

Email Security

Ensuring secure communication

White paper

September 2006

Copyright © Insta DefSec Oy, 2006. All rights reserved.

This document is provided only for informational purposes. It may be used according to the following conditions:

- The document may not be distributed for profit.
- Copies of this document must contain all text without modification and all pages must be included.
- All copies must include the copyright notice.
- This document is for personal use only.

Information in this document is subject to change without notice and does not represent a commitment on the part of Insta DefSec Oy.

Table of Contents

1	E-mail Security - why bother?	4
1.1	Threats to Email Communications.....	4
1.2	Mitigating risks.....	5
2	Digital signing and encryption	6
2.1	Digital signature.....	6
2.2	Encryption.....	6
2.3	Process of sending an e-mail message securely	6
3	Increasing information security with certificates	8
3.1	What are digital certificates	8
3.2	Where digital certificates can be used.....	8
4	Insta E-mail Security	9
5	Insta Security Systems	10

1 E-mail Security - why bother?

Companies need to be able to share information internally and with various parties, such as customers, partners, suppliers and service providers. Reliable, up-to-date information on projects, markets, production and customers is essential for efficient management. The most common way for organisations to exchange information today is by using e-mails. With this fast and easy way to communicate, security is often left aside even though no sensitive data should be exchanged via e-mails to outside organisation. Lack of e-mail security also means that many business benefits that could be gained are not used and more costly methods still apply.

1.1 Threats to Email Communications

E-mail threats have become a serious business issue. Unsecured e-mail is like a postcard: anyone can read it and/or send it pretending to be someone else. Unauthorized access to company's valuable information, such as client and employee records, intellectual property, product development and sales forecasts can do significant damage to a company's brand, competitive position and customer relations. In addition to spam and viruses, the most common threats to e-mail communication are:

1. **Eavesdropping** - There are a lot of people on the internet and it is very easy for someone who has access to the computers or networks to capture information and read it or even copy your messages.
2. **Identity Theft** - If someone can obtain the username and password that you use to access your e-mail servers, they can read your e-mail and send false e-mail messages as you.
3. **Message Modification** - Anyone who has system administrator permission on any of the SMTP Servers that your message visits can not only read your message, but they can delete or change the message before it continues on to its destination.
4. **False Messages** - It is very easy to construct messages that appear to be sent by someone else. Many viruses take advantage of this situation to propagate themselves.
5. **Message Replay** - Just as a message can be modified, messages can be saved, modified, and re-sent later. You could receive a valid original message, but then receive subsequent faked messages that appear to be valid.
6. **Unprotected Backups** - Messages are stored in plain text on all SMTP Servers. Thus, backups of these servers' disks contain plain text copies of your messages. As backups can be kept for years and can be read by anyone with access to them, your messages could still be exposed in insecure places even after you think that all copies have been deleted.
7. **Repudiation** - Because normal e-mail messages can be forged, there is no way for you to prove that someone sent you a particular message. This means that even if someone DID send you a message, they can successfully deny it. This has implications with regards to using email for contracts, business communications, electronic commerce, etc.

1.2 Mitigating risks

Tools for securing e-mails exist but often for closed environments. Different partnering organisations do not often have similar tools for secure e-mails, which is what makes securing e-mail traffic complex. Standard and easy-to-use methods are needed to make secure e-mailing possible globally and take a full advantage of e-mail technology while mitigating risk from e-mail threats with reasonable costs for your company.

2 Digital signing and encryption

Secure e-mail communication is made possible by digitally signing and encrypting the data before sending it. **Signing** a message proves who it came from and that nobody has changed it, but anyone can read the message in transit through the internet. To be effective, digital signatures must be unforgeable, which can be ensured with Public Key cryptography, known also as asymmetric encryption.

Encrypting makes sure the message is unreadable to others than intended recipients. These functions together ensure the authenticity, confidentiality, integrity and non-repudiation of the message.

2.1 Digital signature

Digital signature is a method of authenticating digital information. A digital signature is a digital code that is calculated from the message and can be sent as an attachment along with the e-mail. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be and that the message has not been altered after it was sent.

