Security Defined

A Security Audit of MyMail®

Department of Information Technology
Department of Physics
Angelo State University

September 19, 2007

Mr. Jason M. Brake
Information Technology Security Officer

Dr. Andrew B. Wallace
Professor and Head of Physics

Introduction

This document is the official independent security audit and report of MyMail®'s Secure Email product. The report details our findings of MyMail®'s Secure Email product when tested against known security and cryptographic standards, published laws and regulations, and competitive products. Overall, we find MyMail®'s Secure Email product to provide the highest level of encryption that *is transparent to the end user* among secure email products available on the market today.

Angelo State University (ASU) is the site of the Texas State Data Center[1] (TxSDC) and is recognized by the State of Texas as a leader in computer data and network security as demonstrated by its continuous operation of the TxSDC since 1993. In addition ASU is recognized as a leader in educational and Family Educational Rights and Privacy Act of 1974 (FERPA) compliant software evaluation and testing through its relationship with SunGard Higher Education. This relationship resulted in a complete implementation of Banner and established standards for data, integrity, and security[2] at ASU.

Summary of Findings:

1. MyMail®'s Secure Email product meets the requirements of FERPA 20 USC § 1232g, and in particular finds MyMail®'s Secure Email product meets the requirements of subsection (b)(2), thereby allowing schools and universities to use MyMail®"s Secure Email solution to send and receive private and personally identifiable information, as well as personal education records via a secure email system.

2. MyMail®'s Secure Email product meets the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) 42 USC § 1320d-2(d), and in particular finds MyMail®'s Secure Email product meets the requirements of the HIPAA regulations published at 45 CFR §§ 164.304-306, thereby allowing health care providers, schools and universities, and insurance companies to use MyMail®'s Secure Email product to send and receive private and personally identifiable health information via a secure email system.

3. MyMail®'s Secure Email product is the best secure email solution among competitive products because of MyMail®'s:

    - Secure user authentication
    - Secure point-to-point transmission of electronic data
    - Robust and secure dynamic encryption algorithm
    - Secure key management and data storage
    - Secure audit controls

Overview

One definition of secure is "safe from penetration or interception by unauthorized persons.[3]" This definition applies to electronic information access, storage, and transmission. Two acts of congress, the Family Educational Rights and Privacy Act of 1974 (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) have an effect on our definition of secure and security of electronic information.

Section (b)(2) of FERPA 20 USC S. 1232g states "No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of releasing, or providing access to, any personally identifiable information in education records other than directory information.[4]" This statement requires institutions of public and higher education to address information access control, audit controls, and security.

Section 164.304 of HIPAA defines technical safeguards as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.[5]" This statement is one of four HIPAA standards known as the Security Rule. Technical safeguards include access control, audit controls, integrity, person or entity authentication, and transmission security.

MyMail® addresses FERPA and HIPAA through:

- User Authentication
- Secure Transmission
- Dynamic Encryption Algorithm
- Encrypted Key and Data Storage
- Audit Controls

MyMail® users are authenticated via username and password through a simple web interface shown in Figure 1. If a user checks the "public location" box, then an auto logout of 6 minutes with a 2 minute warning is enforced. If a user does not check the "public location" box, then a user default auto logout of 60 minutes is enforced. The user may change the auto logout time period from 10 minutes to 5 hours.

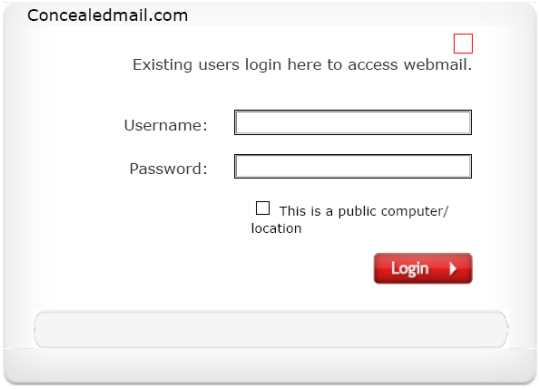

Figure 1: Sample MyMail® user login.

