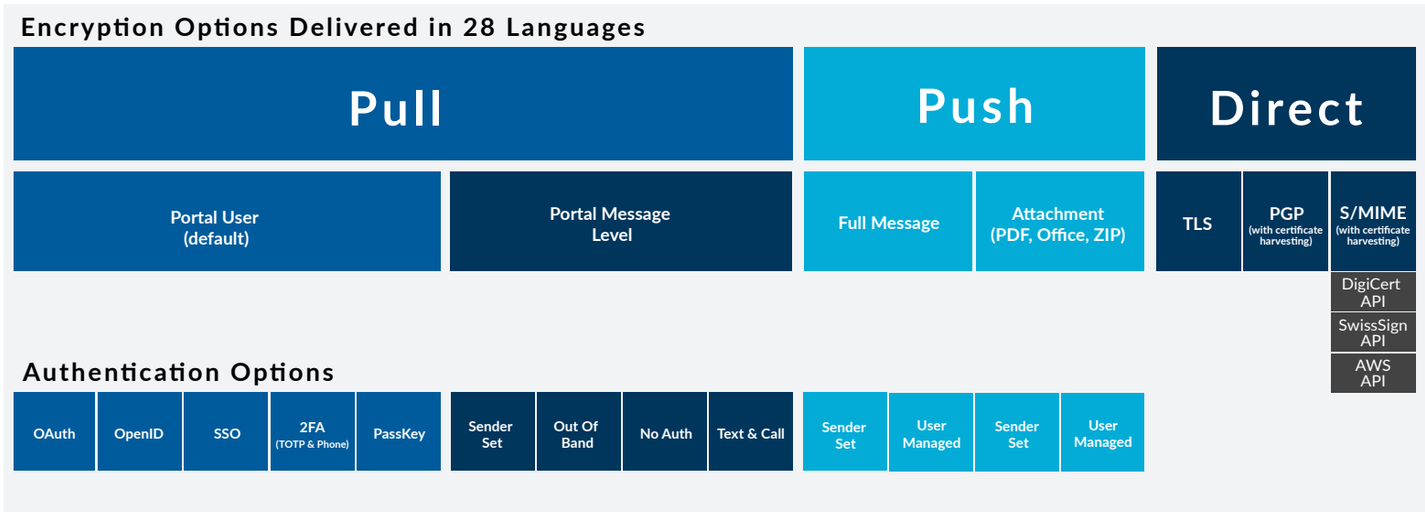
ECHOWORX™

TECHNOLOGIEBERICHT

Eine Plattform. Jeder Empfänger. Jederzeit sicher.

Ihr Leitfaden zu den Echoworx-Zustellungsoptionen — und der intelligentere Weg, jede Nachricht zu schützen, die Ihr Unternehmen verlässt

Jeden Tag sendet Ihre Organisation sensible Informationen an Kunden, Partner, Regulierungsbehörden und Kollegen, die alle unterschiedlich arbeiten und eine unterschiedliche Erfahrung erwarten. Echoworx befindet sich an der Grenze Ihrer Umgebung, bewertet jede ausgehende Nachricht anhand Ihrer Richtlinie und leitet sie automatisch über die richtige Zustellungsmethode weiter. Die folgenden Seiten führen Sie durch jede Option der Reihe nach, damit Sie die richtige Methode dem richtigen Empfänger mit Zuversicht zuordnen können.



Web-Portal

Wenn sensible Informationen einen kontrollierten, nachverfolgbaren Speicherort benötigen, liefert das Sichere Web-Portal diese, ohne die Passwortmüdigkeit, die Empfänger frustriert und die IT mit Reset-Tickets überflutet. Empfänger authentifizieren sich mit Anmeldedaten, denen sie bereits vertrauen, Absender und Administratoren behalten die vollständige Sichtbarkeit über jede Nachricht, und die Governance begleitet jede Kommunikation von der ersten Zustellung bis zur Antwort und zum Rückruf.

