E-MAIL ENCRYPTION GATEWAY

Anleitung für externe Kommunikationspartner

Deutsche Telekom Security GmbH

Version 2.0
Stand 03.2022

ERLEBEN, WAS VERBINDET.

Impressum

HERAUSGEBER

DEUTSCHE TELEKOM SECURITY GMBH
Bonner Talweg 100
53113 Bonn

Telefon: 0228 181-0 | E-Mail: info@telekom.de | Internet: www.telekom.de/security
Aufsichtsrat: Adel Al-Saleh (Vorsitzender) | Geschäftsführung: Thomas Fetten (Sprecher), Dr. Klaus Schmitz, Thomas Tschersich
Handelsregister: Amtsgericht Bonn HRB 15241, Sitz der Gesellschaft Bonn | USt-IdNr. DE 254595345 | WEEE-Reg.-Nr. DE 56768674

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Dieses Dokument beschreibt die Funktionen des E-Mail Encryption Gateways (im nachfolgenden EEGW genannt) die dem externen Kommunikationspartnern der Deutschen Telekom zur Verfügung stehen um vertrauliche E-Mails sicher zu empfangen. Das EEGW bietet folgende Möglichkeiten verschlüsselte E-Mails zu senden und zu empfangen:

- mittels eines sicheren WebMail-Portals
- mittels einer verschlüsselten HTML Datei
- mittels eines S/MIME Zertifikats
- mittels eines PGP Schlüssels

Über die Zustellung einer verschlüsselten E-Mail wird der externe Empfänger durch eine automatisiert generierte Benachrichtigung per E-Mail informiert. Mit Hilfe eines WebMail-Portals kann der Empfänger nach erfolgreicher Registrierung und nachfolgender Authentifizierung alle ihm zugestellten verschlüsselten E-Mails lesen.

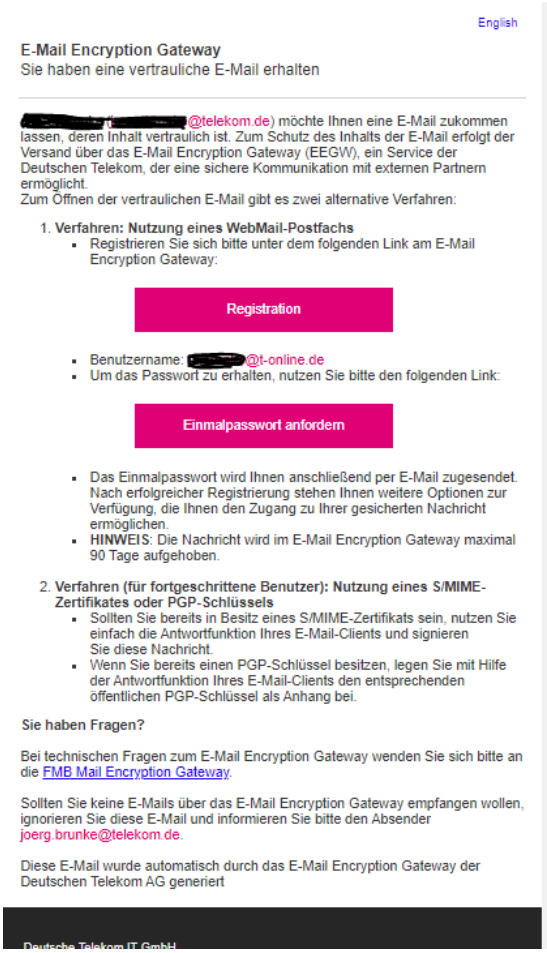
Falls ein externer Empfänger über die S/MIME- bzw. PGP-Technologie verfügt, kann er E-Mails auch direkt verschlüsselt empfangen bzw. versenden.

Alternativ zum WebMail-Portal kann der externe Kommunikationspartner eine Weiterleitung der an ihn adressierten verschlüsselten E-Mails konfigurieren. Die weitergeleiteten E-Mails werden dabei inklusive Anhängen in ein verschlüsseltes HTML-Dokument konvertiert. Durch ein zuvor von ihm in WebMail spezifiziertem Passwort können das HTML Dokument entschlüsselt werden. Man spricht hier von einer sogenannten „Registered Envelope“-Technologie.

2 WebMail Portal

2.1 Nutzung des WebMail Portals

Wenn ein externer Empfänger bisher noch keine verschlüsselte Nachricht von der Deutschen Telekom bekommen hat und somit nicht auf dem EEGW registriert ist, wird die originale Mail eines internen Absenders aus dem Telekom Konzern im EEGW zurückbehalten. Anstelle dessen erhält der externe Empfänger automatisiert die folgend dargestellte Benachrichtigung über die Zustellung einer verschlüsselten E-Mail.



English

E-Mail Encryption Gateway
Sie haben eine vertrauliche E-Mail erhalten

[redacted]@telekom.de) möchte Ihnen eine E-Mail zukommen lassen, deren Inhalt vertraulich ist. Zum Schutz des Inhalts der E-Mail erfolgt der Versand über das E-Mail Encryption Gateway (EEGW), ein Service der Deutschen Telekom, der eine sichere Kommunikation mit externen Partnern ermöglicht.
Zum Öffnen der vertraulichen E-Mail gibt es zwei alternative Verfahren:

1. **Verfahren: Nutzung eines WebMail-Postfachs**
   - Registrieren Sie sich bitte unter dem folgenden Link am E-Mail Encryption Gateway:

   Registration

   - Benutzername: [redacted]@t-online.de
   - Um das Passwort zu erhalten, nutzen Sie bitte den folgenden Link:

   Einmalpasswort anfordern

   - Das Einmalpasswort wird Ihnen anschließend per E-Mail zugesendet. Nach erfolgreicher Registrierung stehen Ihnen weitere Optionen zur Verfügung, die Ihnen den Zugang zu Ihrer gesicherten Nachricht ermöglichen.
   - **HINWEIS**: Die Nachricht wird im E-Mail Encryption Gateway maximal 90 Tage aufgehoben.
2. **Verfahren (für fortgeschrittene Benutzer): Nutzung eines S/MIME-Zertifikates oder PGP-Schlüssels**
   - Sollten Sie bereits in Besitz eines S/MIME-Zertifikats sein, nutzen Sie einfach die Antwortfunktion Ihres E-Mail-Clients und signieren Sie diese Nachricht.
   - Wenn Sie bereits einen PGP-Schlüssel besitzen, legen Sie mit Hilfe der Antwortfunktion Ihres E-Mail-Clients den entsprechenden öffentlichen PGP-Schlüssel als Anhang bei.

