CipherMail provides centrally managed solutions for automatic encryption and digital signing of email.

CipherMail Email Encryption Gateway supports all major email encryption standards like S/MIME, PGP, TLS and PDF encryption and is compatible with any SMTP-based infrastructure. The built-in Data Leak Prevention (DLP) module can be used to prevent certain information from leaving the organization via email.

CipherMail Webmail Messenger can be used as a secure alternative to the Gateway when a recipient does not support S/MIME, PGP or PDF encryption.

Why do we need email encryption and digital signing?

Mail servers use Simple Mail Transfer Protocol (SMTP) for sending and receiving email. SMTP is one of the oldest Internet protocols still in use today. It was designed at a time when the Internet, as we know it, did not exist. In the early days, open relays, encryption, authentication and other security issues were not considered important since the Internet was more or less a closed network of trusted users. The main focus was on providing reliable email delivery.

The good thing about SMTP is that it can be extended with new functionality. For example, even though SMTP was initially not designed to support attachments, support for attachments was added with the introduction of Multipurpose Internet Mail Extensions (MIME). MIME itself was later extended to support encryption and digital signatures (S/MIME).

Sending an email to a final recipient requires several steps:

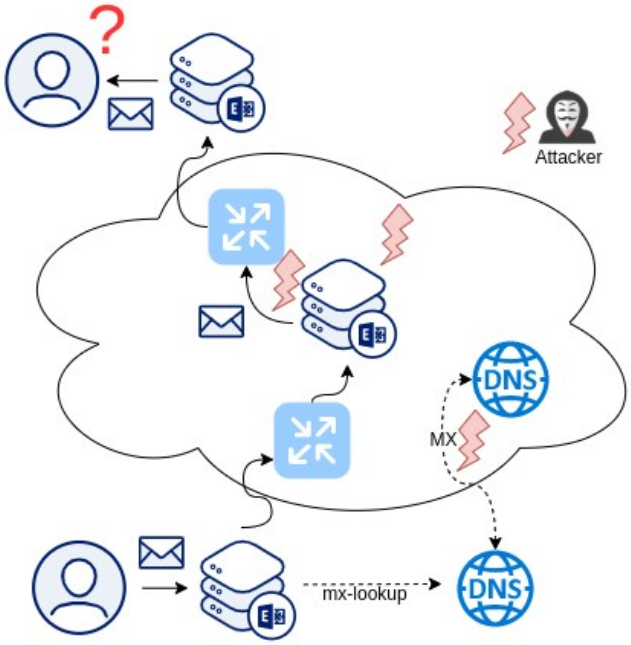
1. The mail server of the final recipient needs to be looked up via DNS (MX lookup)
2. Email must be delivered to the next mail server(s)
3. The recipient receives the mail from the final mail server.

The DNS lookup process involves multiple external DNS servers and multiple lookups. Unless DNSSEC is used to validate these lookups, the lookup results can not be trusted. Unfortunately this has not been widely deployed yet. Office 365, for example, does not support DNSSEC. SMTP is therefore susceptible to a man-in-the-middle attack.

Email is not always delivered directly to the final mail server. In large mail setups, multiple intermediate mail servers (for example, a centralized anti-virus/anti-spam scanner) might be used. If the email is not encrypted, the message might be intercepted while the email is handled by the intermediate mail server.

Data on the Internet travels via multiple hubs. Email can be intercepted in transit when the email is delivered from one mail server to the other.

Even if the email does not contain any secret information, can the contents of the email be trusted? Was the email modified in transit? Can the recipient check the identity of the sender? Can you protect yourself against CEO fraud?



TLS to the rescue?

Nowadays, most mail servers support TLS. Even though TLS improves the security of SMTP, there are still security issues that are not solved with TLS alone.

TLS protects the connection but not the message itself. Email is still stored in plain text on a mail server. With TLS you are only in control of the connection to the first mail server. Whether or not TLS is used between the other mail servers is beyond your control. Even though TLS protects the channel, you are still vulnerable to a man-in-the-middle attack unless you strongly validate the connection. Because TLS does not authenticate the sender and does not protect the contents of the email, you are still vulnerable to CEO fraud.

