Office Standardization. E-Mail Encryption Gateway.

Instructions for external communication Partners.



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.	
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. Receiving and sending e-mails using WebMail. Receiving and sending e-mails using PushedPDF.	
Password Reset.	14
Announcement by the Issuing CA.	
Troubleshooting	19
List of abbreviations.	

Table of Figures

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	
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.

Case 1: S/MIME certificate or PGP key is available.



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.

: D	stel Ber	rbeiten	Ansicht	Enfügen	Format	Egtras	Aktionen	TIKS 2000	2					
	ISenden		18 0	2 2	1100	8.13	1 4	* 🙆	0	ptionen	E	At an	0 🖿	
An	al		- 10	• <u>A</u>	F K	U 📕	==;	三三律	理会					

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	sacure OSt1 2	Mp 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: Datum: An: Betreff:	astrid Sonnhag, 10. August 2000 13:25 rike 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							
b4eaDezl2	drLK8LCp6l0yFT+W6PL2gpeTaFfakevf/mpIMpkfpDX4yiGRgO31psf						



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:

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



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:

👌 Selece Trendal Webber, Nicrosoft Internet Laple		- 6
first destates waits Trankes Tirtle 1		
🗿 Anis + 🔘 🔳 🔮 🐔 🔎 Satur 👷	frantes 🙆 🔗 🛬 🖩 🔛 🗱	
1844 China (Lana reputational tablets duffer Hallistochart	*	👻 🔂 Viettolitzi 💷
・・中・·Systems・	Trusted Services [®] Jacoby the fails a Miller	
Willie anwein Die talen, die Wojschief, die Sicherungste Bite wählen nie unter der unter aufgeführt Wijsblief Wijsblief Wijsblief	ennde von Thurdfäll auf annum anderen Aden zu nieben m Kinglichteiden Balt sin har und Hanguare, in Huare Rimachar ansahan Welchtan	
- POF Zistalian		Pathone
Durch diese Option werden gesicherte Pr	Ft vis E-Mail reiserdet.	
		E-Malazza (

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:

enutzer Informationen		
e warden andere entersellach regisitiet.	Um die gestaterie 2 Mail zu erheiten, Gilen Sie bille die antimakrienie Farm aus und sendern Die als zeröch.	
Senutzer ID:	user@domain.com	
/oler Name:	testuseOI	
Neues Passwort.	*******	
registed trowless		
luraine	Deutach -	

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.