Sie haben Fragen?

Bei technischen Fragen zum E-Mail Encryption Gateway wenden Sie sich bitte an die FMB Mail Encryption Gateway.

Sollten Sie keine E-Mails über das E-Mail Encryption Gateway empfangen wollen, ignorieren Sie diese E-Mail und informieren Sie bitte den Absender joerg.brunke@telekom.de.

Diese E-Mail wurde automatisch durch das E-Mail Encryption Gateway der Deutschen Telekom AG generiert

Deutsche Telekom IT GmbH

Um die E-Mail lesen zu können, muss sich der Empfänger am WebMail Portal registrieren bzw. anmelden. Dies erfolgt über den in der Benachrichtigung angegebenen Link des Portals:“Login Page“ (https://www.mysafemail.telekom.de). Ihm wird darauf die folgende Eröffnungsseite in seinem Web- Browser angezeigt:

Abbildung 1 Benachrichtigung zum erstmaligen Registrieren

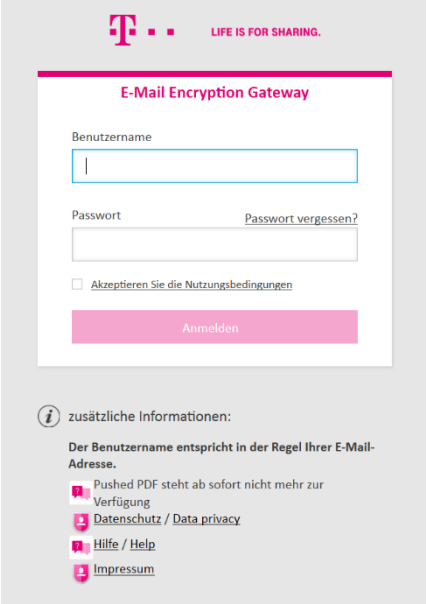
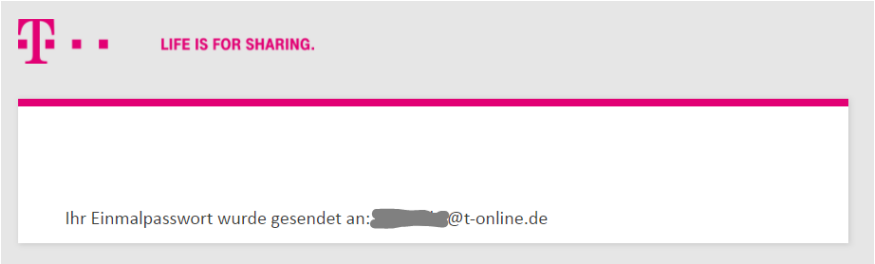


Abbildung 2 WebMail - Portal

Zur Anmeldung am WebMail-Portal wird der Benutzername (hier die E-Mailadresse des Empfängers) und das Passwort benötigt.
Nach Betätigung des Passwort-Links „Einmalpasswort anfordern“ aus der ersten Benachrichtigungsmail (*Einmalpasswort anfordern*) , wird ein Einmalpasswort zugesendet.



Der externe Empfänger erhält daraufhin eine E-Mail ähnlich der folgend abgebildeten:

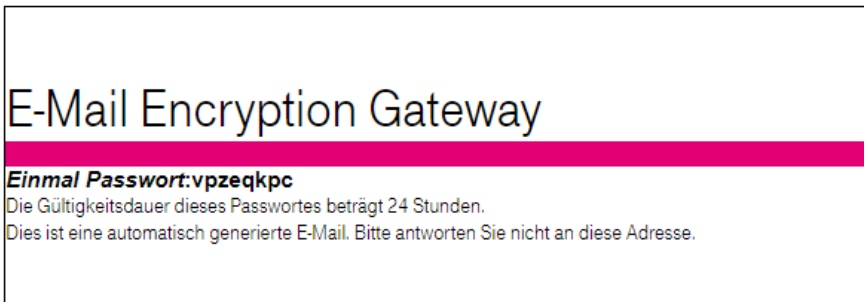
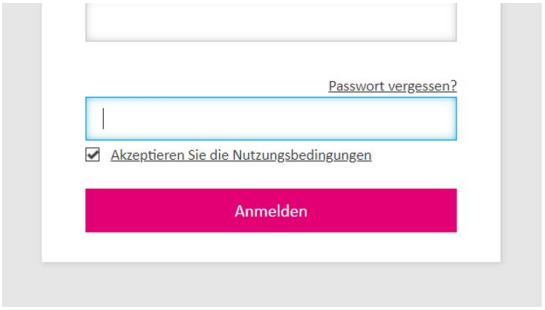


Abbildung 3 Benachrichtigung mit Einmal Passwort

Bitte beachten, der „Anmelden“ Button wird erst aktiv, wenn die Nutzungsbedingungen akzeptiert wurden.



Nach erfolgreicher Anmeldung erfolgt die eigentliche Registrierung und die Vergabe eines eigenen sicheren Passworts.

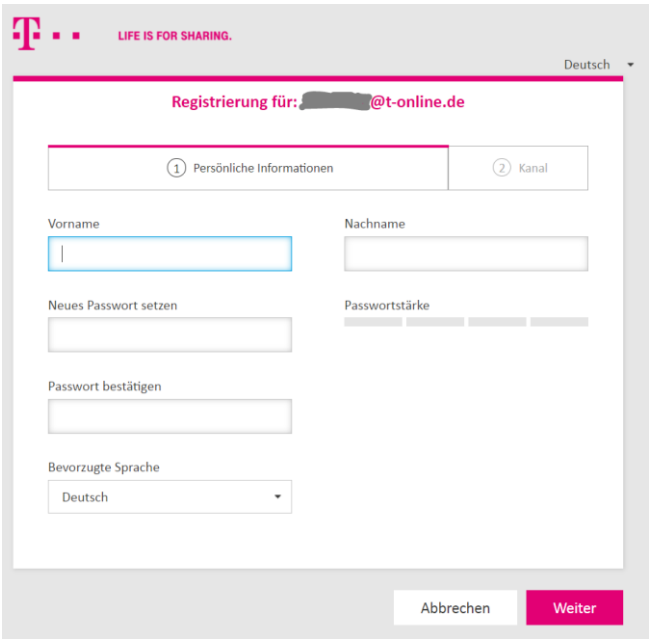


Abbildung 4 Erstmalige Registrierung

Auf der nächsten Seite muss entschieden werden, ob man verschlüsselte Mails

a) im WebMail-Portal erhalten möchte

b) **als verschlüsseltes HTML Dokument direkt zugesendet bekommen möchte (Registered Envelope)**

