



ITS-4.03

Nutzung des E-Mail-Encryption-Gateways-Handout (extern)

Version 1.2
07.03.2025

Dokument-Status: 03 - freigegeben

Toll Collect GmbH
IT Sicherheit

Dokument-Status und Freigabe				
	Datum	Name, Abteilung, Firma	Version	
Letzte Änderung	07.03.2025	A. Wendland, Chapter IT-Sicherheit, Toll Collect GmbH	1.2	
Freigabe	07.03.2025	A. Wendland, Chapter IT-Sicherheit, Toll Collect GmbH	1.2	
Dokumenten-Verantwortlicher				
Fachbereich BZS, IT-Sicherheit				
Versionshistorie				
Version	Datum	Bearbeiter	Änderungen	Bemerkungen
0.1	28.11.2019	A. Wendland	Neuerstellung	
0.2	05.12.2019	A. Wendland	Fertigstellung der Version für den internen Review	
0.95	08.01.2020	A. Wendland	Überarbeitung nach internem Review, Vorbereitung zur Freigabe und Bereitstellung für Veröffentlichung im Intranet	
1.0	22.01.2020	M. Frisch	Freigabe	
1.1	10.08.2020	A. Wendland	Änderung der Einordnung von 3.11.02 auf 4.03	
1.2	07.03.2025	A. Wendland		
Gültigkeit				
Gültig ab	Ersetztes Dokument			
07.03.2025	Version 1.1 des Dokuments			

Inhaltsverzeichnis

1	Einleitung	5
2	Registrierung	5
2.1	Variante 1 – PGP:	5
2.2	Variante 2 – S/MIME:	6
2.3	Variante 3 – Secure-WebMailer:.....	6
3	E-Mails sicher empfangen / lesen / beantworten	6
3.1	Nutzung von PGP bzw. S/MIME.....	6
3.2	Nutzung des Secure-WebMail-Dienst.....	9
4	Verschlüsselungsmethode ändern / Aktualisierung von Schlüsseln	11
5	Multi-Faktor-Authentifizierung.....	13
6	Öffentliches Schlüsselmaterial anfragen.....	15
7	Einrichten von festen Kommunikationsregeln.....	16

1 Einleitung

Die Toll Collect setzt zur Absicherung der E-Mail-Kommunikation ein zentrales E-Mail-Encryption-Gateway (im Folgenden EEGW genannt) ein.

Durch dieses EEGW werden folgende Verschlüsselungsmethoden unterstützt:

- PGP,
- S/MIME,
- Secure Web-Mail via Webzugriff auf <https://email.toll-collect.de>.

Im Folgenden wird eine Kurzanleitung gegeben, wie Sie als Externer Kommunikationspartner mit Toll-Collect-Mitarbeitern sicher per E-Mail kommunizieren.

2 Registrierung

Bei der ersten verschlüsselten E-Mail die ein Toll Collect – Mitarbeiter über das EEGW an Sie sendet, wird ein Registrierungsprozess ausgelöst. Sie erhalten eine E-Mail von secure-email@toll-collect.de mit dem Hinweis, dass eine vertrauliche Nachricht an Sie versandt worden ist (siehe Abbildung 1 - Abbildung 2).



Abbildung 1

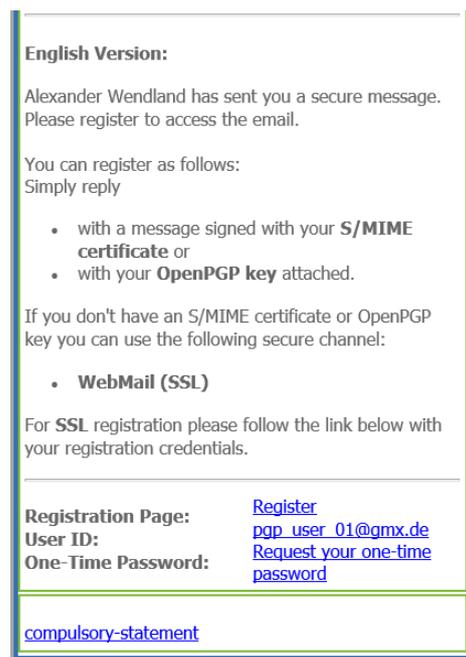


Abbildung 2

Es gibt nun 3 Varianten wie Sie auf diese E-Mail reagieren können.

2.1 Variante 1 – PGP:

Sofern Sie im Besitz eines persönlichen PGP-Keys sind antworten Sie auf diese Mail und hängen Ihren öffentlichen PGP-Schlüssel als Anhang an die Antwort-E-Mail. Damit ist Ihre Registrierung bereits abgeschlossen.

2.2 Variante 2 – S/MIME:

Wenn Sie S/MIME zur E-Mail-Verschlüsselung nutzen, antworten Sie ebenfalls auf die Registrierungs-E-Mail und signieren ihre Antwort. Damit ist für Sie die Registrierung ebenfalls abgeschlossen.

