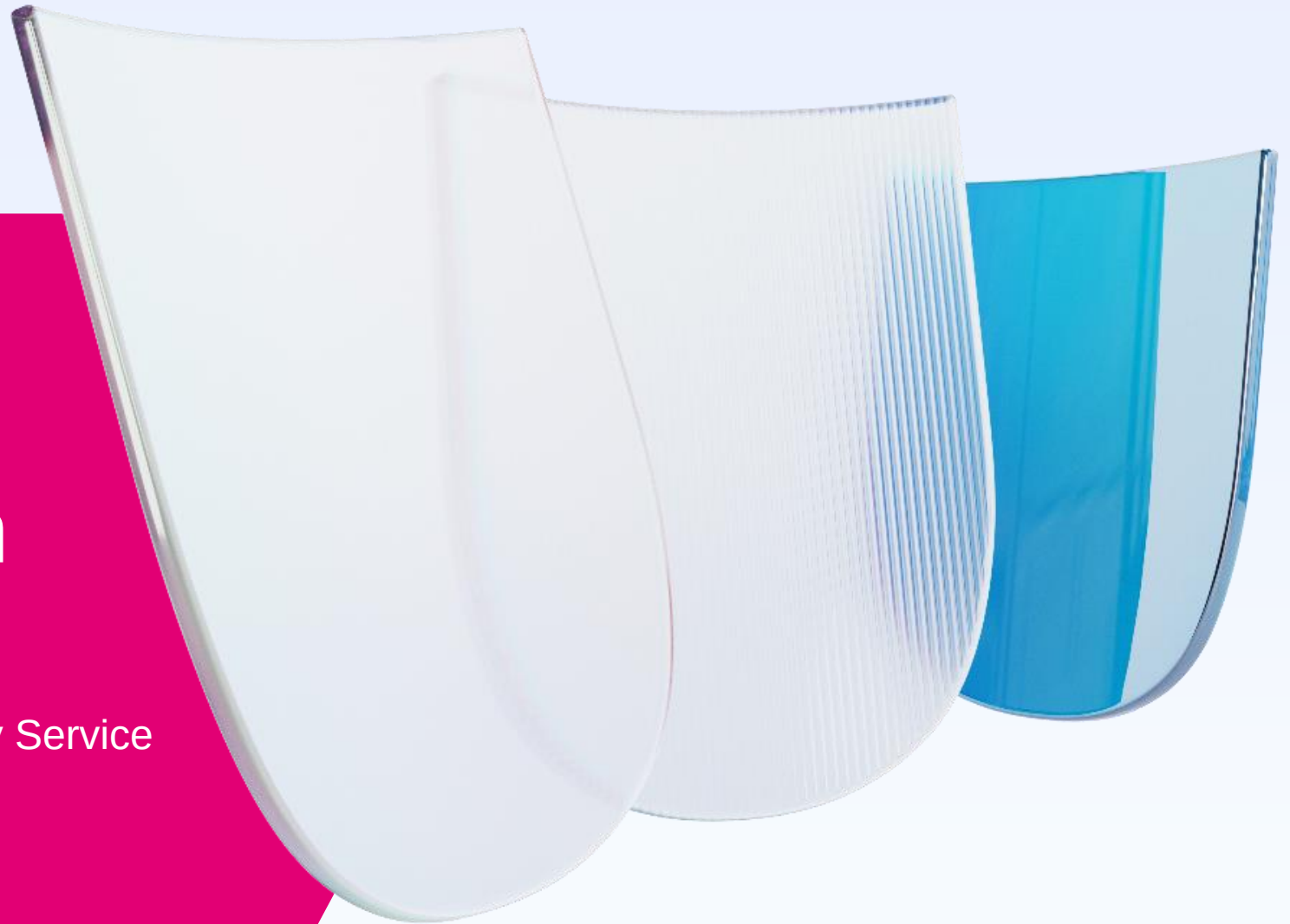


TELEKOM SECURITY

E-Mail Encryption Gateway

Kurzbeschreibung Encryption Gateway Service
für den MD-WL | Kiel | 18. April 2024



Allgemeine Informationen

Dieses Dokument beschreibt den Encryption Gateway Dienst des MD-WL. Der Dienst wird von der Deutschen Telekom Security GmbH bereitgestellt und wird im folgenden Encryption Gateway (EGW) genannt. Der Dienst realisiert die sichere verschlüsselte E-Mail Kommunikation für den MD-WL. Die bereitgestellten Funktionen für den Empfang und/oder Versand werden im folgenden näher beschrieben:

