

White Paper On Email Encryption Technologies

A principal SFA security risk is the failure to secure personal information provided by students. Schools, lenders, state agencies, contractors and other government agencies routinely exchange this type of information with SFA. Inappropriate disclosure not only impairs the trust between SFA and their applicants it may also violate the Privacy Act of 1974. As presented by the SFA Security and Privacy Advocate (SPA), this failure to secure personal information requires addressing through the challenge of improving the confidentiality of email communications with SFA's 6,000+ partners. The complexity of the challenge compounds since each partner has their own infrastructure, operating systems and mail clients. SFA must confront the implementation of email confidentiality in a heterogeneous environment before successfully meeting this challenge.

The purpose of this paper is to present encryption technology solutions specifically designed to address the challenge of transmitting and receiving email messages and files contained in email through (1) File Encryption and (2) Session Encryption. A brief description follows:

- ***File Encryption:*** Uses a mathematical function to alter the email message, which can include an attached file, to render it incomprehensible. The email message or attached file is then sent across the Internet without further protection. The recipient receives the message in encrypted format and must decrypt the message to read it. This method requires the originating and receiving parties to possess an automated system to discover the necessary encryption / decryption keys.
- ***Session Encryption:*** Creates a secure communication path between the originator and the receiver and then sends the email message in its native, unencrypted state. The originator and receiver automatically agree to use unique session keys for this method to work, and therefore render all transmissions encrypted between the originator and the receiver. When finished communicating, the originator and receiver agree to end the session and revert to their respective unencrypted exchanges. Inherent in this method is the need to have compatible systems at both ends to agree on encryption standards and keys.

Each of the above solutions has benefits and drawbacks, which requires evaluation in relation to SFA's goals and future technology efforts. To assist in this evaluation, these solutions are compared against six methods of implementation; each implementation was selected for their responsiveness to SFA's challenge.

File Encryption Technology

- ***Virtual Private Network (VPN)*** - A virtual private network (VPN) is a private data network, which uses public telecommunication infrastructure to maintain privacy through the use of tunneling protocols and security procedures. This is in contrast to a system of owned or leased lines that can only be used by one organization. The VPN gives an organization the same capabilities at much lower cost by using shared public infrastructure rather than a private one.
- ***Hypertext Transfer Protocol (HTTP)*** - The set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the Web. Relative to the TCP/IP suite of protocols, which are the basis for information exchange on the Internet, HTTP is an application protocol.

- HTTP with Secure Socket Layer and Certificates – A HTTP server configured with a server certificate can request a client transmit their certificate for identification purposes. This variant of HTTP with SSL is moderately more expensive than HTTP with SSL however the issues of certificate authority operations and procedures must be defined. The application that handles the email must be capable of accepting certificates and using them for identification and authentication.

Session Encryption Technology

- PGP® - Pretty Good Privacy® is a powerful cryptographic product family that enables people to securely exchange messages, and to secure files, disk volumes and network connections with both *privacy* and *strong authentication*. PGP is more convenient to use in conjunction with an interface that integrates it into programs for reading and sending mail. Several such interfaces are available for popular mail programs.
- S/MIME - S/MIME (Secure Multi-Purpose Internet Mail Extensions) is a secure method of sending email that uses the RSA encryption system (a public key encryption algorithm). S/MIME is included in the latest versions of the Web browsers from Microsoft and Netscape and has the endorsement of other vendors that make messaging products.
- Password Protected Files - Attaches a password protected file to an email

Each implementation is compared against six attributes of cost, complexity, time to market, authentication, encryption, and cross platform. Of these attributes, *authentication* is the most relevant when applied to SFA communications due to Privacy Act of 1974 requirements. The following table summarizes the findings when the implementation and attributes are compared against the two, encryption technologies. The table depicts solutions, which are rated as high, medium or low. The more desirable solutions are colored green and the least desirable red.

	Session Encryption			File Encryption		
	VPN	HTTP w/ SSL	HTTP w/ SSL & Certificate	S/MIME	PGP	Password Protected
Cost	High	Low	Medium	Medium	Medium	Low
Complexity	High	Low	Medium	Medium	High	Low
Time to Market	High	Low	Medium	Medium	High	Low
Authentication	High	Low	High	High	High	Low
Encryption	High	High	High	High	High	Low
Cross Platform	Medium	High	High	High	High	Medium
Pro	Strong identification and encryption	Quick, easy and inexpensive, possible interim solution	Possibly integrates into SFA future PKI and CA plans	Strong identification and encryption, possibly integrates into SFA future plans for PKI and CA	Strong identification and encryption, best cross platform	Currently in place
Con	Expensive and difficult deployment due to site install	Weak identification based upon userid	Requires a certificate server and application modification to identify based upon certificate	Must lock into certificates, certificates expire	Difficult installation and maintenance, requires user training	Easy to break, technically or procedurally

File Encryption Technology:

VPN	
<p>Either hardware or software based, the entire transmission channel from the originator to the receiver becomes encrypted regardless of the protocol used. The hardware-based implementation requires router, or other communications device, distribution and connection at each user site. The software-based implementation of VPNs entail the distribution of identification tokens, e.g., fobs, and software to each user site</p>	
Pros	Cons
<ul style="list-style-type: none"> ■ High levels of identification, authentication and encryption ■ Users maintain current email applications ■ Few transitional issues other than the implementation of the VPN 	<ul style="list-style-type: none"> ■ Higher cost ■ Labor intensive installation, configuration and maintenance ■ Expensive configuration management of the distributed hardware or software

HTTP with SSL	
<p>Allows a user to sign-on to a web site to read and send messages similar to Microsoft's HotMail. All communication with the web server is encrypted so data is protected in transit. Requires a server certificate (about \$500) and webmail software from a vendor such as IPSwitch.</p>	
Pros	Cons
<ul style="list-style-type: none"> ■ Most users use a web browser that supports SSL transactions ■ Minimal user configuration ■ Minimal user intervention or coordination of keys or protocols since SSL keys are derived by SSL software ■ Easy to implement since user simply uses the tool for email communications, which contains data protections 	<ul style="list-style-type: none"> ■ Requires server certificate and applications to process and store email messages ■ Users may have to change to an unfamiliar email client ■ Mail requiring privacy protection must originate within the webmail tool versus existing email client ■ Difficult and inconvenient to require a user to use a separate mail tool

HTTP with SSL and Certificates	
<p>Works similarly as the above implementation, but certificates are added to increase the identification and authentication of the entire process. As a combination of two technologies, HTTP with SSL and certificates, its benefits and detractions are essentially the summation of the HTTP with SSL and the certificate process of S/MIME.</p>	
Pros	Cons
<ul style="list-style-type: none"> ■ Most users use a web browser that supports SSL transactions ■ Minimal user configuration ■ Minimal user intervention or coordination of keys or protocols since SSL keys are derived by SSL software ■ Easy to implement since user simply uses the tool for email communications, which contains data protections ■ High levels of identification, authentication 	<ul style="list-style-type: none"> ■ Requires server certificate and applications to process and store email messages ■ Users may have to change to an unfamiliar email client ■ Mail requiring privacy protection must originate within the webmail tool versus existing email client ■ Difficult and inconvenient to require a user to use a separate mail tool ■ SFA users may not have email clients supporting S/MIME protocol

<ul style="list-style-type: none"> ■ and encryption at a medium cost ■ Supported by most major email clients currently on the market 	<ul style="list-style-type: none"> ■ Requires a certificate authority (CA) server, (either be outsourced or housed internally) ■ Requires development and management of both SFA certificate policy and the certificates ■ Higher cost via annualized cost of certificates, certificate expiration, and key issuance and exchange issues
--	---

Session Encryption Technology:

S/MIME	
<p>Uses certificates to sign an encrypted email message between the sender and receiver. Supports Microsoft Outlook, cc:Mail, Eudora and Netscape Communicator. Prepares for message delivery by encrypting the entire message minus the subject in the sender's and recipient's keys. This creates an encrypted message, which only the recipient can decrypt, and authenticates the originators' identity.</p>	
Pros	Cons
<ul style="list-style-type: none"> ■ High levels of identification, authentication and encryption at a medium cost ■ Supported by most major email clients currently on the market 	<ul style="list-style-type: none"> ■ SFA users may not have email clients supporting S/MIME protocol ■ Requires a certificate authority (CA) server, (either be outsourced or housed internally) ■ Requires development and management of both SFA certificate policy and the certificates ■ Higher cost via annualized cost of certificates, certificate expiration, and key issuance and exchange issues

PGP	
<p>Used either as a VPN implementation or an encryption and / or certificate based implementation. Uses unique public / private key pairs to create one-way encryption / decryption paths similar to certificate authorities or PKI solutions. Allows SFA to obtain high levels of identification, authentication and encryption. Set-up is a stand-alone solution that provides client-to-client email encryption with requirement to pass a public key to those who want to send secured email.</p>	
Pros	Cons
<ul style="list-style-type: none"> ■ Stand-alone capacity allows an incremental implementation, with only those most in need of it, and willing to employ it loading the software and creating a key pair ■ Compatible across all platforms including different command prompts such as MS-DOS, Solaris and Linux 	<ul style="list-style-type: none"> ■ Requires key-server to access public keys for email recipients ■ Requires software distribution and installation on every computer used for email transmission ■ Requires users to create a key pair and submit their public key to a key server ■ More complex than certificate based execution

Password Protected Email

The sixth possible implementation attaches a password-protected file to an email. The option to password protect files exists in numerous applications including Word and Word Perfect. The implication of this is that the entire method for protecting privacy data in emails is user intervention.

