CompuMail Gateway

Technical whitepaper

2019

E-Mail

Encryption

Compumatica SECURE NETWORKS

Cybersecurity with a personal touch

English

> ‘‘Every innovative company runs the risk of falling victim to industrial espionage’’

// E-mail today

Today, e-mail is by far the most frequently used application in the Internet – also referred to as the Internet’s “Killer application”.

E-mail is increasingly replacing letters and the telephone as a means of communications between organizations or between an organization and its customers. There is also a sharp decline in the use of fax machines as communications tasks are taken over by e-mail.

Unfortunately, e-mails do not offer any degree of confidentially. If you send a postcard, you are at least aware that the post office staff may well read your massage, but the possible risks of your e-mails being read by unauthorized outsiders are much, much higher.

Unlike a fax going directly from the sender to its recipient, e-mails pass through many stations on their way across the world, over the Internet, and they can be captured, read or even changed at any of those stations. There are usually run be different operators (providers, telecoms companies, online services or universities).

As a result, the information that is so critical to your business (and therefore also worth protecting) is processed on these servers.

Sensitive or confidential information can therefore easily fall into unauthorized hands if it is transmitted without first being protected.

In addition, anyone who receives an e-mail cannot be sure that the contents of this electronic letter **have reached them in their original state.**

Anyone who can read third party e-mails on a server is also in the position of being able to change or falsify its contents. It is not only the text of an e-mail that can be changed, but as well the sender details. This opens the way for hackers and criminals to create and use false identities.

Economic and industrial espionage becomes much easier if e-mails are transferred without first being encrypted. Every innovative company runs the risk of falling victim to industrial espionage. Data theft is a very real danger!

This places your company secrets and your intellectual property in danger, and in the worst case scenario, your entire company is at risk.

Due to the Internet, industrial espionage is really becoming a ‘big business’ – however, the resulting damage from this trend can be effectively countered, or at least considerably educed, by using properly protect IT system

"The security of your data is our mission - Cybersecurity with a personal touch"

// Table of Content

"The CompuMail Gateway ensures confidentiality intergrity and authenticity"

// CompuMail Gateway

The e-mail exchange is the most used Internet application. The electronic exchange of information within a company does not necessarily reflect its specific organizational structure.

For some procedures, possibly bearing far-reaching consequences, it should be handled this way. The usage of encrypted and signed e-mails is absolutely imperative, especially with regard to representation arrangements, processing of documents distributed to several people or issuing of receipts. But cryptographic operation can constrict the workflow, especially if bound to single persons or workplaces.

This is the starting point of the CompuMail Gateway. It is centrally integrated into the network and allows the application of a central company directive regarding the distribution of e-mails as well as the application of cryptographic operations. It is thus possible to implement both encryption and signing of e-mails in a way that is perfectly transparent for the users.

A hardware Security Module is available for secure storage cryptographic keys within the CompuMail Gateway.

System overview

According to the concept of 'common point of trust', the CompuMail Gateway is centrally located within the network.

It encrypts and/or signs outgoing e-mails and decrypts and verifies incoming e-mails respectively - if necessary. The CompuMail Gateway ensures confidentially (encryption), integrity (signature) and authenticity (signature verification) for the entire e-mail communication.

PDF Mail

Another possibility to send encrypted e-mails to external recipients who do not have a certificate based infrastructure in place is offered by PDF Mail. The recipient does need a PDF reader only (Adobe Reader® as of Version 7 recommended), in order to be able to decrypt an e-mail secured by PDF Mail. Nearly all computers installed in companies or public authorities do cover this prerequisite.

Figure 1: Process of CompuMail Gateway within network infrastructure

"The outgoing e-mail can be encrypted automatically"

// Functionality

The CompuMail Gateway is an enhancement of already used e-mail infrastructure, enabling defined user groups or single users to encrypt and sign their e-mails automatically before sending them.

Both operations can thereby be implemented in a transparent and interactive manner for the user. As for the interactive option the CompuMail Gateway is controlled by the user by using keywords in the subject line of the e-mail.

Even though receiving encrypted e-mails, the user can see them in clear text due to the automatic decryption procedure. The security status of the original e-mail can be

reported to the recipient. Encryption, decryption, signature and verification run in a transparent manner for the user. If the certificate of a recipient is available, the outgoing e-mail can be encrypted automatically. Due to the central storage of incoming certificates, encryption is still possible even in absence of a previous direct contact between the communication partners.

The centralized verification of certificates acts as a common point of trust within the company. Gateway rules for processing incoming or outgoing e-mails are as well centrally administered.

The e-mail system is attached to the operating system and is configured by using the web management. It is the actual functionality of the CompuMail Gateway.

E-mails procedure

E-mails are processed by the CompuMail Gateway in a three-step procedure:

- **Receiving of e-mails**
- **Processing of e-mails (encryption, signing, etc.)**
- **Sending of e-mails**

For implementing those three steps in a sturdy and secure manner each step is realized within an individually assigned process:

- **Receiving of e-mails: ESMTP proxy**
- **Processing of e-mails: SMTP daemon**
- **Sending of e-mails: MTA (Postfix)**

The architecture is shown in the block diagram.