2.2 Encryption

Encryption is a way of protecting information before sending it from one computer to another. Encryption is the process of transforming the contents of a message using the recipient's public key so that the message cannot be read. Decryption is the process of transforming the message back into a readable form by using the recipient's private key. Message encryption and decryption is the foundation upon which a secure messaging system is built.

2.3 Process of sending an e-mail message securely

When you use an application to digitally sign a message, you are basically attaching your public key to the message along with other information that ensures the integrity of your e-mail message. Before the e-mail message and public key are sent, the message goes through an encoding process, called a *hashing algorithm*, whereby the message you are sending is used to mathematically generate a kind of digital fingerprint that could only be created by your exact message. This digital fingerprint is also called a *message digest*.

Once the e-mail application creates the message digest, it uses your private key to encrypt it. Your e-mail application sends the e-mail with the public key and encrypted message digest as attachments.

When someone receives your e-mail message, their application uses your public key to decrypt the signature changing it back into a message digest. If it works, it proves that it came from you. Then the application runs your e-mail text through the same hash algorithm that your application used and compares the message digests. If they match to each other, then the signed message was not altered during the transfer.

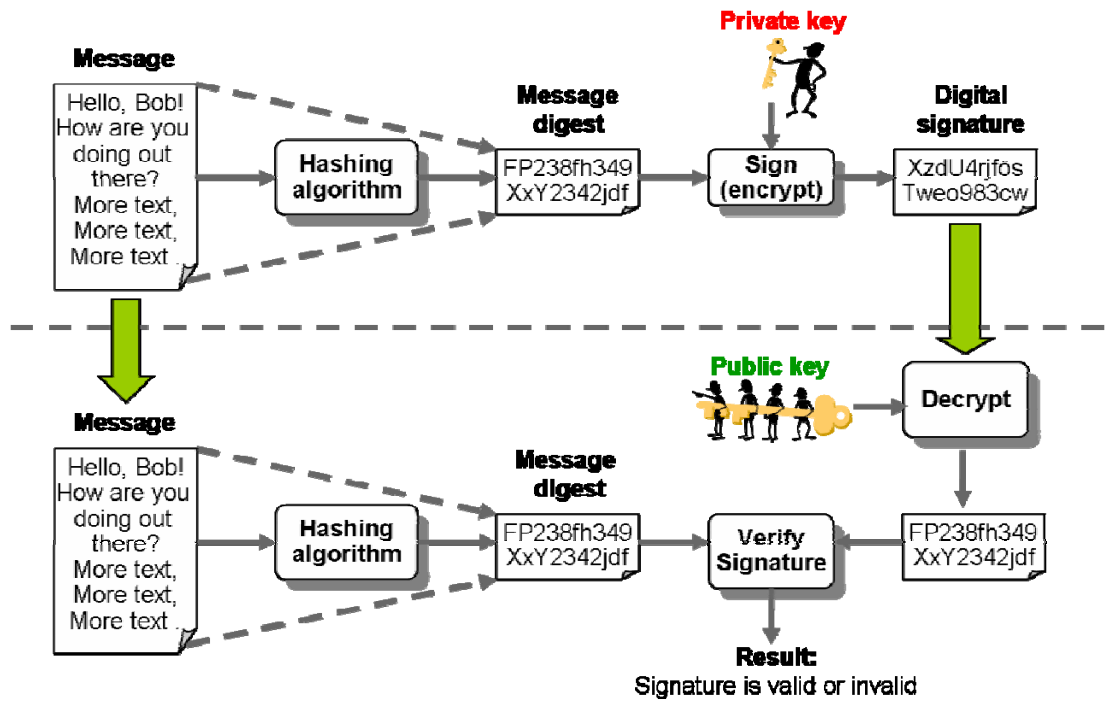


Figure 1: Digital signature

Before you can send someone an encrypted message, you need his or her Digital ID, which contains his or her public key. Your e-mail application uses his or her public key to encrypt the message. You can distribute your Digital ID (and its public key) to as many people as you would like without harming the integrity of your Digital ID. However, you must guard your private key, since it is used to decrypt any messages sent to you and sign new messages with your identity.

