zertificon®
securing digital business

Z1 SecureMail ONE – Data Sheet

E-Mail-Verschlüsselung für bis zu 100 Postfächer

Teil 1:

Für wen ist Z1 SecureMail ONE geeignet?

Z1 SecureMail ONE ist speziell für kleine und mittlere Unternehmen konzipiert, die die Lösung selbst betreiben können – entweder On-Premises oder in der Cloud.

Zertificon stellt **Anleitungen** für die Installation, Integration und den Betrieb in Standardinfrastrukturen bereit.

Volllizensierung erforderlich

Alle E-Mails Ihres Unternehmens werden durch Z1 SecureMail ONE geroutet und bearbeitet. Deshalb ist eine Volllizenzierung erforderlich. Bei der Auswahl Ihres Paketes wählen Sie eine **Userzahl, die größer ist als die Anzahl aller E-Mail-Accounts** Ihres Unternehmens. Zählen Sie Ihre Funktionspostfächer wie info@ mit.

Z1 SecureMail ONE ist derzeit zur Nutzung mit **maximal 100 E-Mail-Konten** begrenzt. Es ist nicht möglich, mehrere Z1 SecureMail ONE Instanzen miteinander zu kombinieren, um größere Nutzerzahlen zu erreichen. Für größere Nutzerzahlen oder ein besonders hohes Mailvolumen fragen Sie unter www.zertificon.com gern ein Angebot für *Z1 SecureMail Gateway* an.

Technische Mindestvoraussetzungen

- **Virtuelle Maschine** exklusiv für das Z1 Produkt, mindestens 8 GB RAM (bei sehr hohem Volumen 16 GB RAM), 2 CPUs und 80 GB Speicher. Wir empfehlen Backups extern vorzunehmen. Die virtuelle Maschine wird bei der Installation neu formatiert.
- **Eigene Domain – keine Freemailer-Adressen**
- **Firmeneigener Mailserver,** entweder On-Premises oder als Cloud-Lösung, z. B. Microsoft Exchange Online (Microsoft 365) oder Google Workspace.
- **Port 25 muss geöffnet sein** für die E-Mail-Verarbeitung. Firewall-Konfigurationen können erforderlich sein.
- **Standleitung/feste IPv4-Adresse.**

Getestete Hosting-Anbieter

- **IONOS Cloud:** Siehe Cloud Server-Angebote unter ionos.de z.B. Cloud Server RAM L max. 40 EUR/ Monat*
- **Hetzner:** Siehe Cloud-Angebote unter hetzner.com z.B. Shared vCPU (x86) CX31 ab 9,70 EUR/ Monat*
- **Derzeit KEIN Betrieb in AZURE möglich:** Der Betrieb von Z1 SecureMail ONE in Azure wird nicht standardmäßig unterstützt.

*Produkt und Preis Stand März 2024

Unterstützte E-Mail-Infrastrukturen

- **Mailserver On-Premises oder in der Cloud**

  Alle Standard-SMTP/TLS-Mailserver können On-Premises, in der Cloud oder in Hybridszenarien mit Z1 SecureMail eingesetzt werden.

- **Microsoft 365**

  Nur für Business-Pakete mit Exchange-E-Mailserver.

- **Google Workspace**

  Nur für Business-Pakete mit E-Mailserver.

- **3rd Party Services (Drittanbieter)**

  Systeme für Antispam & Antivirus, Data Loss Prevention und Archivierung können über Standardschnittstellen angebunden werden (siehe Abb. 2).

Mailrouting + Integration Antispam-/Antivirus-Lösungen von Drittanbietern

Z1 SecureMail ONE ist für den Einsatz in Kombination mit Antispam (AS) und Antiviruslösungen (AV) zur Inhaltsprüfung konzipiert. Diese Systeme nehmen E-Mails aus dem Internet an (inbound) und übergeben E-Mails an das Internet (outbound). Nur unverdächtige sowie verschlüsselte E-Mails werden an Z1 SecureMail ONE übergeben. Z1 SecureMail ONE entschlüsselt die E-Mails und leitet sie zur erneuten Inhaltsprüfung in einer weiteren Schleife an die AS/AV-Systeme.

