julia mailoffice

julia mailoffice 3.5

ALLGEIER IT

julia mailoffice

julia mailoffice hat sich bereits im Einsatz bei Konzernen und Behörden bewährt. Insbesondere sind Stabilität, Skalierbarkeit und Performance sowie nahtlose Integration in Betriebsprozesse hervorzuheben. Wenn vor Jahren vielleicht noch die Frage bestand „Wie kann ich sicher per E-Mail kommunizieren?“, muss man heute feststellen, dass Server-basierte Verschlüsselungssysteme längst fester Bestandteil von IT-Infrastrukturen mit entsprechenden Sicherheitsanforderungen sind. Die Version 3.5 bietet darüber hinaus neue Features, die den gewachsenen Bedarfen und rechtlichen Anforderungen gerecht wird.

Die Features

Erfüllung des Leitfadens der Prüfstelle des Bundes

Im Zuge immer weitreichenderer digitalisierter Geschäftsprozesse in der Versicherungsbranche ist für diese - insbesondere beim Austausch von (Kunden) Dokumenten mit der Pflicht auf eine Entfaltung rechtlicher Wirkung und entsprechendem Integritätsschutz - ein rechtskonformer Ablauf und Zustand herzustellen. Diese Vorgaben, die über einfache Standards in der Archivierung nicht abbildbar sind, werden durch die Prüfdienste des Bundes (BMI,BSI,BVA) erhoben. Demnach sind eingehende Nachrichten (sämtliche Teile einer E-Mail, DE Mail oder eines elektronischen Faxes) unmittelbar ab dem Zeitpunkt des Empfangs in ihrem ursprünglichen, originalen Zustand zu erhalten. Ziel ist es, aus diesen Originalen direkt nach ihrer Annahme jeweils ein archivierbares und qualifiziert signiertes Dokument zu erzeugen. Dieses muss zu jeder Zeit innerhalb sämtlicher internen Prozesse wieder aufrufbar sein, wobei sein ursprünglicher Zustand rechtskonform über das Anbringen eines Qualifizierten Zeitstempels oder einer Qualifizierten Signatur nachzuweisen ist. Alle für die Erfüllung der Vorgaben der Prüfstellen des Bundes notwendigen Maßnahmen können mit julia mailoffice abgebildet werden.

Regelbasiertes TLS

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

Integration in office 365

Sicherheit in der Office 365 Welt – dies ist mit julia mailoffice zu erreichen. 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 genutzt werden, auch wenn eigene Mail-Server in der Cloud betrieben wird.

LFE

Der Austausch großer Dateien via E-Mail ist per se problematisch, weil in nahezu in allen E-Mail-transportierenden Mail-Servern ein Beschränkung der Mail-Größe vorgenommen wird. Dies führt dazu, dass große Mails zwar unter Umständen versendet werden können, aber das empfangende E-Mail-System diese Mail 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 Mails werden automatisch auf den julia Webmailer ausgesteuert, der Empfänger erhält einen Link per E-Mail, mit dessen Hilfe er die große Datei herunterladen kann.

emily Webmailer

Der emily Webmailer erlaubt die sichere Kollaboration auch entfernter Kommunikationspartner. Mit Hilfe des Channel-Konzepts kann ein Nutzer sichere Komunikationsräume schaffen. Als Besitzer des Channels lädt er Partner ein und legt deren Rechte (schreiben/lesen) fest. Alle in emily Webmailer gespeicherten Daten werden so verschlüsselt, dass ein Betrieb in der Cloud möglich ist. Auch wenn ein Administrator Zugang zu einem emily Webmailer Server hat, kann dieser die Daten nicht einsehen.

