zertificon®
securing digital business

Z1 SecureMail ONE – Data Sheet

Email encryption for up to 100 mailboxes

Part 1:

Who can use Z1 SecureMail ONE?

Z1 SecureMail ONE is specifically designed for small and medium-sized businesses that can operate the solution themselves – either on-premises or in the cloud.

Zertificon provides **instructions** for installation, integration and operation in standard infrastructures.

Full licensing required

All emails from your company are routed through Z1 SecureMail ONE. Full licensing is therefore required. When selecting your package, choose a **number of users that is higher than the number of all your company's email accounts**. Remember to include functional mailboxes such as info@.

Z1 SecureMail ONE is limited to a maximum of **100 email accounts**. It is not possible to combine multiple Z1 SecureMail ONE instances to reach larger numbers of users.

For larger numbers of users or a particularly high mail volume, please request a quote for *Z1 SecureMail Gateway* at zertificon.com.

Minimum technical requirements

- **Virtual machine** exclusively for the Z1 product, at least 8 GB RAM (16 GB RAM for very large volumes), 2 CPUs and 80 GB memory. We recommend making backups externally. The virtual machine undergoes reformatting during installation.
- **Own domain – no freemailer addresses**
- **Your company's own mail server**, either on-premise or as a cloud solution, e.g. Microsoft Exchange Online (Microsoft 365) or Google Workspace.
- **Port 25 must be open** for email processing. Firewall configurations may be required.
- **Leased line/fixed IPv4 address.**

Tested hosting providers

- **IONOS Cloud:** Check cloud server options at ionos.com e.g. Cloud Server **RAM L** max. 40 EUR/ month*
- **Hetzner:** See cloud offers at hetzner.com e.g. Shared vCPU (x86) **CX31** starting from 9,70 EUR/ month*
- **Currently NO operation in AZURE possible:** The operation of Z1 SecureMail ONE in Azure is not supported by default.

*product and pricing status from March 2024

Supported email infrastructures

- **Mail server on-premises or in the cloud**

  All standard SMTP/TLS mail servers can be used on-premises, in the cloud or in hybrid scenarios with Z1 SecureMail.

- **Microsoft 365**

  Only for business packages with Exchange server.

- **Google Workspace**

  Only for business packages with mail server.

- **3rd party services**

  Systems for anti-spam, anti-virus, data loss prevention, and archiving can be connected through standard interfaces (see figure 2).

Mail routing + integration of anti-spam/anti-virus solutions from 3rd parties

Z1 SecureMail ONE is compatible with anti-spam (AS) and anti-virus (AV) solutions for content inspection. These systems handle emails from and to the Internet (inbound and outbound). Z1 SecureMail ONE receives only encrypted emails that pass the initial security check. These emails are then decrypted and sent back to the AS/AV systems for a further content check.

Microsoft 365 users do not need any extra software: EoP or MS Defender can take care of these tasks effectively. Google Workspace users can also combine Z1 SecureMail ONE with Gmail Security, which has AS and AV features.

Z1 SecureMail ONE must not be used as a mail exchange (MX) for accepting emails directly.

Examples for routing scenarios:

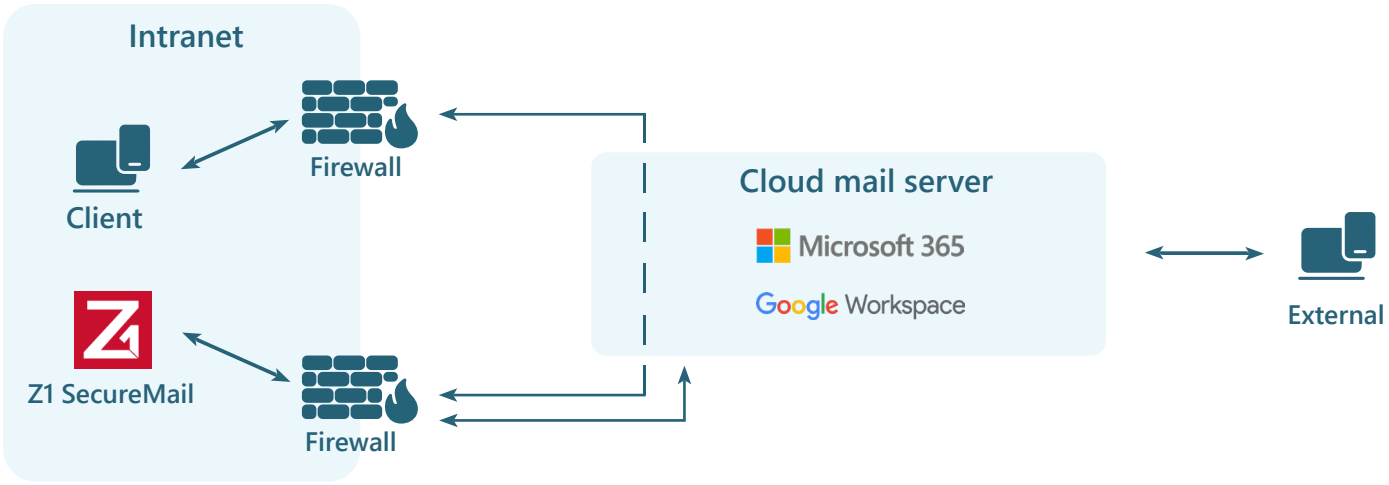


Fig. 1: Email routing with Microsoft 365 or Google Workspace. Your Z1 SecureMail can be installed on-premises or in the cloud.

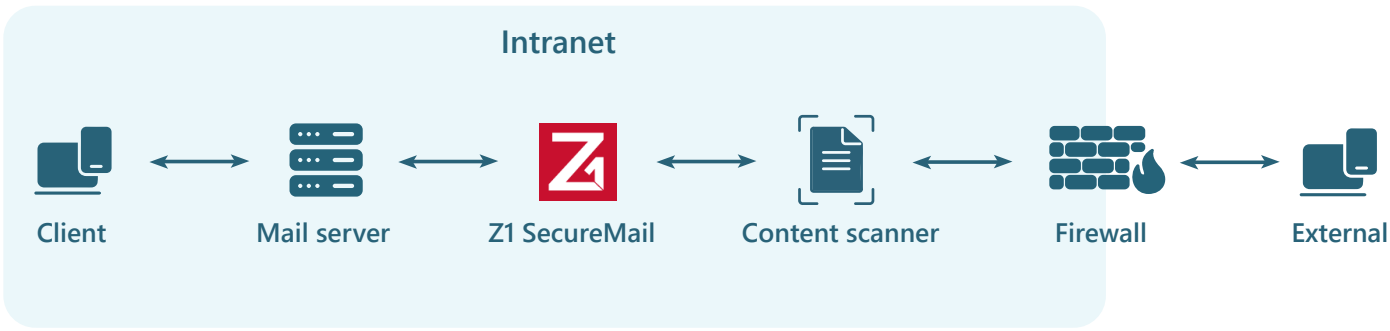


Fig. 2: Email routing with your own mail server in the SMTP chain. Your Z1 SecureMail can be installed on-premises or in the cloud.

Part 2:

Product overview

Z1 SecureMail ONE is a central gateway solution for automated email encryption and digital signatures.

- Secure, confidential, and GDPR-compliant email exchange with any contact (B2B and B2C)
- Email certificates included
- Centralized and automated - no need for employee training
- From €5.00 user/month; monthly cancellation after an initial six-month term

Certificate-based email encryption

Automated email encryption with S/MIME and OpenPGP

Z1 SecureMail ONE uses certificates to encrypt emails according to international S/MIME and OpenPGP standards. These standards are commonly used for encrypting emails with companies, banks, insurance companies, and government agencies. Z1 SecureMail ONE automates the complex processes of encryption and decryption, including the validation of certificate material, for all of your company's email addresses.

Z1 SecureMail ONE protects your email communication from Internet threats. It does not use certificates for encryption within your company, simplifying the process for everyone. No certificate management is required in the mail program. Centralized implementation of IT compliance requirements such as content inspection or archiving is still possible. To ensure a high level of protection for your internal infrastructure, you should activate TLS encryption between Z1 SecureMail ONE and other servers.

Set and validate digital signatures

Outgoing emails can be automatically signed digitally using certificates. The digital signatures of incoming emails are verified. The result of the verification is embedded into the original email sent to the recipient in your organization. This allows your employees to immediately see if an email is trustworthy.

