



System Assessment and Validation for Emergency Responders (SAVER)

Encryption Software Tools Market Survey Report

March 2014



**Homeland
Security**

Science and Technology

U.S. Department of Homeland Security



System Assessment and Validation for Emergency Responders

Prepared by the National Urban Security Technology Laboratory

The *Encryption Software Tools Market Survey Report* was prepared by the National Urban Security Technology Laboratory for the U.S. Department of Homeland Security, Science and Technology Directorate.

The views and opinions of authors expressed herein do not necessarily reflect those of the U.S. Government.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government.

The information and statements contained herein shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the U.S. Government.

With respect to documentation contained herein, neither the U.S. Government nor any of its employees make any warranty, express or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose. Further, neither the U.S. Government nor any of its employees assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed; nor do they represent that its use would not infringe privately owned rights.

Distribution authorized to Federal, state, local, and tribal government agencies only for administrative or operational use, March 2014. Other requests for this document shall be referred to the SAVER Program, U.S. Department of Homeland Security, Science and Technology Directorate, FRG Stop 0203, 245 Murray Lane, Washington, DC 20528-0203.

FOREWORD

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercial equipment and systems, and provides those results along with other relevant equipment information to the emergency responder community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL). The SAVER Program mission includes:

- Conducting impartial, practitioner-relevant, operationally oriented assessments and validations of emergency response equipment; and
- Providing information, in the form of knowledge products, that enables decision-makers and responders to better select, procure, use, and maintain emergency response equipment.

Information provided by the SAVER Program will be shared nationally with the responder community, providing a life- and cost-saving asset to DHS, as well as to Federal, state, and local responders.

The SAVER Program is supported by a network of Technical Agents who perform assessment and validation activities. Further, SAVER focuses primarily on two main questions for the emergency responder community: “What equipment is available?” and “How does it perform?”

As a SAVER Program Technical Agent, the National Urban Security Technology Laboratory has been tasked to provide expertise and analysis on key subject areas, including chemical, biological, radiological, nuclear, and explosive weapons detection; emergency response and recovery; and related equipment, instrumentation, and technologies. In support of this tasking, NUSTL conducted a market survey of commercially available encryption software tools. Encryption software tools fall under AEL reference number 05EN-00-ECRP titled Software, Encryption.

Visit the SAVER website at <http://firstresponder.gov/SAVER> for more information on the SAVER Program or to view additional reports on encryption software tools and other technologies.

POINTS OF CONTACT

SAVER Program

U.S. Department of Homeland Security

Science and Technology Directorate

FRG Stop 0203

245 Murray Lane

Washington, DC 20528-0203

E-mail: saver@hq.dhs.gov

Website: <http://firstresponder.gov/SAVER>

National Urban Security Technology Laboratory

U.S. Department of Homeland Security

Science and Technology Directorate

201 Varick Street

New York, NY 10014-7447

E-mail: nustl.saver1@hq.dhs.gov

TABLE OF CONTENTS

Foreword.....	i
Points of Contact.....	ii
1. Introduction.....	1
2. Encryption Software Overview.....	1
2.1 Current Technologies.....	2
2.1.1 Symmetric-Key Ciphers	2
2.1.2 Asymmetric-Key Ciphers	3
2.1.3 Public Key Infrastructure.....	3
2.1.4 Digital Signatures	4
2.2 Applications	4
2.3 Standards/Regulations.....	4
3. Product Data.....	5
3.1 File Encryption Programs	5
3.1.1 Cryptzone U.S., Inc., Simple Encryption Platform	8
3.1.2 Cypherix, Secure IT.....	8
3.1.3 Dekart, Keeper	9
3.1.4 East-Tec, Invisible Secrets.....	9
3.1.5 East-Tec, SafeBit	10
3.1.6 Intercrypto, Ltd., Advanced Encryption Package Professional	10
3.1.7 Midwest Research Corporation, KetuFile	11
3.1.8 Ranquel Technologies, Cryptoforge.....	12
3.2 E-mail Encryption Programs.....	12
3.2.1 Cryptzone U.S., Inc., Simple Encryption Platform (Secured eMail)	14
3.2.2 Entrust, Inc., Entelligence Messaging Server	14
3.2.3 Lux Scientiae, Inc., SecureLine.....	15
3.2.4 Privato Security, PrivateMail.....	16
3.2.5 Privato Security, PrivateMail Plus.....	17
3.2.6 Symantec, Encryption Management Server	17
3.2.7 Voltage Security, Inc., SecureMail.....	17
4. Vendor Contact Information	19
5. Summary	20

Appendix A. Request for Information.....	A-1
--	-----

LIST OF TABLES

Table 3-1. Product Comparison Matrix for File Encryption Programs	7
Table 3-2. Product Comparison Matrix for E-mail Encryption Programs.....	13
Table 4-1. Vendor Contact Information.....	19

LIST OF FIGURES

Figure 1. Asymmetric key encryption with public and private keys.	3
--	---

1. INTRODUCTION

Encryption software tools are computer programs used to protect sensitive or confidential data by converting it to a form that cannot be read by humans or computers without access to a numeric key that can restore the data to its original form. As long as the key remains confidential, encrypted data can safely be stored or transmitted without fear of being intercepted and disclosed to an unauthorized person or entity. To provide emergency responder and law enforcement organizations with information on encryption software tools, the System Assessment and Validation for Emergency Responders (SAVER) Program conducted a market survey on commercially available encryption software tools.

This market survey report is based on information gathered between October 2013 and November 2013 from a search of vendor websites, industry publications, and a government-issued Request for Information (RFI) posted on the Federal Business Opportunities (FedBizOpps) website (<https://www.fbo.gov>).

For inclusion in this report, encryption software tools had to meet the following criteria:

- Commercially available software product; and
- Able to encrypt and decrypt data files stored on a computing device or transmitted to another device via e-mail or some other form of digital communication.

A large number of encryption software products that meet these criteria are available. Due diligence was performed to develop a report that is representative of products in the marketplace.