Opt-Out-Verfahren

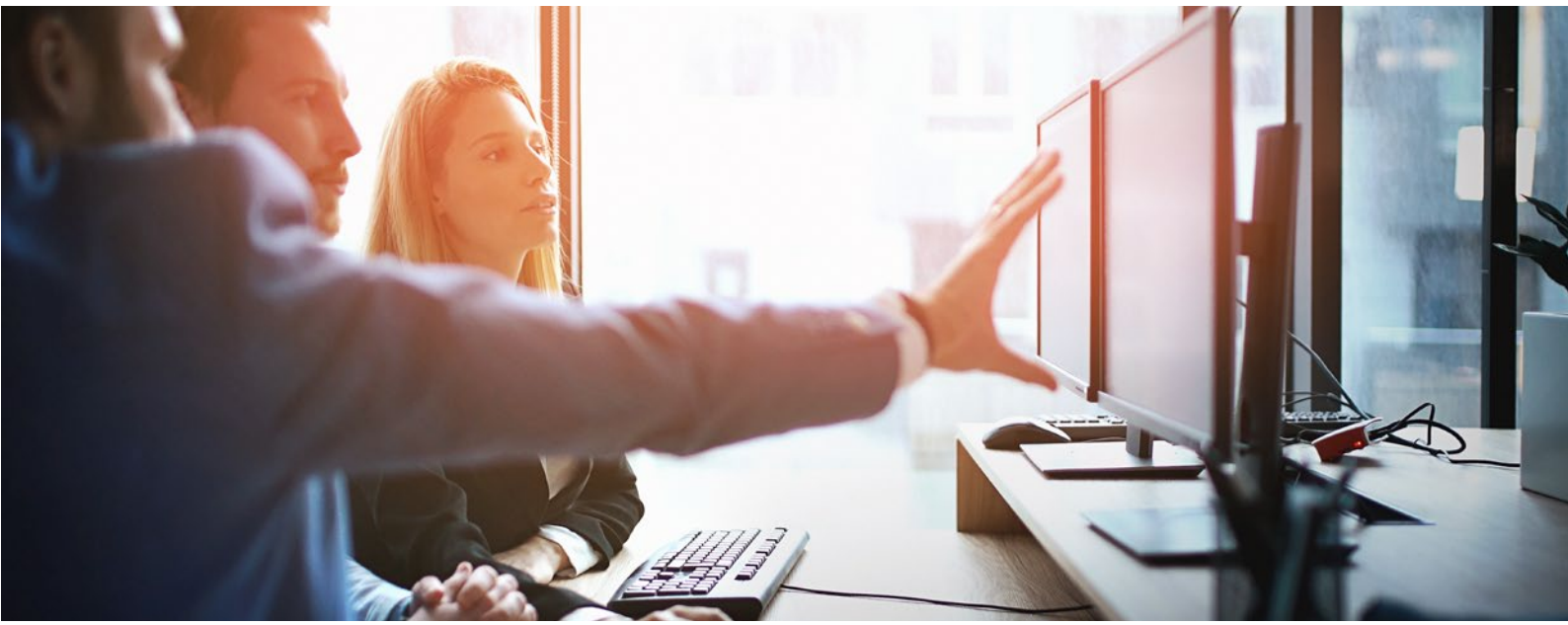
Opt-out Verfahren bezeichnet im Permission Marketing ein Verfahren, bei dem eine Information zugesandt wird oder persönliche Daten gespeichert werden, sofern der Betroffene dem nicht aktiv widersprochen hat. Mit Hilfe dieses Verfahrens kann der externe Kommunikationspartner in julia mailoffice zum Beispiel bestimmen, dass er keine Veränderung in der Art der E-Mail-Kommunikation wünscht und die Daten weiterhin unverschlüsselt gesendet werden können.

LDAP Integration

Abläufe in julia mailoffice können über LDAP-Server (z.B. AD-Server einer Domäne) gesteuert werden. Zum Beispiel liefern Informationen in einem LDAP-Server Parameter für das Regelwerk. Diese Parameter legen fest, welcher Benutzer zum Beispiel Schlüssel beantragen kann, wer verschlüsseln oder signieren darf.

