1. Why should we use secured and signed e-mail?

This question can be best answered by looking at the most important aspects of security and compliance:

- Availability;
- Exclusivity;
- Integrity;
- Control.

Availability

The availability of e-mail is critical to organization and for that reason the load balancing, capture, storage, archiving, recovery and deletion of e-mail has high priority on ICT agendas. In order not to store unwanted content most organisations filter on spyware, spam, viruses and other unwanted and unsolicited content and malicious code. The basis forms their E-mail Security Regulations since not having a high availability could lead to violations of government and industry regulations (for example the Sarbanes-Oxley Act), productivity of staff and a breach in security. The secure e-mail signed and encrypted for that reason should be available in a decrypted manner to the relevant persons in the organization.

Exclusivity

The internal, outbound and inbound messaging by e-mail should only be sent, edited, read and received by the people who are authenticated, authorized (by privileged rights) to access the content in those e-mails. However according to an estimate of IDC 8.33 Million e-mail messages were sent in 2005. How can we be sure that only the intended recipients received those messages? How can we be sure that the message really came from this sender. With relatively little effort clever people can read and with more effort change your e-mail and attached files and documents. E-mail is compared to postcards in a glass mailbox. Exposing e-mail to the wrong persons could lead to violations of government and industry regulations, violations of corporate e-mail policy and best practices, loss and leakage of intellectual property and confidential or private information.

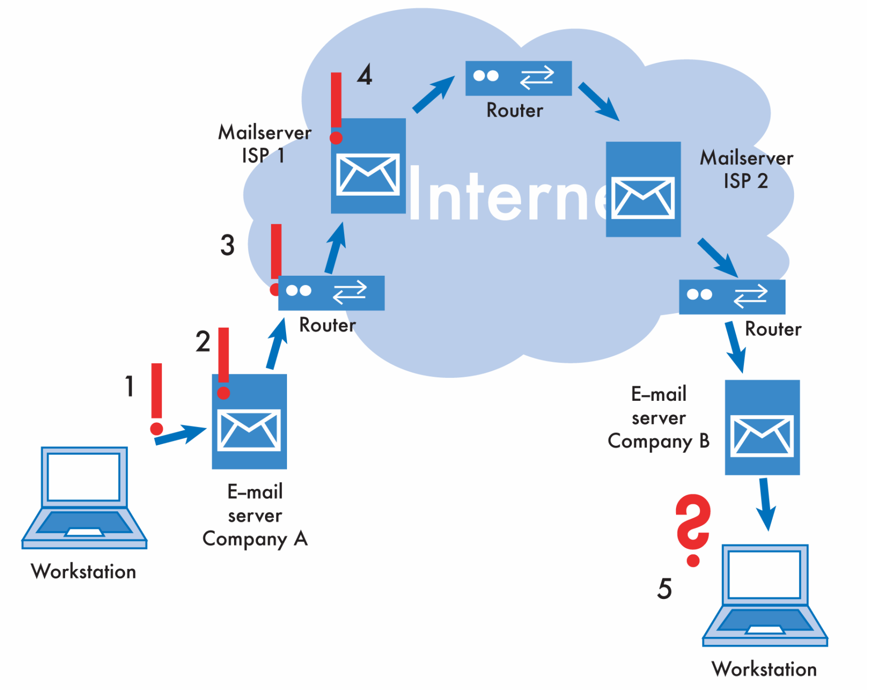
Integrity

E-mail is compared to postcards in a glass mailbox, but could also be opened or faked. Is the message the receiver receives the same message as the sender has sent? Identity theft is *the fastest growing crime in America; 9.9 MILLION victims were reported last year, according to a Federal Trade Commission survey*

Control

Is the sender really who he says he is? Can the sender deny having sent the message? Could the message be changed while being in transit?

As email travels from sender to recipient, it can be intercepted at a number of places.



1. At the local (wifi) network, network sniffing allows hackers to read your email.
2. Your mail server is maintained by IT staff that may be loyal long term employees with your company, but also may be temporarily employees hired only yesterday. Can you trust them? They can read your email.
3. As soon as your email message leaves your company, you have no control over who reads your messages.
4. At the ISP your company is using for internet access or email, several people can read your email. Do you know them? Can you trust them with your company confidential information?
5. At recipient's end the same "leaks" are present. Also, when recipient reads your message, how do they know that it actually comes from you?

So how do we make the appropriate and wanted content available to our partners, member, customers, suppliers, staff and/or investors?