2.3 Variante 3 – Secure-WebMailer:

Sollten Sie weder PGP noch S/MIME nutzen können, gibt es eine weitere Möglichkeit, wie Sie ebenfalls auf sicherem Wege E-Mails lesen können, die von Toll-Collect an Sie verschlüsselt gesendet worden sind. Hierzu müssen Sie sich jedoch aktiv an dem Secure-WebMail-Dienst anmelden. Klicken Sie hierzu auf den Link („Request your one-time password“) in der Registrierungs-E-Mail. Daraufhin wird Ihnen ein Passwort zugesendet, mit dem Sie sich einmalig anmelden können.

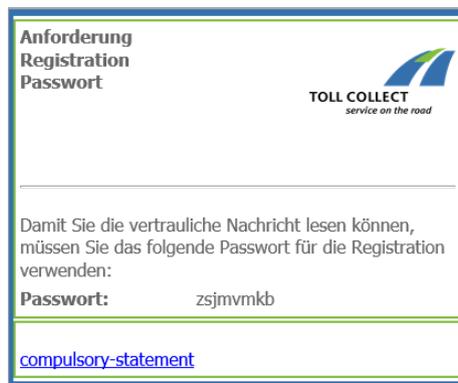


Abbildung 3

Rufen Sie nun mit Ihrem Browser die Adresse: <https://email.toll-collect.de> auf und melden Sie sich an. Als Benutzername verwenden Sie ihre E-Mail-Adresse. Nach erfolgreicher Anmeldung werden Sie direkt aufgefordert das Passwort zu ändern. Wenn Sie Ihr Passwort geändert haben ist für Sie der Registrierungsprozess abgeschlossen. Sie können sich ab sofort mit Ihrer E-Mail-Adresse und Ihrem neuen Passwort anmelden.

3 E-Mails sicher empfangen / lesen / beantworten

3.1 Nutzung von PGP bzw. S/MIME

Sofern Sie sich als PGP- bzw. S/MIME-Nutzer registriert haben, werden Ihnen die verschlüsselten E-Mails direkt an Ihr Postfach zugestellt. Es sollte grundsätzlich keine weiteren Einstellungen benötigen. Sie können wie gewohnt mit Ihrem Mail-Programm und ihrer eingerichteten Mail-Verschlüsselung arbeiten wie bisher.

Beachten Sie jedoch bitte, dass mit der Einführung des EEGW bei Toll Collect neue Schlüssel (PGP und S/MIME) für Toll Collect-Mitarbeiter generiert wurden. Der neue öffentliche PGP-Key bzw. öffentliche Teil des neuen S/MIME-Zertifikats wird standardmäßig mit jeder verschlüsselten E-Mail als Anhang mitgeliefert.

4 Weiterhin gibt es noch die Möglichkeit über die Anmeldemaske des Secure-WebMail-Dienstes öffentliches Schlüsselmaterial von Toll-Collect abzurufen (siehe Kapitel 6 - Multi-Faktor-Authentifizierung)

Wechseln Sie nach der Anmeldung über die Registerkarten im oberen Bereich in die „Kontoübersicht“ und anschließend über die linke Navigationsleiste in den Bereich „Zweistufige Verifizierung“ (siehe Abbildung 11).

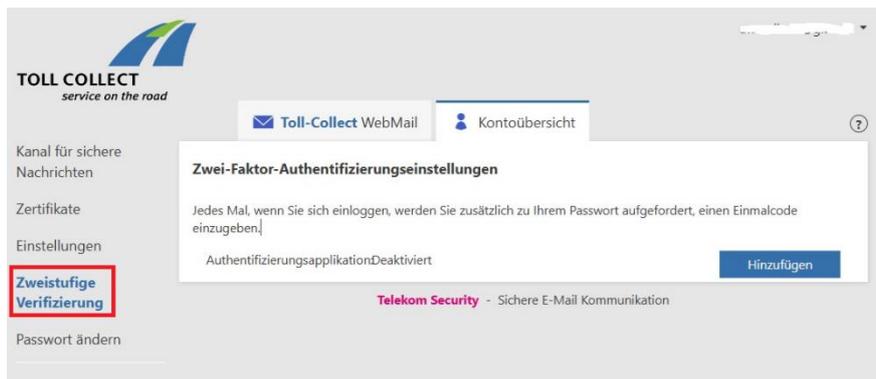


Abbildung 11

Aktuell wird die Multi-Faktor-Authentifizierung optional angeboten (je nach Lage kann sich dies jedoch auch noch auf verpflichtend ändern). Jeder Benutzer kann daher noch selbst entscheiden, ob diese Funktionalität verwendet werden soll oder nicht. Durch Klick auf den Button "Hinzufügen" wird die Einrichtung gestartet.

Hierzu versendet das System einen Verifizierungs-Link an die zum Konto gehörende E-Mail-Adresse.

