

# Office Standardization. E-Mail Encryption Gateway.

Anleitung für externe Kommunikationspartner.

Erleben, was verbindet.



## Einleitung.

Der E-Mail Encryption Gateway, der im Folgenden „TrustMail®“ 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.....	8
Empfang und Versand von E-Mails über WebMail.....	10
Empfang und Versand von E-Mails mit Hilfe von PushedPDF.....	12
Passwort zurücksetzen.....	14
Bekanntmachung der ausstellenden CA.....	16
Behebung von Problemen.....	19
Abkürzungsverzeichnis.....	20
<b>Abbildungsverzeichnis</b>	
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: Erstmöglicher Webzugang in WebMail.....	9
Abbildung 9: Registrierung in WebMail.....	10
Abbildung 10: Beantwortung von Sicherheitsfragen.....	10
Abbildung 11: WebMail-Interface.....	11
Abbildung 12: Benachrichtigung über zugestellte WebMail.....	11
Abbildung 13: Passwörterstellung für Absicherung der PDF-Dokumente.....	12
Abbildung 14: Erfolgreiche Registrierung für die PDF-Zustellung.....	12
Abbildung 15: PDF-Empfang 01.....	12
Abbildung 16: PDF-Empfang 02.....	13
Abbildung 17: Antwort auf PDF-E-Mail.....	13
Abbildung 18: Passwortzurücksetzung initiieren.....	14
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.

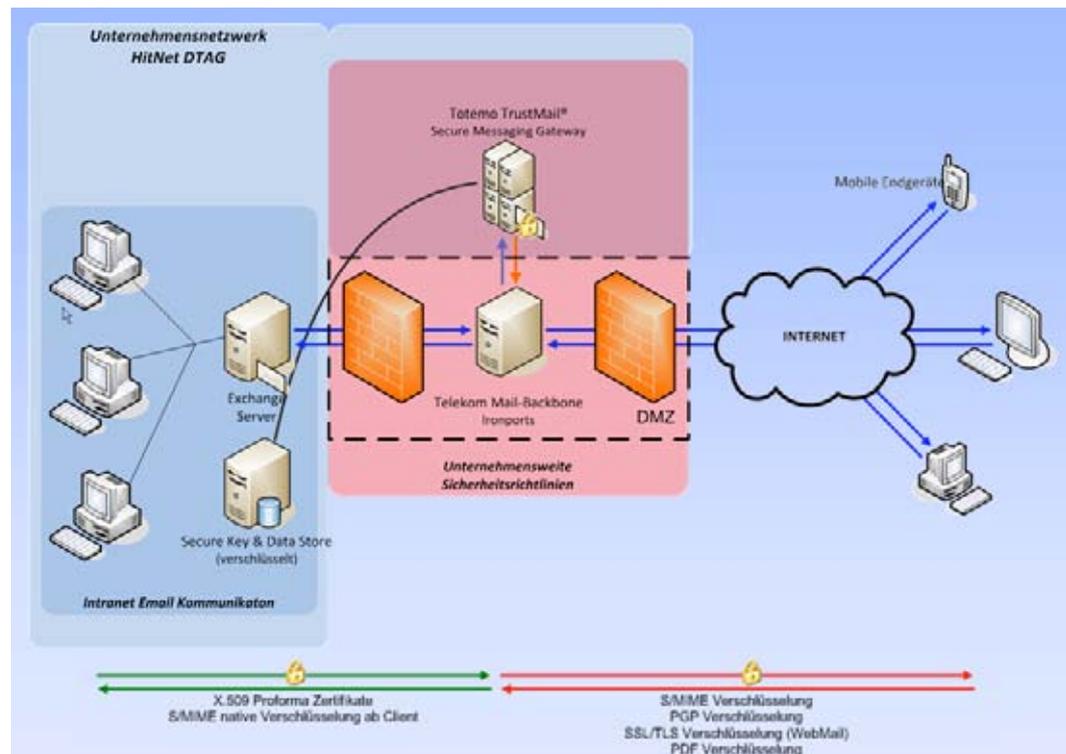


Abbildung 1: Ende-zu-Ende-Verschlüsselung von E-Mails

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.