Once authenticated, the user is presented a secure HyperText Transfer Protocol (HTTPS) interface shown in Figure 2. Directions for using the user web interface are provided under the help option.

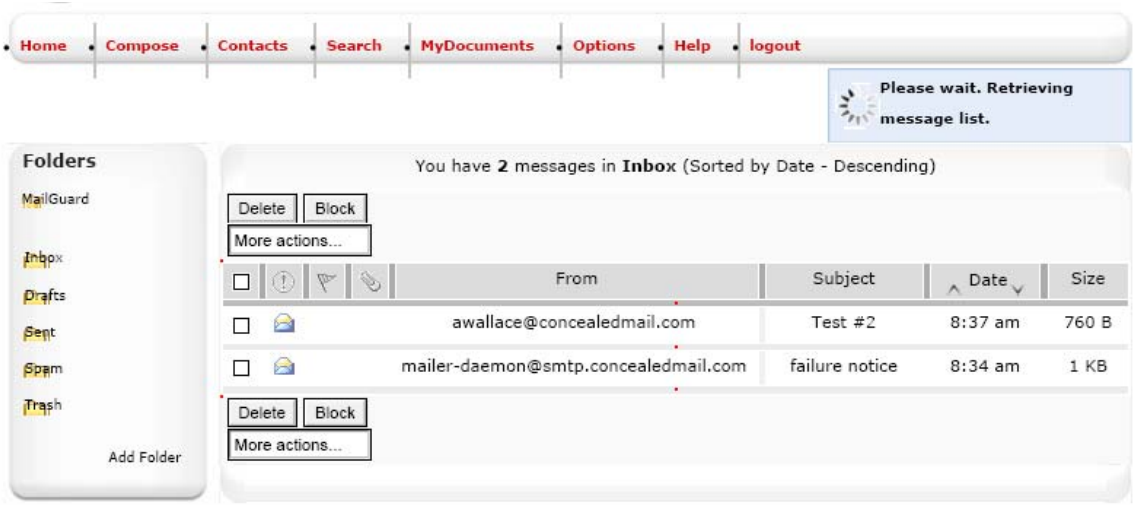

Figure 2: Sample MyMail® user interface.

There are three user configurable options concerning security. These options are EsSentry, Custom Filters, and Spam blocking. EsSentry allows each MyMail® user to control addresses they receive mail from by either adding a sender's email address to a white list or by forcing a sender authenticate him/herself through a challenge-and-response protocol. When EsSentry is enabled, only email messages whose email addresses appear in the recipient's white list or those who have successfully authenticated themselves through the challenge-and-response protocol are delivered to the recipient's mail box. All other messages are held in a non-authenticated user storage space of each recipient's mail box until one of the following events occurs:

1) a message sender authenticates him/herself,
2) an intended mail recipient accepts or rejects the message,
3) a message is deleted by the system after a period of time (default is 15 days),
4) a user's mail box space is full and deleting older non-authenticated messages would allow delivery of an authenticated senders' message, or
5) a sender fails to authenticate him/herself through a challenge-and-respond protocol after several attempts (default is nine).

It is important to note, that although a sender may have failed the challenge-and-response protocol, a sender is not automatically "black listed". EsSentry does have a black listing feature, which immediately terminates attempted mail delivery to a recipient from an email address listed in the recipient's black list. MyMail® requires a recipient to manually add an email address they want black listed from their account to prevent unintentional loss of legitimate email messages. White and black lists are configurable by the user or administrator. The user may move sender addresses between white and black lists as needed. Custom filters direct incoming email to specific folders. Up to ten custom filters are allowed in MyMail®. The user can set the order in which custom filters are applied to redirect unwanted incoming mail. Spam blocking simply blocks incoming mail by banning a sender's email address. Spam blocking is different from EsSentry in that there is no time limit on a banned sender's email address. The user may unblock a banned sender's email address if desired. All three of these options discussed above address the "safe from penetration" portion of our definition of secure. "Interception by unauthorized persons" is addressed through secure transmission, dynamic encryption, and encrypted key/data storage.