	Trusted Services [®] away your day in adduct
Sicherheitstragen;	anti-jodomain.aum
Fals Sie fir Passwort ver konnen, gute Sicherheits	ngessen sollten, werden Sie aufgefürdert, hine Sicherheitstragen zu teanbiorten. Her sind einige Hirweise, welche Innen helten iftigen auszuwählten
 Wählen Bie die An Worm Bie Informatinehmen Sie ander 	fworten so, dass Sie sich gut daran ernnern lidinnen und dass dese nicht leicht zu erraten sind tonon zu Fragen ouf Euzalen Nictiwenen we Footboaw, MySpece daer auf Inter persönischen Homopoge veröffortfaht haloor, re Fragen.
We erreichen Sie, dass r	de Fragen und Astworten geheim bleben
 Erzählen Sie nemi Verschücken Rie nä Wechsein Sie hire 	andom von den ≻fagen und Adtworten und schneiten isie delse nicht auf. Heigen periodisch.
Um die Schechell nu gew	skhrieisten, wilten die Artwinsten frigende Rectingungen erfüllen
Dis Anteusian usur Dis Anteusian solt	ler na frem bekank jeln. En sich Ger Briser Zell nicht ändern.
Die Anbronten müs Die Anbronten dünt	ssen mindestens 4., mainai 200 Buchtsben lang sehr. Ian In Samar Maisa m5 dan Banubamaman odar Jam Pasakort zusammenhängen.
Die Anbiorten mos Die Anbiorten dürf Watters sie eine mage ale	ssen mindestens 4, marinal 200 Buchtsben lang sehr Inn in isanar Waisa mit den Benutzamanen oder dem Pasiword zusammenhängen.
Die Anthroffen müs Die Anthroffen müs Watten Sie ette ette Frage alle lier Antre	ssen mindestens 4, marinal 200 Buchtsben lang sehr Inn in isanar Waisa mit den Bendbarnamen oder dem Paseword zusammenhängen. Im Was warite Spitzname in Iter Kostheit?
Oile Antheorien mice Oile Antheorien don wantee Sie encorrage au lite Anteo Waters Sie encorrage au	ssen mindestens 2, maximal 200 Buchtsbein lang sehr Inn in seiner Weise mit dem Benutzernamen oder dem Paseword zusernmenhängen. Im Weise war ihr Spitzname in Ihrer Kostheit/ Constraint Constraint (Constraint) Im Eteil Constraint Constraint Pathen/Ime P
Die Anthronten mus Die Anthronten dan Wallien Sie eine mage all Die Anthro Wählen Sie eine Frage all Die Anthro	ssen mindestens 2, maximal 200 Buchtsbein lang sehl Inn In samar Wasa mit dem Benutzernamen oder dem Paseword zusammenhängen. Im Wasa war ihr Spitznume in Iher Kostheit? Im Einei Im wichter Stadt haben Sie Ihen Pathen/ihre Patherin zum ersten mal getroffes? Im Paria
Die Anthonfern müs- Die Anthonfern dürf Watten Sie eine mage all Die Anthon Wählen Sie eine Frage all Dire Anthon Geben Sie eine frage all	ssen mindestens 2, marinal 200 Buchtsbein lang sehl ten in isanar Weise mit dem Benutzernamen oder dem Paceword zusammenhängen. 15. Weise wir tri Spitzname in Iher Kesthet? <u> </u>
Die Anthronten mus Die Anthronten dan Wallies Sie eine mage all Die Anthro Wallies Sie eine Frage all Die Anthro Galves Sie eine frage all Die Anthro	ssen mindestens 2, maximal 200 Buchtstein lang sehl ten in isanar Wasa mit den Bendzemannen oder dem Paseword zusammenhängen. 15. Was warter Spitznumein Iher Kosthet/ 14. Etei 15. In wichter Stadt haben Sie Ihen Pather/ihre Patherin zum enten mit getroßes? 15. Parlo 16. Mit 00000000000000000000000000000000000
Die Anthronten müs Die Anthronten dür Wannen Sie eine Hrage als Die Anthro Wählen Sie eine Trage als Die Anthro Geben Sie eine Trage als Die Anthro	ssen mindesters & , maximal 200 Buchtsbein lang sehl fen in samer Weise mit dem Benubarmannen oder dem Paseword zusammenhängen. 15. Veis veriter spitzname in Iher Kesthelf?
Die Antibiothern müs- bei Antibiothern dürf Watten Sie eine strage als Fliet Antibio Wählten Sie eine Frage an Thre Antibio Gebes Sie eine finage an Hitre Antibio	ssen min besters 2, marinai 200 Buchtstein lang seht fan in samar Wase mit den Bendzerrannen oder dem Paseword zusensteinhängen. ** Vres ver ihr Spitzname in Iter Kathet/ ** Eitei ** In webber Statt haben Sie Itern Patterithe Patrierin zum enten mal getroßen? ** Paris #* Mo bin (bh? ** pier

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:

··· Ŧ··· Systems·	Trusted Services [®] survey har	ana m Mitrori		6	Leave
Otomane Muse Harders III Pasterspace	Ubersicht		Hille		
Oceaning fouriers term Gell is the the third bion	United or driver	B-Mails	Neue Nachrichten	Grüsse	
di Encisitungun	Pesteingung Gesenstein Kachtoben Gulbochts Kachtichton	1	(0) 0) 0) 0) 0) 0) 0) 0) 0) 0) 0)	0 bries 0 bries 1 bries	
	Total	,	(1	Ebytes	
	E Starriger (1)-4.				

