

Ablauf einer verschlüsselten Kommunikation mittels eines Gateways

1. Ein Mitarbeiter sendet eine E-Mail an einen externen Kunden.
2. Das Gateway prüft auf der Grundlage der vom Unternehmen definierten Regeln, ob diese E-Mail verschlüsselt werden muss.
3. Falls ja, wird geprüft, ob für den externen Kunden ein Zertifikat vorliegt.
4. Wenn kein Zertifikat vorliegt, startet der automatische Registrierungsprozess.
5. Die zu versendende E-Mail wird zunächst im verschlüsselten E-Mail-Speicher abgelegt.
6. Das Gateway sendet automatisch eine signierte E-Mail zur Registrierung an den Kunden.
7. Falls der Kunde ein Zertifikat besitzt, verschlüsselt und signiert das Gateway die E-Mail und sendet sie an den Kunden.

Der Kunde hat nun vier Möglichkeiten, um die sichere E-Mail zu empfangen:

- a) Er benutzt sein vorhandenes Zertifikat und entschlüsselt und signiert die E-Mail.
- b) Er hat kein Zertifikat, möchte sich aber eines zulegen: Dann klickt er auf die URL in der E-Mail, die das Gateway an ihn geschickt hat. Danach wird automatisch ein Zertifikat für ihn erstellt, mit dem er diese und zukünftige E-Mails des Absenders öffnen kann.
- c) Er hat kein Zertifikat und möchte auch keines: Über einen vom Gateway verschickten Link hat er Zugriff auf ein SSL-verschlüsseltes Webmailsystem, über das er die E-Mail abrufen kann.
- d) Er kann die E-Mail als verschlüsselte PDF-Datei empfangen.