

# Office Standardization. E-Mail Encryption Gateway.

Instructions for external communication Partners.

Life is for sharing.



## Introduction.

The E-Mail Encryption Gateway is an expansion of the existing e-mail infrastructure at Deutsche Telekom. It offers comprehensive communications security that supports encrypted and/or signed e-mails for both internal as well as external communications contacts. The E-Mail Encryption Gateway was installed as a highly available centralized entity between the Deutsche Telekom Intranet and the Internet. It is one of the most sophisticated secure messaging platforms on the market today.

One of the primary advantages of the E-Mail Encryption Gateway, among other things, is the secure e-mail communication between internal employees at Deutsche Telekom and external contacts.

Below we will illustrate and explain all of the scenarios and communication interfaces that external contacts will be faced with, both at the beginning and in later phases of their e-mail communications with employees or functional mailboxes of Deutsche Telekom. Based on these scenarios, we will describe all of the necessary steps to be taken by external users when navigating through the various interfaces and situations that occur when using the The E-Mail Encryption Gateway.

# Table of Contents and Figures.

|   |    |
|---|----|
| Introduction.....   | 2  |
| Table of Contents and Figures.....  | 3  |
| Short Description of the Solution.....  | 4  |
| Case 1: S/MIME or PGP key available.....  | 6  |
| Case 2: Neither the S/MIME certificate nor the PGP key available.....             | 8  |
| Receiving and sending e-mails using WebMail.....                                  | 10 |
| Receiving and sending e-mails using PushedPDF.....                                | 12 |
| Password Reset.....   | 14 |
| Announcement by the Issuing CA.....   | 16 |
| Troubleshooting.....  | 19 |
| List of abbreviations.....  | 20 |
| <b>Table of Figures</b>   |    |
| Figure 1: End-to-end encryption of e-mails.....                                   | 5  |
| Figure 2: E-mail flow with existing S/MIME encryption or PGP encryption keys..... | 6  |
| Figure 3: Notification for first-time registration.....                           | 7  |
| Figure 4: Outlook receiving an encrypted S/MIME e-mail.....                       | 7  |
| Figure 5: Receiving an encrypted PGP e-mail.....                                  | 7  |
| Figure 6: Mail flow without an existing S/MIME or PGP key and use of WebMail..... | 8  |
| Figure 7: Notification for first-time registration.....                           | 9  |
| Figure 8: First-time Web access in WebMail.....                                   | 9  |
| Figure 9: Registering in WebMail.....   | 10 |
| Figure 10: Answering the security questions.....                                  | 10 |
| Figure 11: WebMail interface.....   | 11 |
| Figure 12: Notification of delivered WebMail.....                                 | 11 |
| Figure 13: Creating a password for saving PDF documents.....                      | 12 |
| Figure 14: Successful registration for PDF delivery.....                          | 12 |
| Figure 15: Receiving PDFs 1.....  | 12 |
| Figure 16: Receiving PDFs 2.....  | 13 |
| Figure 17: Answering a PDF e-mail.....  | 13 |
| Figure 18: Initiating the password reset process.....                             | 14 |
| Figure 19: Entering the e-mail address during the password reset process.....     | 14 |
| Figure 20: Security questions during the password reset process.....              | 15 |
| Figure 21: Specifying a new password.....   | 15 |

## A Brief Description of the Solution.

All employees of Deutsche Telekom AG can use the E-Mail Encryption Gateway for sending e-mails to any internal or external contacts or for receiving and decrypting encrypted e-mails from those contacts. Encrypted e-mails can also be forwarded to all involved recipients 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, hereinafter referred to as "WebMail". An automatically generated notification e-mail will inform the external contact that he/she received an encrypted e-mail. Using WebMail, he/she can then log in and, after authentication, read all of the encrypted e-mails delivered to him/her.

If required, the external contact can choose in WebMail to forward encrypted e-mails. The forwarded e-mails along with their attachments will be converted into encrypted PDF files that can later be decrypted using the password previously specified by the user 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 E-Mail Encryption Gateway can use it to encrypt and send e-mails using the corresponding technology in the future.

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 E-Mail Encryption Gateway, depending on the technology used by the external recipient, for example using the conversion required by PGP.