Hauptfunktionen

- **Föderierte Anmeldung und OAuth 2.0:** Vollständige OAuth 2.0-Unterstützung für Microsoft 365, Gmail, Hotmail, Facebook, LinkedIn, Salesforce und weitere Anbieter. Empfänger melden sich mit Anmeldedaten an, die sie bereits besitzen — keine neuen Konten, keine neuen Passwörter.
- **OpenID Connect:** Organisationen, die OpenID zur Authentifizierung unterstützen, ermöglichen es Empfängern, sich mit aktuellen Anmeldedaten anzumelden und die Erstellung neuer Konten vollständig zu umgehen.
  SSO-Integration: Die Webdienste-Integration ermöglicht die automatische Anmeldung über ein bestehendes Unternehmensportal und bettet den sicheren Nachrichtenzugriff nahtlos in die vertraute Umgebung des Empfängers ein.
- **Modus ohne Authentifizierung:** Bei risikoarmen Kommunikationen greifen Empfänger über einen direkten Link ohne erforderliche Anmeldung auf Nachrichten zu, während die Nachrichtenaktivität und das sichere eingehende Antwortverfolgung aktiv bleiben.
- **Vom Absender festgelegtes Passwort:** Absender definieren eine gemeinsame Passphrase mit einem optionalen Hinweis über das M365 Outlook Add-On, die dem Empfänger über einen separaten Kanal mitgeteilt wird. Empfänger greifen auf die Nachricht zu, ohne sich zu registrieren.
- **Textnachrichtenverifizierung:** Absender geben über das M365 Outlook Add-On eine Empfänger-Telefonnummer ein, und ein Einmalcode wird zur Portal-Authentifizierung an das Gerät des Empfängers gesendet.
- **Sprachanrufverifizierung für die 2-Schritt-Verifizierung:** Für Empfänger, die keine Textnachricht empfangen können — sei es aufgrund von Standort, Konnektivität oder Zugänglichkeitsbedürfnissen — bietet die Sprachanrufzustellung eine zuverlässige Alternative und hält den Zugang ohne Verzögerungen oder Beschwerden aufrecht.
- **Passkeys (passwortloser Zugang):** Die biometrische Authentifizierung über einen Fingerabdruckscanner oder die Biometrie des Geräts ermöglicht einen sicheren, einstufigen Portalzugang mit einer PIN oder biometrischer automatischer Ausfüllung.
- **Antwort-an-alle-Kontrollen:** Beschränkt das Portal-Antwort-an-alle auf interne Abonnenten und entfernt automatisch nicht erkannte Domänen aus Entwürfen, schließt einen häufigen Weg zur versehentlichen Datenoffenlegung und stärkt Ihre DLP-Richtlinie.
- **Sichere Nachrichtenweiterleitung:** Beschränkt registrierte Empfänger auf die Weiterleitung von Nachrichten nur innerhalb erlaubter Domänen und hält die Zusammenarbeit in einem sicheren, vollständig auditierbaren Kanal.
- **Hinzufügen von Portal-Empfängern:** Erlaubt registrierten Empfängern, bei Antwort- oder Weiterleitungsaktionen Teilnehmer hinzuzufügen, innerhalb derselben richtliniengesteuerten Umgebung, sodass echte Teamarbeit Ihre definierten Grenzen nie verlässt.
- **Pro-Empfänger-Benachrichtigungskontrollen:** Ermöglicht es Empfängern, sich von Erinnerungs- und Abschlussbenachrichtigungen abzumelden, und reduziert so die Posteingangsreibung, ohne die Austauschintegrität zu beeinträchtigen.
- **Barrierefreiheit:** Die erweiterte WCAG-Konformität im gesamten Empfängerportal erfüllt den Barrierefreiheitsstandard, der nun in Unternehmens-Ausschreibungen und Compliance-Audits üblich ist.