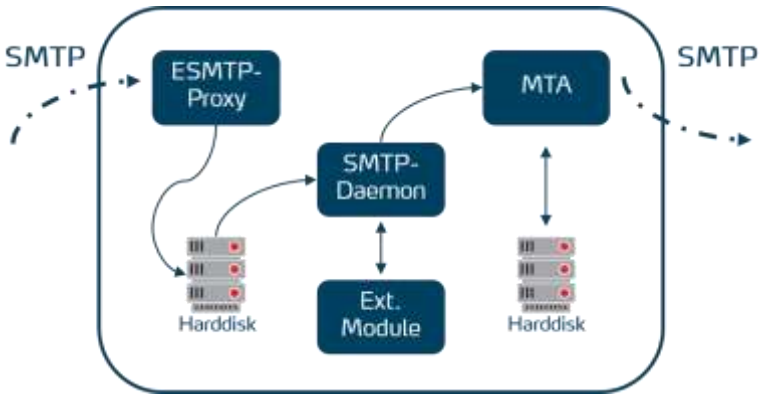


Figure 2: System architecture of the e-mail system

"Received e-mail are stored on hard disk for being processed by the SMTP daemon"

// SMTP daemon

The SMTP daemon checks the hard disk for new e-mail regularly. For each e-mail a new process is initialized, which is responsible for the further processing of the e-mail. The e-mail processing is divided into two steps:

The first step decides which rules have to be considered for the further processing of the e-mail. When selecting the rules the following conditions are evaluated:

- **Sender address**
- **LDAP attribute for the sender**
- **Is the sender licensed?**
- **Recipient address**
- **LDAP attribute for the recipient**
- **Is the recipient licensed?**
- Further properties of the e-mail:
  - Size
  - Attachments
  - Priority
  - Sensitivity
  - is encrypted
  - is signed

It is also taken into account which kind of encryption is possible, i.e. if an S/MIME certificate or an OpenPGP key is available for the recipient or none of both. Since the rules respectively the kind of encryption may differ for different recipients of an e-mail each recipient is treated separately.

Afterwards, the actions which have been defined in the selected rules are performed during the second step. The following possible actions are defined:

- **No processing**
- **Acknowledge the sender**
- **Send alert**
- **Automatic generation of keys**
- **Encryption and Signature**
- **Decryption and verification**
- **Forwarding**
- **Deleting of the e-mail**
- **Back to sender**
- **Add header field / Delete header field**

The SMTP daemon supports various transformations which are implemented internally (i.e. S/MIME, OpenPGP). The OpenPGP implementation is based upon GNU Privacy Guard (GPG: http://www.gnupg.org/). This program is included as a standard tool within the system and is called by the SMTP daemon. The communication between the SMTP daemon and GPG takes place via command line parameters as well as standard input and output.

"Received e-mails are stored on hard disk for being processed by the SMTP daemon"

// ESMTP Proxy

The ESMTP Proxy listens on port 25 and accepts connections from e-mail servers. Thereby, the extended SMTP protocol for the e-mail transport is supported.

The ESMTP-Proxy proves by means of its rule type if connections to the external (i.e. sending) e-mail servers may be established and which conditions are valid for those connections. The adequate connection rule is chosen according the following criteria:

- **IP address of the external mail server**
- **Local IP address of the established connection**
- **Local TCP port (in general 25)**

By means of selected connection rules, the following aspects are proved or filtered:

- SMTP commands used
- ESMTP options used
- E-mail sender
- E-mail recipient
- 'Received from lines' in the e-mail header

The following aspects can be globally configured:

- Timeout
- Maximum e-mail size
- Maximal number of recipients per e-mail
- DNS check up for the external e-mail server
- DNS check up for the recipient
- Log file entries

The ESMTP proxy supporters the SMTP protocol (Simple Mail Transfer Protocol) according to RFC 2821 as well as the following ESMTP options:

- Option SIZE according to RFC 1870
- Option DNS according to RFCs 1891 and 1894
- Option 8BITMIME according to RFC 1652
- Option CHUNKING according to RFC 1830
- Option BINARYMIME according to RFC 1830
- Option CHECKPOINT / RESTART according to RFC 1845
- Option ETRN according to RFC 1985
- Command EHLO according to RFC 1651
- STARTTLS

Received e-mails are stored on hard disk for being processed by the SMTP daemon. A direct access from the ESMTP proxy to SMTP daemon or MTA is not possible.

"The MTA is used for forwarding processed e-mails via the ESMTP protocol"

// Mail Transfer Agent (MTA)

The MTA (Mail Transfer Agent) is used for forwarding processed e-mails via the ESMTP protocol. Within the gateway the program "Postfix" is used as MTA. The MTA can only by addressed locally and not directly from the outside.

MTA's tasks are:

- **Sending of e-mails via ESMTP to the next e-mail server or to the recipient**
- **Caching of those e-mails which cannot be delivered immediately. This takes places on the local hard disk.**

The MTA queries the responsible e-mail server for each recipient via DNS whereas the administrator can still overrule the DNS queries with a mailer table.

"Classic e-mail providers offer no secure possibility to prove the origin of an e-mail"

// Signature services

Two major problems regarding modern e-mail communication are authenticity and integrity. Although differentiating between e-mails and written documents, users have increasing confidence in the e-mail communication. Thus, a severe, damage could emerge, if faked e-mails misled the user.

Classic e-mail providers offer no secure possibility to prove the origin of an e-mail. By means of digital signature the origin (sender's digital signature) may be verified in a secure and easy-to-understand way.

"E-mail encryption is an important mechanism to use e-mail communication without taking security risks"

// Encryption services

Along with the authentication, confidentiality is a basic aspect of modern e-mail communication. Due to its convenience, it is invisible for the user whether an e-mail remains within the secure network of the company or whether e-mails are led through insecure, public networks. The world economy empowering teleworks and outsourcing makes the situation even more critical.

E-mail encryption is an important mechanism, enabling companies to use e-mail communication without taking security risks.