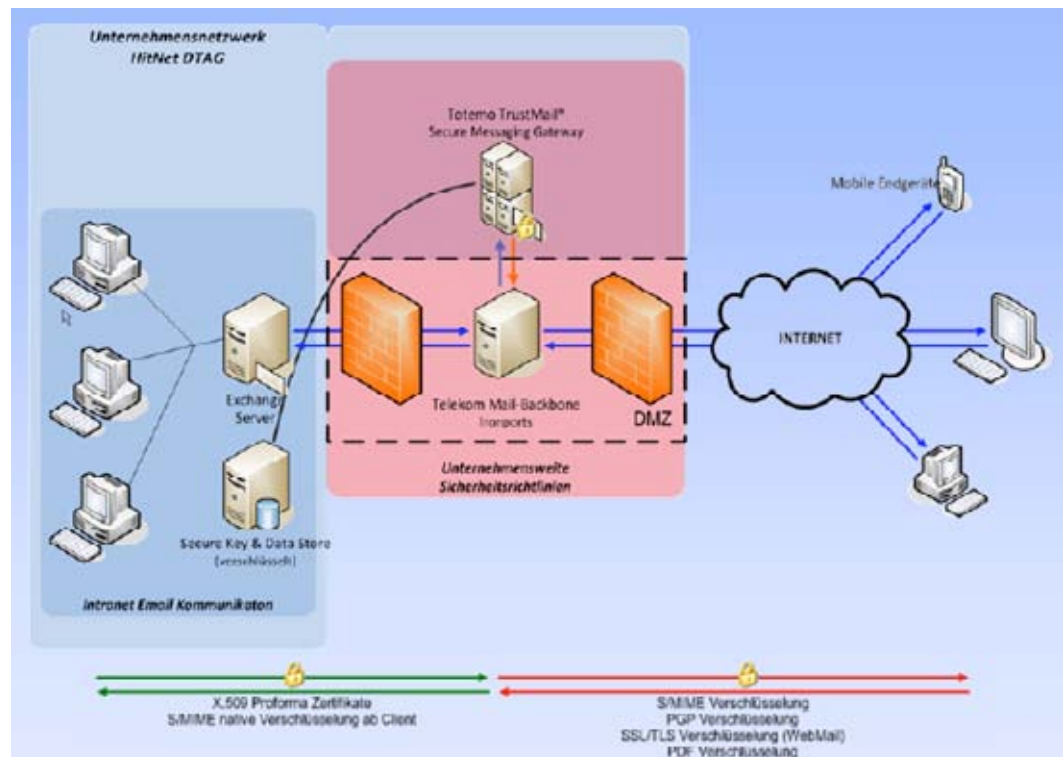


Figure 1: End-to-end encryption of e-mails

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 e-mail encryption and signatures. In order to avoid requiring external recipients to migrate from PGP to S/MIME, however, outgoing e-mails from 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 is available.

The following scenarios describe the secure e-mail communications between Deutsche Telekom and an external user when the user is already able to encrypt or add signatures to e-mails using S/MIME or PGP technology.

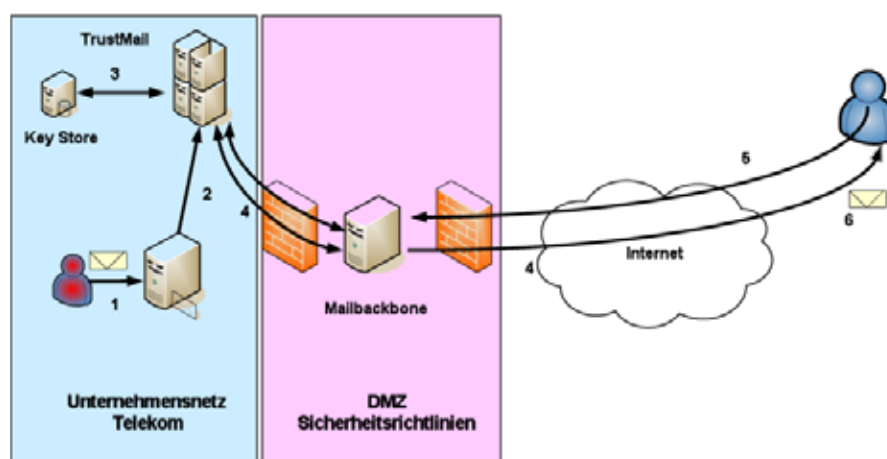


Figure 2: Mail flow with existing S/MIME encryption or PGP encryption keys

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 partner 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 contact, or if one cannot be found via the associated 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 in the following form.

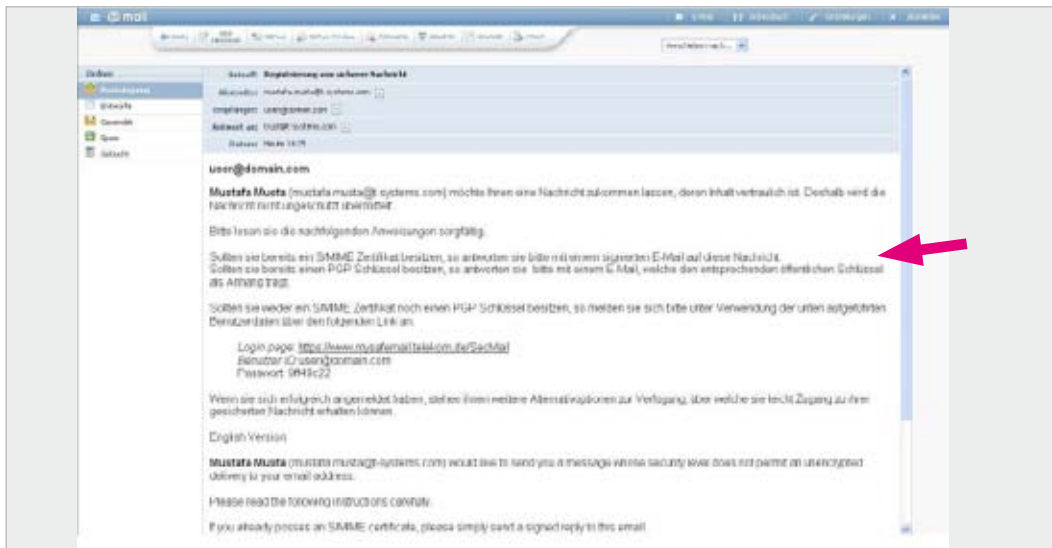


Figure 3: Notification for first-time registration

5. If the external user already has an S/MIME certificate for e-mail encryption and signatures (see red arrow in Figure 3), he/she replies to the e-mail mentioned above with an e-mail containing an S/MIME signature. If the external contact is using Microsoft Outlook as an e-mail client, for example, this can be activated by simply selecting the appropriate button for signatures.