Secure email requirements

A secure email solution should at least provide the following security services:

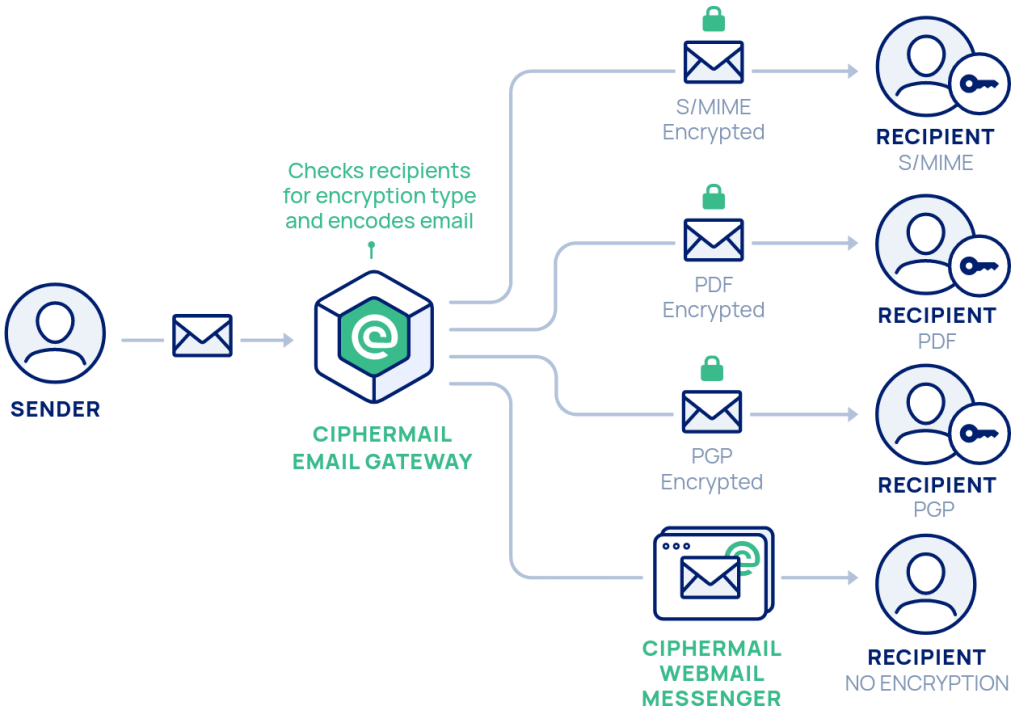
- Confidentiality: can you be certain that only the intended recipient can read the message?
  - Solution: encrypt the message
- Integrity: has the message been altered?
  - Solution: digitally sign the message
- Authenticity: who sent the message?
  - Solution: digitally sign the message with a trusted certificate or key

S/MIME and OpenPGP are the only two official email standards that can provide all the required security services.

CipherMail Gateway

CipherMail Email Encryption Gateway supports all four major encryption standards: S/MIME, PGP, PDF encrypted email and TLS.

S/MIME and PGP use public key encryption (PKI) for encryption and signing. PDF encryption can be used as a lightweight alternative to S/MIME and PGP. The only requirement for the recipient is a PDF reader.



The CipherMail Gateway automatically detects which encryption standard is supported by the recipient. For example, if an email is sent to four recipients and each recipient supports a different encryption method, the email is encrypted with four different methods.

The sender does not have to think about the capabilities of the recipients, the Gateway will automatically handle this for you.

Features

- S/MIME, PGP, PDF encryption, TLS, Webmail Messenger (if installed)
- Digital signatures (S/MIME, PGP)
- DLP module
- Store and forward SMTP server, compatible with any SMTP based infrastructure
- Domain to domain encryption (S/MIME and PGP)
- High Availability (HA) active/active cluster
- Hardware Security Module (HSM) support

- Office 365 Integration
- Can interface with external CAs
- Auto certificate enrollment
- Web-based user interface
- Available as a Virtual Appliance for VMware, HyperV, Azure, Digital Ocean, Open Virtualization Format (OVF)
- RPM packages for RHEL8

S/MIME

S/MIME is the most widely used email encryption and digital signature standard, especially in enterprises and governmental organizations.

Most email clients, like Outlook, support S/MIME out of the box.

S/MIME is based on Public Key Infrastructure (PKI). PKI is a technology that can be used to securely exchange information over insecure networks using public key cryptography. PKI uses X.509 certificates to bind a public key to an identity. S/MIME uses a hierarchical trust model where trust is inferred bottom-up. The root of the trust hierarchy is blindly trusted. All the leaf nodes and branches (the end-user and intermediate certificates) are trusted because they are children of the trusted root.

In PKI, the trust chain, from root to end-user certificate, is built using a chain of signed certificates. The root certificate signs the intermediate certificate, and the intermediate certificate signs the end-user certificate. A certificate is signed using the private key of the issuer. Any changes to the certificate after signing will break the signature and will make the certificate invalid.

The CipherMail Email Encryption Gateway can be configured to automatically encrypt and sign emails with S/MIME.

Certificate store

The certificate store contains all the end-user and intermediate certificates. End-user certificates are used for signing and decryption. New certificates or keys can be imported into the certificate store.

The Gateway will automatically extract and import certificates from digitally signed emails. If the certificate is trusted, the certificate can then be automatically used by the Gateway.

Root store

The root store contains all the trusted CA root certificates. The administrator decides which CA certificates are trusted. New root CA certificates can be imported into the Gateway.