Advantages of a central Gateway for e-mail security

The classic approach for securing e-mail infrastructures provides a decentralized solution. Each user is provided with a "secure" e-mail software.

By means of a central PKI (Public Key Infrastructure) all users are provided with their own and with external keys. That implies a highly unitary, i.e. compatible technology on the user's side, which widely applies to the Windows-based workstation for instance.

But the latter is not an appropriate solution for mobile field workers and web mailers. Thereby, the coverage of mobile staff members is of outstanding importance.

Due to the central approach of the CompuMail Gateway, PKI functionality can be implemented fast and easily. Secure of data has been taking place via cost-intensive archiving complete security instead. By using the CompuMail Gateway and the time signatures, the protection and security of data are based on background procedures.

"Security is no one-on-one decision any longer"

Core advantages:

- The broadly reduced complexity via a central arrangement as well as
- User-friendliness, because no additional software has to be used or taught in addition at the user's side.
- No complicated, decentralized rollout scheduling and high maintenance costs on the user's part (updates, patches).
- At the same time the problem of "key/message recovery is addressed
- Consistent implementation of a company's security policy.
- Security is no one-on-one decision any longer
- Vacation replacement easy to realize.
- External filtering devices protection against virus and spam can be applied easily.
- Role-based administration
- Private/public key methods (OpenPGP and S/MIME) External communications partners, who have no secure e-mail infrastructure for exchanging encrypted e-mails (S/MIME, OpenPGP), can communicate by means of PDFMail.

The central gateway is able to decide transparently for the user how an e-mail is securely transported to the desired recipient. Sender and recipient can concentrate on their daily work.

Increased interoperability with external systems delivers a vital impulse to the company. Significant inhibition is overcome.

"The CompuMail Gateway is integrated into the existing IT infrastructure"

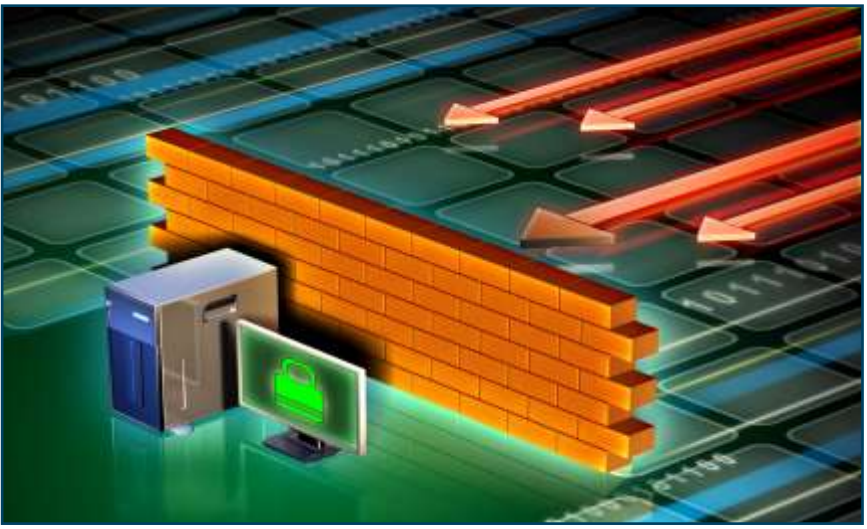
// System architecture

The CompuMail Gateway is designed to be an appliance solution consisting of e-mail gateway application and an underlying operating system based on Linux. It delivers a fully integrated overall solution to the user, without generating hidden costs for additional software components (e.g. operating system, database) and the integration of the particular components.

The CompuMail Gateway is integrated into the existing IT infrastructure, working as an SMTP-based e-mail gateway. Normally, it is located between the central firewall and the internal e-mail server. This central firewall provides the gateway to the Internet and is responsible for the central surveillance of the entire outgoing and incoming communication. The firewall should only allow the CompuMail Gateway to send or receive e-mails.

The internal e-mail server provides the connection of modern e-mail workstations. This can as well mean an integrated messaging solution like Lotus Notes or Microsoft Outlook. The internal e-mail server processes the entire communication with external e-mail addresses by using the CompuMail Gateway.

Figure 3: Overview



"CompuMail Gateway is based on the Operating System CentOS"

// The operating system

CompuMail Gateway is based on the Operating System CentOS, which is freely available. For further information on CentOS we refer to the respective website.

Clustering

Developing the CompuMail Gateway we also considered the still growing need of clustered systems on the customer's side. Keeping down-times as small as possible, the loss of configuration data and smooth workflow inside the SMTP chain are only some reasons why one should think of clustering important servers.

Clustering with internal database

If – in contrast to clustering based on an external database – a realization of a cluster of CompuMail Gateways without an external database shallbe integrated into a given infrastructure all necessary information (certificates, keys, policy, etc.) is replicated between those two gateways.

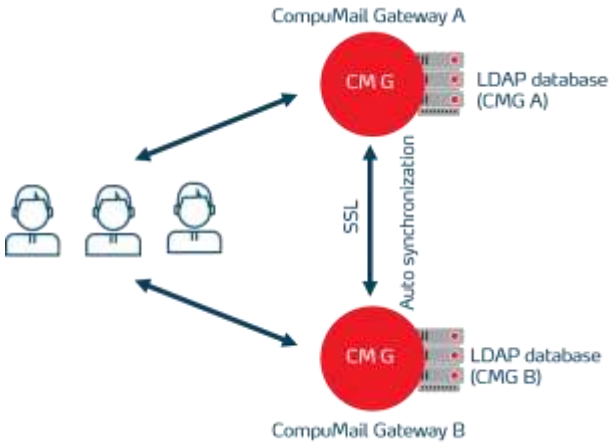


Figure 4: Cluster of two e-mail Gateways

Extending such sort of realization by more than two gateways lets the first two act as the external database for the others. Thus, in case of failure of one of the gateways one of the others will take over. No interruption of service will appear and no configuration will be lost.

