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.

Table of Figures

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.

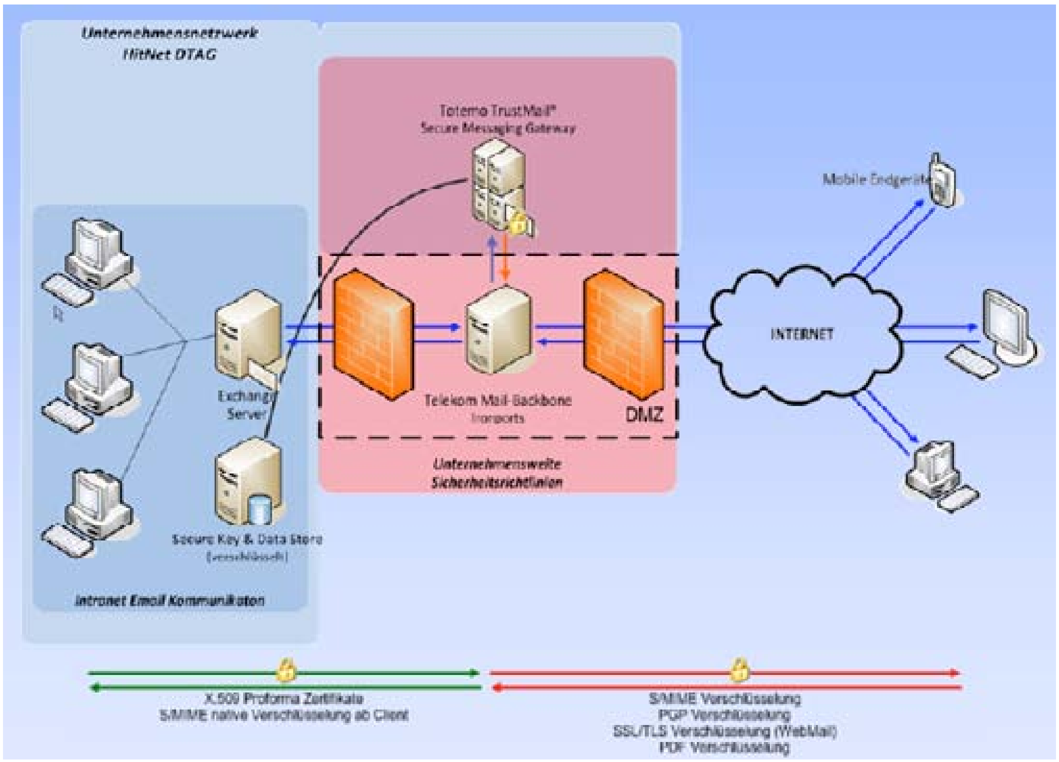


Figure 1: End-to-end encryption of e-mails

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.

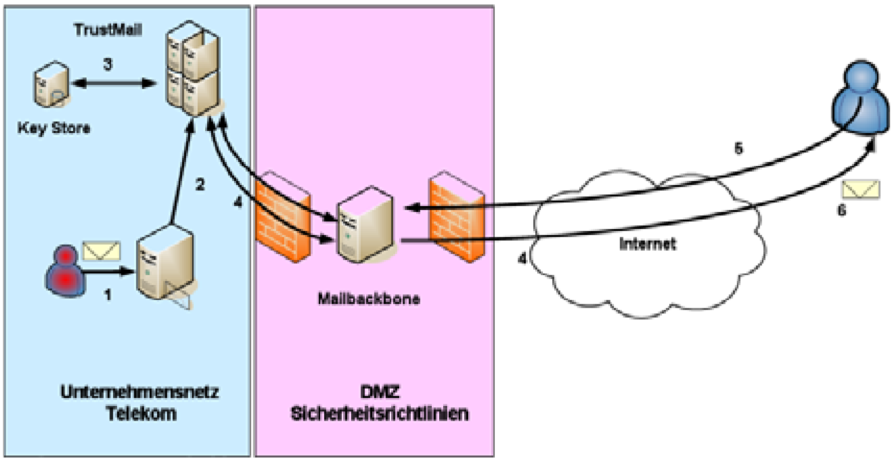
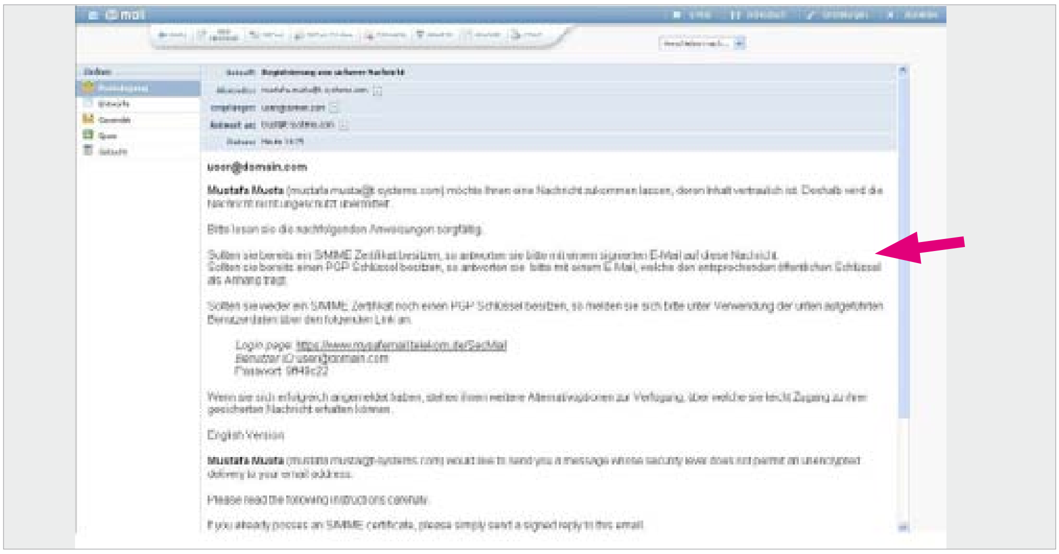


Figure 2: Mail flow with existing S/MIME encryption or PGP encryption keys

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.



user@domain.com

Mustafa Musta (mustafa.musta@t-systems.com) möchte Ihnen eine Nachricht zukommen lassen, deren Inhalt vertraulich ist. Deshalb wird die Nachricht nicht ungeschützt übermittelt.

Bitte lesen sie die nachfolgenden Anweisungen sorgfältig.

Sollten sie bereits ein S/MIME Zertifikat besitzen, so antworten sie bitte mit einem signierten E-Mail auf diese Nachricht.
Sollten sie bereits einen PGP Schlüssel besitzen, so antworten sie bitte mit einem E-Mail, welche den entsprechenden öffentlichen Schlüssel als Anhang trägt.

Sollten sie weder ein S/MIME Zertifikat noch einen PGP Schlüssel besitzen, so melden sie sich bitte unter Verwendung der unten aufgeführten Benutzerdaten über den folgenden Link an.

Login page: https://www.mysafemail.telekom.de/SecMail
Benutzer ID: user@domain.com
Passwort: 9f48c22

Wenn sie sich erfolgreich angemeldet haben, stehen Ihnen weitere Alternativoptionen zur Verfügung, über welche sie leicht Zugang zu dem gesicherten Nachricht erhalten können.

