

The Holy Grail for Electronic Mail Security



Much of the industrialized world has become all too familiar with the use of email via the Internet. While many industry groups recommend the use of technology to secure communication using the Internet, technical and cost considerations remain barriers to widespread adoption in the health care industry. The security and therefore privacy of sending email on the Internet containing confidential information is another major concern. In the US, two federal requirements specify appropriate electronic safeguards to protect electronic mail. Due to HIPAA (Health Insurance Portability and Accountability Act) security requirements, “covered” health care entities need to adopt secure communication practices. While encryption is considered an “*addressable*” requirement by the final security rule, it should not be ignored. In addition, while digital signatures are not required under HIPAA but are required to be compliant with FDA 21CFR Part 11 rule.

Encryption is most often thought as the method used to secure electronic communication between two individuals. Digital signature adds a measure of authentication and in some measure of integrity control. However, email encryption requires the exchange of a public key certificate to send an encrypted message and a private key to decrypt the message. The interoperability of this security mechanism and the exchange of key certificates has proved difficult to implement in a cost-effective manner. In addition, if encryption is to succeed at the user’s desktop, the exchange of a large number of certificates becomes complex. Therefore for encryption to become widely adopted as a method of securely exchanging private health information, a simpler process is required. Securely exchanging electronic mail is a vital requirement for the further development and exchange of electronic health records.

For email encryption, PKI (public key infrastructure) has often proved difficult and costly to use and other technologies have proved easier to implement. The use of S/MIME (secure multipurpose internet mail extension) is a messaging standard involving digital certificates that is widely available. One can choose to purchase individual certificates from a trusted certificate authority or CA but the process of maintaining and exchanging them without PKI becomes unmanageable. One work-around is instead to deploy encryption at the organization's gateway or at a server level. This process is referred to as SMG (secure messaging gateway). Having the need to exchange only one certificate (i.e., the organization) at the gateway greatly simplifies the encryption and decryption process. For the process to be implemented successfully, a key requirement is that the encryption-decryption process should be somewhat transparent to the user by encrypting everything from particular email domains or addresses (i.e., all or nothing method). A more selective alternative would be to encrypt based on the content of a message or better yet by encrypting based on a keyword rule in the subject line. How and at what point encryption/decryption is employed is an important consideration, since encrypted messages cannot be scanned for viruses or filtered for spam. So scanning must occur before the message is encrypted on outbound messages and scanned after decryption on inbound messages.

Some other policy and technical requirements to consider as well.

1. Interoperability. The ideal solution must work with other S/MIME based gateways among participating business partners. The ideal solution should work with various email clients including older and less common products.
2. File Formats. The solution must accommodate standard email messages along with various types of file attachments and file formats.
3. Scalability. The ideal solution must accommodate a large volume of email traffic and attachments without consuming a large amount of processing resources.
4. Authentication. The solution allows for the authentication of the sending and receiving entities. The solution provides for effective and efficient key management.
5. Security. The solution provides acceptable encryption strength and provides for the satisfactory protection of keys.
6. Cost-effectiveness. The implementation of the solution must be cost-effective.
7. Accuracy. Some software that may use business rules and algorithms to search for health information content which may fail to consistently identify confidential information..
8. Virus Checking and Content Filtering: The solution allows for virus checking and content filtering of messages and their attachments.
9. Ease of Use. The solution should be easy to use and implement by healthcare entities. The solution should be "transparent" to the end-user and should simplify enablement.

Key Success Factors

An evaluation of the following success factors will determine whether the S/MIME gateway solution will be successful as an enterprise secure messaging solution. One, the ideal solution satisfies the identified business requirements of the health care organization (HCO) and its trading partners. Two, the ideal solution fits well within the HCO's enterprise messaging and security infrastructure with a minimum of customization. Three, the ideal solution does not add unacceptable delays to the bi-directional transmission of email messages.

Conclusion

The SMG encryption process described here is practical today and has been tested in a few pilot projects (Healthkey, Commonwealth of Massachusetts HIPAA pilot, and SMG Workgroup). As described for this process to be widely used, software vendors need to provide a technical platform to allow interoperability based on a standard for messaging exchange. A group of software vendors under the guidance of the Massachusetts Health Data Consortium and the Open Group (SMG Workgroup) have voluntarily agreed to discuss adopting a specific encryption standard. Unless the process of encryption allows interoperability among different products and platforms, the likelihood of successfully implementing secure email practices is considerably reduced. Nevertheless this voluntary group represents one small though important locally based effort. For secure messaging to succeed and be widely adopted by the health care industry will require a larger outreach effort. The ideal solution is a viable community based solution for securing email transmissions in the health care sector.

(c) Copyright 2003 HealthCIO Inc. All rights reserved. You may forward or reproduce copies of this white paper with the copyright intact.

Jon Bogen, founder and President of HealthCIO Inc (www.healthcio.com), a training and consulting firm focused on information technology to the healthcare industry. He can be reached at (610) 344-4909 or Info@healthcio.com.