2. ENCRYPTION SOFTWARE OVERVIEW

Emergency responders often store sensitive information on portable computers and handheld devices and transmit sensitive information through e-mail, instant messaging, and other forms of digital communications. Encryption software tools prevent this information from being disclosed when a computing device is lost or stolen or when a message is intercepted by a third party.

Encryption is the process of converting readable data (called plaintext) to an encoded form of the original data (called ciphertext) by using a software algorithm and a numeric key. The key locks the data into ciphertext form. The ciphertext contains all the information in the original plaintext, but cannot be read by humans or computers until decrypted. Decryption is the process of converting ciphertext back to the original plaintext. The algorithms used to encrypt and decrypt data are known as ciphers. Ciphers employ a long series of mathematical operations or substitutions involving the data and a numeric key in order to encrypt plaintext data. An opposite set of operations is used to decrypt the data. Symmetric-key ciphers use the same key to encrypt and decrypt. Asymmetric-key ciphers use separate keys to encrypt and decrypt.

A large variety of encryption software tools are available for protecting sensitive and confidential data stored on computers or sent by digital communications through insecure networks such as the Internet. These tools encrypt data files and messages so that they are protected from disclosure to unauthorized individuals if a computer is lost or stolen or if a message is intercepted in transit.

2.1 Current Technologies

This section describes the key technologies used by encryption software tools. These include symmetric-key ciphers, asymmetric-key ciphers, public key infrastructure (PKI), and digital signatures.

2.1.1 Symmetric-Key Ciphers

Symmetric-key encryption ciphers use the same key to encrypt and decrypt data. These algorithms are fast, efficient, and well suited to applications for storing encrypted documents on computing devices. They are not often used for communications, however, because they require both parties to have access to a single key that must be kept secret before a message is sent.

In January 1997, the National Institute of Standards and Technology (NIST) announced that it was seeking a symmetric-key cipher to be used as a new standard algorithm approved for encrypting sensitive information by U.S. Government agencies. Fifteen different symmetric-key cipher designs were submitted and tested in an open competition. In November 2000, NIST announced that the Rijndael cipher, named for its two inventors, Vincent Rijmen and Joan Daemen, was selected as the new standard. The algorithm, now known as the Advanced Encryption Standard (AES), breaks data into 128-byte blocks and allows key sizes of 128, 192, or 256 bits. Although having been subjected to great scrutiny, the AES has proven to be resistant to all known forms of attack. For instance, a supercomputer running a brute force attack, in which the key is repeatedly guessed at until decryption is successful, would require 10^{18} years in order to determine a 128-bit AES keyⁱ. Other more sophisticated forms of attack have also proven to be computationally infeasible. The AES algorithm is documented in Federal Information Processing Standard (FIPS) Publication 197 issued by NIST.

The AES has replaced the Digital Encryption Standard (DES), which originated in 1977 and uses a 56-bit key. With recent advances in computers, a DES key can now be broken in less than 24 hours. Triple DES, a cipher that employs three DES keys in succession, is much more secure and still commonly used. Many other symmetric-key ciphers such as Blowfish, Twofish, CAST, and GOST are publicly available and provide very high levels of encryption with large key sizes.

Key sizes are normally given in bits. A bit is a very small unit of information, representing either the number 0 or 1. However, a key that is 128 bits in length can have 2^{128} , or 3.40×10^{34} , possible numeric values. This represents a huge number of possible keys. Key values are often written in hexadecimal (hex) notation in which four bits are combined into a single hex character ranging from 0 to F. Hex values greater than 9 are represented by A, B, C, D, E, and F, so that a total of 16 values can be represented by a single hex character. A 128-bit key can be written with 32 hex characters, and a typical key value may look like the following:
3AE7BA9A73E349867FE343A2BFC2EC45.

ⁱ Mohit Aurora, Senior Systems Engineer and Security Architect, Freescale Semiconductor, in an article for the EE Times entitled, *How Secure is AES Against Brute Force Attacks?*, http://www.eetimes.com/document.asp?doc_id=1279619

2.1.2 Asymmetric-Key Ciphers

Asymmetric-key encryption (also called public key cryptography) allows parties that do not regularly communicate to send each other encrypted messages. It works by generating pairs of mathematically related keys. One key is used to encrypt a message, and a separate key is used to decrypt the message (Figure 1). Each party that wishes to receive messages is assigned its own key pair, with each pair comprising one public and one private key. A sender encrypts a message using the receiver's publicly available key.

The message is then decrypted with the receiver's private key. This is analogous to a locked mailbox with a slot for receiving messages. Anyone who knows the address of the mailbox (the public key) can insert a message, but only the owner of the mailbox can read the message (using the private key).

A *de facto* standard for asymmetric-key encryption is the RSA algorithm, named for its developers Ron Rivest, Adi Shamir, and Leonard Adleman. The Transportation Layer Security (TLS) protocol, which is used as the basis for secure web-based transactions, uses the RSA algorithm to encrypt data. RSA is also one of several algorithms supported by common e-mail encryption protocols such as Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME).

A disadvantage to asymmetric-key encryption is that the algorithms are complex and require large keys. Key sizes of 1,024 bits or more are needed for high-strength encryption. The RSA algorithm allows variable key sizes, and its inventors recommend 2,048-bit keys for messages that must remain secure until 2030 and 3,072-bit keys for data that must remain secure beyond that year. The mathematical operations needed to encrypt messages with such large keys create a large workload for computer processors. As a result, asymmetric encryption can be very slow for large messages. PGP and other encryption tools send long messages by first randomly generating a symmetric key and transmitting it by RSA or some other asymmetric-key cipher. The rest of the message is then transmitted with symmetric-key encryption.

2.1.3 Public Key Infrastructure

With asymmetric encryption, a method is needed for exchanging public keys and ensuring that they belong to a certain individual or organization. PKI is an arrangement in which digital certificates that uniquely identify communicating parties are issued and made publicly available by a certificate authority (CA). The digital certificates contain the publicly available key for each party. The CA may be an entity within an organization or a trusted third party that allows two organizations to engage in secure communications. The CA also provides directory services for storing the certificates and making them publicly available. CAs generally have the authority to revoke certificates when necessary.