Figure 5 show the connections between the members in a cluster are protected.

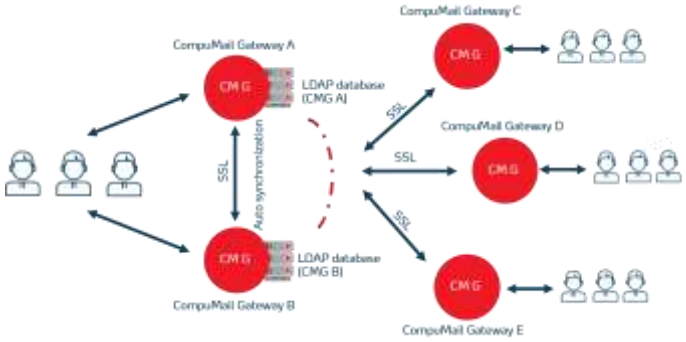
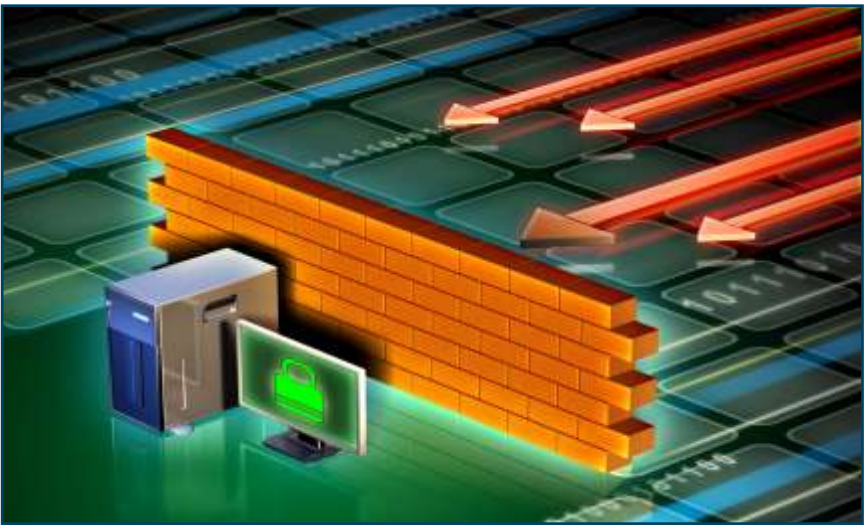


Figure 5: Distributed cluster



"Two different scenarios to run a cluster, centralized or decentralized"

Clustering based on an external database

This chapter depicts the realization of a cluster of CompuMail Gateways using an external database. There are two different scenarios running a cluster:

- centralized or
- decentralized

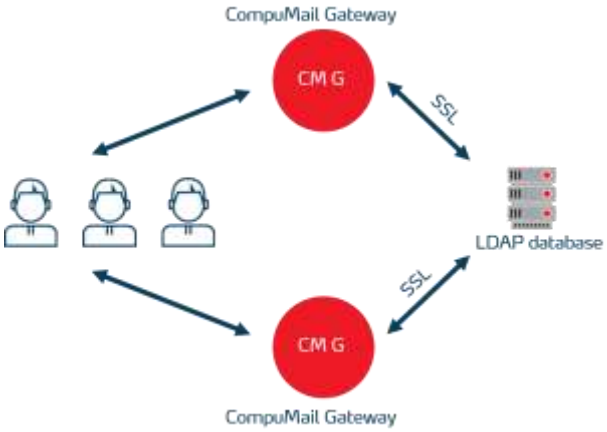


Figure 6: Cluster with external database

Figure 6 shows a logical sketch of a cluster that is run in one location. The external database server is connected to the two gateways via LDAP (Lightweight Directory Access Protocol). Keys, certificates and policies configured on the gateways are stored in the database and it is possible to just change parts on the configuration on one gateway in order to transfer these changes to the other one.

Figure 7 shows the decentralized approach of a cluster. A cluster of five CompuMail Gateways running in four different locations shares one central database.

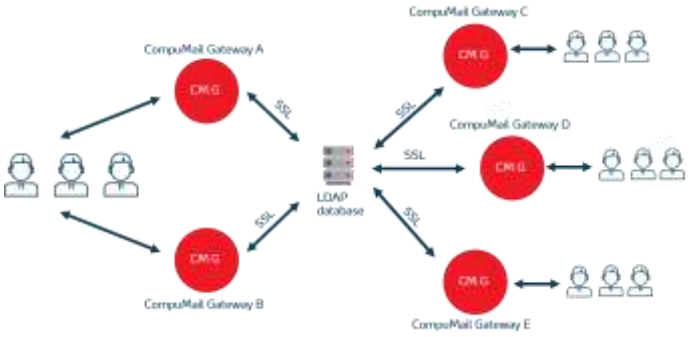


Figure 7: Distributed cluster with external database

It would be reasonable to have the central database server in a cluster of two machines as well. The concrete configuration of the cluster of the databases may differ regarding the database system that is used. Several customers running the CompuMail Gateway use OpenLDAP for the realization of such a clustered database.

"It is possible to integrate external user databases both online and offline"

// Administration

Web management

The costs for maintenance and processing often exceed the costs of acquisition. For that reason, those costs have to be particularly considered when deciding on investment opportunities. This term is generally described as Total Cost of Ownership. Costs of operation and maintenance are very low for the CompuMail Gateway.