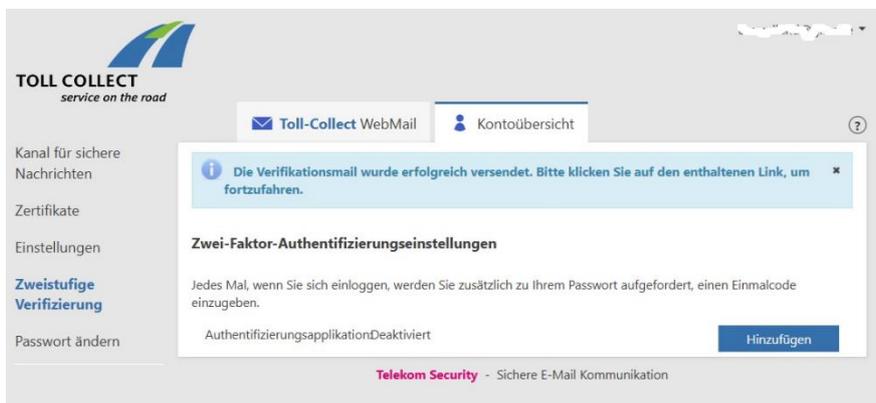


Abbildung 12

Öffnet man den Link in der E-Mail, wird folgende Seite (siehe Abbildung 13) angezeigt (ggf. nach erneuter Anmeldung mit Username und Passwort).



Abbildung 13

Den QR-Code kann man nun in jede beliebige sog. OTP-App (z.B. FreeOTP+, Microsoft Authenticator etc.) einlesen.

Von der Toll Collect IT-Sicherheit empfohlene OTP-Apps:

- Microsoft Authenticator (IOS/Android)
- FortiToken Mobile (IOS/Android)
- FreeOTP+ (IOS/Android)
- Aegis Authenticator (Android)

Von der Toll Collect IT-Sicherheit ausdrücklich nicht empfohlene OTP-Apps (die jedoch trotzdem nutzbar sind):

- Google Authenticator (IOS/Android)

Danach werden in der App Einmal-Token generiert welche nur eine begrenzte Zeit gültig sind. Diese sind nun bei jeder Anmeldung erforderlich. Den ersten können Sie verwenden um die MFA zu aktivieren, indem Sie diesen als Verifizierungscode eingeben.

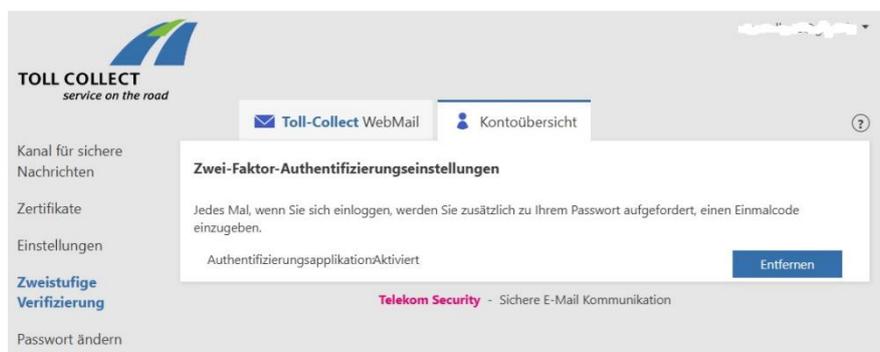


Abbildung 14

Öffentliches Schlüsselmaterial anfragen).

4.1 Nutzung des Secure-WebMail-Dienst

Sollten Sie zunächst keine eigene E-Mail-Verschlüsselung einsetzen, können Sie den Secure-WebMail-Dienst (<https://eemeil.toll-collect.de>) nutzen.

Nach der ersten Anmeldung erscheint folgende Ansicht:

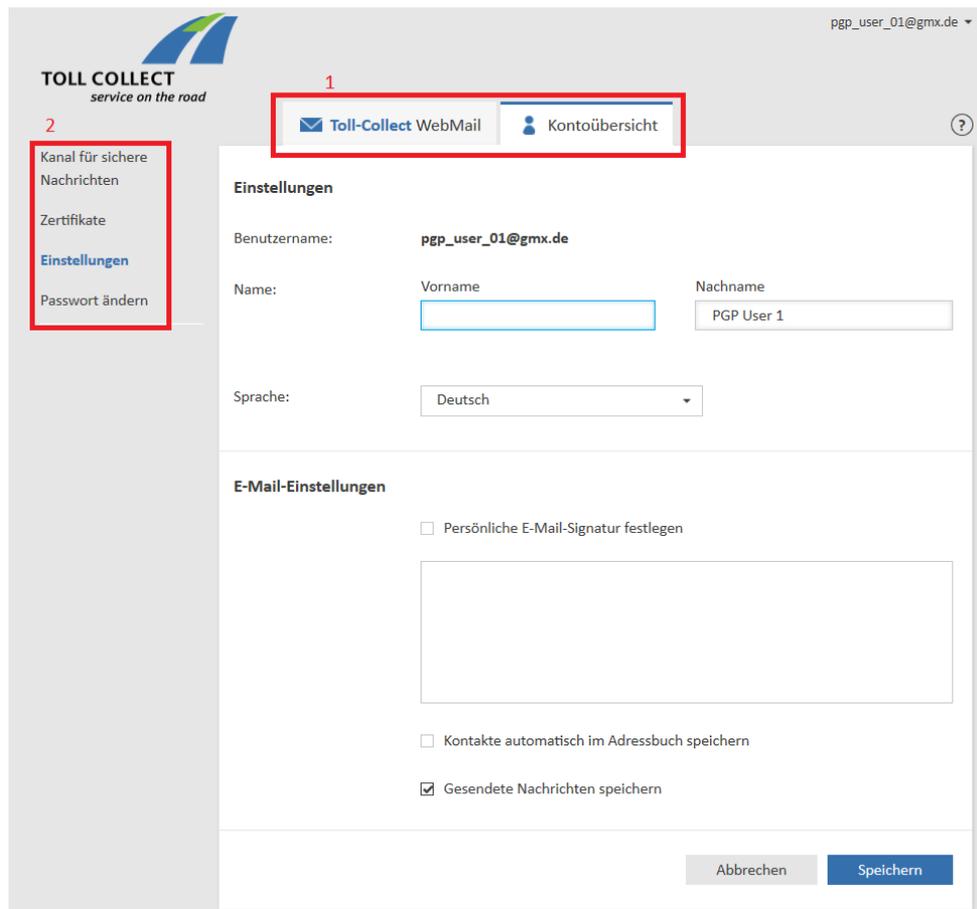


Abbildung 4

Die oberen Reiterkarten (siehe 1 in Abbildung 4) nutzen Sie zum Wechsel zwischen dem eigentlichen E-Mail-Dienst und der Kontoübersicht, in der Sie die Möglichkeit haben einige Einstellungen vorzunehmen. Standardmäßig ist als Kommunikationssprache „Deutsch“ vorausgewählt. Sollte dies anders gewollt sein, können Sie das hier ändern.

Die linke Navigationsleiste (siehe 2 in Abbildung 4) kann genutzt werden um das Passwort zu ändern oder das grundsätzliche Verhalten und die verwendete Verschlüsselungsmethode zu wechseln (siehe Kapitel 5 - Verschlüsselungsmethode).

Wechseln Sie in die WebMail – Ansicht und Sie werden E-Mails aufgelistet bekommen, die von Toll-Collect – Mitarbeitern verschlüsselt an Sie gesendet worden sind.

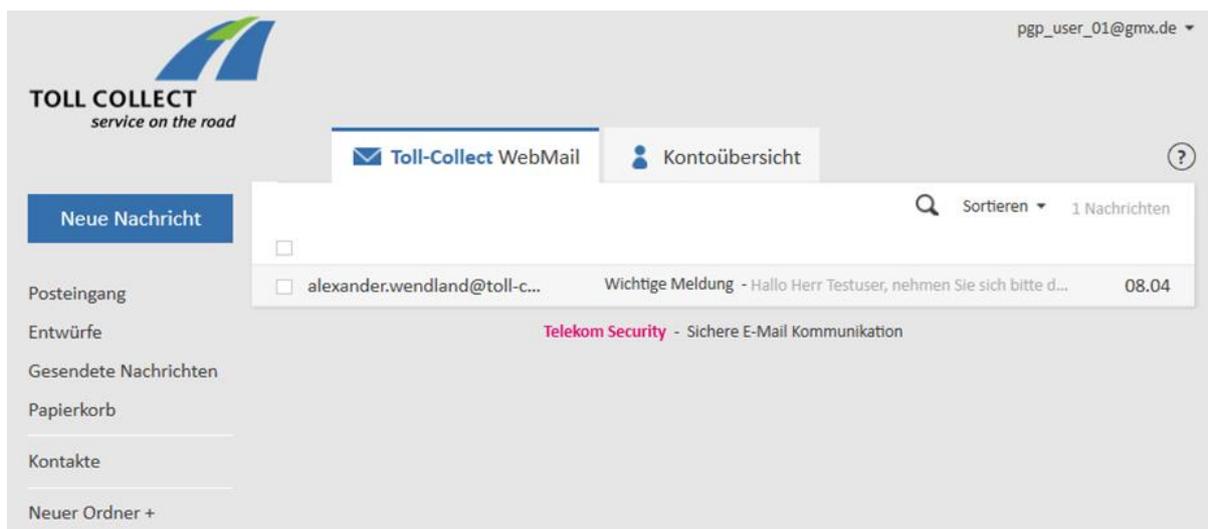


Abbildung 5

Hier können Sie die E-Mails lesen und auch beantworten. Sie haben hier die Möglichkeit die gesamte E-Mail als PDF oder auch einzelne Anhänge der E-Mail herunterzuladen. Die Verbindung zum Secure-WebMail-Dienst ist über Ihren Browser verschlüsselt und kann daher ebenfalls als sicher angesehen werden. Auch der Download von Anhängen erfolgt somit verschlüsselt.

Bitte beachten Sie, dass Sie ausschließlich auf E-Mails antworten können bzw. neue E-Mails nur an Toll-Collect interne Mitarbeiter verfassen können mit denen Sie bereits sicher kommuniziert haben.

Die Vorhaltezeit der E-Mails auf dem Secure-WebMail ist beschränkt (90 Tage). Der maximale Postfachspeicher beträgt 20 Mbyte. Daher sollten Sie die Download-Funktion nutzen, wenn Sie die E-Mails über diesen Zeitraum hinaus benötigen bzw. wenn Ihr Postfach voll ist und Sie Speicherplatz für neue E-Mails schaffen müssen.