Bei Microsoft 365 ist keine Zusatzsoftware notwendig: EoP oder MS Defender übernehmen diese Aufgaben zuverlässig. Google Workspace enthält mit Gmail Security AS- und AV-Funktionen, die in Kombination mit Z1 SecureMail ONE genutzt werden können.

Z1 SecureMail ONE darf keinesfalls direkt als Mail Exchange (MX) zur E-Mail-Annahme verwendet werden.

Beispiele für Routing-Szenarien:

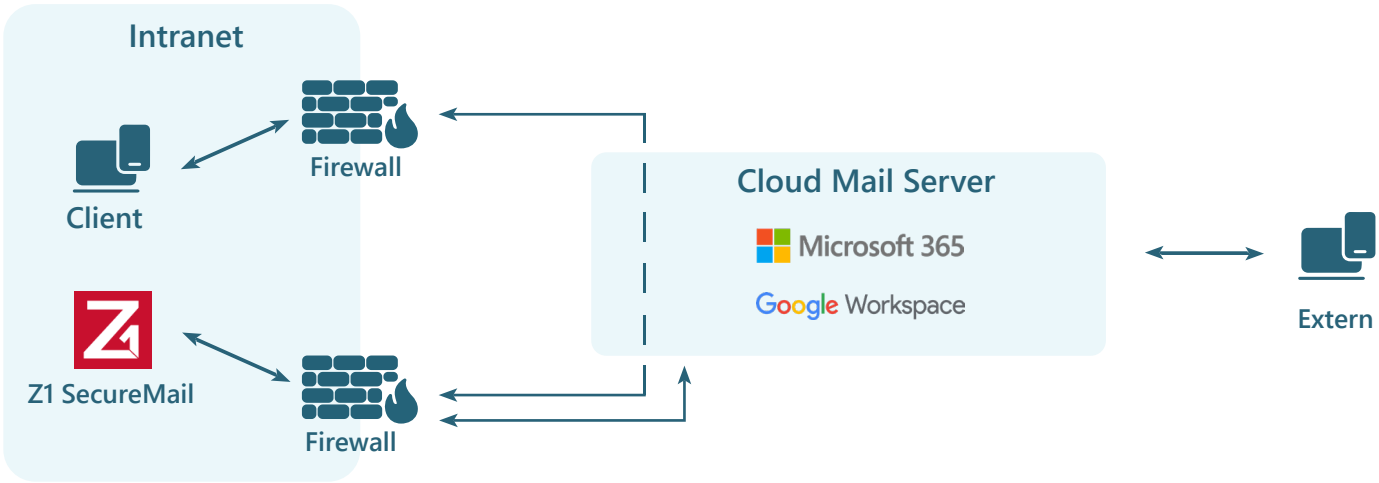


Abb. 1: E-Mail-Routing mit Microsoft 365 oder Google Workspace. Ihr Z1 SecureMail ONE kann On-Premises oder in der Cloud installiert sein.

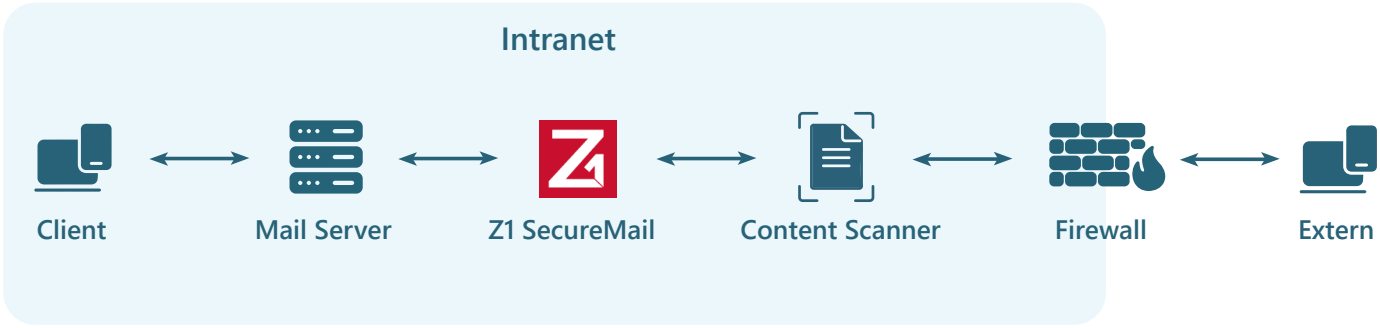


Abb. 2: E-Mail-Routing mit eigenen Mail Server in der SMTP Kette. Ihr Z1 SecureMail ONE kann On-Premises oder in der Cloud installiert sein.