Opt-In-Verfahren

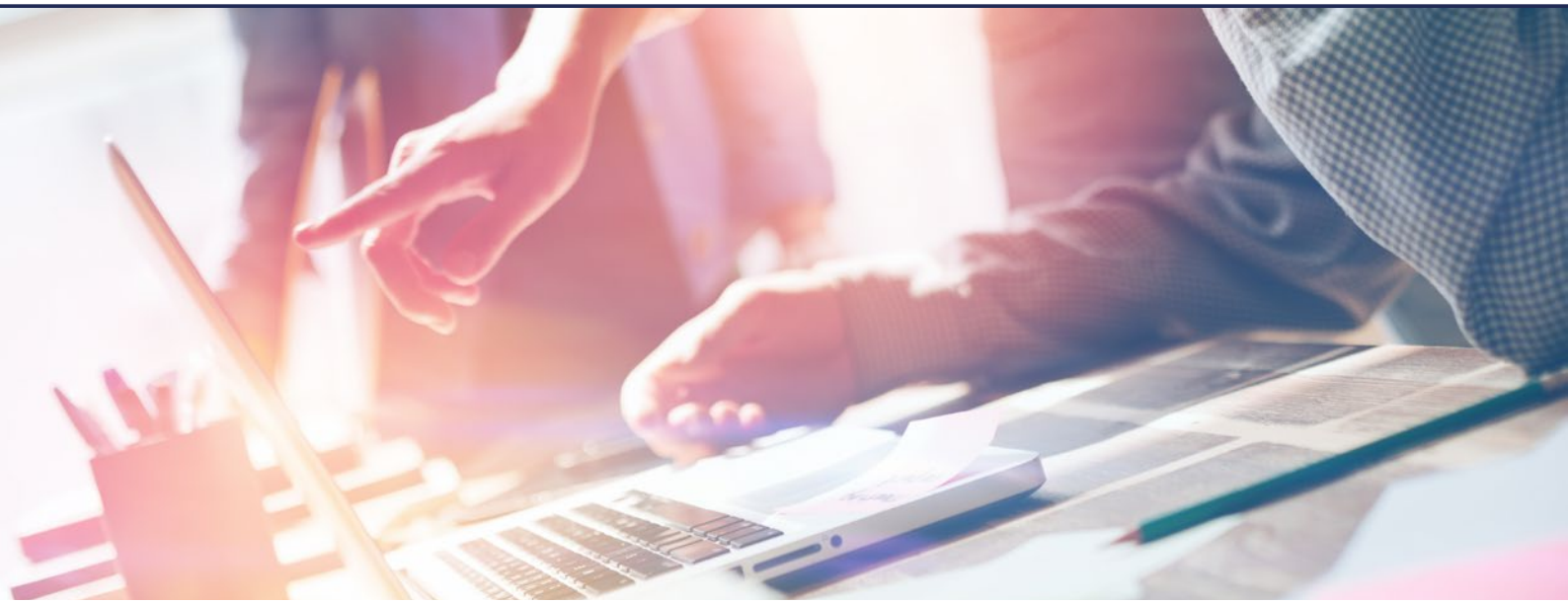
Soll ein Kommunikationspartner explizit einem Vorgehen zustimmen, werden Opt-in-Verfahren eingesetzt. Der interne Benutzer möchte die Zustimmung von einem externen Kommunikationspartner zu einem Vorgang oder Verfahren einholen. Der interne Benutzer sendet eine vorbereitete Erklärung per E-Mail. Der externe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



Neuer EDIFACT Standard

Wenn mit der in der deutschen Energiewirtschaft eine EDIFACT-Übertragungsdatei per E-Mail ausgetauscht wird, dann ist spätestens ab dem 01.06.2017 ausschließlich nach dem S/MIME-Standard zu verschlüsseln und zu signieren. Es ist mindestens die S/MIME-Version 3. 2 IETF RFC 5751, Veröffentlichungsjahr 2010 einzuhalten. Alle dort genannten Vorgaben für die erforderlichen kryptographischen Operationen erfüllt julia mailoffice, insbesondere RSASSA-PSS signierte Zertifikate.

julia mailoffice



Trustcenter-Anbindung

julia mailoffice ermöglicht die parallele 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 administrativen 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 eingesetzt.