MyMail® secures transmission of electronic information through its secure architecture[6] shown in Figure 3. Users connect to MyMail® using a web browser capable of HTTPS and their local internet service provider (ISP). After a MyMail® user is authenticated on the Email Data Host (EDH), a Secure Socket Layer (SSL) is opened between the EDH and the user's web browser. Specifically, the EDH assigns a dedicated port to the web browser and all information through this port is encrypted. Security certificates on the EDH must be up to date and valid for SSL to open between the EDH and user's web browser. If a user does not have a SSL compliant web browser, then no SSL connection between EDH and the user's web browser is made. Failed SSL requests cause the EDH to return an error to the user's web browser. This error instructs the user to switch to a SSL compliant web browser before using MyMail®. Server to server connections between EDH and Paired Key Store (PKS) and between Key Signing Authority (KSA) and PKS are accomplished through Secure Shell (SSH®) on dedicated ports. All information on these dedicated ports is encrypted by SSH®. MyMail® secure architecture meets our definition of secure. User-to-user connections are encrypted point-to-point with SSL and server-to-server connections are encrypted through SSH®. One advantage of this secure architecture is that encryption is transparent to users of MyMail®.

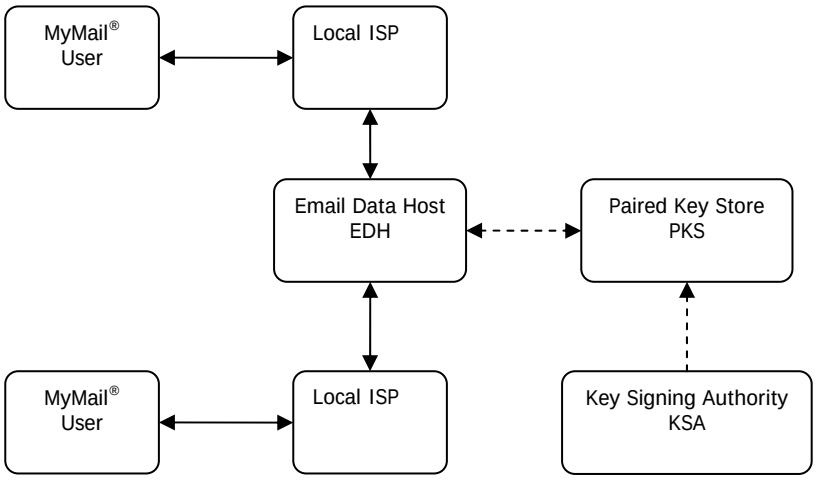

Figure 3: MyMail® Secure Email Architecture. Solid arrows represent SSL connections after user authentication and dashed arrows represent SSH® connections.

MyMail® uses a dynamic encryption algorithm[6], shown in Figure 4, which provides a unique solution for integrity and security of electronic information. Upon creation of a user account, public and private keys are generated and stored on the PKS. When a user sends an email message, their public key is retrieved from the PKS and a Dynamic Row Secret (DRS) is generated by the KSA using a robust random number generator which ensures each DRS is unique. The public key and DRS are encrypted via OpenSSL and stored on the EDH. Electronic mail data is compressed, shredded into four blocks, and encrypted with the DRS using the Advanced Encryption Standard (AES). The National Institute of Standards and Technology[7] states there are approximately 10^{38}, 10^{57}, and 10^{77} possible keys for 128-bit, 192-bit, and 256-bit AES keys respectively. MyMail® uses 256-bit AES encryption; therefore, the initial number of keys is approximately 10^{77} per DRS. It would take a machine trying 1 key per second 10^{69} years to recover a single 256-bit AES key if the same DRS is used to encrypt all email messages on the EDH. To put this time in perspective, scientists set the upper limit for the age of the universe at 10^{10} years. MyMail®'s dynamic encryption algorithm meets our definition of secure. Dynamic row secrets are only used once, 256-bit AES encryption is used, and encrypted email data is shredded and stored on the EDH.

