

Kommunikationssicherheit und sicherer Datenaustausch mit:

julia mailoffice



Einleitung

E-Mail ist integraler Bestandteil der Geschäftskorrespondenz und muss damit einige Regeln einhalten. Zum Beispiel legt die EU-DSGVO als nur eine von vielen Regularien fest, dass personenbezogene Daten geschützt werden müssen und daher nicht im Klartext per E-Mail verschickt werden dürfen.

Diese Regeln für E-Mail gelten für alle Mitarbeitenden des Unternehmens. Ein Unternehmen muss sicherstellen, dass nur E-Mails verschickt werden, die konform mit allen vereinbarten Regeln sind. Die Entscheidung ob, und wie eine E-Mail verschickt wird, darf nicht von den jeweiligen Benutzerinnen und Benutzern, sondern muss an zentraler Stelle durch ein System getroffen werden. Nur mit einem serverbasierten System können diese Regeln zentral festgelegt und deren Einhaltung geprüft bzw. erzwungen werden.



Diese Herausforderungen meistert julia mailoffice:

- ✓ Steuerung der Sicherheit in E-Mails an zentraler Stelle
- ✓ Sicherung der Vertraulichkeit / Integrität / Authentizität von zu übertragenden oder zu speichernden Informationen
- ✓ Automatisierung von technischen Vorgängen im Umfeld von Signatur und Verschlüsselung
- ✓ Reduktion der Komplexität in der Verwaltung des Systems und der benötigten Ressourcen (z. B. Schlüssel(paare), Zertifikate, Berechtigungen etc.)

Überblick

Überblick julia mailoffice

julia mailoffice ist ein System, das Verschlüsselung und Signatur von E-Mails an zentraler Stelle erlaubt. Als Gateway-Lösung kann julia mailoffice nahtlos in die bestehende Mail-Infrastruktur integriert werden.

- ✓ E-Mail-Gateway/-Server mit der Fähigkeit, an zentraler Stelle E-Mails zu verschlüsseln und/oder zu signieren
- ✓ Sichere Austauschplattform für Dateien, auch für große Dateien
- ✓ Sicherer Datenspeicher
- ✓ DSGVO-konform
- ✓ Vertrauenswürdige IT-Sicherheitslösung seit über 20 Jahren
- ✓ Namhafte Kunden aus den Bereichen öffentliche Einrichtungen, Bundesbehörden, Versicherungen, KRITIS-Unternehmen, Industrie und Produktion, kleine, mittelständische und große Unternehmen vertrauen auf julia mailoffice
- ✓ Betrieb On-premises, in der Cloud und integriert in M365
- ✓ IT-Sicherheitsforschung und -entwicklung findet in Deutschland statt
- ✓ Deutschsprachiger Support



Kernfunktionen



Verschlüsselung und Entschlüsselung

E-Mails oder deren Anhänge (Attachments) werden automatisch und ohne, dass eine Benutzerinteraktion erforderlich ist, verschlüsselt.

Für die Verschlüsselung stehen alle gängigen Verfahren (S/MIME, PGP, AES etc.) zur Verfügung. Ein Regelwerk legt fest, für welche Kommunikationsbeziehungen welche Verschlüsselungsverfahren eingesetzt werden.

Eingehende E-Mails, die selbst oder deren Anhänge verschlüsselt sind, werden automatisch entschlüsselt.



Signatur und Signatur-Prüfung

E-Mails oder deren Anhänge (Attachments) werden automatisch und ohne, dass eine Benutzerinteraktion erforderlich ist, signiert.

Für die Signatur stehen die gängigen Verfahren (S/MIME, PGP) zur Verfügung. Ein Regelwerk legt fest, für welche Kommunikationsbeziehungen eine Signatur der ausgehenden E-Mail erfolgt.

Eingehende E-Mails, die selbst oder deren Anhänge signiert sind, werden automatisch einer Signaturprüfung unterzogen. Das Ergebnis dieser Prüfung wird der E-Mail als Bericht angehängt.



Automatisierung

Alle Vorgänge im Bereich sicherer Versand oder Empfang von E-Mails sind automatisiert.

Die Vergabe von Schlüsseln, Ausweismechanismen bei ungültigen Schlüsseln und die automatisierte Sammlung öffentlicher Schlüssel sind ohne Nutzerinteraktion gewährleistet.