PKI-Verwaltung

Die PKI-Verwaltung von julia mailoffice ermöglich die parallele Nutzung mehrerer CAs. Private PKI oder offizielle Trust Center – die gleichzeitige Verwendung mit denselben Mechanismen ist problemlos möglich.

Interne Verschlüsselung

Auch die innerhalb des Unternehmens verlaufenden E-Mail-Strecken können gesichert werden. Die so genannte „interne Verschlüsselung“ ermöglicht die lückenlose Verschlüsselung von E-Mails, die zwischen externen Kommunikationspartnern und internen Benutzern ausgetauscht werden. Diese wird zum einen durch Umverschlüsselung der E-Mails erreicht, die von julia mailoffice transportiert werden. Zum anderen werden interne E-Mails, die nur auf dem Exchange Server ausgetauscht und julia mailoffice nicht erreichen, mit Schlüsseln aus der internen Microsoft-PKI verschlüsselt. Die Vorteile eines Server-basierten Ansatzes (zentrale Schlüsselverwaltung, zentrales Regelwerk, etc.) bleiben erhalten, es sind dazu keine Maßnahmen auf dem Client erforderlich. Stellvertreter-Regelungen sind mit Hilfe von julia mailoffice auch bei eingesetzter E-Mail-Verschlüsselung umsetzbar.

Sicherer Informationsaustausch

Sicherer Informationsaustausch per E-Mail beschränkte sich früher auf die reine Verschlüsselung von E-Mails unter Einhaltung der gängigen Standards wie S/MIME, PGP und TLS für eine Transportverschlüsselung. Als integraler Bestandteil der Geschäftskorrespondenz ist heutzutage der Kontext und die Prozesse zu beachten. julia mailoffice ist nicht länger nur ein E-Mail-Gateway, sondern (eher) ein Workflow-System für den sicheren Transport von Informationen unter Zurhilfenahme von E-Mail. Workflows erfordern eine zuverlässige und sichere Kommunikation, die über die reine Verschlüsselung von E-Mails hinaus geht. Können zum Beispiel E-Mails nicht mit S/MIME oder PGP verschlüsselt werden, kommen andere Verfahren zum Einsatz, um die geforderte Sicherheit in der Kommunikation durchzusetzen. Beispiele für solche Ausweichverfahren sind der Versand verschlüsselter ZIP- oder PDF-Dateien oder die Aussteuerung auf ein sicheres Web-Portal (julia webmailer).

Freigaberegelungen

Manuelle Freigaben bestimmter E-Mails können durch eine autorisierte Person vorgenommen werden – eine wichtige Funktion, um interne Workflows implementieren zu können.

