Standard ID:	**SE-SEM-001**
Title:	**Secure email**
Domain:	**Security**
Discipline:	**Network Security**
Effective Date: Revision no.: Original date:	**3/22/2018** **7** **07/07/04**

I. Authority, Applicability and Purpose

A. **Authority:** Title 29, Chapter 90C provides broad statutory authority to the Department of Technology and Information to implement statewide and interagency technology solutions, policy, standards and guidelines for the State of Delaware's technology infrastructure. "Technology" means computing and telecommunications systems, their supporting infrastructure and interconnectivity used to acquire, transport, process, analyze, store and disseminate information or data electronically. The term "technology" includes systems and equipment associated with e-government and Internet initiatives.

B. **Applicability:** Applies to all State of Delaware communications and computing resources. DTI is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as School Districts, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of funding, and continued use of these resources.

C. **Purpose:** Due to the insecurity of standard email and to comply with federal regulations, a need exists to secure email containing sensitive and private information.

II. Scope

A. **State of Delaware e-mail** –This standard will cover all e-mails, including any attachments, requiring security due to their sensitive and private information.

B. **Areas Covered** - Email

C. **Environments –** Desktop, Laptop, Cellular, Wireless, PDA

III. Process

A. Adoption – These standards have been adopted by the Department of Technology and Information (DTI) through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the state of Delaware.

B. Revision – Technology is constantly evolving; therefore the standards will need to be regularly reviewed. It is the intent of the TASC to review this standard semi-annually. The TASC is open to suggestions and comments from knowledgeable individuals within the state, although we ask that they be channeled through your Information Resource Manager (IRM).

C. Contractors – Contractors or other third parties are required to comply with these standards when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection by the Delaware Technology Investment Council. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@state.de.us.

D. Implementation responsibility – DTI and/or the organization's technical staff will implement this standard during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

E. Enforcement – DTI will enforce this standard during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. This standard may also be enforced by others during the course of their normal business activities, including audits and design reviews.

F. Contact us – Any questions or comments should be directed to dti_tasc@state.de.us.

IV. Definitions/Declarations

A. Definitions

1. **Secure Email**: Involves secure electronic messages and their attachments. This does not include cellular telephone calls, text messaging over cellular telephones, or ftp – type data transfers.
2. **Secure:** It means ensuring that only the intended recipient can read the message, and also guaranteeing that it was not intercepted, or modified, and that it was delivered. This requires that email be protected, controlled, tracked and recallable.
3. **SMTP**: SMTP does not encrypt messages. All communications between SMTP servers send messages in plain text for any eavesdropper to see. Additionally, if an email server requests that you send your username and password to "login" to the SMTP server in order to relay messages to other servers, then these are also sent in plain text, subject to eavesdropping. Finally, messages sent via SMTP include information about which computer they were sent from and what email program was used. This information, available to all recipients, may be a privacy concern.
4. **POP** and **IMAP**: These protocols require that you send your username and password to login; these credentials are not encrypted. So, messages and credentials can be read by any eavesdropper listening to the flow of information between a personal computer and an email service provider's computer.

5. **Backups**: Email messages are stored on SMTP servers in plain, unencrypted text. Backups of the data on these servers may be made at any time and administrators can read any of the data on these machines. The email messages may be saved unexpectedly and indefinitely and may be read by persons unknown as a result.
6. **Eavesdropping:** The Internet is a big place with a lot of people on it. It is very easy for someone with access to computers or networks through which information is traveling to capture this information and read it. Just like someone in the next room listening in on a phone conversation, people using computers "near by" the path an email takes through the Internet can potentially read and save messages.
7. **Identity Theft:** If someone can obtain the username and password used to access email servers, they can read email and send false email messages as someone else. Very often, these credentials can be obtained by eavesdropping on SMTP, POP, IMAP, or WebMail connections, by reading email messages in which this information is included, or through other means.
8. **Invasion of Privacy:** If privacy is a concern, then backups (listed above) will also be a concern. Concern may exist about the recipients of SMTP email being able to tell what IP address sent the email. This information may be used to tell in what city the sender is located in, or even to find out what the street address is in some cases. This is not an issue with WebMail, POP, or IMAP, but is an issue when sending email, securely or unsecurely, from any email client over SMTP.
9. **Message Modification:** Anyone who has system administrator permission (even if they are not supposed to) on any of the SMTP Servers that a message visits can not only read the message, but they can delete or change the message before it continues on to its destination. Your recipient has no way to be told if the email message that was sent has been tampered with or not. And, if the message was merely deleted, they wouldn't even know.
10. **False Messages:** It is very easy to construct messages that appear to be from someone other than who they are actually from. Many viruses use this facility to propagate themselves. In general, there is no way to be sure that the apparent sender of a message actually sent the message - it could just as easily be fabricated.
11. **Message Replay:** Just as a message can be modified, messages can be saved, modified, and re-sent later. This could result in getting multiple messages and thus taking actions that were not requested.
12. **Repudiation:** Because email messages can be forged, there is no way to prove that someone sent a particular message. This means that even if someone did send a message, they can successfully deny it. This has implications with regards to using email for contracts, business communications, electronic commerce, etc.
13. **Non-Repudiation:** A process and use of technologies that ensure the following:
    a) The data (message, document, file, etc) that was sent is the same data that was received.
    b) The person who sent the message has been identified and can be directly tied to the data.

