

**Sichere E-Mail-
Kommunikation mit**

MAILU
— Secure —

E-Mail-Verschlüsselung mit S/MIME & PGP

Die Digitalisierung von Geschäftsprozessen schreitet immer schneller voran

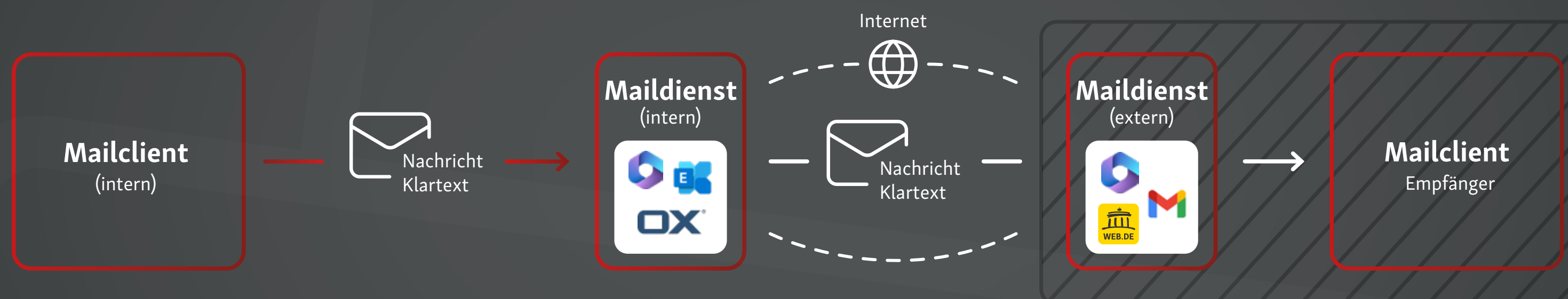
Kaum etwas in der Informationstechnik im Unternehmen oder in der Behörde entwickelt seine Anforderungen in einer solchen Vielfalt und Geschwindigkeit. Entscheidend sind dabei vornehmlich Kostenersparnis, eine höhere Qualität und die schnellere Bearbeitungsgeschwindigkeit von Vorgängen.

Das **Kommunizieren**, ganz gleich ob im **Dialog** oder im **Austausch von Daten**, spielt dabei eine immer größere Rolle. Bisher war dabei zumeist das Einhalten von Datenschutzkriterien im Blick, inzwischen werden jedoch immer klarer die eigenen Geschäftsprozesse als ein Gesamthema erkannt – mit positiven Auswirkungen auf Sicherheit, Effizienz und letztlich auch die Produktivität.

Unsere jahrelange Erfahrung als Partner für den Betrieb und die Beratung sicherer Kommunikationslösungen konnten wir nun bündeln: mit dem aus eigener Entwicklung stammenden Mail-Gateway **mail:u Secure**. Diese Software erfüllt nicht allein die Anforderungen des modernen IT-Betriebs, sie zeigt **neue Wege** in der **Digitalisierung** von Abläufen auf, immer mit Fokus auf den Unternehmenszweck.

Über eine Technologiepartnerschaft integrieren wir hierbei den zertifizierten GnuPG VS-Desktop® nahtlos. Damit erreicht mail:u Secure im Zusammenspiel mit GnuPG VS-Desktop® das Sicherheitsniveau VsnfD für ausgewählte Nutzer.

Unverschlüsselter Mailverkehr



Gateway

Die Möglichkeiten des **mail:u Secure** Gateways inklusive der Schlüsselverwaltung umfassen mehrere zentrale Aspekte. Im Vordergrund steht dabei die Digitalisierung von Prozessen bei gleichzeitiger Absicherung.

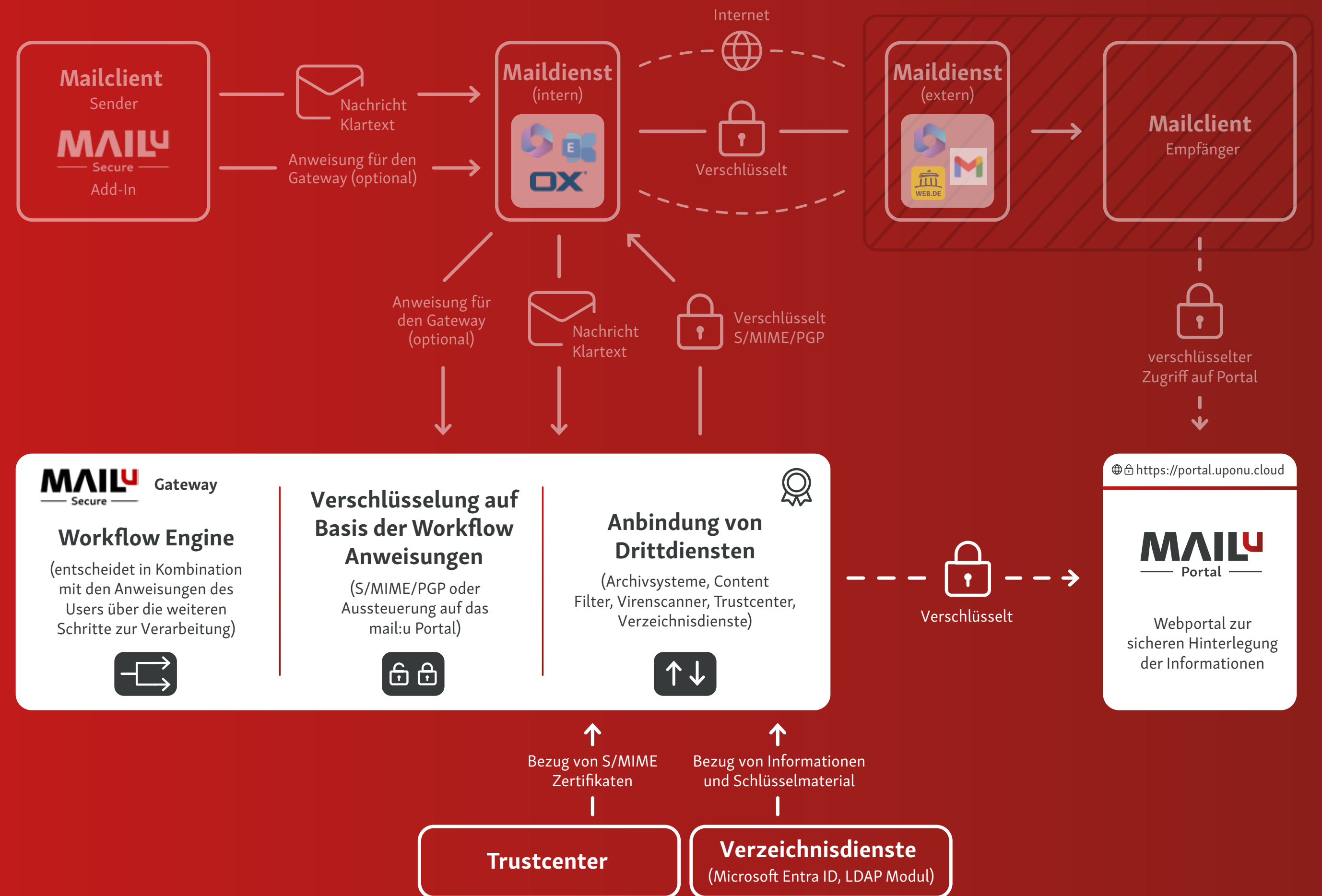
Die Schlüsselverwaltung ermöglicht eine effiziente Handhabung von privaten sowie öffentlichen Schlüsseln, die für die sichere Kommunikation unerlässlich sind. Durch die Automatisierung des Schlüsselverwaltungsprozesses wird der Aufwand für die manuelle Verwaltung erheblich reduziert, was zu einer höheren Effizienz führt.

Zudem bieten einfache Workflows Unterstützung bei Verschlüsselung und Signatur. Diese Workflows sind darauf

ausgelegt, manuelle Tätigkeiten zu minimieren, sodass sich die Administratoren auf andere Aufgaben konzentrieren können.

Schließlich wird durch den Einsatz modernster Kryptografie sichergestellt, dass die höchsten Sicherheitsstandards erfüllt werden. Zusätzlich werden mittels automatisiert bezogener Klasse 2 Zertifikate die Datenintegrität sowie Vertrauenswürdigkeit gewahrt. Insgesamt trägt dieses System dazu bei, die Sicherheit der Kommunikation zu gewährleisten und gleichzeitig den Verwaltungsaufwand zu verringern.