Access to information stored on the EDH is controlled and restricted. Authenticated users can access information in human readable form through an HTTPS web browser or a Post Office Protocol version 3 Secure (POP3S) email client. MyMail® system administrators can only view encrypted data on the EDH if they have the correct authentication and permission. The robustness of MyMail®'s secure email product prevents others, including system administrators, from viewing any user's email message in a human readable form.

MyMail® data storage on the EDH is different than data storage on the PKS. On the EDH, encrypted data is stored in a database format by default. A file system format for data storage is available to the administrator if desired. The encrypted DRS serves as the fingerprint/signature for a particular email message. Mail header information needed to send the encrypted MyMail® message through the internet is not encrypted. This information must remain in plain text in order for the encrypted DRS (fingerprint/signature) and email data (message body) to propagate through the internet. Email data for a particular message is shredded into four 256-bit AES encrypted blocks and then base 64 encoded in the database. These 4 blocks are tied to the base 64 encoded DRS and plain text mail header information. On the PKS, public keys are stored in a database format. Public keys for each MyMail® user are encrypted in the database along with the user's authentication data. This data format allows the EDH to retrieve a user's public key to be encrypted with the DRS obtained from the KSA. Encrypted key and data storage meet our definition of secure.

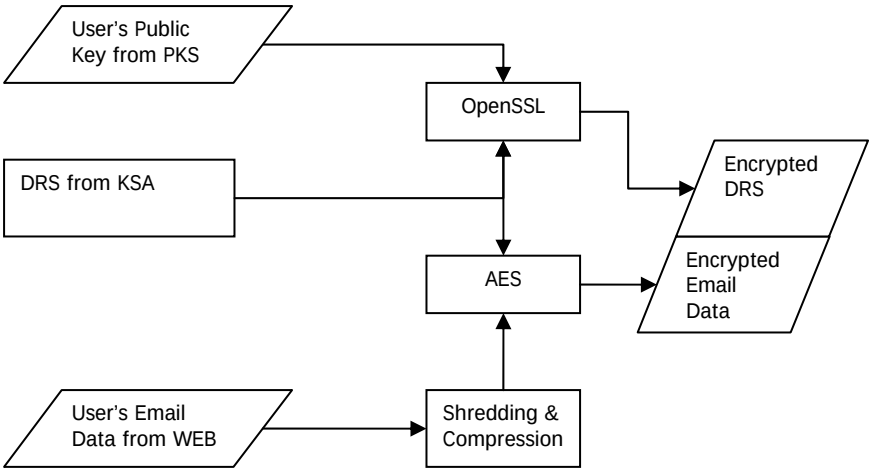

Figure 4: MyMail® dynamic encryption algorithm.

For security, MyMail® provides options for user key management and database management. These options are only configurable at the time of system installation. The system installer or administrator has the following key management options:

1) The ability to allow a system administrator to set or reset user passwords at their discretion;
2) The ability to reset a user account password with a "universal" reset password; and
3) Disallowing a system administrator to set, reset, or recover user account passwords.

Options 1 and 2 provide detailed audit control for password changes made by system administrators. Option 3 provides the highest level of user security by only allowing the user to change and modify passwords. Database management tools can be installed to enable secure email data storage backup and restore service.

Any person that either controls or has access to one or more pieces of the architecture or algorithm is subject to audit control. This control is necessary to meet and document our definition of secure. An administrator must be able to determine what has been done, when it happened, how it happened, and potentially who penetrated or intercepted one or more pieces of the architecture or algorithm. For example, if someone purges a MyMail® user's encrypted email, what email was purged, when the email was purged, and who purged the email are critical pieces of information for audit control to function properly.