c) The message has been “stamped” with the appropriate time and date to ensure the transaction is verified as final.

14. **Symmetric Key Encryption:** In symmetric key encryption, the sender and receiver share a "secret" key. Using this key, a message can be encrypted into "cyphertext". Cyphertext looks like a random sequence of characters and is completely meaningless to anyone unless they also have the secret key, in which case they can decrypt the cyphertext back into the original message and read it.

    Using symmetric key encryption, eavesdropping and unwanted backups of messages no longer are a problem (unless the eavesdropper knows what the secret key is). It also becomes harder for someone to modify messages in transit in any kind of a meaningful way.

    The problem with symmetric key encryption is precisely the fact that the sender and receiver must share the same secret key. Unless you meet in person, how do you communicate this key in a way that is secure? What if you want to send a secure message to someone on the other side of the world? How do you get them the secret key quickly in a way that eavesdroppers can't detect?

15. **Asymmetric Key Encryption:** In asymmetric key encryption, also known as "public key" encryption, each person has two keys. Any cyphertext created using one of the keys can only be decrypted using the other key. For example, keys "K1" and "K2". If you encrypt your message with K1, then only K2 can be used to decrypt it. Similarly, if you encrypt using K2, only K1 can be used to decrypt it. This is distinctly different from symmetric encryption where you only have one key that performs both functions on the same message.

    In asymmetric key encryption, the two keys that each person possesses are commonly named the "private" and "public" keys because the "public" one is published or given out freely to anyone who wants a copy and the "private" one is kept secret. The security of asymmetric key encryption depends on the fact that no one except you can ever access your private key.

    Asymmetric key encryption allows you to do many clever things:

    a) **Send an Encrypted Message:** To send a secure message to someone, encrypt it with their public key. In this way, only the intended recipient, who has the respective private key, should ever be able to decrypt and read the message. This solves the problem of eavesdropping and the problem of communicating secret keys that is inherent in symmetric encryption.

    b) **Prove You Sent A Message:** To prove to someone that you sent a message, encrypt the message (or just a piece of it) with your private key. Then, anyone can decrypt it with your public key and read the contents. The fact that your public key decrypts the message proves that you sent it -- you cannot deny this fact.

c) **Sign a Message:** A message signature proves that you sent the message AND allows the recipient to determine if the message was altered in transit. This is done by encrypting a digest of the message using your private key. The recipient can decrypt this and compare it to a digest the message actually received. If they match, then the message is unaltered and was sent by you.

d) **Encrypted, Signed Messages:** The most secure form of communication is to first add a signature to the message and then to encrypt the message plus signature with the recipient's public key. This combines all of the benefits of all of the techniques: security against eavesdropping and unexpected storage, proof of sender, and proof on message integrity.

16. **PGP, GnuPG(GPG) and S/MIME:** There are a few widely used forms of asymmetric key encryption for email: S/MIME and PGP/GPG. These allow you to add signatures and/or encryption to messages. GnuPG(GPG) can be obtained from **GnuPG.org** and has various client and plug-in options. S/MIME is built into many email clients like Microsoft Outlook, but you must obtain an S/MIME certificate from a third-party company such as **Thawte.com**.

