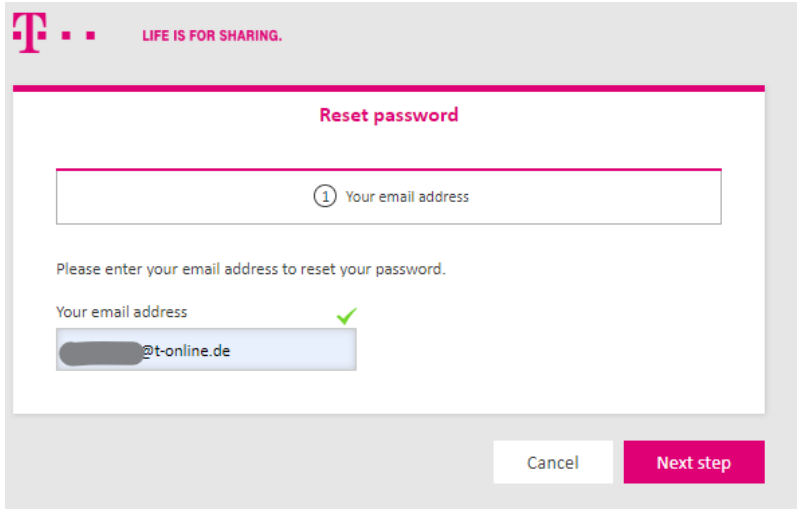
If the password for accessing the WebMail portal or for decrypting the HTML file at "Registered Envelope" has been lost or forgotten for any reason, it is possible to reset the password yourself.

To do this, the WebMail portal must be accessed:

URL: https://www.mysafemail.telekom.de

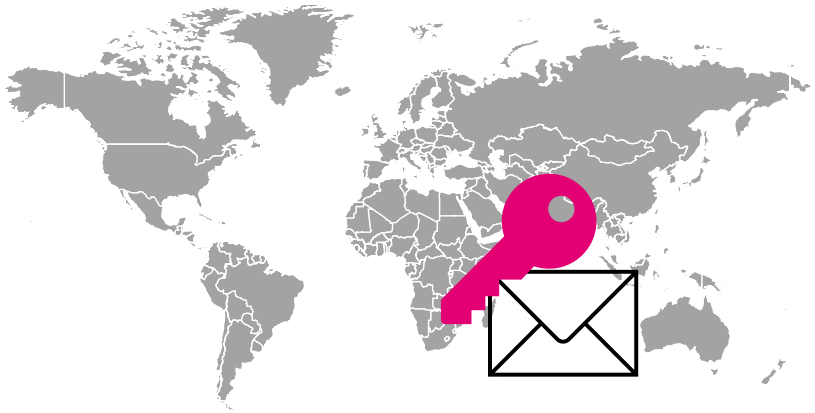


Via "**Forgot password**" you will be redirected to the adjacent page, where your own e-mail address must be entered. With the "**next step**", a new one-time password will be sent to the e-mail address.



03
Use of S/MIME Zertifikat or PGP Keys

In the following, the use of S/MIME certificates or PGP keys is explained in more detail.