English Version

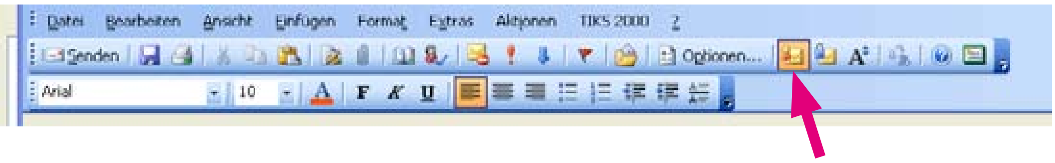
Mustafa Musta (mustafa.musta@t-systems.com) would like to send you a message whose security level does not permit an unencrypted delivery to your e-mail address.

Please read the following instructions carefully.

If you already posses an S/MIME certificate, please simply send a signed reply to this email.

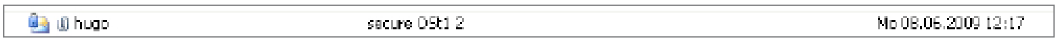
Figure 3: Notification for first-time registration

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.

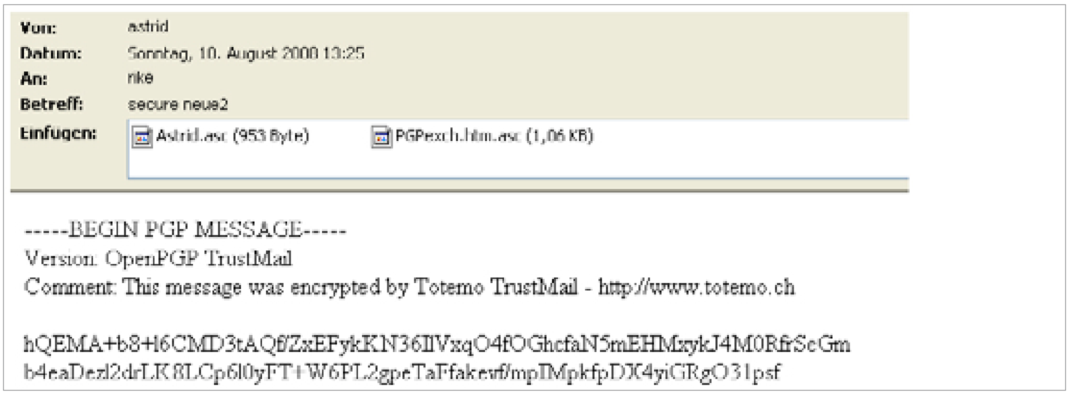
6. The E-Mail Encryption Gateway will verify the validity of the key information received and save the public key (S/MIME or PGP) in its Key Store.
7. The temporarily saved e-mail will now be encrypted and delivered based on either the S/MIME key technology indicated by the external user:



hugo secure 09t1 2 Mo 08.06.2009 12:17

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

Or the mail will be encrypted using PGP and delivered:



Von: astrid
Datum: Sonntag, 10. August 2008 13:25
An: rike
Betreff: secure neue2
Einfügen: Astrid.asc (953 Byte) PGPexch.htm.asc (1,06 KB)

```
-----BEGIN PGP MESSAGE-----
Version: OpenPGP TrustMail
Comment: This message was encrypted by Totemo TrustMail - http://www.totemo.ch

hQEMA+b8+l6CMD3tAQf/ZxEFykKN36lIVxqO4fOGhcfaN5mEHMzykJ4M0RfrSeGm
b4eaDezl2drLK8LCp6l0yFT+W6PL2gpeTaFfakewf/mpIMpkfpDX4yiGRgO31psf
```

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.

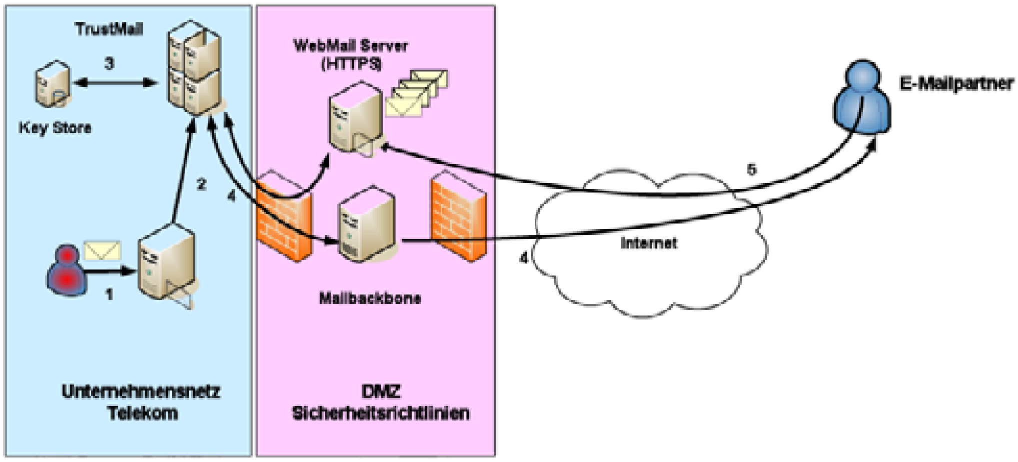
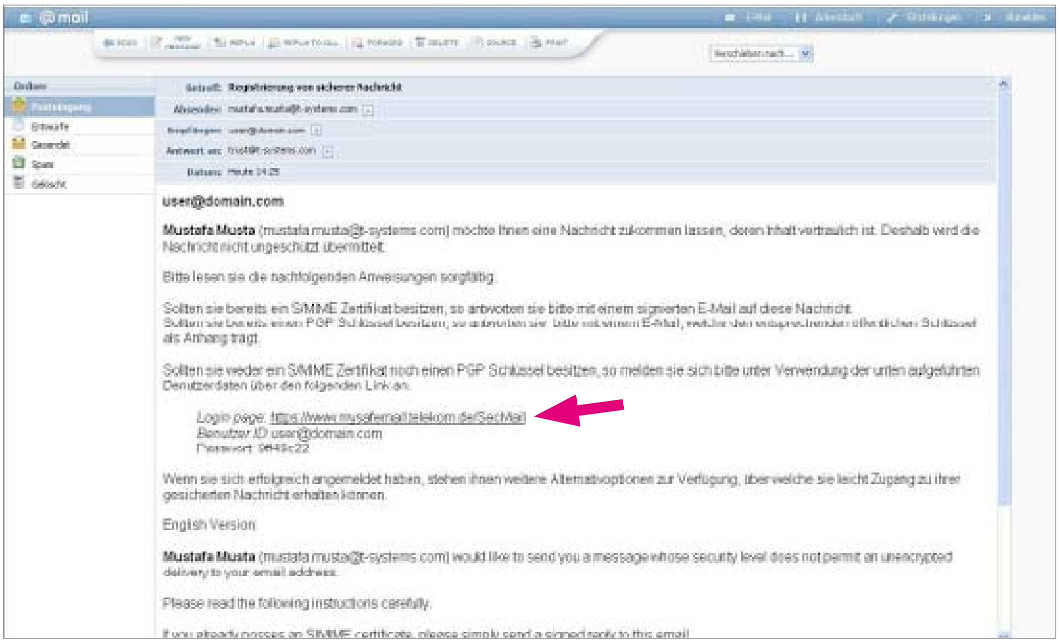


Figure 6: E-mail flow without an S/MIME or PGP key when using WebMail

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:



Betreff: Registrierung von sicherer Nachricht
Absender: mustafa.musta@t-systems.com
Empfänger: user@domain.com
Antwort an: trust@t-systems.com
Datum: Heute 14:25

user@domain.com

Mustafa Musta (mustafa.musta@t-systems.com) möchte Ihnen eine Nachricht zukommen lassen, deren Inhalt vertraulich ist. Deshalb wird die Nachricht nicht ungeschützt übermittelt.