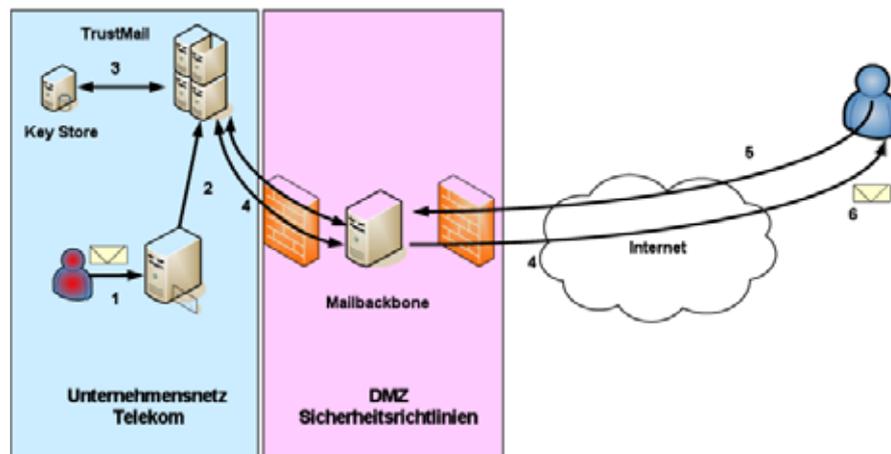


Abbildung 2: Mailfluss bei bereits verfügbarem S/MIME- oder PGP-Schlüssel für Verschlüsselung

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.
3. 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:

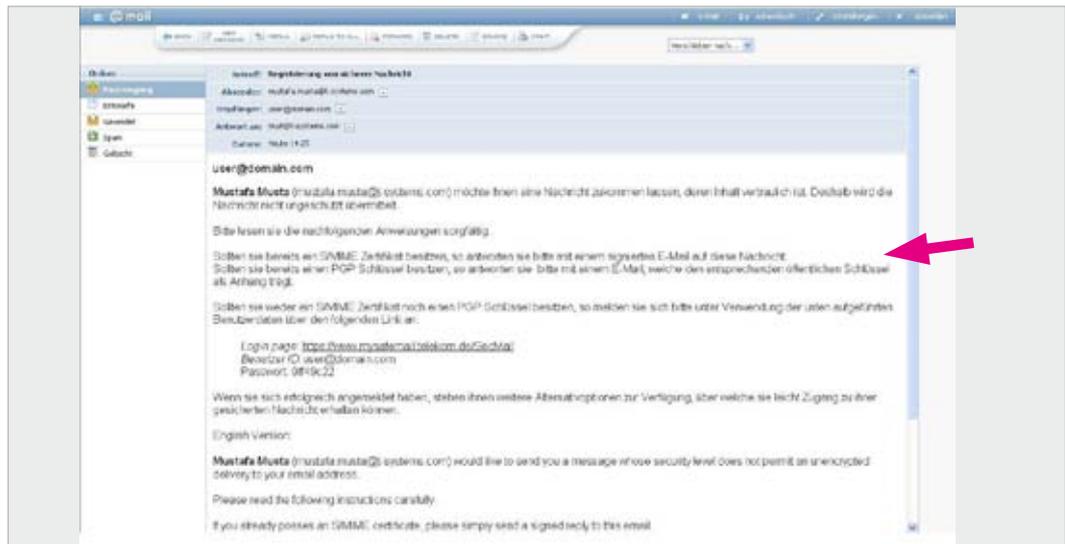


Abbildung 3: Benachrichtigung zum erstmaligen Registrieren

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:



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 verwendete Verschlüsselungstechnologie entweder mit S/MIME verschlüsselt und zugestellt:



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

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

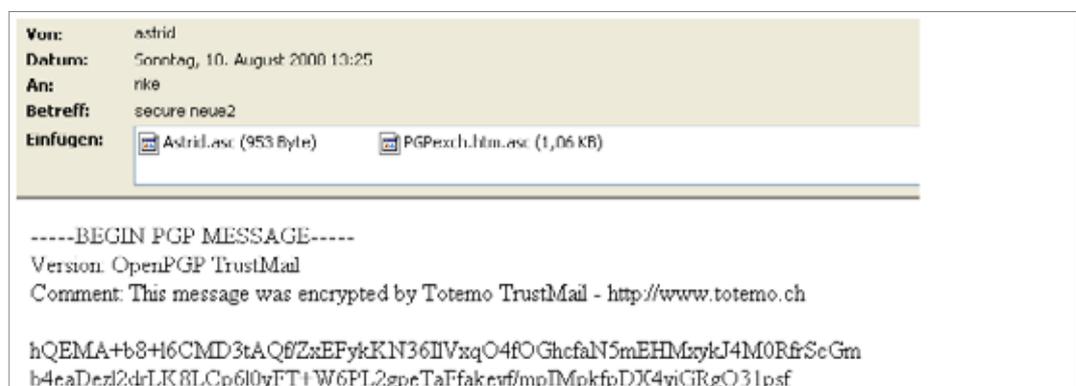


Abbildung 5: Empfang einer verschlüsselten PGP-E-Mail



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.

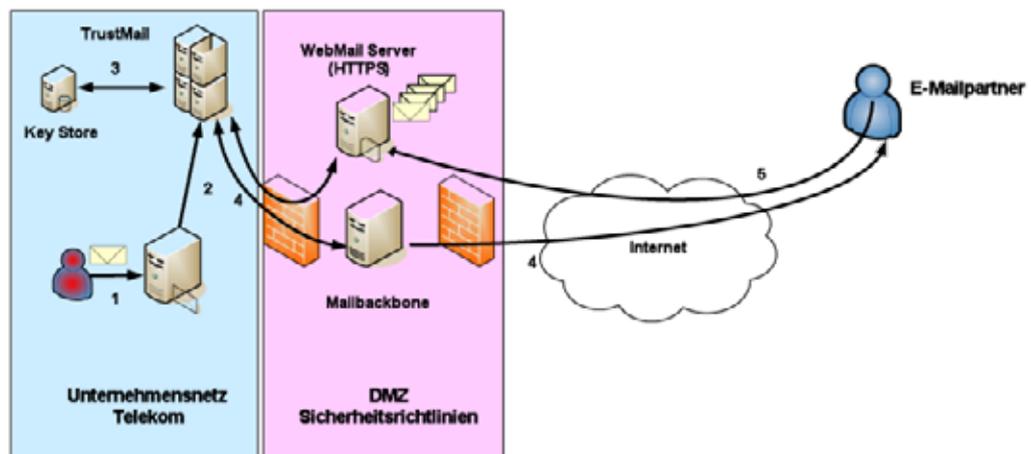


Abbildung 6: Mailfluss bei nicht vorhandenem S/MIME- oder PGP-Schlüssel und Verwendung von WebMail

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.
3. 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:

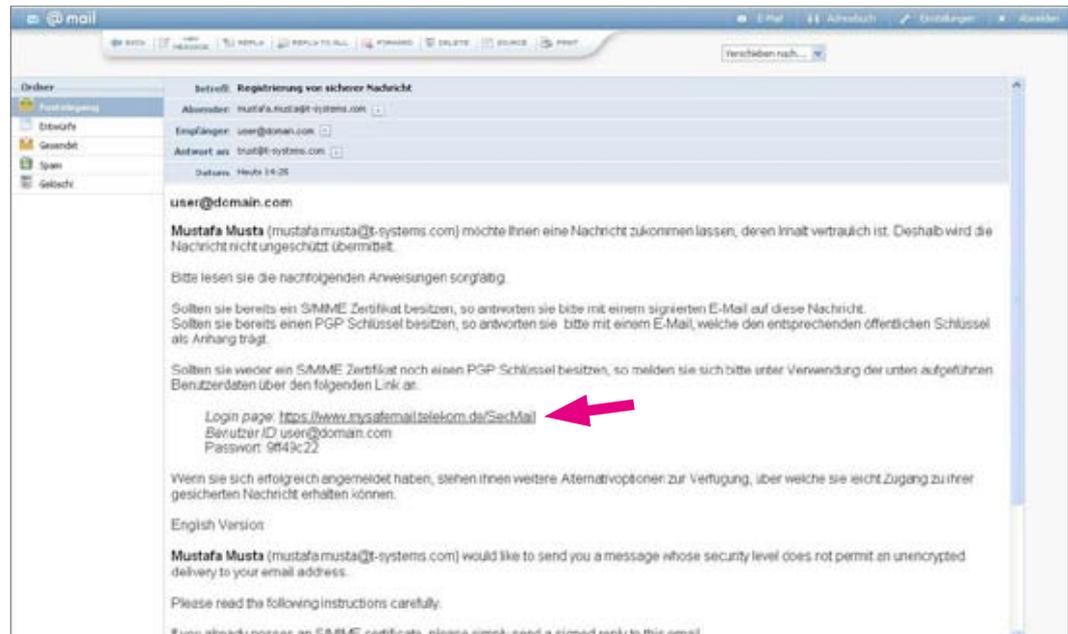


Abbildung 7: Benachrichtigung zum erstmaligen Registrieren

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:

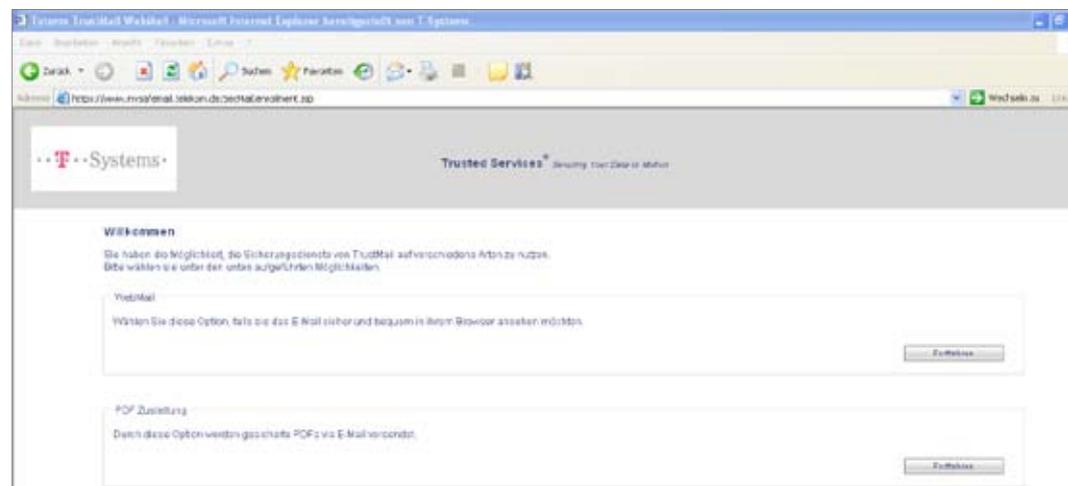


Abbildung 8: Erstmöglicher Webzugang in WebMail

### 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:



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 Sicherheitsfragen sind der Webseite zu entnehmen.