If the external contact is already using PGP encryption, he/she replies to this e-mail and includes the PGP key as an attachment.

6. The E-Mail Encryption Gateway will verify the validity of the key information received and save the public key (S/MIME or PGP) in its Key Store.
7. The temporarily saved e-mail will now be encrypted and delivered based on either the S/MIME key technology indicated by the external user:



Figure 4: Outlook receiving an encrypted S/MIME e-mail

Or the mail will be encrypted using PGP and delivered:



Figure 5: Receiving an encrypted PGP e-mail

**!** After the registration is complete, any subsequent exchanges of encrypted e-mails between an internal employee or Deutsche Telekom functional mailbox and an external contact will be handled by the E-Mail Encryption Gateway using the public S/MIME or PGP key now saved in the Key Store, meaning that steps 4, 5 and 6 required for the registration are now no longer necessary.

## Case 2: Neither an S/MIME certificate nor a PGP key is available.

The following scenarios illustrate secure e-mail communication between Deutsche Telekom and an external user who does not yet have e-mail encryption technology (S/MIME or PGP) available.

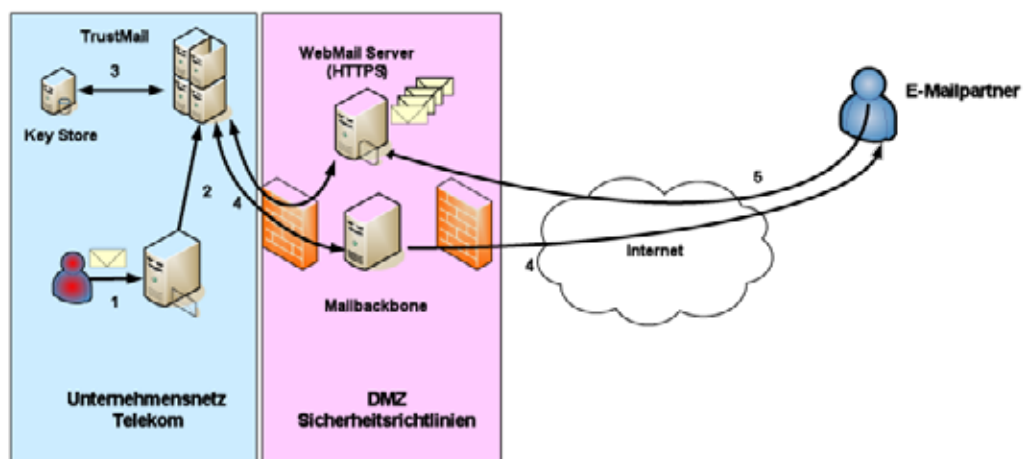


Figure 6: E-mail flow without an S/MIME or PGP key when using WebMail

1. A Deutsche Telekom employee sends an external recipient a (signed) e-mail that is to be encrypted by TrustMail®.
2. The e-mail is routed internally to TrustMail®.
3. TrustMail® 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 if one cannot be found via the associated indexing services or key servers, the e-mail will be temporarily stored in TrustMail® and the external user will be sent the following notification:

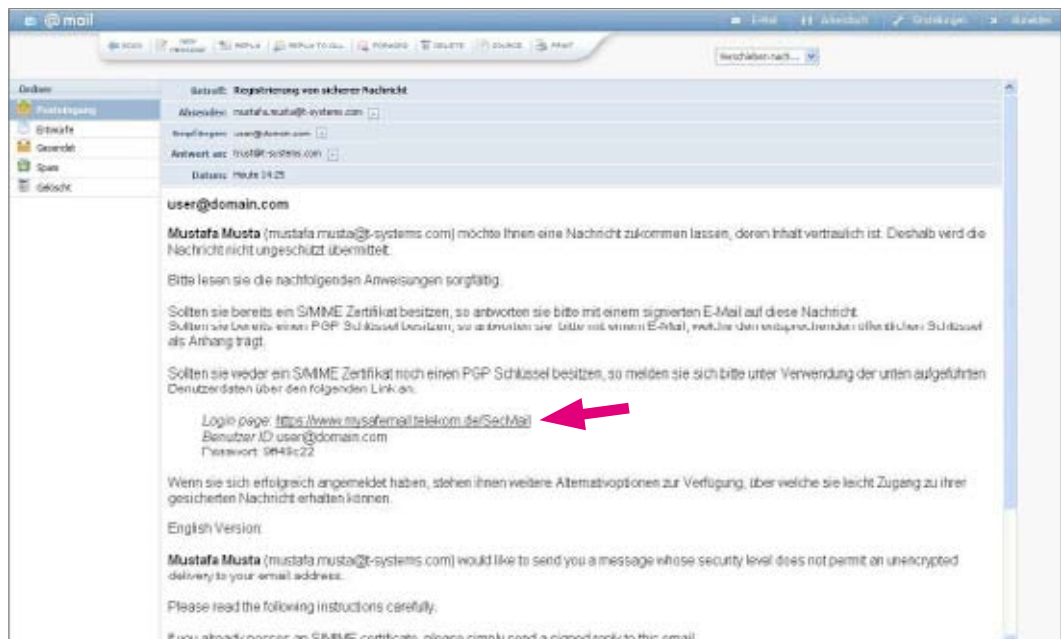


Figure 7: Notification for first-time registration

- Because the external contact has no proprietary S/MIME certificate or PGP key pair for e-mail encryption or signatures, he/she has the option to access the encrypted e-mail via WebMail or to receive an encrypted PDF file sent directly to him/her via e-mail. To do this, the user must register in WebMail (SSL secure) using the URL in the e-mail notification that was sent to him/her (see red arrow in Figure 7). The following page will be opened in a Web browser:

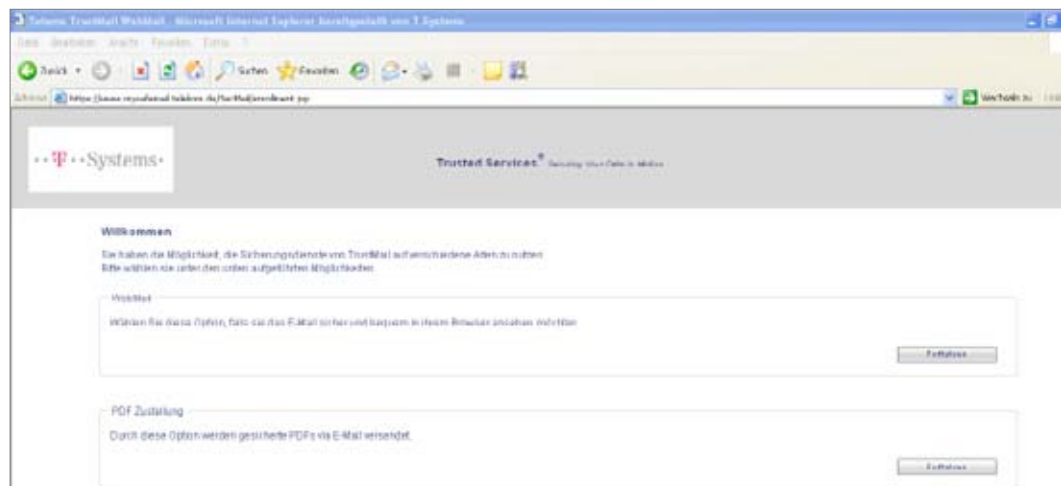


Figure 8: First-time access in WebMail

**The external contact can now decide between "WebMail" or "PDF delivery":**

**The "WebMail" option** means that the encrypted e-mails (including any attachments) will not be delivered directly to the external user, but rather will be available via a WebMail interface (similar to applications like GMX or Web.de) that must be authenticated and SSL secure.

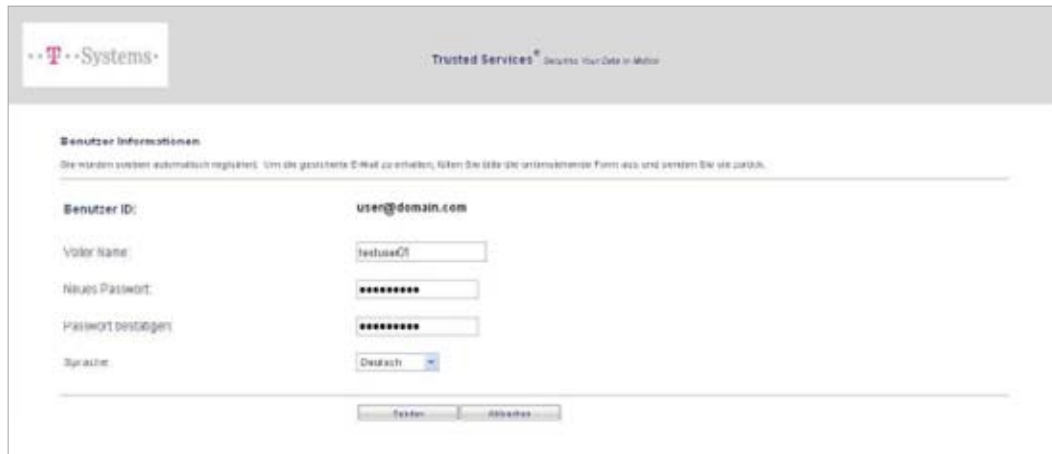
**The "PDF delivery" option** means that the sent e-mail and any attachments will be converted into a PDF file and encrypted with a password previously specified by the user. This PDF file will then be delivered to the external contact via e-mail. All future e-mails sent by internal employees of Deutsche Telekom will now be delivered directly via e-mail as encrypted PDF files.

## Receiving and sending e-mail using WebMail.

Below we describe the initial registration process for WebMail and how to access encrypted e-mails using the WebMail interface of the E-Mail Encryption Gateway. We also tell you how to create and send encrypted e-mails.