Sichere Workflowfunktionalitäten

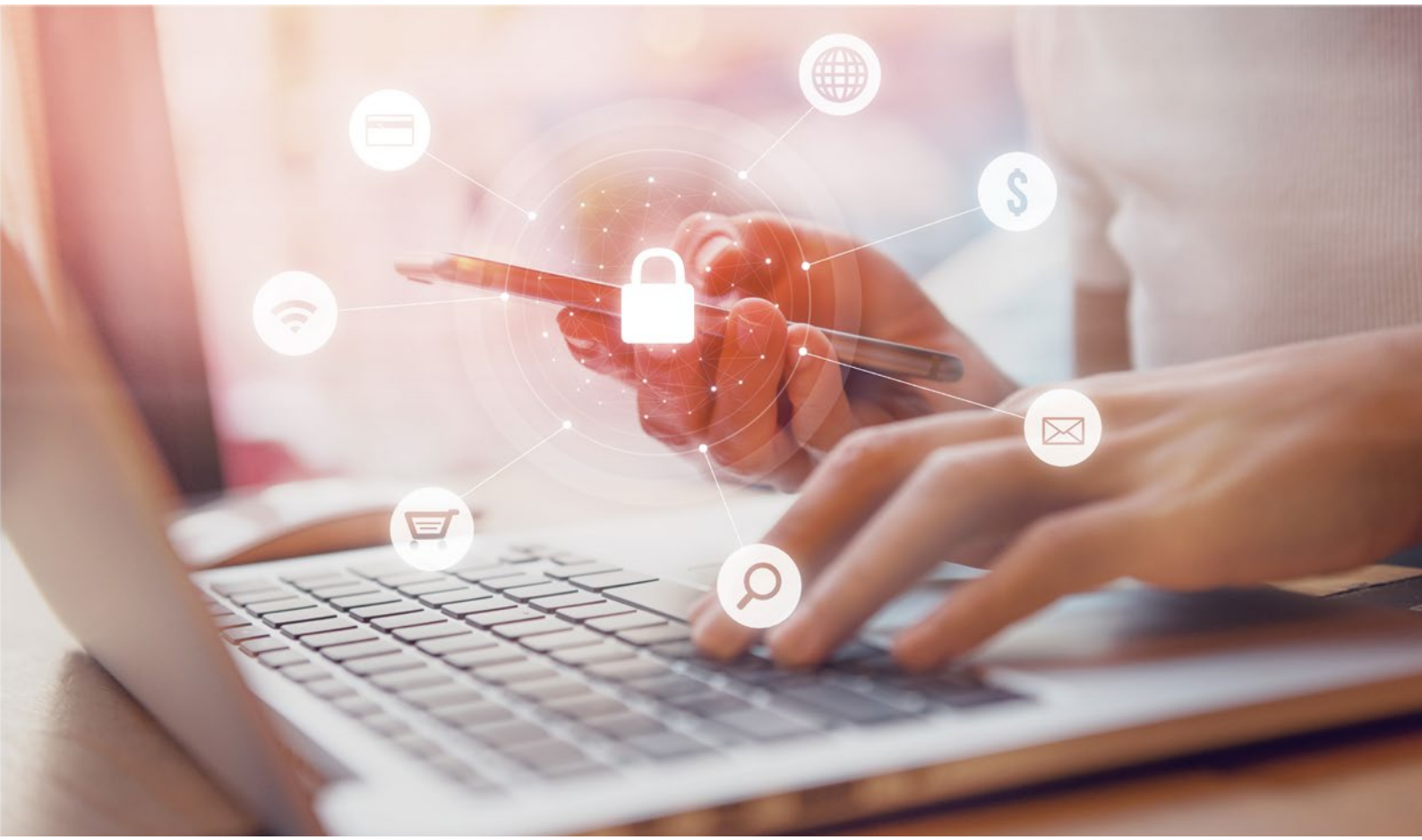
Alle Aktivitäten in julia mailoffice, wie zum Beispiel „Verschlüsseln“, „Signieren“, „Entschlüsseln“, „Prüfen“, „Archivieren“, können durch eine Skriptsprache von externen Komponenten genutzt werden. So ist es leicht möglich, sichere, elektronische Workflows durch ein entsprechendes Zusatzmodul zu implementieren. Ein einfaches Beispiel ist ein Rundschreiben, das von mehreren Personen gelesen und abgezeichnet werden muss: jeder Teilnehmer bestätigt durch das Anbringen einer Signatur an dem Dokument, dass er es gelesen hat. Wird das Dokument am Ende in einem Archiv abgelegt, ist so nicht nur das Dokument sondern auch die Information, von wem es gelesen wurde, mit gesichert.

