



Secure Mail

E-Mail Security for Microsoft® Outlook + Office

Much of today's daily business communication takes place by e-mail. Many e-mails contain company-relevant information that should be seen only by specific individuals or groups.

Often e-mails also contain arrangements and agreements that are deemed binding by the respective contacts.

It is crucial that corporate e-mail correspondence is both confidential and binding, yet conventional e-mail clients generally cannot meet these demands. Secure Mail enhances Microsoft Outlook with encryption, decryption, and digital signing of e-mails with verification of digital signatures.

Secure Mail is designed for use in large corporate groups with heterogeneous IT infrastructures. It's ready for immediate use and can also be customized to accommodate individual requirements. Administrators can centrally manage and roll out the product and security policies, and individual users readily accept its user-friendly interface. Client Security as the Cornerstone of Your Business

Processes SECUDE products meet the need for high security in eCommerce, eBusiness, and eGovernment. Client Security provides for digital signing and encryption of documents. Digital signatures enable the authorship of electronic document contents to be authenticated. And, because only specifically selected recipients can decrypt and view the documents, electronic processes become binding and confidential.

Why Secure Mail?

Business processes are increasingly mapped electronically. This makes it essential for companies to ensure data privacy and security for everyday e-mail communications.



SECUDE IT Security GmbH
Sales, Service & Solution Center
Goebelstrasse 21
64293 Darmstadt
Germany

Tel : +49 6151 828 97 0
Fax : +49 6151 828 97 26
info@secude.com



For your company, this means:

> Confidentiality

Encryption of e-mail with the S/MIME or PGP standards guarantees the confidentiality of company e-mail.

> Integrity

The integrity of mail content is ensured by digital signatures and can be verified by the recipient.

> Identity

The authenticity as well as the non repudiation of origin by digital signatures can ensure that e-mails are legally binding.

> User Acceptance

Just two buttons – one for signatures and one for encryption – let users control the entire application.

Interoperability and Standardization

Secure Mail is a plug-in for Microsoft Outlook that provides secure e-mail communication. Strict adherence to international standards such as X.509, PKCS#11, LDAP, and OCSP ensures compatibility with other products such as Microsoft Outlook Express or Netscape Communicator. Secure Mail supports both S/MIME and PGP encryption and offers ideal interoperability with both formats. For companies, this means that communication partners can use all kinds of secure e-mail formats. For users, the selection of the correct format for secure e-mail is completely transparent. The administrator can even set the preferred e-mail standard and all other integral functions of Secure Mail from a central point of control.

Secure Mail provides the best formula for successful deployment in large companies.

Integration through Intelligent Architecture

Soft tokens, smart cards, USB tokens, and Microsoft's CryptoAPI can be used to store all necessary keys. This allows the degree of security to be tailored to individual requirements and/or to the regulations of each company.

SECUDE also demands a high level of security from the algorithms used. For this reason, internationally recognized algorithms such as RSA, DSA, AES, Triple DES, IDEA, SHA-1, and RIPEMD-160 are integrated into Secure Mail.

Secure Mail supports S/MIME, PGP, and ISIS-MTT e-mail formats. The respective format is selected automatically based on the recipient's domain. The integrated LDAP client provides access to encryption certificates not contained in the local address book. Revocation lists can be downloaded with LDAP as required, and are accessed automatically to retrieve certificate status for verification. Alternatively, users can also employ OCSP (Online Certificate Status Protocol) to retrieve certificate status.



Features:

Client:

- Microsoft Windows 2000/XP/Vista
- Microsoft Outlook 2000/XP/2003/2007

Server:

- Microsoft Exchange Server 2000
- Microsoft Exchange Server 2003
- Microsoft Exchange Server 2008

Certificate Infrastructure:

Technical Features:

Card Terminals:

- PC/SC or CT-API connection

Smart Cards:

- Deutsche Telekom (PKS 2.0/3.0, NetKey, NetKey 2000, NetKey E4)
- Deutsche Post (Signtrust SEA)
- Datev (e:secure), others via PKCS#11

SECUDE IT Security GmbH
Sales, Service & Solution Center
Goebelstrasse 21
64293 Darmstadt
Germany

Tel : +49 6151 828 97 0
Fax : +49 6151 828 97 26
info@secude.com