Revocation checking

If a certificate is compromised, or a certificate should no longer be used for whatever reason, the certificate should be revoked. Certificates can be revoked by putting the certificates on a

"Certificate Revocation List" (CRL). A CRL is issued by a certificate authority (CA) and is periodically updated. After a certificate is revoked, it should no longer be used.

The Gateway periodically scans (by default every 6 hours), the list of CA certificates for CRL distribution points and then tries to download a CRL from the URL defined in the CRL distribution points. If a new CRL is downloaded it is stored in the CRL store replacing the old CRL.

Certificate selection

The Gateway will automatically select the correct certificates for signing and encryption. Only certificates that are valid, i.e., trusted, not expired, not revoked etc., are used automatically. This requires that certificates are trusted by a root certificate and that the root certificate is installed into the root store.

Certificate Authority

The Gateway contains a built-in CA server that can create end-user certificates for internal and external users. This helps to quickly set up an S/MIME infrastructure without having to resort to external CAs for certificates and keys. Certificates and private keys can be securely transported to external recipients using a password-encrypted PKCS#12 certificate store. The external recipients can use the certificate with any S/MIME-capable email client like Outlook, Thunderbird, CipherMail for Android etc. and start receiving and sending S/MIME-encrypted email.

The Gateway can also interface with external CAs via a pluggable framework that allows new certificate request handlers to be registered. A certificate request handler is responsible for creating and/or retrieving a certificate and private key from internal or external CAs. The Gateway comes with various certificate request handlers: Global Sign, EJBCA, CSR, Intellicard. New certificate request handlers can be added easily.

PGP

OpenPGP (which is the RFC standard for PGP) is an email encryption and digital signing standard like S/MIME. OpenPGP works with public and secret keys. Public keys can be signed by other public keys (although in practice most keys are only self-signed). PGP public keys can be published to publicly accessible key servers. Public keys can be downloaded from public key servers.

OpenPGP supports two forms of encoding: PGP/MIME and PGP/INLINE. PGP/MIME encrypts and signs the complete MIME message and has full support for HTML email. With PGP/INLINE, every MIME part must be individually signed or encrypted. PGP/INLINE support for HTML email is limited and is not supported by all email clients. Because PGP/INLINE must scan the complete MIME message, PGP/INLINE is more resource intensive.

Because PGP/MIME keeps the structure of the original message intact, has full support for HTML and has better performance, PGP/MIME is strongly advised.

PGP keys

The PGP keyring stores all the public and secret keys.

A PGP key contains two parts, a secret key and a public key (a key pair). The secret key is used for signing and decrypting of email. In most cases a PGP user has multiple key pairs, one primary key and one or more subkeys. The primary key identifies the user, i.e., it contains the “User ID”, and the primary key signs the subkeys. A “User ID” typically contains the email address of the owner of the key. A PGP key can be valid for signing, for encryption or for both.

Existing public and secret PGP keys can be imported into the keyring by uploading a key file or by searching for a key on a remote PGP key server.

Key selection

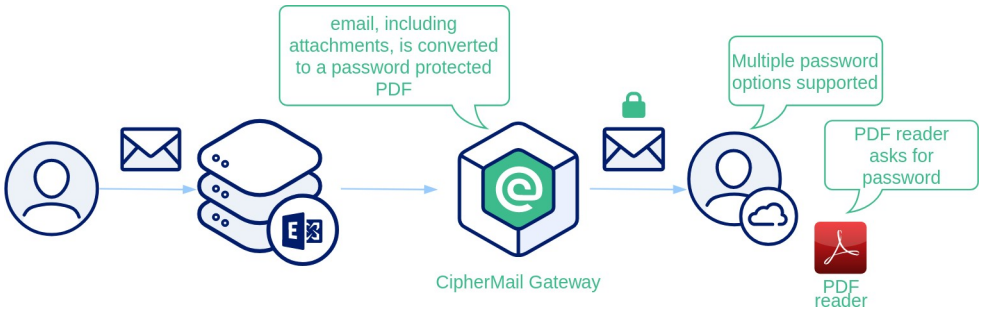
The Gateway will automatically select the keys for encryption and signing. Whether or not a key is used for encryption and/or signing depends on several factors.

A key will be used for encryption if the following key requirements are met:

- The key must be trusted
- The key must not be expired
- The key must not be revoked
- The email recipient must match an associated email address or domain of the key
- The key must be valid for encryption

PDF Messenger

A problem with S/MIME and PGP is that the sender and recipient require an S/MIME certificate or PGP key. Although installing a certificate and a private key is not hard, even less so when using the Gateway’s built-in CA functionality, for most recipients getting a certificate and configuring the mail client is too difficult.



PDF encryption is a lightweight alternative to S/MIME or PGP. With the PDF encryption module, the complete email, including all attachments, is converted into a password-protected PDF document. The password-protected document is then sent to the recipient. The recipient can open the document using a standard PDF reader.