Integration in den Mailflow via SMTP (Integration als SaaS oder On-Premises möglich)



Marketing

DashboardGatewayPortalPublickeysAdd-InsFormulare

Marketing UPONU

Dashboard

Übersicht über die aktivierten Module des Mandanten

Gateway

Bearbeiten

URL:
<https://marketing.admin.mail-u.cloud>

IDP URL:
<https://marketing.admin-auth.mail-u.cloud/ui/console>

Mandant:
368423853187138175

Entra ID:
AKTIVIERT

Version
V0.42.17

Portal - marketing

BearbeitenLöschen

URL:
<https://marketing.portal.mail-u.cloud>

IDP URL:
<https://marketing.portal-auth.mail-u.cloud/ui/console>

Version
V0.42.17

Publickeys

BearbeitenLöschen

URL:
<https://marketing.publickeys.mail-u.cloud>

Basic:
AKTIVIERT

WKD:
AKTIVIERT

LDAP:
AKTIVIERT

Version
V0.42.17

Formulare

BearbeitenLöschen

URL:
<https://marketing.forms.mail-u.cloud>

Version
V0.42.17

Addin

BearbeitenLöschen

URL:
<https://marketing.addin.mail-u.cloud>

Version
V0.42.17

Filelink

BearbeitenLöschen

Filelink:
<https://marketing.filelink.mail-u.cloud>

Version
V0.42.17

E-Mail-Adressen

Workflow

Portal Modul hinzufügen

Workflowbasiertes Regelwerk

Das **mail:u Secure** Regelwerk ist ein leistungsstarkes System, das durch eine Workflow Engine umfangreiche Bearbeitungsmöglichkeiten für durchlaufende Nachrichten bietet. Es ermöglicht die Entscheidungsfindung über verschiedene Bearbeitungsprozesse, die auf einer Vielzahl von Bedingungen basieren. Diese Bedingungen können miteinander verknüpft werden, um komplexe Entscheidungsstrukturen zu erzeugen.

Zu den entscheidenden Faktoren gehören unter anderem Steuerbefehle, die vom Anwender über Add-Ins, Header oder den Betreff der Nachricht gegeben werden. Darüber hinaus können Entscheidungen auch auf Basis von Absender- oder Empfängerinformationen sowie dem Inhalt und den Anhängen der Nachricht getroffen werden. Bei der Analyse von Inhalten und Anhängen spielen Aspekte wie der Inhalt,

die Größe und der Dateityp eine wesentliche Rolle.

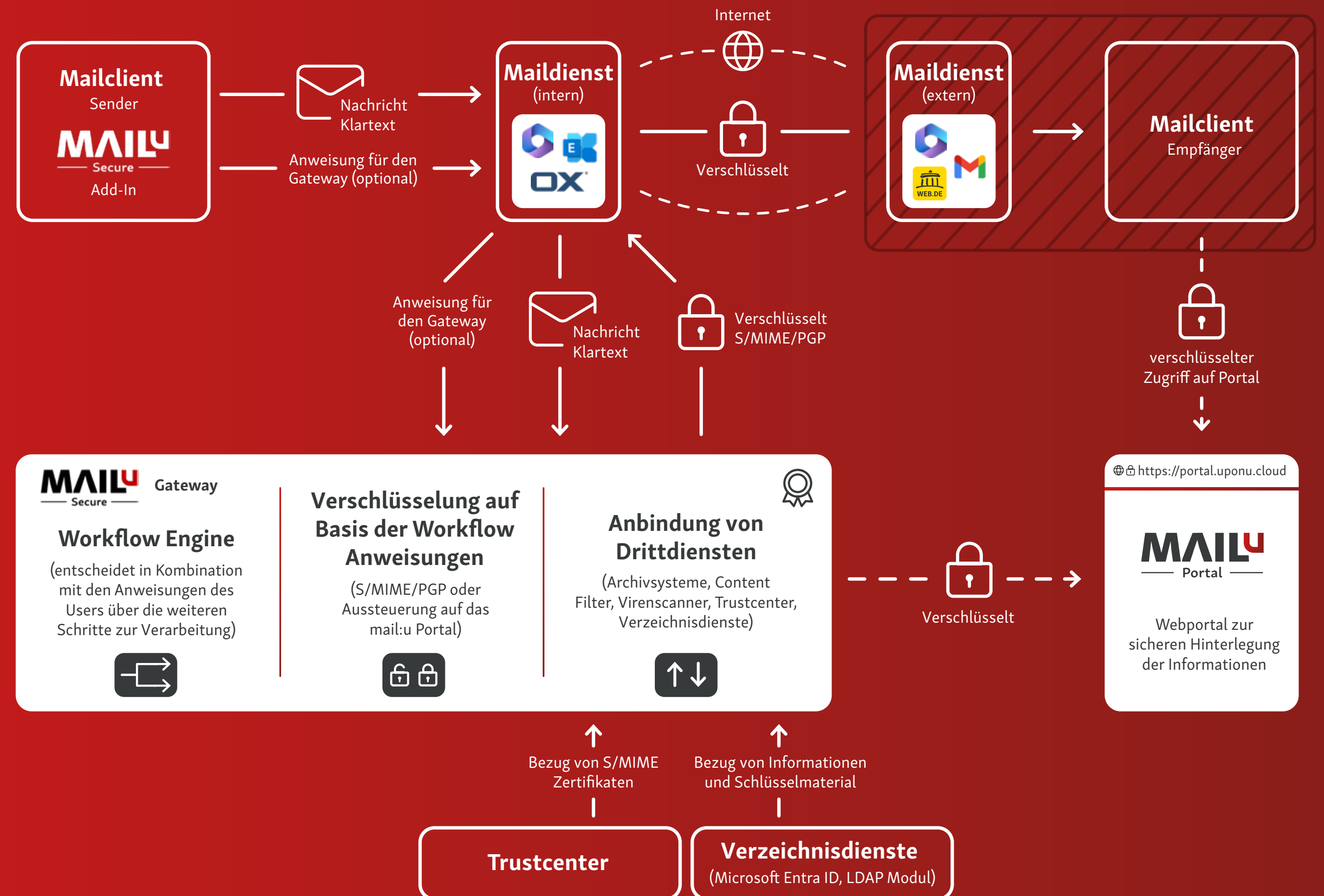
Dank der modularen Architektur können in der nachfolgenden Verarbeitung flexibel verschiedene Dienste integriert werden, wie beispielsweise die Anbindung an ein Archivsystem.

Ein praktisches Beispiel verdeutlicht die Funktionsweise: Wenn eine ausgehende E-Mail mit einer .docx-Anlage versendet wird und keine spezifischen Regeln für Absender oder Empfänger sowie keine Steuerbefehle vom Benutzer vorliegen, kann das Regelwerk so konfiguriert werden, dass die .docx-Anlage aus der E-Mail extrahiert und sicher über unser Modul zum Austausch großer Dateien an den Empfänger übermittelt wird.

Die eigentliche Nachricht wird dann „normal“ mit einem Verweis auf die Anlage versendet. Ein Beispiel für die flexible

Architektur ist der via Partnerschaft angebundene GnuPG VS-Desktop®: Die Workflow Engine lässt die E-Mails unverändert passieren und die benötigten Öffentlichen-Schlüssel werden über Schnittstellen abgerufen, sodass die gesamte kryptografische Verarbeitung auf VsnfD-Niveau mit minimierten Aufwand im Hintergrund abläuft.

Integration in den Mailflow via SMTP (Integration als SaaS oder On-Premises möglich)



Workflow

Schlüsselverwaltung

Autocert

Konfiguration

SMTP-Konfiguration

Logs

PDF-Passwörter

Nutzungsberichte

Warteschlange

Demo GmbH

DashboardGatewayPortalPublickeysAdd-InsFormulare

Andreas Blumberg

Regelset

Aktueller Arbeitsstand der Regeln.