MyMail® uses several audit controls on the EDH to meet our definition of secure. MyMail® audit controls depend on the type of administrator: webmaster or provider. Through the MyMail® webmaster interface, the webmaster has access to site configuration, user account management, security and operations, package control, and statistical reports. Figure 5 shows a sample of audit control tools available to the MyMail® webmaster. Security and operation of the EDH includes white listing (API Access), black listing (Ban IP Address), relay and spam prevention (Reject incoming address), and chronological mail purging (Purge mails). The webmaster has access to statistical reports for usage and click through (Banner stats) besides graphical and charted data on mail volume, user sign up activity, and mail size.

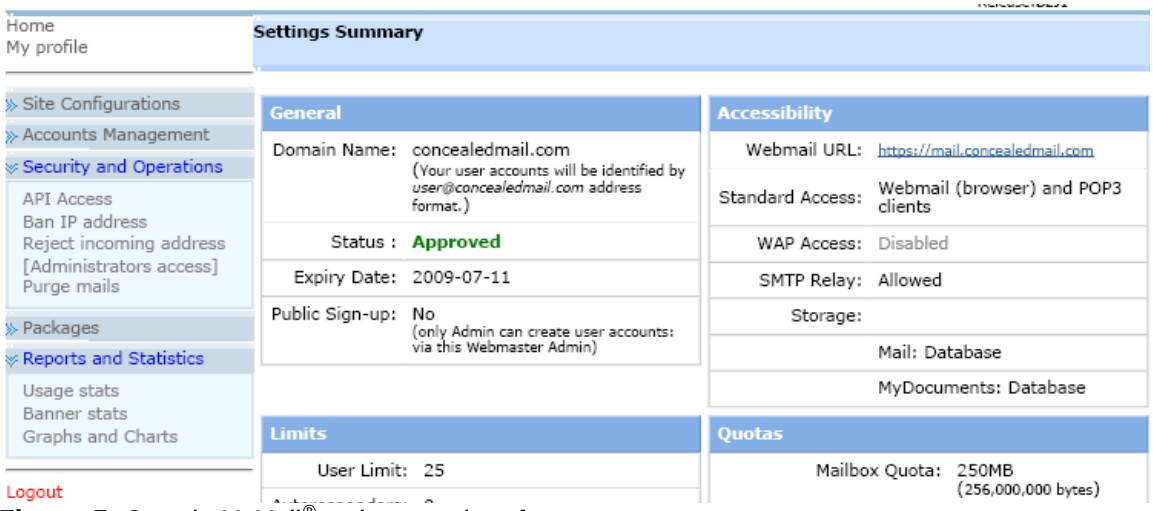

Figure 5: Sample MyMail® webmaster interface.

The MyMail® provider interface, shown in Figure 6, gives the provider audit control over data compression and storage format, domains, remote email access (POP3 server), database management, and statistical reports. Compressing HTTPS data increases the amount of data sent to the user's web browser through an SSL connection. Encrypted email data storage on the EDH increases storage capacity and security. The provider also has the option of whether to store data in a database format or in a regular file system format. Email domains can be added, removed, and edited by the provider. Email aliasing is turned off by default for a domain. The provider must turn on email aliasing for a domain before the webmaster can add an alias for a username. Quotas can be set on a per domain basis through the provider interface or on per user basis through the webmaster interface. Remote email access may be configured, disabled, or enabled on a per domain basis. If installed, database management tools provide backup and restore options. The provider has access to statistical reports for domain usage with graphical and charted reports on user sign up activity and mail volume.