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:

vien mutalaruntakontana am () apre: werkkonstaan ()
gn: wr@enstors
days 11 87 2510 99-21
er01:
la Musta (mustafauruste@-systems.com.) hat Innen eine vertrauliche Nachricht gesendet, deren Sicherheitsatule es nicht erlaubt, die icht unverschlusseit zu ubermizeln.
ben sich bereft zu einem früheren Zeitpunkt auf unserem WebMail Server als WebMail User registniert. Nutzen Sie Ihren Web Browser • Nacht cht unter <u>https://www.mysafemail.telekom de/SecMailfogin ko/tusemame.kuser@dommin.com</u> .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:

••• Ŧ•••Systems•	Trusted Services [®] densing the data Admin	
Benußzer informationen Sie wurden solden ektimatisch registriet	Um die geschiefte 5-Mailzu erheiten, tilten Sie bilte die orfernstellende Form aus und sierden Sie tie zurlick.	
Benutzer ID:	usergidomain.com	
Votor Naveo	testusedt	
Neues Passwort		
Plasswort de statigen:		
Sprache	Deutsch 🛩	
	Tender Modelser	2

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:

🖀 Tatara Teamiali Watalat - Nicesya B Internet	Explorer Arringentially was 1 Systems	- 0
Sales Translation Analy Parallel Private T		
🔇 aval. + 🔘 - 💽 🛋 🐔 🔎 autor	👷 Faradan 🕘 🌐 - 🍒 💷 🛄 🛄	
tores a here I wood walteblands Sechalted	apphalar Sorie na	🖂 🛃 Medisela 2. 11-1
$\cdots \Psi \cdots \mathrm{Systems} \cdot$	Trusted Services [®] terms the base allow	
Replicierung erfogreich beend Bie kolen sich erfogreich als PDF B	R. Ingling is registrat. Disk be justif dass fluetions fau to ale ticheer Hadrichtes als einstriken elle PDF Dekoverie e	ugende Browersiaan (Lie Johnstein (Te
Browneller job on lacton.		

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.

ing destrict seat	te Talastes, Torne -1			
C test + C	🔹 🛃 🐔 💭 Sates 👷 Gaudes 🥝 ⊘ + 🍒 🗟 + 🔂 🔛			
Antonia Station (Joanna)	دەقەر بەتەرىيە تەتەر قىيەتىيەت بەتەر قىيەت بەتەر ئايەتەر ئېچىتەر بەتەر بەتەر يەرىخى بەتەر يەت		🔁 Machanikani 🛛 Ir	
😑 🗇 mail		w E-ful al Admittant 2 Database	en 16 allenbier	
	en Stream (Banch Banchilder Stender Banch Banch Banch	versitivetives reads		
lister	Industria PER National Contemport		*	
😫 Posteliaina (1)	Absender: Rettifts net site or an			
Fritsdafe	freedenger: tradigeograde []]			
sesencer.	Andmunt wei trieblikt sisterik (UM 💽			
la taves	Datain: Peda 2022			
e secol	# Tantanal pri			
	testuser01			
	Mustafe Muste (mustaformusto@brysterns.com) hot lithen eine vertrauliche Nachri Nachricht unverschussent zu übermitten Sie haben sich bereits zu einem früheren Zeitpunlid als PDF Empfänger registriert. N Nachricht zu lesen	cht gesondet, denen Sicherholtsstufe es nicht erlaub utzen Sie Ihren PDF Reader um die als Ashang ges	r, die endete	
	Die Nachricht wurde mit dem Passwert verschlüsselt, welches Sie bei der Registrierung eingegeben haben.			
	Bite artworten Sie nicht auf diese vom System generente Benachrichtigung			
	Eventuell existentende F-Mail-Arbänge wenden in dem PCF Dokument verfügbet sei berutzen, so käcken sie einfach auf die Eurokämmer in der unteren inken Ecke des	n Solten sie beispielsweise den Adobe Acrobet Re Reader Fensters, um ihre gesamten Anhänge zu se	ader hon	

