# Global Information Assurance Certification Paper

# Secure Email Solutions and Considerations

Jim Yarbrough
August 25, 2003
SANS GSEC Practical Assignment v.1.4b

**Abstract**

In a recent META Group study, it was determined that email is now a more important business communications tool than the telephone. Businesses that rely on email must understand the need for secure email and then be aware of the types of secure email solutions available. Security measures can be implemented to protect sensitive information that travels via email.

Encryption is one of the major security defenses that can be used protect email. This paper further defines the need for secure email, the different types of email encryption solutions, and the items to consider when selecting a solution.

**Table of Contents**

## Introduction

Although email spam seems to be the most popular email topic lately, security is slated to become one of the top email concerns by 2007. Email security is becoming an increasingly important security discipline and can consist of the following items:

- Anti-Virus scanning
- Content scanning
- Message encryption
- Firewall protection
- Image scanning
- Spam filtering
- URL blocking

This paper focuses on the email security control of encryption. Encrypting email ensures that unauthorized people cannot read or change a message. Without encryption, a plain text email is similar to a postcard being sent using the postal system. A postcard can be read or altered during delivery and may not come from the person who actually sent it.

## The Need for Secure Email

Businesses can have many different reasons to secure email. There are four common reasons to implement a secure email encryption solution.

### 1. Regulation Compliance

Businesses need to ensure compliance with regulations that are mandated by international and federal law. Most of these regulations specify that businesses need to protect customer data when transmitted electronically (email).

Here's a list of some regulations that email encryption can be used for compliance:

- Gramm-Leach–Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- NASD 3010d
- SEC Rule 17-CFR 270.17a-4 (SEC 17a-4)
- US Patriot Act

For example, secure email controls should have been used at a bank in Colorado. In April 2003, regulators fined two former workers at a bank in Colorado and banned them from the banking industry for copying customer loan files and emailing them to a third party. These actions violated privacy regulations and were unsafe, unsound banking practices.

**2. Cost Reduction**

Email encryption mechanisms allow us to send information via the Internet in a safe and confidential manner. If confidential or sensitive information can be sent via email, this can provide a cost savings of thousands of dollars for a business. Secure email solutions can allow a business to use email instead of mailing paper communications. In addition, a business may be able to eliminate costly private or leased phone lines if secure email communications can be sent safely via the Internet.

**3. Information Protection**

Email security breaches can occur in varying forms. Three examples are included below:

- Confidentiality: email is read by unauthorized person
- Integrity: email contents are modified by an unauthorized person
- Authenticity: email is forged to appear as from a certain person

Email encryption solutions can be applied to control unauthorized disclosure, ensure integrity and authenticity of email.

**4. Best Practice**

By using secure email controls, businesses can gain the trust of their customers and build a solid reputation for protecting customer data. Secure email solutions are often overlooked and can be implemented to enhance best practices.

**Secure Email Solutions**

Several secure email vendor solutions are available today. Listed below are three primary email encryption solutions along with each solution's advantages and disadvantages.

**Three primary methods to secure email messages**

**1. End-to-End**

This solution provides message encryption from the originating sender's desktop to the desktop of the recipient. Upon receipt, the recipient would decrypt the message on their desktop. Secure Multipurpose Internet Mail Extensions (S/MIME) using public-key cryptography is a common technique used for this method. In addition, PGP and other proprietary client solutions are available.

**Advantages:**

- Very secure method, since encryption is provided end-to-end from the sender's device to the recipient's device.
- Messages can be signed by the sender to bind a legitimate identity to a message and guard against forgery.
- For S/MIME, popular email clients already have S/MIME capability built-in.

**Disadvantages:**

- Sender and recipient must have cooperating encryption software. This may require a purchase and installation of additional client software.
- Public key exchanges must take place between sender and recipient.
- Email content and/or virus scanning processes may not be able to process at the gateway for end-to-end encrypted mail.
- For S/MIME, interoperability problems may exist between sender and recipient.
- For S/MIME, S/MIME does not provide message compression.

**2. Boundary to Boundary**

This method provides email encryption over vulnerable links such as the Internet. Email that is sent within a trusted network (inside a business network), may not be encrypted. For example, if a bank sends a mortgage application via email to a mortgage broker, the following steps may occur:

1. The mortgage application email is transmitted in the clear within the bank's internal network.
2. A gateway appliance encrypts the mortgage application email before it leaves the bank and travels on the Internet.
3. The mortgage application email is encrypted as it flows across the Internet.
4. Once received inside the mortgage broker's network, the mortgage application email is decrypted and handled in the clear within its network.