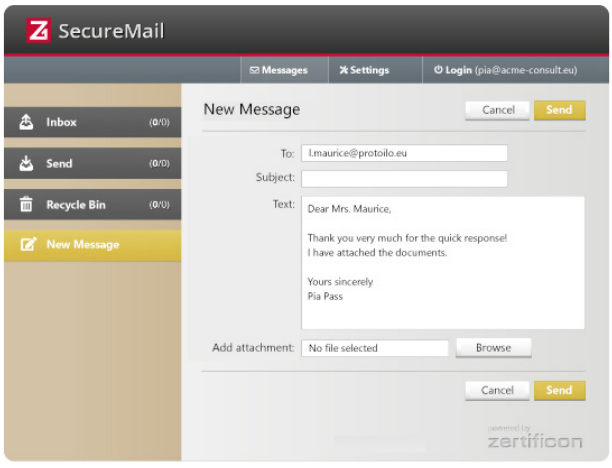
Password-based email encryption

Password-based encryption is used to exchange confidential emails with communication partners who do not use keys and certificates. This allows you to protect emails sent to customers, patients, and smaller service providers. It also allows HR to easily send GDPR-compliant emails to private addresses of employees and applicants.

Secure webmailer in your corporate design

Emails are encrypted and delivered to a secure HTTPS webmailer which you operate in your own infrastructure via Z1 SecureMail. The email recipient receives a notification for every new incoming email in their main email inbox. A reply function is included in the webmailer.

You can customize the user interface to your corporate design, including your logo and colors, using a theme editor that does not require any HTML or CSS knowledge.



Part 3:
Features overview

Management of your own keys and certificates

Subscription to S/MIME X.509 email certificates

All users get certificates from a trusted certification authority that meets the standards of etsi.org and cabforum.org as part of the subscription. Currently these are domain-validated SwissSign certificates with a 4096-bit key length.

The certificates can only be used with your Z1 SecureMail ONE product. Upon termination or expiration of your subscription, the certificates are automatically revoked and become invalid.

Domain validation for S/MIME email certificates

Domain validation must be completed before you can use the product. You will be guided through the process in the Customer Portal. Please note: You will need access to your domain to add the validation code as a .txt file or to make a DNS record. The validation process is assisted by us and is usually completed within one business day.

Automatically create S/MIME key and certificate pairs

Keys and certificates are issued automatically for all licensed users. When onboarding new employees, no manual input is required to issue user keys and certificates.

Onboard OpenPGP key generator

OpenPGP keys are automatically generated for all users directly in Z1 SecureMail ONE.

Central OpenPGP signature key

All of the OpenPGP keys that your company creates are countersigned with your company's own central signature key. This makes it easy for third parties to recognize your keys as trustworthy.

Lifecycle management for keys and certificates

For keys and certificates issued with Z1 SecureMail products, the management of the entire certificate lifecycle is automated. You don't have to keep track of deadlines to manually create and publish new keys.

Automatically publish keys and certificates

Your OpenPGP keys and S/MIME certificates are published automatically on the Z1 Global TrustPoint certificate portal right after they are created. Simply point your contacts there and save yourself the time of manually exchanging keys.

If your contacts also use Z1 products, key exchange occurs automatically between both parties. All Z1 SecureMail products are connected to Z1 Global TrustPoint.

Management of external keys and certificates

Automated search and storage

Public keys and certificates of your business partners and customers are automatically retrieved through Z1 Global TrustPoint. Certificates and CA key chains in signed email messages will be automatically extracted and saved.

Automated real-time validation

Business partners and customer certificates are automatically validated. The certificate revocation lists (CRLs) of the issuing certificate providers are checked and, if available, the Online Certificate Status Protocol (OCSP) is used for queries.

Trust process for external OpenPGP keys

Because OpenPGP certification authorities do not exist, you must verify PGP keys that are sent to you or that you find in directory services and decide whether to trust them.
In order to use PGP keys that get harvested by your Z1 SecureMail ONE from incoming emails, you must acccept the key. You will receive an alert for each newly imported OpenPGP key.