Figure 15: Receiving PDFs 1

the second				14
ein.	f" ist geschützt. Geben Sie ein H	Cennwort zum (Offnen des Dokum	ents
	Kennwort einnehen:			
	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 Web-Mail. 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:

2 Teterre Trustweil Webstell - Mb	crossff Internet Explorer herefigestellt von 1-Systems
Sele Beabeler Wealt Provide	r Eduar (1
() aval + () + 💌 🖉 (🟠 🔎 Suchen 👷 Favoriten 🐵 🎧 - 🌺 🗃 - 🧫 🛍
Altheode 🗿 house lineer mys afore all told	lon.defodhelfodh.pp
••• T ••Systems•	Trissted Services [®] Security Hardon Advances
Anmelden	Denutiner D Passwort Passwort verbssourt?

Figure 18: Initiating password reset process

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

・・ 罪・・Systems・	Trusted Services [®] searcy the determined	
Zuracksetzen Hier können Sie	des Passworts I Ihr Passwort int Hitle der zuvon definierten Olchemeitstragen zurück setzen. Olch geden Gie Ihre DiMal-Adre Ihre Eußalf-Edeese	1858 SI.

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:

Zunicksetzen des Passwi	rts fur die E-Mail-Adresse: user@domain.com		
Ette geben Sie die Artworte	ein, weiche Sie Rührr für die von Ihren ausgewählten Fragen gegeben haben.		
Who was the Spitzname in their	9-8-87		
Ciel			
In writches Shart ballets Sir Bore	Partner illare Partnetin min enten mai genatten?		
Paris			
We bin lich?			
140			
Fails 24 da bahadan mat	nahr ussan mahman (2) 1975 mil Ivan Universit Labour sites (2014) 24 a.f.		
T 212 GET & C PENNENCES INVIT	The resident includes and an according to the residence in the second second second second second second second	200	-

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:

··· P ···Systems·	Trusted Services [®] Income for Galact Mer
Passwort andern Henre Passwort Passwort hestalagers	
Figure 21: Specifying a new passwo	ord

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 nit der Signatur aufgetreten. Klicken Sie für Details auf die Signaturschaltfläche.

۹

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:

retifikat anzeigen	2
Algemein Details Zentitzierungsplad Vertrauen	
Der Vertrauensstatus göt an, ob Sie der Person, Gruppe od vertrauen, der dieses Zertifkat ausgestellt wurde. Ein Zert die angegebnen Zwecke verwinnledt werden, zum Beispiel 5 Empfangen von E-Mall, Bestimmen der Vertrauerswurdigkei usw.	ler Firma fikat kann für Senden und t einer Website,
- Das Zehlikat als vertrauenswürdig einstuten für	
E-Mail-Verschlüsselung und Authentifizierung	
Vertrauensstatus beabeiten	
③ Verhauensstatus des Assistellers überrehmen.	
 Dieses Zertifikat als vertrauenswürdig einstufen. 	
O Dieses Zehlikat als nicht vertrauenswardig einstule	n
	OK

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":

Informationen zur Zei	rtifizierungss	telle	
Ihre Nachricht wurde mit Zertifizierungsstelle ausge Die Signatur ist ungültig, k vertrauen oder sie noch r	einem Zertifikal sstellt wurde, d da Sie der folge icht als vertra.	, das von einer Igtal signiert. ndon Zertifizieri ienswürdig eing	ingsstelle nicht istuft haben:
Ausgestellt von: Gültig ab: Klicken Sie auf "Details", u erhalten, das für die digt	CA Comp 21.08.200 m wetere Info ale Signatur de	any 6 bis 16.00.202 mationen zum 2 r Nachricht verw	0 tertifikat zu endet wurde. Detais
Der Zertifizierungsste	le vertrauer	,	
Einer Zertifizierungsstelle die mit Zertifikaten von die als vertrauenswürdig eins	zu vertrauen b eser Zertifizien tufen.	edeutet, dass S ingsstelle digital	e Nachrichten, signiert wurden,
Möchten Sie diese Zertifiz	ierungsstelle al	s vertrauenswür	dig einstufen?
Wenn Sie "Vertrauen" wä "Stammzertifikatsspeicher Ihrem System hinzugefüg	Nen, müssen S " auch auf "Ja" t werden kann	ie im nächsten D klicken, damit d	ialogfeld as Zertifikat
[Martin mart	Esthelen