Sichere Kollaboration

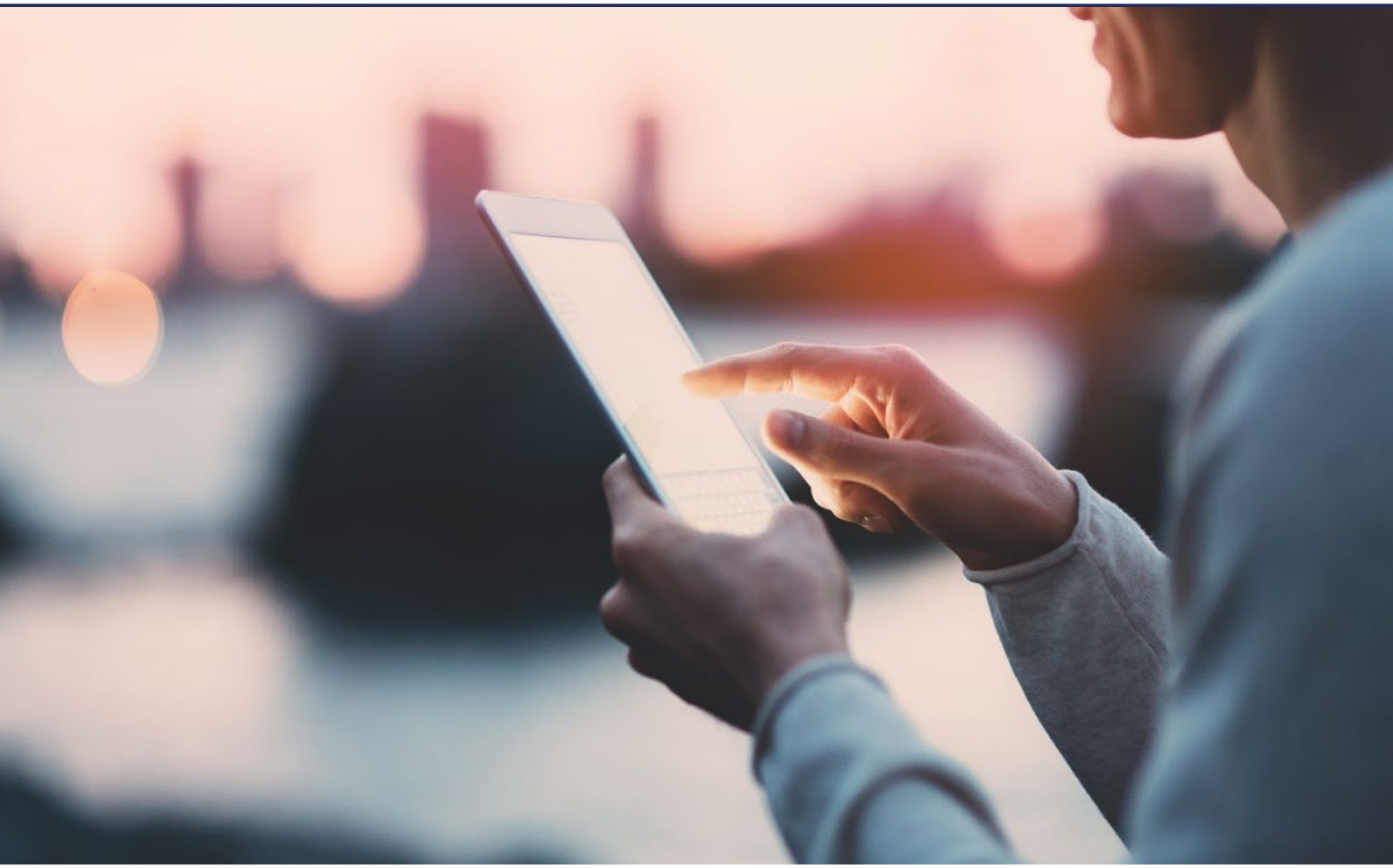
Aus Anwendersicht ist sichere Kollaboration, dass ein entsprechendes System folgendem Paradigma genügen muss:

„Ein authentifizierter Anwender soll zu jedem beliebigen Zeitpunkt, von jedem beliebigen Ort aus, mit Hilfe eines beliebigen Endgeräts mit den für ihn oder sie freigegebenen Dokumenten arbeiten können.“

Das bedeutet, dass sowohl die Speicherorte der Dokumente als auch deren Transportwege verschlüsselt sind. Und zwar genau so, dass ein Dritter, der die Infrastruktur betreibt, die Information trotz seines administrativen Zugangs nicht lesen kann.



julia mailoffice



Flexible Integration in SaaS-Modelle

Eine Integration in beliebige SaaS-Module ist mit julia mailoffice problemlos möglich. Die erforderlichen technischen (Cluster- und Mandantenfähigkeit) als auch organisatorischen Mechanismen (Accounting und Reporting) stellt das System zur Verfügung.

