

Email Security Options

This paper can form a foundation for comparing Email Security Solutions. Several members of the industry and individuals have contributed by providing content and editing. The audience for this Technical Perspective includes both the businessperson looking for a high level description of the technology and the IT professional who is unfamiliar with Email Security concepts. Our goal is to familiarize the reader with the requirements of Email Security, the architectural components and how they interact.

The requirements of e-mail security are as follows:

- R1. Message confidentiality using encryption** - protects your sensitive information from being viewed by anyone other than the intended recipients.
- R2. Authentication with digital signatures** - verifies that the sender and the recipient are exactly who they say they are.
- R3. Integrity with digital signatures** - ensures the contents of your email cannot be altered in transit without detection.
- R4. Non-repudiation with digital signatures** - ensures the sender cannot deny emailing the message at a later date (this is particularly vital with financial transactions being conducted and authorized over email)

"Email Security Options - is a deliverable from the Wonder Software's Business Solutions Group (BSG). Several member organizations and individuals have contributed by providing content, editorial assistance and editorial reviews.

Authors:

R K Verma
Gromax Infonet

R Saran
Wonder Software Tech.

To meet these challenges the solutions may provide several options. While some solutions may meet only 1, 2 or 3 requirements, the business goal requires that a solution should be able to meet all 4 requirements.

Message Broker or Independent

First of all it must be clear to the user that whether he is going to hand over the security of his messages to a third party or is he going to keep the control over his messages in his own hands. Bringing the third party in transacting his operations over the wire means relying upon the integrity, efficiency and reliability of the third party. Based on these considerations the solution can be classified as one of the following two types:

1. **Desktop:** In this kind of solution the user is independent of any third party for message authentication, storage or forwarding. The user has complete control over whom he trusts, and who is reading his messages. The only third party can be a government approved Certificate Authority who authenticates the public keys of others with whom the user corresponds.
2. **MiddleWare:** In this kind of solution a third entity is involved who acts as a message broker, i.e. the user takes authorization from a third party to connect to the third party's specific server to send and receive messages. The recipient of the message, on receipt of the message, must log on to the same third party's specific server then register before he can read the contents of the message. In this case the authentication reliability of the sender depends upon the integrity and reliability of the system of the third party.

Password or PKI

To meet the very first requirement of confidentiality, the solution can use one of the following techniques i.e.

Either

1. **Password-Based:** Software that secure the E-Mail using a password only.

Or,

2. **PKI-Based:** Software that provide security using Public Key of the recipient and the Private Key of the sender. PKI has been explained in a different document entitled “PKI Options for Secure Email”

Standards

The user would generally like to use the software that follow standards in their implementation. While there are not any defined standards for Password Based security of email, there do exist standards for PKI Based solutions.

1. The standard of the E-Mail securing key, as defined by Internet Engineering Task Force (website: <http://www.ietf.org/html.charters/pkix-charter.html>), is known as **X.509**. There are some software that use this standard and there are other that use their own standard.
2. The standards for encryption are various to pick and choose. However, in PKI the most popular are **RSA** and **Diffie-Hellman**.

Utility Features

The utility features of the software are as important as its security features. A solutions can do one or all of the below mentioned functions.

Meets Requirements

1. Encrypts but does not sign i.e. no authentication of the sender. Meets requirement R1 only.
2. Signs but does not encrypt i.e. no confidentiality of the message. Meets requirements R2, R3 and R4.
3. Encrypts and Signs. Meets all the requirements i.e. R1, R2, R3, and R4.

Types of Messages that it handles

1. E-Mail Text messages only.
2. Files only. Also what kind i.e. format of files can it handle.
3. E-Mail text messages and Files both.

Protection of the Protector

A security guard without a gun means the guard himself is unprotected. The password or if PKI is being used then the private key are the protector of the user. It is important to know as to how does the solution protect the password or the private key of the user.

1. While using a message broker service it is obvious that the password is known to the third party using which they provide connectivity.
2. If PKI is being used and the private key is stored on the hard drive, then anyone who knows the password can sign as the user. However, if the private key is stored on a removable and mobile token such as Smart-Card or USB token then this can be considered as secure.

Mail Client, Account & Server Independence

The user may find himself in difficulty if suddenly he realizes that a new email id that he created with another email service provider cannot be used with the security solution that he has. Hence, mail client independence is as important as any other feature of the solution. Moreover, security solutions are self-centric, this means that the sender and the recipient somehow must use the solution. Thus if the sender becomes mail client dependent then so does the recipient.

1. If the software forces the user to use a specific mail client, account or server then the solution may be used only within a closed group.
2. However, if the software allows the user to use any mail client, account or server then the solution can be used freely for correspondence by anyone with anyone.

Everybody Must Buy

It is normal for any solution provider to expect that every user of his solution will buy it. However, for the user this is a problem. In a situation where a buyer of the solution must correspond in security and with authentication with several people, some of whom are not willing to buy the solution, then the user's capability becomes limited and he must find a different solution that does not force the recipient to buy to read the message or to verify the sender's signature on it. Hence, there can be two kinds of solutions.

1. The solutions that force the recipient to buy the solution or join a closed group.
2. The solutions that make available a free version of the software that any recipient can use to verify and read the messages received.

Mobility

The last question a user must ask while evaluating various options of Email Security Solutions is that will he really be mobile with the solution he is paying for. By mobility it means the solution can be used from anywhere. The best example of anywhere is a Cyber Café. The user goes to a cyber café, wants to write or receive mail on his existing email account. However, he desires the same level of email security that he has in his office or home. How does he get it?

1. The solution must be available in the Cyber Café or at least be available for free download.
2. If the solution is password based then the user should remember his password.
3. If the solution is PKI based then the user must have his private key with him.