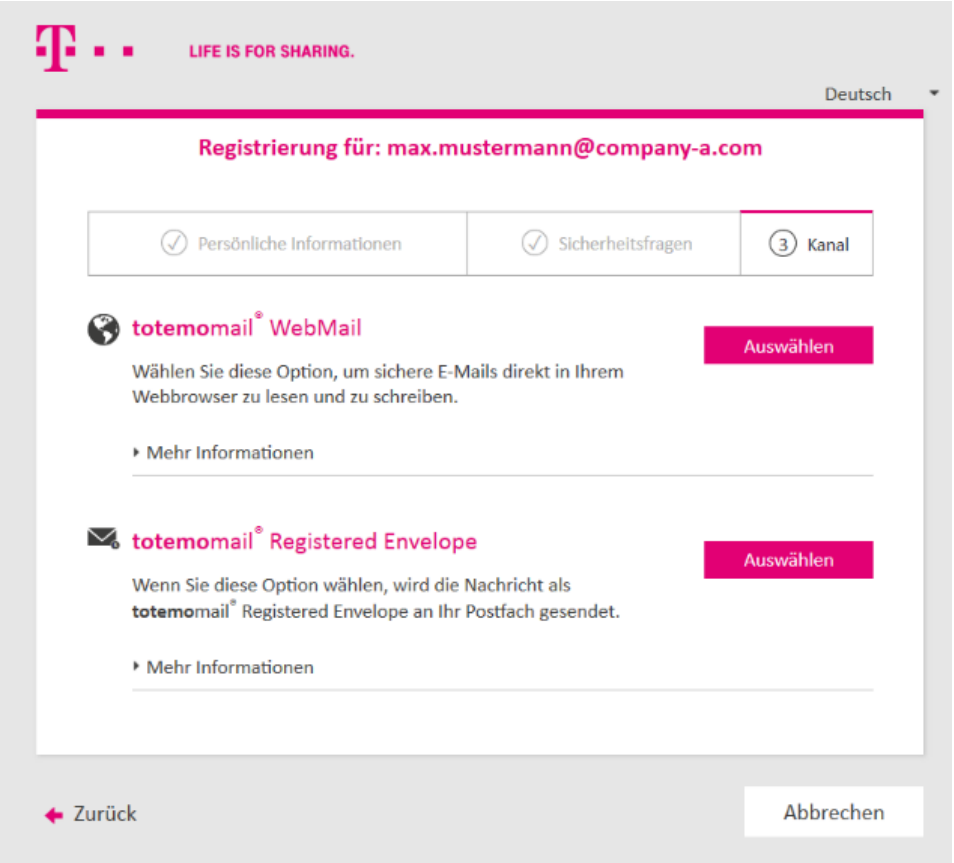


Abbildung 5 Auswahl der sicheren Übertragungsart

Die Option „WebMail“ bedeutet, dass die verschlüsselten E-Mails inklusive etwaiger Anhänge dem externen Kommunikationspartner nicht direkt zugestellt werden, sondern über das WebMail-Portal (vergleichbar mit WebMail-Anwendungen wie z. B. GMX oder Web.de) zu lesen sind.

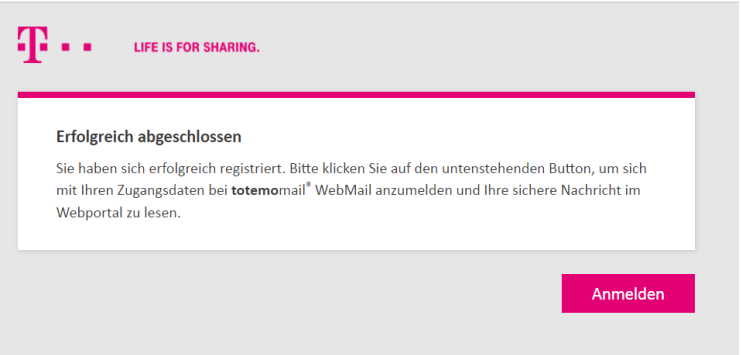
Die Option „Registered Envelope“ bedeutet, dass die für ihn hinterlegte E-Mail inklusive etwaiger Anhänge in ein HTML- Dokument konvertiert und mit einem vorher von ihm selbst zu spezifizierenden Passwort verschlüsselt wird. Dieses HTML-Dokument wird dem externen Kommunikationspartner per E-Mail zugestellt.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

2.1.1 Funktionen der WebMail-Schnittstelle.

Im Folgenden wird beschrieben, wie man sich im WebMail Portal erstmalig registriert und wie man auf zugestellte E-Mails über die WebMail-Schnittstelle von EEGW® zugreifen sowie verschlüsselte E-Mails erstellen und zurücksenden kann.

Registrierung des externen Kommunikationspartners in WebMail:
Zur Nutzung des WebMail-Portals muss die Option totemomail WebMail ausgewählt werden
Achtung
Die Nutzung der WebMail Schnittstelle setzt die Aktivierung von Java Script im Webbrowser voraus.

Bei erfolgreicher Registrierung erhalten Sie folgende Meldung.



Über Anmelden muss man sich am WebMail-Portal erneut anmelden.
Benutzername: eigene E-Mailadresse
Passwort: Das selbst zuvor generierte Passwort

Nach erfolgreicher Anmeldung gelangt man auf die Übersichtsseite des WebMail-Portals. Über die Benutzeroberfläche von WebMail kann der externe Empfänger seine E-Mails lesen und beantworten, neue E-Mails versenden sowie E-Mails löschen. Das Auswahlmenü in der linken Spalte ist leicht verständlich, d. h. alle Menüoptionen sind selbsterklärend.

Empfang

Im Posteingang werden alle an den Empfänger versendeten E-Mails in der Übersicht angezeigt.

