

Secure E-Mail



Benefits

- Guaranteed authenticity and integrity of e-mails
- Our transparent solution takes a burden off your staff
- End-to-end security is guaranteed
- No need to train your employees
- No need to install any software
- Integrates easily into Outlook, Lotus Notes, Mozilla etc.
- Prompt integration
- Based on standards
- Users can decide which e-mails to sign and/or encrypt
- Low administrative requirements

Electronic communication as a strategic success factor

Today, e-mail is by far the most widely used online application. E-mail is increasingly replacing conventional means of communication such as traditional mail and telephone. The use of faxes is also on the decline. According to the IDC, 84 billion e-mails were sent worldwide every day in 2006.

The downside is that when writing and receiving e-mails, there is no secrecy of correspondence and, as a result, no privacy in communication processes. While most of us are aware of the minimum risk involved with sending vacation postcards – postal service employees might read them – the risk that unauthorized people will read our e-mails is significantly higher, but this fact is largely unknown.

There are many opportunities for unauthorized persons to intercept, read or even modify e-mails as they make their

way through the World Wide Web. All e-mails, including information that is decisive for corporate processes and must therefore be protected, are processed on many servers around the world. As a consequence, sensitive information might end up in the wrong hands if it is transmitted insecurely, i.e., without protection mechanisms.

Another important aspect is that e-mail recipients have no way of knowing if the content they receive is the same content sent by the sender. As soon as unauthorized persons have gained access to servers, they are in a position to modify and manipulate the content of e-mails. This not only includes modifications or manipulations to the content, but also to sender information. In doing so, people can be misled about identities, which could have devastating consequences for any company.

Every company is a potential victim of cybercrime

Hackers and industrial spies go after internet connections and local company-owned networks. Since corporate processes are increasingly done electronically, it is paramount for companies and institutions to protect sensible data from unauthorized readers and unnoticed manipulation during transmission.

The extent of this threat is very significant: as early as in 2004, the Baden-Württemberg Security Forum estimated the potential damage of industrial espionage at seven billion euros in the German state of Baden-Württemberg alone.

The sobering conclusion: every innovative and successful company, regardless of its size, may become a victim of cybercrime! Without great effort, your competitors could, for example, intercept e-mails written by you and the person or institution in charge with patent applications. As the case of



Enercon has shown, this could be a great threat to your corporate secrets and your intellectual property.

Increasing legal requirements

Specific legal and regulatory measures about the dissemination, storage and archiving of business e-mails and related information have been introduced. The time frame for data storage has also been clearly defined.

Violations of relevant data protection regulations or fiscal regulations as well as other offenses subject to criminal prosecution may be subject to drastic fines. Persons with corporate responsibility including managing directors, board members or IT directors may be held personally liable for damages. In extreme cases, serious offenses may even entail a prison sentence. A lack of IT security might of course also lead to direct damage such as the loss of data or loss of production and, not less importantly, to negative publicity if security gaps become publicly known.

Secure e-mail communication

Client-based e-mail encryption and signatures have been successfully tried and tested in many companies to provide complete end-to-end e-mail security. They help organizations ensure that personal data is protected at all times. End-to-end security refers to digital signatures and the encryption of electronic mail at the work place: one benefit is that digital signatures establish the authorship of e-mails beyond doubt. Another benefit is that recipients have the option

of checking if the data has been modified before reaching them. Encryption, for its part, ensures that only a selected number of recipients are authorized to decrypt and therefore read the documents in question. This ensures the level of commitment and privacy typically needed for corporate online processes.

Secure Mail offers the following advantages:

- **Privacy**
E-mails are encrypted with trusted and secure cryptoalgorithms to ensure e-mails remain private at all times.
- **Interoperability**
Standards for Secure Mail solutions (S/MIME Open PGP) warrant the interoperability of the secure e-mail communication with the business partner in question.
- **Anti-manipulation component**
Recipients rely on the digital signature on e-mails to verify their integrity, i.e., to check if they have not been modified.
- **Identity**
The authorship of any e-mail can be established irrefutably and definitely, which provides the level of commitment needed in a corporate environment.
- **User acceptance**
To operate the entire application, users need 2 buttons in Outlook only: sign and/or encrypt.

The solution

IDpendant's Secure E-Mail Evaluation Package is a complete solution for the protection of your e-mail communication and includes support services. This solution created by IDpendant is the easiest way of implementing a consistent company-wide e-mail security policy. Electronic signatures and encryption are reliably integrated into this solution in accordance with corporate guidelines and implemented accordingly.

Secure Mail evaluation package:

- 5 USB tokens; or choose 5 smart cards and card readers
- 1 day of installation support
- 1 CD SafeSign IC (5 licenses)
- 5 online IDpendant CA certificates

IDpendant GmbH
Edisonstrasse 3
D-85716 Unterschleissheim/Munich

Phone +49 89 3700 110-0
Fax +49 89 3700 110-10
info@idpendant.com