Office Standardization. E-Mail Encryption Gateway.

Anleitung für externe Kommunikationspartner.



Einleitung.

Der E-Mail Encryption Gateway, der im Folgenden "Trust-Mail[®]" genannt wird, ist eine zentrale Erweiterung der bestehenden E-Mail-Infrastruktur der Deutschen Telekom und bietet einen umfangreichen Kommunikationsschutz, der die verschlüsselte und/oder signierte E-Mail-Kommunikation sowohl intern als auch mit externen Kommunikationspartnern unterstützt. TrustMail[®] wurde als eine zentrale hochverfügbare Instanz zwischen dem Intranet der Deutschen Telekom und dem Internet aufgebaut und repräsentiert eine der innovativsten Secure-Messaging-Lösungen im heutigen Markt.

Im Rahmen der Einführung von TrustMail[®] wird u. a. die E-Mail-Kommunikation zwischen E-Mail-Konten interner Mitarbeiter der Deutschen Telekom und externen Kommunikationspartnern abgesichert.

Im Folgenden werden alle Szenarien und Kommunikationsschnittstellen beschrieben, bei denen ein externer Kommunikationspartner zu Beginn und im späteren Verlauf der abgesicherten E-Mail-Kommunikation mit Mitarbeitern oder Funktionsmailboxen der Deutschen Telekom involviert ist. Anhand der Einsatzszenarien werden alle benötigten Handlungsanweisungen für externe Kommunikationspartner beschrieben, die bei der Interaktion mit TrustMail[®] auftreten können.

Inhalts- und Abbildungsverzeichnis.

Einleitung	2
Inhalts- und Abbildungsverzeichnis	3
Kurzbeschreibung der Lösung	4
Fall 1: S/MIME-Zertifikat oder PGP-Schlüssel vorhanden	6
Fall 2: Weder S/MIME-Zertifikat noch PGP-Schlüssel vorhanden. Empfang und Versand von E-Mails über WebMail. Empfang und Versand von E-Mails mit Hilfe von PushedPDF.	
Passwort zurücksetzen	14
Bekanntmachung der ausstellenden CA	16
Behebung von Problemen	19
Abkürzungsverzeichnis.	

Abbildungsverzeichnis

Abbildung 1: Ende-zu-Ende-Verschlüsselung von E-Mails	5
Abbildung 2: Mailfluss bei bereits verfügbarem S/MIME- oder PGP-Schlüssel für Verschlüsselung	6
Abbildung 3: Benachrichtigung zum erstmaligen Registrieren	7
Abbildung 4: Outlook-Empfang von verschlüsselter S/MIME-E-Mail	7
Abbildung 5: Empfang einer verschlüsselten PGP-E-Mail	7
Abbildung 6: Mailfluss bei nicht vorhandenem S/MIME- oder PGP-Schlüssel und	
Verwendung von WebMail	8
Abbildung 7: Benachrichtigung zum erstmaligen Registrieren	9
Abbildung 8: Erstmaliger Webzugang in WebMail	9
Abbildung 9: Registrierung in WebMail	
Abbildung 10: Beantwortung von Sicherheitsfragen	
Abbildung 11: WebMail-Interface	11
Abbildung 12: Benachrichtigung über zugestellte WebMail	11
Abbildung 13: Passworterstellung für Absicherung der PDF-Dokumente	
Abbildung 14: Erfolgreiche Registrierung für die PDF-Zustellung	
Abbildung 15: PDF-Empfang 01	
Abbildung 16: PDF-Empfang 02	13
Abbildung 17: Antwort auf PDF-E-Mail	13
Abbildung 18: Passwortzurücksetzung initiieren	
Abbildung 19: E-Mail-Angabe bei Passwortzurücksetzung	14
Abbildung 20: Sicherheitsfragen bei Passwortzurücksetzung	15
Abbildung 21: Passwort neu vergeben	15

Kurzbeschreibung der Lösung.

Alle Mitarbeiter der Deutschen Telekom können mit Hilfe von TrustMail[®] E-Mails verschlüsseln und zu jeder beliebigen internen oder externen E-Mail-Adresse senden oder von dort eine verschlüsselte E-Mail empfangen und entschlüsseln. Verschlüsselte E-Mails können darüber hinaus von allen beteiligten Kommunikationspartnern weitergeleitet und verschlüsselt beantwortet werden.

Falls ein externer Kommunikationspartner noch nicht über die S/MIME- bzw. PGP-Technologie verfügt, um E-Mails zu ver- bzw. zu entschlüsseln, so werden ihm die verschlüsselten E-Mails in einer SSL-abgesicherten Webanwendung, die im Folgenden "WebMail" genannt wird, zur Verfügung gestellt. Über die Zustellung einer verschlüsselten E-Mail wird der externe Kommunikationspartner durch eine automatisiert generierte Benachrichtigung per E-Mail informiert. Mit Hilfe von WebMail kann er nach erfolgreicher Registrierung und nachfolgender Authentifizierung alle ihm zugestellten verschlüsselten E-Mails lesen.

Bei Bedarf kann der externe Kommunikationspartner eine Weiterleitung der an ihn adressierten verschlüsselten E-Mails konfigurieren. Die weitergeleiteten E-Mails werden dabei inklusive Anhängen in verschlüsselte PDF-Dokumente konvertiert, die durch ein zuvor von ihm in WebMail spezifiziertes Passwort entschlüsselt werden können. Man spricht hier von einer sogenannten "PushedPDF"-Technologie.

Falls ein externer Kommunikationspartner bereits über eine Verschlüsselungstechnologie (PGP oder S/MIME) verfügt, so kann er sein Zertifikat bzw. seinen öffentlichen PGP-Schlüssel TrustMail[®] bekannt machen, damit diese zukünftig von TrustMail[®] verwendet werden können, um E-Mails basierend auf der entsprechenden Verschlüsselungstechnologie verschlüsseln und direkt zustellen zu können.