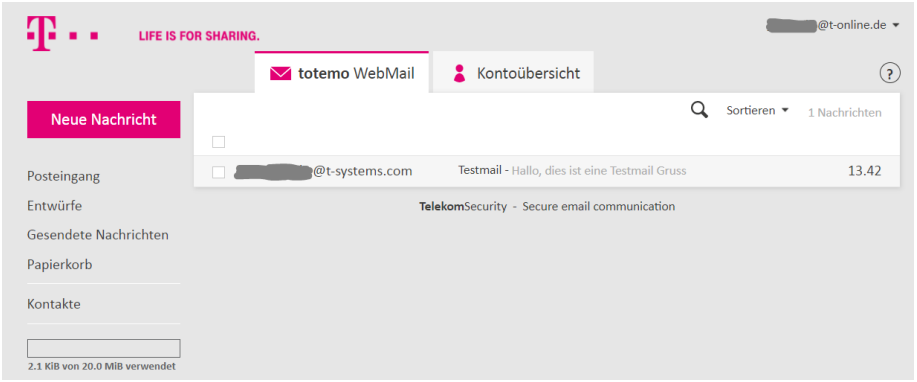


Abbildung 6 WebMail Posteingang / Übersicht

Durch das auswählen einer E-Mail besteht entweder die Möglichkeit auf die Nachricht zu Antworten oder bei Bedarf die E-Mail über die Downloadfunktion auf seinen Desktop zu laden (EML, HTML, PDF).

Sollte der externe Empfänger weitere zu sichernde E-Mails von Mitarbeitern aus dem Konzern der Deutschen Telekom erhalten, bekommt er vom EEGWeine Benachrichtigung per E-Mail, dass eine neue Nachricht im WebMail für ihn bereitgestellt wurde:

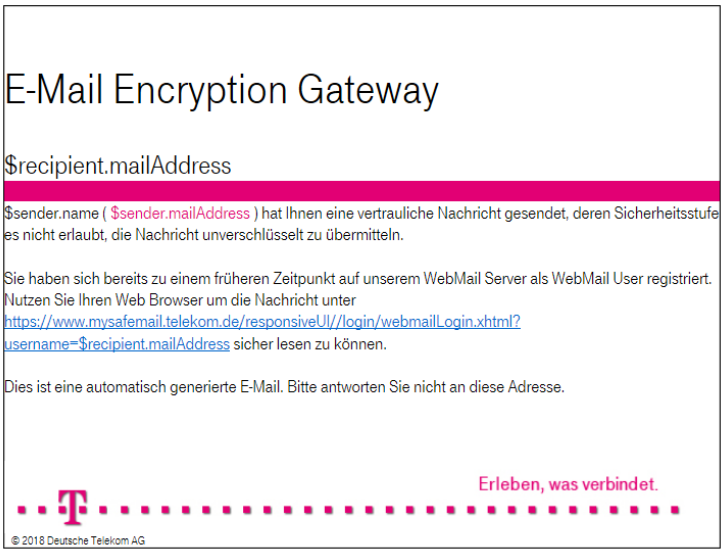


Abbildung 7: Benachrichtigung über zugestellte WebMail

Antworten

Über den Menüpunkt "Neue Nachricht" kann eine E-Mail sicher an einen internen Mitarbeiter verfasst und gesendet werden.

Achtung: Der Versand an E-Mailadressen externer Domänen ist nicht möglich.

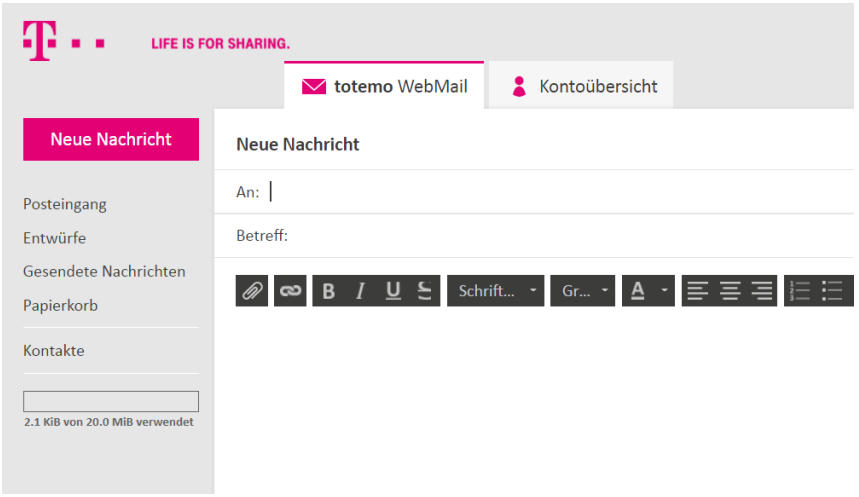


Abbildung 8 Versand aus dem WebMail

Eine E-Mail wird im Ordner "Entwurf" abgelegt, wenn sie bei dem Verfassen einer neuen Nachricht gespeichert wurde. Der Entwurf kann bearbeitet und ggf. gesendet werden.

Im Ordner "Gesendete Nachrichten" werden alle gesendeten E-Mails aufgelistet.

Im Ordner "Papierkorb" sind die gelöschten E-Mails aufgeführt. Diese Objekte sind noch nicht endgültig gelöscht und belegen nach wie vor Speicherplatz in dem WebMail-Portal. Erst durch

markieren der Objekte und ein Bestätigen durch den "Löschen" Button erfolgt die endgültige Löschung der Objekte und die damit einhergehende Freigabe von Speicherplatz.

Kontoübersicht

In der Kontoübersicht können individuelle Konfigurationen des Empfängers durchgeführt werden.

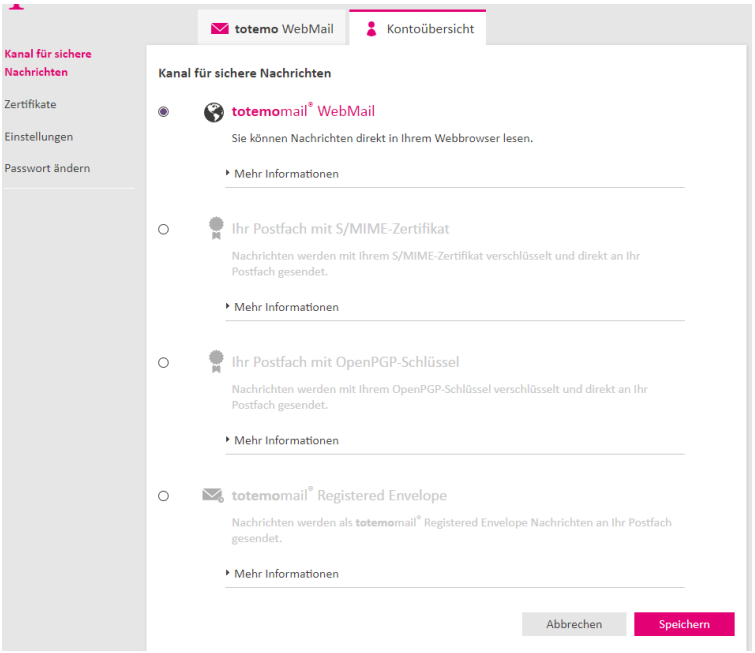


Abbildung 9 Festlegung der sicheren Übertragungsart

Kanal für sichere Nachrichten:

Hier kann die Übertragungsart der E-Mail neu festgelegt werden. Der Empfänger kann je nach Wunsch bzw. Verfügbarkeit einen der zur Verfügung stehenden Kanal wählen:

- WebMail — Zustellung der Mail im WebMail Portal
- S/MIME Zertifikat — Zustellung der E-Mail direkt und S/MIME verschlüsselt
- PGP — Zustellung der E-Mail direkt und PGP verschlüsselt
- Registered Envelope — Zustellung der Mail als verschlüsseltes HTML Doument

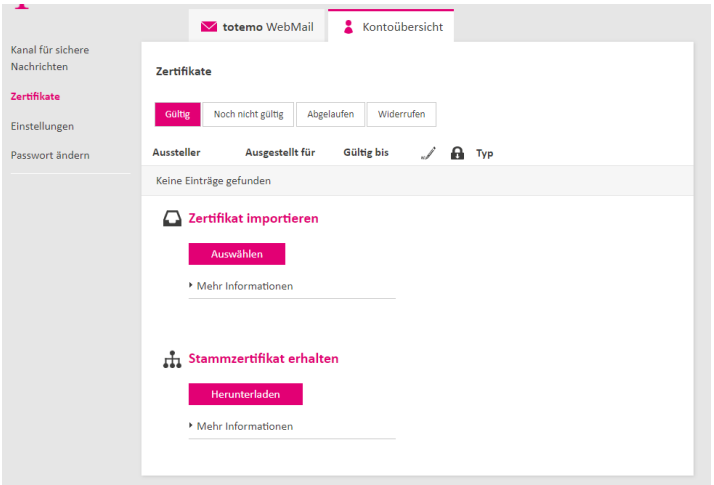


Abbildung 10 Zertifikatsimport

Zertifikate

Um zertifikats- oder PGP- verschlüsselte E-Mails direkt zugestellt zu bekommen, muss entweder ein gültiges S/MIME Zertifikat oder ein PGP Key hinterlegt sein. Über die die Funktion „Auswählen" kann ein Zertifikat oder Schlüssel in das EEGW hochgeladen werden.

Einstellungen

In den Einstellungen können persönliche Daten geändert werden, wie der Name oder die verwendete Sprache des WebMail Portals. Als Sprache kann zwischen Deutsch, Englisch, Italienisch oder Französisch gewählt werden. Des Weiteren ist es möglich eine eigene Signatur zu erstellen und die verwendeten Kontakte in einem eigenen Adressbuch zu speichern. Sollte „Gesendete Nachrichten aktivieren“ ausgewählt werden, erfolgt die Speicherung unter „gesendete Nachrishten“.

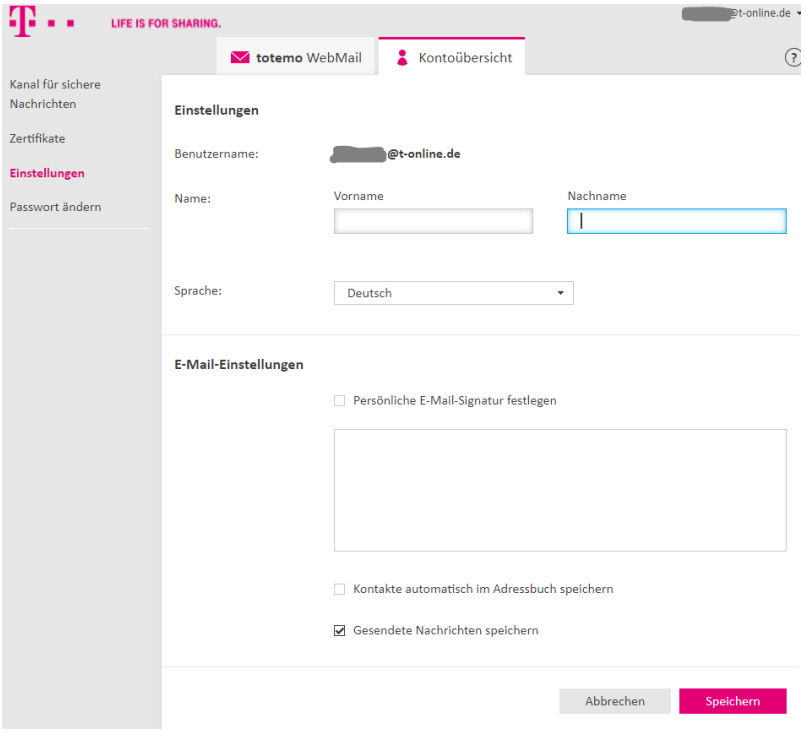


Abbildung 11 WebMail Einstellungen festlegen

Passwort ändern

Über den Auswahlpunkt ”Passwort ändern” kann ein neues Passwort gesetzt werden.

