



## Gegenstelle ohne Zertifikat

Sollte ein Empfänger / Kommunikationspartner über kein Schlüsselmaterial bzw. eine Verschlüsselungslösung verfügen, so bietet JULIA MailOffice vielfältige Alternativen, diesem Empfänger verschlüsselte Nachrichten zuzustellen und von diesem solche zu empfangen.

### Alternative 1: Die JULIA MailOffice Webmailer Komponente

JULIA MailOffice verfügt über eine Webmailer Komponente. Dabei handelt es sich um eine eigenständige JULIA, die auf einem weiteren, vom Web aus zugänglichem Server, installiert ist. Je nach Ihren Bedürfnissen in Bezug auf den Automatisierungsgrad und Sicherheit stehen verschiedene Betriebsmodi zur Verfügung:

#### A: Webmailer mit „Einmal-Passwort“

Die Gegenstelle ohne Zertifikat bekommt eine Standard-E-Mail von Ihnen, in der sich der HTTPS-Link zu Ihrem Webmailer befindet. Zusätzlich teilen Sie der Gegenstelle einen individuellen Login mit und übersenden separat (Medienbruch ist wünschenswert!) das Passwort zum Login.

Das Passwort kann auch in einer zweiten E-Mail an den Empfänger gesendet werden. Das gewünschte Verhalten kann in JULIA MailOffice konfiguriert werden.

#### B. Webmailer mit persönlichem Postfach

Dieser Betriebsmodus unterscheidet sich von dem bereits beschriebenen darin, dass für jeden Empfänger nur ein Passwort erzeugt wird. Dieses kann / muss der Benutzer ändern, sobald er das erste Mal das speziell für ihn angelegte Postfach angesteuert hat. Alle weiteren E-Mails werden in diesem Postfach abgelegt und können dort bearbeitet werden.

E-Mails, die eine voreingestellte Vorhaltezeit überschreiten, können automatisch gelöscht werden.

#### „Password self service“

Um die Interaktion zwischen Absender und Empfänger einer E-Mail zu reduzieren, wurde folgendes Verfahren implementiert, welches die vollständige Kommunikation ohne Passwort-Austausch zwischen Absender und Empfänger ermöglicht:

1. Durch erzwungene Verschlüsselung und wegen des Fehlens eines öffentlichen Schlüssels für den Empfänger wird die E-Mail auf den Webmailer übertragen.
2. Der Empfänger erhält eine E-Mail mit einem Link, mit dessen Hilfe ein Passwort für den Empfänger erstellt wird. Dieses Passwort wird dem Empfänger zeitnah per E-Mail zugestellt.
3. Mit dem Passwort kann sich der Empfänger am Webmailer anmelden und wird gezwungen, das Passwort zu ändern.
4. Hat der Empfänger das Passwort vergessen, kann er ein neues Passwort erstellen lassen, welches ihm per E-Mail zugestellt wird.

### Anpassung an Ihre Corporate Identity

Das Erscheinungsbild des Webmailers ist an das Corporate Identity Ihres Unternehmens vollständig anpassbar.

### Alternative 2: Schlanke PKI-Lösung

Innerhalb von JULIA MailOffice haben Sie die Möglichkeit, Zertifikate zu erzeugen. Sie teilen Ihrer Gegenstelle mit, wie mit dem Zertifikat zu verfahren und wo der Private Key zu hinterlegen ist. Nach der einmaligen Übermittlung und Einrichtung kann über das von Ihnen erzeugte Schlüsselpaar kommuniziert werden.