- S/MIME
- PGP
- Webmail



Allgemeine Informationen

S/MIME Zertifikat oder PGP Schlüssel (intern - @md-wl.de)

Das Encryption Gateway unterstützt PGP Schlüssel und S/MIME Zertifikate:

- Das Domänenzertifikat für die Domäne md-wl.de kann unter folgenden Link heruntergeladen werden: <https://www.md-wl.de/mailverschluesselung>
- Nutzerzertifikate (Personen bezogene Zertifikate) können über folgenden Link abgefragt werden: <https://secure-email.t-systems-service.com/mdwl/>
- S/MIME Zertifikate und PGP Schlüssel können auch über die DT Security GmbH abgefragt werden (siehe (4) Support)

S/MIME Zertifikat oder PGP Schlüssel (extern)

- Das Encryption Gateway unterstützt PGP Schlüssel und S/MIME Zertifikate externer Kommunikationspartner für Domänen oder Benutzer.

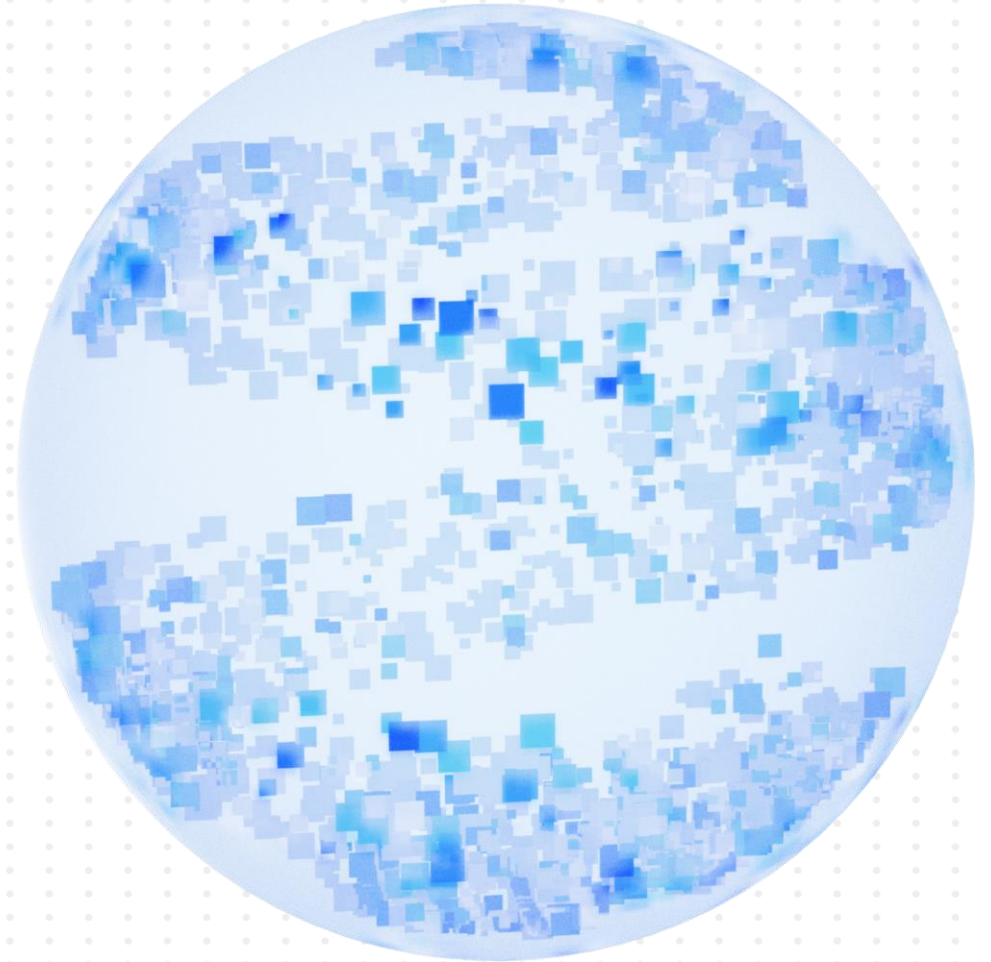
Webmail Portal

- Das Webmail Portal ist ein dritter sicherer Kanal für die sichere E-Mailkommunikation. Es kann genutzt werden, wenn kein S/MIME oder PGP vom Kommunikationspartner unterstützt wird.



Agenda

- 01** S/MIME (x.509)
- 02** PGP (INLINE/ MIME)
- 03** Sicherer Kanal zur Kommunikation
(Webmail Portal)
- 04** FAQ / Support



01 S/MIME (x.509)

Im folgenden wird beschrieben, wie die verschlüsselte Kommunikation mit Hilfe von S/MIME realisiert werden kann.