Bitte lesen sie die nachfolgenden Anweisungen sorgfältig.

Sollten sie bereits ein S/MIME Zertifikat besitzen, so antworten sie bitte mit einem signierten E-Mail auf diese Nachricht.
Sollten sie bereits einen PGP Schlüssel besitzen, so antworten sie bitte mit einem E-Mail, welches den entsprechenden öffentlichen Schlüssel als Anhang trägt.

Sollten sie weder ein S/MIME Zertifikat noch einen PGP Schlüssel besitzen, so melden sie sich bitte unter Verwendung der unten aufgeführten Benutzerdaten über den folgenden Link an:

Login page: https://www.mysafemail.telekom.de/SecMail
Benutzer ID: user@domain.com
Passwort: 9f49c22

Wenn sie sich erfolgreich angemeldet haben, stehen ihnen weitere Alternativoptionen zur Verfügung, über welche sie leicht Zugang zu ihrer gesicherten Nachricht erhalten können.

English Version:

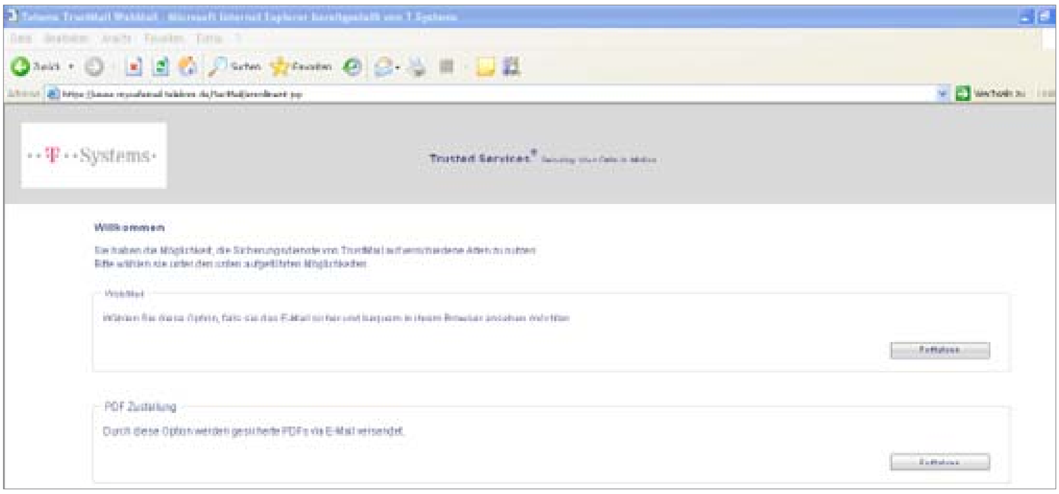
Mustafa Musta (mustafa.musta@t-systems.com) would like to send you a message whose security level does not permit an unencrypted delivery to your email address.

Please read the following instructions carefully.

If you already posses an S/MIME certificate, please simply send a signed reply to this email.

Figure 7: Notification for first-time registration

5. 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:



Willkommen

Sie haben die Möglichkeit, die Sicherungsdienste von TrustMail auf verschiedene Arten zu nutzen.
Bitte wählen sie unter den unten aufgeführten Möglichkeiten.

WebMail

Fortfahren

PDF Zustellung

Durch diese Option werden gesicherte PDFs via E-Mail versendet.

Fortfahren

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.

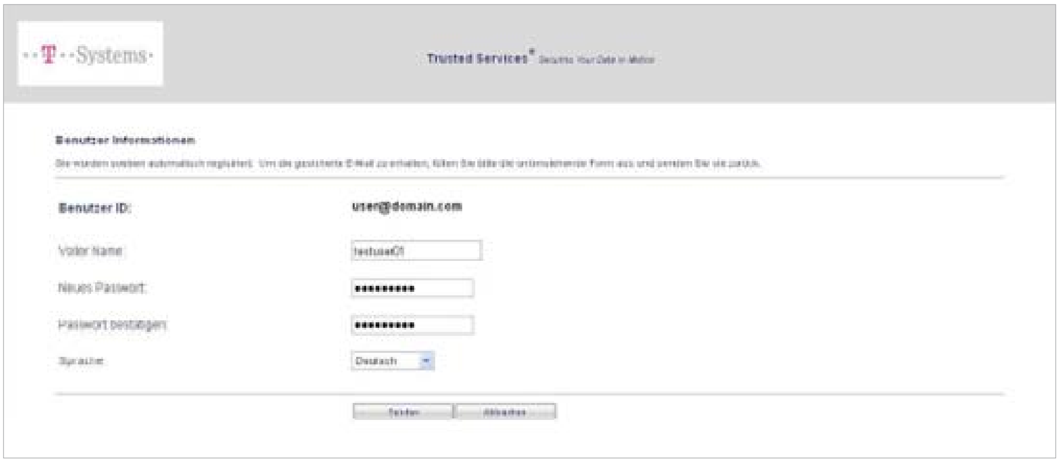
The "PDF delivery" option means that the sent e-mail and any attachments will be converted into a PDF file and encrypted with a password previously specified by the user. This PDF file will then be delivered to the external contact via e-mail. All future e-mails sent by internal employees of Deutsche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



Benutzer Informationen

Sie wurden soeben automatisch registriert. Um die gesicherte E-Mail zu erhalten, füllen Sie bitte die untenstehende Form aus und senden Sie sie zurück.