Modulare Template-Engine

Alle Meldungen – insbesondere Rückmeldungen an Benutzer – und Web-Seiten werden durch Templates gesteuert. Anpassungen an eigene Bedarfe oder an die Unternehmens-CI sind einfach möglich.

Zertifizierter kryptographische Kern

Die Kernfunktionen von julia mailoffice (Ver- und Entschlüsseln, Signieren und Signaturen prüfen) erfolgen über Funktionen der bekannten OpenSSL-Bibliothek. Auf Wunsch läuft julia mailoffice zudem mit einer speziellen Variante dieser Bibliothek, die vom amerikanischen National Institute of Standards and Technology (NIST) gemäß dem Federal Information Processing Standard (FIPS 140-2) zertifiziert wurde. Die kryptographischen Kernfunktionen genügen damit höchsten Sicherheitsansprüchen.

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.

Bereitstellung flexibler Mechanismen zur 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. Dies ist wichtig, da es sich bei julia mailoffice nicht nur um ein E-Mail-Gateway mit kryptografischer Funktionalität, sondern um eine skalierbare, integrierte Lösung für Dokumenten- und Informationsverarbeitung auf der Basis von Standardprotokollen handelt. Die integrierte Skriptsprache ermöglicht alle denkbaren Veränderungen an ausgehenden oder eingehenden E-Mails ohne großen Aufwand. LUA-Skripte können in belieber Zahl als „Before-" und „After-Gateway-Filter" für die Verarbeitung eingehender E-Mails und als „Before-" und „After-MailOffice-Filter" für die Verarbeitung ausgehender E-Mails eingesetzt werden.

Aus den Skripten heraus kann auf jede Eigenschaft und jedes Element (Anhang, Header, From, To, etc.) beliebig zugegriffen werden. Auf diese Weise ist z.B. die Integration eines Viren-Scanners oder Content-Filters in das julia mailoffice System sehr einfach möglich.

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

- Alle E-Mails, die ein PDF 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.

Dokumentenerkennung und Dokumentenklasse-basierte Verschlüsselung

Der Schutzbedarf ist bei Dokumenten von deren Inhalt abhängig. julia mailoffice unterstützt die Klassifikation von Dokumenten und kann Informationen zu Dokumentenklassen verwenden, um die kryptographischen Operationen durchzuführen, bevor diese Dokumente verschickt werden. So können zum Beispiel für jede Dokumentenklasse die durchzuführenden Schutzmaßnahmen festgelegt werden. Die Klassifikation eines Dokuments steuert dessen Verschlüsselung in Abhängigkeit von der Einstufung der zu versenden Dokumente – z.B. „vertraulich", „geheim" oder „streng geheim". Die Zuordnung zwischen einzusetzenden Verschlüsselungsverfahren und Dokumentenklassen wird in einer Tabelle hergestellt. Die Anzahl der Dokumentenklassen ist nicht beschränkt.

Outlook-plugin

Zum Lieferumfang von julia mailoffice gehört ein Outlook-plugin. Mit Hilfe dieses Plugins können neben sämtlichen Kernfunktionen auch beispielsweise LFE, die Krypto-Vorschau oder der Versand als DE-Mail kombiniert und ausgelöst werden.

Übergang in DE-Mail mit julia mailoffice

julia mailoffice erlaubt den sicheren Übergang von der „normalen" E-Mail-Welt in die DE-Mail-Umgebung. Der Absender verwendet wie gewohnt seinen E-Mail-Client und stellt entsprechende Versandoptionen in Outlook oder Notes ein. julia mailoffice übernimmt den Austausch zwischen E-Mails und DE-Mail-Nachrichten.

Protokoll- und Auswertungsfunktionen

Die Auswertung von Protokolldateien in julia mailoffice erfolgt transparent und Cluster-übergreifend 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, die Anzahl interner Benutzer, die kryptographische Operationen auslösen, etc..

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

julia mailoffice

ALLGEIER IT

Allgeier IT Solutions GmbH

Hans-Bredow-Straße 60
28307 Bremen

Telefon: +49 421 43841 0
Telefax: +49 421 43808 1

info@allgeier-it.de
www.allgeier-it.de