Teil 2:

Produktübersicht

Z1 SecureMail ONE ist eine zentrale Gateway-Lösung zur automatisierten E-Mail-Verschlüsselung und digitalen Signatur.

- Sicherer, vertraulicher und DS-GVO-konformer E-Mail-Austausch mit jedem Kontakt (B2B und B2C)
- E-Mail-Zertifikate sind bereits enthalten
- Zentral und automatisiert – keine Mitarbeiterschulungen notwendig
- ab 5,00 € pro User / Monat; monatlich kündbar nach einer initialen Laufzeit von sechs Monaten

Zertifikatsbasierte E-Mail-Verschlüsselung

Automatisierte E-Mail-Verschlüsselung mit S/MIME und OpenPGP

Z1 SecureMail ONE setzt für Sie die zertifikatsbasierte Verschlüsselung für den E-Mail-Austausch nach den internationalen Standards S/MIME und OpenPGP um. Diese Standards sind üblicherweise im Austausch mit Unternehmen, Banken, Versicherungen oder Behörden anzuwenden. Die komplexen Prozesse zur Ver- und Entschlüsselung inklusive der Validierung des Zertifikatsmaterials werden von Z1 SecureMail ONE automatisiert für alle E-Mail-Adressen Ihres Unternehmens ausgeführt.

Z1 SecureMail ONE schützt Ihre E-Mail-Kommunikation gegen Angriffe aus dem Internet. Innerhalb Ihres Unternehmens werden E-Mails nicht mit Zertifikaten verschlüsselt. Dies vereinfacht die Anwendung für alle Teilnehmer. Zertifikate müssen nicht mehr im Mailprogramm verwaltet werden. Vorgaben zur IT-Compliance wie Content Inspection oder Archivierung können weiterhin zentral umgesetzt werden.

Wenn Ihr Anwendungsfall ein höheres Schutzniveau erfordert, empfehlen wir Ihnen, zusätzlich die interne Infrastruktur zu schützen und die TLS-Verschlüsselung auf internen Strecken anzuwenden.

Digitale Signaturen setzen und validieren

Ausgehende E-Mails können automatisch zertifikatsbasiert digital signiert werden. Die digitalen Signaturen eingehender E-Mails werden überprüft. Das Ergebnis der Überprüfung wird in die Original-E-Mail eingebettet, die an den Empfänger in Ihrem Unternehmen gesendet wird. So erkennen Ihre Mitarbeiter bei jeder einzelnen E-Mail sofort, ob diese vertrauenswürdig ist.

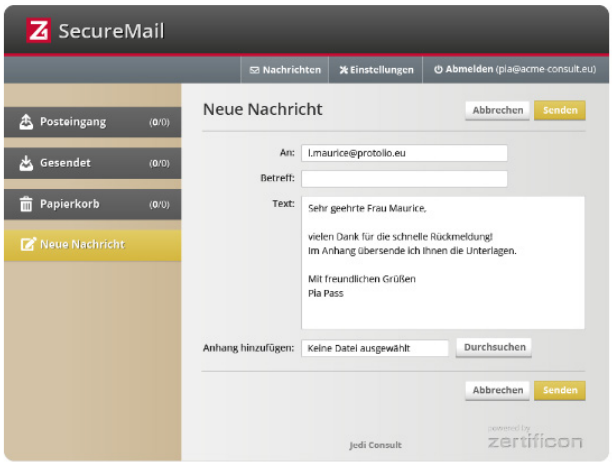
Passwortbasierte E-Mail-Verschlüsselung

Passwortbasierte Verschlüsselung dient dem vertraulichen E-Mail-Austausch mit Kommunikationspartnern, die keine eigenen Schlüssel und E-Mail-Zertifikate nutzen. So lassen sich E-Mails im Austausch mit Kunden, Patienten und kleineren Dienstleistern schützen. Die Personalabteilung kann ganz einfach DS-GVO-konforme E-Mails an Privatadressen von Mitarbeitern und Bewerbern senden.