Benutzer ID: user@domain.com

Voller Name: testuser01

Neues Passwort: ••••••••••

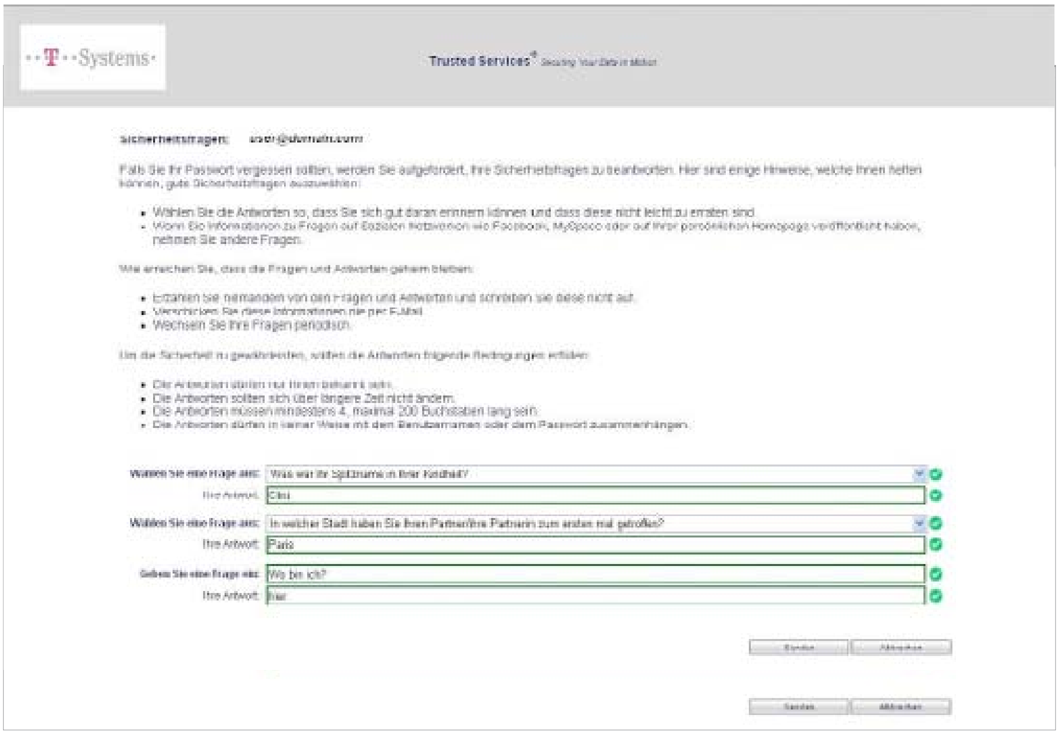
Passwort bestätigen: ••••••••••

Sprache: Deutsch

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.



Sicherheitsfragen: user@domain.com

Falls Sie Ihr Passwort vergessen sollten, werden Sie aufgefordert, Ihre Sicherheitsfragen zu beantworten. Hier sind einige Hinweise, welche Ihnen helfen können, gute Sicherheitsfragen auszuwählen:

- Wählen Sie die Antworten so, dass Sie sich gut daran erinnern können und dass diese nicht leicht zu erraten sind.
- Wenn Sie Informationen zu Fragen auf Sozialen Netzwerken wie Facebook, MySpace oder auf Ihrer persönlichen Homepage veröffentlicht haben, nehmen Sie andere Fragen.

Wie erreichen Sie, dass die Fragen und Antworten geheim bleiben:

- Erzählen Sie niemandem von den Fragen und Antworten und schreiben Sie diese nicht auf.
- Verschicken Sie diese Informationen nie per E-Mail.
- Wechseln Sie Ihre Fragen periodisch.

Um die Sicherheit zu gewährleisten, sollten die Antworten folgende Bedingungen erfüllen:

- Die Antworten dürfen nur Ihnen bekannt sein.
- Die Antworten sollten sich über längere Zeit nicht ändern.
- Die Antworten müssen mindestens 4, maximal 200 Buchstaben lang sein.
- Die Antworten dürfen in keiner Weise mit dem Benutzernamen oder dem Passwort zusammenhängen.

Wählen Sie eine Frage aus: Was war Ihr Spitzname in Ihrer Kindheit?

Ihre Antwort: Cini

Wählen Sie eine Frage aus: In welcher Stadt haben Sie Ihren Partner/Ihre Partnerin zum ersten mal getroffen?

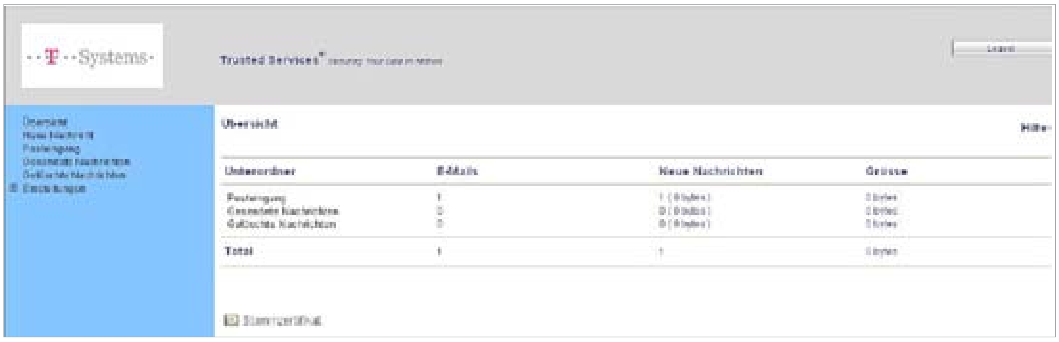
Ihre Antwort: Paris

Geben Sie eine Frage ein: Wo bin ich?

Ihre Antwort: hier

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:



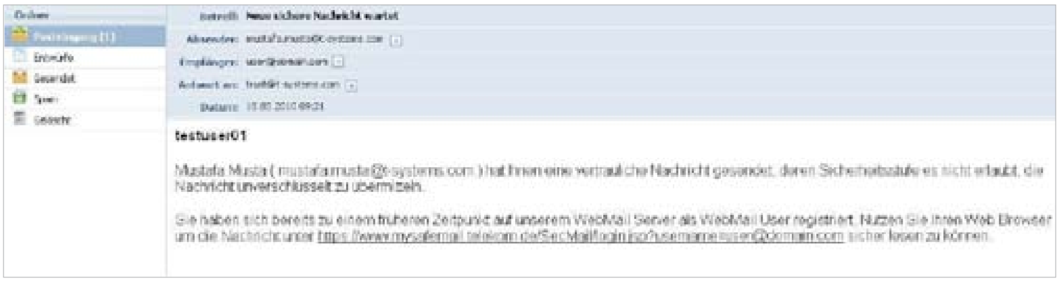
Übersicht

Unterordner	E-Mails	Neue Nachrichten	Grösse
Posteingang	1	1 (0 bytes)	0 bytes
Gesendete Nachrichten	0	0 (0 bytes)	0 bytes
Gelöschte Nachrichten	0	0 (0 bytes)	0 bytes
Total	1	1	0 bytes

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:



Betreff: Neue sichere Nachricht wartet
Absender: mustafa.musta@t-systems.com
Empfänger: user@domain.com
Antwort an: trust@t-systems.com
Datum: 15.03.2010 09:21

testuser01

Mustafa Musta (mustafa.musta@t-systems.com) hat Ihnen eine vertrauliche Nachricht gesendet, deren Sicherheitsstufe es nicht erlaubt, die Nachricht unverschlüsselt zu übermitteln.

Sie haben sich bereits zu einem früheren Zeitpunkt auf unserem WebMail Server als WebMail User registriert. Nutzen Sie Ihren Web Browser um die Nachricht unter https://www.mysafemail.telekom.de/SecMailLogin.jsp?username=user@domain.com sicher lesen zu können.