Connection to a central company directory

Along with the administration of all users within the CompuMail Gateway, it is possible to integrate external user databases both 'online' and 'offline'.

In the case of online integration, access is provided via LDAP (e.g. access to user-assigned certificates). Furthermore, the membership in a certain MS ActiveDirectory group can be taken into account.

While using the offline procedure, the integration is based on text documents.

Policy Management

The way the CompuMail Gateway will process incoming and outgoing e-mails depends on the security policy configured on the machine. To represent a certain policy on the Gateway the so called "rules" have to be configured at this central point. The main objective in the design of these rules was to develop a tool for the administrators which gives them the highest flexibility to represent the given security policy on CompuMail Gateway.

Encryption and digital signature of e-mails can be set up very granularly and arranged in a clear way. Integration of a central company directory such as MS Active Directory (AD) is implemented in a straight-forward way. Administrators are able to define not only a single way how an e-mail becomes processed on CompuMail Gateway but it is also possible to compose rules which consist of different passes (concatenation of actions in a single rule). Hence, it is possible to define a rule which in the first step of processing an e-mail will send this e-mail to an external archiving system.

After this action is completed the second step – decryption of this e-mail – will be handled and in the last step the e-mail will be sent out to the recipient. Furthermore, CompuMail Gateway provides conditions on e.g. the e-mail address of the sender of an e-mail: An e-mail processed can become encrypted if the e-mail address of the sender is listed in the AD groups 'Member of the Board' or 'Human Resources'. This last example demonstrates at the same time that unlike other solutions which are only able to encrypt e-mails based on the recipient of a certain e-mail, CompuMail Gateway is also able to handle encryption of e-mails based on the sender of an e-mail.

Thus, it is possible to configure even the most complex requirements regarding the IT security policy of a company or an organization on CompuMail Gateway in an easy way.

"CompuMail Gateway can be integrated into different existing e-mail infrastructure"

// Example of operation

In this chapter some examples of how the CompuMail Gateway may be integrated into an existing e-mail infrastructure will be presented.

Conventional operation of the CompuMail Gateway

Figure 8: Integration of the CompuMail Gateway

Figure 8 depicts the most conventional integration of a CompuMail Gateway.

On the internal side (on the left hand side of the CompuMail Gateway) an example of an already existing e-mail infrastructure is shown. It consists of e-mail clients and server, an anti-virus filter and a solution for content-filtering. The filtering devices would – behind a spam filter – be the first ones an incoming e-mail would pass coming inside the company and the last ones outgoing e-mails would pass respectively.

Applying CompuMail Gateway stands for the extension of an infrastructure exactly at this central position. The CompuMail Gateway delivers, after a spam filter has been passed, incoming e-mails to the internal infrastructure and outgoing e-mails to your provider or directly to the Internet.

Thus, all incoming e-mails are encrypted at first and sent to the scanning servers afterwards – no e-mail will normally be delivered encrypted to the internal side; all e-mails can be scanned for viruses or for other malicious code. Outgoing e-mails are processed (signed and/or encrypted, sent in plain-text) regarding the e-mail policy that is stored on the gateway.

CompuMail Gateway as key server for external communication partners

The CompuMail Gateway can as well be used as a key-server that delivers keys and/or certificates of internal users to the outside world. Using this feature an external communication partner could get the key of an internal user before sending the first e-mail to this user. Thus, the e-mails will be encrypted starting with the first one and this principle is independent of the external sender using client-based encryption or a gateway.

The URL where one can find the certificates of the company's employees (the address of the key server company's website.

It is not relevant if the sender encrypts the e-mail on his client PC, or if on the other side also a central secure e-mail process runs.

"Decrease the work of the administrators"

Encryption up to the internal clients

One goal when applying a central solution for e-mail security is to decrease the work of the administrators. Storing the keys of the external communication partners of all internal machines and keeping all of these machines up-to-date with the newest versions of the e-mails clients and e-mail security applications used will not be necessary any more using a solution for server-based e-mail security.

But you will always have some people in the company who still need a client-based solution running in parallel (human resources department, members of the board, etc.) either due to security reasons or in order to cover governmental regulations. They will keep sure that nobody inside the company can get his hands on information they transfer via the internal LAN. There are no limitations combining these two approaches using the CompuMail Gateway.

Combination with existing client-based solutions

If there are any employees whose certificates were not yet installed on the gateway they will get all encrypted e-mails addressed to them delivered to their client encrypted as well. Thus, they must have a client-based solution in order to be able to read their secured e-mails.

The e-mail will be transferred encrypted through the internal LAN and no central devices protecting the LAN against viruses or other malicious code are able to handle such an e-mail. In this case the e-mails must be checked for viruses or other malicious code that can be present in the e-mail at the user's system itself.

Looking at this scenario the other way round, i.e. an internal sender encrypts an outgoing e-mail on his own client, the CompuMail Gateway is still able to sign this e-mail (if it holds the private key of the sender) and can be configured that way, that it would not encrypt this e-mail again – encrypting an e-mail twice does not give you any more protection than doing it just once.

An e-mail sent by an employee who does not secure his e-mail using his client and which is addressed to the same recipient will still be encrypted on the gateway.

Thus, using a hybrid solution of client-based and server-based e-mail security does not mean any trouble for the communicating partners involved.