Die Verschlüsselung der E-Mail erfolgt dabei nahezu Ende-zu-Ende, d. h., die E-Mail wird bereits im Outlook-Client der Mitarbeiter der Deutschen Telekom verschlüsselt und gegebenenfalls durch den E-Mail Encryption Gateway in Abhängigkeit von den technologischen Gegebenheiten des externen E-Mail-Empfängers z. B. bei einer erforderlichen Umschlüsselung nach PGP umgeschlüsselt.



Abbildung 1: Ende-zu-Ende-Verschlüsselung von E-Mails

Alle Mitarbeiter der Deutschen Telekom können E-Mails signieren (mit und ohne Verschlüsselung) und zu jeder beliebigen internen oder externen E-Mail-Adresse senden oder signierte E-Mails von dort empfangen und eine eventuell angefügte digitale Signatur verifizieren.

Die Deutsche Telekom favorisiert die Verwendung von S/MIME für die Verschlüsselung und Signierung von E-Mails. Um externe Kommunikationspartner nicht zu verpflichten, von PGP auf S/MIME zu migrieren, kann TrustMail® ausgehende E-Mails nach PGP umschlüsseln bzw. eingehende PGP-verschlüsselte E-Mails nach S/MIME umschlüsseln.

Damit ist eine hochgradige Transparenz und Flexibilität sowohl auf interner als auch auf externer Kommunikationsseite gewährleistet.

Fall 1: S/MIME-Zertifikat oder PGP-Schlüssel vorhanden.

Die folgenden Szenarien beschreiben die geschützte E-Mail-Kommunikation zwischen der Deutschen Telekom und einem externen Kommunikationspartner, wenn dieser bereits in der Lage ist, entweder mittels S/MIME oder PGP E-Mails zu verschlüsseln und/oder zu signieren.



Abbildung 2: Mailfluss bei bereits verfügbarem S/MIME- oder PGP-Schlüssel für Verschlüsselung

- 1. Ein Mitarbeiter der Deutschen Telekom sendet eine (signierte) E-Mail, die verschlüsselt werden soll, an einen externen Kommunikationspartner.
- 2. Die E-Mail wird intern an TrustMail® geroutet.
- TrustMail[®] prüft, ob der externe Kommunikationspartner bereits registriert ist und sein öffentlicher Schlüssel (S/MIME oder PGP) entsprechend verfügbar ist.
- 4. Wenn kein S/MIME-Zertifikat oder öffentlicher PGP-Schlüssel des externen Kommunikationspartners verfügbar ist oder über angebundene externe Verzeichnisdienste bzw. Key Server gefunden werden kann, wird die verschlüsselte E-Mail in TrustMail[®] zwischengespeichert und dem externen Kommunikationspartner eine Benachrichtigung in folgender Form zugesendet:

Fall 1: S/MIME-Zertifikat oder PGP-Schlüssel vorhanden.

***	an (Farmer Street Street Street Street Street Street Street	
(h-h-m	terrindi tegeteterang ona at lever habitett	
No. of Concession, Name	Abanden midden andel inden en	
C amounts	ing angle gan and gana and 💷	
M caused	Advantage (Add) Advantage (
13 Ipen	Darwey Male (42)	
E. GRUNT	Liter Below Main Some	
	Mustafa Mveta (mustafa mustafa)s esternis conti módele trien eine Nacimidit pakonmentacien, derentishall vetraulich rist. Des Nacimidit nocit ungeschutzt asemidiet.	hab wird die
	Sitte lesen sie die nacht/igenoen Anweaungen sorgfabg.	
	Bothers are benefits and SMMEZ Zeithland beatzen, so architecten sie bete not ansen sognanten E-Abel auf diese Nachorste Sollten sie benefits allwar POP Bothinsam besitzen, au arbeisten die bette mit alsent E-Mail, welche den anzumenbanden offentlich als Antomiz trag.	en Schlane
	Balten sie weder ein SMME Bentikst noch einen PGP Schlässelbesitten, so melden sie sich hite unter Verwendung der unter Benutzerbaten iber den folgenden Link en:	adgetiteten
	Eogin page Ingestimus mysakema Indekom dotšechka) Beomise (D. overtidenna nuorm Praziverti (BH942)	
	Wenn sie such erfolgneich angemeidet haben, steben ihnen weitere Attenutivoptionen nir Vertigung, äber neliche sie leicht Zuger gesicherten Nachsicht erhalten können.	ig zu êrer
	English Vertilion	
	Mustafa Musta (mustafa mustafa mustafa) eystema.com) exuld live to cend you a message whose security level does not permit an une delivery to your email address.	kryglød
	Please read the following instructions carability	
	If you stready posses an UMMAT certificate, please samply send a signed reply to this email	-

Abbildung 3: Benachrichtigung zum erstmaligen Registrieren

5. Falls der externe Kommunikationspartner bereits über ein S/MIME-Zertifikat für E-Mail-Verschlüsselung und -Signierung verfügt (siehe roter Pfeil in Abbildung 3), antwortet er auf die o. a. Mail mit einer S/MIME-signierten E-Mail. Verwendet der externe Kommunikationspartner z. B. Microsoft Outlook, so ist dies einfach durch Aktivierung der entsprechenden Schaltfläche für Signatur möglich:

E Datei Bearbeiten	Ansicht	Enfugen	Format	Egtras	Aktionen	TIKS 2000	2	
I 🖃 Senden 🔛 🎒	1 X D	2 2	1 100	8,13	1 4	* 10018	Optionen	🖬 🛃 🗚 🖓 👘 🖬 📮
Arial	- 10	• <u>A</u>	F K	u 📕	==:	日间编辑	F 12 .	

Falls der externe Kommunikationspartner bereits PGP-Verschlüsselung im Einsatz hat, so antwortet er auf diese E-Mail und hängt dabei seinen öffentlichen PGP-Schlüssel als Attachment an.