Weitere Funktionen

- Geräteunabhängige Zustellung auf allen wichtigen Plattformen und Formfaktoren, wo immer Ihre Empfänger arbeiten.
- Umfangreiche Branding-Kontrollen für kundenseitige Seiten, verschlüsselte Nachrichten und Benachrichtigungen, damit Empfänger die Quelle stets erkennen.
- Lokalisierungsunterstützung in 28 Sprachen.
- Alle Nachrichten werden verschlüsselt im Ruhezustand in der Echoworx-Cloud gespeichert, mit standardmäßigen Aufbewahrungsfristen von 30, 60 oder 90 Tagen und auf Anfrage verfügbaren verlängerten Laufzeiten.
- Lokaler Nachrichtenexport in Outlook- und verschlüsselten PDF-Formaten für die langfristige Empfängeraufbewahrung.
- Passwortverwaltung für Absender und Empfänger verfügbar.
- Sichere Antwort- und Lesebestätigungsfunktionalität für laufende, auditierbare Austausche.
- Vollständige Nachrichtenaudit- und Rückruffähigkeiten für Absender und Administratoren.
- Barrierefreiheit: Die erweiterte WCAG-Konformität im gesamten Empfängerportal erfüllt den Barrierefreiheitsstandard, der nun in Unternehmens-Ausschreibungen und Compliance-Audits üblich ist.

Technischer Hinweis

Nachrichten werden online über das Portal abgerufen und werden nicht dauerhaft auf dem lokalen Gerät des Empfängers gespeichert. Empfänger, die eine Kopie langfristig aufbewahren müssen, sollten Nachrichten beim Empfang speichern oder exportieren.

Was das für Sie bedeutet: Ihre Empfänger melden sich mit Anmeldedaten an, denen sie bereits vertrauen, und erreichen ihre Nachrichten in Sekunden — auf jedem Gerät, in jeder Sprache, ohne neue Konten erstellen zu müssen. Ihre Absender behalten die volle Kontrolle darüber, wer jede Nachricht liest, beantwortet und weiterleitet. Und Ihre Organisation erfüllt die Governance-, Barrierefreiheits- und Compliance-Standards, die Regulierungsbehörden und Beschaffungsteams heute als Standard erwarten.

Verschlüsseltes PDF

Manchmal ist der schnellste Weg, sensible Informationen zu schützen, sie als gesperrtes Dokument zu senden, nicht als Portallink. Die verschlüsselte PDF-Zustellung sichert sowohl den Nachrichtentext als auch seine Anhänge mithilfe der vertrauenswürdigen Technologien Secure PDF, Office 365 und ZIP. Die Empfänger erhalten eine vertraute Datei, die sie öffnen, speichern und behalten können, während Ihre Organisation den Inhalt von dem Moment an schützt, in dem er Ihr Gateway verlässt.

Hauptfunktionen

- **Zugang per Verifizierungscode:** Stellen Sie sich vor, Sie senden ein sicheres Dokument an einen nicht-technischen Empfänger mit einem engen Zeitplan. Die Registrierung wird zum Engpass. Diese Dokumentenverschlüsselungsmethode beseitigt ihn vollständig. Der Absender teilt einen spontan generierten Code über einen separaten Kanal, wie einen kurzen Telefonanruf, und der Empfänger verwendet ihn, um das verschlüsselte PDF oder die Anhänge sofort zu öffnen. Keine Registrierung, keine Passwörter, keine Verzögerungen — nur Sicherheit, die im Tempo des Gesprächs voranschreitet.
- **Selbst-Registrierung:** Empfänger legen ihr eigenes Passwort über eine einzige einmalige Eingabeaufforderung fest, sodass der erste Zugriff einfach bleibt.
- **Passwortverwaltung:** Empfänger stellen ihr Passwort wieder her oder aktualisieren es über einen Self-Service-Link, ohne Ihren Helpdesk anzurufen.
- **Vom Absender festgelegte Passwörter:** Absender erstellen eine gemeinsame Passphrase und übermitteln sie dem Empfänger außerhalb des Kanals, wodurch beide Seiten die Kontrolle über den Zugriff erhalten.
- **Nahtlose Anzeige:** Verschlüsselte PDFs und Office-Dokumente öffnen sich direkt in Gmail oder Outlook für das Web, ohne dass etwas Neues heruntergeladen oder installiert werden muss.

