

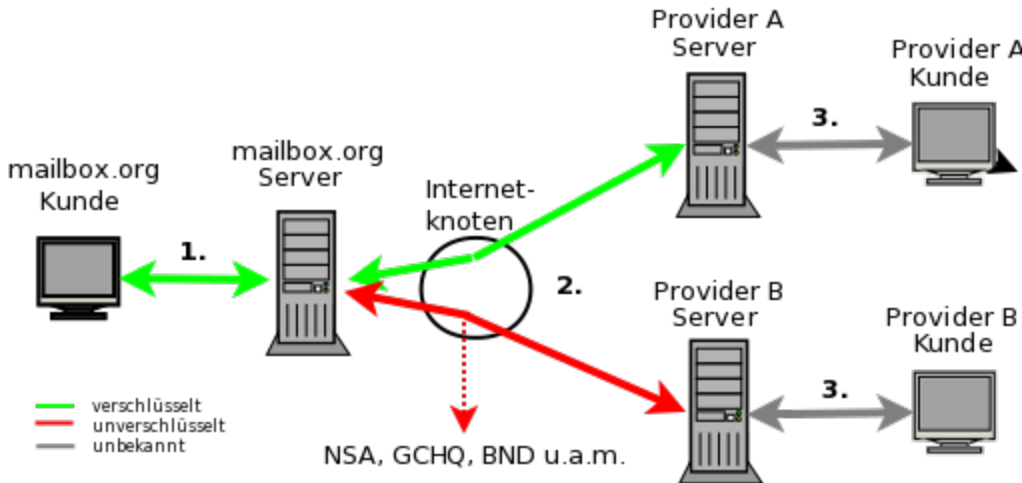
SSL-TLS-Verschlüsselung bei mailbox.org

Vorteile des E-Mail-Versands über Ihr mailbox.org-Office

- **SSL-verschlüsselt oder nicht:** Die Eingabe einer Empfänger-Adresse liefert ein klares Ergebnis.
- **Einfache Symbole informieren Sie über die Transportverschlüsselung zu E-Mail-Providern.**

Wie der E-Mail-Versand funktioniert

Die folgende Grafik demonstriert Ihnen die Transportwege einer E-Mail zwischen einem mailbox.org-Kunden und zwei Kunden bei anderen E-Mail-Providern:



Für die Verbindung (1.) zwischen unseren Kunden und den mailbox.org-Servern wird **immer eine Transportverschlüsselung** nach aktuellem Stand der Technik erzwungen.

Für die Verbindungen (2.) zwischen unseren Servern und den Servern anderer Provider bieten wir alle Voraussetzungen, um eine sichere Transportverschlüsselung herzustellen.

Bei manchen Providern (**Provider B**) ist es jedoch entweder nicht möglich, eine verschlüsselte Verbindung zu nutzen, oder die angebotene Verschlüsselung entspricht nicht mehr aktuellen Sicherheitsanforderungen.

E-Mail-Versand bei mailbox.org

Folgende Richtlinien setzen wir **standardmäßig** bei der **Versendung von E-Mails**:

1. Wenn der **Provider A** einen **TLSA/DANE-Eintrag** mit dem Fingerprint des SSL-Zertifikates des Servers via DNSSEC veröffentlicht hat ([siehe auch](#)), dann wird eine Transportverschlüsselung mit diesem Zertifikat erzwungen. **Als Kunde von mailbox.org** können Sie sicher sein, dass die E-Mail somit über einen sicheren Kanal zum Provider des Empfängers versendet wird.
2. Auch wenn Sie ein E-Mail an Gmail, Yahoo o.ä. schicken, wird bei mailbox.org standardmäßig eine **TLS-Verschlüsselung** erzwungen. Falls unsere Server **bereits einmal** eine **SSL/TLS-verschlüsselte Verbindung** zu dem entsprechenden Server eines anderen Providers aufbauen konnten, dann wird zukünftig **immer eine Transportverschlüsselung** für diese Verbindung erzwungen. Als Kunde von mailbox.org können Sie sicher sein, dass **immer eine verschlüsselte Verbindung erzwungen wird**, falls es bereits einmal möglich war.
3. Für die Server einiger E-Mail-Provider war und ist es nicht möglich, eine SSL/TLS-verschlüsselte Verbindung aufzubauen. **In diesem Fall wird die Mail über eine unsichere Verbindung gesendet.** Falls Ihre E-Mail nicht (z.B. per PGP) verschlüsselt ist, **kann jeder Server, über den die E-Mail von unserem Mailserver zum Mailserver des Empfängers geleitet wird (2.), den Klartext Ihrer Nachricht lesen oder verändern** (siehe auch: [Man-in-the-Middle-Angriff](#)).