Figure 12: Notification of delivered WebMail

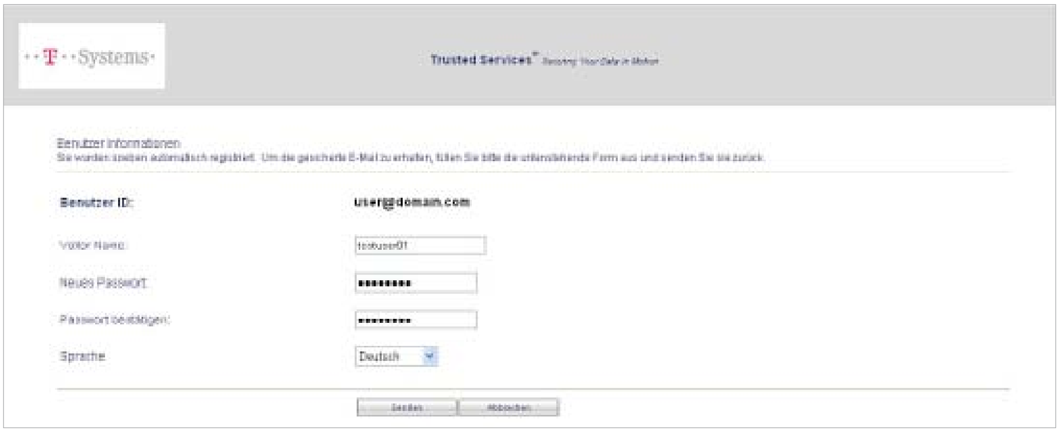
⚠ **The external contact can use WebMail to send a new e-mail only to internal employees or functional mailboxes at Deutsche Telekom. In addition, only internal employees or automated mailboxes can be added to a reply to the sent e-mail. This restriction is intended to prevent abuse of the WebMail application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

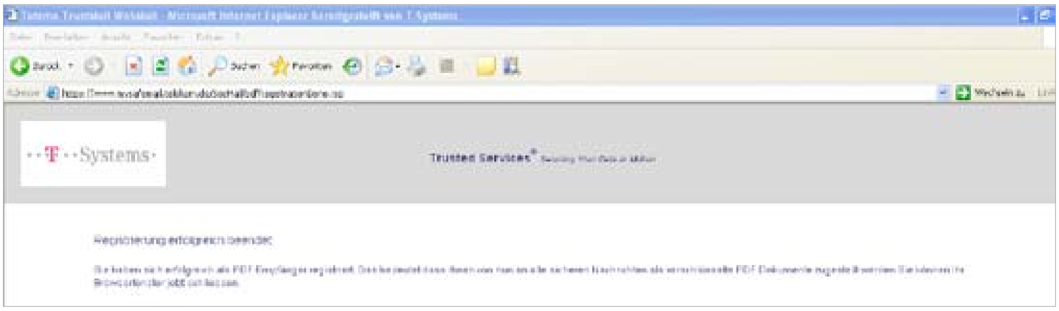


Benutzer Informationen
Sie wurden soeben automatisch registriert. Um die gesicherte E-Mail zu erhalten, füllen Sie bitte die untenstehende Form aus und senden Sie sie zurück.

Benutzer ID: user@domain.com
Voller Name: testuser01
Neues Passwort: ••••••••
Passwort bestätigen: •••••••••
Sprache: Deutsch

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:

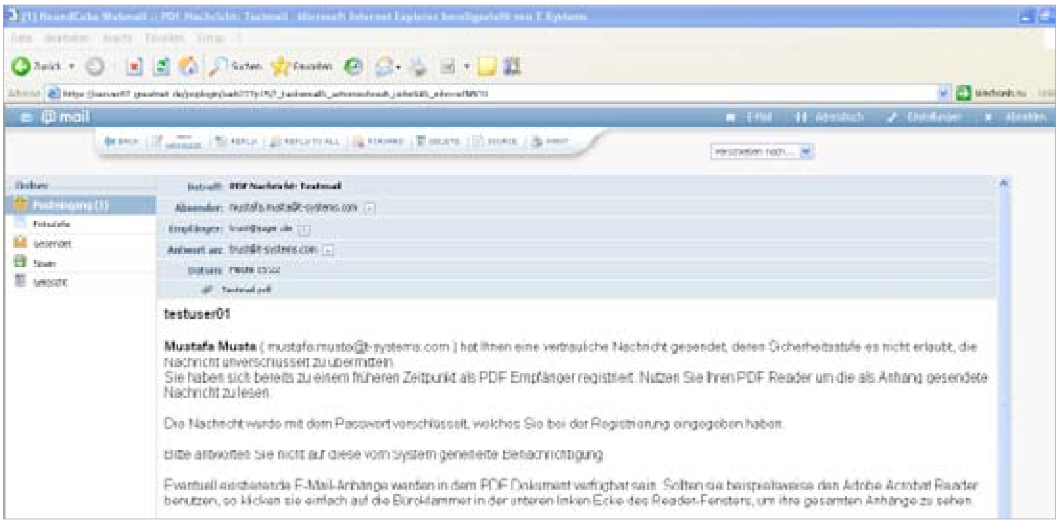


Registrierung erfolgreich beendet

Sie haben sich erfolgreich als PDF Empfänger registriert. Das bedeutet dass Ihnen von nun an alle sicheren Nachrichten als verschlüsselte PDF Dokumente zugestellt werden. Sie können Ihr Browserfenster jetzt schließen.

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.



Betreff: PDF Nachricht: Testmail
Absender: mustafa.musta@t-systems.com
Empfänger: trust@sage.de
Antwort an: trust@t-systems.com
Datum: Heute 13:22
Testmail.pdf

testuser01

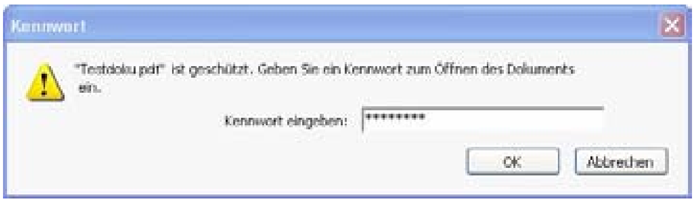
Mustafa Musta (mustafa.musta@t-systems.com) hat Ihnen eine vertrauliche Nachricht gesendet, deren Sicherheitsstufe es nicht erlaubt, die Nachricht unverschlüsselt zu übermitteln.
Sie haben sich bereits zu einem früheren Zeitpunkt als PDF Empfänger registriert. Nutzen Sie Ihren PDF Reader um die als Anhang gesendete Nachricht zu lesen.

Die Nachricht wurde mit dem Passwort verschlüsselt, welches Sie bei der Registrierung eingegeben haben.

Bitte antworten Sie nicht auf diese vom System generierte Benachrichtigung.

Eventuell existierende E-Mail-Anhänge werden in dem PDF Dokument verfügbar sein. Sollten sie beispielsweise den Adobe Acrobat Reader benutzen, so klicken sie einfach auf die Büroklammer in der unteren linken Ecke des Reader-Fensters, um ihre gesamten Anhänge zu sehen.

Figure 15: Receiving PDFs 1



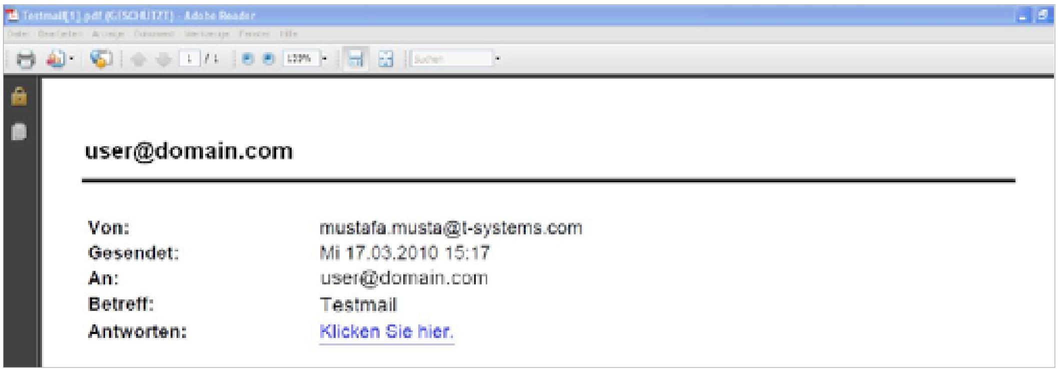
"Testdoku.pdf" ist geschützt. Geben Sie ein Kennwort zum Öffnen des Dokuments ein.