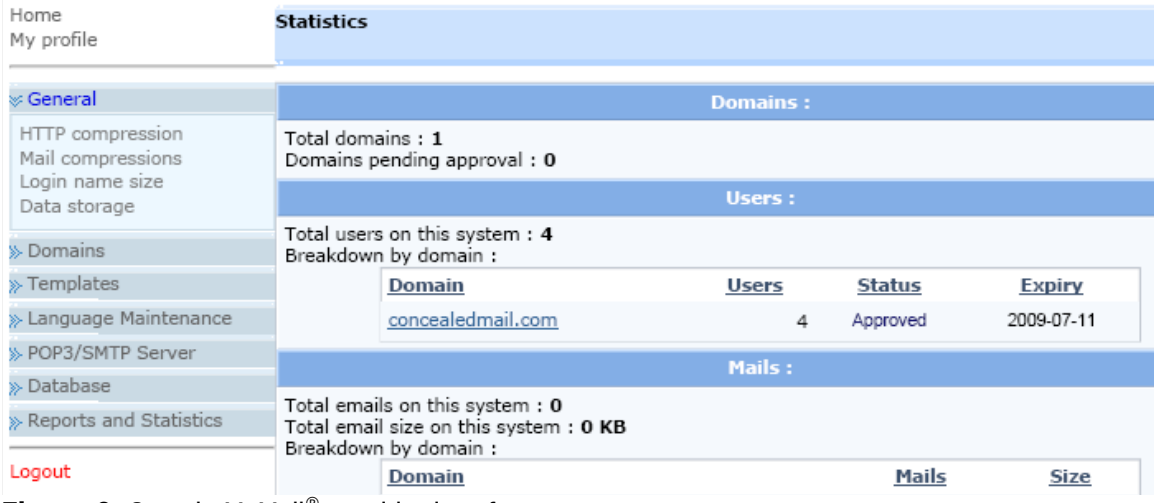

Figure 6: Sample MyMail® provider interface.

No user accounts for the webmaster or provider exist on the EDH. Therefore, neither the webmaster nor the provider can change audit control information. This information can only be changed by a MyMail® system administrator. Audit control information available to the EDH system administrator includes user activity, web server activity, SSH® activity, mail server activity, database activity, and operating system messages. Audit control information available to the PKS/KSA system administrator includes administrator activity, SSH® activity, database activity, and operating system messages. Audit control logs are rotated and backed up automatically by the operating system. All of these audit controls can be used to meet and document our definition of secure.

Benchmarking MyMail®

MyMail® provided documentation[6, 8] and two virtual machines running version 2.3.0: one machine for the EDH and one machine for the PKS/KSA. Although this architecture is not identical that shown in Figure 3, the combination of PKS and KSA into a single virtual machine was satisfactory for benchmarking MyMail®. Our benchmarking process included a cryptanalysis of encrypted email data, an email feature comparison to similar secure email products, and a MyMail® end user ease-of-use analysis. The same cryptanalysis was performed on similar secure email products if encrypted email data was available. We chose CertifiedMail, HushMail, and PGP® for cryptanalysis and email feature comparison. Documents were downloaded from CertifiedMail[9, 10], HushMail[11], and PGP®[12] addressing secure email features.

Our cryptanalysis included frequency analysis, length of alphabet, variance, index of coincidence, probable key length, and disorder of encrypted email data. A standard email message was used to benchmark each secure email product. Cryptanalysis source code is available from the authors of this security audit. The results of our cryptanalysis are summarized in Table 1. Length of cipher alphabet is the number of unique characters in the encrypted message body. The variance of the encrypted message body is a measure of its statistical dispersion, indicating how far an encrypted character is from the expected plain text value. Index of coincidence is the probability that two characters selected from an encrypted message body are identical. If plain text is used to calculate index of coincidence, the result is 0.0656. If random, but uniformly distributed, plain text is used to calculate index of coincidence, the result is 0.038. Smaller values of index of coincidence indicate random, but non-uniformly distributed text. Index of coincidence is inversely related to probable key length. Small index of coincidence implies a large probable key length. Disorder is a statistical measure of information contained in the encrypted message body. Information is inversely proportional to probability. Therefore; the larger the

disorder in the encrypted message body is, the smaller the probability of identifying information. The data in Table 1 states that the MyMail® dynamic encryption algorithm produces a larger variance and larger disorder with a larger index of coincidence and hence shorter probable key length. Our cryptanalysis of the MyMail® dynamic encryption algorithm meets our definition of secure.

Table 1: Cryptanalysis summary.