S/MIME (x.509)

Sie erfüllen die technischen Voraussetzungen für die inhaltliche E-Mailverschlüsselung mit S/MIME Zertifikaten, dann können Sie die Zertifikate einzelner Mitarbeiter des MD-WL über den folgenden Link abfragen (öffentlichen Schlüssel erfragen):

<https://secure-email.t-systems-service.com/mdwl/>

Sie haben eine zentrale Lösung für die inhaltliche Verschlüsselung via S/MIME, dann können Sie gerne das Domänenzertifikat (md-wl.de) über folgenden Link herunterladen und entsprechend einrichten:

<https://www.md-wl.de/mailverschluesselung>

Im Gegenzug senden Sie dem MD-WL ihr S/MIME Zertifikat zu. Dies senden Sie einfach per digital signierte (x.509) E-Mail an trustedservices@md-wl.de. Ihr Zertifikat wird dann vom Encryption Gateway automatisch importiert und kann so von Seiten des MD-WL für die Verschlüsselung zu ihnen genutzt werden.

Besitzen Sie auch ein S/MIME Domänenzertifikat können Sie dies entweder über den MD-WL (ticket-system@md-wl.de) oder direkt an die DT Security GmbH (mail_encryption_gateway@telekom.de) übermitteln. Das Domänenzertifikat wird dann im Encryption Gateway hinterlegt, so dass die Verschlüsselung auch in ihre Richtung funktioniert.

02 PGP (INLINE/ MIME)

Im folgenden wird beschrieben, wie die verschlüsselte Kommunikation mit Hilfe von PGP realisiert werden kann.



PGP (INLINE/ MIME)

Sie erfüllen die technischen Voraussetzungen für die inhaltliche E-Mailverschlüsselung mit PGP Schlüsseln, dann können Sie die PGP Schlüssel einzelner Mitarbeiter des MD-WL über den folgenden Link abfragen (öffentlichen Schlüssel erfragen):

<https://secure-email.t-systems-service.com/mdwl/>

Sie haben eine zentrale Lösung für die inhaltliche Verschlüsselung via PGP, dann können Sie gerne den Domänenschlüssel (md-wl.de) über folgenden Link herunterladen und entsprechend einrichten:

<https://www.md-wl.de/mailverschluesselung>

Im Gegenzug senden Sie dem MD-WL ihren öffentlichen PGP Schlüssel zu. Diesen senden Sie einfach als Anhang an eine E-Mail an trustedservices@md-wl.de. Ihr Zertifikat wird dann vom Encryption Gateway automatisch importiert und kann so von Seiten des MD-WL für die Verschlüsselung zu ihnen genutzt werden.

Besitzen Sie auch ein S/MIME Domänenzertifikat können Sie dies entweder über den MD-WL (ticket-system@md-wl.de) oder direkt an die DT Security GmbH (mail_encryption_gateway@telekom.de) übermitteln. Das Domänenzertifikat wird dann im Encryption Gateway hinterlegt, so dass die Verschlüsselung auch in ihre Richtung funktioniert.

03 Sicherer Kanal zur Kommunikation (Webmail Portal)

Im Folgenden wird beschrieben, was das Webmail Portal ist und wie man sich damit verbindet und arbeiten kann. Über das Webmail Portal werden E-Mails über einen sicheren Kanal zur Verfügung gestellt und können auch beantwortet werden.