For this method, usually an email gateway device is used at the sending and receiving locations to provide the email encryption between the sending location and the receiving location. Secure Sockets Layer (SSL) and Secure Multipurpose Internet Mail Extensions (S/MIME) are the common ways used to encrypt messages. Key exchange is much easier since only one key pair needs to be exchanged for each location. Keys do not have to be exchanged between individual users.

**Advantages:**

- Additional client software is not required for end user.
- Email content and/or virus scanning processes can process at the gateway for the email that will be encrypted.
- Consistent message encryption can be provided between selected destinations.
- Key exchanges do not occur between end users, but between business domains.

**Disadvantages:**

- End users may not be aware of when messages are encrypted and when they are not encrypted.

- Both sending business and receiving business must have compatible gateway solution in place.

**3. Staging Servers**

A staging server is used to store an encrypted email for a recipient. Encrypted email can be created and sent to this staging server from email encryption client software or from a boundary email gateway device. Vendors offering these staging services include Zix Corp., Tumbleweed Communications, and CertifiedMail.

The intended recipient of an encrypted email on the staging server can retrieve an awaiting encrypted email using one of the following processes:

1. A clear text alert message is sent to the recipient that includes a URL to the staging server. The recipient connects to the staging server using SSL. The recipient would authenticate as required. The email is then decrypted on the staging server location and transmitted over the SSL connection to the recipient's device.

-- or --

2. A clear text alert message is sent to the recipient that includes a URL to a company's web portal site. The recipient connects to the web portal site server using SSL and authenticates. The portal web site accesses and displays the intended email for the recipient. In this case, the email is decrypted on the staging server location and transmitted over the SSL connection to the web portal site for the recipient.

In the two scenarios above, the email is decrypted at the staging server location and then sent via SSL to the recipient. There are a few vendors (Sigaba) that actually pass a key to the recipient's browser allowing the decryption of the retrieved email to occur on the recipient's desktop.

If a staging server is outsourced, it is essential to ensure that the contracting vendor's network space is safe and meets your standards. In addition, service level agreements need to outline standards required and other support requirements.

**Advantages:**

- No additional software demands are placed on the email recipient. All that is required is browser access to the Internet.
- Email content and/or virus scanning processes can process at the gateway for the email that will be encrypted.
- Consistent message encryption can be provided between selected destinations.
- Key exchanges do not need to occur between end users or business domains.

**Disadvantages:**

- Email senders may not be aware of when messages are encrypted and when they are not encrypted.
- Two messages are sent instead of just one. One with the URL in the clear and the other message sent directly to the staging server.
- Internet connections are required in order to view secure messages.
- Recipients have to register to the staging server service in order to retrieve their encrypted email.

**Additional methods to secure email messages**

In addition to the three solutions listed above, other encryption controls can be used to add more protection for email. A common overlooked strategy is the encryption of the communication channel from the email client to the email server.

## SMTP with SSL or TLS

The Simple Mail Transport Protocol (SMTP) is the standard protocol used to send an email. SMTP is used between an email client and a mail (SMTP) server. SMTP does not provide encryption for messages, so all communications to SMTP servers is in the clear unless controls are put into place. Secure Sockets Layer (SSL) or Transport Layer Security (TLS) can be implemented to encrypt SMTP communications.

## IMAP and POP with SSL

To retrieve an email from an SMTP Server, two protocols are available. One is the Internet Message Access Protocol (IMAP) and the other is Post Office Protocol (POP). The username and password credentials used to log on the email server are not encrypted using IMAP or POP. SSL can be used with IMAP and POP to secure these communications.

## Email Storage - Backups

Unless encrypted, email stored on SMTP servers is in clear text. Backups of the email server data can be made and administrators can read any of the data on these servers. If you read an encrypted email, it may be decrypted and stored on the email server. You may need to the email or make sure it remains encrypted on the SMTP server.

**Which solution is best?**

A business may need to combine several of the primary and additional methods listed above to meet their specific needs. Several factors need to be considered in order to select the best solution to meet your needs.

**Factors to consider in determining the best solution**

1. **Be easy to use and intuitive for both senders and recipients.**

This is one of the most important factors to consider when analyzing possible solutions. If an email encryption system is too complex and difficult to use, it may be perceived as an obstruction and may not be consistently used. If external recipients find it too complicated to use, they may decide that the sender is difficult to do business with. Users must not be required to understand cryptography specifics to use the product.