Erstellen

Ansehen

Löschen

Kopieren

Nach oben

Nach unten

Standard

Aktiviert

Name

Aktiviert

Name

Eingabetyp

Stoppen

Akzeptieren

Zuletzt geändert

	1	✓	Test Lagacy AddIN	Original	✓	✓	31.01.2026 18:07:51
	2	✓	untouched by force	Original	✓	✓	03.07.2025 15:48:45
	3	✓	untouched by calendar and group	Original	✓	✓	16.09.2025 01:25:22
	4	✓	internal recipients	Entschlüsselt und verifiziert	✓	✓	16.09.2025 01:25:23
	5	✓	Header Clean	Addition	✗	✗	30.09.2025 02:06:32
	6	✓	Portal Command	Original	✓	✓	29.04.2026 22:47:50
	7	✓	Portal Command - Neu	Original	✓	✓	29.04.2026 22:47:56
	8	✓	PDF Command	Original	✓	✓	16.10.2025 23:39:22
	9	✓	sign and encrypt - S/MIME	Original	✓	✓	16.09.2025 01:27:02
	10	✓	sign and encrypt - PGP	Original	✓	✓	16.09.2025 01:27:02
	11	✓	encrypt - S/MIME	Original	✓	✓	16.09.2025 01:27:02

Zeilen pro Seite

25

1-18 von 18

Bearbeiten

AllgemeinBedingungenAktionenErweitert

Filelink

Bedingungen

Anhänge durch Links ersetzen, wenn größer als

5 MB

Regulärer Ausdruck, um Anhänge anhand ihres Namens zu ersetzen

Beispiel, um Dateien zu ersetzen, die auf .doc oder .docx enden: \.docx?\$

\.pdf\$

Konfiguration

Gültigkeit der Downloadlinks

96 h

Dem Empfänger erlauben, eigene Dateien hochzuladen

Tag HTML-Vorlage

Wenn keine Vorlage ausgewählt ist, wird die Standardvorlage verwendet.

Header verändern

Dokumentation

Operation

Löschen

Headerpaar angeben, das entfernt werden soll

Schlüssel

Gleich

X-Mailu-Y3tk1esl

Wert

Immer

Template-Vorverarbeitung

PKI

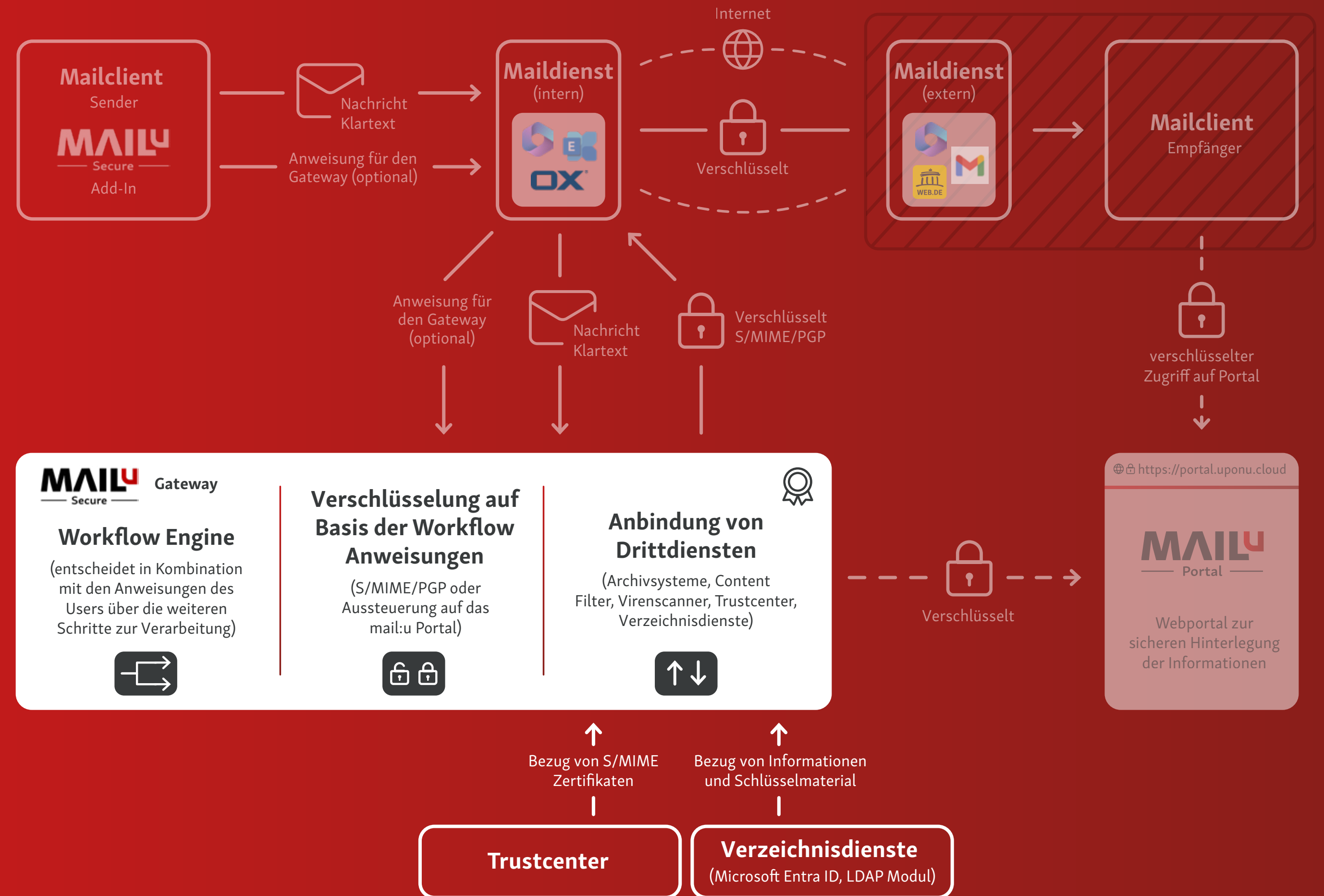
Zur Vertrauenswürdigkeit in der digitalen Kommunikation gehört der Einsatz valide prüfbarer Zertifikate.

Die PKI-Integration unseres **mail:u Secure** Gateways ermöglicht die Anbindung eigener oder externer PKI-Systeme akkreditierter Trustcenter. Aktuell können personenbezogene Zertifikate der Klasse 2 (personenbezogen) von D-TRUST, SwissSign und Sectigo abgerufen und über UPONU erworben werden.

Durch die AD/LDAP und Microsoft Entra ID Integration wird der Bezug von Zertifikaten für Benutzer vollständig automatisierbar, einschließlich der Beantragung, Verlängerung und umfangreichen Reportingfunktionen.

Zudem wird die Gültigkeit öffentlicher Schlüssel geprüft. Der Status kann sowohl dem Anwender als auch der Gegenstelle per E-Mail mitgeteilt werden.

Integration in den Mailflow via SMTP (Integration als SaaS oder On-Premises möglich)



☰

Demo GmbH

Andreas Blumberg

Avatar

Dashboard

Gateway

Portal

Publickeys

Add-Ins

Formulare

Workflow

Schlüsselverwaltung

Autocert

Automationen

Trustcenter

Interne S/MIME-CA

Interne PGP-CA

Interne Datenquelle

Offene Anfragen

Konfiguration

SMTP-Konfiguration

Logs

PDF-Passwörter

Nutzungsberichte

Warteschlange

Trustcenter

Tabelle der eingerichteten Trustcenter-Zugänge.