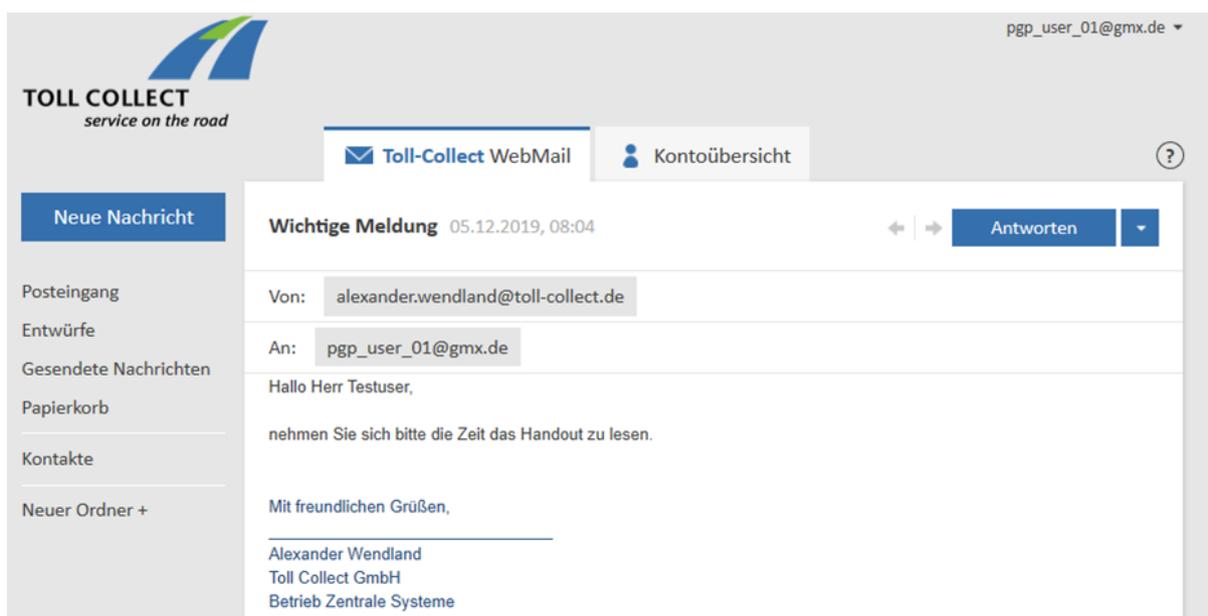


Abbildung 6

Sofern Sie eine neue E-Mail erhalten, welche Sie über den Secure-WebMail abrufen können erhalten Sie an Ihre hinterlegte E-Mail-Adresse eine Benachrichtigung.



Abbildung 7

5 Verschlüsselungsmethode ändern / Aktualisierung von Schlüsseln

Sollten Sie im Laufe der Zeit eine Änderung an der von Ihnen festgelegten Verschlüsselungsmethode wünschen, so können Sie dies einfach selbst tun. Hierzu müssen Sie sich zunächst am Secure-WebMail-Dienst (<https://email.toll-collect.de>) anmelden.

► Nutzer die sich initial per Antwortmail registriert haben, besitzen noch kein gültiges Login. Nutzen Sie hierfür die Funktion „Passwort vergessen?“, geben Sie Ihre E-Mail-Adresse ein und Ihnen wird ein neues Passwort zugeschickt mit dem Sie sich anmelden können.

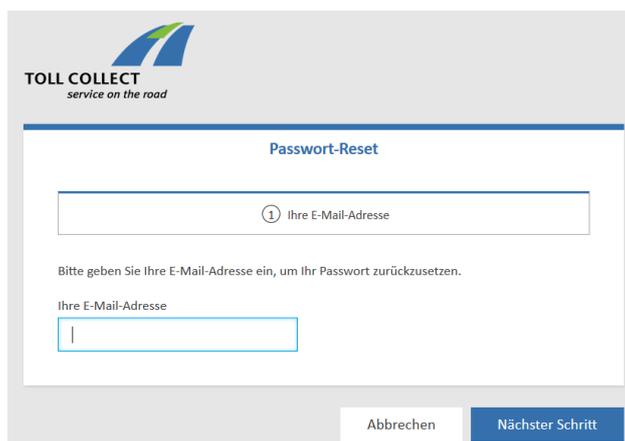


Abbildung 8

Wechseln Sie nach der Anmeldung mittels den Registerkarten im oberen Bereich in die „Kontoübersicht“ und anschließend über die linke Navigationsleiste in den Bereich „Zertifikate“ (siehe Abbildung 9).