2. **Allow senders and recipients to utilize existing software**
   If users can utilize familiar software that they already have, the solution will be more easily accepted. Most users are already familiar with at least one email client and/or one Internet browser. For internal business users, software plug-in could be installed with their existing email client. For external email recipients for a business, a solution that does not require any new software would be preferred.

3. **Be cost effective.**
   In general, it is usually difficult to provide a cost/benefit analysis for a security product. For secure email, a risk assessment should be performed to determine how a business assesses the likelihood of any threats and vulnerabilities associated with non-encrypted email. Based on this assessment, a business could compare the secure email product costs to the implied costs associated with the risk assessment. The product costs, including maintenance and support, should not exceed the cost of the risks that are being mitigated.

4. **Integrate seamlessly with existing and future e-mail infrastructures.**
   The existing network infrastructure of a business should not have to be replaced or drastically overhauled to implement any secure email product. If gateway appliances are installed, they should interoperate with existing firewalls and email servers. If client software needs to be installed, it should work with existing email client software on PCs and/or PDAs. Also, any product should be able to integrate with an existing backup/recovery solution.

   Product integration with anti-virus and content filtering systems that are operating on client systems and/or gateway servers needs to be carefully analyzed. The location of where an email is encrypted can impact the effectiveness of these services. Any secure email product should be able to interoperate with these services.

   Since wireless access is becoming more common, a secure email product should be able to integrate with current or planned wireless email systems.

5. **Meet performance requirements**
   A business will need to test the performance of any secure email solution to verify it does not negatively degrade existing email system performance. The new product should adapt to any load balancing and failover requirements. In

addition, the new solution should not drop or lose any messages regardless of the situation.

6. **Allow users and applications to send encrypted e-mail messages to any recipient (intranet or internet).**
   This factor can have the biggest impact on what type of solution is implemented. One product may work well for sending encrypted messages outside a business. Another product may work best for secure web portal messages. A business will need to conduct a detailed analysis to determine the requirements for email encryption. All potential types of secure email recipients must be known.

   In addition, a business may require the use of programmatic applications to send or receive encrypted emails. This could a very important requirement if a business was automatically sending thousands of secure messages daily. A secure email product may offer software development kits (SDKs) for this functionality, or a policy based gateway solution may be able to be used.

7. **Easy to administer by system and network administrators.**
   A solution must provide good administration tools and also work with existing administration and monitoring solutions. For example, if a business currently uses an industry standard solution on all network devices to monitor availability and performance, any new secure email appliance should be able to interoperate with this monitoring solution.

   Also, in the case where secure email software plug-ins need to be installed with existing email clients, the software installation should be able to be scripted and automated as much as possible. A silent push type installation, with no re-boots required, can drastically reduce the number of installation problem calls to a system support staff.

8. **Provide strong encryption using industry standards.**
   Industry standard encryption algorithms should be used by the solution. The solution should be able to be easily configured to use longer encryption key lengths as needed when computing power increases. Also, any encryption keys utilized by the solution must be securely stored and distributed.

## Decisions and Challenges

Finding the right secure email solution can be easy or difficult depending on your requirements. In order to select the correct solution, you need to consider the entire flow and lifecycle of email. Every stage of email use needs to be evaluated and planned.

If you are not sure what solution is best and your requirements are not extensive, start with a simple solution to meet your immediate needs. A simple solution

may involve implementing only one of the three primary secure messaging techniques (end-to-end, boundary-to-boundary or staging servers) or encrypting the channel between the client and email servers.

For example, a small business that needs to communicate securely with the same 5 customers once or twice weekly may find it easier to implement an end-to-end solution. A large corporate that needs to send thousands of secure emails a day to a broad spectrum of recipients (Business to Employee-B2E, Business to Business-B2B, and Business to Consumer-B2C) may have many additional requirements and need to implement a combination of end-to-end, boundary-to-boundary, and staging server solutions.

Two companies in a B2B partnership may go for a boundary-to-boundary solution if they have a sufficient volume of email traffic and a suitable technical environment and staff to support it.

A company in a B2C situation may use a staging server if there is no influence of the technical environment of the consumer. This approach leverages the existing security of SSL and a browser.