Sicherer Webmailer im eigenen Corporate Design

E-Mails werden verschlüsselt und an einen sicheren HTTPS-Webmailer zugestellt, den Sie über Z1 SecureMail in Ihrer eigenen Infrastruktur betreiben. Der E-Mail-Empfänger erhält eine Benachrichtigung an sein Standardpostfach für jede neu eingehende E-Mail. Eine Antwortfunktion ist im Webmailer enthalten.

Die Nutzeroberfläche können Sie über einen speziellen Theme Editor auch ohne HTML- und CSS-Kenntnisse einfach mit Ihrem Logo und Ihren Farben an Ihr Corporate Design anpassen.



Teil 3:
Funktionsübersicht

Verwaltung eigener Schlüssel und Zertifikate

Bezug von S/MIME X.509 E-Mail-Zertifikaten

Zertifikate von einer anerkannten Zertifizierungsstelle (in Übereinstimmung mit den Standards der etsi.org und cabforum.org) sind für alle Nutzer im Abonnement enthalten. Derzeit erhalten Sie domainvalidierte Zertifikate mit 4096 Bit Schlüssellänge basierend auf SwissSign-Zertifikaten.

Die Zertifikate sind ausschließlich im Z1 SecureMail Produkt verwendbar. Bei Beendigung oder Ablauf Ihres Abonnements werden die Zertifikate automatisch widerrufen und ungültig.

Domainvalidierung für S/MIME E-Mail-Zertifikate

Eine Domainvalidierung ist vor der Nutzung durchzuführen. Im Kundenportal werden Sie dazu durch einen Prozess geführt. Bitte beachten Sie: Sie benötigen Zugriff auf Ihre Domain, um einen Validierungscode als .txt-Datei zu hinterlegen oder einen DNS-Eintrag vorzunehmen. Die Domainvalidierung wird von uns begleitet und wird üblicherweise innerhalb eines Werktags ausgeführt.

Automatische Erstellung von S/MIME-Schlüssel- und Zertifikatspaaren

Schlüssel und Zertifikate werden automatisch für alle lizensierten Benutzer ausgestellt. Beim Onboarding neuer Mitarbeiter sind keine manuellen Eingaben zur Ausstellung von Benutzerschlüsseln und Zertifikaten erforderlich.

Onboard OpenPGP-Schlüsselgenerator

OpenPGP-Schlüssel werden für alle Nutzer automatisch direkt im Z1 SecureMail ONE erstellt.

Zentraler OpenPGP-Signaturschlüssel

Alle von Ihnen erstellten OpenPGP-Schlüssel werden mit Ihrem unternehmenseigenen zentralen Signaturschlüssel gegengezeichnet. Dadurch sind Ihre Schlüssel für Dritte leicht als vertrauenswürdig erkennbar.

Lifecycle-Management für Schlüssel und Zertifikate

Für Schlüssel und Zertifikate, die mit Z1 SecureMail Produkten ausgestellt werden, ist die Verwaltung des gesamten Zertifikatslebenszyklus automatisiert. Sie brauchen keine Termine notieren, um neue Schlüssel manuell zu erstellen und zu veröffentlichen.

Automatisierte Schlüssel- & Zertifikatsveröffentlichung

Ihre öffentlichen OpenPGP-Schlüssel und S/MIME-Zertifikate werden direkt nach der Erstellung automatisch am Zertifikatsportal Z1 Global TrustPoint veröffentlicht. Verweisen Sie Ihre Kontakte einfach dorthin und sparen Sie sich die Zeit für den manuellen Schlüsselaustausch.

Wenn Ihre Kontakte ebenfalls Z1 Produkte verwenden, gelingt der Schlüsselaustausch auf beiden Seiten vollautomatisch. Dafür sind alle Z1 SecureMail Produkte mit Z1 Global TrustPoint verbunden.