Erstellen

Ansehen

Löschen

Kopieren

Zertifikat beantragen

Automatismus aktivieren

Automatismus deaktivieren

Standard

Name

Automatismus

	Name	Typ	Automatismus
☐	Telekom	telekom	⊘
☐	Test-PGP	Interne PKI	⊘
☐	Test-Trustcenter	Interne PKI	⊘

Zeilen pro Seite

25

1-3 von 3

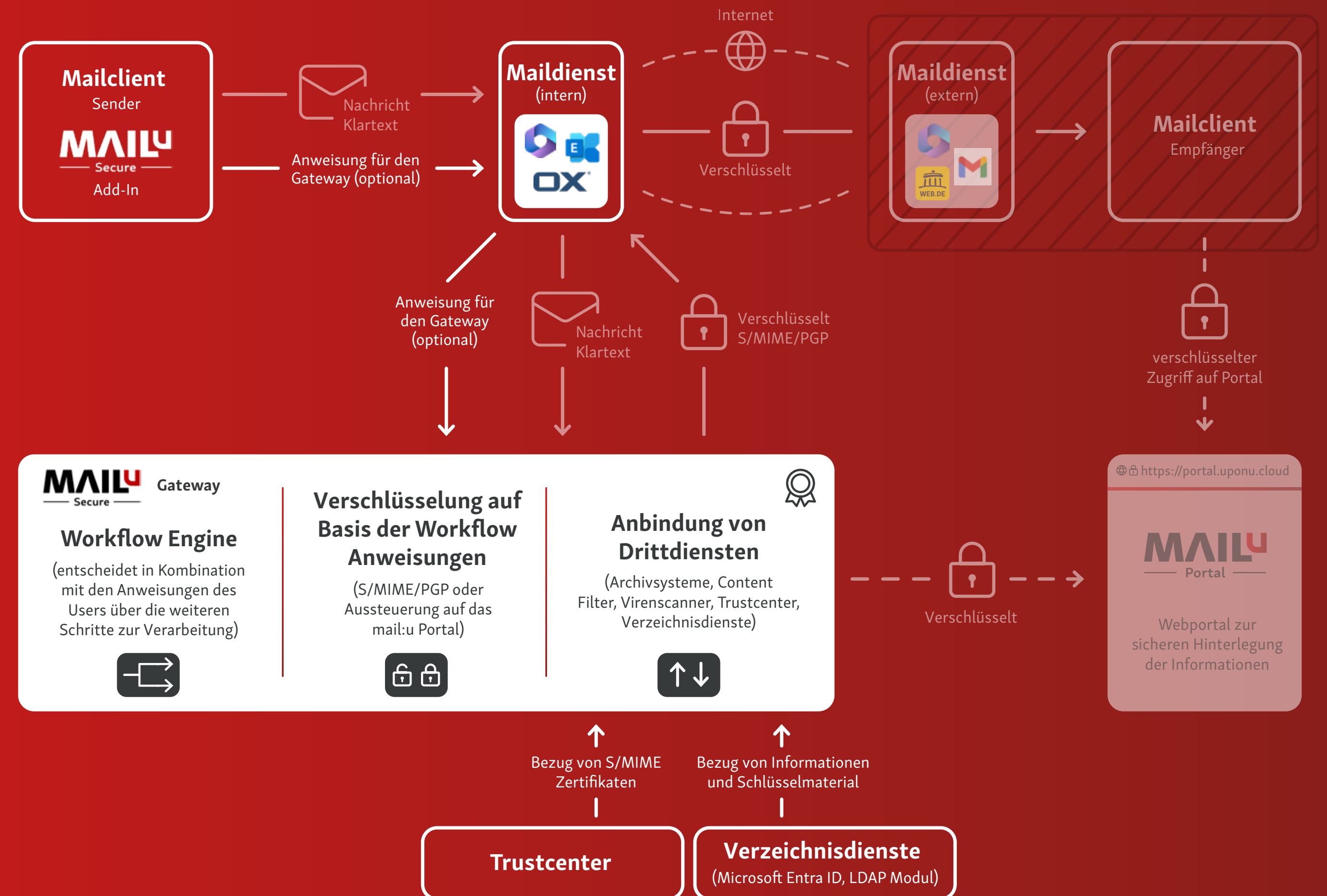
Outlook Add-Ins

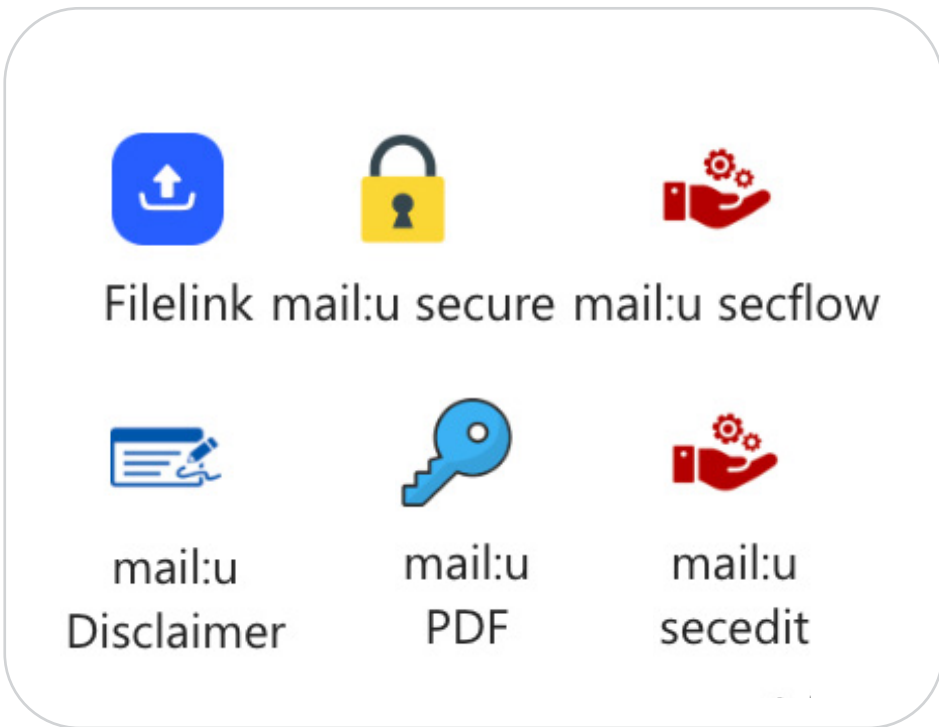
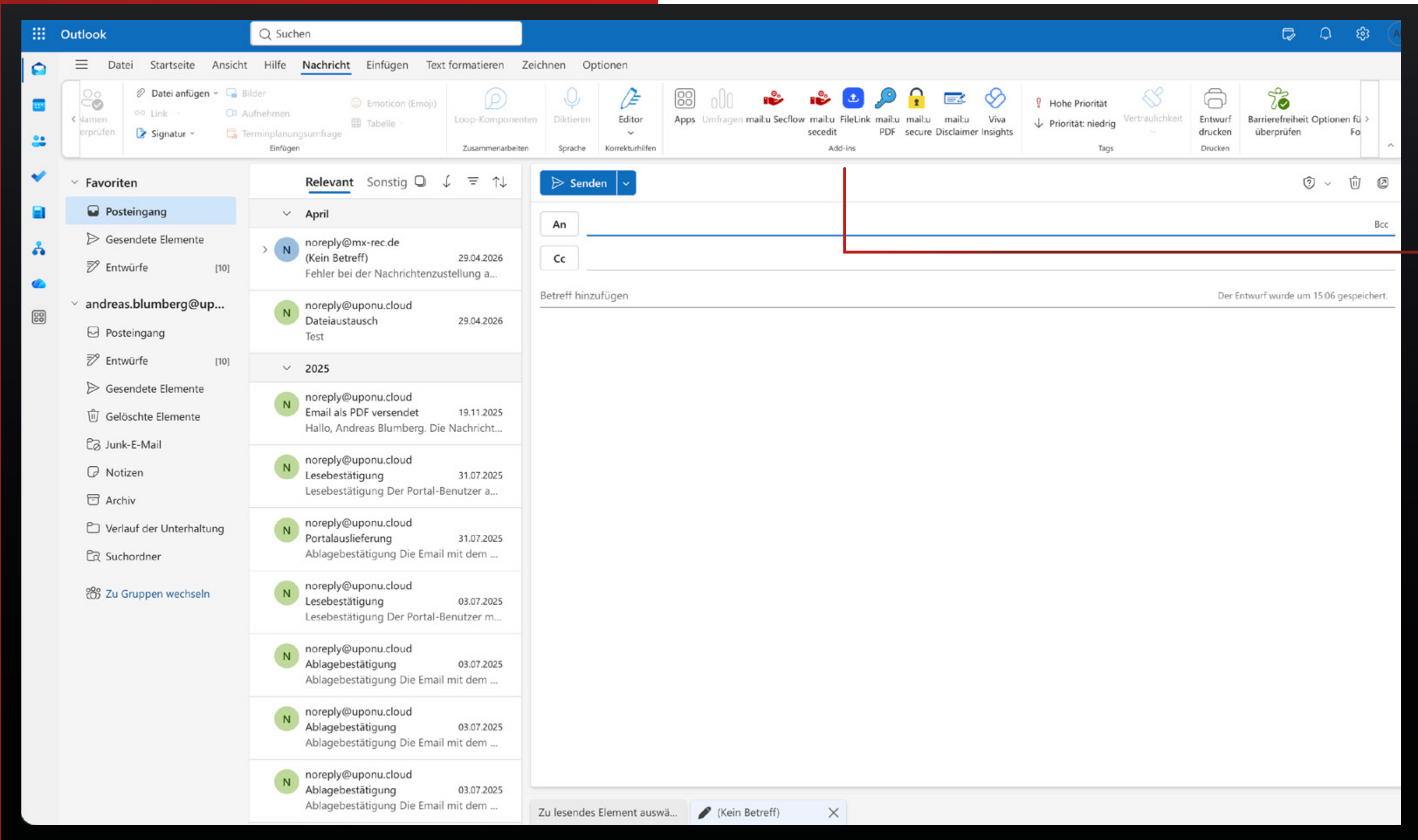
Ein weiteres Werkzeug zur Optimierung von Geschäftsprozessen. Die **mail:u Secure** Client Integration in Outlook ermöglicht es Unternehmen, ihre Prozesse durch diese datenschutzkonforme Lösung zunehmend zu digitalisieren.