3 Increasing information security with certificates

The rapid growth of e-business requires higher and higher levels of security and confidentiality. Identity is the critical component of any transaction. Securing the users identity will increase the security of these systems as well as individuals in a public network. People involved in e-business or working remotely must be able to convince themselves not only of the identity of the other party but also of the authenticity, integrity and confidentiality of the data. This is made possible by digital certificates - data structures authenticated by a trusted party - which are used to provide proof of the identity of the person in question and to share the public key of that person. The purpose of digital certificates therefore is to increase the information security of systems as well as individuals in a public network.

3.1 What are digital certificates

A certificate is a digitally signed document that is used for identifying its bearer. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key and the digital signature of the certificate-issuing authority (CA). In other words, the certificate describes the issuer of the certificate and presents its validity by using a digital signature to bind together a public key with an identity. A Digital Certificate is issued by a Certification Authority (CA) and signed with the CA's private key. The most common certificate standard is the ITU-T X.509 v3.

Certificates are essential for the Public Key Infrastructure (PKI)¹. With certificates, it is possible to check the chain of trust that relates to the certificate and the public key, and to make sure the secret known only by the certificate bearer has not leaked.

The most secure way to use digital certificates is to use two-factor authentication. Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code. In this context, the two factors involved are sometimes spoken of as *something you have* and *something you know*. Using more than one factor is also called strong authentication.

3.2 Where digital certificates can be used

Digital Certificates provide a means of proving your identity in electronic transactions. They can be used for strong authentication of user identities, digital signatures or data encryption. Strong authentication is required for secure remote access (IPSec), login onto Windows domains and web authentication (TLS/SSL). Digital signatures are used to ensure that data, documents or messages cannot be modified and to authenticate the identity of the signatory. For data encryption, digital certificates provide an easy and reliable way of sharing a public key.

¹ Learn more about PKI from our PKI tutorial at www.certificate.fi/resources/materials/white_papers/white_papers.htm

4 Insta E-mail Security

Insta E-mail Security solution provides a quick and an easy way to implement secure communication channels. Our e-mail security solution utilizes PKI (Public Key Infrastructure) methods to create a safe way of communicating between an organisation and its cooperation network. E-mails are secured by digitally signing and encrypting the data with the user certificate. Certificates can be taken into use in an organization's existing e-mail system.

The solution includes:

- CA (Certificate Authority): creates user credentials, certifies user IDs, archives and publishes user certificates and maintains revocation lists
 - User Directory: for publishing certificates centrally and to Microsoft Active Directory, Novell eDirectory or IBM Tivoli, for example
 - Web-based administration
 - Multi-user control and fine-grained separation of duties
 - Event logging and audit trail
 - Simplified administrator GUIs e.g. for help desks
- RA (Registration Authority): tool for enrolling certificates and storing them to smart cards, tokens or other certificate stores
- User certificates for encrypting e-mails and verifying digital signature
 - Tokens or smart cards for storing user IDs
 - CSP: Offers cryptographic services to applications
 - Smart card readers
- Standard based solution that is compliant with e-mail clients supporting S/MIME protocol

Technical features

Solution consists of following components:

- Certificates provided by Insta Service Center or by Insta Certified Partner
- Certificates can delivered in several ways depending on security and interoperability requirements
 - Software certificates, smart cards, USB tokens

Protocols

- S/MIME protocol
- SSL/TLS protocol
- X509v3 certificates
- PKCS#15 and PKCS#11 smart cards and tokens
- LDAP

5 Insta Security Systems

Insta DefSec's Security Systems is a global information security specialist developing and supplying networking and information security solutions. We focus on innovative solutions and applications for customers with high quality and security requirements. Our product and service solutions enable our customers to benefit from improved business models and to develop their operations. Efficient, secure e-business and networking solutions improve our customers' business operations, administration and utilization of modern technology.

Our know-how, technology and processes represent the absolute top in their field, which is why we have reached an internationally recognized position in the information security market.

» *Visit our web pages to learn more about our company and resources at www.certificate.fi.*