The password for the PDF document should then be securely delivered to the recipient.

Password modes

The Gateway supports the following “password modes”:

- The PDF document can be encrypted using a predefined static password.
- The document can be encrypted using a randomly generated password. The password will be sent back to the sender of the message.
- The document can be encrypted using a randomly generated password. The password will then be sent by SMS Text to the recipient.
- The document can be encrypted using a one time password (OTP) algorithm.

TLS

The Gateway uses Postfix (MTA) for sending and receiving email. The connection to another SMTP server can be protected with TLS (TLS version 1.2 and 1.3 are supported).

The main difference between TLS and S/MIME or PGP is that TLS only encrypts the communication channel and not the email itself. With TLS, if the email is stored on a mail server, it will be stored in plain text. With full message encryption like S/MIME or PGP, the email itself will be encrypted. However, S/MIME or PGP do not encrypt the communication channel. The meta information, like sender and recipients will therefore not be encrypted. It is therefore advised to combine S/MIME or PGP with TLS.

The default client TLS policy will connect to external SMTP servers via TLS if the other SMTP server supports TLS. This is known as opportunistic TLS.

Connecting to an SMTP server without TLS or without validating the certificate can result in a “man in the middle” attack. If a connection to an external SMTP server should only be set up if the connection is trusted, an SMTP TLS policy for that domain should be configured.

An SMTP TLS policy will determine whether a connection to another SMTP server should be TLS-protected and if so, what level of validation is required.

The following TLS policies are supported: none, may, encrypt, dane, dane-only, fingerprint, verify and secure.

Digital signatures

Outgoing email can be digitally signed (with S/MIME or PGP). By digitally signing email, you can protect the integrity (protect against modification) and the authenticity (validate the identity) of the email. To validate an S/MIME signature, the recipient requires a mail client that supports S/MIME like Outlook, Thunderbird, IOS Mail, or Gmail. The recipient does not require an S/MIME certificate. The Gateway can be configured to automatically generate a key and certificate for the sender if the email must be signed. The certificate can be issues by a trusted remote CA like Global Sign or D-Trust.

DLP module

The CipherMail Data Leak Prevention (DLP) module prevents certain information from leaving the organization unprotected. What information this is, is defined by the DLP patterns. Typically, it includes credit card numbers, bank account numbers, excessive amounts of email addresses or other personal information in one email message, etc.

The DLP module can monitor various email aspects:

- email body content
- email headers
- email attachments of various types
- nested attachments of various types

The DLP module currently filters email bodies, attachments and nested attachments of type text, html, xml and other text-based formats. Filtering attachments of type pdf, doc, xls etc. will be part of a future offering of CipherMail DLP.

Configuring DLP is done via the web interface. You can specify keywords and sentences that outgoing email messages should not contain. More elaborate filtering is achieved via “regular expressions” which is a specification format that allows you to specify virtually any combination of characters, words or sentences that should be filtered.

DLP scanning can be configured on three levels: at Gateway level, at domain level and at individual user level. The latter is useful in specific cases where some users can send out information via email that other users cannot.

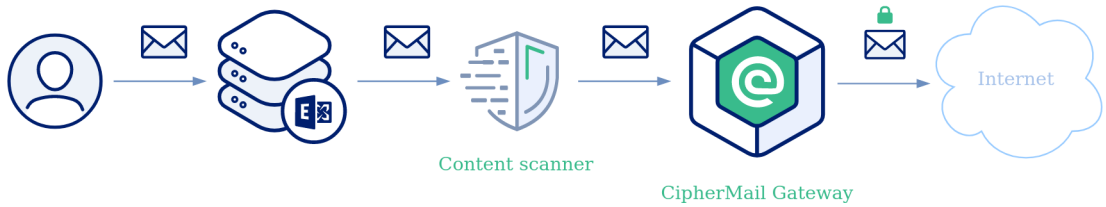
If a DLP rule is violated, the following actions can be executed: Warn, Must Encrypt, Quarantine or Block.

Network Architecture

The CipherMail Gateway is typically installed as a store-and-forward server. There are multiple ways the Gateway can be placed within the existing infrastructure. The following setups are the most typical setups.

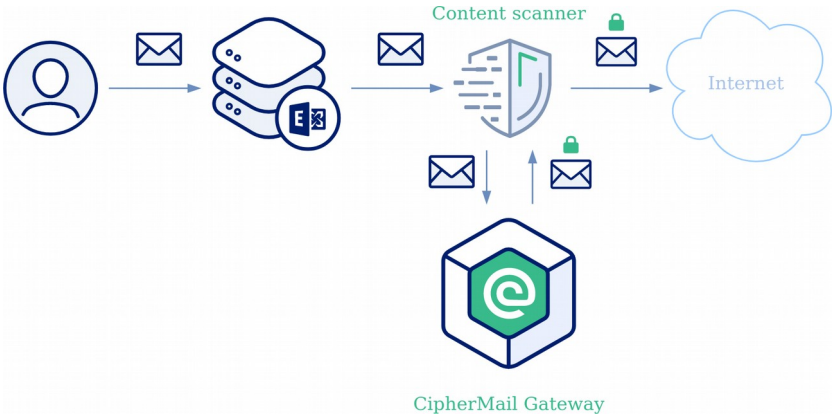
After-content scanner

In this setup the CipherMail Gateway is placed between the content scanner and the Internet. This allows outgoing email to be scanned for viruses, spam and sensitive or confidential information before the email gets encrypted, and incoming email to be scanned after decryption.