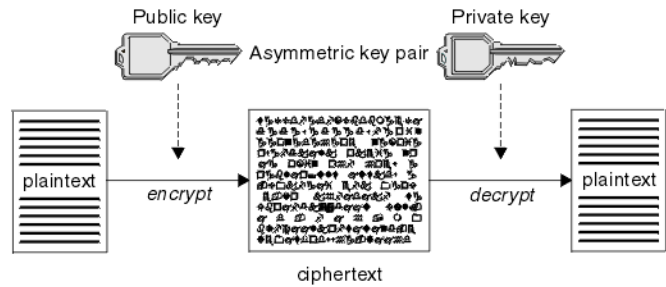


Figure 1. Asymmetric key encryption with public and private keys.

*Reprint courtesy of International Business Machines Corporation,
© 2012 International Business Machines Corporation.*

2.1.4 Digital Signatures

A digital signature is a data stamp that can be added to a message to uniquely identify the sender. A digital signature may be added to an encrypted or unencrypted message, but the signature itself is always encrypted into the message. The mechanism used is generally the opposite of that used for asymmetric encryption. Senders use their private key to encrypt the signature, and receivers use the sender's public key to decrypt it. When a digitally signed message is properly implemented, a sender cannot deny having sent the message, and the receiver cannot deny having received the message.

2.2 Applications

File encryption and e-mail encryption comprise the two main applications of encryption software tools. File encryption programs allow sensitive data to be stored on a computer in ciphertext, so that the data cannot be read without a key or password. Most products on the marketplace use one or more symmetric-key ciphers with large key sizes. Having a strong key protects the data even if the computer is stolen. Many of these products come with additional features such as file compression, file shredding (so that deleted files cannot be recovered), stealth mode (so that encrypted data is hidden), and the ability to create self-decrypting files that can be transmitted to another computer and decrypted without running software.

E-mail encryption tools are widely available for sending secure messages and attachments. These programs can be used throughout an organization on servers, desktop computers, and handheld devices. They can also be hosted on computers remote to the organization that uses them. This is often called Software as a Service (SaaS), or cloud-based computing. The "cloud" refers to groups of interconnected computers that are accessed through the Internet and provide computing services such as data storage and software applications. Whether hosted in house or on the cloud, e-mail encryption applications generally use proprietary technologies for authentication and key management, but may also support common encryption protocols. They will often work compatibly with common e-mail applications such as Outlook, Lotus Notes, and Thunderbird. Most programs support user-initiated encryption or policy-based encryption. With policy-based encryption, software at a network gateway encrypts e-mails automatically based upon criteria such as message content and destination. This takes the decision about whether or not to encrypt out of the hands of the individual user. These tools are generally installed and maintained by an agency's information technology (IT) department and are used according to an agency-wide IT policy.

2.3 Standards/Regulations

The U.S. Government standard for accrediting encryption software is issued by NIST and given in FIPS Publication 140-2, titled *Security Requirements for Cryptographic Modules*. All encryption software purchased by U.S. Government agencies must be FIPS 140-2 compliant. The latest major update was released in December 2006.

A common industry standard concerning encryption is the Payment Card Industry (PCI) Data Security Standard (DSS) issued by the PCI Security Standards Council (SSC). The council accredits companies and organizations that make transactions involving credit card numbers and other cardholder data. The PCI DSS increases controls around cardholder data to reduce credit card fraud. The encryption requirements of PCI DSS are summarized in the document entitled *Payment Card Industry Point-to-Point Encryption*, issued by the PCI SSC.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 contains a Security Rule that sets standards for the nondisclosure of protected health information (PHI). PHI is defined as information that concerns health status, provision of health care, or payment for health care linked to an individual. Under the security rule, HIPAA-covered entities (medical service providers, insurers, and their business associates) must use appropriate encryption for stored and transmitted data when reasonable and appropriate. More information can be found in NIST Special Publication 800-66-Rev 1, entitled *An Introductory Guide for Implementing the HIPAA Security Rule*.

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 added additional requirements to the HIPAA Security Rule. Under HITECH, HIPAA-covered entities must provide notification to the U.S. Department of Health and Human Services and all affected parties in the event of a breach of unsecured PHI. As a result, many organizations are subject to embarrassing disclosures if their computer systems are hacked or messages are intercepted. However, if electronic PHI is stored or transmitted in encrypted form, disclosure is not necessary in such cases.

The Gramm-Leach-Bliley Act (GLBA) of 1999 contains a Safeguards Rule with requirements for financial institutions to protect customers' personally identifiable financial data, also known as nonpublic personal information (NPI). Under the Safeguards Rule, all NPI must be encrypted while in storage and while in transit. Violations can result in large fines and audits. Many vendors of encryption software tools advertise that their products meet the specifications for the standards and regulations mentioned above.

It should also be noted that the U.S. Department of Defense (DoD) has issued a standard method for file shredding on hard drives, a feature included with many file encryption programs. The standard is known as DoD 5220.22-M and specifies that a zero, a one, and a random number must be written over each storage bit in a file that is deleted. Each operation must also be verified, ensuring that the deleted file cannot be recovered by software recovery methods.

3. PRODUCT DATA

The encryption software tools identified in this market survey report are categorized according to their primary application, file encryption or e-mail encryption.

3.1 File Encryption Programs

The file encryption programs covered in this report range in price from \$29.95 to \$125.00. Except where otherwise noted, the reported price is for a perpetual license for a single user. Major upgrades usually involve a separate cost, and some vendors provide an option for a service contract. File encryption programs use many different ciphers and key sizes and satisfy various compliance regulations.

Products are listed in alphabetical order by vendor. The product data was obtained directly from the vendor and supplemented with information from the vendor website except where otherwise noted. The information obtained has not been independently validated by the SAVER program.

Features in Table 3-1 are defined as follows:

Company indicates the manufacturer or developer of the software.

Product indicates the software product name.

Version Number indicates the latest version number assigned by the vendor to the product.

Cost Per User indicates the price in U.S. dollars for a license to use the software product. Unless otherwise noted, the licenses are perpetual, and upgrades to newer versions of the product may cost extra.