Zusätzliche Funktionen

- Flexible Zustellung auf jedem Gerät, wo auch immer Ihre Empfänger arbeiten.
- Anpassbares Branding für Nachrichten und Benachrichtigungen, damit Empfänger die Quelle stets erkennen.
- Unterstützung für 28 Sprachen.
- Offline-Zugriff mit Verschlüsselung im Ruhezustand, sodass Empfänger sichere Kopien so lange aufbewahren können, wie sie diese benötigen.
- Sichere Antworten mit Empfängerkopien, die das Gespräch in beide Richtungen geschützt halten.

Technischer Hinweis

Die Push-Verschlüsselung liefert jede Nachricht direkt an den Empfänger für sofortigen Zugriff. Da das Dokument direkt in seinem Posteingang landet, können auf diese Weise gesendete Nachrichten nicht zurückgerufen werden.

Was das für Sie bedeutet: Ihre Empfänger erhalten ein einfaches, vertrautes Dokument, das sie auf jedem Gerät öffnen können, Ihr Team kann auch nicht-technische Kontakte in Sekunden mit Verifizierungscodes erreichen, und Ihre sensiblen Inhalte bleiben von der Sendung bis zum Öffnen geschützt.

Verschlüsselter Anhang

Wenn vertrauliche Informationen schnell übermittelt werden müssen, ist der sicherste Weg manchmal der einfachste: ein gesperrter Anhang, der direkt im Posteingang des Empfängers landet. Die Zustellung per verschlüsseltem Anhang schützt Ihre Dokumente, während der Nachrichtentext im Klartext verbleibt, sodass Empfänger eine vertraute E-Mail mit einer sicheren Datei erhalten, die sie öffnen, speichern und aufbewahren können. Es ist ideal für dokumentenintensive Arbeiten mit hohem Volumen, wie die Verarbeitung elektronischer Massenkontoauszüge, bei denen Geschwindigkeit und Sicherheit Hand in Hand gehen müssen.

Hauptfunktionen

- **Zugang per Verifizierungscode:** Stellen Sie sich vor, Sie senden ein sicheres Dokument an einen nicht-technischen Empfänger mit engem Zeitplan. Der traditionelle Registrierungsschritt wird zum Engpass. Diese Verifizierungscode-Methode entfernt ihn vollständig. Der Absender teilt einen spontan generierten Code über einen separaten Kanal, wie einen kurzen Telefonanruf, und der Empfänger verwendet ihn, um den verschlüsselten Anhang sofort zu öffnen. Keine Registrierung, keine Passwörter, keine Verzögerungen. Sicherheit, die mit einem Gespräch Schritt hält, nicht mit einer Warteschlange für Papierkram.
- **Sprachanruf-Verifizierung für die 2-Schritt-Verifizierung:** Wenn ein Empfänger keine Textnachricht empfangen kann — aufgrund seines Wohnorts, eines Barrierefreiheitsbedarfs oder einfach einer Signallücke — bietet die Sprachanruf-Verifizierung für die 2-Schritt-Verifizierung eine zuverlässige Alternative. Der Zugang bleibt offen, Authentifizierungsverzögerungen werden reduziert und Empfängerbeschwerden folgen.
- **Native Verschlüsselung für PDF, Microsoft Office und ZIP:** Anhänge werden nativ verschlüsselt, wobei der ursprüngliche Name und die Eigenschaften jeder Datei erhalten bleiben, sodass Empfänger genau erkennen, was sie öffnen. Nahtlose Anzeige: Verschlüsselte PDFs und Office-Dokumente öffnen sich direkt in Outlook für Web und dem Gmail-Client, ohne dass etwas Neues heruntergeladen oder installiert werden muss.
- **Breite Dateiunterstützung:** Andere Anhangstypen werden in ein verschlüsseltes PDF- oder ZIP-Format gebündelt, sodass kein Dokument ungeschützt bleibt.
- **Selbstregistrierung:** Empfänger legen ihr eigenes Passwort über eine einmalige Eingabeaufforderung fest, was den erstmaligen Zugang vereinfacht.
- **Vom Absender festgelegte gemeinsame Passphrase:** Absender erstellen eine gemeinsame Passphrase und teilen sie dem Empfänger außerhalb des Übertragungswegs mit, wobei beide Seiten die Kontrolle über den Zugang behalten.
- **Angepasster, markenkonformer Nachrichtentext:** Kopf- und Fußzeilen können einen Link zur Passwortverwaltung oder einen dezenten Hinweis zur gemeinsamen Passphrase enthalten, sodass Empfänger immer wissen, dass sie am richtigen Ort sind.