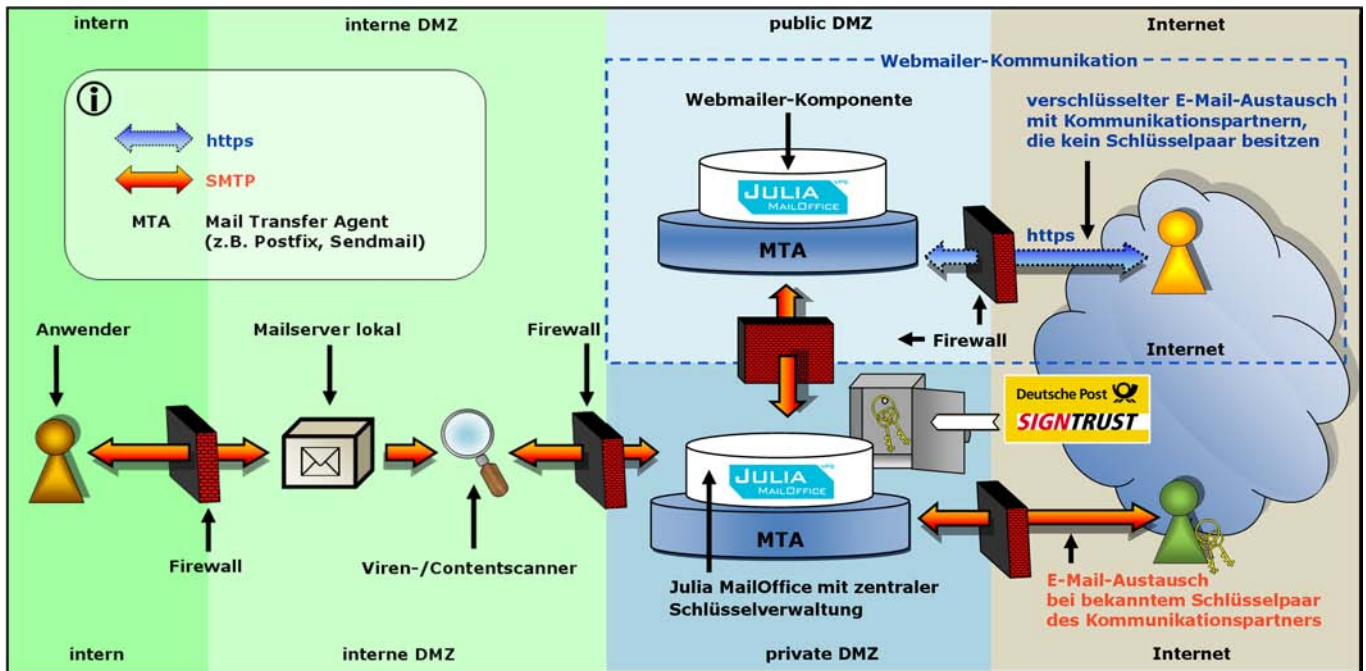
Für die Übermittlung der neu generierten Zertifikate an die Gegenstelle kann Ihr Webmailer verwendet werden. Über den Webmailer kann die Gegenstelle nach erfolgreicher Authentifizierung das von Ihnen selbst erzeugte Zertifikat zur Verwendung abrufen. Bei diesem Szenario wird der Webmailer aber nur initiativ genutzt, die spätere Kommunikation erfolgt daraufhin ausschließlich und komfortabel mit dem erzeugten Schlüsselpaar.

### Alternative 3: Übertragung als verschlüsseltes PDF / Security forced automatically (Sfa)

Besitzt der Empfänger weder S/MIME- noch PGP-Schlüssel, kann neben dem Webmailer und der schlanke PKI-Lösung folgende Variante verwendet werden, um dem Benutzer vertrauliches Material per E-Mail zukommen zu lassen:

Vor dem Versand wird die E-Mail inklusive deren Anhang in eine PDF-Datei umgewandelt. Diese PDF-Datei wird verschlüsselt und als Attachment per E-Mail an den eigentlichen Empfänger verschickt. Mit dem ihm mitgeteilten Passwort kann er die PDF-Datei öffnen und in den E-Mail Client importieren.

## BEISPIELUMGEBUNG



### Funktionsprinzip ausgehender E-Mails

Eine vom Anwender versendete E-Mail wird vom internen Mailserver, z.B. über einen Viren- / Contentscanner, an JULIA MailOffice weitergeleitet.

Anhand eines definierten Regelwerks erfolgt die Entscheidung, ob die Nachricht signiert und / oder verschlüsselt werden soll. Im Anschluss wird die Nachricht dem Empfänger zugestellt.

Steht kein Schlüssel bzw. Zertifikat des Empfängers zur Verfügung, kann die Nachricht (je nach Policy) auf dem JULIA MailOffice Webmailer hinterlegt werden.

Der Empfänger erhält eine Benachrichtigung per E-Mail und kann mit einem Passwort die Nachricht über eine verschlüsselte Internetverbindung (HTTPS) sicher vom Webmailer abrufen und verschlüsselt antworten.

### Kompatibilität

- S/MIME
- PGP
- Kompatibel zu allen gängigen E-Mail-Clients (SPHINX-Interoperabilitätstest)
- Anbindung SMTP-konformer
  - Virens Scanner
  - Content-Checker
  - E-Mail-Archivierer
  - Dokumentenmanagementsysteme (DMS)
- Bezug von Schlüsseln von Verzeichnisdiensten (LDAP)

### Funktionsprinzip eingehender E-Mails

Eine eingehende, signierte und / oder verschlüsselte E-Mail wird von JULIA MailOffice auf Gültigkeit der Signatur geprüft und entschlüsselt.

Bei Bedarf ist eine Weiterleitung an ein Archivsystem zur Aufbewahrung der ursprünglichen E-Mail möglich.

Anschließend wird die Nachricht zur weiteren Verarbeitung, z.B. Viren- / Contentscanner, an die interne E-Mail Infrastruktur übergeben.

Der interne Empfänger erhält auf Wunsch einen Dateianhang, in dem der Signaturprüfungs- bzw. Entschlüsselungsprozess von JULIA MailOffice dokumentiert ist.

### Kompatibilität (Fortsetzung)

- RFC-konforme Zertifikaterzeugung (Trustcenteranbindungen via „managed PKI“)



### Technische Mindestanforderungen

- Prozessor: Intel Pentium III oder SUN Sparc
- Mindestens 512 MB RAM
- Betriebssysteme: Linux auf Intel, Solaris 9 und 10 auf Sparc
- Mindestens 20 GB Plattenplatz

### Referenzen:

<http://www.iccsec.com> -> Unternehmen -> Referenzen