Features



Höchste und aktuelle Sicherheitsstandards

Das Produkt nutzt und unterstützt höchste und aktuellste Sicherheitsstandards. julia mailoffice kann mit einer speziellen Variante der OpenSSL-Bibliothek betrieben werden kann, die vom amerikanischen National Institute of Standards and Technology (NIST) gemäß dem Federal Information Processing Standard (FIPS 140-2) zertifiziert wurde.



Einbindung in die eigene Infrastruktur

julia mailoffice kann in der eigenen Infrastruktur oder in der Cloud betrieben werden. Das Produkt kann nahtlos in M365 integriert und auch als Managed Service angeboten werden.



Erfüllung des Leitfadens der Prüfstelle des Bundes

Alle für die Erfüllung der Vorgaben der Prüfstellen des Bundes (BMI, BSI, BVA) notwendigen Maßnahmen können mit julia mailoffice abgebildet werden. Eine revisions sichere Archivierung ist gewährleistet.



Integration in M365

Sicherheit in der Microsoft-Office-365-Welt: Wird der eigene Exchange Server in der Microsoft Cloud betrieben, kann julia mailoffice Sicherheit in der E-Mail-Kommunikation schaffen. Alle Verfahren und Mechanismen können revisions sicher genutzt werden, auch wenn eigene E-Mail-Server in der Cloud betrieben werden.



Flexible Integration in SaaS-Modelle

Eine Integration in SaaS-Modelle ist mit julia mailoffice problemlos möglich. Die erforderlichen technischen (Cluster- und Mandantenfähigkeit, Containertechnologie) als auch organisatorischen Mechanismen (Accounting und Reporting) stellt das System zur Verfügung. In Ihrer Infrastruktur oder der eines Dienstleisters.



Zertifizierter kryptographischer Kern

Die Kernfunktionen von julia mailoffice (Ver- und Entschlüsselung, Signierung und Signaturenprüfung) erfolgen über Funktionen der bekannten OpenSSL-Bibliothek – auf Wunsch auch gemäß FIPS 140-2. Die kryptographischen Kernfunktionen genügen höchsten Sicherheitsansprüchen und werden fortlaufend angepasst und weiterentwickelt.



Hohe Kompatibilität auch zu proprietären Systemen

julia mailoffice verarbeitet auch E-Mails, die auf proprietären Verfahren und nicht auf den offiziellen E-Mail-Standards beruhen und ist damit abwärtskompatibel.



Integration von julia mailoffice in Geschäftsprozesse durch eine integrierte Skriptsprache

Innerhalb von julia mailoffice sind alle Modulfunktionen von außen durch eine Skriptsprache (LUA) nutzbar. Die Integration von julia mailoffice in Geschäftsprozesse, externe Werkzeuge und andere Systeme ist damit sehr einfach und mit geringem Aufwand möglich.

Aber auch komplexe Operationen an E-Mails lassen sich mit geringem Aufwand realisieren.

Beispiele:

- Alle E-Mails, die ein PDF-Dokument als Anhang enthalten, werden um einen Download-Link für den Adobe Reader ergänzt.
- Alle E-Mails, die von einer .uk-Domain stammen, bekommen einen Anhang mit einer automatisch erzeugten Übersetzung der E-Mail vom Englischen ins Deutsche.
- PDF-Dokumente im Anhang einer E-Mail werden signiert (mit fortgeschrittener oder qualifizierter Signatur) und /oder verschlüsselt.
- Aus Anhängen werden automatisch ZIP-Dateien erstellt.



Add-on: emily secure interchange

Sicherheit bei Dokumentenablage/-austausch:

emily ist ein webbasiertes System für sichere Dokumentenablage und sicheren Dokumentenaustausch. Alle Daten innerhalb von emily werden verschlüsselt. Die Sicherheit kann so hoch eingestellt werden, dass ein Betreiber von emily nicht in der Lage ist, die dort gespeicherten Daten zu lesen.



Opt-in und Opt-out Verfahren

Soll ein Kommunikationspartner explizit einem Vorgehen zustimmen, werden Opt-in-Verfahren eingesetzt. Der interne Benutzer möchte die Zustimmung von einem externen Kommunikationspartner zu einem Vorgang oder Verfahren einholen. Der interne Benutzer sendet eine vorbereitete Erklärung per E-Mail. Der externe Partner erhält einen Link zum emily Webmailer. Dort kann er die Daten einsehen und der Erklärung durch Drücken eines Knopfes explizit zustimmen oder sie ablehnen. Bei erfolgter Zustimmung erhält der interne Benutzer die E-Mail mit der Erklärung als Bestätigung zurück.