Content scanner with redirect

In this setup the CipherMail Gateway is placed below the content scanner. If the content scanner detects that email must be encrypted, for example because of deep email inspection, the content scanner sends the email to the CipherMail Gateway for encryption. The CipherMail Gateway, after encryption, sends the email back to the content scanner. The content scanner then sends the email to the final recipient. Incoming email that is S/MIME or PGP encrypted will first be delivered to the CipherMail Gateway for decryption. The CipherMail Gateway will then send the email back to the content scanner where it will be scanned and, if approved, will be delivered to the internal user's inbox.



Domain-to-domain encryption

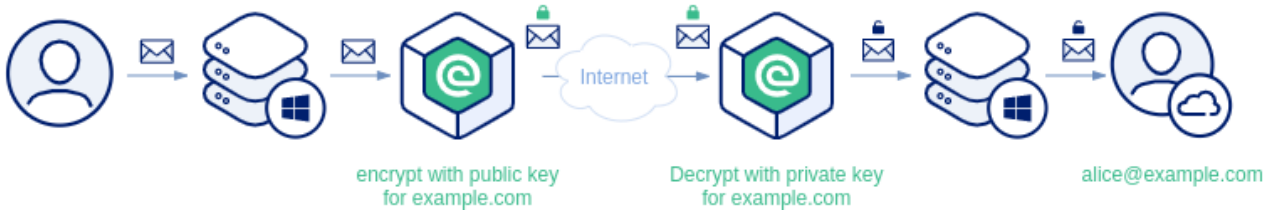
With domain-to-domain encryption, the Gateway is configured to encrypt every email sent to a specific recipient domain with a domain certificate or PGP key. Domain to domain encryption, once configured, is the easiest and most transparent setup for end-users because every email is automatically encrypted and decrypted.

Domain-to-domain encryption is sort of like an SMTP TLS connection. The main difference is that with domain-to-domain encryption, the email is encrypted and not just the connection.

The requirements for domain-to-domain encryption are:

- Both sender and recipient organization need an email encryption server that supports S/MIME or PGP domain-to-domain encryption.

- Both sender and recipient organization need an S/MIME certificate or PGP key that is used for domain-to-domain encryption.



High Availability

The CipherMail Gateway Enterprise Cluster uses an active/active database cluster (MariaDB) to replicate all changes in real time between the active cluster nodes. The majority set of nodes that can communicate with each other over the network form a cluster. In case of a network partition, i.e., a split between nodes, the majority of nodes (quorum) that can access each other will form the cluster. The nodes that got split off from the cluster will no longer be valid and will stop accepting connections. The CipherMail Email Encryption Cluster requires a minimum of three nodes.

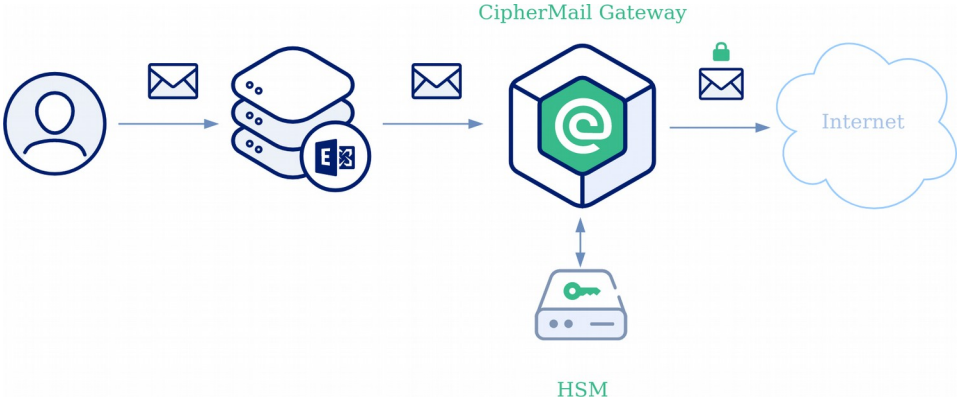
To reach the highest level of availability, each node should be placed on a different data center. For example, Azure provides three availability zones per region. Each availability zone is hosted in a different data center. By using a different data center per node, the Gateway keeps functioning even if a complete data center goes down.