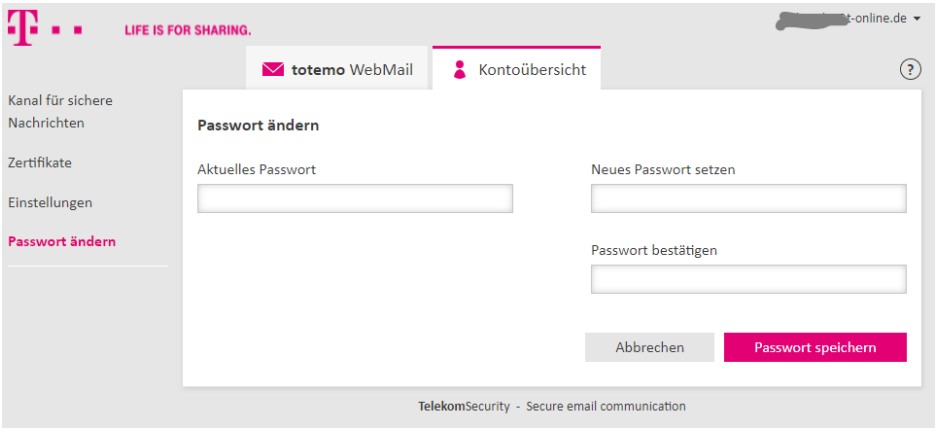


Abbildung 12 Passwort ändern

2.1.2 Empfang und Versand von E-Mails mit Hilfe von Registered Envelope (HTML Datei).

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

Registrierung des externen Kommunikationspartners in WebMail für die Registered Envelope-Zustellung:

Sollte der externe Kommunikationspartner registriert und eine neue verschlüsselte E-Mail ausgehend von einer Mailbox eines Mitarbeiters der Deutschen Telekom zugestellt worden sein, bekommt er vom EEGW eine Benachrichtigung per E-Mail, die die originale Mail nun als HTML verschlüsselten Anhang beinhaltet.

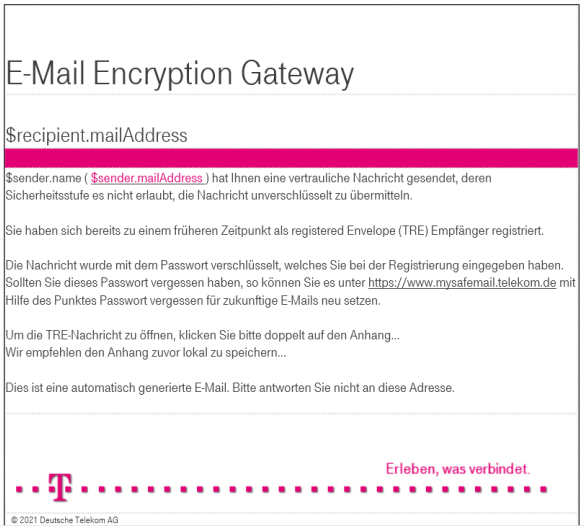


Abbildung 13: Registered Envelope-Empfang (verschl. HTML)

Das verschlüsselte HTML-Dokument, das die zugestellte E-Mail enthält, kann auf Empfangsseite nur mit dem entsprechend vom Empfänger zuvor spezifizierten Passwort geöffnet werden.
Es wird empfohlen die in der Anlage der Mail enthaltene verschlüsselte HTML Datei lokal zu speichern und anschließend mit einem Browser zu öffnen.

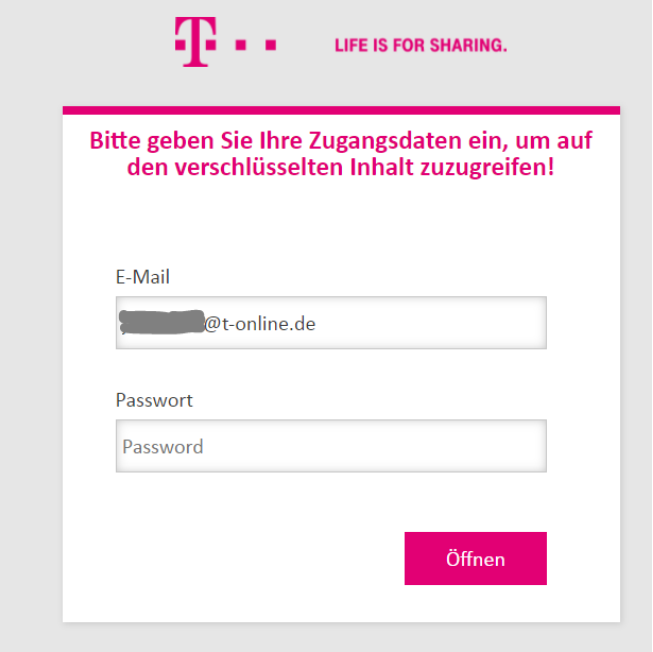


Abbildung 14 Passworteingabe für Registered Envelope

Bevor der Browser die Datei öffnen kann, muss das zuvor bei der Registrierung festgelegte Passwort eingegeben werden. Erst nach Validierung des Passworts kann der Browser die Datei öffnen. Für die Validierung ist immer zwingend eine Internetverbindung mit dem EEGW der Deutschen Telekom notwendig.

Achtung

Die Nutzung der WebMail Schnittstelle setzt die Aktivierung von Java Script im Webbrowser voraus.

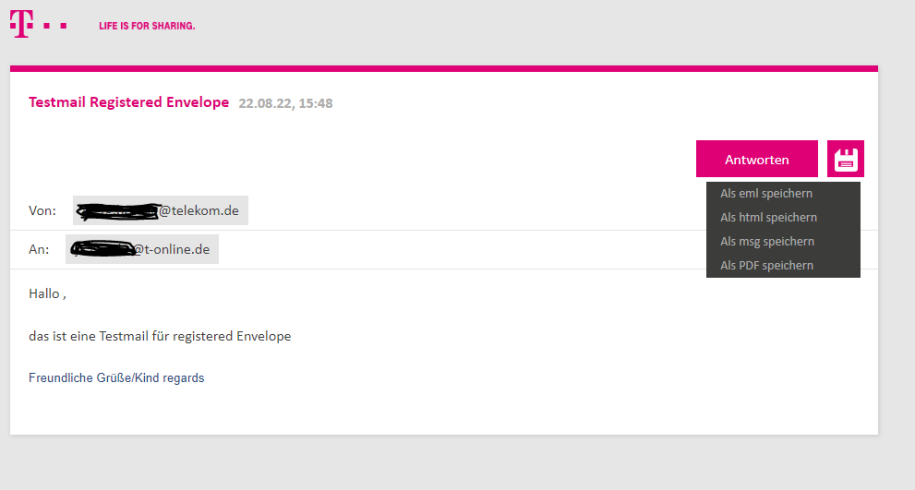


Abbildung 15 Registered Envelelope: Antworten

Antworten auf Registered Envelope

Will der externe Kommunikationspartner auf eine HTML-konvertierte E-Mail in Form einer verschlüsselten E-Mail antworten, so ist dies nur über WebMail möglich. Der Zugriff auf WebMail erfolgt mittels der bekannten URL.

https://www.mysafemail.telekom.de

Hier muss sich der Koomunikationspartner mit seiner E-Mailadresse als „Benutzername“ und seinem Passwort anmelden.