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 Digitalsignaturschicht		1 10 1 A. 1997	1000	
Nachrichten enthalten u.U. Verschlüsselungs- oder Digitalsignaturschichten Jede Digitalsignaturschicht kann mehrere Signaturen enthalten. Sicherheitsschichten Wählen Sie eine Signaturschicht aus, um deren Beschreibung anzuzeigen. Digitalsignaturschicht Digitalsignaturschicht Digitalsignaturschicht Manierer: uzerägdomein.com Deschreibung: Achtung: Die Zertifikatsoperliste, die zur Überprüfung des Signaturzertifikats benötigt wird, ist entweder nicht verfügbor oder nicht mehr giblig. Einsteit und Beschreibung zur Gerprüfung des Signaturzertifikats benötigt wird, ist entweder nicht verfügbor oder nicht mehr giblig. Einsteit und beschlichen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detals anzeigen	Betref	E: Neue sichere Nachr	richt wartet	
Sicherheitsschichten Wählen Sie eine Signaturschicht aus, um deren Beschreibung anzuzeigen. Petreff: Neue sichere Nachricht wartet Digitalsignaturschicht Signierer: user@siomein.com Beschreibung: Achtung: Die Zertifikatssperliste, die zur Überprüfung des Signaturzertifikats benötigt wird, ist entweder nicht werfügber oder nicht mehr gibig. Sieniste une NeueRithschen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detals anzeigen	Nschrichten er Jede Digitalsig	nthalten u.U. Verschlüs naturschicht kann mehr	selungs- oder Digitalsignal rere Signaturen enthalten	turschichter
Wählen Sie eine Signaturschicht aus, um deren Beschreibung anzuzeigen. ✓ Betreff: Neue sichere Nachricht wartet ✓ Digitalisignaturschicht Ø Signierer: user@domain.com Ø Sechreibung: Achturg: Ø Zertifizielassperliste, die zur Überprüfung des Signaturzertifikalss Ø Signierer: user@godomain.com Ölekanse.de unter Vassundense um Ditt fühlt um Centralig wird, ist entwender nicht verfügber oder richt mehr giblig. Centraligen um eine zu bearbeken: Vertrauen Detals anzeigen Zertifizierungsstelle vertrauen Bei Fehler Gigtud signierten Nachrichten Warnhinweis anzeigen.	Sicherheitss	chichten		
Betreff: Neue sichere Nachricht wartet Digitalsignaturschicht Digitalsignaturschicht Signierer: uzerggdomein.com Deschreibung: Achtung: Die Zertifiziensperfiste, die zur Überprüfung des Signaturzertifikalts benätigt wird, ist entweder nicht verfügbar oder nicht mehr gültig. Sonstat und besetikkenne die under Uberprüfung des Signaturzertifikalts benätigt wird, ist entweder nicht verfügbar oder nicht mehr gültig. Sonstat und besetikkenne die under Uberprüfung des Signaturzertifikalts benätigt wird, ist entweder nicht verfügbar oder nicht mehr gültig. Sonstat und besetikkenne die under Uberprüfung des Signaturzertifikalts benätigt wird, ist entweder nicht verfügbar oder nicht mehr gültig. Sonstat und besetikkenne die under Uberprüfung des Signaturzertifikalts benätigt wird, ist entweder nicht verfügbar oder nicht mehr gültig. Sonstat und besetikkenne die under Uberprüfung des Signaturzertifikalts benätigt wird, ist entweder nicht verfügbar oder nicht mehr gültig. Sonstat und besetikkenne die under Uberprüfung des Signaturzertifikalts benätigt wird, ist entweder nicht verfügbar oder nicht mehr gültig. Sonstat und besetikkenne die under Uberprüfung des Signaturzertifikalts benätigt wird, ist entweder nicht verfügbar oder nicht werkenter Uterprüfung des Signaturschicht zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeken: Vertrauen Detals anzeigen Zertifizierungsstelle vertrauen Sonstat digtal signierten Nachrichten Warnhinweis anzeigen.	Wählen Sie ein	e Signaturschicht aus,	um deren Beschreibung a	nzuzeigen.