Mit dem speziellen Web-Add-In, das in allen unterstützten Office-Versionen sowie in Office 365 und Office Online verwendet werden kann, können Benutzer in ihrer täglichen Arbeit ad hoc Entscheidungen zur sicheren Datenübertragung treffen. Die Outlook-Schaltflächen sind individuell konfigurierbar, sodass Anwender E-Mails klassifizieren und deren Bearbeitung auslösen können. Diese Befehle werden

an das **mail:u Secure** Gateway gesendet, wo sie ausgewertet und in den Workflow integriert werden. Dadurch können alle Standards der Verschlüsselung (wie S/MIME oder Portal) und Signaturen aktiviert werden, was die Vertrauenswürdigkeit und Vertraulichkeit bei der Übertragung geschäftsrelevanter und personenbezogener Daten gewährleistet. Die Lösung lässt sich an die spezifischen Bedürfnisse jeder Fachabteilung anpassen, sodass Entscheidungen entweder direkt von den Anwendern oder übergeordnet zentral getroffen werden können.

Integration in den Mailflow via SMTP (Integration als SaaS oder On-Premises möglich)





mail:u Portal

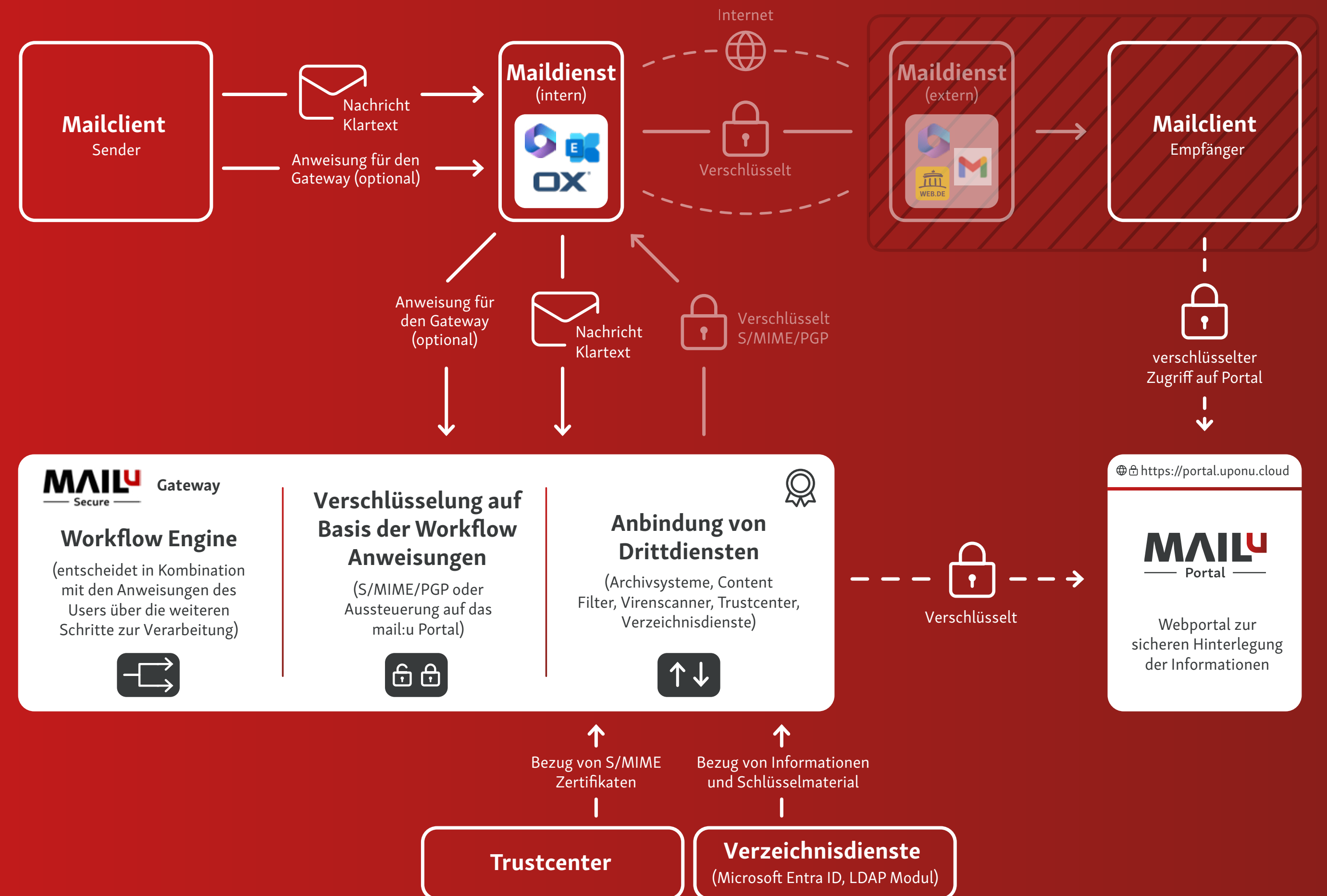
Das **mail:u Secure** Portal stellt eine individuell gestaltbare Kommunikationsplattform dar. Hierbei werden dem Empfänger E-Mails inklusive Anlagen (beispielsweise große und abzusichernde/sensible Dokumente) über unser Webportal zur Verfügung gestellt. Dies geschieht selbstverständlich verschlüsselt und bleibt beim Zugriff auf die individuellen Postfächer, die dabei eröffnet werden, sicher.

Über diesem Weg erfolgen ebenso Antworten und eigene E-Mails Richtung festgelegter Domänen, die dem Adressaten eröffnet werden. Die Lösung wird den höchsten Sicherheitsanforderungen gerecht und bietet auch in großen Umgebungen ein sehr einfaches Onboarding für externe Kommunikationspartner, u. a. mit einer 2 Faktor Authentifizierung.

Diese Alternative dient der Erweiterung jeder gesicherten Unternehmens- oder Behördenkommunikation – vor allem für Adressaten, die keinen öffentlichen Schlüssel zur Verschlüsselung anbieten können, also weder S/MIME noch PGP verwenden. Typischerweise sind dies Privatpersonen, die sich mit Ihren Anbietern im Versicherungs- oder Bankenbereich (u.v.m.) austauschen möchten, womit der wesentliche Anwendungsbereich deutlich wird.

Das **mail:u Portal** kann dafür auf jede Corporate Identity angepasst werden.

Integration in den Mailflow via SMTP (Integration als SaaS oder On-Premises möglich)



☰ Demo GmbH

nutzer@example.com

Neue Nachricht

Posteingang

Postausgang



☐ Alle auswählen



Andreas Blumberg
Demo Nachricht - Sichere ...

06.07.2026
15:58

Demo Nachricht - Sichere Zustellung mittels Portalablage

↩ Antwort

↓ EML

PDF PDF

Datum 06.07.2026 15:58

Von: Andreas Blumberg <andreas.blumberg@uponu.cloud>

An: Beispielnutzer <nutzer@example.com> iu.com>

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Tel +49 271 222958-0

Fax +49 271 222958-90

Ort UPONU Solutions GmbH

Spandauer Straße 32, 57072 Siegen



GF: Jan Mußmann, Marcel Link · HRB 14043 Registergericht Siegen · USt-IdNr. DE400208218

Diese E-Mail enthält vertrauliche und/oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese Mail. Das unerlaubte Kopieren sowie die unbefugte Weitergabe dieser E-Mail sind nicht gestattet.

