

KURZÜBERSICHT

JULIA MailOffice ist eine Erweiterung der vorhandenen E-Mail-Infrastruktur, die an zentraler Stelle ausgehende E-Mails signiert und verschlüsselt bzw. Signaturen eingehender E-Mails prüft und entschlüsselt. JULIA MailOffice wird als SMTP-Mailserver in die Netzwerkumgebung integriert.

Die Basis von JULIA MailOffice

- Signaturprüfung und Signieren an zentraler Stelle
- Ent- und Verschlüsselung an zentraler Stelle

JULIA MailOffice ist Ihre virtuelle Poststelle. Eingehende Post (E-Mail) wird auf Vertrauenswürdigkeit (Signaturprüfung) geprüft. Verschlüsselte E-Mails werden lesbar dem Empfänger zur Verfügung gestellt.

Für die ausgehende Post (E-Mail) werden die hausinternen Regeln (Policies) definiert und auf JULIA MailOffice implementiert. In Abhängigkeit zu diesen zentralen Regeln werden die Signaturen vorgenommen bzw. die Post (E-Mail) elektronisch verschlüsselt.

Unternehmenskritisch

- Umverschlüsselung
- Interne Verschlüsselung
- Mandantenfähigkeit
- Clusterfähigkeit (Lastverteilung und Hochverfügbarkeit)
- Loadbalancer
- Lineare Skalierbarkeit

Die drei Grundbedrohungen

- Verlust der Verfügbarkeit (Kosten der Wiederbeschaffung)
- Verlust der Vertraulichkeit (Haftungsschäden)
- Verlust der Integrität (Kosten der Wiederherstellung)

sind treibende, unternehmenskritische Faktoren. Es gilt diesen drohenden Gefahren entgegen zu wirken. Gleiches gilt für die hausinterne Kommunikation. Diese ist ebenso schützenspflichtig/-wert wie externe Post (E-Mail). Die benötigten Mechanismen (Zertifikate, öffentliche und private Schlüssel) können aber mit Bordmitteln kostenneutral umgesetzt werden.

Integration

- Automatisierter Zertifikatsbezug („managed PKI“) über Trustcenter wie



- Anbindung von Microsoft PKI
- Schlanke JULIA MailOffice PKI-Lösung
- Anbindung von Gegenstellen ohne Zertifikat (Webmailer, Sfa)
- Integration in E-Mailarchivierung (DMS-Systeme)

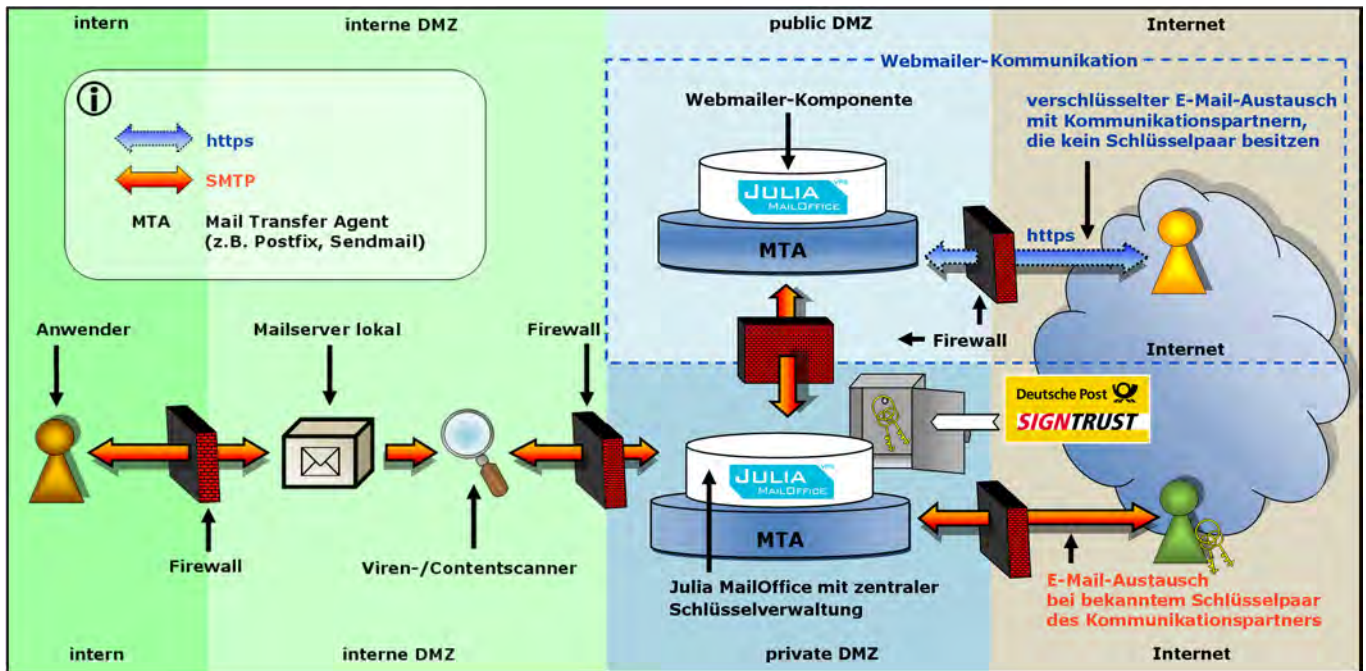
JULIA MailOffice fügt sich nahtlos in die bestehende E-Mail Infrastruktur ein. Zertifikate können selbst erzeugt (interne Kommunikation), automatisch bezogen (Trustcenteranbindung via „managed PKI“) oder aufgrund mangelnder Infrastruktur beim Kommunikationspartner via Webmailer (Gegenstelle ohne Zertifikat) gesetzes- und sicherheitskonform umgangen werden.

Komfort

- Feingranulare Parametrisierbarkeit
- Client unabhängig
- Password self service
- Security forced automatically (Sfa)
- Verschlüsselte PDF-Dateien als E-Mail
- Corporate Identity vollständig einstellbar (Gateway / Webmailer)
- Sicherheitsstufenkonform (katastrophensichere Infrastruktur, geheimhaltungskonform)
- Reine Softwarelösung (Hardware unabhängig / Appliance fähig)

Standardkonformität, hohe Kompatibilität und Anpassbarkeit an eigene Bedürfnisse sind der Investitionsschutz in die Zukunft. Komfortmerkmale wie „password self service“ und die Unabhängigkeit zum individuellen E-Mail-Client reduzieren den Einsatz von Ressourcen und Schulungsmaßnahmen im Betrieb.

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
 - Virenschanner
 - 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