Hardware Security Modules (HSMs)

Like any application that uses private keys, there is always the issue of how to securely store sensitive private key material. The CipherMail Gateway stores all settings, including keys and certificates, in a database. The benefits of storing all data in a database is that it makes it easy to create backups, provide full clustering and fail-over etc.

Even though all sensitive data, like private keys, are encrypted with a configurable password, anyone with access to the database contents and the system password might be able to get access to the private keys. This is not specifically a problem of the CipherMail Gateway. Any application that uses private keys and does not use specialized hardware to securely store the private key material has the same problem. It is therefore important that access to the database is only allowed to authorized personnel and that system backups of the Gateway are encrypted with a strong password.

To make sure that private keys can never be copied, even with full physical access, a Hardware Security Module (HSM) can be used. An HSM is basically a big smart card. It generates private keys directly on the device and stores the private keys on tamper-proof hardware. An HSM also provides additional security functionality like a built-in secure random generator. For FIPS 140 level 2 and up, an HSM is required because FIPS 140-2 requires physical security mechanisms.



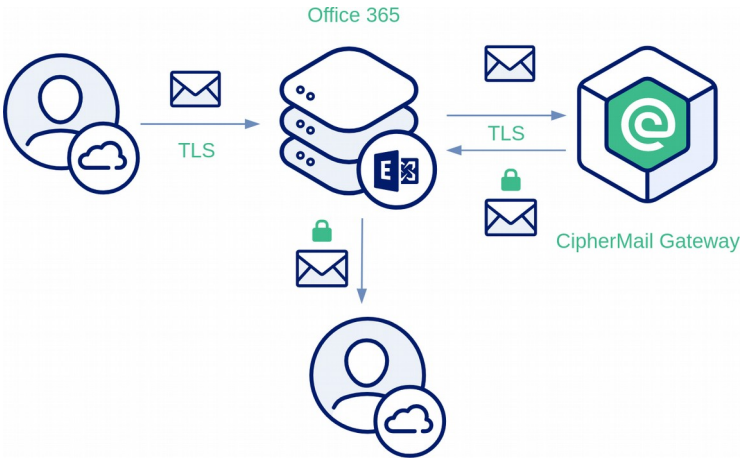
HSMs from the following vendors are supported:

- nCipher
- Thales (formerly Safenet)
- Utimaco
- Securosys

Securosys also provides HSMs as a service (Cloud HSM).

Office 365 integration

In this setup the CipherMail Gateway is configured as a relay for Office 365 (O365). Email from Office 365 to external recipients is relayed via the CipherMail Gateway. After encryption, the CipherMail Gateway sends the email back to Office 365. The Office 365 SMTP servers will then deliver the email to the final recipients. For decrypting incoming email, email will first be delivered to Office 365. Office 365 will then deliver the email to the CipherMail Gateway for decryption. After decryption, the CipherMail Gateway will deliver to email back to Office 365. Office 365 will then deliver the email to the inbox of the user.



The main benefit of this integration is that O365 will still be responsible for anti-spam/virus scanning. By utilizing Office 365 content scanning rules, email can be selectively sent to the CipherMail Gateway, allowing you to apply your own security policies.

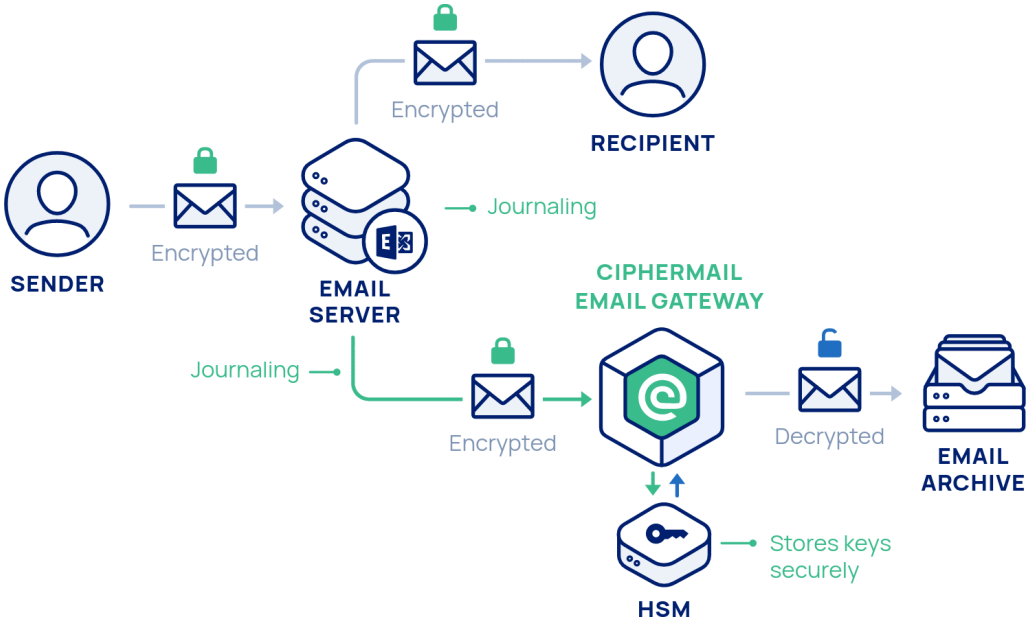
Email archiving & eDiscovery of encrypted email