Digitalsignaturschicht Signierer: uzer@kiomain.com Deschreibung: Achturg: Die Zertifizietssperfiste, die zur Überprüfung des Signaturzertifikalss benötigt wird, ist entweder nicht verfügbor oder nicht mehr gültig. Sanstat sone besetlikkanner des Uberprüfung des Signaturzertifikals benötigt wird, ist entweder nicht verfügbor oder nicht mehr gültig. Sanstat sone besetlikkanner des Uberprüfung des Signaturzertifikals benötigt wird, ist entweder nicht verfügbor oder nicht mehr gültig. Sanstat sone besetlikkanner des Uberprüfung des Signaturzertifikals benötigt wird, ist entweder nicht verfügbor oder nicht mehr gültig. Sanstat sone besetlikkanner des Uberprüfung des Signaturzertifikals benötigt wird, ist entweder nicht verfügbor oder nicht mehr gültig. Sanstat sone besetlikkanner des sone besetlikkanner (Details anzeigen) Bei Fehler, digtal signierten Nachrichten Warnhinweis anzeigen. Sanstat	✓ Betreff: I	Neue sichere Nachricht	wartet	
Signierer: user@domein.com Deschreibung: Achtung: Die Zertifikatssperifiste, die zur Überprüfung des Signakurzertifikats benötigt wird, ist entweder nicht verfügbor oder nicht nehr giblig. Signakurschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detalis anzeigen Zertifizierungsstelle vertrauen Bei Fehler digital signierten Nachrichten Warnhinweis anzeigen. Schlidten	✓ Digit/	alsignaturschicht		
Beschreibung: Achtung: Die Zertflikatssperrliste, die zur Überprüfung des Signaturzertflikats benötigt wird, ist entweder nicht verfügber oder nicht mehr gültig. Sieniste une De Achtaflik Sienister une DEA/Staflik Sienisterung DEA/Staflik Signaturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detals anzeigen Bei Fehle Gigtal signierten Nachrichten Warnhinweis anzeigen.	1	Signierer: user@domair	n.com	
Beschreibung: Achtung: Die Zertifikatssperifiste, die zur Überprüfung des Signeturzertifikats benötigt wird, ist entweder nicht verfrügber oder nicht mehr gibtig. Sieniste zum Die Schaltflächen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detals anzeigen Bei Fehler digtal signierten Nachrichten Warnhinweis anzeigen.				
Beschreibung: Achturg: Die Zertfiffadssperfikte, die zur Überprüfung des Signeturzertifikals- benötigt wird, ist entweder nicht verfügber oder nicht mehr gültig. Sinstat und hundlichkannen die Uberbeitere Informationen zur gewählten Signeturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detals anzeigen Bei Fehler digital signierten Nachrichten Warnhinweis anzeigen.				
Deschreibung: Achtung: Die Zertifikatssperriste, die zur Überprüfung des Signaturzertifikats benötigt wird, ist entweder nicht verfügber oder nicht mehr gibtig. Similat une benöthsammer der unes beisamsederen une DEA (Nach 1). Glicken Sie auf die Schaltflächen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detalis anzeigen Bei Fehler digtel signierten Nachrichten Warnhinweis anzeigen.				
Beschreibung: Achtung: Die Zertifikatssperriste, die zur Überprüfung des Signeturzertifikats benötigt wird, ist entweder nicht verfrügber oder nicht mehr gibtig. Sieniete two beschlesmense du intere Viersiendense um DEA/SUAN um dicken Sie auf die Schaltflächen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detals anzeigen Bei Fehler digtal signierten Nachrichten Warnhinweis anzeigen. Sichlichen				
Deschreibung: Achtung: Die Zertfiffadssperfisite, die zur Überprüfung des Signeturzertfifikats benötigt wird, ist entweder nicht verfügber oder nicht mehr gültig. Soniset von brendfischen, um weiter Unformationen zur gewählten Signeturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detals anzeigen Bei Fehler, digital signierten Nachrichten Warnhinweis anzeigen.				
Beschreibung: Achtung: Die Zertifikatssperifiste, die zur Überprüfung des Signakurzertifikats benötigt wird, ist entweder nicht verfügber oder nicht mehr gültig. Stenistet von beschlichsemse de under Umstere Unormationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detals anzeigen Bei Fehler digital signierten Nachrichten Warnhinweis anzeigen.				