Regulatory Compliances indicates the regulations (FIPS 140-2, GLBA, HIPAA, PCI DSS, etc.) satisfied by the encryption software product.

Cipher and Maximum Key Size indicates the name of a cipher (encryption algorithm) followed by the maximum key size that the encryption software uses for that cipher.

Computer and Operating System indicates the computer types (Personal computer (PC), Mac, Linux workstation, etc.) and operating systems that can run the encryption software tool.

File Shredding indicates whether or not the encryption software tool provides a feature for deleting files from a hard drive in such a way that the files cannot be recovered by software recovery methods.

Stealth Mode indicates whether or not the encryption software tool provides a feature for hiding its existence, so that other users or hackers are unaware that encryption software is installed.

Self Decryption indicates whether or not the encryption software tool provides a feature for creating self-decrypting files that can be transferred to another computer and decrypted without running the software tool.

Table 3-1. Product Comparison Matrix for File Encryption Programs

Company	Product	Version Number	Cost Per User (\$)	Regulatory Compliances	Cipher and Maximum Key Size	Computer and Operating System	File Shredding	Stealth Mode	Self Decryption
Cryptzone U.S., Inc.	Simple Encryption Platform	5.0	NA	GLBA HIPAA PCI DSS	AES-256 RSA-2048	PC-Windows iPhone-iOS	Yes	Yes	Yes
Cypherix	Secure IT	NA	29.95	NA	Blowfish-448	PC-Windows	Yes	NA	Yes
Dekart	Keeper	NA	49.00	FIPS 140-2	AES-256	PC-Windows	Yes	NA	Yes
East-Tec	Invisible Secrets	4	39.95	FIPS 140-2 GLBA HIPAA PCI DSS	AES-256 Blowfish-448 CAST-128 Diamond2-128 GOST-256 RC4-1024 Sapphire II-128 Twofish-256	PC-Windows	Yes	No	Yes
	SafeBit	2	39.95	FIPS 140-2 GLBA HIPAA PCI DSS	AES-256	PC-Windows	NA	NA	NA
Intercrypto, Ltd.	Advanced Encryption Package Professional	5.87	49.95	NA	Supports 20 ciphers including AES.	PC-Windows	Yes	NA	NA
Midwest Research Corporation	KetuFile	1.2.2	75.00 – 125.00	HIPAA	AES-512	PC-Windows	No	Yes	No
Ranquel Technologies	CryptoForge	4.1.0	38.70	HIPAA, PCI	AES-256 Blowfish-448 Triple DES-168 GOST-256	PC-Windows, Tablet-Windows 8 Professional	Yes	No	No

Regulatory compliance abbreviations:
 FIPS = Federal Information Processing Standard
 GLBA = Gramm-Leach-Bliley Act
 HIPAA = Health Insurance Portability and Accountability Act
 PCI DSS = Payment Card Industry Data Security Standard

Cipher abbreviations:
 AES = Advanced Encryption Standard
 DES = Digital Encryption Standard
 RSA = Rivest-Shamir-Adleman
 (Note: GOST, CAST, and RC4 are not abbreviations or acronyms)

Other abbreviations:
 NA = information not available
 PC = personal computer

3.1.1 Cryptzone U.S., Inc., Simple Encryption Platform

The Simple Encryption Platform (SEP) is a software tool that can be licensed separately to support file and folder encryption, Universal Serial Bus (USB) encryption, and encryption of data within Microsoft SharePoint. The SEP can run on a PC, a server, or mobile devices running the iOS or Android operating systems. The e-mail encryption features of the SEP are discussed separately in Section 3.2.1.

The SEP's Secured eFile feature is a policy-based file and folder encryption tool that allows users on an organization's network to encrypt files and apply access rights to encrypted files. Access rights may be assigned to other users and groups of users. This allows users inside and outside of the organization to share files and folders securely. Administrators may also use a central management console to apply automatic encryption rules that depend upon the roles of users or other constructed rules. Built-in technology handles the management of access rights, user authentication, and encryption keys. This provides a secure, centrally managed collaboration platform for an organization. Secured eFile comes with a file shredder that deletes files with a triple-pass overwrite of all bits with random values.

The SEP's Secured eUSB feature is an enterprise-level method for applying encryption and other security standards to USB storage devices, providing centralized control over all USB storage within an organization. With this feature, organizations can protect intellectual property and other sensitive information and ensure compliance with data protection laws and regulations. Secured eUSB can encrypt data onto any USB storage device, enforce encryption policy, generate reports on user activities, and set password policies and user access rights.

The SEP's Secured eCollaboration feature protects information stored within Microsoft SharePoint. Using the same principle as Secured eFile, Secured eCollaboration integrates with SharePoint and adds encryption and user rights management, allowing an organization to share sensitive and confidential information. Secured eCollaboration allows administrators to control security policies centrally and assign access rights in line with policies.

The price of the SEP will depend on the products selected, the feature sets, and the number of users. Licenses are perpetual. Support and maintenance are covered with service contracts that are renewed on a 1-year basis. Customer service is provided by e-mail, and a user guide, video tutorial, and a frequently asked questions (FAQ) page are available on the vendor's website. The program generally needs about 1 to 2 hours to set up and may involve the IT administrator. Training is not usually needed.

3.1.2 Cypherix, Secure IT

Secure IT is a file and folder encryption program for Windows PCs that features data compression, customizable file shredding, and encryption using the 448-bit Blowfish cipher. Users can also create self-decrypting attachments that can be e-mailed to other users and decrypted without software. The vendor also provides a free utility called DeCypherIT that allows users to decrypt any file encrypted with Secure IT. Secure IT may be purchased for \$29.95 and downloaded from the vendor's website. A free 30-day trial version is also available.

The preceding information was compiled from publicly available vendor information.