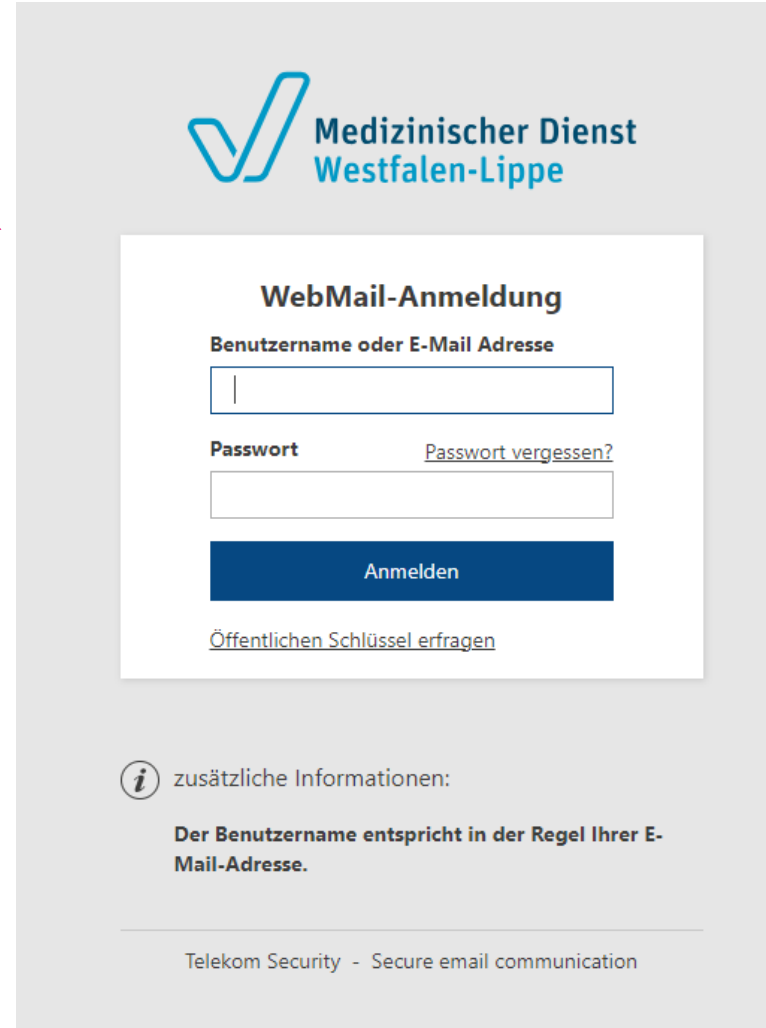
Webmail Portal

Das Webmail Portal ist eine HTTPS Schnittstelle, die über das Internet mit folgender URL erreichbar ist:

<https://secure-email.t-systems-service.com/mdwl/>

Die Nutzung des Webmail Portals wird durch eine Registrationsmail gestartet. In der Registrationsmail ist der Link zum Portal und die Login-Kennung enthalten. Der Login entspricht der eigenen E-Mailadresse. Das Passwort wird an den Absender gesendet. Der Absender und Webmailer Nutzer sollten das Passwort am besten telefonisch austauschen.

Sollte das Webmail Portal benötigt werden, ohne dass eine Registration vorliegt kann diese durch den MD-WL mit einer verschlüsselten E-Mail initiiert werden.



**Medizinischer Dienst
Westfalen-Lippe**

WebMail-Anmeldung

Benutzername oder E-Mail Adresse

Passwort [Passwort vergessen?](#)

Anmelden

[Öffentlichen Schlüssel erfragen](#)

i zusätzliche Informationen:

Der Benutzername entspricht in der Regel Ihrer E-Mail-Adresse.

Telekom Security - Secure email communication

Webmail Portal

Nach erfolgreicher Registration kann man sich anmelden und die rechts beschriebenen Funktionen nutzen.

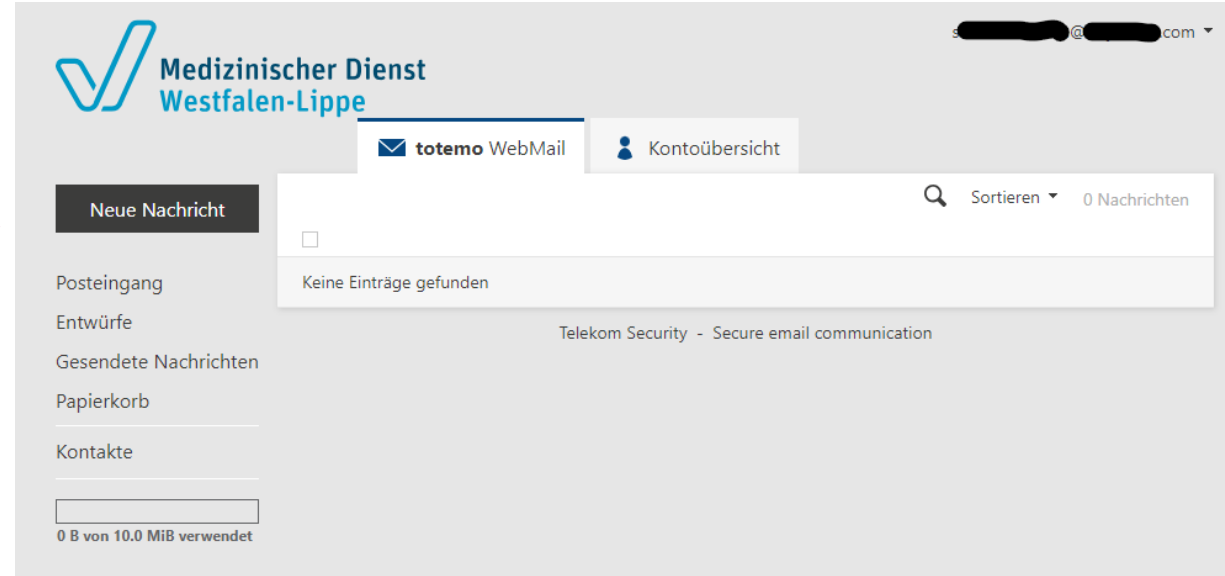
Wenn zukünftig sichere/vertrauliche E-Mails vom MD-WL an einen Webmail Portal Nutzer gesendet werden, erhält der Webmail Portal Nutzer eine Benachrichtigung, die darüber informiert, dass eine neue Nachricht vorliegt.