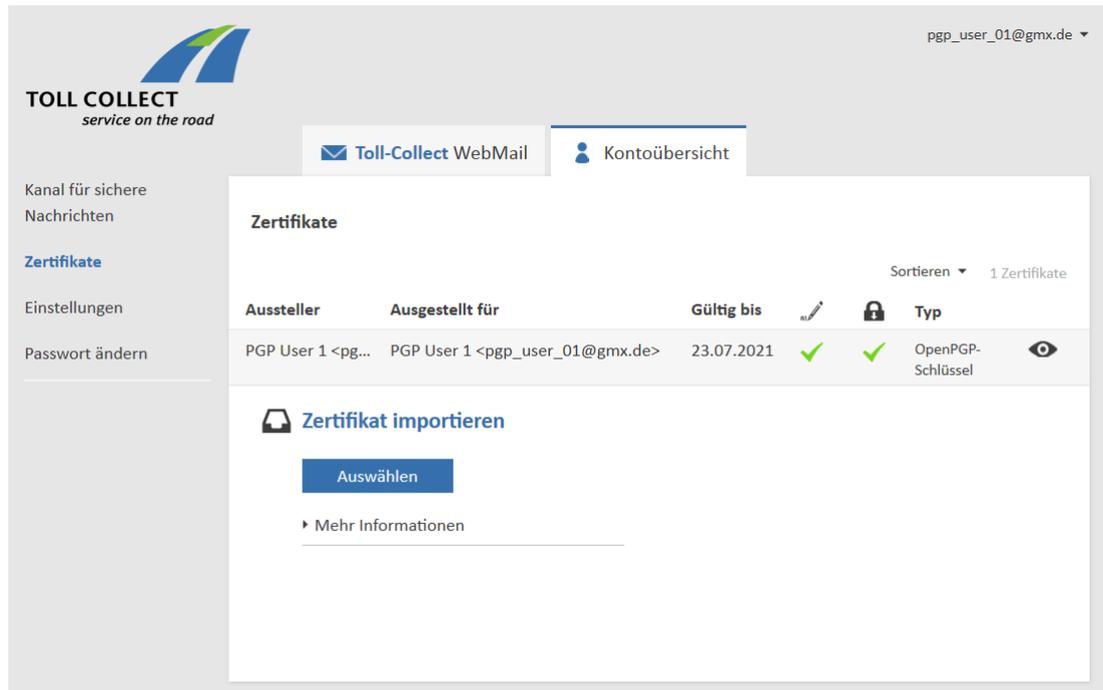


Abbildung 9

Hier haben Sie die Möglichkeit ein neuen PGP-Key oder ein neues S/MIME-Zertifikat hochzuladen. Dieser Schritt kann ebenfalls erforderlich werden, wenn die Gültigkeit Ihres hinterlegten Schlüsselmaterials abgelaufen ist.

Über die linke Navigationsleiste sollten Sie die Einstellungen „Kanal für sichere Nachrichten“ aufrufen und prüfen, ob die gewünschte Verschlüsselungsmethode aktiviert ist.

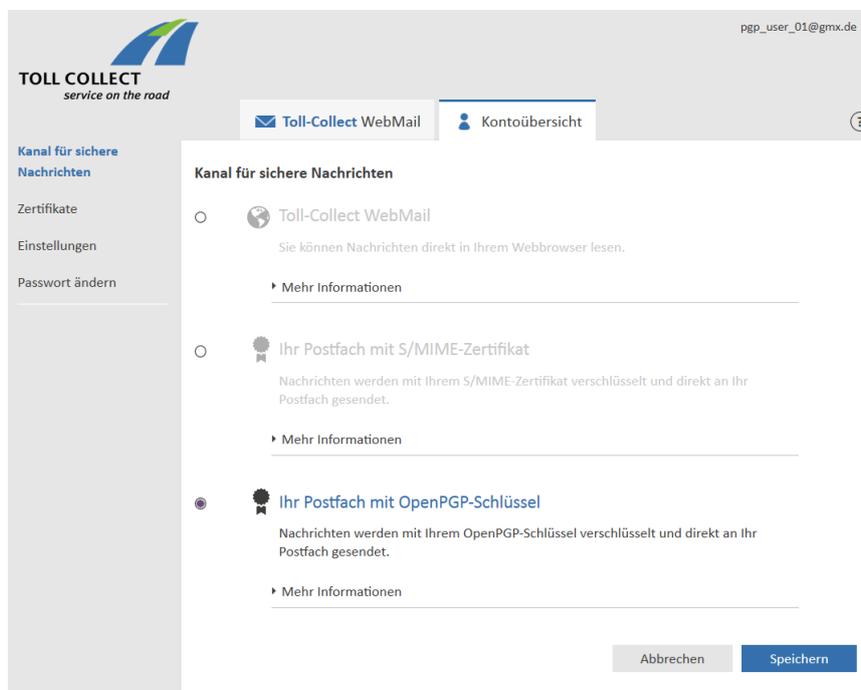


Abbildung 10

6 Multi-Faktor-Authentifizierung

Wechseln Sie nach der Anmeldung über die Registerkarten im oberen Bereich in die „Kontoübersicht“ und anschließend über die linke Navigationsleiste in den Bereich „Zweistufige Verifizierung“ (siehe Abbildung 11).