3.1.3 Dekart, Keeper

Keeper is a file encryption program for Windows PCs that uses the AES cipher with a 256-bit key. Keeper integrates into Windows Explorer and allows encryption of files and folders from Explorer's right-click menu. Users can also shred files and create self-extracting encrypted archive files that can be e-mailed and decrypted without the need to run the software. Keeper allows decryption using a key or a password. A password quality meter is provided so that users can ensure that strong passwords are used. Keeper can be purchased for \$49.00 from the vendor's website.

The preceding information was compiled from publicly available vendor information.

3.1.4 East-Tec, Invisible Secrets

Invisible Secrets is a file encryption program that allows users to encrypt files and folders on a Windows PC and make them invisible to other users. Any file type can be encrypted from within Windows Explorer or from within applications such as spreadsheets, word processors, and e-mail applications. Files and folders can be encrypted onto all types of rewriteable media, including USB drives. Large files can be compressed to reduce size before being encrypted. Users can select from eight strong encryption algorithms—AES, Twofish, RC4, CAST, GOST, Diamond 2, Sapphire II, and Blowfish.

Invisible Secrets allows users to hide encrypted files by disguising them within another file such as a family photo or an audio file. This feature, known as steganography, protects and hides confidential information, diverting the attention of hackers or unauthorized users who may search the computer for sensitive information. Five file types (with extension names of JPEG, PNG, BMP, HTML, and WAV) allow encrypted files to be stored and hidden within them.

Sensitive computer programs can also be encrypted and hidden with the Application Locker that comes with Invisible Secrets. The Application Locker allows access to encrypted or hidden applications on a password basis. Administrators or users can effectively lock other users out from certain sensitive applications. By hiding the application, it will not appear on the Start Menu, but can still be accessed with the password. Hot keys can be set up to quickly lock and unlock an application. In addition, Invisible Secrets can run in stealth mode by checking a box in the setup options. In stealth mode, the program can only be accessed by searching for the executable file. It will not appear on the start menu, desktop, or tray.

Invisible Secrets features a Virtual Keyboard that prevents key-logger software from stealing user passwords. There is also a password manager and generator. With this feature, users can generate secure passwords for multiple accounts, store them in an encrypted list on their computer, and access the list with a single password. This eliminates the security risks involved with using the same password multiple times and storing unencrypted lists of passwords.

Invisible Secrets features an integrated DoD 5220.22-M-compliant file shredder that lets users selectively and permanently erase original and encrypted confidential files and folders, making them unrecoverable to any data-recovery software. All shredding is based on advanced DoD data destruction protocols and includes up to four unique shred methods. With Invisible Secrets, users can also generate self-decrypting packages (SFDs). These are executable files containing encrypted content that can be decrypted by entering the correct password. With this feature, users can encrypt a file and transfer it to another computer by e-mail or USB flash drive and be able to decrypt the file without running Invisible Secrets.

Invisible Secrets has a feature called the Cryptboard that allows users to add files and then perform operations on the entire list of files. Available operations include Hide, Encrypt, Decrypt, Shred, and SFD Package. The Cryptboard is like a shopping basket where you add files, and the security operation is like a “check out.”

Invisible Secrets can be purchased for \$39.95 and downloaded from the vendor’s website. Minor upgrades are free, and major upgrades are provided at special rates. Customer service is provided via e-mail and chat. Customers may also speak with customer service via Skype. A user guide and FAQ page are provided on the vendor’s website. The program takes approximately one minute to install and does not require an IT professional.

3.1.5 East-Tec, SafeBit

SafeBit is a data protection program for Windows PCs that performs on-the-fly disk encryption and allows users to create virtual disk drives called safes, where they can hide file and folder structures, keep them encrypted all the time, yet still work with these files as if they were ordinary computer files. On-the-fly encryption means that data is automatically encrypted just before it is saved and decrypted just after it is loaded, without any user intervention. The encryption and decryption process is transparent to the user. SafeBit also allows users to install and execute programs inside an encrypted safe, giving the safe the look and feel of a separate disk drive.

Encrypted safes can be transferred, copied, or backed up to external hard drives, USB drives, smart cards, or other portable devices. They can also be uploaded to the cloud via programs like Dropbox, Microsoft SkyDrive, or Google Drive. Thus, users can access these safes wherever they go. SafeBit uses the 256-bit AES encryption algorithm for encryption and decryption.

SafeBit allows users to save the passwords for encrypted safes on a removable storage device such as a USB flash drive or memory card. In this way, users avoid the risk of having log-in data stored on the computer being protected. For better security, the password is encoded when saving it on a USB drive. SafeBit also contains a virtual keyboard that allows users to enter passwords without fear of them being stolen by key-logging applications. Encrypted disk drives provide protection against viruses, Trojans, and spyware.

SafeBit can run in stealth mode by choosing some settings from the options page. In stealth mode, the program will not appear on the start menu, desktop, or tray. Users must run the program by finding the executable file in Windows Explorer.

SafeBit can be purchased for \$39.95 from the vendor’s website. Once downloaded, it can be installed in approximately one minute and does not ordinarily require an IT professional. Customer support is available through e-mail, chat, and conversation through Skype. A user guide and FAQ page are also available.

3.1.6 Intercrypto, Ltd., Advanced Encryption Package Professional

Advanced Encryption Package Professional (AEP Pro) is a file encryption software package for Windows PCs. The program integrates with Windows Explorer, allowing users to use Explorer’s context menus to encrypt, decrypt, and shred files and folders. Pre-encrypted files can be removed with a shredding capability that exceeds DoD specifications. AEP Pro uses 20 encryption algorithms including AES, Blowfish, Twofish, GOST, and Serpent. AEP Pro supports asymmetric encryption, allowing users to create public and private keys. By making the public

key available on a website or by e-mail, the user can receive encrypted files from others and decrypt them with the private key. The user can also create self-decrypting files that can be transmitted to others and decrypted without the need for software at the receiving end. The program costs \$49.95 and can be downloaded from the vendor's website.

The preceding information was compiled from publicly available vendor information.

3.1.7 Midwest Research Corporation, KetuFile

KetuFile is a file encryption program that can encrypt any file under 2 gigabytes (GB) in length on Windows PCs. Encrypted files can only be decrypted and read by someone who has the key. Ketufile uses the AES cipher with the option for a 256- or 512-bit key length. The vendor believes that Ketufile is the only product on the market using a 512-bit AES key and claims that a 512-bit key, compared to a 256-bit key, makes it 10^{54} times more difficult to break the encryption.