There are various legal rules requiring emails to be archived for several years (for example HIPAA and SEC). If an encryption system is used, then all email can be archived in plain text, i.e., without encryption. However, if internal email is encrypted, for example because email is encrypted on the desktop with Outlook, those emails will automatically be archived in encrypted form.

Storing email in encrypted form might be problematic when emails must be retrieved from the archive. To read the contents of the email, the correct private key is required for decryption. To make sure that every email can be read from the archive, all private keys must be backed up.

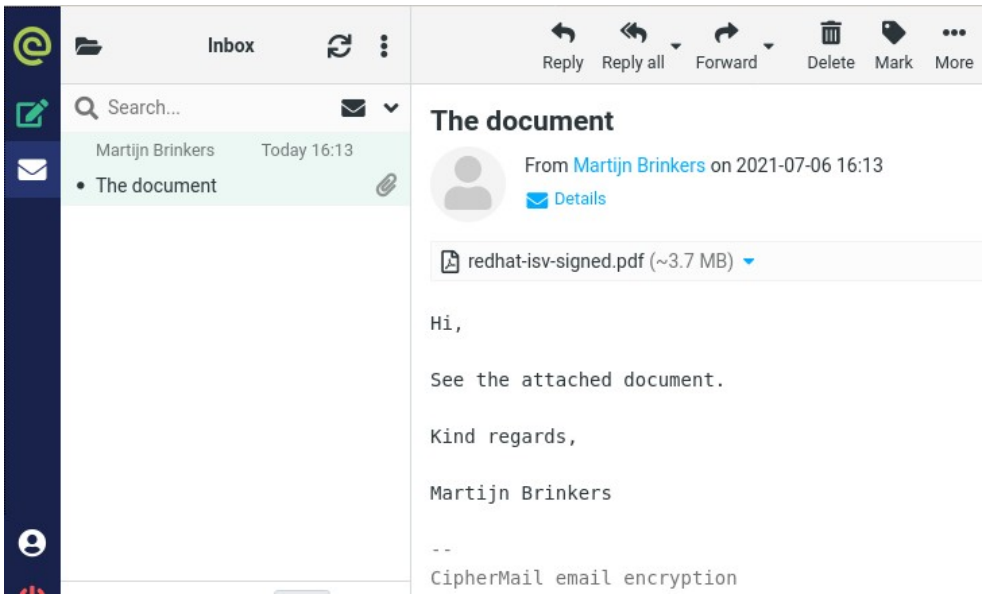
For small organizations this might be doable. For larger organizations however, making copies of all private keys might be more problematic. Even if the company manages to back up all private keys, there might still be problems adhering to eDiscovery rules. Searching the archive for specific content is not possible unless the archiving solution has access to all private keys.

Instead of archiving encrypted email, a better solution is to use the CipherMail Gateway to decrypt all email before archiving. This way, you do not need to keep a backup of all encryption keys and you can be certain that all email can be read from the archive. The Gateway can decrypt emails generated from an Exchange journaling rule.



Webmail Messenger

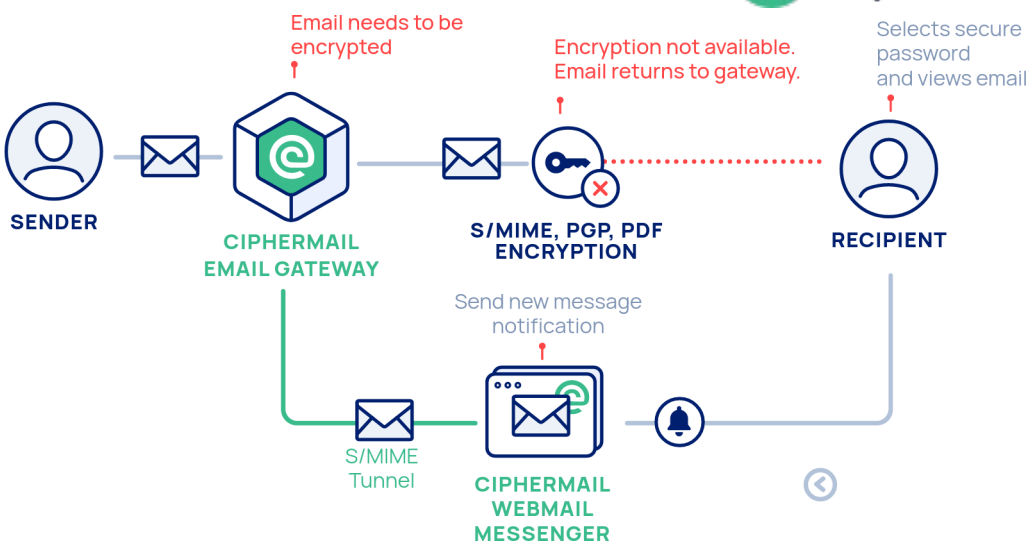
CipherMail Webmail Messenger is a practical solution to communicate securely with external recipients who are unable to use S/MIME or PGP.