Deschreibung: Achtung: Die Zertifikatssperriste, die zur Überprüfung des Signaturzertifikats benötigt wird, ist entweder nicht verfügber oder nicht mehr gültig. Censiet une besoffte werden der verfügber oder nicht mehr gültig. Clicken Sie auf die Schaltflächen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detals anzeigen Bei Fehle digtal signierten Nachrichten Warnhinweis anzeigen.				
Achtung: Die Zertflikatssperifikte, die zur Überprüfung des Signaturzertflikats benötigt wird, ist entweder nicht verfügber oder nicht mehr gültig. Sinsiat une besofflikarene der verfügber oder nicht mehr gültig. Gleisen Sie auf die Schaltflächen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detalis anzeigen Bei Fehle digtal signierten Nachrichten Warnhinweis anzeigen.				
Die Zertifikatssperifste, die zur Überprüfung des Signakurzertifikats benötigt wird, ist entweder nicht verfügber oder nicht mehr gibig. Similat une beschlasmanne die unter Similand eine won EPG (Nath 1) Globen Sie auf die Schaltflächen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detals anzeigen Bei Fehle digtal signierten Nachrichten Warnhinweis anzeigen.	Deschreibung:			
benötigt wird, ist entweder nicht verfügber oder nicht mehr giblig. Cleasast vom breutlichsmark de reter Vassendenn vom DER/EUX1 vom Kicken Sie auf die Schaftlichen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detals anzeigen Bei Pehle digital signierten Nachrichten Warnhinweis anzeigen. Cableden	Deschreibung:	}		
Cientiait une le useffikarmar, de utites Vianusede en une DEA/CUAN (un Clicken Sie auf de Schatflächen, un weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeken: Vertrauen Detalis anzeigen Bei Fehlen, digital signierten Nachrichten Warnhinweis anzeigen.	Deschreibung: Achtung: Die Zertifikats	spernlaste, die zur Über	prüfung des Signeturzerti	ikats
Cicken Sie auf die Schaltflächen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten: Vertrauen Detals anzeigen Bei Fehlen digital signierten Nachrichten Warnhinweis anzeigen.	Deschreibung: Achtung: Die Zertifikats benötigt wird,	speriiste, die zur Über	prüfung des Signekurzerti Fögbar oder nicht mehr gü	likats
Vertrauen Details anzeigen Zertifizierungsstelle vertrauen Bei Fehlore digital signierten Nachrichten Warnhinweis anzeigen.	Beschreibung: Achtung: Die Zertifikats benötigt wird, Geniast uso b	sperilste, die zur Über Ist entweder nicht ver	pröfung des Signeturzerti Fögber oder nicht mehr gö Vannande ein uns DEG föld	fikats ikig.
Bei Fehlen digital signierten Nachrichten Warnhinweis anzeigen.	Beschreibung: Achtung: Die Zertifikats benötigt wird, Sienisst unn h Kicken Sie auf Signaturschich	sperikte, die zur Über ist entweder nicht ver die Schaftenen, um s t zu erhalten oder um s	prüfung des Signeturzerti fügber oder nicht mehr gü Verweitere Informstonen zur is zu bearbeiten:	fikats itig.
Bei Fehldrum digital signierten Nachrichten Warnhinweis anzeigen.	Deschreibung: Achtung: Die Zertifikats benötigt wird, Signaturschich Vertrauen	sperniste, die zur Über ist entweder nicht ver die Schakflächen, um t zu erhalten oder um s Detalis anzeigen	prüfung des Signeturzerbi fügber oder nicht mehr gü Verweitere Informstionen zur ie zu bearbeiten: Zertifizierungsstelle w	likats kig gewählten
(rations	Beschreibung: Achtung: Die Zertfifikals benötigt wird, Geniest um b dicken Sie auf Signaturschich Vertrauen	sperilste, die zur Über Ist entweder nicht ver die Schaltflächen, um i t zu erhalten oder um s Detalis anzeigen	prüfung des Signeturzerti fügber oder nicht mehr gü Varansedens und DEG Mek weitere Unformationen zur se zu bearbeiten: Zertifizierungsstelle w	likats izig gewähiten ertrauen
	Beschreibung: Die Zertifikats benötigt wird, Signaturschich Vertrauen	sperniste, die zur Über ist entweder nicht ver die Schaltflächen, um i t zu erhalten oder um s Details anzeigen digital signierten Na	prüfung des Signakurzerbi fügbar oder nicht mehr gi Weitere Informstionen zur ie zu bearbeiten: Zertifizierungsstelle w chrichten Warnhinweis anz	likats Big. At um gewählten ertrauen zeigen.