KetuFile has an internal file browser that allows users to encrypt files from within the KetuFile environment. Encryption keys are always used as the password for decrypting files. The keys can be quickly accessed from the Keys folder or can be manually entered. The user can encrypt files and keep the key for those files in another secure location (not on the PC). This makes the computer secure even if it is stolen.

Encrypted files may be transferred to USB drives and other removable media. Ketufile itself may be installed on a USB flash drive if an IT professional mimics the Windows Installer file hierarchy upon the drive. This will provide the basics of file encryption and decryption. KetuFile can launch Windows batch files to transfer files to other locations on a hard drive, or to a local area network (LAN) or wide area network (WAN), using the file transfer protocol (FTP) and other methods. A senior IT professional is generally required to implement these special functions.

With Ketufile, users can encrypt files and attach them to an outgoing e-mail using existing e-mail clients such as Thunderbird, Outlook, and Eudora. In addition, when an e-mail containing a Ketufile-encrypted attachment is received, the user may launch Ketufile from within the e-mail client and then proceed to decrypt the file.

KetuFile has been authorized by the U.S. Department of Commerce, Bureau of Industry and Security, under authorization CCATS number G034601, for export to all countries with the exception of embargoed countries and persons who are on the denied parties list. The vendor believes that KetuFile likely satisfies HIPAA requirements and other regulations, but has not researched the issue.

The price for a Ketufile license is \$75 for 256-bit AES encryption and \$125 for 512-bit AES encryption. The usage license is perpetual. Technical support is provided for one year. After that, service contracts can be negotiated. Ketufile can be installed on a PC in approximately 10 minutes. The vendor recommends that an IT professional install the program. A free demonstration version of the program is available for download from the vendor's website. It can be used with short files and short key lengths. Users who are satisfied with its operation may then purchase a registration number in order to make the program fully functional.

3.1.8 Ranquel Technologies, Cryptoforge

CryptoForge is a file encryption program that allows users to encrypt, decrypt, and shred with the built-in file shredder. Files of any type and size, as well as entire folders or drives, can be encrypted from within Windows Explorer or My Computer by right clicking. Users can also decrypt an encrypted file by double-clicking. Additionally, an included secure text editor allows users to create, encrypt, and decrypt documents in such a way that they can be sent by e-mail or messenger systems.

Users can choose from four different symmetric-key encryption algorithms—AES-256, Blowfish-448, Triple DES-168, or GOST-256. Cryptoforge also allows multiple encryption, which involves encryption with more than one algorithm simultaneously. Other features in Cryptoforge include automatic file compression, a file shredder that matches or exceeds DoD specifications, and a password quality meter that estimates the strength of passwords. Cryptoforge passwords can contain up to 256 characters and are stored in random access memory (RAM) only. This memory is cleared when the computer is off, and is overwritten several times by the software prior to being cleared. CryptoForge integrates seamlessly with password managers that provide biometric identification.

A single-user license may be purchased for \$38.70. Multiple licenses may be purchased at discount prices, and group licenses for unlimited users may also be purchased. There are no extra charges for service contracts. Cryptoforge can be freely downloaded and used indefinitely for decryption only. Cryptoforge installs in one minute and does not require an IT professional. Customer support is available by e-mail, and a user guide and FAQ page is provided on the vendor's website. The user interface, user guide, and customer service support come in both English and Spanish.

3.2 E-mail Encryption Programs

The e-mail encryption programs covered in this report range in price from \$48.00 to \$129.95 per user per year. Most vendors sell an annual license that must be renewed, while some vendors provide a perpetual license that may be supplemented with a service contract for maintenance. E-mail encryption programs use many different ciphers and key sizes and satisfy various compliance regulations.

Products are listed in alphabetical order by vendor. The product data was obtained directly from the vendor and supplemented with information from the vendor website except where otherwise noted. The information obtained has not been independently validated by the SAVER program.

Features in Table 3-2 that were not previously defined in Section 3-1 are defined as follows:

Cost Per User Per Year indicates the price in U.S. dollars for an annual license to use the software product.

License Period indicates the amount of time that the license is valid for.

Protocols indicates standard public key cryptography protocols and methods (PGP, S/MIME, IBE [Identity-Based Encryption], etc.) supported by the encryption software product.

Digital Signatures indicates whether or not the encryption software product supports digital signatures as a method for authenticating messages.

Client Software indicates whether or not the product can be installed as client software in an organization's computer systems.

Software as a Service (SaaS) indicates whether or not the product can be hosted on computers remote to the organization using the service.

Table 3-2. Product Comparison Matrix for E-mail Encryption Programs

Company	Product	Version Number	Cost Per User Per Year (\$)	License Period	Regulatory Compliances	Cipher - Key	Protocols	Digital Signatures	Client software	Software as a Service (SaaS)
Cryptzone U.S., Inc.	Simple Encryption Platform (Secured eMail)	5.0	NA	NA	GLBA HIPAA PCI DSS	AES-256, RSA-2048	Proprietary TLS	No	Yes	No
Entrust, Inc.	Entelligence Messaging Server	NA	NA	NA	NA	AES-256, RC2-128, CAST-128, IDEA, Twofish-256, Blowfish-128, RSA- 4096, DSA-1024	PGP S/MIME	Yes	Yes	NA
Lux Scientiae, Inc.	SecureLine	NA	48.00*	1 year	GLBA HIPAA	AES-256, RSA-2048	PGP S/MIME TLS	Yes	No	Yes
Privato Security	PrivateMail	2	99.95	1 year	GLBA HIPAA	User can choose from over 30 ciphers	Proprietary TLS	Yes	Yes	Yes
	PrivateMail Plus	2	129.95	1 year	GLBA HIPAA	User can choose from over 30 ciphers	Proprietary TLS	Yes	Yes	Yes
Symantec	Encryption Management Server	NA	NA	NA	NA	NA	PGP S/MIME	Yes	Yes	NA
Voltage Security, Inc.	SecureMail	5.0	99.00	perpetual	FIPS 140-2	AES-256	IBE	Yes	Yes	Yes

* There is also a charge of \$108 - \$168 per year for the base account for the service. Price depends upon choice of server environment.

