DTS
E-Mail encryption

E-Mail encryption

It is impossible to imagine our everyday life without communication via email. However, emails often contain confidential, sensitive and data-protection-related information. This applies not only to internal exchanges, but also to partnerships and customer relationships. Data theft and espionage often causes major damage, both economically and to a company's image. Secure exchange of emails should therefore be a top priority, especially in terms of compliance. Together with SEPPmail, a leader in this field for 20 years, we provide simple, entirely secure email communication.

- Complete security for email communication
- Complete, automatic email encryption & decryption
- Combination of established methods & patented GINA technology
- Independent selection of the most suitable encryption method
- Convenient digital email signature with user certificate
- Encrypted file transfer
- Centralized approach, easy integration & administration
- DTS managed services & helpdesk

With Secure E-Mail Gateways we provide three modules. All modules are set up and managed with a single management interface.

On the one hand, this includes automatic protection of confidential email traffic sent throughout the company (managed domain encryption) and to external recipients. Full encryption involves the best standard technologies, such as S/MIME, OpenPGP, TLS, SSL and domain encryption. Using the patented GINA technology, secure emails can also be exchanged with recipients who do not have specific software or keys. You can therefore send confidential emails easily, without knowing if and how the recipient uses encryption. The recipient only needs an email client and a web browser. With the centralized approach, the rules of this uncomplicated solution can be adapted at any time, key management involves no administrative effort, and the most suitable encryption method is always selected independently without user intervention.

On the other hand, we can sign your emails digitally. In this way, every recipient knows who the real sender is and that the email has not been modified. The certificates required for this are obtained automatically via Managed Public Key Infrastructure (MPKI) in conjunction with SwissSign, an accredited and globally recognized certification authority, assigned to the user and used to sign all outgoing emails. At the recipient's end, all emails are checked and marked. The procedure is supported by all common email clients.

In addition, we enable secure transfer of large files that are too big for traditional email. For example, databases, images, videos and print files can be exchanged in both directions using GINA technology. The data is encrypted and stored on the appliance for a predefined period of time. Mail can be sent via a plug-in or a web interface.

With email encryption, only secure emails and data are exchanged. This extremely user-friendly solution is easy to integrate and administer. In addition, the appliance is cluster-capable and scalable as required. It is no coincidence that the solution is used in a wide range of industries, including banking, finance, insurance, retail, industry and government.

Spontaneous communication with SEPPmail
With SEPPmail email encryption, entirely secure communication is possible without a second thought:

- Immediate delivery of confidential email, including attachments
- Simple process of sending the initial password (phone, etc.)
- No preparation necessary on the recipient's side, any email client or browser is sufficient
- Intuitive and fast registration (option to set your own password and security question/answer for independent password reset)
- Immediate reading and replying possible, including with attachments