Weitere Funktionen

- Lesen Sie sichere Dokumente überall, auf jedem Gerät, wo auch immer Ihre Empfänger arbeiten.
- Halten Sie den Nachrichtentext im Klartext, während nur die Anhänge verschlüsselt sind, sodass der übliche Kontext lesbar bleibt.
- Senden Sie mehrere verschlüsselte Anhänge in ihren ursprünglichen Formaten in einer einzigen E-Mail.
- Erreichen Sie ein globales Publikum mit mehrsprachiger Unterstützung in 28 Sprachen.
- Stellen Sie direkt im Posteingang des Empfängers zu, kein Portalbesuch erforderlich.
- Schützen Sie verschlüsselte Anhänge im Ruhezustand, sodass Dateien noch lange nach dem Eingang sicher bleiben.
- Wählen Sie flexible Passwortoptionen, die von Absendern oder Empfängern festgelegt werden, einschließlich Telefonverifizierung und Passkeys.
- Öffnen Sie sichere Dokumente offline, wann und wo auch immer Empfänger sie benötigen.

Technischer Hinweis

Echoworx empfiehlt ZIP-Software, die AES-256-Bit-Dateien öffnen kann, darunter WinZip, Secure ZIP, WinRAR und unser Favorit, 7-Zip. Bitte beachten Sie, dass Push-Verschlüsselung jede E-Mail sofort an den Empfänger zustellt, sodass auf diesem Weg gesendete Nachrichten von Echoworx nicht zurückgerufen werden können.

Was das für Sie bedeutet: Ihre Empfänger erhalten eine vertraute E-Mail mit einer sicheren Datei, die sie auf jedem Gerät öffnen können, Ihr Team kann auch nicht-technische Kontakte in Sekunden über Verifizierungscodes und die inklusive Sprachanruf-Verifizierung erreichen, und Ihre vertraulichen Dokumente bleiben vom Versand bis zum Öffnen geschützt.

TLS-Verschlüsselung mit Fallback

Manche Nachrichten müssen sich leise und sofort bewegen, ohne Passwörter, ohne Portale und ohne zusätzliche Schritte für alle Beteiligten. TLS-Verschlüsselung mit Fallback tut genau das: Sie verschlüsselt Ihre Nachrichten und Anhänge während der Übertragung und stellt sie direkt an den Empfänger zu. Wenn die Domain eines Empfängers TLS nicht unterstützen kann, lässt die Plattform eine Nachricht niemals ungeschützt. Sie wechselt automatisch auf einen anderen sicheren Kanal, sodass der Schutz konstant bleibt und die Zustellung mühelos bleibt..

Hauptfunktionen

- **TLS-Validierung in Echtzeit:** Die Plattform überprüft die Gültigkeit jeder TLS-Verbindung in Echtzeit, sodass jede Nachricht auf einen wirklich sicheren Weg geprüft wird, bevor sie gesendet wird.
- **Steuerung per Zulassungsliste:** Konfigurieren Sie eine Zulassungsliste, um Nachrichten nur an vertrauenswürdige TLS-Domains zu senden, und erhalten Sie so eine strenge Kontrolle darüber, wohin sichere E-Mails reisen können.
- **Steuerung per Sperrliste:** Erstellen Sie eine Sperrliste, um bestimmte TLS-Domains auszuschließen und alle Routen zu sperren, die Sie nicht verwenden möchten.
- **Automatischer sicherer Fallback:** Wenn eine Domain nicht für die TLS-Zustellung geeignet ist, wechselt Echoworx nahtlos zu einer alternativen sicheren Methode, wie dem Web-Portal oder einem sicheren PDF, sodass der Schutz niemals unterbrochen wird.
- **Mühelose Compliance:** Dieser nahtlose Fallback setzt Ihre Sicherheitsrichtlinie ohne manuellen Eingriff durch und unterstützt resiliente Kontrollen, die im Rahmen von Regelwerken wie DORA und NIS2 erwartet werden.