Webmail Messenger Inbox

Webmail Messenger is a secure pull delivery webmail add-on to the CipherMail Email Encryption Gateway. If the rules of the CipherMail Gateway determine that a message must be encrypted, and S/MIME, PGP or PDF cannot be used, the email will be sent to the CipherMail Webmail Messenger box via an S/MIME secured tunnel. The recipient gets a notification that a new message is available. The first time the user receives a message, the user needs to select a secure password. The user can read and reply to the message using any web browser.

Webmail Messenger can be configured as an add-on to the Gateway or can be installed as a stand-alone application.



Features

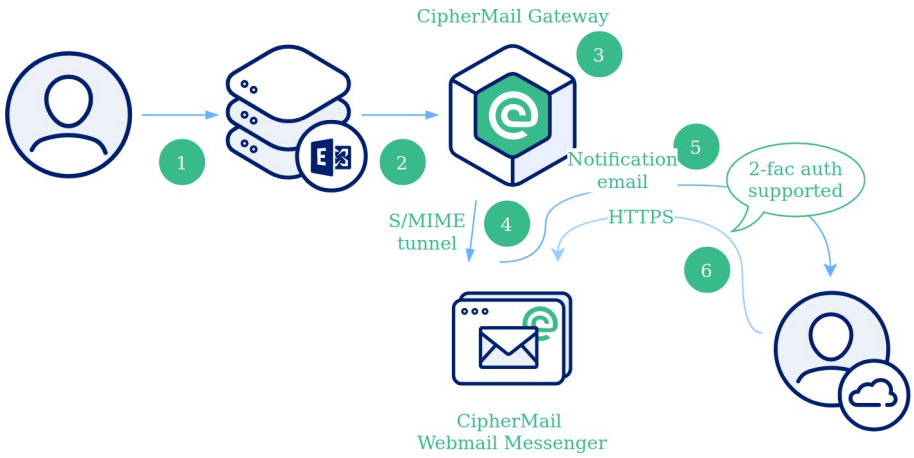
- Easy to use for end users
- Supports all major browsers and mobile devices
- Support for multiple languages
- Automatically managed
- Read confirmation
- Two-factor authentication
- Available as a Virtual Appliance for VMware, HyperV, Azure, Digital Ocean, Open Virtualization Format (OVF)
- RPM packages for RHEL8

Network architecture

Webmail Messenger can be configured as an add-on to the CipherMail Gateway or in stand-alone mode. When Webmail Messenger is configured as an add-on to the Gateway, the Gateway decides whether an email should be sent via Webmail Messenger. In stand-alone mode, all email relayed via Webmail Messenger will be sent via Webmail Messenger.

Add-on mode

In this setup CipherMail Messenger is configured as an add-on to the CipherMail Gateway. The CipherMail Gateway decides whether email should be sent via Webmail Messenger.



1. User sends an email via Exchange (or some other mail server)
2. Exchange forwards the email to the CipherMail Gateway.
3. A rule on the CipherMail Gateway decides that the email must be delivered via Webmail Messenger.
4. The email gets S/MIME signed with the webmail sender key and encrypted with the webmail recipient certificate and forwarded via email to Webmail Messenger. Webmail Messenger decrypts the mail, checks the signature and places the email in the mailbox of the recipient(s).
5. A notification email is sent to the recipient.
6. The user logs in, using 2-factor authentication if enabled, with a browser via HTTPS and reads the email online.

Stand-alone mode

In this setup CipherMail Messenger is configured in stand-alone mode. The mail server connecting to CipherMail Messenger should have some rule that decides whether email should be sent via Webmail Messenger.

1. User sends an email via Exchange (or some other mail server)
2. Some rule on Exchange decides that the email should be sent via Webmail Messenger.
3. A notification email is sent to the recipient.
4. The user logs in, using 2-factor authentication if enabled, with a browser via HTTPS and reads the email online.

Contact information

CipherMail B.V.

Email: info@ciphermail.com

Tel: +31 20 290 0088

Postal address

Tweede C. Huygensstr. 50-I
1054 CV Amsterdam
The Netherlands

Visiting address

Jacob van Lennepkade 334-R
1053 NJ Amsterdam
The Netherlands