Verwaltung fremder Schlüssel und Zertifikate

Automatische Suche und Speicherung

Öffentliche Schlüssel und Zertifikate von Geschäftspartnern und Kunden werden automatisch über Z1 Global TrustPoint abgerufen. Zertifikate und CA-Schlüsselketten, die in signierten E-Mail-Nachrichten enthalten sind, werden automatisch aus dem E-Mail-Datenverkehr ausgelesen und gespeichert.

Automatisierte Echtzeitvalidierung

Die Zertifikate von Geschäftspartnern und Kunden werden automatisch validiert. Dabei werden die Zertifikatswiderufslisten (CRLs) der ausstellenden Trustcenter geprüft und ggf. das Online Certificate Status Protocol (OCSP) zur Abfrage genutzt.

Vertrauensverfahren für externe OpenPGP-Schlüssel

Da es keine OpenPGP-Zertifizierungsstellen gibt, müssen Sie mitgesendete oder in Verzeichnisdiensten gefundene PGP-Schlüssel überprüfen und entscheiden, ob Sie diesen vertrauen möchten.

Um PGP-Schlüssel nutzen zu können, die im Z1 Global TrustPoint gespeichert sind, wird Ihnen mit der Benachrichtigung eine Akzeptanzoption zur Freigabe des Schlüssels angeboten.

Sicherheitsfunktionen

Zentrale Richtlinien

Konfigurieren Sie regelbasierte Richtlinien („Z1 SecureMail Policies") zur zentralen Steuerung der Verschlüsselung und Signierung von E-Mail-Nachrichten für alle E-Mail-Adressen in Ihrem Unternehmen. Die Einhaltung von Vorgaben, z. B. der DS-GVO, kann problemlos im gesamten Unternehmen durchgesetzt werden.

Beispiele:

- E-Mails immer verschlüsseln an „*@unsere-bank.de"; bei Fehlern, Senden blockieren.
- E-Mails immer digital signieren beim Senden von „info@meine-domain.de"

Verdächtige E-Mail-Nachrichten

Automatische Warnungen bei fehlerhaften Signaturen oder ungültigen Zertifikaten sind standardmäßig aktiviert. Sie können die verdächtigen Nachrichten optional blockieren.

Steuerung über Benutzerkommandos

Benutzerkommandos, die in der Betreffzeile eingegeben werden, ermöglichen es Ihren Mitarbeitern als interne Sender, Aktionen wie „Verschlüsseln" oder „Signieren" für einzelne E-Mails manuell auszulösen.

Komfortfunktionen

Disclaimer Management, Einfügen von E-Mail-Signaturen

Das Disclaimer Management sorgt dafür, dass Kontaktdaten, Logo, Haftungs- oder Veranstaltungsinformationen in der E-Mail-Fußzeile einheitlich dargestellt werden.

Konfigurieren Sie zentral, welche Textblöcke in der Fußzeile einer E-Mail automatisch eingefügt werden sollen. Die Aufnahme der Textblöcke wird eingestellt in Abhängigkeit von Sender- oder Empfängeradresse, Gruppenzugehörigkeit oder Domainname.

Massenimport per CSV

Benutzer- und Funktionsadressen können aus anderen Verzeichnissen exportiert und dann als CSV-Datei in Z1 SecureMail eingespielt werden.

Betriebsplattform & Administration

Virtualisierungsumgebung

Die gängigen Virtualisierungsumgebungen für Unternehmen werden in den aktuellen Versionen unterstützt.

On-Premises oder Cloud

Z1 SecureMail wird als ISO-Datei geliefert. Diese wird entweder On-Premises oder in der Cloud auf einer virtuellen Maschine installiert.

Gehärtetes Linux-Debian-Betriebssystem

Debian Linux als Betriebssystem wurde auf die wesentlichen Funktionen zum Betrieb unserer Software reduziert. Unnötige Ports wurden geschlossen. Es gelten restriktive Rechte und Systemrichtlinien.

Z1 Appliance Management Software

Updates und Standardkonfigurationen für das Z1 System werden über die Z1 Appliance Management Software verwaltet.

Software- und Sicherheitsupdates

Neue Software und Security Updates werden in der Admin-Oberfläche angezeigt und sind mit einem Klick installierbar.