- 6. TrustMail[®] überprüft das erhaltene Schlüsselmaterial auf Gültigkeit und speichert den öffentlichen Schlüssel (S/MIME oder PGP) in seinem Key Store.
- 7. Die zwischengespeicherte E-Mail wird jetzt abhängig von der vom externen Kommunikationspartner verwendeten Verschlüsselungstechnologie entweder mit S/MIME verschlüsselt und zugestellt:

🛃 🕕 hugo	sacure 05t1 2	Mp 08.06.2009 12:17
-		

Abbildung 4: Outlook-Empfang von verschlüsselter S/MIME-E-Mail

Oder die E-Mail wird mit PGP verschlüsselt und zugestellt:

Betreff: secure neua2	
Einfügen: Astrid.ast (953 Byte) PGPexch.htm.ast (1,06 KB)	
BEGIN PGP MESSAGE Version: OpenPGP TructMad	
Comment: This message was encrypted by Totemo TrustMail - http://www.totemo.ch	
hQEMA+b8+l6CMD3tAQf/ZxEFykKN36IIVxqO4fOGhcfaN5mEHMxykJ4M0RfrSeGm b4eaDezl2drLK8LCp6l0yFT+W6PL2gpeTaFfakevf/mpIMpkfpDX4yiGRgO31psf	

Abbildung 5: Empfang einer verschlüsselten PGP-E-Mail



Bei dem nach der Registrierung erfolgten Austausch von weiteren verschlüsselten E-Mails zwischen einem internen Mitarbeiter oder einer Funktionsmailbox der Deutschen Telekom und dem nun registrierten externen Kommunikationspartner nutzt TrustMail® dessen im Key Store enthaltenen öffentlichen S/MIME- oder PGP-Schlüssel zur Verschlüsselung, d. h. die für die Registrierung erforderlichen Arbeitsschritte 4., 5. und 6. entfallen.

Fall 2: Weder S/MIME-Zertifikat noch PGP-Schlüssel vorhanden.

Die folgenden Szenarien beschreiben die geschützte E-Mail-Kommunikation zwischen der Deutschen Telekom und einem externen Kommunikationspartner, der noch nicht über eine E-Mail-Verschlüsselungstechnologie (S/ MIME oder PGP) verfügt.



Abbildung 6: Mailfluss bei nicht vorhandenem S/MIME- oder PGP-Schlüssel und Verwendung von WebMail

- 1. Ein Mitarbeiter der Deutschen Telekom sendet eine (signierte) E-Mail, die durch TrustMail[®] verschlüsselt werden soll, an einen externen Kommunikationspartner.
- 2. Die E-Mail wird intern an TrustMail[®] geroutet.
- TrustMail[®] prüft, ob der externe Kommunikationspartner bereits registriert ist und sein öffentlicher Schlüssel entsprechend verfügbar ist.
- 4. Wenn kein S/MIME-Zertifikat oder öffentlicher PGP-Schlüssel des externen Kommunikationspartners verfügbar ist oder über angebundene externe Verzeichnisdienste bzw. Key Server gefunden werden kann, wird die E-Mail in TrustMail[®] zwischengespeichert und dem externen Kommunikationspartner die folgende Benachrichtigung zugesendet:

Fall 2: Weder S/MIME-Zertifikat noch PGP-Schlüssel vorhanden.



Abbildung 7: Benachrichtigung zum erstmaligen Registrieren

5. Da der externe Kommunikationspartner noch kein eigenes S/MIME-Zertifikat oder PGP-Schlüsselpaar für E-Mail-Verschlüsselung bzw. -Signierung besitzt, bietet sich für ihn der Zugriff auf die verschlüsselte E-Mail per WebMail oder in Form einer direkten Zusendung einer verschlüsselten PDF-Datei per E-Mail an. Dazu registriert sich der externe Kommunikationspartner SSL-geschützt in WebMail mit Hilfe der in der Benachrichtigung angegebenen URL (siehe roter Pfeil in Abbildung 7). Ihm wird darauf die folgende Eröffnungsseite in seinem Webbrowser angezeigt:

2) Tatarta Tatalitat Wakita I Distance Contacted I	aphrone Renetingerhald were T. Spätnere	
Las builds must finder Low r		
🔾 Darak + 💭 💽 📓 🐔 💭 Sadam	👷 Tanatas 🐵 🍰 😳 🚆 🔛 🛄	
La	ert sp	💌 🔂 Wedselaus 💷 🗤
··· T ···Systems·	Trusted Services [®] desarry the Date of Adver	
WEFcommen Sie nation die Möglichtert, die Sichera Dite wählen zie unter der unter aufge	agadiwata wa Tuddhai aufvarozhodona Artanza nutza. Under McGlitikkaten	
VoetsMaai		
Wahlen Sie diese Option, talls pie di	s E Noll sinter and bequers in item Reswar another induttor.	
		To Walking a
POF Zummana		
Dwith diese Option weedon gas cho	ta POFe via E-Mail vercendat.	
		To Myddag

Abbildung 8: Erstmaliger Webzugang in WebMail

Der externe Kommunikationspartner kann nun entscheiden zwischen "WebMail" oder "PDF-Zustellung": Die Option "WebMail" bedeutet, dass die verschlüsselten E-Mails inklusive etwaiger Anhänge dem externen Kommunikationspartner nicht direkt zugestellt werden, sondern über eine zu authentifizierende und SSL-geschützte WebMail-Schnittstelle (vergleichbar mit WebMail-Anwendungen wie z. B. GMX oder Web.de) zu lesen sind.