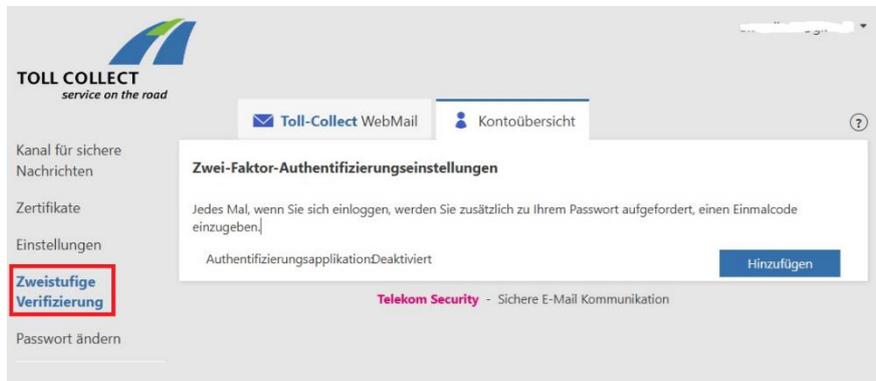


Abbildung 11

Aktuell wird die Multi-Faktor-Authentifizierung optional angeboten (je nach Lage kann sich dies jedoch auch noch auf verpflichtend ändern). Jeder Benutzer kann daher noch selbst entscheiden, ob diese Funktionalität verwendet werden soll oder nicht. Durch Klick auf den Button "Hinzufügen" wird die Einrichtung gestartet.

Hierzu versendet das System einen Verifizierungs-Link an die zum Konto gehörende E-Mail-Adresse.

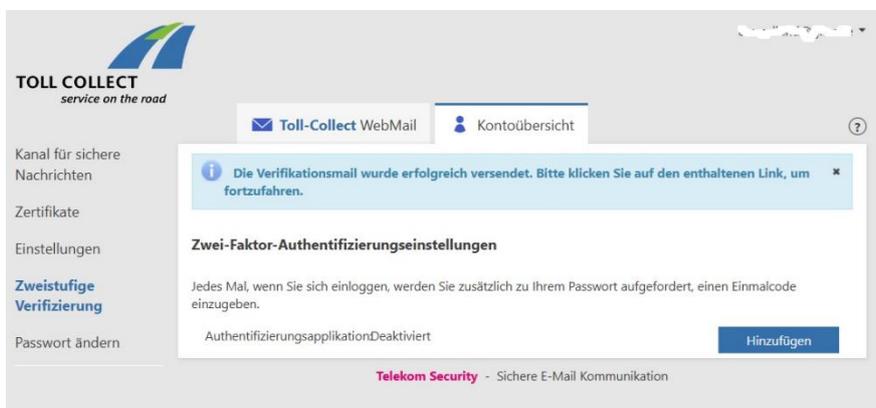


Abbildung 12

Öffnet man den Link in der E-Mail, wird folgende Seite (siehe Abbildung 13) angezeigt (ggf. nach erneuter Anmeldung mit Username und Passwort).



Abbildung 13

Den QR-Code kann man nun in jede beliebige sog. OTP-App (z.B. FreeOTP+, Microsoft Authenticator etc.) einlesen.

Von der Toll Collect IT-Sicherheit empfohlene OTP-Apps:

- Microsoft Authenticator (IOS/Android)
- FortiToken Mobile (IOS/Android)
- FreeOTP+ (IOS/Android)
- Aegis Authenticator (Android)

Von der Toll Collect IT-Sicherheit ausdrücklich nicht empfohlene OTP-Apps (die jedoch trotzdem nutzbar sind):

- Google Authenticator (IOS/Android)

Danach werden in der App Einmal-Token generiert welche nur eine begrenzte Zeit gültig sind. Diese sind nun bei jeder Anmeldung erforderlich. Den ersten können Sie verwenden um die MFA zu aktivieren, indem Sie diesen als Verifizierungscode eingeben.

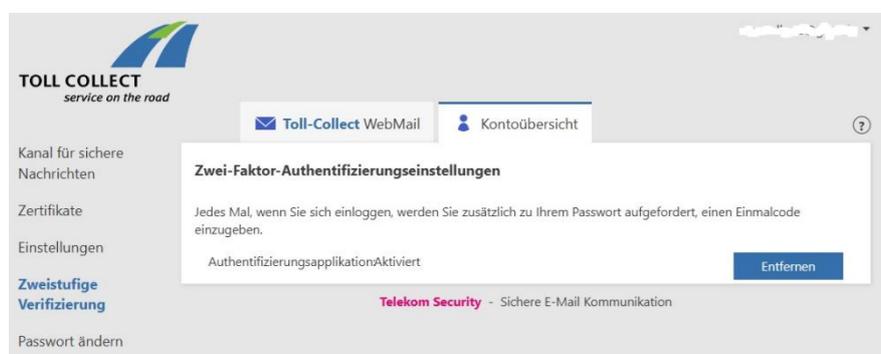
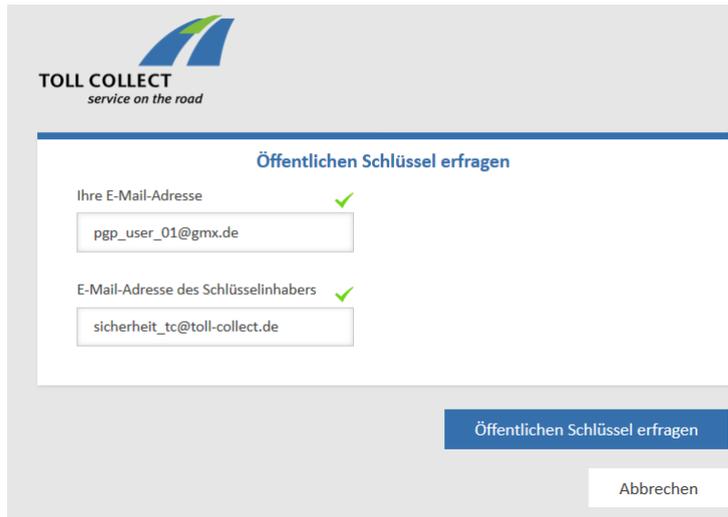