NA = Information not available

Regulatory compliance abbreviations:

FIPS = Federal Information Processing Standard

GLBA = Gramm-Leach-Bliley Act

HIPAA = Health Insurance Portability and Accountability Act

PCI DSS = Payment Card Industry Data Security Standard

Cipher abbreviations:

AES = Advanced Encryption Standard

DSA = Digital Signature Algorithm

IDEA = International Data Encryption Algorithm

RSA = Rivest-Shamir-Adleman

(Note: CAST, and RC2 are not abbreviations)

Protocol abbreviations:

IBE = Identity-Based Encryption

PGP = Pretty Good Privacy

S/MIME = Secure Multipurpose Internet Mail Extensions

TLS = Transportation Layer Security

3.2.1 Cryptzone U.S., Inc., Simple Encryption Platform (Secured eMail)

The Simple Encryption Platform (SEP) is a software tool that can be licensed for e-mail encryption. The Secured eMail feature integrates with e-mail systems such as Outlook and Lotus Notes, providing a “Send Secured” option for automatically encrypting messages and attachments. The secured content is delivered as an attachment wrapped in an ordinary e-mail. The “wrap-mail” provides plaintext instructions telling the recipient what needs to be done to read the secured contents.

Recipients of secured e-mails can open them and reply securely on almost any computer or smart device (including a PC, Mac, Linux workstation, iPhone, iPad, Blackberry, Android phone, or Windows mobile phone) without having to install software or purchase a license. The only requirement is an Internet connection and web browser. Thus, organizations can establish a secured communications channel with customers and partners. An unlicensed recipient can click on a link in the e-mail and get routed to the sender’s hosted web portal. At the portal, the recipient registers (if a first-time user) and can then open the e-mail and reply securely. An unlicensed recipient can alternatively open the e-mail by downloading the free Secured eMail Reader, which integrates into e-mail applications such as Outlook and Lotus Notes. Licensed recipients can open and reply to secured e-mails with their client software.

Secured eMail contains a Central Management Console that uses active directory technology and enables IT administrators to deploy and manage all aspects of e-mail security. Administrators can set policies, licenses, and secure groups, and automatically push the settings out to clients. Secured eMail generates encryption keys at the end point, where content is encrypted. The key is then encrypted with additional keys determined by policy. These keys are then synchronized between authorized end points with a central key server. The key server delegates keys to those who are authorized. Thus, no certificates are needed.

Secured eMail does not place size restrictions on messages or attachments. Archiving of e-mails is provided, and the system can be configured so that encrypted e-mails are automatically archived without user intervention. Although digital signatures are not supported, message integrity and authentication is a byproduct of the system architecture.

The price of licenses varies with options chosen, number of users, and feature sets. Licenses are perpetual, and support and maintenance is renewed on a one-year basis. Support is offered through e-mail. A user guide, video tutorial, and FAQ page are also provided. The vendor should be contacted for more information.

3.2.2 Entrust, Inc., Entelligence Messaging Server

Entelligence Messaging Server is a server-based secure e-mail communications software package that is shipped as a turnkey appliance (a completed product that can be used by any organization) with optional hardware included. Entelligence Messaging Server works with popular e-mail programs such as Outlook, Lotus Notes, Yahoo, Hotmail, Gmail, and other web-based e-mail services. It delivers standards-based e-mail encryption capabilities, allowing recipients to communicate securely through encryption standards such as PGP, S/MIME, SecurePDF, WebMail Pull, and WebMail Push. Entelligence Messaging Server supports mobile e-mail clients such as Blackberry, Apple iOS, Android, Java-based platforms, and Wireless Access Protocol (WAP)-compatible browser-based cell phones.

Entelligence Messaging Server scans e-mail content and can be configured to automatically encrypt upon finding personal employee data, financial information, or other categories of sensitive information. Automatic encryption can also be based upon the sender, recipient, and recipient domain. User-initiated encryption is provided through e-mail plug-ins for Outlook and Lotus Notes. Entelligence Messaging Server can be configured to provide desktop encryption, authentication, and e-mail archiving.

The preceding information was compiled from publicly available vendor information.

3.2.3 Lux Scientiae, Inc., SecureLine

SecureLine is an end-to-end e-mail encryption service that provides encryption via TLS, PGP, S/MIME, or the SecureLine Escrow web-based portal system. SecureLine is fully hosted on computers remote to organizations that use the service. It does not require any hardware or software installation to implement. SecureLine is built into Lux Scientiae's proprietary WebMail platform for Internet browsers, and integrates seamlessly with standard e-mail clients such as Outlook, Thunderbird, MacMail, and mobile devices.

SecureLine supports user-initiated and policy-based encryption of e-mails. Users can choose to encrypt an e-mail by checking an "Encrypt" checkbox in their e-mail composition window. Alternatively, policy settings allow e-mails to be automatically encrypted based on content, recipient, subject line, or other filter settings. HIPAA-designated accounts have maximum security settings and do not allow users the choice of whether or not to encrypt. Administrators also have the option of disallowing users the option of turning off encryption.

Users can create or import their own PGP or S/MIME security certificates into their WebMail account. This allows encrypted e-mail exchanges with other parties with PGP or S/MIME certificates through public-key cryptography. The Escrow web portal allows any recipient to receive encrypted e-mails. Recipients decrypt e-mails by choosing a link in the notification message of the e-mail that routes them to the web portal. Upon successful registration, recipients are shown the decrypted message. Alternatively, recipients may choose a separate link in the notification message that routes them to a page containing a question preconfigured by the sender. Recipients must enter the correct answer before being shown the decrypted message. E-mails sent through SecureLine Escrow secure portal system are available to the recipient until they expire. The default expiration period is 30 days, but customers can configure this to as long as 10 years. Messages and attachments up to 70 megabytes (MB) may be encrypted and sent.