Die Option "PDF-Zustellung" bedeutet, dass die für ihn hinterlegte E-Mail inklusive etwaiger Anhänge in ein PDF-Dokument konvertiert und mit einem vorher von ihm selbst zu spezifizierenden Passwort verschlüsselt wird. Dieses PDF-Dokument wird dem externen Kommunikationspartner per E-Mail zugestellt. Alle zukünftigen E-Mails, die ein interner Mitarbeiter der Deutschen Telekom an diesen externen Kommunikationspartner schickt, werden dann ebenfalls als verschlüsseltes PDF-Dokument per direkter E-Mail zugestellt.

Empfang und Versand von E-Mails über WebMail.

Im Folgenden wird beschrieben, wie man sich in WebMail erstmalig registriert und wie man auf zugestellte verschlüsselte E-Mails über die WebMail-Schnittstelle von TrustMail[®] zugreifen sowie verschlüsselte E-Mails erstellen und verschicken kann.

Registrierung des externen Kommunikationspartners in WebMail:

Da mit der o. a. E-Mail (vgl. Abbildung 7) nur ein One Time Password (OTP) vergeben wird, muss der externe Kommunikationspartner zuerst ein eigenes neues Passwort erstellen:

Benutzer Informationen		
De wurden brahen automatisch registrart.	Um die geschede E-Maliza erhaben, führt lie hille die unterschleerde Torm aus und sender Die sie harück.	
Benutzer ID:	user@domain.com	
voler hane;	(Chatzana)	
Neues Passwort		
Passwort bestilligen		
Sprache	Deutsca 💌	

Abbildung 9: Registrierung in WebMail

Beantwortung von Sicherheitsfragen:

Damit der externe Kommunikationspartner zukünftig die Möglichkeit hat, bei Verlust seines Passworts für WebMail dieses zurückzusetzen, ohne einen Helpdesk dafür in Anspruch zu nehmen, wird er aufgefordert, drei Sicherheitsfragen zu beantworten. Zwei dieser Sicherheitsfragen können aus einer Auswahl verschiedener Fragen ausgewählt werden und eine dritte Sicherheitsfrage ist frei definierbar. Hinweise zur Auswahl und Beantwortung der Sicherheitsheitsfragen sind der Webseite zu entnehmen.

Sixberheitstragen: Da	ierğ domain, com
Fails Gelitr Passwort verg Können, gute Sicherheitstri	esten sollten werden Sie aufgefordent, füre Sicherheitsfrägen zu beanbichten. Hier sind einige Himietse, welche finnen heifen ögen auszuwählen:
Wahlen Sie die Ante Wenn Sie Information nehmen Sie andere	orber so, stass Sie sich gut staran einnem können und dass Siese nicht leicht zu ersten sind. nes zu Fingen auf Sosalen Netzwerken we Facebook, MySpace oder auf ihrer personichen Honopags veröffentlicht haben, Frägen.
We erreichen Sie, dass die	eFragen und Antworten gebeim bielben:
Ercählen Sie neman Verschicken Sie des Wechsein Sie Ihre Fr	dem von den Fragen und Anbeoten und schreiben Sie diese nicht auf. ie Informätionen nie per E-Mail. ragen periodisch.
Un die Schemet zu gewählt	nleisten, sollten die Arbeuten folgende Bedingungen erfüllen:
Die Antworten dürfer Die Antworten solten Die Antworten müsse Die Antworten müsse Die Antworten dürfer	inwillimen bekannt sein. Isch: Geer Jangere Ziet nicht andern. In innostenn 4. maamai 200 Buchstaben lang sein. In lainer Weise mit dem Benutsemanen soler dem Passwort zusammentlängen.
Wildow Sin eine Frage auss	Was war fit Spitzmanne in from Kindheit?
three Autovort:	Civi G
Wildow Sie eine Trage ant:	In welcher Stadt haben Sie Reen Partnerlihre Partnerin zum sraten mal gebroffen]
Itre Arbvort	Pais
	Mu bin ich?
Geben Sie eine Frage ein:	

Abbildung 10: Beantwortung von Sicherheitsfragen

Zugriff auf zugestellte E-Mail über WebMail:

Anschließend muss sich der externe Kommunikationspartner mit dem neuen Passwort erneut anmelden und hat Zugriff auf die verschlüsselten E-Mails über die WebMail-Schnittstelle:

•• T ••Systems•	Trusted Services [®] Jacomy Inc.	Carlos en Milleren		_	Lignal
CharterM Neue Nachriche Politierreans	Ubersieht				Hare
Generaliste Nachrichten Geleschte Nachrichten	Unterordmer	E-Mails	Neue Nachrichten Grösse	Grösse	
F Binisteisungen Gesonders Nachrichten Gelsechte Nachrichten	1 0 0	1 (0 01166) 0 (0 0166) 0 (0 10166)	0 talles 0 bytes 0 talles		
	Total	,	4	0 bytes	
	Stanveet/kat				

Abbildung 11: WebMail-Interface

Über die Benutzeroberfläche von WebMail kann der externe Kommunikationspartner seine E-Mails lesen und beantworten, neue E-Mails versenden sowie E-Mails löschen. Darüber hinaus kann er sie bei Bedarf auf seinen Desktop runterladen (EML, HTML, PDF). Das Auswahlmenü in der linken Spalte ist leicht verständlich und gleicht dem bekannter WebMail-Anbieter wie GMX, T-Online etc., d. h., alle Menüoptionen sind selbsterklärend.

Sollte der externe Kommunikationspartner bereits registriert sein und eine neue verschlüsselte E-Mail ausgehend von einer Mailbox eines Mitarbeiters der Deutschen Telekom zugestellt worden sein, bekommt er von TrustMail® eine Benachrichtigung per E-Mail, dass eine neue Nachricht in WebMail für ihn bereitgestellt wurde:

Instanti Neue skhere Nachechi martet
Absender: mstal a matage-systems.com
Frequency uter@denotin.com -
Antwort and Dautor-cont (1)
Datama 18.00.2010.09/21
testuser01
Mustafa Musta (mustafa musta(gt. systems.com) hat ihnen eine vertrauliche Nachricht gesendet, deren Sicherheitsstafe es nicht erlaubt, die Nachricht unverschlüsselt zu übermitteln.
Sie haben sich bereits zu einem früheren Zeitpunkt auf unserem WebMail Server als WebMail User registriert. Natzen Sie hren Web Browser um die Nachricht unter https://www.mysafemail.w/ekom.de/SecMailfogin.jsp?username=user@domain.com sicher lesen zu können.