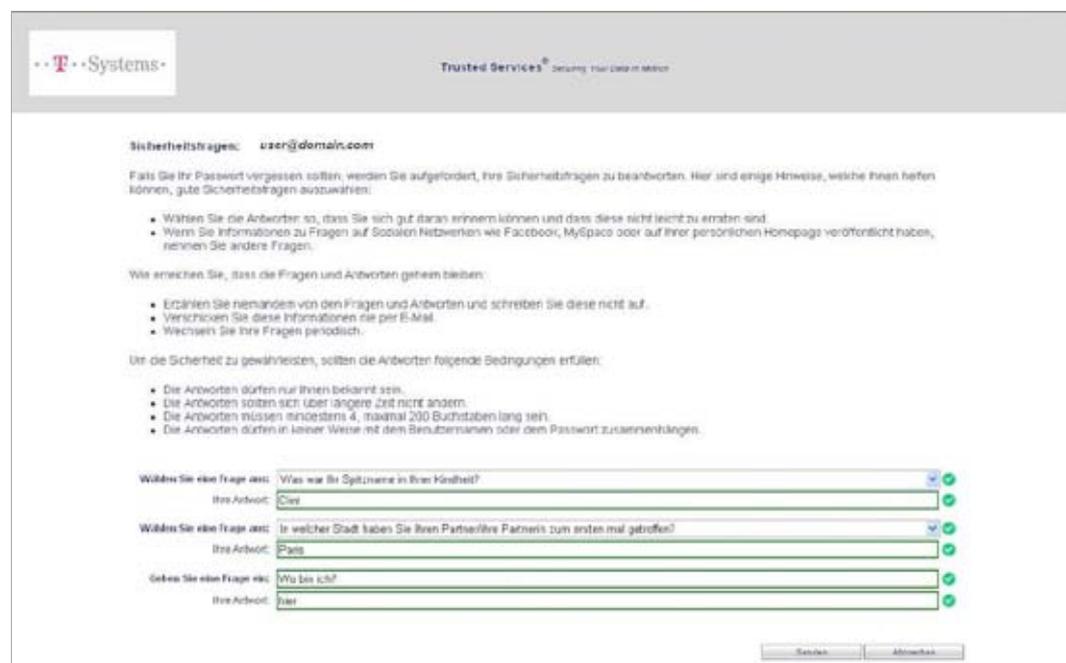


Abbildung 10: Beantwortung von Sicherheitsfragen

### 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:

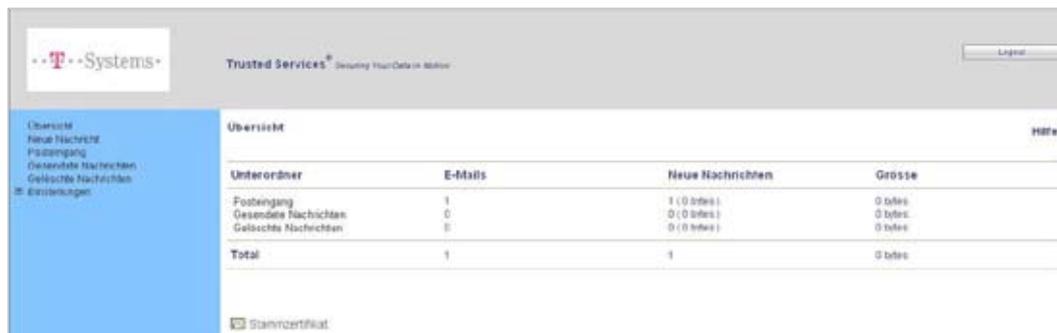


Abbildung 11: WebMail-Interface

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:



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 weitergeleiteten 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:



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:

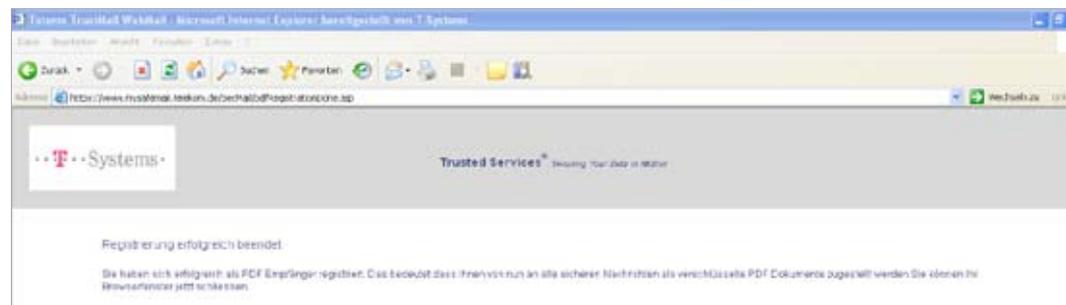


Abbildung 14: Erfolgreiche Registrierung für die PDF-Zustellung

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

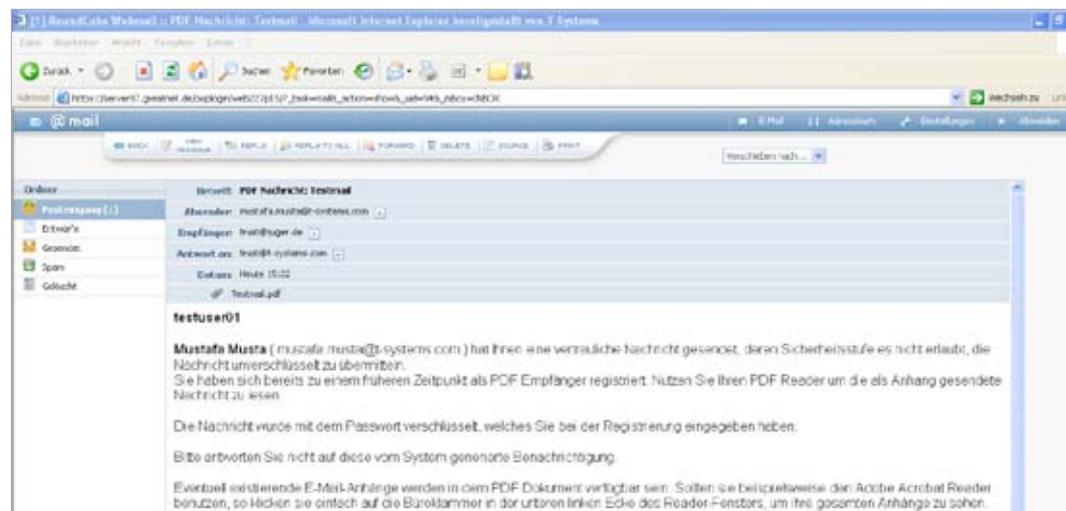


Abbildung 15: PDF-Empfang 01

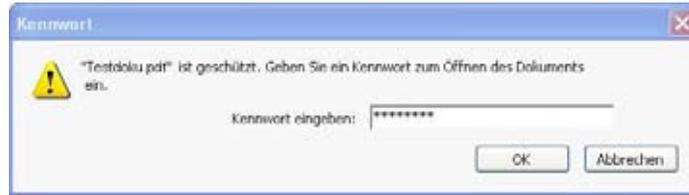


Abbildung 16: PDF-Empfang 02



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:

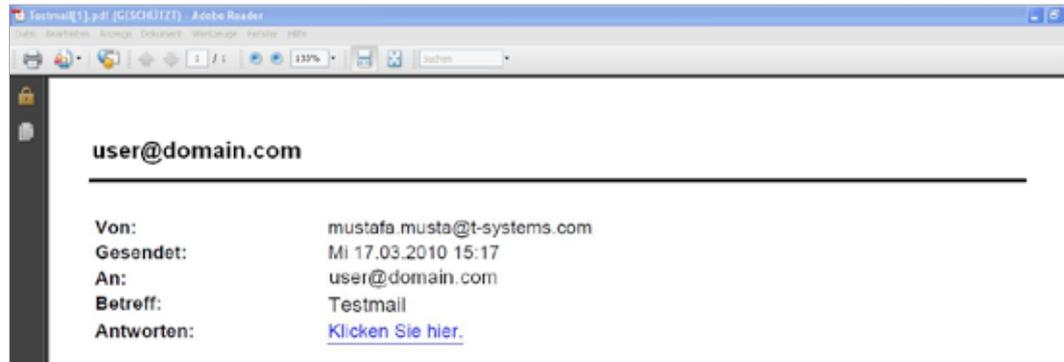


Abbildung 17: Antwort auf PDF-E-Mail



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:

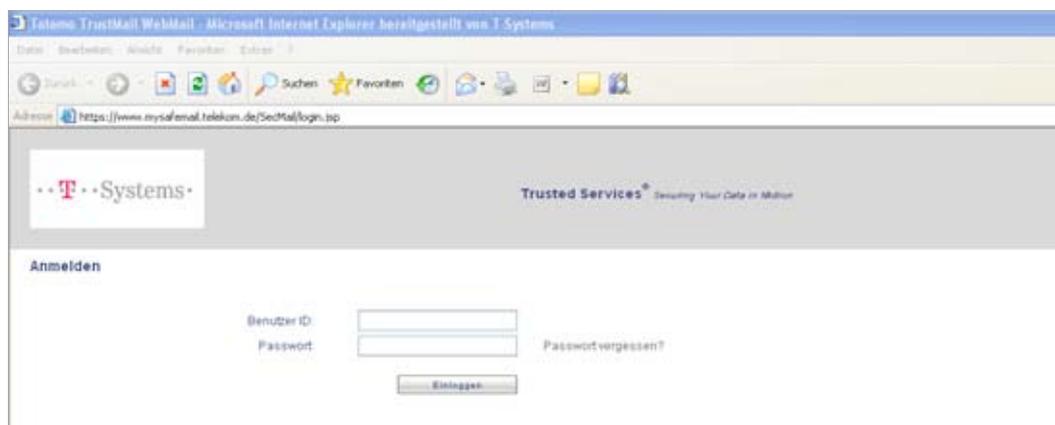


Abbildung 18: Passwortzurücksetzung initiieren

Danach muss er seine E-Mail-Adresse spezifizieren:

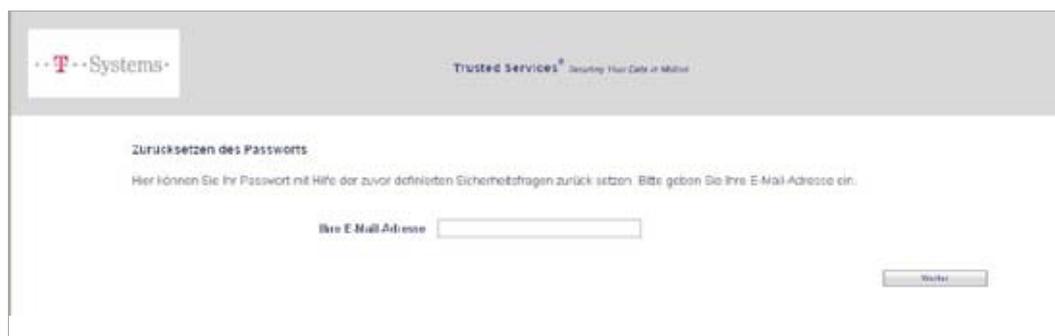


Abbildung 19: E-Mail-Angabe bei Passwortzurücksetzung

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



The screenshot shows a web interface for password reset. At the top left is the logo for 'T-Systems' and at the top right is 'Trusted Services' with the tagline 'Securing Your Data in Motion'. The main heading is 'Zurücksetzen des Passworts für die E-Mail-Adresse: **user@domain.com**'. Below this, a message reads: 'Bitte geben Sie die Antworten ein, welche Sie früher für die von Ihnen ausgewählten Fragen gegeben haben.' There are three security questions with input fields: 'Was war die Spitze von Ihrer Nase?' (input: 'Cint'), 'In welcher Stadt haben Sie Ihren Partner/ Ihre Partnerin zum ersten Mal getroffen?' (input: 'Paris'), and 'Wo bin ich?' (input: 'hier'). A note at the bottom states: 'Falls Sie die Antworten nicht mehr wissen, nehmen Sie bitte mit Ihrem Kommunikationspartner Kontakt auf.' There are 'Zurück' and 'Weiter' buttons at the bottom right.

Abbildung 20: Sicherheitsfragen bei Passwortzurücksetzung

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



The screenshot shows a web interface for changing a password. At the top left is the logo for 'T-Systems' and at the top right is 'Trusted Services' with the tagline 'Securing Your Data in Motion'. The main heading is 'Passwort ändern'. Below this, there are two input fields: 'Neues Passwort:' and 'Passwort bestätigen:'. A 'Speichern' button is located below the second input field.

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. Klicken 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:



Anschließend muss der Zertifizierungsstelle vertraut werden:



Dies muss anschließend bestätigt werden:



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



Und daraufhin bitte auf die Schaltfläche „Vertrauen“ klicken:





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:



# 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 ausschließlich 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\[versionnummer]\FeatureLockdown\cDefaultLaunchAttachmentPerms`
4. Doppelklicken Sie auf den Wert: `sBuiltInPermlist`
5. 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: `.zip: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

---

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](mailto:trust@t-systems.com)

Erleben, was verbindet.