Im mailbox.org-Office werden Sie automatisch beim Auswählen des Empfängers einer E-Mail **über die Sicherheit der Transportverschlüsselung informiert** und können dann **selbst entscheiden**, ob Sie die E-Mail entsprechend versenden wollen. Dargestellt wird diese Information durch ein Symbol hinter jeder Empfängeradresse. Dabei werden die Empfänger (bzw. die Mailserver derer Provider) in drei Stufen klassifiziert:

1. **SSL-fähig zzgl. DANE/DNSSEC:**
Erfüllt das Zielsystem den höchsten SSL-Sicherheitsstandard und bietet auch DANE und DNSSEC-gesicherte Verbindungen an, wird Ihnen dieser besondere Verbindungsschutz durch einen **grünen gehobenen Daumen und der Info „DANE ok“** symbolisiert.
2. **SSL-fähig:**
Beherrscht das Zielsystem normale SSL-Verschlüsselung, dann können Sie, als Absender, sich über einen **grünen gehobenen Daumen** freuen.
3. **Keine Transportverschlüsselung möglich, dann werden Sie durch ein rotes „no SSL“ gewarnt.**
4. **Haben wir noch keine Informationen zum Zielsystem, wird ein graues „SSL?“ angezeigt.**

Von Maxima Mustermann <maxima.mustermann@mailbox.org>

An mailbox.org DANE ok x user@yahoo.de SSL ok x CC BCC
info@kabelbw.de no SSL x mail@example.com SSL x

Betreff

Anlagen v Sicherheit v Signaturen v Optionen v

Sie können zusätzlich mit der Maus über das Verschlüsselungssymbol fahren, um weitere Informationen zu den verwendeten Verschlüsselungsalgorithmen und der TLS-Version zu erhalten:

user@yahoo.de SSL ok x CC BCC

Die E-Mail wird über eine SSL/TLS-verschlüsselte Verbindung zum Mailserver des Empfängers übertragen.

Verschlüsselung: TLSv1.2, ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits)

secure.mailbox.org - manchmal lieber gar nicht, als unverschlüsselt

Bei mailbox.org können Sie neben Ihrer normalen E-Mail-Adresse „ich@mailbox.org“ zusätzlich auch „ich@secure.mailbox.org“ zur Verwendung aktivieren. Diese neue E-Mail-Adresse können Sie immer dann benutzen, wenn Ihnen wichtig ist, dass eine sichere Datenübertragung **zwischen den Mailservern des Absenders und des Empfängers** zustande kommt und Sie **lieber gar nicht, als versehentlich unverschlüsselt** per E-Mail kommunizieren wollen. Ihnen wird dann auch eine entsprechende secure.mailbox.org-Adresse für jedes Alias eingerichtet!

Aktivieren Sie den Verschlüsselten Versand (also Ihre secure.mailbox.org-Adresse) einfach über „Einstellungen -> mailbox.org -> Verschlüsselter Versand -> Einschalten“:

The screenshot shows the mailbox.org user interface. At the top is an orange navigation bar with links for Portal, E-Mail, Adressbuch, Kalender, Aufgaben, and Drive, along with icons for refresh, help, and a menu. Below the navigation bar is a sidebar menu with categories like Grundeeinstellungen, Accounts, Portal, E-Mail, Guard Sicherheit, Adressbuch, Kalender, Aufgaben, Drive, Dokumente, Veröffentlichungen, Fehleranalyse, Gruppen, and Ressourcen. The main content area is titled 'Verschlüsselter Versand' and contains the following settings:

- Vertrag und Tarif
- Kontoauszug
- Guthaben auffüllen
- Rechnungskopien
- Passwort ändern
- E-Mail-Aliase
- Alternative Absender
- Wegwerf-Adressen
- Verschlüsselter Versand** (highlighted)

The 'Verschlüsselter Versand' section is currently set to 'Einschalten' (checked). Below the settings is an orange 'Speichern' button. The explanatory text reads: 'Bei mailbox.org haben Sie die Möglichkeit, E-Mails ausschließlich über verschlüsselte Verbindungen versenden zu lassen, was jedoch nicht mit allen Providern funktioniert. Bitte beachten Sie dazu unbedingt die Erläuterungen auf: <https://mailbox.org/mails-definitiv-sicher-versenden/>'.

Sobald Sie als Absender eine secure.mailbox.org-Adresse (z.B. meinalias@secure.mailbox.org) ausgewählt haben, versenden unsere Mailserver diese E-Mail **definitiv nur noch über eine** (mindestens) **SSL/TLS-verschlüsselte Verbindung**. Diese muss vom Provider des Empfängers auch angeboten werden, sonst kann die E-Mail nicht versandt werden und Sie erhalten eine Fehlermeldung.

Antworten an Ihre secure.mailbox.org-Adresse

Eine Versandgarantie über eine verschlüsselte Verbindung wäre **sinnlos**, wenn diese Garantie nicht auch für den Empfang gelten würde: würde Ihnen der Empfänger antworten und dabei vollständig Ihre ursprüngliche E-Mail zitieren, dann kann jeder Server, über den die E-Mail zurückgeleitet wird, die Informationen der ursprünglichen, eigentlich TLS-verschlüsselten abgreifen - **falls diese Antwort nicht ebenfalls durch eine sichere Transportverschlüsselung geschützt ist**. Deshalb gelten bei uns die selben Standards auch für den E-Mail-Empfang an secure.mailbox.org-Adressen.

Achtung: kann der Mailserver dieses Providers (Ihres Kommunikationspartners) E-Mails nicht mit aktivierter Transportverschlüsselung versenden, dann scheitert der Empfang. In diesem Fall erhält der Absender die E-Mail als unzustellbar zurück.

Verwandte Artikel

- [E-Mail-Adressen der eigenen Domain nutzen](#)
- [E-Mail-Einrichtung mit K-9 Mail unter Android](#)
- [Umzug zu mailbox.org](#)
- [Von Gmail zu mailbox.org umziehen](#)
- [Externe E-Mail-Accounts einbinden](#)