2. SEVEN STEPS TO E-MAIL SECURITY

1. Define and analyze the regulations, standards and laws towards your organization must be compliant (f.e. Sarbanes Oxley, DNB) (SOLL-situation);

2. Collect, Analyze, Classify and Define the information needed for a Reliability and Vulnerability Analysis such as e-mail senders, receivers inside and outside your organization on the basis of low, medium and high risk and threats with regard to availability, exclusivity, integrity and control (SOLL-situation)?

3. Collect, Analyse, Classify and Define the information needed for a Reliability and Vulnerability Analysis such as e-mail contents on the basis of words, numbers, texts, files and documents (f.e. corporate financial information) inside and outside your organization on the basis of low, medium and high risk with regard to availability, exclusivity, integrity and control (SOLL-situation)?

4. Plan, execute and control a technical e-mail audit on the basis of contents and attachments in relation to e-mail recipients and senders inside and/or outside the organization over a period of one to three month(s) with an E-mail Content Monitoring and Filtering Solution (with intelligent context analysis) to have an impression of the IST situation?

5. Evaluate SOLL and IST situation when comparing the audit with the e-mail security regulations, available policy and law in order to assess the gap which carries the risk of e-mail for your organizations’ partners, employees, customers, investors and suppliers.

6. Write or adjust the E-mail Security Policy and Plan;

7. Management by execution, enforcement and control of the Security Plan with e-mail security related required measures to fill up the gap between SOLL and IST with E-mail Acceptable Use Protocols, E-mail Filtering, Anti-Spam, Legal Liability, Virus and Spyware Management, Bandwidth and business related content control, E-mail Content Security, PKI and Security Awareness trainings.

3. Who needs, is using what and is going to use E-mail Security?

The awareness of E-mail related security, legal and compliance risks and threats is very low at users' level.

In order to find out what the risks and threats with e-mail are the 7 step approach is very handy. However without knowing and understanding you could also make a benchmark of what other organizations are doing in the field of e-mail encryption and decryption and signing. Below you will find the results of an in 2005 published research of Osterman Research Inc. among 115 organizations in order understand the e-mail encryption market.

1. Which of the following systems have been deployed and where have they been deployed?	Server	36%
	Desktop	33%
	Gateway	20%
	Hosted or ISP	5%
	Not deployed	34%
2. For which of the following types of traffic it is important in your organization to have secure messaging?	Business/supply chain	82.7%
	Remote employees	76.9%
	Customers/consumers	70.2%
	Internal employees	52.9%
3. Which secure messaging/encryption method(s) does your organization require to communicate securely with these people?	S/MIME	57.4%
	PGP	43.6%
	A Web Mailbox	43.6%
4. How broadly do you require to deploy secure messaging/encryption within your organization now?	Selected individuals	71.1%
	A single business group or department	53.8%
	Multiple business groups	52.1%
	Company wide	36.6%
5. What or who is driving the need for secure messaging/encryption?	Security/IT department	66.4%
	Compliance department	57.4%
	End users	30.1%

Source: Hosted Messaging Market Trends 2006-2009

What is interesting to see is that the IT, Security and Compliance or basically pushing the e-mail encryption market. At the same time the relation with the business and supply chain, remote employees, customers and consumers are relatively regarded as important to securely exchange e-mail and that most of the organizations implement server and desktop solutions and many have not deployed anything in this field. If they have choosen more organziaation choose for S/Mime which is pushed by the digital signature laws of many countries. Users are not really willing to put effort in e-mail security which requires minimal user interference and administrational resources. After conducting an e-mail audit as mentioned in step 4 most organization want to reduce the number of e-mails with risks and threats of violations related to compliance, security, corporate imago, financial damage, productivity loss and legal liability with e-mail encryption and decryption.

When we look at the market of E-mail Security we define 4 segments in E-mail secure messaging:

Segment	**Decription**	**Worldwide E-mail Encryption Revenue by segment in 2003 (In Million $) (and yearly growth in % per year till 2008)**
1. Secure Content Messaging Security	Solutions are offered separately as gateway, server or appliance. Antivirus, anti-spam and content filters are also offering secure messaging as part of their solution.	44.6 (64.6%)
2. PKI	The issuing of S/MIME certificates that are primarily used for e-mail encryption.	40.9 (16.6%)
3. Desktop	Standalone software or plug-ins placed on desktops in order to encrypt and decrypt e-mail	45.0 (12.9%)
4. Service	Offering of e-mail encryption offered as a managed service	69.0 (31.8%)
Total		168.4 (37.0%)

* Source: IDC Market Analysis E-mail Encryption 2004-2008