Über das Speichern Symbol besteht die Möglichkeit die Mail lokal in den dargestellten Formaten abzuspeichern. So kann beispielsweise das eml Format genutzt werden, um Mails im lokalen Mailprogramm abzuspeichern.

3 Passwort vergessen

Sollte der externe Kommunikationspartner das Passwort für WebMail aus irgendwelchen Gründen verloren bzw. vergessen haben, so besteht die Möglichkeit über die „Passwort vergessen“- Funktion das Passwort neu zu definieren.

Hierzu muss er auf der Anmeldeseite der Link „Passwort vergessen?“ gnutzt werden:

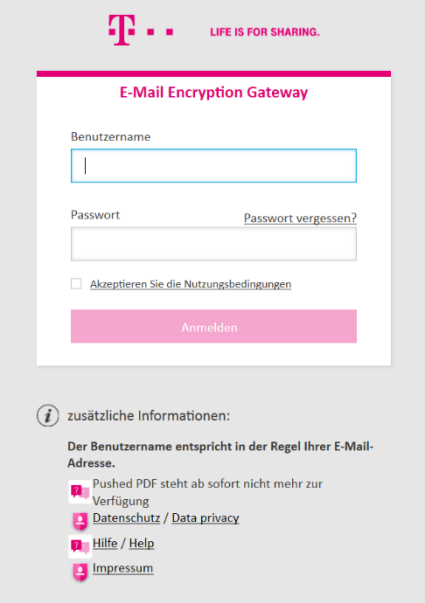


Abbildung 16: Passwortzurücksetzung initiieren

Danach muss die eigene E-Mail-Adresse eingtragen werden:

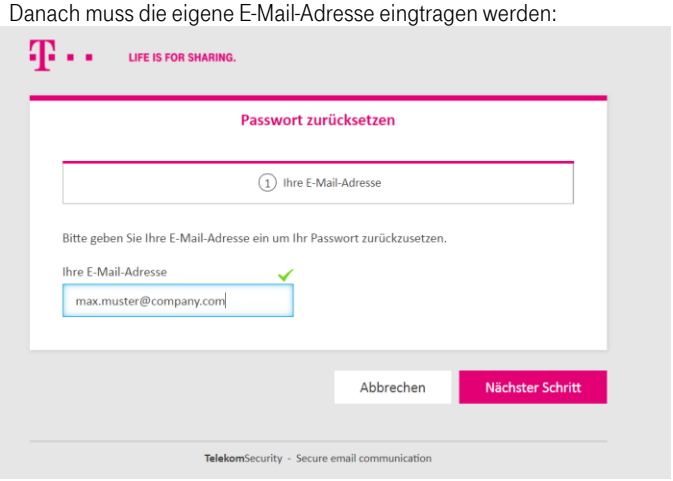


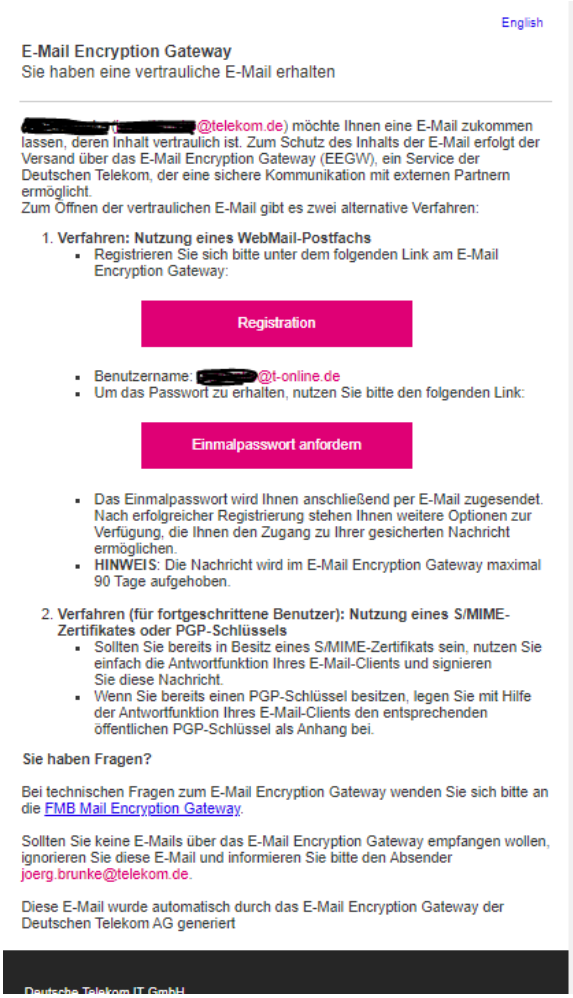
Abbildung 17: E-Mail-Angabe bei Passwortzurücksetzung

Im Anschuß wird an die angegebene E-Mailadresse ein vom System generiertes Einmalpasswort zugestellt.

4 S/MIME Zertifikat oder PGP Key

4.1 Der externe Empfänger ist im Besitz eines S/MIME Zertifikats oder PGP-Schlüssels

Wenn ein externer Empfänger bisher noch keine verschlüsselte Nachricht von der Deutschen Telekom bekommen hat und somit nicht auf dem EEGW registriert ist, wird die originale Mail eines internen Absenders aus dem Telekom Konzern im EEGW zurückbehalten. Anstelle dessen erhält der externe Empfänger automatisiert ein Benachrichtigung über die Zustellung einer verschlüsselten E-Mail.