Administrationsoberfläche

Alle Standardkonfigurationen können in der einfach zu bedienenden, browser-basierten Administrationsoberfläche vorgenommen werden.

Systemlimitierungen

Fünf Domains/Subdomains

Die Anzahl Ihrer eigenen Domains oder Subdomains, die Sie in Z1 SecureMail ONE verwalten können, ist auf fünf begrenzt.

Zwei E-Mail-Aliases pro Nutzerkonto

Pro Nutzeraccount sind zwei Aliases zulässig. Aliases erhalten kein Zertifikat. Wir empfehlen, eine E-Mail-Adresse *z1-admin@...* zum Emfpang von Alerts anzulegen und diese mit den Aliases *postmaster@...* und *abuse@...* zu belegen.

Systembenachrichtigungen verarbeiten

Das System sendet Hinweise und Alerts zum Systemstatus. Als Kunde haben Sie die Pflicht, diese Systembenachrichtigungen zeitnah zu prüfen. Dazu zählen auch Release-Informationen. Der Kunde verpflichtet sich, die Software innerhalb von sechs Wochen nach Releasedatum upzudaten. Veraltete Systeme werden nicht supportet. Zertificon ist berechtigt, die Systeme nach entsprechenden Hinweisen automatisch upzudaten. Dies geschieht spätestens drei Monate nach Releasedatum.

Mailvolumen von 3.000 E-Mails pro Nutzerkonto

Z1 SecureMail ONE unterstützt ein monatliches Volumen von 3.000 E-Mails pro Nutzerkonto. Gezählt werden sowohl eingehende als auch ausgehende Nachrichten. Diese Summe zählt kumuliert über alle Nutzerkonten. Ungenutzte Nutzerkonten oder solche mit geringem Mailvolumen geben dieses für andere Nutzer frei.

Sie können das E-Mail-Volumen somit durch die Buchung einer höheren Nutzerzahl steuern. Der Zählerstand ist jederzeit in der Administrationsoberfläche der Z1 Lösung überprüfbar. Sie erhalten zusätzlich E-Mail-Benachrichtigungen rechtzeitig vor Erreichen des Limits. Dann haben Sie die Möglichkeit, innerhalb von Minuten zusätzliches Volumen über das Kundenportal hinzuzubuchen.

Mit der größtmöglichen Lizenzierung von 100 Nutzern ergibt sich ein maximales Volumen von 300.000 E-Mails pro Monat für das Produkt Z1 SecureMail ONE.

Zulässige Mailgröße 30 MB

Bei Mailgrößen oberhalb von 30 MB würde die Performance leiden, bis hin zum Systemstillstand. Das Produkt weist deshalb übergroße E-Mails ab.

Z1 SecureMail ONE jetzt kaufen: www.zertificon.com/jetzt-kaufen

Kundenservice

Hersteller-Support

Unser eigenes Zertificon Inhouse Support-Team unterstützt Sie beim bestmöglichen Einsatz unserer Z1 Lösungen. Wir sprechen Deutsch und Englisch.

Ausführliche Dokumentation

Die Handbücher enthalten Erläuterungen zu grundlegenden Konzepten und viele Schritt-für-Schritt-Anleitungen. Die Dokumentation ist als Online-Help über das Produkt erreichbar und als PDF im Kundenportal verfügbar. Sie ist zum besseren Verständnis mit zahlreichen Screenshots und Schemazeichnungen bebildert. Die Dokumentation ist in einfacher englischer Sprache verfasst.

Z1 SecureMail ONE Self-Service

Das Z1 SecureMail ONE Kundenportal bietet ausführliche Hilfe-Seiten, Handbücher und FAQ. Ihre Kundendaten mit Vertragsverwaltung und Rechnungen stehen hier ebenfalls zur Verfügung.

Ticket-basierter Hersteller-Support

Sie können Support-Tickets bequem online im Zertificon-Portal erstellen. Wir antworten auf Ihre Anfragen schnellstmöglich innerhalb unserer Bürozeiten.

Zertificon Solutions GmbH
Berlin, Germany

www.zertificon.com
E-mail: sales@zertificon.com