Benchmark	**MyMail®**	**HushMail**	**PGP®**
Length of Cipher Alphabet	71	69	69
Variance	777	103	114
Index of Coincidence	0.0154258	0.0152943	0.0153750
Probable Key Length	38	62	57
Disorder	4.17603	4.17384	4.17261

Besides cryptanalysis, an email feature comparison of MyMail® and other secure email products was conducted to assess point-to-point encryption, key management, amount of encrypted message body text available to an attacker, and potential of user identity theft. MyMail® is encrypted point-to-point using SSL compliant web browsers and POP3S connections for remote email access with a third-party email client. MyMail® encryption keys are dynamic in that each key is only used once *per message per user*. This type of key management is one of the best approximations of the one-time pad key. One-time pad keys are only used once and in theory provide the highest level of information security[13]. MyMail®'s default mail box quota and file attachment limit indicate a potential attacker does not have access to large amounts of encrypted message data. User identity theft is minimized with MyMail® because user authentication is achieved through an email address internal to the EDH. An external email address such as jonsmith@myoffice.com can be pulled into the EDH by a provider administrator. Authenticating users internally prevents unauthorized persons from using MyMail®. User authentication with other secure email products is through an external email address which can be cloned by a potential attacker.

Table 2: Email feature comparisons between MyMail®, CertifiedMail, HushMail, and PGP®.

Feature	**MyMail®**	**CertifiedMail**	**HushMail**	**PGP®**
Encrypted Point to Point	Yes	No	Yes	Yes
SSL/HTTPS Connectivity	Sender/Recipient	Recipient Only		
Encrypted Message Store	Yes	Yes	Available	Available
Encryption Standard	256-bit AES	128 bit "heavy"	AES	
Key Generation Standard	DRS/PKS		RSA	RSA
Keys	Per Message	Per User	Per User	Per User
Digital Fingerprint/Signature	Yes (DRS)	Yes	Yes	Yes
Logs and Reporting	Yes	Yes		No
Mail Filtering	Yes	Yes	Yes	No
Web-based Administration	Yes	Yes		No
Firewall Compatible	Yes	Yes		
User ID	Internally Hosted	Externally Hosted	Externally Hosted	Externally Hosted
Key Storage on Server	Yes	Yes	Yes	Available
Attachment Limit	5 MB to 20 MB	100 MB	25 MB	Depends on ISP
Mailbox Quota	50 MB to 3 GB		250 MB	Depends on ISP
Sender Interface	Outlook/Web	Outlook Only	Outlook/Web	Outlook
Recipient Interface	Outlook/Web	Outlook/Web	Outlook/Web	Outlook
Remote Email Access	POP3S	POP3/IMAP	POP3/IMAP	

Our final analysis centered on MyMail® web site design keeping end user ease-of-use a high priority. Web site design analysis included speed, home page design, ease of navigation, use of multimedia, browser compatibility, content presentation, currency, and availability of further information. We applied this analysis to user, provider, and webmaster interfaces. Results of this analysis are shown in Table 3 indicate MyMail® secure email provides good end user ease-of-

use. The MyMail® webmaster has control over website title, logo, index, text display options, and footer information. Menus are clear and easy to navigate. Graphics are not overused and they provide a good user experience. We tested MyMail® web interfaces in Internet Explorer 7 and Firefox 2.0.

Table 3: MyMail® web site design.