Abbildung 12: Benachrichtigung über zugestellte WebMail



Der externe Kommunikationspartner kann in WebMail eine neue E-Mail nur an interne Mitarbeiter bzw. Funktionsmailboxen der Deutschen Telekom adressieren. Eine Antwort auf eine zugesandte E-Mail kann ebenfalls nur um interne Mitarbeiter bzw. Funktionsmailboxen der Deutschen Telekom erweitert werden. Diese Einschränkung soll verhindern, dass die WebMail-Anwendung für Telekomfremde Kommunikation missbraucht wird.

Empfang und Versand von E-Mails mit Hilfe von PushedPDF.

Im Folgenden wird beschrieben, wie ein externer Kommunikationspartner sich in WebMail erstmalig registrieren und auf die ihm zugestellten, E-Mails zukünftig in Form von PDF-konvertierten und weitergeleiten E-Mails zugreifen kann.

Registrierung des externen Kommunikationspartners in WebMail und PDF-Zustellung:

Da mit der o. a. E-Mail (vgl. Abbildung 7) nur ein One Time Password (OTP) vergeben wird, muss der externe Kommunikationspartner ein neues Passwort für die zukünftige Absicherung der PDF-Dateien erstellen:

••Systems•	Trusted Services [®] Security four Data is Motor	
Benutzer informationen Sie wirden siebes automatisch repistiert. I	Urs de gesisterte E-Mailzu en aben, fullin Sie bille de untenstehende fiorm ave und senden Sie sie zurück.	
Benutzer ID:	uter@domain.com	
Voter Name:	testuseOt	
Neues Pacewort		
Pesswort bestätigen		
Sproche	Deutsch 🖌	
	Tenter E Minister	

Abbildung 13: Passworterstellung für Absicherung der PDF-Dokumente

Er muss danach analog zu Abbildung 10 drei Sicherheitsfragen beantworten. Anschließend ist der externe Kommunikationspartner als PDF-Empfänger registriert und bekommt zukünftig alle verschlüsselten E-Mails ausgehend von einer Mailbox eines Mitarbeiters der Deutschen Telekom als verschlüsselte PDF-Dokumente per E-Mail direkt zugestellt:

2) Tatarte Travillad Wakita I. Karouari Internet	Leptorer harvitgeitett over 7 Spitzees	20
Las Buttle with finder Long 1		
🔾 brak - 💭 💽 📓 🏠 🔎 bere	👷 Terraturi 🥹 📴 - 🍒 📰 - 🔚 🛍	
salaran 🔄 https://www.mysalamak.teakun.de/bechallodho	nget-atoritione.htp	🗟 🔯 vedselaa 👘
··· T ···Systems·	Trusted Services [®] second row data evaluate	
Registrerung erfolgreich beenide Die haten sich erfolgreich als PCP Br Revenderienzer sich erheiten.	f - gränger registeret. Dass beseudet dass i ihner von nun an alle sicheren Nachrichsen als verschütstelle PDF Dokume	ns buges with werden Sie ofernen the

Abbildung 14: Erfolgreiche Registrierung für die PDF-Zustellung

Das verschlüsselte PDF-Dokument, das die zugestellte E-Mail enthält, kann auf Empfangsseite nur mit dem entsprechend vom Empfänger zuvor spezifizierten Passwort geöffnet werden:

5) (Thursday area	all 1: PDF Nachricht, Technall, Microsoft Internet Explorer heraligistellt was 7 System	
Car Batter wall		
G pass + O	🖬 🗑 🕐 Yean Xilinates 🗞 😳 🖑 🗐 . 🦰 📅	
Administration (Nerverson)	gentel.debsplogrowb222pl5pl5pl5alwindb_actors=drowb_adwids_nbcs=3dCH	Vetsehzu - Lzi
😑 (it mail		a the pressure of factory a divide
60 M	 A stress of secs (Theorem) if seems 15 secs (Theorem 9 sec) 	weathdan haft
Dedeer	lictuit. FOF Nubrick: Testmal	1
Postcingerg (1)	Absender metalsindslik-interson j	
Ditwin's	Englanger buldsger in 🗋	
General General	Accessit on: Institit cylines can [-]	
E obet	Estats Heat 15.22	
a voice	🦸 Techniqui	
	testuser01 Mustafa Musta (muscafa musca@t-systems.com.) hat hinen eine vermauliche Nachrin Nachricht unverschlüssoft zu einem früheren Zeitpunkt als PDF Empfänger registriert. Na Nachricht zu eisen	cht gesencet, deren Sicherheihsstufe es nicht erlaufu, die utzen Sie Ihren PDF Reacer um die als Anhang gesendete
	Die Nachricht wurde mit dem Passwort verschlusseit, welches Sie bei der Registren.	ing eingegeben hoben.
	Bitte artworten Sie nicht auf diese vom System genenorte Benachnotogung.	
	Eventuel insisterende E-Meik-Anhänge werden in dem PDF Dokument verlagter sen benutzen, so klicken sie einfech auf die Baroklammer in der unteren linken Ecke des	n. Sollten sie belispieleweise den Acobe Acrobet Roeder Roeder Fensters, um ihre gesemten Anhänge zu sohen

Abbildung 15: PDF-Empfang 01

ein.	eu par- ist geschu	Ezt, Geben sie ein K	ennwort zum (Jirrnen des Liokur	nents
	ĸ	ennwort eingeben:	******		
				-	a lancestaria

Abbildung 16: PDF-Empfang 02

Ein bereits bei WebMail registrierter externer Kommunikationspartner (vgl. Punkt "Empfang und Versand von E-Mails über Webmail.") kann sich auch jederzeit später dafür entscheiden, zukünftig E-Mails als verschlüsselte PDFs zugestellt zu bekommen. Hierfür muss er dann in WebMail ein neues Passwort angeben, mit dem zukünftig die PDFs verschlüsselt werden. Bereits erhaltene E-Mails, die über WebMail abgerufen werden können, werden jedoch nicht automatisch rückwirkend nach PDF konvertiert, verschlüsselt und zugestellt. Der externe Kommunikationspartner kann sich jedoch die bereits gespeicherten E-Mails in WebMail als verschlüsselte PDF-Dateien herunterladen.