Kennwort eingeben: *********

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:


Testmail[1].pdf (GESCHÜTZT) - Adobe Reader
Datei Bearbeiten Anzeige Dokument Werkzeuge Fenster Hilfe
1 / 1
Suchen

user@domain.com

Von:	mustafa.musta@t-systems.com
Gesendet:	Mi 17.03.2010 15:17
An:	user@domain.com
Betreff:	Testmail
Antworten:	Klicken Sie hier.

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:

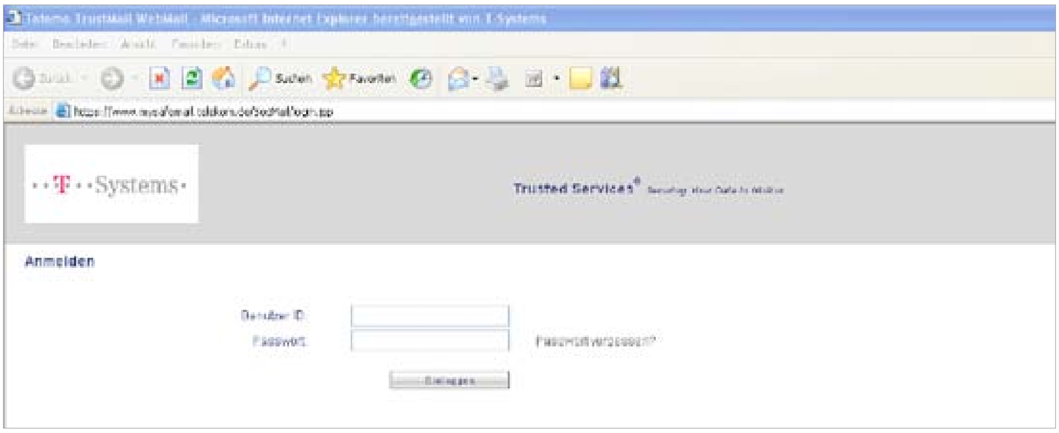
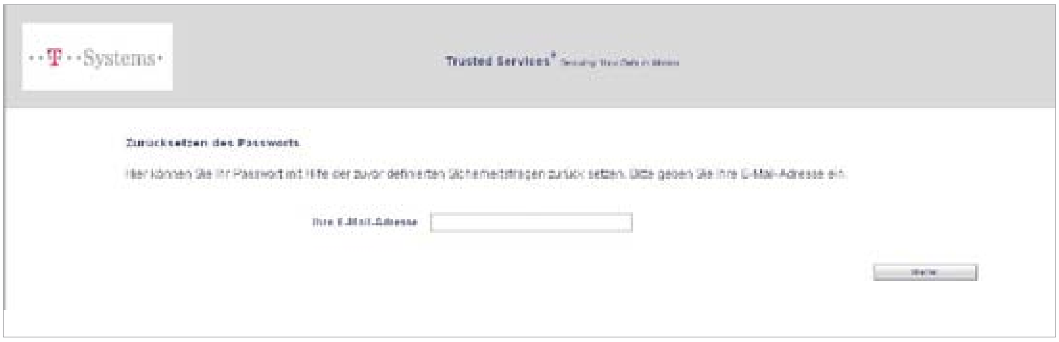

TeleMail TrustMail WebMail - Microsoft Internet Explorer bereitgestellt von T-Systems
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Adresse
T-Systems
Trusted Services® Securing Your Data in Motion
Anmelden
Benutzer ID
Passwort
Passwort vergessen?
Einloggen

Figure 18: Initiating password reset process

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

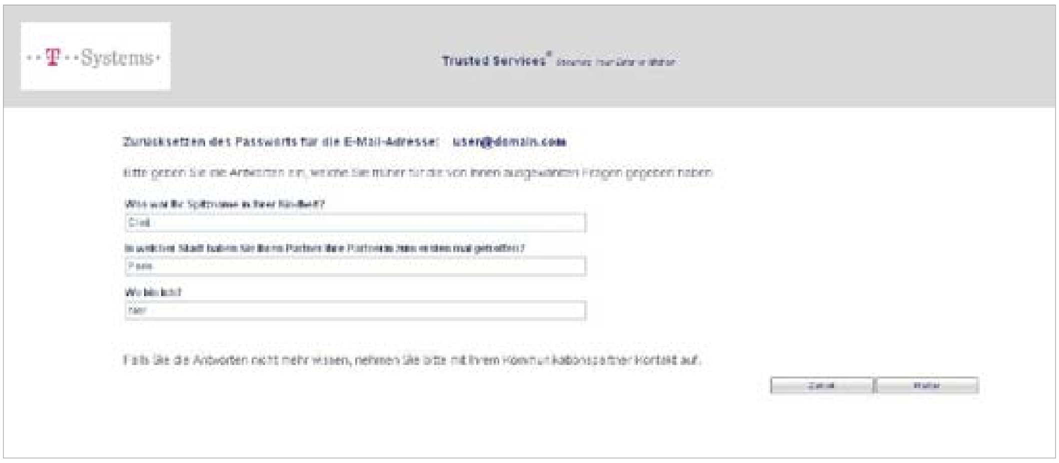


Zurücksetzen des Passworts

Hier können Sie Ihr Passwort mit Hilfe der zuvor definierten Sicherheitsfragen zurück setzen. Bitte geben Sie Ihre E-Mail-Adresse ein.

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:



Trusted Services® Securing Your Data in Motion

Zurücksetzen des Passworts für die E-Mail-Adresse: user@domain.com

Bitte geben Sie die Antworten ein, welche Sie früher für die von Ihnen ausgewählten Fragen gegeben haben.

Wie war Ihr Spitzname in Ihrer Kindheit?
Chili

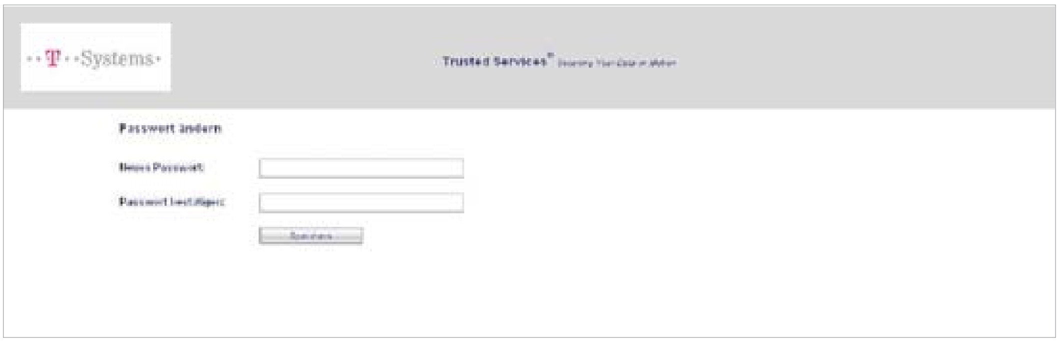
In welcher Stadt haben Sie Ihren Partner/Ihre Partnerin zum ersten mal getroffen?
Paris

Wo bin ich?
hier

Falls Sie die Antworten nicht mehr wissen, nehmen Sie bitte mit Ihrem Kommunikationspartner Kontakt auf.