Dokumentenerkennung und Dokumentenklassen-basierte Verschlüsselung

julia mailoffice unterstützt die Klassifikation von Dokumenten und kann Informationen zu Dokumentenklassen verwenden, um die kryptographischen Operationen durchzuführen, bevor diese Dokumente verschickt werden.

Die Klassifikation eines Dokuments steuert dessen Verschlüsselung in Abhängigkeit von der Einstufung der zu versendenden Dokumente nach Grad der Vertraulichkeit.



Trustcenter-Anbindung

julia mailoffice ermöglicht die parallele und automatisierte Anbindung aller in Deutschland von Behörden und Unternehmen akzeptierten Trustcenter. Die Vorteile solcher akkreditierten Zertifikatsaussteller sind sehr vielschichtig: durch die Möglichkeit Zertifikate aller Güteklassen abrufen, einsetzen, prüfen sowie Zeitstempel aller Klassen einbeziehen zu können, lassen sich sämtliche Prozesse mit oder ohne Entfaltung rechtlicher Wirkkraft rechtskonform umsetzen, beispielsweise in den Bereichen Vertrauenswürdigkeit / Signatur, Archivierungsszenarien aller Art, Compliance und Verschlüsselung, inklusive der Auffindbarkeit dazugehöriger Zertifikatsketten. Dies geschieht zudem unter geringstem administrativem Aufwand.

Aufgrund der variablen Rollenmodelle sind der Erhebung von Policies praktisch keine Grenzen gesetzt. In den größten deutschen Bundesbehörden und internationalen Konzernen wird dies seit Jahren bereits so gehandhabt.



Regelbasiertes TLS

Kommunikationsstrecken, die einen geringeren Schutzbedarf haben, können mit TLS abgesichert und im Regelwerk von julia mailoffice gesteuert werden.



LFE – Austausch von (großen) Dateien

Der Austausch großer Dateien via E-Mail ist per se problematisch, weil in nahezu allen E-Mail-transportierenden Servern eine Beschränkung der Größe vorgenommen wird. Dies führt dazu, dass große E-Mails zwar unter Umständen versendet werden können, aber das empfangende System diese ablehnt. Die Meldung, dass diese E-Mail wegen ihrer Größe nicht zugestellt werden konnte, erhält der Absender zeitversetzt. Verwendet man den julia mailoffice Mechanismus LFE, können Dateien beliebiger Größe transparent via E-Mail verschickt werden. Diese E-Mails werden automatisch auf den emily Webmailer weitergeleitet. Der Empfänger erhält einen Link per E-Mail, mit dessen Hilfe er die große Datei herunterladen kann.



Integration von Verzeichnisdiensten (LDAP, Active Directory) möglich



Outlook-Plugin

Zum Lieferumfang von julia mailoffice gehört ein Outlook-Plugin.



Protokoll- und Auswertungsfunktionen

Die Auswertung von Protokolldateien und Logfiles in julia mailoffice erfolgt transparent und clusterübergreifend und ist darüber hinaus auch mandantenfähig. Alle Mechanismen wurden auf die Handhabung großer Datenmengen (Big Data) abgestimmt. Mögliche Auswertungen sind:

- Anzahl der eingehenden verschlüsselten oder signierten E-Mails
- Anzahl interner Benutzer, die kryptographische Operationen auslösen



Anwendungsbeispiele

Anwendungsfälle

- Verschlüsselte E-Mail-Kommunikation mit den bestehenden Geschäftspartnern, die über Schlüssel und Zertifikate verfügen.
- Sichere interne Kommunikation und Übertragung personenbezogener Daten gemäß der EU-DSGVO zwischen Ämtern, Behörden, Vorständen, Betriebsräten, Dienstleistern oder anderen Gremien, die Inhalte untereinander bereitstellen, bearbeiten und Externe einbinden müssen.
- Wenn in der deutschen Energiewirtschaft eine EDIFACT-Übertragungsdatei per E-Mail ausgetauscht wird, dann ist ausschließlich nach dem S/MIME-Standard zu verschlüsseln und zu signieren. Alle dort genannten Vorgaben für die erforderlichen kryptographischen Operationen erfüllt julia mailoffice, insbesondere RSASSA-PSS-signierte Zertifikate.
- Sichere Kommunikation mit Privatanwendern, die selbst keine Verschlüsselungstechnologie einsetzen (über Webmailkonten), zum Beispiel:

- ✓ Bei Landes-, Stadtverwaltungs- und kommunalen Behörden: E-Mail-Austausch personenbezogener Daten und verschlüsselte Kommunikation mit Bürgerinnen und Bürgern.
- ✓ Bei Krankenkassen: Verschlüsselung sensibler Patientendaten.
- ✓ In der Versicherungsbranche: Die Schadensabwicklung und der E-Mail-Austausch personenbezogener Daten sowohl mit den Versicherten als auch intern zwischen den Krankenkassen und dem Medizinischen Dienst der Krankenkassen (MDK).
- ✓ Im Bankwesen: E-Mail-Austausch personenbezogener Daten und verschlüsselte Kommunikation vertraulicher finanzieller Informationen.
- ✓ Im juristischen Bereich: Rechtsanwältinnen oder Rechtsanwälte können einen verschlüsselten E-Mail-Austausch mit ihren Mandantinnen und Mandanten durchführen.
- ✓ Bei der Polizei (Beispiel): Eine Bürgerin oder ein Bürger eröffnet konkreten Fall auf Portal „Meine Polizeiwache“ und könnte hier Dokumente wie Beweismittel hinterlegen.
- ✓ Im Bereich Personalwesen: Der Versand und die Bereitstellung von Gehaltsnachweisen.

Zusammenfassung

Vorteile und Nutzen

Merkmale:

- ✓ Hohe Betriebsstabilität und Performance
- ✓ Skalierbar für jede Unternehmensgröße
- ✓ Nahtlose Integration in Betriebsprozesse
- ✓ Aufrechterhaltung der Integrität und Vertraulichkeit
- ✓ Sichere Kommunikation auch mit Empfängern ohne eigene Verschlüsselung
- ✓ Regelwerk adaptierbar nach unternehmenseigenen Compliance-Vorgaben
- ✓ Einbindung von VS-NfD-konformer Kommunikation

Vorteile/Mehrwerte:

- ✓ Weniger Aufwand durch Automatisierung bzw. Zentralisierung der Prozesse
- ✓ Nachhaltigkeit durch Prozess-Digitalisierung
- ✓ Erfüllung gesetzlicher Vorgaben, Verordnungen und Compliance-Richtlinien
- ✓ Vermeidung von Bußgeldern durch Datenschutzverstöße
- ✓ Minimierung von Reputationsrisiken
- ✓ Automatisierte Anbindung etablierter Trust Center zum effizienten und direkten Bezug von Zertifikaten über Allgeier CyRis

Fazit

Eine sorgfältig geplante Digitalisierung kann enorme Vorteile bringen, wenn die E-Mail-Verschlüsselung als Basistechnologie in die Digitalisierungsstrategie des Unternehmens integriert wird und auch die Kommunikation mit Privatpersonen umfasst.

Durch die hohe Automatisierung werden die Sicherheitsvorgaben fehlerfrei, effizient und DSGVO-konform umgesetzt.

Unternehmen und Institutionen, die ihren Interessenten, Kunden, Klienten, Patienten, Mandanten oder Bewerbern eine einfach zu bedienende und sichere Kommunikationslösung anbieten können, haben einen klaren Wettbewerbsvorteil.

Sorgen Sie für einen rundum verschlüsselten Austausch von E-Mails und Daten mit julia mailoffice.

Vereinbaren Sie noch heute ein unverbindliches Beratungsgespräch mit unseren Cybersecurity-Experten unter

+49 (0) 421 438 41 875

oder nutzen Sie ganz einfach unser [Kontaktformular](#).



Impressum / V.i.S.d.P.

Herausgeber: Allgeier CyRis GmbH
Hans-Bredow-Straße 60 28307 Bremen

Redaktionsleitung: Sebastian Rüter · Tel: +49 40 389 071-172
sebastian.rueter@allgeier-cyris.de

Grafikdesign: Tobias Wölky · www.woelky-grafik.de

Haftungsausschluss: Die Inhalte dieses Dokuments wurden mit größtmöglicher Sorgfalt recherchiert. Eine Haftung für die Richtigkeit, Vollständigkeit und Aktualität kann jedoch nicht übernommen werden. Allgeier CyRis übernimmt insbesondere keinerlei Haftung für eventuelle Schäden oder Konsequenzen, die durch die direkte oder indirekte Nutzung entstehen.

**Sie möchten mehr
über unsere Lösungen
erfahren?**

✉ **Allgeier CyRis GmbH**
Hans-Bredow-Straße 60
28307 Bremen

+49 (0) 421 438 41 875
info@allgeier-cyris.de
www.allgeier-cyris.de

ALLGEIER
CyRis