"E-mail security up to the clients and central e-mail scanning"

E-mail security up to the clients with central e-mail-scanning

Some institutions do want to have centralized e-mail security in combination with central scanning servers. In such a case a so called 'sandwich of two gateways' can be deployed. In between the gateways in the SMTP chain the malware solutions are integrated. The advantage of such a construction is an e-mail infrastructure which offers e-mail security up to the clients (including signature check) and central e-mail scanning (viruses, spam, etc.) simultaneously. After the examination the second CompuMail Gateway encrypts the e-mails again and sends them to the internal e-mail server.

Thus, it is possible for selected people (human resources department, board, etc.) or for all staff to secure the e-mail-traffic to the client, without waiving the advantage of centralized tools to protect from threats by e-mails.

Role-based administration

Big companies or legal authorities have different people for the administration of different parts of the network – even regarding the administration of different components of one single machine. To cope with this the CompuMail Gateway offers the so-called 'Role-based administration'. Different people are given different administrational rights for different components. Looking at the predefined roles in the chart below one can see that all but the roles of an "Administrator" and an "Auditor" are disjunctive.

The predefined roles are:

Role	Description
Administrator	Unreserved rights – complete access to all components of the system
Network Operator	Administration of the network configuration
User Operator	Administration of certificates and keys of the internal and external users
CA certificate Operator	Administration of the CA certificates
Policy Operator	Administration of the services for e-mail security
System Operator	General administration of the system: ○ Changing of the runlevel ○ Monitoring the status of the machine ○ Creating back-ups ○ System configuration
Auditor	Can see everything but can change nothing – unreserved access but no ability to change any values.

In case that an auditing has to take place – conducted of an independent auditor for example – a role for an auditor has already been implemented. An 'Auditor' has access to the complete browser-based management tool but is not able to change any values whatsoever. It is kind of an 'Administrator' in read-only mode.

"The geographic processing of e-mails takes place within the SMTP daemon"

// Cryptographic concept

The cryptographic processing of e-mails takes place only within the SMTP daemon. It supports the following standards:

- S/MIME according to RFC 2633
- OpenPGP according to RFC 2440 and RFC 3156
- PDFMail protected by AES encryption. Key length is 128 or 256 bit.
- Customer specific upgrades

The following cryptographic methods are supported:

Method	S/MIME	OpenPGP	PDFMail
Asymmetric	DSA RSA Diffie-Hellmann	DSA RSA ELGamal	
Symmetric	RC4 3DES AES	3DES Blowfish Cast5 AES 128, AES 192, AES 256	RC4 AES
Hashing function	MD5 SHA1 MDC2	MD5 RipeMD160 SHA1	

Private/public key operation

S/MIME

The access to X.509 certificates is done by using the local certificate database or by external database access via LDAP. This also applies to Certificate Revocation Lists (CRL). Beside LDAP, CRLs can be accessed via http/https as well.

The usage of different certificates for encryption and signatures (key separation) is provided by the CompuMail Gateway.

Certificate check-up using OCSP

When receiving an e-mail the SMTP daemon checks a certificate chain and subsequently uses the certificate daemon (cert daemon) in order to retrieve revocation status information. The procedure runs as follows:

Figure 9: Certificate check-up using OCSP

If the SMTP daemon has to process an e-mail it starts checking a certificate chain. SMTP daemon will subsequently pose an OCSP

(Online Certificate Status Protocol) query to the cert-daemon (certificate daemon) in order to retrieve revocation status information on the processed certificate from one or several CRLs (Certificate Revocation List). In this respect the cert daemon serves as an OCSP server. The following check of the validity of certificates may take place against a local CRL, an external CRL or against revocation status information provided by an OCSP server. These external revocation lists may be addressed via the http, https or LDAP protocols. After the accomplishment of the validity check, the result is sent back to the cert daemon which will respond according to the revocation status gained during the query evaluation.

"The key management is done by the web interface"

OpenPGP

The key management is done by the web interface. Keys can be imported, exported, signed and trusted. Mass-import of keys can also be done by the web interface. Furthermore, keys can be imported from a PGP key server.

Besides LDAP the HKP protocol for queries on OpenPGP servers is supported as well.

Distribution of keys and certificates

To make it most comfortable for the internal users to distribute their keys and certificates to external communication partners the CompuMail Gateway offers the following commands. The commands are executed when added to the subject line of an e-mail.

Command	Purpose
{send_keys}	Delivered e-mail will have attached all keys, certificates and the respective CA certificates of the sender and his company.
{send_keys_pgp}	Delivered e-mail will have attached all OpenPGP keys and the respective CA certificate of the sender and his company.
{send_keys_smime}	Delivered email will have attached all S/MIME certificates and the respective CA certificate of the sender and his

CompuMail Gateway will attach the keys/certificates before sending out the e-mail.
As possible with any other subject line commands administrators are able to redefine the ones listed above as well.

Automatic import of incoming keys and certificates

CompuMail Gateway is also capable of processing incoming keys and/or certificates automatically. If an incoming e-mail has an S/MIME certificate of the sender and the corresponding CA certificate as attachments the CompuMail Gateway can detach these files from the e-mail and store both directly to its own certificate store.

Thus, the administrator does not have to act manually in case an e-mail with such certificates is sent to an employee inside the company. The CompuMail Gateway does offer this functionality both for S/MIME and OpenPGP.

> ‘‘Supported protocols for this purpose are LDAP and HKP’’

External key servers

The signature that is attached to an incoming e-mail has to be verified. In most cases the corresponding CA certificate will not be available and furthermore the actual CRL of this CA has to be checked in the very moment an e-mail arrives to be sure that this certificate is still valid.