E-Mail

1

Mailbox Speicher

26.85 KB

Benutzer aktivieren



andreas.blumberg@uponu.com

Bestätige deine E-Mail-Adresse mit dem unten stehenden Code und lege dein Passwort fest.

Code

ST8N3A



Neues Passwort



Passwort bestätigen



✗ Muss mindestens 8 Zeichen lang sein.

✗ Muss einen Großbuchstaben enthalten.

✗ Muss eine Zahl enthalten.

✗ Passwortbestätigung stimmt überein.

✓ Muss weniger als 70 Zeichen lang sein.

✗ Muss einen Kleinbuchstaben enthalten.

✗ Muss ein Symbol enthalten.

Code erneut senden

Weiter

Benutzeraktivierung

mail:u FileLink – sichere Bereitstellung großer Dateien

Die Übermittlung großer oder sensibler Dateien per E-Mail bringt zahlreiche Herausforderungen mit sich – etwa Größenbeschränkungen, unsichere Empfängerinfrastrukturen oder Datenschutzvorgaben.

Mit dem Modul FileLink bietet **mail:u Secure** eine Lösung, die den Versand durch Aussteuerung der Anlage ersetzt und stattdessen einen Link der sicher zur Verfügung gestellten Datei bereitstellt.

Die Aussteuerung erfolgt entweder manuell durch das Outlook Add-in oder automatisch über die zentrale Workflow Engine. Dabei können Bedingungen wie Dateityp, -größe oder Empfängerdomäne berücksichtigt werden.

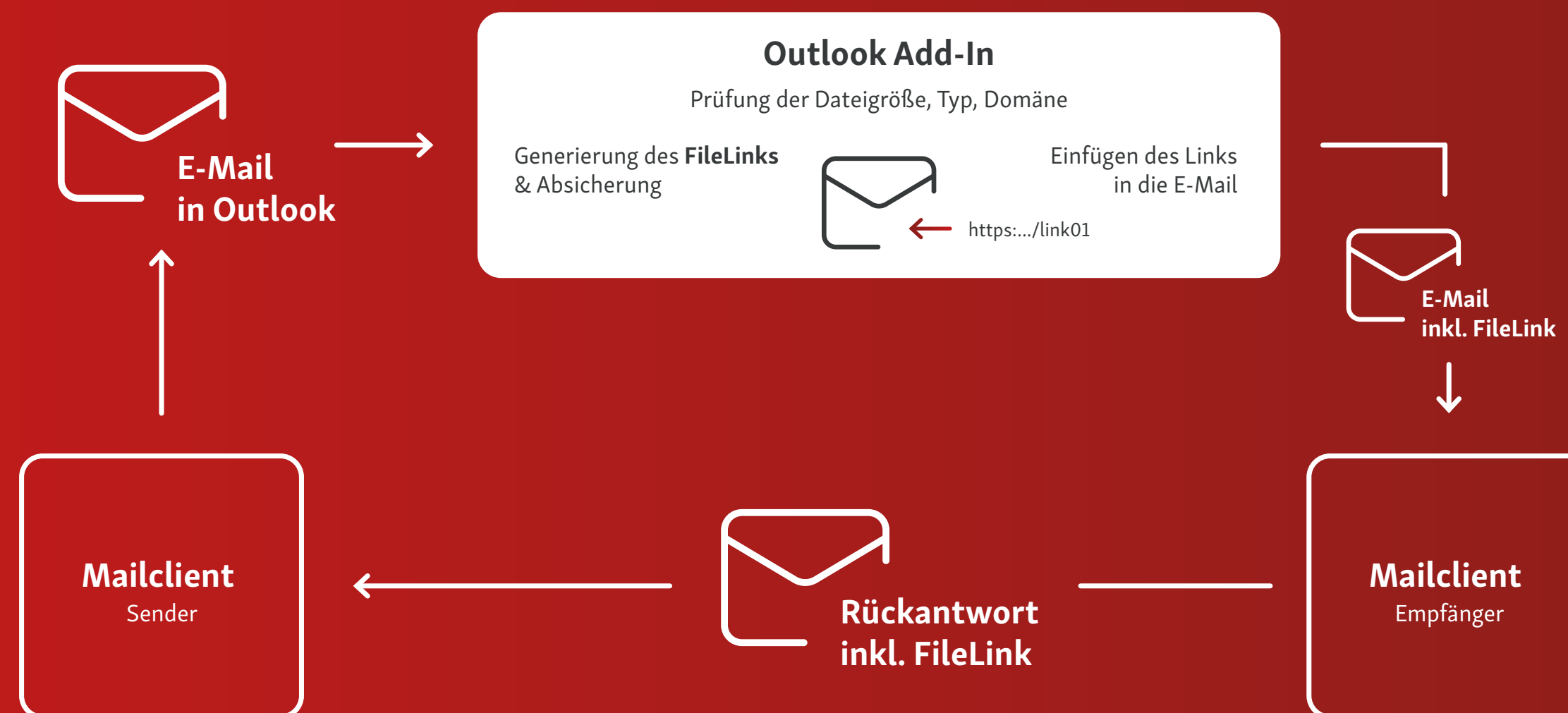
Der Zugriff auf den FileLink lässt sich über verschiedene Mechanismen absichern:

- Kennwortschutz (frei definierbar oder automatisch vergeben)
- optional Authentifizierung über Benutzerkonto mit Zweifaktor-Verfahren (z. B. TOTP oder Passkey).

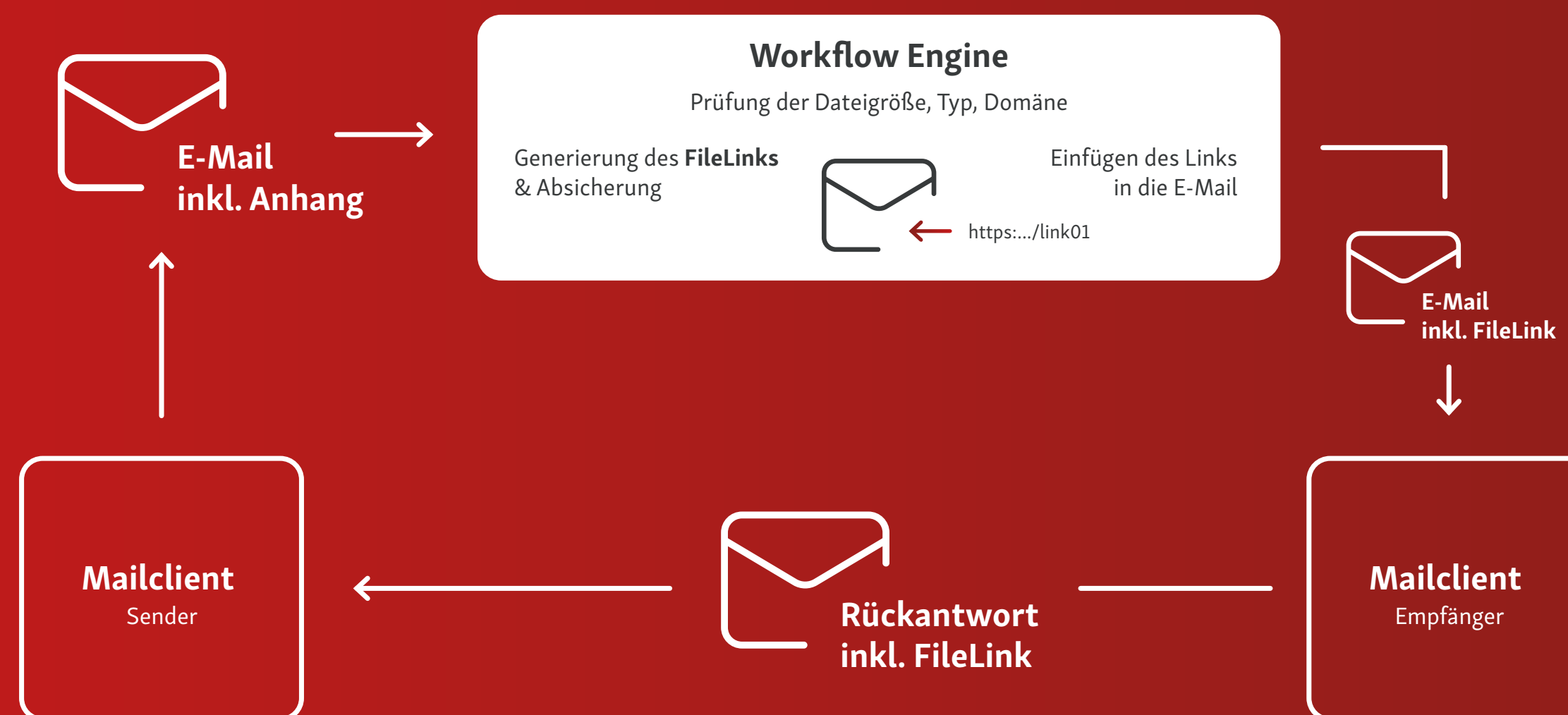
FileLink ist Teil des Webportal-Dienstes, der verschlüsselt über HTTPS in einer Public-DMZ bereitgestellt wird. Der Link kann zusätzlich eine Rückkanalfunktion enthalten.