Will der externe Kommunikationspartner auf eine PDF-konvertierte E-Mail in Form einer verschlüsselten E-Mail antworten, so ist dies nur über WebMail möglich. Der Zugriff auf WebMail erfolgt mittels einer URL, die im PDF-Dokument angegeben ist:

📵 Testmail(1].pdf (GISCHÚTZT) - Adobo Roade		- 6
Duter Beater	ten Avonon Dokumert Werlonupe Fer		
19 🌒	• 🦻 🗇 🖗 🗉 🕫 💌	• m A 🕺	
6			
•	user@domain.c	com	
	area Garana		_
	Von:	mustafa.musta@t-systems.com	
	Gesendet:	Mi 17.03.2010 15:17	
	An:	user@domain.com	
	Betreff:	Testmail	
	Antworten:	Klicken Sie hier.	

Abbildung 17: Antwort auf PDF-E-Mail



Eine Antwort (Reply) auf die E-Mail, die das verschlüsselte PDF-Dokument enthält, ist nicht zulässig, da die E-Mail nicht zum ursprünglichen internen Absender gelangt und die E-Mail nicht verschlüsselt verschickt wird. Darauf wird in der zugestellten E-Mail mit dem verschlüsselten PDF-Dokument an mehreren Stellen hingewiesen.

Passwort zurücksetzen.

Sollte der externe Kommunikationspartner das Passwort für WebMail aus irgendwelchen Gründen verloren bzw. vergessen haben, so kann er es unter Angabe der bei der Registrierung spezifizierten Antworten zu den Sicherheitsfragen zurücksetzen und neu definieren.

Hierzu muss er auf der Anmeldeseite mit der Maus auf "Passwort vergessen?" klicken:

🕽 Talamo TrustMail WebMail - M	
Data dasbatan Alakta Parada	film ()
(3 Test + () + 💽 📓	🕽 🔎 Suchen 👷 Pavarken 🔗 🎯 - 🌄 🔟 - 🔜 🗱
Adresur Antes://www.mysafemal.tele	m.de/SecMal/logn.pp
•• T ••Systems•	Trusted Services [®] Sensing Har Cate in Million
Anmelden	Benutter ID Passwort vergessen? Etislagen

Abbildung 18: Passwortzurücksetzung initiieren

Danach muss er seine E-Mail-Adresse spezifizieren:

·· T ··Systems·	Trustee Services [®] Insuring Your Cast in Million	
Zurucksetzen Hier können Sie	des Passworts Ihr Passwort nit Hilfe der zuvor definierten Sicherheitstragen zurück setzen. Bite geben Sie ihre E Ma Ihre E Mail Adresse	al Adresse cin.

Abbildung 19: E-Mail-Angabe bei Passwortzurücksetzung

Im darauf folgenden Schritt muss er die Sicherheitsfragen genauso beantworten wie bei der Registrierung:

··· T·· Systems·	Thusted Services [®] desures muchative addres
Zursicksetzen de Bitte geben Sie de Was was in Spitans Cost in welden Stad hat Paris Woltminh? Jim Fails Sie die Acord	s Passworts für die E-Mail-Adresser usen@domain.com (Artekoten en, welche Sie huner für de von ihren ausgewählten Pragen gegeten haben, an is Bren Ruslief? In Sie Bren Patrieite den Patrieite zum eintermal getreffen?

Abbildung 20: Sicherheitsfragen bei Passwortzurücksetzung

Hat der externe Kommunikationspartner die richtigen Antworten angegeben, so kann er ein neues Passwort vergeben:

··· T ··Systems·	Trusted Services [®] sensing that data in datase
Passwort andern Hynes Passwort Passwort bestätigers	

Abbildung 21: Passwort neu vergeben

Bekanntmachung der ausstellenden CA.

Beim externen Kommunikationspartner kann es zu Warnhinweisen hinsichtlich der Signatur kommen. Dies kann dann passieren, wenn der E-Mail-Client des externen Kommunikationspartners die Zertifizierungsstelle (Trustcenter der Deutschen Telekom AG), die das Zertifikat des internen Mitarbeiters ausgestellt hat, noch nicht kennt:

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

In diesem Fall muss der externe Kommunikationspartner dem anliegenden Zertifikat vertrauen bzw. es importieren. Im Folgenden ist dies exemplarisch auf einem Windows-PC dargestellt.