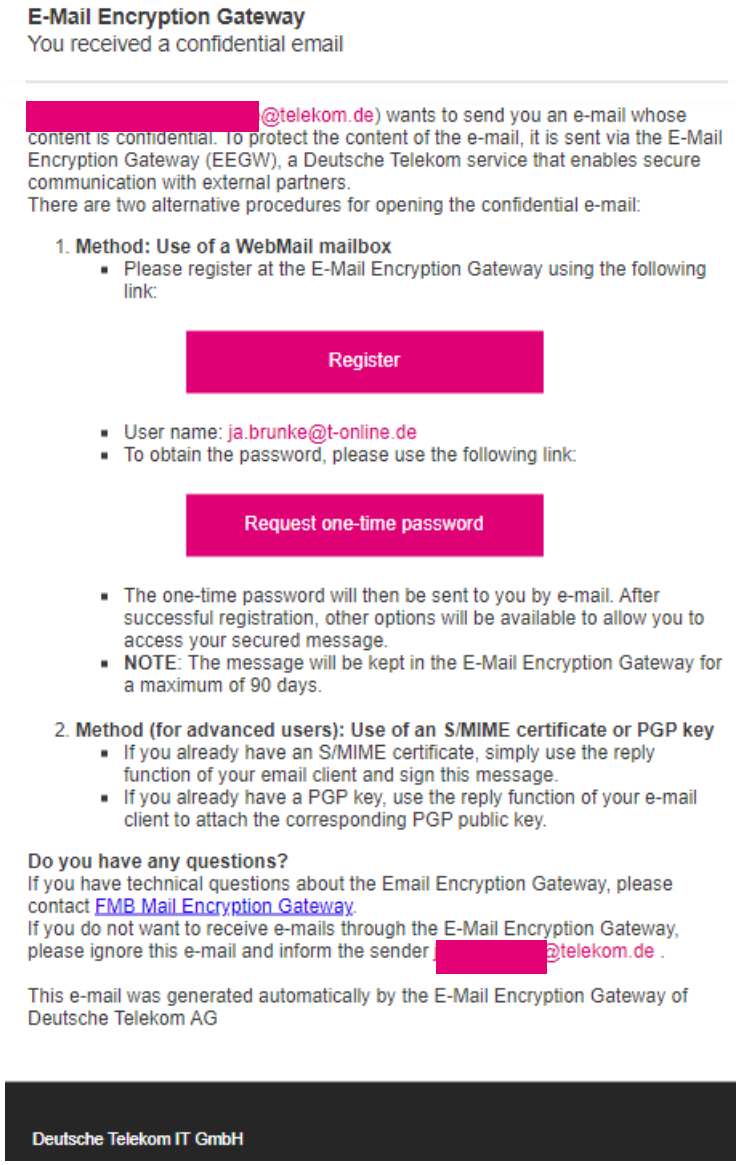


Use of S/MIME oder PGP

If an external recipient has not yet received an encrypted message from Deutsche Telekom and is therefore not registered on the EEGW, the original mail from an internal sender from the Telekom Group will be retained in the EEGW. Instead, the external recipient automatically receives the notification of the delivery of an encrypted e-mail shown next to it.

If an S/MIME certificate is available, you only need to reply to the adjacent notification with an electronically signed S/MIME mail.

If a PGP key is available, the reply mail must contain the public PGP key. This can be sent as an attachment in ASC format or copied directly into the reply mail.



E-Mail Encryption Gateway
You received a confidential email

[redacted]@telekom.de) wants to send you an e-mail whose content is confidential. To protect the content of the e-mail, it is sent via the E-Mail Encryption Gateway (EEGW), a Deutsche Telekom service that enables secure communication with external partners.
There are two alternative procedures for opening the confidential e-mail:

1. **Method: Use of a WebMail mailbox**
   - Please register at the E-Mail Encryption Gateway using the following link:

   Register

   - User name: ja.brunke@t-online.de
   - To obtain the password, please use the following link:

   Request one-time password

   - The one-time password will then be sent to you by e-mail. After successful registration, other options will be available to allow you to access your secured message.
   - **NOTE**: The message will be kept in the E-Mail Encryption Gateway for a maximum of 90 days.

2. **Method (for advanced users): Use of an S/MIME certificate or PGP key**
   - If you already have an S/MIME certificate, simply use the reply function of your email client and sign this message.
   - If you already have a PGP key, use the reply function of your e-mail client to attach the corresponding PGP public key.

Do you have any questions?
If you have technical questions about the Email Encryption Gateway, please contact FMB Mail Encryption Gateway.
If you do not want to receive e-mails through the E-Mail Encryption Gateway, please ignore this e-mail and inform the sender [redacted]@telekom.de .

This e-mail was generated automatically by the E-Mail Encryption Gateway of Deutsche Telekom AG