### Registration for an external contact in WebMail:

Because the e-mail above (see Figure 7) will only generate a one-time password (OTP), external users first have to create their own new password:

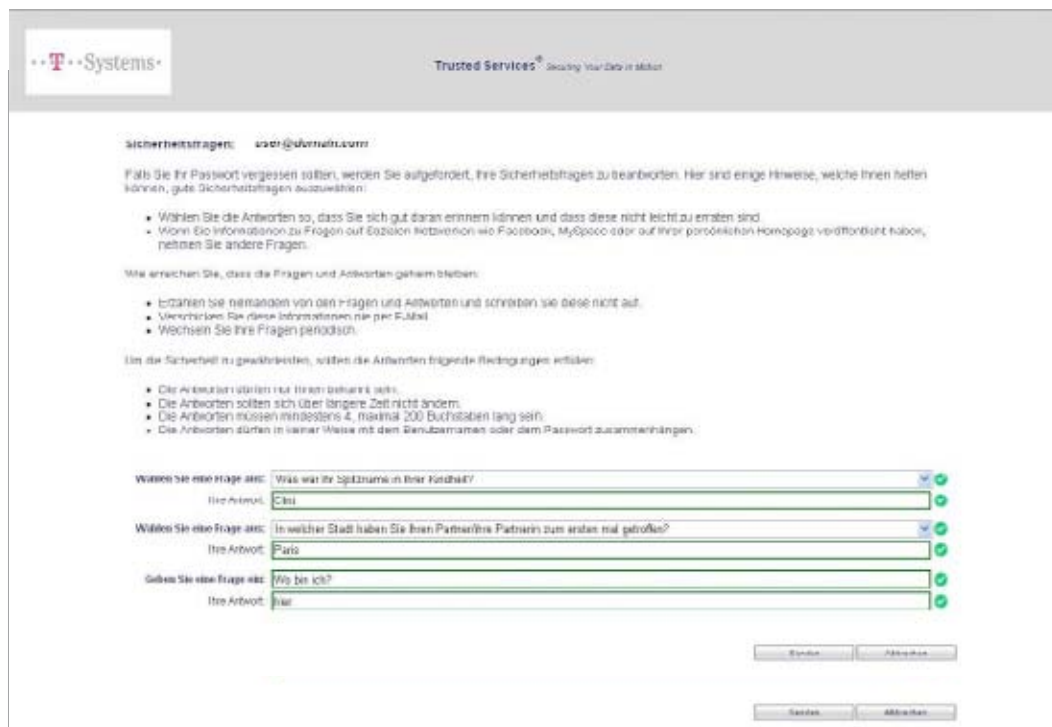


The screenshot shows the registration page for WebMail. At the top left is the logo for 'T-Systems' and at the top right is 'Trusted Services' with the tagline 'Security Your Data in Motion'. The main heading is 'Benutzer Informationen' (User Information). Below this, there is a sub-heading 'Sie wurden werden automatisch registriert. Um die gesicherte E-Mail zu erhalten, füllen Sie bitte die untenstehende Form aus und senden Sie sie zurück.' (You will be automatically registered. To receive the secured email, please fill out the form below and send it back). The form fields are: 'Benutzer ID:' with the value 'user@domain.com'; 'Vorname:' with the value 'testuser'; 'Neues Passwort:' and 'Passwort bestätigen:' both with masked characters '\*\*\*\*\*'; and 'Sprache:' with a dropdown menu set to 'Deutsch'. At the bottom of the form are two buttons: 'Zurück' and 'Absenden'.

Figure 9: Registering in WebMail

### Answering the security questions:

In the event that an external user loses or forgets his/her WebMail password, he/she can answer three security questions to reset it without needing to contact a help desk. Two of these can be selected from the available questions and the third can be freely defined. Tips for selecting and answering the security questions can be found on the web site.



The screenshot shows the security questions page for WebMail. At the top left is the logo for 'T-Systems' and at the top right is 'Trusted Services' with the tagline 'Security Your Data in Motion'. The main heading is 'Sicherheitsfragen: user@domain.com'. Below this, there is a sub-heading 'Falls Sie Ihr Passwort vergessen sollten, werden Sie aufgefordert, Ihre Sicherheitsfragen zu beantworten. Hier sind einige Hinweise, welche Ihnen helfen können, gute Sicherheitsfragen auszuwählen:' (If you should forget your password, you will be asked to answer your security questions. Here are some tips which can help you choose good security questions:). The tips are: 'Wählen Sie die Antworten so, dass Sie sich gut daran erinnern können und dass diese nicht leicht zu erraten sind.' (Choose the answers so that you can remember them well and that they are not easy to guess.); 'Wählen Sie Informationen zu Fragen auf sozialen Netzwerken wie Facebook, MySpace oder auf Ihrer persönlichen Homepage vorfindbar haben, nennen Sie andere Fragen.' (Choose information from questions on social networks like Facebook, MySpace or on your personal homepage that can be found, name other questions.); 'Machen Sie, dass die Fragen und Antworten geheim bleiben:' (Make it so that the questions and answers remain secret:); 'Erklären Sie niemandem von den Fragen und Antworten und schreiben Sie diese nicht auf.' (Explain to no one the questions and answers and do not write them down.); 'Verstecken Sie diese Informationen nie per E-Mail.' (Never hide this information via email.); 'Wechseln Sie Ihre Fragen periodisch.' (Change your questions periodically.); 'Um die Sicherheit zu gewährleisten, sollten die Antworten folgende Bedingungen erfüllen:' (To ensure security, the answers should meet the following conditions:); 'Die Antworten sollten nur Ihnen bekannt sein.' (The answers should only be known to you.); 'Die Antworten sollten sich über längere Zeit nicht ändern.' (The answers should not change over a long period.); 'Die Antworten müssen mindestens 4, maximal 200 Buchstaben lang sein.' (The answers must be at least 4, maximum 200 characters long.); 'Die Antworten dürfen in keiner Weise mit dem Benutzernamen oder dem Passwort zusammenhängen.' (The answers must not be in any way related to the username or password.). Below the tips, there are three questions with input fields and green checkmarks indicating they are correct: 'Wählen Sie eine Frage aus: Was war ihr Spitzname in Ihrer Kindheit?' (Your answer: Citi); 'Wählen Sie eine Frage aus: In welcher Stadt haben Sie Ihren Partner/Ihre Partnerin zum ersten Mal getroffen?' (Your answer: Paris); 'Geben Sie eine Frage ein: Wo bin ich?' (Your answer: hier). At the bottom of the form are two buttons: 'Zurück' and 'Absenden'.