If an e-mail signed with a certificate distributed by an official trust center (for example) arrives on the gateway the server is able to send a request to this trust center asking about the status of this certificate. Thus, the verification of signatures happens on time.

Supported protocols for this purpose are:

- S/MIME: LDAP (Lightwight Directory Access Protocol)
- OpenPGP: LDAP and HKP (Horowitz Key Protocol)

To speed up the search on these external servers it is also possible to deploy search patterns to these external servers which are known to the CompuMail Gateway. If the gateway searched for example on a server from company XYZ, it would not make sense – and sometimes make the search much slower – if it searched in such a case for any other e-mail pattern ‘*@XYZ’. Thus, the administrator would add this special pattern to the LDAP server which should be searched for certificates from employees of the company XYZ.

"CompuMail Gateway offers to send encrypted e-mails to external recipients"

// PDFMail

PDFMail is an additional method CompuMail Gateway offers to send encrypted e-mails to external recipients having no appropriate certificate infrastructure in place.

On almost every computer a reader for PDF files can be found nowadays and PDFMail is based on the file format PDF. External users receiving e-mails secured on the basis of PDFMail must have a PDF reader installed on their systems. Compumatica recommends Adobe Reader®. When an external communication partner is receiving an e-mail protected by PDFMail it works as follows:

- After the evaluation of the appropriate policy or a subject line command on CompuMail Gateway the body of the e-mail sent and all attached files are stored in an encrypted PDF file. Encryption is based on the algorithm AES.
- The recipient now receives an e-mail which has the encrypted PDF file attached.
- The sender of this e-mail receives a notice from CompuMail Gateway including the password that was used to encrypt the PDF file. This notice is also sent by e-mail. The sender has to communicate this password to the recipient, e.g. by telephone. Alternatively, self-registration is also possible.
- Using the PDF reader installed on his machine the recipient is now able to decrypt and read the protected e-mail. He can as well detach all attachments included in this e-mail.
- Clicking on the 'Reply' button included in the PDF the recipient's web browser is setting up a secure connection (based on the HTTPS protocol) to CompuMail Gateway inside the infrastructure of the sender's organization.
- Authentication is carried out using the password the original PDF document in the e-mail was encrypted with.
- After authenticating himself the external communication partner can write an answer to the original e-mail using his web browser. Attachments can be added to his e-mail as usual.
- This answer is then delivered to the initial sender and a copy of this answer is sent to the external partner. Thus, he is able to store his answer in his own e-mail client – also encrypted with the same password as the original e-mail.

E-mails exchanged between the two communication partners in the example described above are protected with the same password that was used to encrypt the initial e-mail.

"CompuMail Gateway offers to send encrypted e-mails to external recipients"

Figure 11: Example for PDF cover

The encrypted PDF file, which was sent via PDFMail, consists of two parts, a permanent and a non-permanent one. The permanent one consists of the title page and of the last page of the document. The first page of the document may be customized by the company employing PDFMail.

Thus, an e-mail protected by PDFMail can be designed according to the organization's corporate design. The last page contains a brief introduction into answering e-mails sent protected with PDFMail and the already mentioned 'Reply' button. The non-permanent part of the PDF file contains the e-mail itself and all attachments.

Passwords used to encrypt the PDF document when PDFMail comes into play are stored in the database on CompuMail Gateway. In this database a matching between the e-mail addresses of the sender, the recipient and the password securing the exchange of e-mails between those two exists. For this reason CompuMail Gateway is able to identify the external communication partners when they would like to send an answer to a received e-mail. Any consecutive e-mail exchanged between the same combination of sender and recipient is protected with the same password.

To compose a secure answer to an e-mail delivered based on PDFMail the external communication partner uses his browser. The page for this 'PDF Reply' presented by CompuMail Gateway is sown in figure 8.

> ‘‘Recipients do neither need an e-mail client having S/MIME or OpenPGP capability’’

// CompuWebmail

CompuWebmail is an extension to CompuMail Gateway. Its purpose is to enable external communication partners to be able to receive encrypted e-mails without having the necessary tools in place which are usually needed. So, the recipients do neither need an e-mail client having S/MIME or OpenPGP capability nor do they have to install a single piece of software on their computer. They only need a conventional browser.

Mode of Operation

The following steps are performed to integrate an external recipient to the secured communication provided by CompuWebmail:

The internal user sends an e-mail to an external recipient who doesn’t have a user account on the CompuWebmail yet.

Given a matching rule that this e-mail has to be sent to CompuWebmail it is routed to that server by CompuMail Gateway.

- CompuWebmail automatically creates a user account for this recipient and stores the e-mail into that account. At the same time a password for this account is generated.
- The password is sent back by the CompuWebmail to the internal sender. He now has to get in contact with the recipient, for example by telephone, to submit the password to the external recipient.
- The external recipient gets an e-mail by the CompuWebmail containing the weblink (HTTPS) which the recipient has to open in his browser. As user name the e-mail address is used.
- Now the recipient is able to log on to CompuWebmail by means of his user name and password. After the first login the user has to change the password received from the internal sender. Afterwards, the external recipient gets access to his mail box on CompuWebmail and can participate in the secured e-mail communication with organizations of the sender.

"CompuWebmail is integrated into the DMZ of the IT infrastructure at the customers site"

A new account on CompuWebmail can only be generated by internal users of the organization which uses the product. Every time an e-mail is sent to an existing account the recipient also receives an e-mail sent to his regular account to inform him that he got another secured e-mail.

So, external communication partners do not have to poll CompuWebmail on a regular basis in order to guarantee to keep up with their secured e-mails. The e-mails stored on CompuWebmail are encrypted asymmetrically.