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:



Trusted Services® Securing Your Data in Motion

Passwort ändern

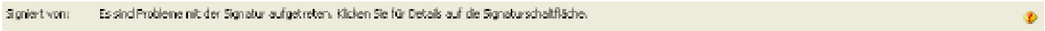
Neues Passwort:

Passwort bestätigen:

Figure 21: Specifying a new password

Announcement by the Issuing CA.

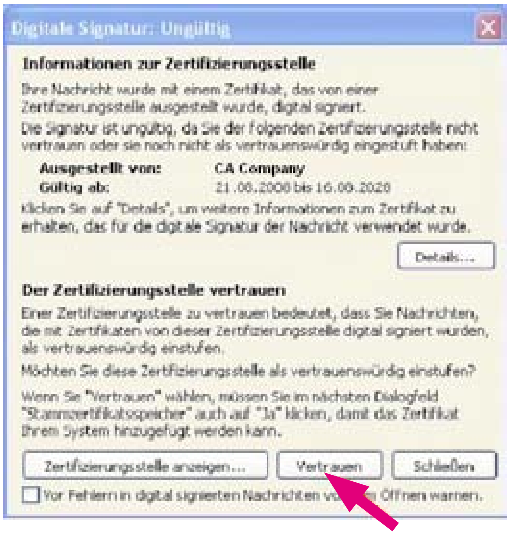
The external user may receive warnings regarding the signature. This can happen if the e-mail client of the external user does not recognize the certification center (Deutsche Telekom TrustCenter) that issued the internal employee certificate.



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:



Digitale Signatur: Ungültig

Informationen zur Zertifizierungsstelle

Ihre Nachricht wurde mit einem Zertifikat, das von einer Zertifizierungsstelle ausgestellt wurde, digital signiert.

Die Signatur ist ungültig, da Sie der folgenden Zertifizierungsstelle nicht vertrauen oder sie noch nicht als vertrauenswürdig eingestuft haben:

Ausgestellt von: CA Company
Gültig ab: 21.08.2008 bis 16.08.2028

Klicken Sie auf "Details", um weitere Informationen zum Zertifikat zu erhalten, das für die digitale Signatur der Nachricht verwendet wurde.

Der Zertifizierungsstelle vertrauen

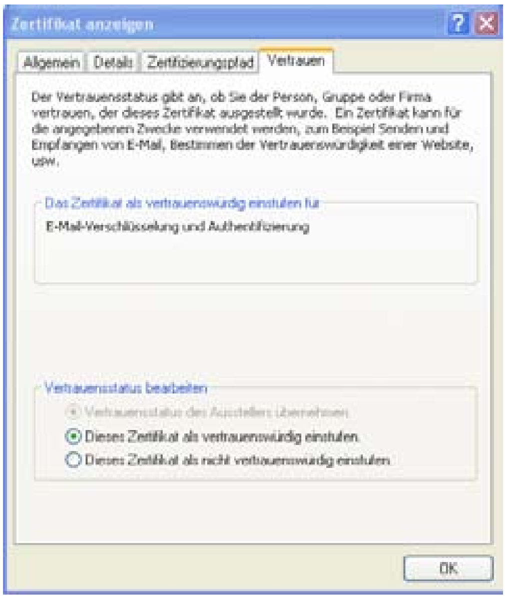
Einer Zertifizierungsstelle zu vertrauen bedeutet, dass Sie Nachrichten, die mit Zertifikaten von dieser Zertifizierungsstelle digital signiert wurden, als vertrauenswürdig einstufen.

Möchten Sie diese Zertifizierungsstelle als vertrauenswürdig einstufen?

Wenn Sie "Vertrauen" wählen, müssen Sie im nächsten Dialogfeld "Stammzertifikatsspeicher" auch auf "Ja" klicken, damit das Zertifikat Ihrem System hinzugefügt werden kann.

□ Vor Fehlern in digital signierten Nachrichten vor dem Öffnen warnen.

At this point the certification center must be trusted:



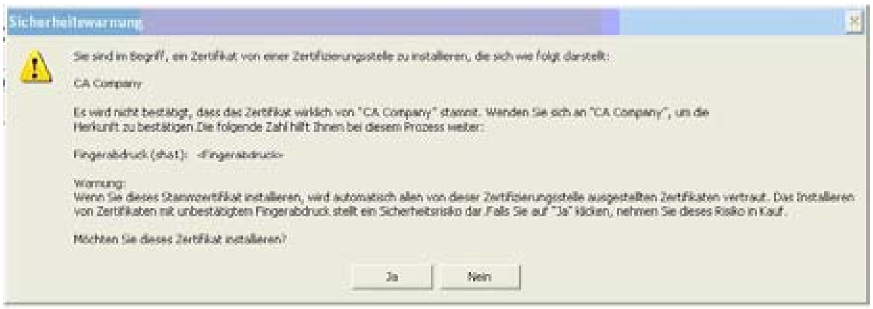
Zertifikat anzeigen

Der Vertrauensstatus gibt an, ob Sie der Person, Gruppe oder Firma vertrauen, der dieses Zertifikat ausgestellt wurde. Ein Zertifikat kann für die angegebenen Zwecke verwendet werden, zum Beispiel Senden und Empfangen von E-Mail, Bestimmen der Vertrauenswürdigkeit einer Website, usw.

Das Zertifikat als vertrauenswürdig einstufen für
E-Mail-Verschlüsselung und Authentifizierung

Vertrauensstatus bearbeiten
○ Vertrauensstatus des Ausstellers übernehmen
● Dieses Zertifikat als vertrauenswürdig einstufen
○ Dieses Zertifikat als nicht vertrauenswürdig einstufen

This must then be confirmed:



Sie sind im Begriff, ein Zertifikat von einer Zertifizierungsstelle zu installieren, die sich wie folgt darstellt:

CA Company

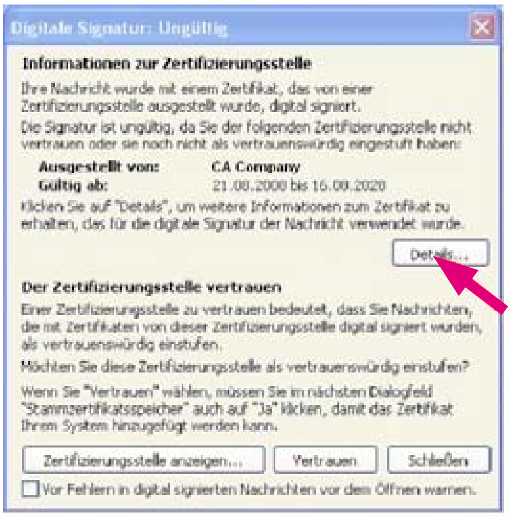
Es wird nicht bestätigt, dass das Zertifikat wirklich von "CA Company" stammt. Wenden Sie sich an "CA Company", um die Herkunft zu bestätigen Die folgende Zahl hilft Ihnen bei diesem Prozess weiter:

Fingerabdruck (sha1): <Fingerabdruck>

Warnung:
Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen von dieser Zertifizierungsstelle ausgestellten Zertifikaten vertraut. Das Installieren von Zertifikaten mit unbestätigten Fingerabdruck stellt ein Sicherheitsrisiko dar.Falls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf.