Abbildung 14

7 Öffentliches Schlüsselmaterial anfragen

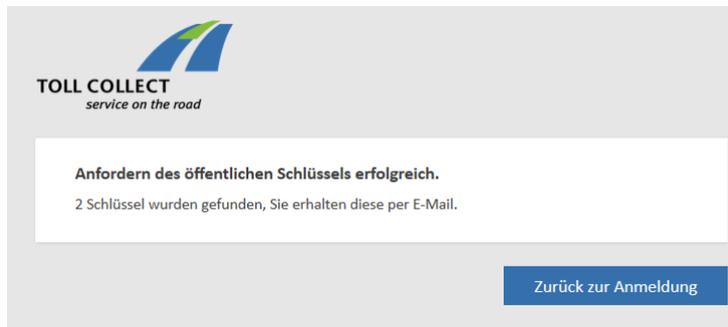
Da Sie zum Verschlüsseln von E-Mails die jeweiligen öffentlichen Schlüssel der Empfänger benötigen und diese möglicherweise noch nicht zugesandt bekommen haben, bietet das Secure-WebMail die Möglichkeit diese Schlüssel bereitzustellen.

Hierzu verwenden Sie auf der Anmelde-Maske des Secure-WebMail-Dienstes (<https://email.toll-collect.de>) die Funktion „Öffentliche Schlüssel anfragen“ direkt unterhalb des Anmelde-Buttons (siehe Abbildung 15 - Abbildung 16).



The screenshot shows a web form titled "Öffentlichen Schlüssel erfragen" (Request Public Keys) on the Toll Collect website. The form contains two input fields, each with a green checkmark to its right, indicating successful validation. The first field is labeled "Ihre E-Mail-Adresse" and contains the text "pgp_user_01@gmx.de". The second field is labeled "E-Mail-Adresse des Schlüsselinhabers" and contains the text "sicherheit_tc@toll-collect.de". Below the form, there is a blue button labeled "Öffentlichen Schlüssel erfragen" and a white button labeled "Abbrechen".

Abbildung 15



The screenshot shows a success message box on the Toll Collect website. The message text reads: "Anfordern des öffentlichen Schlüssels erfolgreich." followed by "2 Schlüssel wurden gefunden, Sie erhalten diese per E-Mail." Below the message box, there is a blue button labeled "Zurück zur Anmeldung".

Abbildung 16

Als Ergebnis wird Ihnen eine E-Mail zugesandt, welche mit dem S/MIME-Zertifikat des angefragten Empfängers signiert ist. Weiterhin ist der entsprechende öffentlichen PGP-Key als Dateianhang der E-Mail beigefügt.

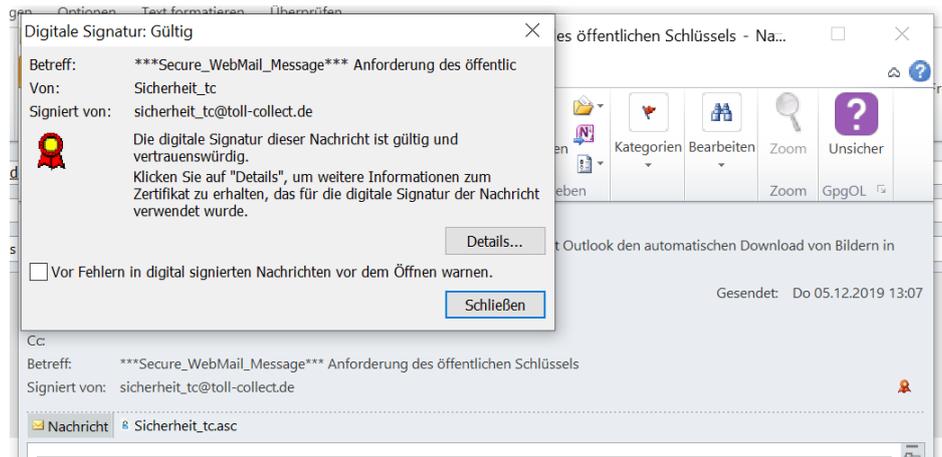


Abbildung 17

S/MIME-Benutzer können diese Signatur direkt einem Kontakt zu weisen und sofort nutzen. PGP-Nutzer sollten den öffentlichen PGP-Key in Ihre Verschlüsselungs-Software importieren.

8 Einrichten von festen Kommunikationsregeln

Unter bestimmten Voraussetzungen ist es sinnvoll über die Einrichtung / Anpassung vorhandener Regeln nachzudenken. Gründe könnten sein:

- in Ihrem Unternehmen wird ebenfalls ein E-Mail-Encryption-Gateway verwendet,
- eine grundsätzliche Verschlüsselung soll zwischen bestimmten Adressen verpflichtend eingerichtet werden,

Sollte dies der Fall sein, wenden Sie sich mit Ihrem Anliegen bitte an secure-email@toll-collect.de.