Figure 10: Answering the security questions

**Accessing delivered e-mails via WebMail:**

The external user must then log in again with the new password, after which he/she will have access to encrypted e-mails via the WebMail interface:

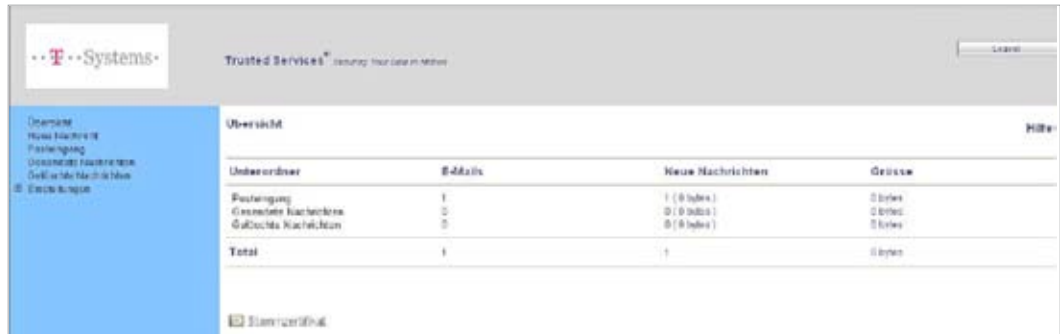


Figure 11: WebMail interface

Using the WebMail interface, external users can read, answer, send or delete e-mails. He/she can also download e-mails to the desktop (EML, HTML, PDF). The menu in the left column is easy to understand and resembles well-known provider interfaces such as GMX, T-Online, etc. The options are self-explanatory.

If the external user is already registered and has already received a new, encrypted e-mail from a Deutsche Telekom employee address, he/she will receive a notification from the E-Mail Encryption Gateway that a new message is waiting in the WebMail system:



Figure 12: Notification of delivered WebMail



**The external contact can use WebMail to send a new e-mail only to internal employees or functional mailboxes at Deutsche Telekom. In addition, only internal employees or automated mailboxes can be added to a reply to the sent e-mail. This restriction is intended to prevent abuse of the WebMail application for non-Telekom communications.**

## Receiving and sending e-mails using PushedPDF.

Below we describe how an external user registers with WebMail for the first time and how he/she can access e-mails that have been forwarded to his/her address or converted to PDF files.

### Registering as an external user in WebMail and receiving PDF deliveries:

Because the e-mail (see Figure 7) above will only generate a one-time password (OTP), external users first have to create their own new password in order to save PDF files in the future:



Figure 13: Creating a password for securing PDF documents

The user must then answer the three security questions as described in Figure 10. The user is then registered as a PDF recipient and will receive all encrypted e-mails from Deutsche Telekom employee addresses as encrypted PDF files in an e-mail in the future:



Figure 14: Successful registration for receiving PDF e-mails

The encrypted PDF document containing the delivered e-mail can only be opened by the recipient using the password previously specified by that recipient.