Security features

Central policies

Configure rule-based policies („Z1 SecureMail Policies“) to centrally control encryption and signing for all company email addresses. This makes it easy to enforce compliance with regulations, such as GDPR, across the entire company.

Examples:

- Always encrypt emails sent to „*@our-bank.com“; if an error occurs, block sending.
- Always sign emails sent from „info@my-domain.com“

Suspicious email messages

Automatic warnings for invalid signatures or invalid certificates are activated by default. You can optionally block suspicious messages.

Manual control with user commands

Internal senders can manually trigger actions like „Encrypt“ or „Sign“ for individual emails by using specific commands in the subject line of the email.

Convenience features

Disclaimer management, adding email signatures:

Disclaimer management ensures that any type of information, such as contact details, logo, legal notice, or event information, is displayed consistently in the email footer.

You can centrally configure which text blocks should automatically be inserted into the email footer. The inclusion of text blocks is set based on the sender or recipient address, group affiliation, or domain name.

CSV bulk import

User addresses and functional addresses can be exported from other directories and then imported into Z1 SecureMail as a CSV file.

Operating platform & administration

Virtualization environment

The most common virtualization environments for companies are supported in the current versions.

On-premises or in the cloud

Z1 SecureMail is provided as an ISO file that can be installed either on-premises or in the cloud on a virtual machine.

Hardened Linux Debian operating system

Debian Linux as an operating system has been reduced to the essential functions for running our software. Unnecessary ports have been closed. Restrictive rights and system guidelines apply.

Z1 Appliance Management Software

Updates and standard configurations for the Z1 system are managed via the Z1 Appliance Management Software.

Software and security updates

New updates for software and security are shown on the admin interface and can be installed with one click.

Administration interface

All standard configurations can be made in the easy-to-use, browser-based administration interface.

System limitations

Five domains/subdomains

The number of your own domains or subdomains that you can manage in Z1 SecureMail ONE is limited to five.

Two email aliases per user account

Two aliases are allowed per user account. Alias addresses do not receive certificates. To receive alerts, we recommend creating a *z1-admin*@... email address and linking it to the *postmaster*@... and *abuse*@... aliases.

Dealing with system notifications

The system regularly sends notifications and alerts. As a customer, it's your responsibility to check these notifications in a timely manner. This includes updates about new software releases. You are required to update the software within six weeks of any new release. Please note that support is not provided for outdated systems. Zertificon reserves the right to automatically update systems, provided that customers are appropriately notified in advance. Such updates will occur no later than three months after a new release is available.

Mail volume of 3,000 emails per user account:

Z1 SecureMail ONE allows a maximum of 3,000 emails per user account every month. This includes both incoming and outgoing messages. The total email count is combined across all users. This way, unused accounts or those with low email traffic will free up volume for other users. This allows you to control the email volume limit by simply adding more users to your account.

You can check your current mail volume status in the Z1 administration interface. You will receive an email notification before you reach your limit, allowing you to purchase additional capacity in the Zertificon Customer Portal within minutes.

With a maximum of 100 users, Z1 SecureMail ONE can handle up to 300,000 emails per month.

Alowed email size: 30 MB

Emails larger than 30 MB can significantly reduce system performance, potentially leading to a complete halt. To prevent this, the system automatically rejects any emails exceeding the 30 MB size limit.

Get Z1 SecureMail ONE at www.zertificon.com

Customer service

Manufacturer support

Our dedicated Zertificon In-house support team is committed to assisting you in optimizing the use of our Z1 solutions. We provide support in both German and English.

Comprehensive documentation

Our manuals clearly explain key concepts and provide step-by-step instructions. You can access this documentation online through the product itself or download it as a PDF from the Customer Portal. The documents include plenty of helpful screenshots and diagrams. All documents are written in easy-to-understand English.

Z1 SecureMail ONE self-service

The Z1 SecureMail ONE Customer Portal offers comprehensive support through detailed help pages, manuals, and FAQs. Additionally, it provides access to your customer data, including contract management and billing information.

Support tickets

Easily submit support tickets via our Support Portal. Our team is committed to providing timely responses during standard business hours.

Zertificon Solutions GmbH
Berlin, Germany

www.zertificon.com
Email: sales@zertificon.com