Zusätzliche Funktionen

- Absender senden einfach, während die Verschlüsselungsplattform entscheidet, wann TLS verwendet werden soll und wann auf eine andere Methode zurückgegriffen werden soll.
- Empfänger ändern nichts, da die transparente Zustellung das Erlebnis von Anfang bis Ende vertraut hält.
- Umfangreiche Branding-Optionen ermöglichen es Ihnen, Kopf- und Fußzeilen anzupassen, damit jede Nachricht unverwechselbar Ihre eigene ist.
- Ideal für B2B-Umgebungen, in denen sich beide Parteien bereits auf TLS für den sicheren Austausch verlassen.

Technischer Hinweis

Sobald eine Nachricht über TLS zugestellt wird, ist sie im Postfach des Empfängers nicht im Ruhezustand verschlüsselt. Sichere Antworten werden außerhalb der Echoworx-Plattform übertragen und sind während der Übertragung auf die eigene TLS-Verbindung des Empfängers für den Schutz angewiesen.

Was das für Sie bedeutet: Ihre Absender senden weiterhin ohne einen zweiten Gedanken, Ihre Empfänger erhalten sichere E-Mails ohne etwas Neues lernen zu müssen, und Ihre Organisation hält ihre Sicherheitsrichtlinie automatisch durchgesetzt – bis hin zu den Compliance-Kontrollen, die Regulatoren erwarten.

Zertifikatsverschlüsselung

Wenn Ihre Empfänger bereits über ein vertrauenswürdiges S/MIME- oder PGP-Zertifikat verfügen, setzt die Zertifikatsverschlüsselung dieses automatisch ein. Nachrichten und Anhänge werden Ende-zu-Ende verschlüsselt, zur Authentizität signiert und zugestellt, ohne dass jemand seine Arbeitsweise ändern muss

Hauptfunktionen

- **Flexible Zertifikatserkennung:** Empfängerzertifikate werden automatisch über externe Suchen in LDAP-Verzeichnissen ermittelt, sodass der vertrauenswürdige Austausch ohne manuellen Aufwand beginnt.
- **Dynamische Empfängerschlüsselsuche:** Echoworx findet PGP-Schlüssel auf einem LDAP-Schlüsselserver mithilfe eines Standard-URIs in der Domain des Empfängers und vereinfacht so die sichere Zustellung in Ihrem gesamten Partnerökosystem.
- **Selbstbedienungs-Uploads durch Empfänger:** Empfänger laden ihr eigenes x509-Zertifikat oder ihren öffentlichen PGP-Schlüssel direkt über das Webportal hoch oder generieren ein selbstsigniertes S/MIME-Zertifikat, wenn sie keines besitzen.
- **Vertrauenswürdige Stammzertifikate auf Abruf:** Die nahtlose Integration mit DigiCert und SwissSign ruft vertrauenswürdige S/MIME-Anmeldeinformationen für Ihre Mitarbeiter ab und generiert diese in dem Moment, in dem ein Schlüssel benötigt wird.
- **PGP-Schlüsselgenerierung in Echtzeit:** Echoworx erstellt PGP-Öffentlich/Privat-Schlüsselpaare für Absender spontan, und der Empfänger der verschlüsselten Nachricht erhält den öffentlichen Schlüssel des Absenders als Anhang, wodurch jeder Austausch in sich geschlossen bleibt.
- **Richtlinienbasiertes Signieren mit Fallback:** Ausgehende Nachrichten werden digital mit einem Schlüssel signiert, der an die E-Mail-Adresse des Absenders gebunden ist, ob hochgeladen oder generiert. Steht keiner zur Verfügung, übernimmt ein unternehmensweiter, domainübergreifender Schlüssel, sodass Nachrichten stets signiert sind.
- **PGP-Signierung „Nur Absender”:** Jede Nachricht, die das Gateway nicht gültig signieren kann, wird mit einer Unzustellbarkeitsmeldung zurückgesendet, womit derselbe bewährte Schutz, der bereits für S/MIME gilt, auf PGP-signierte Kommunikation ausgedehnt wird.
- **Konfigurierbare Schlüsselgrößen:** Legen Sie die automatisch generierten S/MIME- und PGP-Schlüsselgrößen auf Profilebene fest — RSA 2048, 3072 oder 4096 Bit — wobei der Standard nun auf 3072 Bit angehoben wurde, um die kryptografische Stärke gemäß modernen Standards zu erhalten.
- **Eingehende Entschlüsselung:** Eingehende S/MIME- und PGP-verschlüsselte Nachrichten werden mithilfe privater Schlüssel entschlüsselt, die sicher innerhalb der Echoworx-Plattform gespeichert sind, und dann mit angewendeten Marken-Headern und -Footern zugestellt.
- **Selbstbedienungs-PGP-Entschlüsselung:** Leiten Sie ältere endpunktverschlüsselte Nachrichten zur Entschlüsselung über das Gateway, damit historische Aufzeichnungen zugänglich, prüfbar und vollständig bleiben.