Die Bereitstellung kann automatisiert durch die Workflow Engine erfolgen – z. B. bei Überschreiten von Dateigrößen oder durch explizite Steuerbefehle (Header/Betreff, Outlook Add-In). Daten können direkt über das Portal hochgeladen oder durch das Gateway angesteuert werden.

Manueller Vorgang über Outlook Add-In



Automatischer Vorgang über Workflow Engine



Nachricht

Einfügen

Text formatieren

Zeichnen

Optionen

12

Font Face

Font Size

Font Color

Text Color

Text Background Color

Text Alignment

Text Indentation

Text Orientation

Text Direction

Text Language

Text Spell Check

Text Grammar Check

Text Auto Correct

Text Auto Format

Text Auto Link

Text Auto Save

Text Auto Sync

Text Auto Backup

Text Auto Restore

Text Auto Recover

Text Auto Undo

Text Auto Redo

Text Auto Save As

Text Auto Save With

Text Auto Save When

Text Auto Save Where

Text Auto Save How

Text Auto Save Why

Text Auto Save What

Text Auto Save Who

Text Auto Save When

Text Auto Save Where

Text Auto Save How

Text Auto Save Why

Text Auto Save What

Text Auto Save Who

Formatvorlagen

Formatvorlagen

Datei anfügen

Link

Signatur

Aufnehmen

Bilder

Emoticon (Emoji)

Tabelle

Apps

Umfragen

Filelink

mail:u

secure

mail:u

secflow

Viva Insights

Basistext

Formatvorlagen

Einfügen

Add-ins

Senden

?

An

Marcel Link

Marcel Link (Intern)

Bcc

Cc

siehe Anhang

Der Entwurf wurde um 11:41 gespeichert.

Hallo Marcel,

anbei die versprochene Datei.

[extract.csv](#)

Viele Grüße

Filelink

Lade Dateien hoch und kopiere die generierten Download-Links zu diesen Dateien in den E-Mail Entwurf.

Lege Dateien per Drag 'n' drop hier ab oder klicke hier, um Dateien auszuwählen

Ausgewählte Dateien

extract.csv - 14.41 MiB

Verfügbarkeit der Dateien (in h)

48

Hochladen

Downloadlinks

extract.csv

<https://securefile.uponu.cloud/filelink/public/30>

Links in E-Mail kopieren

Beispiel:

Eine Nachricht mit einer .zip-Anlage von 45 MB wird versendet. Das Regelwerk erkennt Dateityp und Größe, wandelt die Anlage automatisch in einen FileLink um und stellt dem Empfänger einen sicheren Link zur Verfügung. Die ursprüngliche E-Mail enthält nur einen Hinweis und den Zugriffspfad.

SECFLOW – Regelvalidierung vor dem Versand

Mit dem Modul SECFLOW lassen sich Nachrichten bereits vor dem Versand auf ihre Verarbeitung im Gateway prüfen. Diese Vorschaufunktion steht über das Outlook Add-in (lokal und online) zur Verfügung und simuliert den gewählten Versandweg anhand des aktuellen Regelwerks.

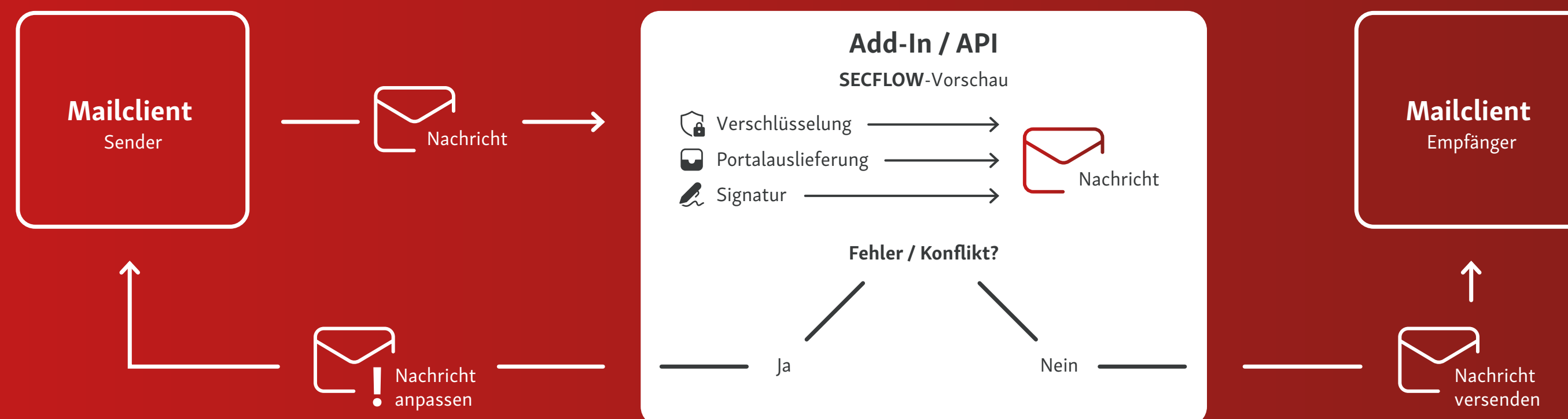
Dabei wird angezeigt:

- ob die Verschlüsselung mittels eines vorhandenen öffentlichen Schlüssels/Zertifikats erfolgen kann
- ob das Signieren erfolgen kann
- ob eine Aussteuerung (z. B. in FileLink, Portal oder PDF) erfolgt
- ob zusätzliche Informationen an Empfänger oder Absender übermittelt werden

SECFLOW trägt maßgeblich zur Transparenz und Sicherheit im täglichen Versand bei. Fehlerhafte oder nicht erwünschte Verarbeitungen lassen sich vorab erkennen und verhindern. Die Validierung berücksichtigt Empfänger, Dateitypen, Steuerbefehle und alle weiteren Schritte der Workflow Engine.

Die Integration erfolgt API-basiert über Microsoft 365 – unabhängig vom klassischen SMTP-Fluss. Dadurch sind clientseitige Rückmeldungen in Echtzeit möglich, bevor die Nachricht das System verlässt. Die API kann ebenfalls aus beliebigen Dritt Systemen angesprochen werden.

Vorschau und Validierung mit SECFLOW



Mailu

Secure

SECFLOW – Regelvalidierung
vor dem Versand

UPONU

Datei

Nachricht

Einfügen

Text formatieren

Zeichnen

Optionen

Einfügen

Zwischenablage

Aptos

12

aA

Ab

B

I

U

S

Y

X

X

99

=

=

=

=

=

Adressbuch

Namen überprüfen

Namen

Datei anfügen

Link

Signatur

Bilder

Aufnehmen

Terminplanungsumfrage

Einfügen

Emoticon (Emoji)

Tabelle

Loop-Komponenten

Zusammenarbeiten

Diktieren

Sprache

Editor

Korrektur

Senden

An

Andreas Blumberg

max@uponu.com

klaus@uponu.com

info@uponu.com

Bcc

Cc

Betreff hinzufügen

Der Entwurf wurde um 16:15 gespeichert.

Apps

mail:u secflow

Mailfluss prüfen

Suche...