    PGP/GPG and S/MIME have interoperability problems that come in when sending or receiving encrypted or signed messages. The first problem is that PGP/GPG and S/MIME are completely incompatible. If you are using PGP/GPG and the correspondent is using S/MIME, you will not be able to send each other secure messages.

    That said, PGP/GPG have been fully compliant with an Internet messaging standard (OpenPGP Message Format - RFC 4880) since 1997 and PGP/GPG -encrypted email accounts for well over 90% of the current encrypted email traffic on the Internet. So, using PGP/GPG will make you compatible with the majority. However, what really counts is the minority that you actually need to communicate with and their needs. Therefore you may find a need for the use of S/MIME if your correspondents like using its 3rd party issued certificates for email communications rather than PGP/GPG 's trust model. It is useful to know that some email clients, such as Microsoft Outlook, can be configured to use BOTH PGP/GPG and S/MIME so that you can correspond securely using whatever method is necessary at the moment.

    The other interoperability issue involves "key exchange". If you want to send an encrypted message, you first need a public key; if you want to prove that you signed a message or that the message that you sent was unaltered, you first need your public key. So there is the necessity of trading public keys before secure communication can ensue. There are various ways of doing this (including email) and PGP/GPG offers "key servers" from which your correspondents' keys can be downloaded to make the process easier. However, not everyone has their PGP/GPG keys listed on a key server, let alone the same key server, and not everyone uses PGP/GPG, so the key exchange issue is still an impediment to sending secure messages -- especially if you have to send them quickly.

17. **Desktop to Desktop:** With desktop to desktop encryption, the message is encrypted at the originating desktop and is decrypted at the destination desktop(s).

18. **Gateway:** An email device that is used to virus check, content filter and perform administrative functions such as forwarding, ensuring delivery, etc.

19. **Push:** Sending a message to multiple recipients, for example, pay advices.
20. **Pull:** Each node requests its message from a server, a technique usually used to keep software updated.
21. **Sender control**: To be able to expire the message before or after it is read so that it can no longer be read by the recipient(s).

B. Declarations

1. Must comply with Federal regulations.
2. Must allow server document broadcast (for example - pay statements).
3. Must be accessible to the internet for external customers.
4. Must provide automatic key management at the server level.
5. Must have an audit trail capability.
6. Must provide sender control.
7. Must support desktop to desktop and gateway communication.
8. Must utilize push technology and not pull.
9. Must run on all standard desktop operating systems.
10. Must be Server Based or appliance based, and centrally managed.
11. Must be Active Directory / LDAP integrated.
12. Outside entities must incur no extra cost to respond to an encrypted email created and sent to them by the State.
13. Must not require outside entities to install software to use the solution.
14. Must be housed within the State's infrastructure.
15. Must allow for tight integration of virus scanning and content filtering at the gateway.
16. Must support standard State email package(s).
17. Must be asymmetric.
18. Must provide security for attachments.
19. Must provide central Key Management.
20. Must not unreasonably impact email response time negatively.
21. Must provide a mechanism for recovering emails for cases like e-records.
22. Must be capable of encrypting 'data at rest'.

V. Definition of Ratings

COMPONENT RATING	USAGE NOTES
STANDARD – DTI offers internal support and/or has arranged for external vendor support as well (where applicable). DTI believes the component is robust and solidly positioned in its product life cycle.	These components can be used without explicit DTI approval for both **new projects** and **enhancement** of existing systems.
DECLINING – Deprecated - DTI considers the component to be a likely candidate to have support discontinued in the near future. A deprecated element is one becoming invalid or obsolete.	Via the State's waiver process, these components must be explicitly approved by DTI for **all projects**. They must not be used for **minor enhancement** and **system maintenance** without explicit DTI approval via the State's waiver process.
DISALLOWED – DTI declares the component to be unacceptable for use and will actively intervene to disallow its use when discovered.	No waiver requests for new solutions with this component rating will be considered.

A. Missing Components – No conclusions should be inferred if a specific component is not listed. Instead, contact the TASC to obtain further information.

VI. Component Assessments

The use of the secure email feature will be governed by the Delaware Information Security Policy. The only exception is correspondence with Federal Agencies where Federal guidelines require the use of a product of their specific choice.

.

#	Component	Rating	Comments
1	Egress	Standard	