CompuWebmail is integrated into the DMZ of the IT infrastructure at the customer's side. Thus, there is no security risk for the organization's private keys which are stored on the CompuMail Gateway.

The options of the rules for e-mail encryption on CompuMail Gateway have been extended by the option 'Webmail'. 'Webmail' can be defined as general methode for a certain rule, or be set as fall-back, e.g. for S/MIME and OpenPGP.

Extending e-mail communication by CompuWebmail does not require any software installation or further modifications of the e-mail infrastructure on the recipient's side.

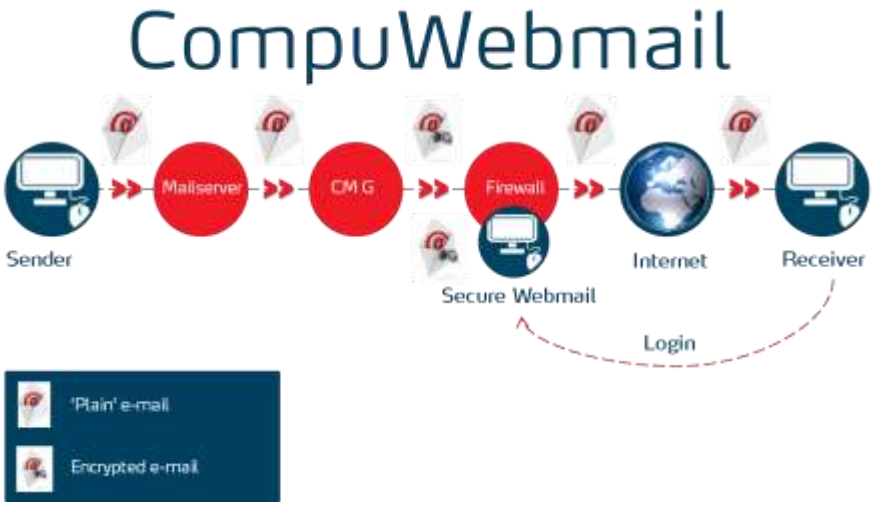


Figure 11: CompuWebmail

"Compumatica offers a temper proof key key storage as an extension"

// Secure key storage (Hardware Security Model)

If higher demands regarding the security of certificates store on the CompuMail Gateway arise, Compumatica offers a tamper proof key storage as an extension. The hardware security module SG CryptoServer by Utimaco/Sophos provides the opportunity for operations based on secret keys taking place within the tamper proof area.

SG CryptoServer is used for securing the private keys of the S/MIME certificates, thus it will be possible to encrypt these keys with an additional 'key encryption key'. Private keys will therewith be of no avail for a potential attacker as the 'key encryption key' is saved/stored inside SG CryptoServer so that it would be impossible even for the administrator to export it. SG CryptoServer is certified in accordance with FIPS 140-2 Level 3 gaining Level 4 for 'Physical Security'.

"The security of your data is our mission - Cybersecurity with a personal touch"

// Abbreviations

AD	Active Directory
AES	Advanced Encryption Standard
CMG	*CompuMail Gateway*
CA	Certificate Authority
CRL	Certificate Revocation List
DES	Data Encryption Standard
DNS	Domain Name Server
DSN	Delivery Status Notification
ESMTP	Extended Simple Message Transport Protocol
FIPS	Federal Information Processing Standard
GPG	GNU Privacy Guard
HKP	Horowitz Key Protocol
LAN	Local Area Network: Any physical network technology that spans short distances (up to a few thousand meters).
LDAP	Lightweight Directory Access Protocol
MTA	Mail Transfer Agent
OCSP	Online Certificate Status Protocol
OpenPGP	Standard for encryption and digital signature of e-mails on the Internet (based on asymmetric cryptography)
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
RFC	Request for Comment
S/MIME	Standard for encryption and digital signature of e-mails on the Internet (based on asymmetric cryptography)
SMTP	Simple Mail Transfer Protocol
TCP-Port	Transmission Control Protocol-Port
UMTS	Universal Mobile Telecommunications System

"The security of your data is our mission - Cybersecurity with a personal touch"

// Short profile

Compumatica secure networks – based in Germany and the Netherlands – is a fully independent private company with main task securing IP traffic of its customers.

Compumatica develops, produces and implements high level security solutions for all types of IP networks and all types of customers. Customers can be small organizations with just a few countrywide connections up to international enterprises with world-wide networks.

Compumatica staff and products meet high standards of reliability and quality. The products are based on systems that are approved, or even certified, according to the strict regulations of the BSI (in Germany) and the NLNCSA (in the Netherlands). Every single product goes through a quality assurance phase in which it is subject to a long-term test. All Compumatica products are backward compatible for more than ten years. Herewith we guarantee our customers investment protection.

Our customers are well-known top 500 enterprises as well as government agencies and public organizations in different countries which protect their critical data with the aid of Compumatica systems.

As world-wide approved producer and system integrator Compumatica secure networks provides complete IT security solutions for networks of each size.

The security of your data is our mission – Cybersecurity with a personal touch.

"The security of your data is our mission - Cybersecurity with a personal touch"

// Contact data

The Netherlands

Compumatica secure networks BV

Oude Udenseweg 29
5405PDUden
The Netherlands

Phone: +31 (0) 413 334 668
Fax: +31 (0) 413 334 669

www.compumatica.com
info@compumatica.com

Germany

Compumatica secure networks GmbH

Monnetstraße 9
52146 Würselen
Germany

Phone: +49(0) 2405 8924 400
Fax: +49(0) 2405 8924 410

www.compumatica.com
info@compumatica.com