Möchten Sie dieses Zertifikat installieren?

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



Informationen zur Zertifizierungsstelle

Ihre Nachricht wurde mit einem Zertifikat, das von einer Zertifizierungsstelle ausgestellt wurde, digital signiert.
Die Signatur ist ungültig, da Sie der folgenden Zertifizierungsstelle nicht vertrauen oder sie noch nicht als vertrauenswürdig eingestuft haben:

Ausgestellt von: CA Company
Gültig ab: 21.08.2000 bis 16.08.2020

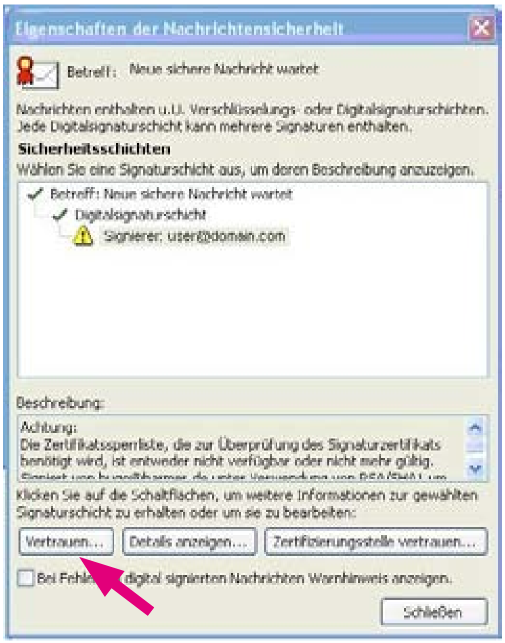
Klicken Sie auf "Details", um weitere Informationen zum Zertifikat zu erhalten, das für die digitale Signatur der Nachricht verwendet wurde.

Der Zertifizierungsstelle vertrauen

Einer Zertifizierungsstelle zu vertrauen bedeutet, dass Sie Nachrichten, die mit Zertifikaten von dieser Zertifizierungsstelle digital signiert wurden, als vertrauenswürdig einstufen.
Möchten Sie diese Zertifizierungsstelle als vertrauenswürdig einstufen?
Wenn Sie "Vertrauen" wählen, müssen Sie im nächsten Dialogfeld "Stammzertifikatsspeicher" auch auf "Ja" klicken, damit das Zertifikat Ihrem System hinzugefügt werden kann.

□ Vor Fehlern in digital signierten Nachrichten vor dem Öffnen warnen.

Then click the "Trust" button:



Betreff: Neue sichere Nachricht wartet

Nachrichten enthalten u.U. Verschlüsselungs- oder Digitalsignaturschichten. Jede Digitalsignaturschicht kann mehrere Signaturen enthalten.

Sicherheitsschichten

Wählen Sie eine Signaturschicht aus, um deren Beschreibung anzuzeigen.

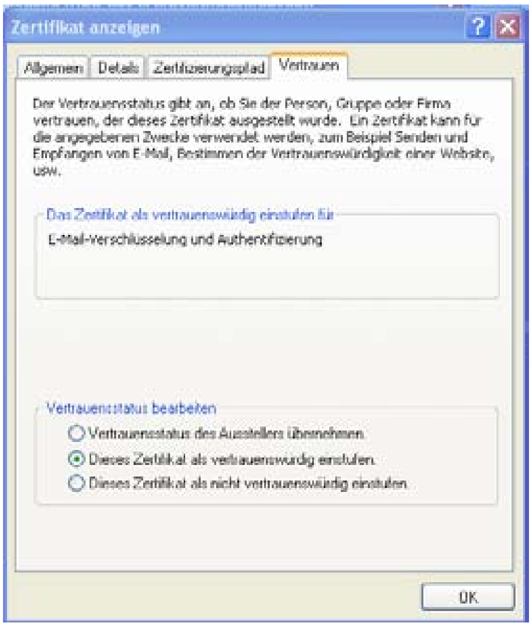
- ✓ Betreff: Neue sichere Nachricht wartet
  - ✓ Digitalsignaturschicht
    - ⚠ Signierer: user@domain.com

Beschreibung:

Achtung:
Die Zertifikatssperrliste, die zur Überprüfung des Signaturzertifikats benötigt wird, ist entweder nicht verfügbar oder nicht mehr gültig.

Klicken Sie auf die Schaltflächen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten:

□ Bei Fehlern in digital signierten Nachrichten Warnhinweis anzeigen.



Zertifikat anzeigen

Der Vertrauensstatus gibt an, ob Sie der Person, Gruppe oder Firma vertrauen, der dieses Zertifikat ausgestellt wurde. Ein Zertifikat kann für die angegebenen Zwecke verwendet werden, zum Beispiel Senden und Empfangen von E-Mail, Bestimmen der Vertrauenswürdigkeit einer Website, usw.

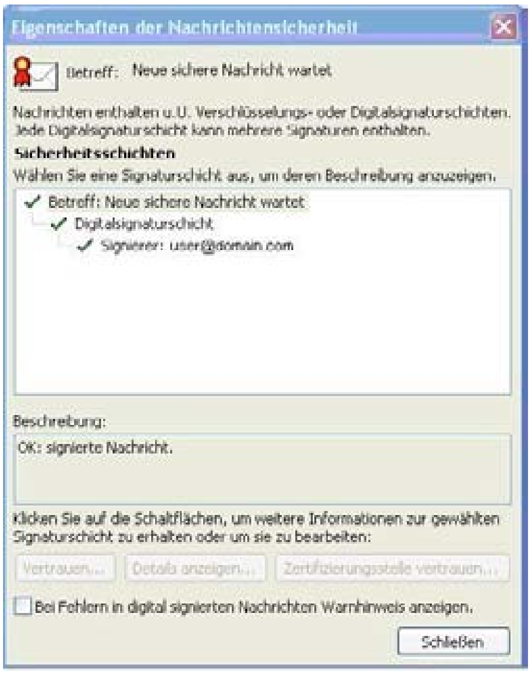
Das Zertifikat als vertrauenswürdig einstufen für

E-Mail-Verschlüsselung und Authentifizierung

Vertrauensstatus bearbeiten

○ Vertrauensstatus des Ausstellers übernehmen
● Dieses Zertifikat als vertrauenswürdig einstufen.
○ Dieses Zertifikat als nicht vertrauenswürdig einstufen.

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:



Eigenschaften der Nachrichtensicherheit

Betreff: Neue sichere Nachricht wartet

Nachrichten enthalten u.U. Verschlüsselungs- oder Digitalsignaturschichten. Jede Digitalsignaturschicht kann mehrere Signaturen enthalten.

Sicherheitsschichten

Wählen Sie eine Signaturschicht aus, um deren Beschreibung anzuzeigen.

✓ Betreff: Neue sichere Nachricht wartet
  ✓ Digitalsignaturschicht
    ✓ Signierer: user@domain.com

Beschreibung:

OK: signierte Nachricht.

Klicken Sie auf die Schaltflächen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten:

□ Bei Fehlern in digital signierten Nachrichten Warnhinweis anzeigen.

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