Mit einem Klick auf das Signatursymbol erscheint folgendes Fenster:

ligitale Signatur: Un			X
Informationen zur Zei	rtifizierungs	stelle	
Ihre Nachricht wurde mit Zertfizierungsstelle ausge Die Signatur ist ungültig, «	einem Zertifika estellt wurde, da Sie der folg	it, das von ein digital signiert. enden Zertifizi	er erungsstelle richt
vertrauen oder sie noch n	icht als vertra	wenswürdig eit	igestuft haben:
Ausgestellt von: Gültig ab:	CA Com 21.08.20	pany 08 bis 16.09.2	020
Kicken Sie auf "Details", u erhaten, das für die digt.	m weitere Inf ale Signatur d	ormationen zur er Nachricht ve	n Zertifikat zu rwendet wurde.
			Details
Der Zertifizierungsste	lle vertraue	n	
Ener Zertifizierungsstelle die mit Zertifikaten von die als vertrauenswürdig eins	zu vertrauen eser Zertifizier tufen.	bedeutet, dass ungsstelle digt	Sie Nachrichten, tal signiert wurden,
Möchten Sie diese Zertifiz	ierungsstelle a	als vertrauens»	vürdig einstufen?
Wenn Sie "Vertrauen" wäl "Stammzertifikalsspeicher Ihren System hinzugefug	hlen, müssen 1 " auch auf "Ja t werden kann	Sie im nächsber i" käcken, dami N	Dialogfeld Ldas Zertifikat
Zertifizierungsstelle ar	zeigen	Vertrauen	Schleßen
Vor Fehlern in digital si	onierten Nach	e is bit and the	Officers manners

Anschließend muss der Zertifizierungsstelle vertraut werden:

rtificat	anzeig	2m		<u> </u>
Algemein	Details	Zentifizierungsplad	Vertrauen	
Der Vert vertraue die ange Empfang usw.	rauenssta n, der die gebenen jen von E-	tus gibt an, ob Sie de ses Zertifikat ausges Zwecke verwendet w Mal, Bestimmen der	er Person, Gruppe (tellt wurde. Ein Ze erden, zum Beispie Vertrauenswürdigk	oder Firma rtifikat kann für I Senden und eit einer Website,
DatZ	entitik at al	verhauenswürdig ei	satuten tur	
E-Mai	Verschlüs	selung und Authentil	idierung	
Vetra	venistatu	bearbeiten		
	Verhause	sstatue des Ausstelle	ra izberrehown	
0	Dieses Z	ertifikat als vertrauens	würdig einstuten.	
0	Dieses Z	entifikat als nicht verts	auenowiadig einstu	len.

Dies muss anschließend bestätigt werden:



Jetzt muss noch das User-Zertifikat importiert werden. Dafür bitte erneut das Signatursymbol anklicken und anschließend auf "Details" klicken:

Informationen zur Ze	rtifizierungsstelle
Ihre Nachricht wurde mit Zertifizierungsstelle ausge	einem Zertifikat, das von einer istelk wurde, digital signiert.
vertrauen oder sie noch r	ucht als vertrauenswürdig eingestuft haben:
Ausgestellt von: Gültig ab: Hicken Sie auf "Detais", u erhäten, das für die digt	CA Company 21.00.2000 bis 16.00.2020 In wetere Informationen zun Zerbfikat zu ale Signatur der Nachricht verwendet wurde.
	Detais
Der Zertifizierungsste	lle vertrauen
Einer Zertifizierungsstelle die mit Zertifikaten von di als vertrauenswürdig eins	zu vertrauen bedeutet, dass Sie Nachrichten, eser Zentifizierungsstelle digital signiert wurden, Aufen.
Möchten Sie diese Zertifiz	ierungsstelle als vertrauenswürdig einstufen?
Wenn Sie "Vertrauen" wä "Stammzertifikatsspeicher Ihrem System hinzugefüg	hlen, müssen Sie im nächsten Dialogfeld " auch auf "Ja" klicken, damit das Zertifikat t werden kann.
[

Und daraufhin bitte auf die Schaltfläche "Vertrauen" klicken:

-	10 AL 10000	(03) - 112WS	
Betref	E: Neue sichere Nachri	icht wartet	
Nachrichten er Jede Digitalsig Sicherheitss Wählen Sie ein	ithalten u.U. Verschlüss naturschicht kann mehri chichten e Signaturschicht aus, i	ekungs- oder Digitalsign ere Signaturen enthalter um deren Beschreibung (aturschichten n. anzuzeigen.
Betreff: I Digit/	Neue sichere Nachricht slsignaturschicht Signierer: user@domain	wartet	
Jeschreibung:			
Beschreibung:			~
Jeschreibung: Achtung: Die Zertifikats benötigt wird,	sperniste, die zur Überp Ist entweder nicht verf	rüfung des Signaturzer Tigbar oder nicht mehr g	tilkats jäkig.
Deschreibung: Achtung: Die Zertifikats benötigt wird, Signaturschich	sperniste, die zur Überp ist entweder nicht verf undfinammer die unter t die Schaltflächen, um w zu erhalten oder um si	rüfung des Signakurzen ügber oder nicht mehr g insurank mer und PEA/Ek weitere Informationen zu e zu bearbeiten:	tilikats jukig. «A rum r gewählten
Deschreibung: Die Zertifikats benötigt wird, Gistist um b dicken Sie auf Jignaturschich Vertrauen	sperniste, die zur Überp ist entweder nicht verf um öhnemer die under ti die Schaltflächen, um w t zu erhalten oder um si Detalis anzeigen	rüfung des Signakurzen ügbor oder nicht mehr g insusark mar uns DEA/Ek eitere Informationen zu e zu bearbeiten: Zertifizierungsstelle v	ulikats ukig ah
Deschreibung: Achtung: Die Zertifikats benötigt wird, Sieniset wen h dicken Sie auf Jignaturschich Vertrauen	sperniste, die zur Überg ist entweder nicht verf um ähnemes der ister t die Schaftlichen, um wi t zu erhalten oder um si Detals anzeigen (digital signierten Nac	rüfung des Signeturzer ligber oder nicht mehr g innsredens und DEN för either Informsbionen zu e zu bearbeiten: Zertifizierungsstelle v trichten Warnhinweis a	efikats jukig. r gewählten vertrauen