Criteria	Yes/No/Not Applicable
1. Homepage downloads efficiently.	Yes
2. Homepage is attractive, has strong eye appeal.	Yes
3. You can tell where you are immediately (clear title, description, image captions, etc...)	Yes
4. There is an index, table of contents, or some other clear indicator of site contents.	Yes
5. Site sponsor/provider is clearly identified.	Yes
6. Information/method for contacting sponsor/provider is readily available.	Yes
7. Copyright date or date site established is easy to determine.	Yes
8. User is able to move around within the site with ease.	Yes
9. Directions for using the site are provided if necessary.	Yes (user), No (admin)
10. Directions are clear and easy to follow.	Yes
11. Links to other pages within the site are helpful and appropriate.	Yes
12. Internal and external links are working properly.	Yes
13. Each graphic, audio file, video file serves a purpose.	Yes
14. Graphics, animations, sound clips make a significant contribution to the site.	Yes
15. Site is equally effective with a variety of browsers.	Yes
16. There is sufficient information to make site worth visiting.	Yes
17. The same basic format is used consistently throughout site.	Yes
18. Information is easy to find (no more than three clicks).	Yes
19. List of links are well organized and easy to use.	Yes
20. The date of last revision is clearly labeled.	Yes
21. Out-dated material has been removed.	Not Applicable
22. A working link is provided to a contact person or address for further information.	Yes
23. Links to other useful Web sites are provided.	Not Applicable

Conclusion

The strengths of MyMail®"s secure email product may be summarized as:

- Secure user authentication
- Secure point-to-point transmission of electronic data
- Robust and secure dynamic encryption algorithm
- Secure key management and data storage
- Secure audit controls

Weaknesses of MyMail®'s secure email product may be summarized as:

- Directions for using administrative sites are nonexistent.

We recommend the MyMail® user interface change "This is a public location/computer" to "My location is public.", add a link to the user login interface directing the user on how to reset a lost or forgotten user password, and provide user information on how MyMail® interacts with external spam filtering services, email backup, and email recovery.

We recommend the MyMail® webmaster interface add a help feature for using the webmaster interface, either populate or remove the drop down menu for default country in miscellaneous settings, remove the add alias option in user management because email aliases are added through browse users option, change the administrators access link in Figure 5 to a tool tip because it's purpose is unclear, add a repeating mail purge feature such as 1 day, 1 week, or 1 month of selected email age, clarify instructions for adding custom fields, and set a dynamic minimum width for the random string image to prevent string width exceeding display width.

We recommend the MyMail® provider interface add a help feature for using the provider interface.

In closing, there were a few MyMail® secure email product features we could not audit. These features include auto-repeaters, packages, email data shredding before storage on the EDH, interaction with packet-shaping and spam filtering services, and load testing for scalability.

References

1. Texas State Data Center Services Overview, Department of Information Resources, (Feb 2003). See http://www.dir.state.tx.us/datacenter/consolidationOverview/contents.htm for more information.

2. Guidelines for Data Standards, Data Integrity and Security, Portico Project, Angelo State University, (Apr 2007). See http://www.angelo.edu/services/banner/documents/Data_Standards_Document.pdf for download.

3. See http://dictionary.reference.com/.

4. Family Educational Right to Privacy Act, US Department of Education, 20 USC S. 1232g, (1974). See http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html for download.

5. HIPAA Security Series, Volume 2/Paper 4, Centers for Medicare & Medicaid Services (May 2005). See http://www.cms.hhs.gov/hipaa/hipaa2 for download.

6. Introduction to MyMail®, Bob Derby and Tom Selgas, (MyMail, Inc. Aug 2007).

7. Advanced Encryption Standard (AES) Questions and Answers, Computer Science Division, National Institute of Standards and Technology, (Aug 2007). See http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html for download.

8. MyMail® Email Security White Paper, Bob Derby and Tom Selgas, (MyMail, Inc. Aug 2007).

9. CertifiedMail Server Version 3.0, CertifiedMail.com, Inc. (Aug 2007). See http://www.certifiedmail.com/ for download.

10. Secure Messaging and the Final HIPAA Security Standard, CertifiedMail, Inc. (Aug 2007). See http://www.certifiedmail.com/ for download.

11. Hush Encryption EngineTM White Paper, Version 2.0, Hush Communications Corporation, (Jul 2001). See http://www.hushmail.com/ for download.

12. PGP® Desktop Email 9.6, PGP Corporation, (Aug 2007). See http://www.pgp.com/ for download.

13. Cryptology, Albrecht Beutelspacher, (The Mathematical Association of America, 1994).