If more than one encryption solution is needed to meet your requirements, the solutions must work together in harmony. For example, it may be possible to install both an end-to-end solution (email client software) and a boundary-to-boundary solution (gateway appliance). In this situation, if a confidential email is sent to an external customer using email encryption client software, the boundary gateway appliance must not reduce the level of security already placed on the email, and it should not impact the transmission of the message. It is critical to analyze every stage of email use before combining multiple types of solutions.

## Financial Strength

There is no shortage of secure email solutions. Before purchasing any product, financial analysis needs to be performed to determine the financial status of the vendor. If the vendor has not been profitable in the past few years, you need to question if the company and/or product will exist in the near future. Support agreements and future software enhancements may be critically impacted by a vendor's negative financial results.

## Secure Email Policy and Training

Companies have not finished their task if they only implement an email encryption product. Work needs to be performed to make sure any implemented technical solution aligns with company email policies.

Additionally, user education is also an important component. End users need to be informed that email misuse can have negative consequences for them and the company. These users should understand and accept the company policy.

Frequent communications to users about the latest email security issues help keep information security fresh in their minds.

The best management of secure email requires a careful combination of an acceptable email use policy, employee education and technology to secure content.

## Conclusion

Simply, it makes good business sense to encrypt email. In recent months, there have been several cases where private information was deceptively made public and other cases where electronic data was compromised. Email systems need to be scrutinized to ensure they can be relied upon for secure messaging. Email use will continue to increase and secure email will remain a key issue.

**List of References**


1. Desmond, Paul. "Time to Get Tough About Email Security." 12 May 2003. URL: http://itmanagement.earthweb.com/columns/secugud/article.php/2205041 (6 August 2003)

2. "Who cares about spam?." 25 July 2003. URL: http://spamisbad.com/comment.php?168 (18 August 2003)

3. Hinton, Craig. "Email Security." SC Magazine. February 2003. URL: http://www.scmagazine.com/scmagazine/2003_02/test_01/index.html

4. "Enterprise Secure Email Requirements." February 2003. URL: www.agorics.com/Library/CriticalRequirements.pdf (3 August 2003)

5. "Introduction to Secure Email." 12 October 2002. URL: http://www.sigaba.com/products/whitepapers/SG_wpaper_IntroEmail.pdf (3 August 2003)

6. "Comprehensive Compliance." ZipLip Inc. URL: www.ziplip.com/products.html (7 August 2003)

7. Chandrasekaran, Vanessa. "Who's Reading Your Email?" SC Infosecurity News. March 2003. URL: http://www.infosecnews.com/opinion/2003/03/12_03.htm (6 August 2003)

8. Udell, Jon. "Overlooked best practices." InfoWorld. 23 August 2002. URL: http://www.infoworld.com/infoworld/article/02/08/23/020826fepractices_1.html (6 August 2003)

9. Chan, Sally. "e-Risks, What to consider when creating your e-mail risk management policies." CMA Management. November 2002. URL: http://globeandmail.workopolis.com/content/partners/cma/pdf/nov2002-Article9.pdf (6 June 2003)

10. Howell, Donna. "Banks Building Vaults Around Customer Data - But Still No Standard - Financial Firms Working With Security Companies On Communication Tools." Investor's Business Daily. 30 April 2003. URL:

http://www.mirapoint.com/company/news_events/articles/04-30-2003InvestorsBusinessDaily.pdf (3 August 2003)

11. Graff, Joyce. “Four ways to secure messages.” 5 September 2002. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2879336-2,00.html (3 August 2003)

12. "Secure Messaging as a Strategic Decision: What are the Issues?" 18 December 2002. URL: http://www.zixcorp.com/webseminars/webseminars_QA.php?KEY=2 (18 August 2003)

13. Kangas, Erik. “The Case For Secure Email.” 2002. URL: http://luxsci.com/extranet/articles/email-security.html (3 June 2003)

14. “Secure Messaging, Part 5: Protecting Confidential Financial Information with a Turn-Key Email Security Solution.” 29 May 2002. URL: http://www.novell.com/coolsolutions/gwmag/features/trenches/tr_tovaris_5_gw.html (22 August 2003)

15. Candia, Tanya. “Redefining Email Security Policies.” 11 December 2002. URL: http://www.infosecnews.com/opinion/2002/12/11_02.htm (22 August 2003)

16. Getgood, Susan. “Educating users, Smart moves on spam.” SC Magazine. August 2003. URL: http://www.scmagazine.com/scmagazine/2003_08/feature_5/05.html