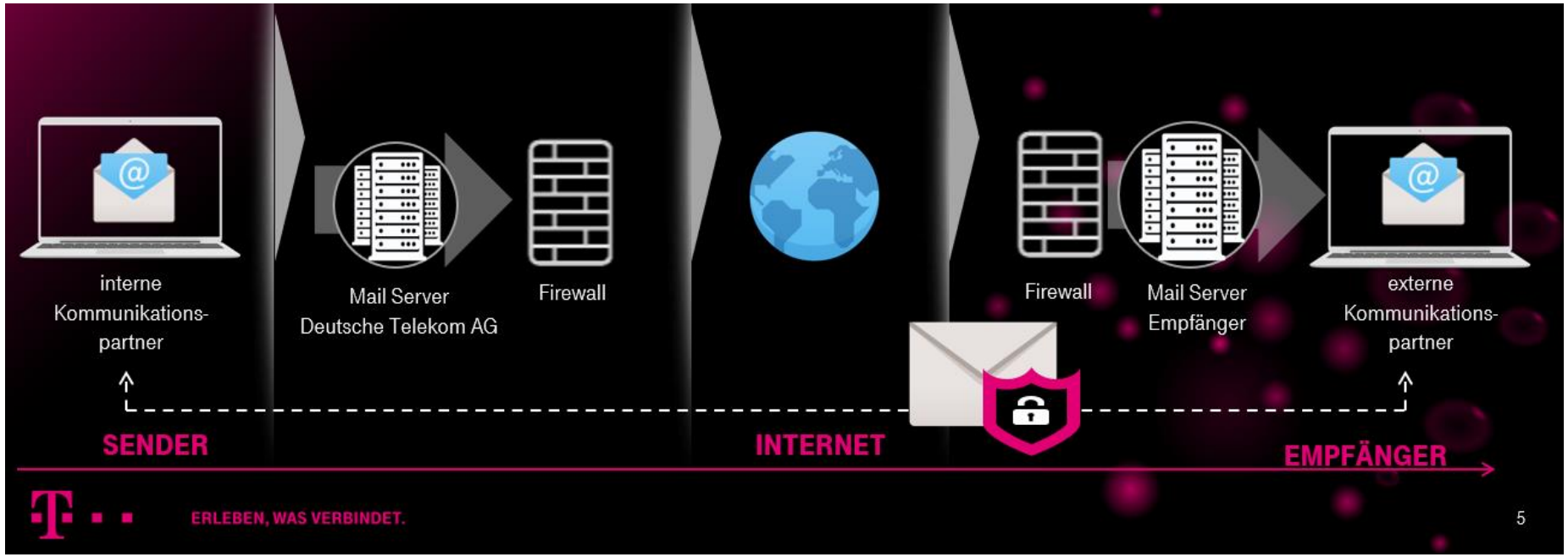
Deutsche Telekom IT GmbH

Use of S/MIME oder PGP

The reply e-mail is intercepted in the EEGW and the key material it contains is extracted and stored.

Future encrypted e-mails from the Telekom Group will be encrypted based on the appropriate encryption technology (S/MIME or PGP) and delivered directly.

A separate notification is no longer required.



04
General Information

General Information

Mailbox size

The mailbox on the WebMail portal has a size of 20 MB. It follows that it is not intended to store or store confidential/encrypted emails, but only provides the ability to deliver them securely. The e-mails should therefore be deleted from the webmail folders as soon as possible.

Even e-mails in the trash are not yet deleted. Only by marking the objects and confirming them with the "Delete" button does the final deletion of the objects and the associated release of storage space take place.

When the mailbox storage limit is reached, both the sender and recipient receive a message that the maximum mailbox size has been exceeded and the email could not be delivered. This also applies to e-mails that have an attachment that is larger than 20 MB.

Inactivity

After 90 days of inactivity, the external user is deleted from the EEGW. As soon as he receives a confidential/encrypted e-mail from a customer employee, he is newly created and thus also receives a new registration e-mail.

Delete E-Mails

After 90 days, mails are automatically removed from the WebMail mailbox.

General Information

Notifications in case of non-registration

The sender receives a message if the external communication partner has not registered after 5 days and has therefore not yet read the e-mail. The external communication partner will receive a reminder message after 3 days if he has not registered by then. For this purpose, he will receive the registration e-mail again.

Change "Channel for safe messages"

Both external recipients registered as WebMail and external recipients registered as "Registered Envelope" can change the "Secure Messages Channel" at any time. In the WebMail under Account Overview, the "Channel for Secure Messages" can be changed. However, e-mails that have already been sent are not automatically converted to HTML, encrypted and delivered retroactively.

For S/MIME or PGP registered external recipients, this is not easily possible. These recipients still need a new one-time password.

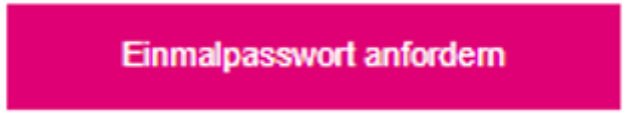
To do this, please contact the helpdesk of the E-Mail Encryption Gateway.

Mail_Encryption_Gateway@telekom.de

Facts in a nutshell

- URL WebMail-Portal : https://www.mysafemail.telekom.de
- or via link in registration mail

- Request initial password via link in the registration er



- Contact E-Mailencryption Team: Mail_Encryption_Gateway@telekom.de