Das Webmail Portal bietet einen begrenzten Speicherplatz und dient der Übermittlung von sicheren/vertraulichen E-Mails und nicht als genereller Speicherort. Aus diesem Grund wird empfohlen die E-Mails nach Bearbeitung zu löschen oder herunterzuladen und zu löschen. →

Über die Oberfläche hat man wie in einem Mail-Programm einen Posteingang mit den eingegangenen E-Mails.

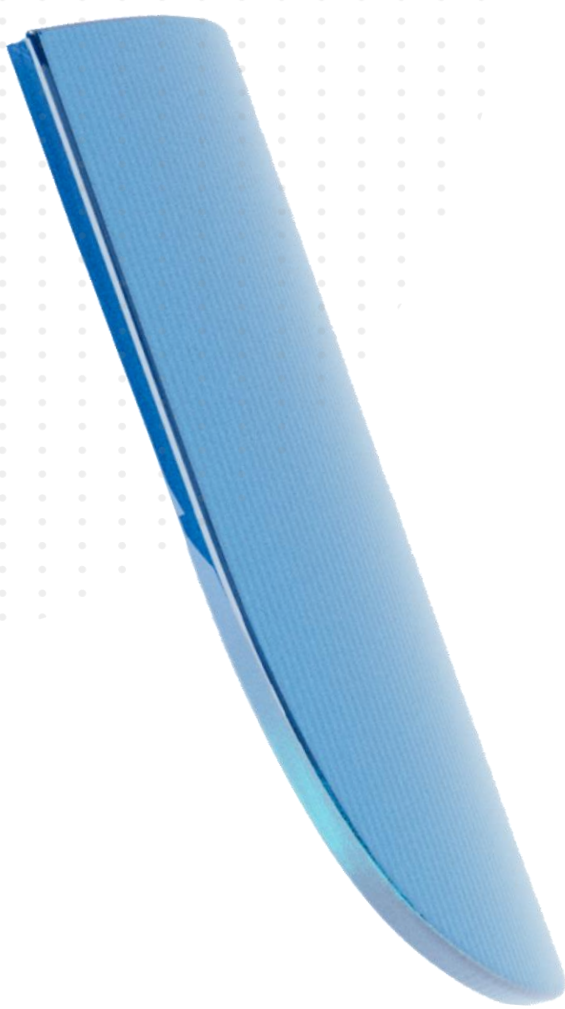
Es werden folgende Funktionen bereitgestellt:

- E-Mails lesen
- E-Mails beantworten
- E-Mails schreiben
- E-Mails herunterladen
- E-Mails löschen



04 FAQ / Support





FAQ

Webmail Portal Postfachgröße: 10 MB

Inaktivität: 90 Tage

- Nach 90 Tagen ohne Maileingang im Webmail Portal oder ohne Login, wird ein Account automatisiert gelöscht. Bei erneuten Bedarf kann die Registration wieder durchgeführt werden.

Löschung von E-Mails: 90 Tage

- Nach 90 Tagen werden automatisiert E-Mails aus dem Webmail Portal gelöscht. Aus diesem Grund empfiehlt sich die Herunterladen-Funktion.

Account-Type-Wechsel

- Sollte nach der Registration als Webmail Portal Nutzer ein S/MIME Zertifikat oder PGP Schlüssel vorliegen, kann jederzeit der Account-Type gewechselt werden. Über die „Kontoübersicht“ kann man das Zertifikat oder den PGP Schlüssel importieren und den „Kanal für sichere Nachrichten“ eigenständig umstellen.

Support

Supportanfragen bei Problemen mit der Mail Encryption:

Mail_Encryption_Gateway@telekom.de