English

E-Mail Encryption Gateway
Sie haben eine vertrauliche E-Mail erhalten

[redacted]@telekom.de) möchte Ihnen eine E-Mail zukommen lassen, deren Inhalt vertraulich ist. Zum Schutz des Inhalts der E-Mail erfolgt der Versand über das E-Mail Encryption Gateway (EEGW), ein Service der Deutschen Telekom, der eine sichere Kommunikation mit externen Partnern ermöglicht.
Zum Öffnen der vertraulichen E-Mail gibt es zwei alternative Verfahren:

1. **Verfahren: Nutzung eines WebMail-Postfachs**
   - Registrieren Sie sich bitte unter dem folgenden Link am E-Mail Encryption Gateway:

   Registration

   - Benutzername: [redacted]@t-online.de
   - Um das Passwort zu erhalten, nutzen Sie bitte den folgenden Link:

   Einmalpasswort anfordern

   - Das Einmalpasswort wird Ihnen anschließend per E-Mail zugesendet. Nach erfolgreicher Registrierung stehen Ihnen weitere Optionen zur Verfügung, die Ihnen den Zugang zu Ihrer gesicherten Nachricht ermöglichen.
   - **HINWEIS**: Die Nachricht wird im E-Mail Encryption Gateway maximal 90 Tage aufgehoben.
2. **Verfahren (für fortgeschrittene Benutzer): Nutzung eines S/MIME-Zertifikates oder PGP-Schlüssels**
   - Sollten Sie bereits in Besitz eines S/MIME-Zertifikats sein, nutzen Sie einfach die Antwortfunktion Ihres E-Mail-Clients und signieren Sie diese Nachricht.
   - Wenn Sie bereits einen PGP-Schlüssel besitzen, legen Sie mit Hilfe der Antwortfunktion Ihres E-Mail-Clients den entsprechenden öffentlichen PGP-Schlüssel als Anhang bei.

Sie haben Fragen?

Bei technischen Fragen zum E-Mail Encryption Gateway wenden Sie sich bitte an die FMB Mail Encryption Gateway.

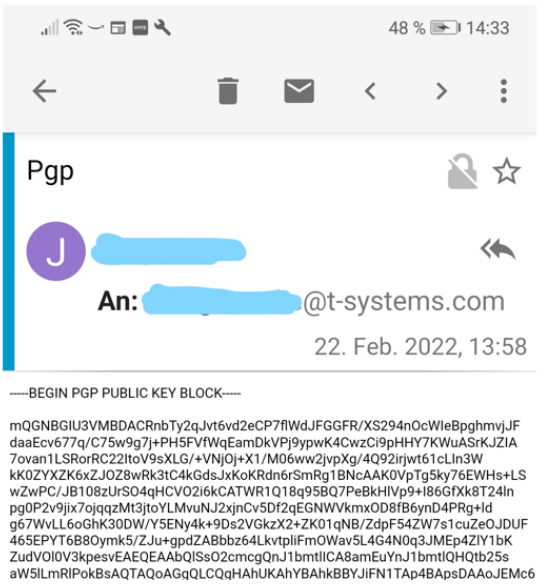
Sollten Sie keine E-Mails über das E-Mail Encryption Gateway empfangen wollen, ignorieren Sie diese E-Mail und informieren Sie bitte den Absender joerg.brunke@telekom.de.

Diese E-Mail wurde automatisch durch das E-Mail Encryption Gateway der Deutschen Telekom AG generiert

Deutsche Telekom IT GmbH

Falls der externe Empfänger bereits über eine Verschlüsselungstechnologie (PGP oder S/MIME) verfügt, so kann er sein Zertifikat bzw. seinen öffentlichen PGP-Schlüssel dem EEGW bekannt machen, damit diese zukünftig vom EEGW verwendet werden können.
Dazu braucht der externe Empfänger nur auf die Benachrichtugungsmail zu antworten.
Ist ein S/MIME Zertifikat vorhanden, muss die Antwortmail mit dem S/MIME Zertifikat elektronisch signiert werden.
Ist ein PGP Schlüssel vorhanden, muss die Antwortmail den public PGP Schlüssel enthalten. Dieser kann als Anhang im ASC Format mitgesendet werden oder direkt in die Antwortmail hineinkopiert werden.

Die Antwortmail wird im EEGW abgefangen und das enthaltene Schlüsselmaterial extrahiert und abgespeichert. Zukünftige Verschlüsselte E-Mails aus dem Telekom Konzern werden basierend auf der entsprechenden Verschlüsselungstechnologie (S/MIME oder PGP) verschlüsselt und direkt zugestellt.



5 Allgemeine Informationen

5.1.1 Postfachgröße

Das Postfach auf dem WebMail-Portal hat eine Größe von 10 MB. Daraus folgt, dass es nicht zum Speichern oder Aufbewahren von vertraulichen/verschlüsselten E-Mails gedacht ist, sondern nur die Möglichkeit bietet, diese sicher zu übergeben. Die E-Mails sollten daher möglichst zeitnah wieder aus den Webmailordnern gelöscht werden.
Auch im Papierkorb befindliche E-Mails sind noch nicht gelöscht. Erst durch markieren der Objekte und ein Bestätigen durch den "Löschen" Button erfolgt die endgültige Löschung der Objekte und die damit einhergehende Freigabe von Speicherplatz.
Bei Erreichen der Postfachspeichergrenze erhält der Sender eine Nachricht, dass die maximale Postfachgröße überschritten wurde und die E-Mail somit nicht zugestellt werden konnte. Das gilt auch für E-Mails, die einen Anhang haben, der größer als 10 MB ist.

5.1.2 Inaktivität

Nach 90 Tagen Inaktivität wird der externe Benutzer auf dem EEGW gelöscht. Sobald er dann wieder eine vertrauliche/verschlüsselte E-Mail von einem Kunden Mitarbeiter bekommt, wird er neu angelegt und bekommt damit auch eine neue Registrierungsmail.

5.1.3 Benachrichtigungen bei Nichtregistrierung

Der Sender bekommt eine Nachricht, wenn der externe Kommunikationspartner sich nach 5 Tagen nicht registriert und die E-Mail somit noch nicht gelesen hat. Der externe Kommunikationspartner bekommt nach 3 Tagen eine Nachricht zur Erinnerung, wenn er sich bis dahin nicht registriert hat. Dazu bekommt er die Registrierungsmail erneut zugesendet.

5.1.4 Löschung von E-Mails

Nach 90 Tagen werden Mails automatisch aus dem WebMailpostfach entfernt.

5.1.5 Wechsel „Kanal für sichere Nachrichten“

Sowohl als WebMail registrierte externe Empfänger als auch „Registered Envelope“ registrierte externe Empfänger können den „Kanal für sichere Nachrichten“ jederzeit ändern. Im WebMail unter Kontoübersicht kann der „Kanal für sichere Nachrichten“ geändert werden. Bereits versendete E-Mails werden jedoch nicht automatisch rückwirkend nach HTML konvertiert, verschlüsselt und zugestellt.

Für S/MIME oder PGP registrierte externe Empfänger ist das nicht ohne Weiteres möglich. Diese Empfänger benötigen erst noch ein neues Einmalpasswort.
Hierfür wenden Sie sich bitte an den Helpdesk des E-Mail Encryption Gateways. trust@t-systems.com .