Der Vertrauensstatus gibt an, ob Sie der Perse vertrauen, der deses Zertfikat ausgestellt wu die angegebenen Zwecke verwendet werden, Enforangen von E-Mail, Bestimmen der Vertrau usw. - Das Zentfikat als vertrauenswürdig einstufen E-Mail-Verschlüsselung und Authentifizierun	n, Gruppe oder Firma rde. Ein Zertfikat kann für zum Bespiel Senden und enswürchglich einer Website für
- Das Zentifikat als vertrauenswärdig einstuten E-Mal-Verschlüsselung und Authentifizierun	1
E-Mal-Verschlüsselung und Authentifizierun	1
Vertrauencstatus bearbeiten Vertrauencstatus des Ausstellers üben Dieses Zettilikat als vertrauenswardig Dieses Zettilikat als nicht vertrauensw	ehnen einstufen Liidig einstufen

Hier bitte ebenfalls das Zertifikat als vertrauenswürdig einstufen. Danach sollte das Zertifikat inklusive der ausstellenden Zertifizierungsstelle erfolgreich importiert worden sein und es sollten keine Warnhinweise mehr kommen:

Elgenschafte	en der Nachrichte	nsicherheit	X
Betreff	: Neue sichere Nachri	cht wartet	
Nachrichten en Jede Digitalsign	thaiten u.U. Verschlüss aturschicht kann mehre	elungs- oder Digitalsignati sre Signaturen enthälten.	urschichten.
Sicherheitss	chichten		
Wählen Sie eine	e Signaturschicht aus, u	m deren Beschreibung an	zuzeigen.
→ Digta ✓ Si	lsignaturschicht gnierer: user@domain	com	
Beschreibung:			
Beschreibung: OK: signierte N	iachricht.		
Beschreibung: OK: signierte M Klicken Sie auf	lachricht. die Schaltflächen, um w zu erhalten oder um si	eitere Informationen zur (e zu bearbeiten:	gewähiten
Beschreibung: OK: signierte M Kilcken Sie auf Signaturschicht	lachricht. die Schaltflächen, um w zu erhalten oder um si	eitere Informationen zur o e zu bearbeiten:	pewähiten trauen
Beschreibung: OK: signierte M Kicken Sie auf Signaturschicht Vertrauenus Bei Fehlern	lachricht. die Schaltflächen, um w zu erhalten oder um si Cetalo anzeigen in digital signierten Naci	eitere Informationen zur e e zu bearbeiten: Zertifizierungsstelle ve	gewählten rtrauen
Beschreibung: OK: signierte N Klicken Sie auf Signaturschicht Vertrauenung Bei Fohlern	lachricht. die Schaltflächen, um w zu erhalten oder um si Oetalo anzeigen. in digital signierten Naci	eitere Informationen zur e e zu bearbeiten: Zertifizierungsstelle ve hrichten Warnhinweis anz	pewähiten rtrauen

Behebung von Problemen.

Adobe Reader kann keine Zip-Dateien öffnen.

Adobe Reader in den Versionen 7, 8 und 9 können keine Attachments öffnen, die Zip-Dateien enthalten. Die Ursache ist eine restriktive Policy-Einstellung von Adobe in der Windows Registry, da Zip-Dateien Schadprogramme enthalten können.

Falls Sie als externer Kommunikationspartner "PushedPDF" (vgl. Punkt "Empfang und Versand von E-Mails mit Hilfe von PushedPDF.") für die verschlüsselte E-Mail-Kommunikationsbeziehung mit einem oder mehreren Mitarbeitern der Deutschen Telekom ausgewählt haben, so kann Sie diese Einschränkung bei einer Standardinstallation von Adobe Acrobat Reader betreffen, falls Ihnen eine verschlüsselte E-Mail mit einer oder mehreren Zip-Dateien als Anhang zugeschickt wird.

Man kann diese Einstellung in der Registry ändern, was im Folgenden beschrieben wird.



Eine Änderung in der Registry sollte nur in Absprache mit der IT-Abteilung sowie konform zu den Behörden- bzw. Unternehmenssicherheitsrichtlinien durchgeführt werden. Die Änderungen sollten <u>ausschließlich</u> von entsprechendem Fachpersonal (z. B. Windows-Administration) vorgenommen werden.

Adobe Acrobat Reader 7.x:

Führen Sie folgende Schritte aus, um die Windows Registry zu editieren und die Sicherheitseinstellungen für die Behandlung von Datei-Attachments im Adobe Acrobat Reader 7 zu ändern:

- 1. Wählen Sie Start > Run.
- 2. Tippen Sie regedit in die Open Box und klicken Sie dann OK, um den Windows Registry Editor zu starten.
- 3. Navigieren Sie zu dem folgenden Registry-Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\AcrobatReader\[versionnumber]\ FeatureLockdown\cDefaultLaunchAttachmentPerms
- 4. Doppelklicken Sie auf den Wert: sBuiltInPermList
- Scrollen Sie (falls nötig), um die Dateityperweiterung (.zip) zu lokalisieren. Die Dateityperweiterung ist in der rechten Spalte der Werteliste dargestellt.
- 6. Editieren Sie die Zahl, die direkt hinter der Dateityperweiterung folgt, und ändern Sie den Wert auf 1: . z i p: 1

Nähere Informationen sind zu finden unter: http://kb2.adobe.com/cps/331/331371.html

Adobe Acrobat Reader 8.x, 9.x:

Die notwendige Modifikation ist ähnlich wie die für Adobe Acrobat Reader 7.x. Lediglich die Lokation des Registrierungsschlüssels in Schritt 3 lautet anders:

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

Abkürzungsverzeichnis.

DMZ	Demilitarisierte Zone
DTAG	Deutsche Telekom AG
OTP	One Time Password

TrustMail® ist eine registrierte Marke der Totemo AG.

Office Standardization. E-Mail Encryption Gateway. Anleitung für externe Kommunikationspartner. Stand: 12.01.2011

Herausgeber

Deutsche Telekom AG Programm Office Standardization

Kontakt

Internet: http://os.telekom.de E-Mail: trust@t-systems.com