Pros	Cons
<ul style="list-style-type: none">■ Cost is nearly zero	<ul style="list-style-type: none">■ Uses common password with all partners■ Password changes results in notifying 6000+ users■ Utilities can recover passwords for numerous file types, including Word and Word Perfect■ Requires each user deliberately type privacy data in a text document outside of the email, password protect it, then attach it to the email message

Any of the above solutions may satisfy SFA's requirements for confidentiality for email communications. However, it is evident that none of these implementations provides a simple, clearly preferred choice. Each solution requires evaluation based on the solution, which most appropriately supports users and supports the information technology architecture's strategic vision. Since no "silver bullet" implementation exists, SFA management must consider the array of options best suited for the organization.

All of the presented implementations can solve SFA's challenge, but the proper solution within the unique conditions at SFA should align with SFA's business needs and technical infrastructure.

Addendum on September 26, 2000

When this white paper was written, it was envisioned that the chosen solution would employ only a single technology. It is now obvious that a single technology on its own is capable of providing an optimal solution across the entire user base.

With the additional information gathered, it is now known that individuals using this email application might not be from the same organizational entity or even the same Department. These individuals could be from both the government and the private sector and each user may have a different operating system or browser type. Each user could be connected via dial-up or dedicated Internet enabled local area networks. Because of these issues, the integration of a single technical approach across the entire user base is not possible.

By bridging two technical approaches, it is possible to take the best of each approach while eliminating some of the requirements and drawbacks of using a single technical solution. A product called ZixMail uses a cross technology approach by performing both the S/MIME and the HTTP with SSL operations. The rest of this paper deals with a product called ZixMail.

ZixMail is a service that allows individuals to communicate via encrypted and digitally signed messages with anyone who has an email address. Users do not have to change their existing email address to use ZixMail. If one of the parties of the email communication does not have a digital certificate, ZixMail stores the email on their server and prompts the user to sign on to a secure web site.

There are generally four operational paths which could exist when using ZixMail. They are

Sender	Recipient	Comments
S/MIME	S/MIME	Since both the sender and recipient are using S/MIME, ZixMail passes the message through the mail relay host directly to the recipient.
S/MIME	HTTP with SSL	ZixMail authenticates the sender, receives the secure message, stores it for the recipient on the server, and sends a notification email to the recipient stating a message is in their in-box. The user clicks on the link and the message is displayed in the web browser with SSL enabled.
HTTP with SSL	S/MIME	The user is connected to the ZixMail web server over a SSL connection and composes the email message on the web page. After clicking on the send button the ZixMail server creates an S/MIME email message to the recipient using their public key.
HTTP with SSL	HTTP with SSL	The sender signs onto the secure web site and composes the email message on the web page. After clicking on the send button the ZixMail server stores the email message on the server and sends a notification email to the recipient stating a message is in their in-box. The user clicks on the link and the message is displayed in the web browser with SSL enabled.

The risk in the ZixMail process flow involves the fact that it must perform wrapping procedures that are required when converting the email message to/from S/MIME to HTTP with SSL. During this phase, the

ZixMail server will have access to the raw email message. The issue which poses the greatest risk is the requirement that ZixMail relay email using the senders mail server. The commercial cost of ZixMail is \$1.00 per month per user plus applicable mail relay charges, see attached.

ZixMail	
ZixMail is an application which is used by at least one of the parties in the email communication. This application uses both HTTP with SSL and S/MIME for mail delivery and receipt. The application allows for the sender's creation of a digital certificate	
Pros	Cons
<ul style="list-style-type: none"> ■ Allows secure email to individuals without a digital certificate ■ High levels of identification, authentication and encryption even for individuals without digital certificates ■ Supported by most major email clients and web browsers currently on the market 	<ul style="list-style-type: none"> ■ A separate application must be loaded on SFA workstations ■ ZixMail server processes the message in clear text while wrapping and unwrapping messages however is more secure than clear text email ■ Must configure corporate mail server to allow mail relaying

	Session Encryption			File Encryption			
	VPN	HTTP w/ SSL	HTTP w/ SSL & Certificate	ZixMail	S/MIME	PGP	Password Protected
Cost	High	Low	Medium	Medium	Medium	Medium	Low
Complexity	High	Low	Medium	Low	Medium	High	Low
Time to Market	High	Low	Medium	Low	Medium	High	Low
Authentication	High	Low	High	High	High	High	Low
Encryption	High	High	High	High	High	High	Low
Cross Platform	Medium	High	High	High	High	High	Medium
Pro	Strong identification and encryption	Quick, easy and inexpensive, possible interim solution	Possibly integrates into SFA future PKI and CA plans	Strong identification and encryption even to individuals without certificates	Strong identification and encryption, possibly integrates into SFA future plans for PKI and CA	Strong identification and encryption, best cross platform	Currently in place
Con	Expensive and difficult deployment due to site install	Weak identification based upon userid	Requires a certificate server and application modification to identify based upon certificate	Must enable relaying on mail server and software must be installed on client computers	Must lock into certificates, certificates expire	Difficult installation and maintenance, requires user training	Easy to break, technically or procedurally