Zusätzliche Funktionen

- **Automatische Erneuerung ablaufender S/MIME-Schlüssel:** Für DigiCert- und SwissSign-Kunden werden Mitarbeiterzertifikate automatisch vor ihrem Ablauf neu generiert, wodurch die Sicherheit von reaktiv zu proaktiv übergeht und kurzfristige Dienstunterbrechungen verhindert werden.
- **Einblick in die Signaturverifizierung:** Wenn Echoworx eine eingehende signierte Nachricht verifiziert, fügt das System zusätzliche MIME-Header ein, um Verifizierungsprobleme zu kennzeichnen, und stellt einen detaillierten Bericht als signature_verification_results.html für einen übersichtlicheren Verwaltungsworkflow bereit.
- **Granulare LDAP-Serversteuerung:** Unternehmensadministratoren können bestimmte LDAP-Verzeichnisse innerhalb ihrer Profile aktivieren oder deaktivieren und so die genaue Kontrolle darüber behalten, welche Server durchsucht werden.
- **Separate S/MIME- und PGP-LDAP-Suchen:** Aktivieren Sie externe Schlüsselserver-Suchen unabhängig voneinander für S/MIME, PGP oder beides, damit die Schlüsselerkennung Ihren Regeln folgt und keinem festen Standard.
- **PGP-Privatschlüssel-Export-API:** Exportieren Sie PGP-Privatschlüssel programmgesteuert über einen REST-Endpunkt, was Portabilität, Kontinuität und die von Regulierungsbehörden erwartete Schlüsselsouveränität unterstützt.
- **Reibungslose Migration und globale Reichweite:** Importieren Sie alle Zertifikate und Schlüsselpaare Ihrer Mitarbeiter auf einmal, generieren Sie bei Bedarf automatisch neue Schlüssel und stellen Sie sicher an jede E-Mail-Adresse weltweit zu — alles unter einer konsolidierten Plattform für PGP und S/MIME.

Technischer Hinweis

Um eingehende Nachrichten zu entschlüsseln und Zertifikate aus eingehenden Kommunikationen zu extrahieren, konfigurieren Sie zusätzliche Regeln in Ihrem Gateway, um diese Nachrichten an Echoworx weiterzuleiten. Sobald dieses Routing eingerichtet ist, laufen Erkennung, Entschlüsselung und Signaturverifizierung automatisch ab.

Was das für Sie bedeutet: Ihre Empfänger arbeiten weiterhin genau so wie heute, Ihre Absender erreichen stets vertrauenswürdige Partner mit dem richtigen Schlüssel, und Ihre Administratoren profitieren von proaktiver Erneuerung, präziser Verzeichnissteuerung und klarem Verifizierungseinblick — alles auf einer Plattform, die zertifikatbasierte Kommunikation vom Senden bis zum Öffnen sicher hält.