Empfänger

max@uponu.com

klaus@uponu.com

info@uponu.com

Hilfe

mail:u secedit

Überprüfe die Mailverschlüsselung für jeden Empfänger

Mail senden

Absender: Andreas Blumberg <andreas.blumberg@uponu.cloud>

Empfänger

max@uponu.com

klaus@uponu.com

info@uponu.com

Verschlüsseln

Portal

Signieren

TLS

PDF

PDF-Passwort

Aktion ausführen

Änderungen verwerfen

COMPANY NAME

Beispiel:
Ein Mitarbeiter möchte ein Excel-Dokument an eine externe Adresse senden. Über SECFLOW erkennt er, dass der Anhang gemäß Workflow in einen FileLink überführt wird. Zusätzlich wird ein Vermerk an den Empfänger gesendet. Die Information ermöglicht es, vor dem Versand eine bewusste Entscheidung zu treffen.

16 | E-Mail-Verschlüsselung mit S/MIME & PGP

PDF-Verschlüsselung – Alternativer Versandweg für sensible Inhalte

Nicht jeder Empfänger kann Nachrichten per S/MIME oder PGP entschlüsseln. Für diese Fälle bietet **mail:u Secure** die Möglichkeit, Nachrichten und Anlagen vollständig in ein kennwortgeschütztes PDF-Dokument zu überführen.

Die Umwandlung erfolgt automatisiert durch die Workflow Engine– abhängig von:

- Dateityp oder -größe,
- Empfängertyp oder -domäne,
- Inhalten im Betreff oder Header,
- expliziten Steuerbefehlen über Add-in oder Drittanwendung

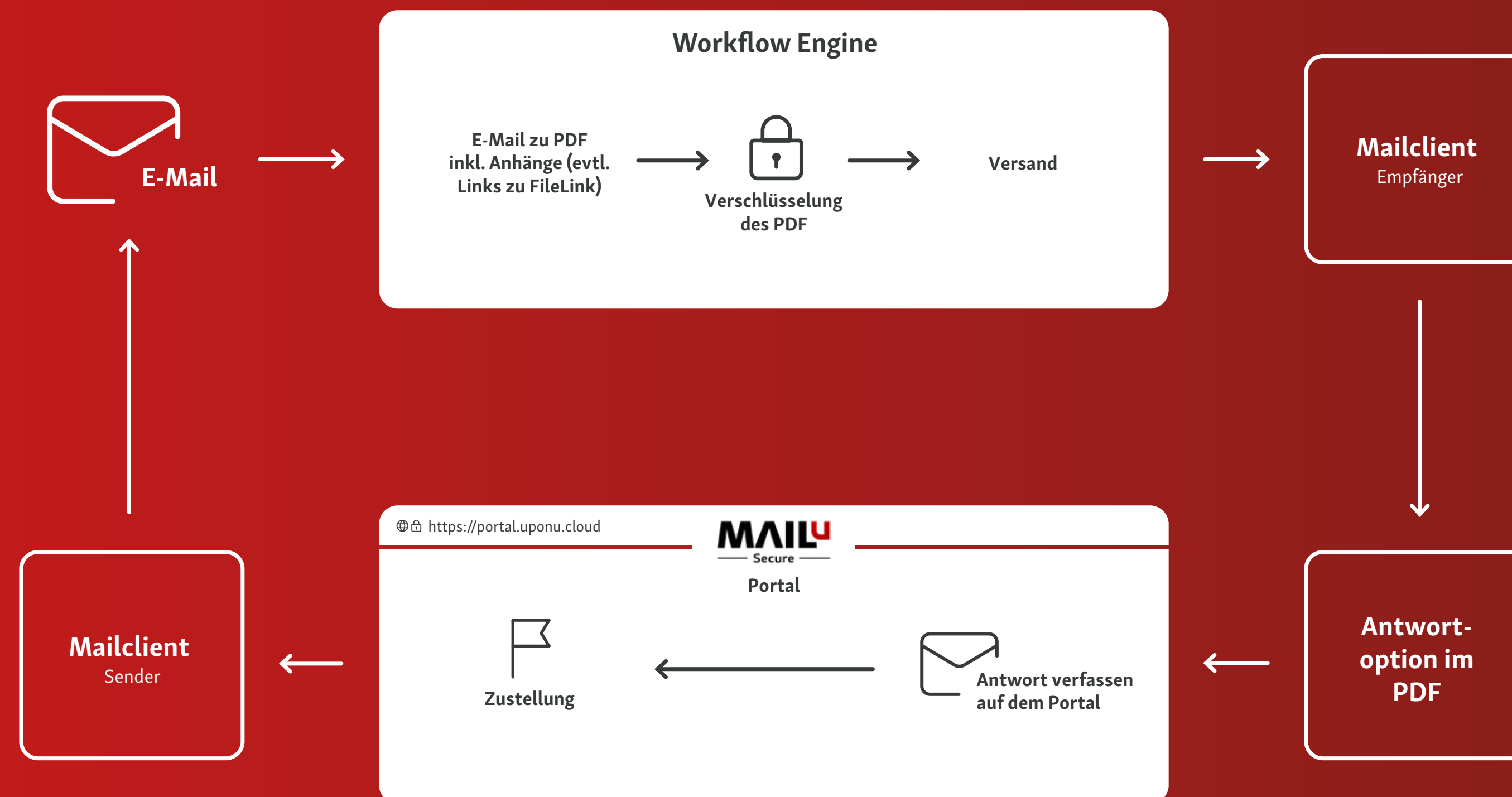
Das Kennwort kann:

- vom Absender gesetzt,
- aus einer internen Datenquelle bezogen,
- oder automatisch generiert werden

Die PDF-Datei wird mit allen Inhalten und Anhängen erzeugt und verschlüsselt versendet. Eine Antwortfunktion kann optional integriert werden, um Rückmeldungen sicher zu ermöglichen.

Diese Methode ermöglicht DSGVO-konformen Versand – auch an Empfänger ohne eigenes Schlüsselsystem.

PDF-Verschlüsselung inkl. Anlagen



☰

Demo GmbH

Startseite

Schlüsselverwaltung

Workflow

Regelset

Gruppen

Schlüsselquellen

Revisionen

Testmodus

Audit

Autocert

Konfiguration

Logs

Workflow

Archivierte Workflow-Logs

Autocert

CRL Logs

Portal

Benutzer

E-Mails

Regelset

Aktueller Arbeitsstand der Regeln.

+ Erstellen

Kopieren

Bearbeiten

Nach oben

Nach unten

☐	Aktiviert	Name	Eingabetyp
☐	✓	internal recipients	Entschlüsselt und verschlüsselt
☐	✓	sign and encrypt - S/MIME	Original
☐	✓	sign and encrypt - PGP	Original
☐	✓	encrypt - S/MIME	Original
☐	✓	encrypt - PGP	Original
☐	✓	sign - S/MIME	Original
☐	✓	sign - PGP	Original
☐	✓	untouched	Original
☐	✓	portal use	Original
☐	✓	portal create	Original
☐	✓	pdf	Original

Bearbeiten

×

Allgemein

Bedingungen

Aktionen

Erweitert

Header verändern

Operation

Ändern

In vorhandenen Headern suchen, welche geändert werden sollen

Key

Gleich

Subject

Wert

Regex

`^(.*?)(?:\s*sicher\s*)(?:\s*secure)(?:\s*pdf))(.*)$`

Ersatzmodus

Festgelegt

Schlüsselwert, welcher bestehenden Schlüsselwert ersetzen soll

Ersetzen mit

`$1$2`

PDF versenden

Zugangsdaten

☐ Passwort aus Header extrahieren

Benutzerpasswort

Wird kein Benutzerpasswort angegeben, wird ein zufällig generiertes verwendet.

Adminpasswort

Wird kein Adminpasswort angegeben, wird das Benutzerpasswort verwendet.

Passwortnutzung

Laden & Speichern

Beispiel:
Ein Versicherer übermittelt vertrauliche Vertragsdaten an einen Privatkunden. Da keine S/MIME- oder PGP-Zertifikate vorliegen, wird die Nachricht automatisch als verschlüsseltes PDF-Dokument erzeugt und übermittelt. Der Kunde öffnet dieses mit einem separat kommunizierten Kennwort.

Kontakt



Thomas Paar

thomas.paar@uponu.com



Andreas Diekmannshenke

andreas.diekmannshenke@uponu.com



Thomas Walgenbach

thomas.walgenbach@uponu.com

UPONU Solutions GmbH
Spandauer Str. 32
57072 Siegen, Germany

Echt performant.

[Zur Website](#)