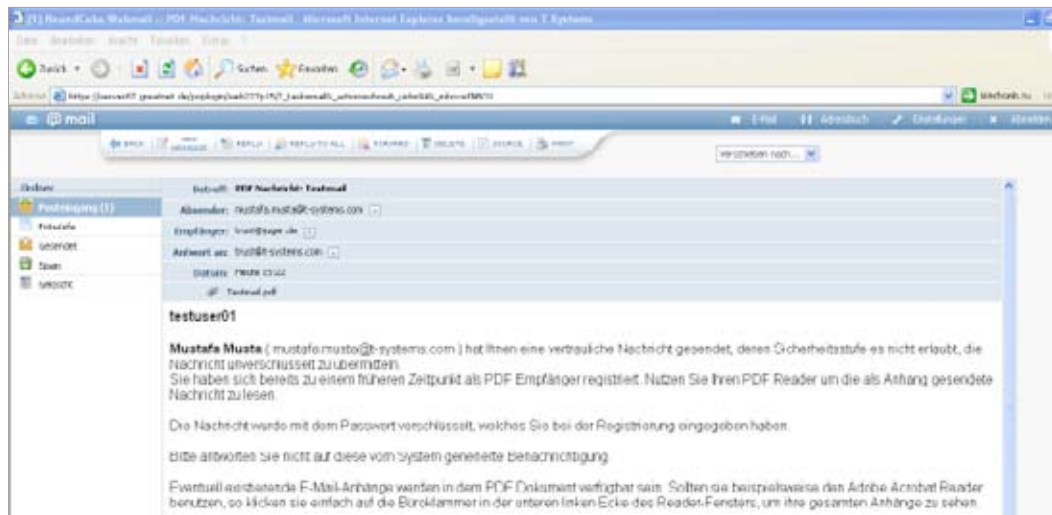


Figure 15: Receiving PDFs 1

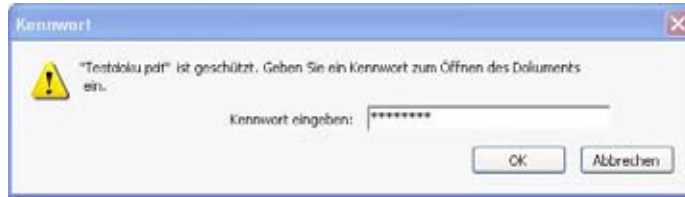


Figure 16: Receiving PDFs 2



A registered external WebMail user (see "Receiving and sending e-mails using WebMail") can decide at any point that he/she wants to receive e-mails as encrypted PDF files. To do this, he/she must enter a new password in WebMail with which the PDFs will be encrypted in the future. Already received e-mails that can be opened via WebMail, however, cannot be retroactively converted into PDFs, encrypted and sent. Having said that, the external contact can download saved e-mails in WebMail as encrypted PDF files.

If the external user would like to reply to this type of PDF e-mail with an encrypted e-mail, it is only possible via WebMail. To access WebMail, follow the URL contained in the PDF file:

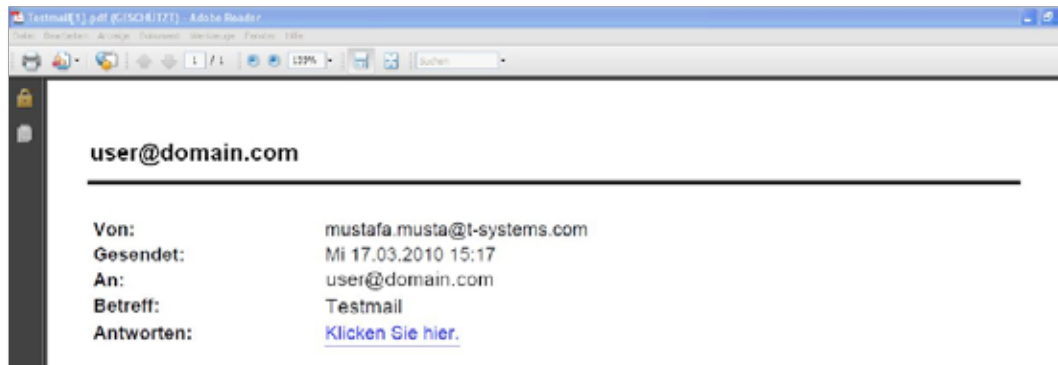


Figure 17: Answering a PDF e-mail



A direct reply to the e-mail containing the encrypted PDF file is not permitted because the e-mail will not reach its original internal sender and the e-mail is not sent in encrypted form. This is mentioned a number of times in the e-mail delivered with the PDF file.

# Password Reset.

If the external contact has for some reason either lost or forgotten his/her password, it can be reset and changed if the correct answers are given to the security questions specified during registration.

To do this, the user must click the "Forgot password" button:

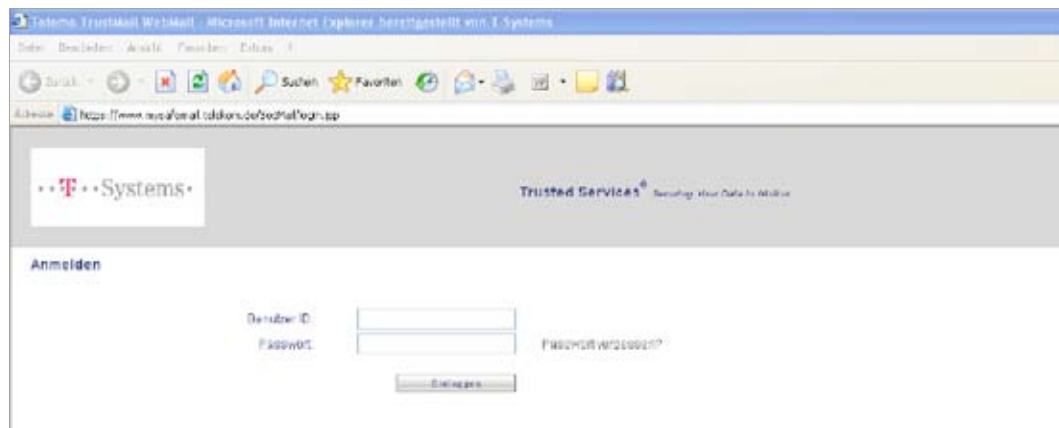


Figure 18: Initiating password reset process

The user must then specify his/her e-mail address:

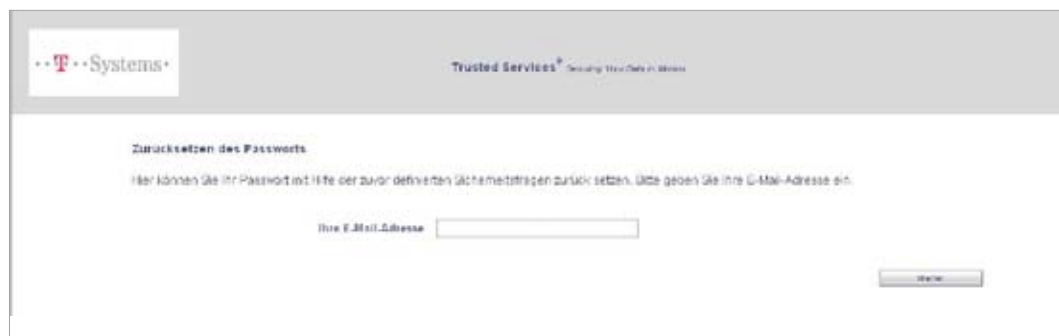


Figure 19: Entering the e-mail address during the password reset process


In the next step, the security questions must be answered exactly as they were during registration:



The screenshot shows a web interface for password reset. At the top left is the logo for 'Systems' and at the top right is 'Trusted Services'. The main heading is 'Zurücksetzen des Passworts für die E-Mail-Adresse: user@domain.com'. Below this, a message asks the user to provide answers to security questions from their registration. There are three input fields: 'Wie war die Spielweise in Ihrer Kindheit?' with 'Ciao' entered, 'In welcher Stadt haben Sie beim Parken das Parkhaus das erste mal getroffen?' with 'Paris' entered, and 'Wo wohnt?' with 'Paris' entered. A note at the bottom states: 'Falls Sie die Antworten nicht mehr wissen, nehmen Sie bitte mit Ihrem Kundenkassenzentraler Kontakt auf.' There are 'Zurück' and 'Weiter' buttons at the bottom right.

Figure 20: Security questions during the password reset process

If the external user enters the correct answers, he/she can then specify a new password:



The screenshot shows a web interface for changing a password. At the top left is the logo for 'Systems' and at the top right is 'Trusted Services'. The main heading is 'Passwort ändern'. Below this, there are two input fields: 'Neues Passwort:' and 'Passwort bestätigen:'. A 'Speichern' button is located below the second input field.

Figure 21: Specifying a new password

## Announcement by the Issuing CA.

The external user may receive warnings regarding the signature. This can happen if the e-mail client of the external user does not recognize the certification center (Deutsche Telekom TrustCenter) that issued the internal employee certificate.

Signiert von: Es sind Probleme mit der Signatur aufgetreten. Klicken Sie für Details auf die Signaturschaltfläche.

In this case, the external user must trust or import the associated certificate. Below is an example of this process on a Windows PC.

By clicking on the Signature icon, the following window will appear:



At this point the certification center must be trusted:



This must then be confirmed:



Now the user certificate has to be imported. To do so, click once more on the Signature icon and then on "Details":



Then click the "Trust" button:





Please also specify here that the certificate is trustworthy. After that, the certificate and the associated certificate center should be successfully imported and no further warnings should appear:



## Troubleshooting.

### Adobe Reader cannot open ZIP files.

Adobe Reader versions 7, 8 and 9 cannot open attachments containing ZIP files. The cause of this is a restrictive policy setting in the Adobe Windows registry because ZIP files can contain dangerous programs.

If you as an external contact have selected "PushedPDF" (see "Receiving and sending encrypted e-mail using PushedPDF") for encrypted e-mail communications with one or more employees of Deutsche Telekom, this limitation may affect you if you have a standard installation of Adobe Acrobat Reader and receive an encrypted e-mail with one or more ZIP files attached.

This setting can be changed in the registry, as explained below.



**A change to the registry should only be made after an agreement has been reached with the IT department that conforms the security guidelines of both the regulatory authorities and company. The changes should only be made by the appropriate specialist personnel (e. g. a Windows administrator).**

---

#### **Adobe Acrobat Reader 7.x:**

Follow the steps below to edit the Windows registry and change the security settings for handling file attachments in Adobe Acrobat Reader 7:

1. Select Start > Run.
2. Type `regedit` in the Open box and click OK to start the Windows Registry Editor.
3. Navigate to the following registry key:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\AcrobatReader\[versionnumber]\FeatureLockdown\cDefaultLaunchAttachmentPerms`
4. Double-click on the value: `sBuiltInPermlist`
5. If necessary, scroll down to find the file extension (.zip). The file extension is in the right-hand column of the list of values.
6. Edit the number just after the file extension type and change the value to 1: `.zip:1`

Further information is available at: <http://kb2.adobe.com/cps/331/331371.html>

#### **Adobe Acrobat Reader 8.x, 9.x:**

The required modification is similar for Adobe Acrobat Reader 7.x. The location of the registry key in step 3 is the only thing that is different:

`HKEY_LOCAL_MACHINE\software\policies\adobe\acrobatreader\[version]\FeatureLockDown\cDefaultLaunchAttachmentPerms`

## List of Abbreviations.

|      |                     |
|------|---------------------|
| DMZ  | Demilitarized Zone  |
| DTAG | Deutsche Telekom AG |
| OTP  | One-Time Password   |

Office Standardization.  
E-Mail Encryption Gateway.  
Instructions for external 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](mailto:trust@t-systems.com)

Life is for sharing.