Announcement by the Issuing CA.

Ugemen	Details	Zertifizierungsplad	Vertrauen	
Der Vertr vertrauer die anger Empfangi usw.	auenssta n, der die jebenen en von E-	itus gibt an, ob Sie di ses Zertifikat ausges Zwecke verwendet w Mail, Bestimmen der	er Person, Gruppe od tellt wurde. Ein Zert verden, zum Beispiel 3 Vertrauenswürdigkeit	ler Firma fikat kann für Senden und Folner Website,
DasZe	elikat ak	vertrauenswürdig ei	nstulen für	
E-Mai-	Verschlus	selung und Authentit	fizierung	
Vertrau O O	encstatu Vertrauer Dieces Z Dieces Z	<mark>i beaibeiten</mark> testatus des Ausstelle erblikat als verbauen erblikat als nicht verb	rs übernehmen. swurdig einstufen. auenswürdig einstufe	n

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:

Eigenschafte	n der Nachrichte	nsicherheit	X
Betreff	: Neue sichere Nachri	cht wartet	
Nachrichten en Jede Digitalsign	thaiten u.U. Verschlüss aturschicht kann mehre	elungs- oder Digitalsignat ere Signaturen enthalten.	urschichten.
Sicherheitssi	hichten		
Wählen Sie eine	Signaturschicht aus, u	um deren Beschreibung ar	nzuzeigen.
✓ Digita ✓ Si	signaturschicht gnierer: user@domain	com	
Beschreibung:			
Beschreibung: OK: signierte N	lachricht.		
Beschreibung: OK: signierte N Klicken Sie auf d Signaturschicht	lachricht. die Schaltflächen, um w zu erhalten oder um si	veitere Informationen zur e zu bearbeiten:	gewählten
Beschreibung: OK: signierte N Kicken Sie auf Signeturschicht Vertrauen	lacheicht. die Schaltflächen, um w zu erhalten oder um si	veitere Informationen zur e zu bearbeiten:	gewähiten antrauen
Beschreibung: OK: signierte N Kicken Sie auf Signaturschicht Vertrauenu	lachricht. die Schaltflächen, um w zu erhalten oder um si Oetalo anzeigen n dioltal signierten Nac	eitere Informationen zur e zu bearbeiten:	gewählten ortroudnasi
Beschreibung: OK: signierte N Klicken Sie auf Signaturschicht Vertrauen Bei Fehlern	lacheicht. die Schaltflächen, um w zu erhalten oder um si Oetolu anzeigen. n digital signierten Nac	veitere Informationen zur e zu bearbeiten: Zizrtifizierungsstelle ve hrichten Warnhinweis and	gewähiten Intrautnun zeigen,

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 <u>only</u> 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 reged it 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: . z i p : 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