Customers can optionally purchase a premium e-mail archiving service which stores a copy of each inbound and outbound e-mail for all addresses within a customer's domain(s) for 10 years. Messages stored in this archive are immutable, but searchable and exportable by users and administrators.

SecureLine supports private labeling, so that the web service can be branded to the customer's business identity instead of the vendor's. The service can also be used in conjunction with the vendor's bulk e-mailing service to provide high-volume secure sending of sensitive information such as lab test results and financial statements. The encrypted e-mails can be sent from and received on mobile devices with no need for a special mobile application.

A base account can be purchased for between \$108 and \$168, depending upon the choice of server environment. Licenses for the web portal are \$48 per year per user. There are no additional charges for customer support or service contracts. Customer support is provided by

e-mail and telephone with a toll free number. A user guide, video tutorial, and FAQ page are also available. All customers receive one free personalized 30-minute phone training session. Additional personalized phone training is available at \$50 per 30-minute session. One-hour web-based classes are also offered for \$300 per class.

3.2.4 Privato Security, PrivateMail

PrivateMail is software that integrates directly into popular e-mail clients such as Outlook and Thunderbird to create a new communications channel to ensure that sensitive e-mail, documents, and personal information are delivered and received only by the intended recipients. Users open their PrivateMail account, compose e-mails, and click the "Send Securely" button. All e-mails sent are automatically encrypted. No one other than the intended recipient can access and read the message as it remains encrypted until the authorized recipient downloads the message, when it is automatically decrypted.

Using PrivateMail, law enforcement and other government agencies can assemble secure networks for task forces and interagency operations. These can be as simple as communicating case information with the regional district attorney's office or as complex as multilevel international agency coordination. Verified members keep communications privileged for each distinct group of users. The networks are scalable to expand and contract as PrivateMail membership changes based on case needs. Authentication can be added to ensure member identity for information access and transfer.

PrivateMail can run on a PC, Mac, server, and any Linux workstation. Installation of the software should take under 2 minutes. PrivateMail accounts can be used independently and issued directly to agency personnel. The software is not integrated with biometric authenticators but would support installation on biometric access-governed devices. PrivateMail can be hosted on premise or in the cloud as a webmail service. In this case, the software directs traffic through a privately addressed SaaS. The entire e-mail is encrypted, including the body, headers, and attachments. There are no limits on file encryption size. Policy-based encryption is not native, but can be added upon request.

PrivateMail generates public and private keys upon first use by properly authenticated users of the software. Private keys are stored locally to the client software, while public keys are stored in a central repository. A patented hybrid encryption scheme is used to encrypt e-mails and route them through a private domain using private routing addresses. A one-time symmetric cipher key is generated and encrypted with the recipient's public key. The rest of the message is encrypted with the symmetric cipher. The recipient decrypts the symmetric key with his or her private key, and uses the symmetric key to decrypt the rest of the message. The e-mail is then transparently presented in the recipient's e-mail program.

PrivateMail contains a feature called Crypto-Bank that allows the user to choose from over 30 different encryption ciphers. The program uses 128-bit AES and 1024-bit RSA by default, but users can customize their encryption schemes by choosing other algorithms and key sizes. PrivateMail also generates compliance activity reports to track, monitor, and demonstrate compliance with sensitive data. E-mail archiving is available with the web service.

Licenses for PrivateMail cost \$99.95 per user per year. The software is available for immediate download when purchased. E-mail customer service support, a user guide, video tutorial, and

FAQ page are included in the standard PrivateMail subscription. Additional customer service support contracts are available, but not mandatory.

3.2.5 Privato Security, PrivateMail Plus

PrivateMail Plus includes all of the features of PrivateMail and also allows users to send secure messages to any e-mail address. Nonsubscribers are directed to a secure web portal where they can log in, read the decrypted messages, and reply securely to the sender. E-mails and attachments are automatically encrypted when sending and decrypted when receiving. All content, attachments, and e-mail addresses are multi-tier encrypted and completely hidden to the outside world.

Licenses for PrivateMail Plus cost \$129.95 per user per year. Accounts include a standard bundle of 1,000 annual send/read/reply messages for communications with nonsubscribers, and message bundle upgrades can be purchased. An unlimited number of secure messages can be sent to other PrivateMail subscribers. A 14-day free trial of PrivateMail Plus is available at the vendor's website.

3.2.6 Symantec, Encryption Management Server

Encryption Management Server software provides centrally managed e-mail encryption for an organization to secure communications with customers and partners. Running on a network server, the software centralizes the creation, enforcement, management, and reporting of data protection and encryption policies. Encryption Management Server provides multiple delivery options, including PGP, S/MIME, Encryption Web E-mail Protection, and Encryption PDF E-mail Protection. Other features of Encryption Management Server include policy enforcement that ensures encryption within expected parameters, reporting and logging that provides oversight of user activity, key management that creates, distributes, and stores encryption keys, and centralized management of multiple data protection applications. Encryption Management Server supports iOS, Android, and Blackberry mobile devices.

The preceding information was compiled from publicly available vendor information.

3.2.7 Voltage Security, Inc., SecureMail

Voltage SecureMail is file encryption software that enables users to send and receive secure e-mail messages and attachments similar to regular e-mail. SecureMail can be deployed on premise or delivered as SaaS from the Voltage SecureMail Cloud™. Voltage's push-based single message format works with many e-mail clients (e.g., Outlook, Thunderbird), operating systems, and computing devices (e.g., PC, Mac, Blackberry, iOS, Android).

SecureMail uses IBE to generate public keys based on the user's e-mail address. With IBE, there is no need to register partners or deliver PKI certificates into the field. Only the e-mail address is needed to send encrypted e-mail. A key server generates a corresponding private key on the fly and delivers it in real time to encrypt or decrypt messages as they are being sent or opened on the device being used. This process is known as stateless key management. It derives the needed key for any user and delivers it to the platform they are using. It also allows security policies to be encoded directly into encryption and authentication methods. With automated key management, the system requires fewer hours of administrative attention per month. By relying on an

infrastructure that never stores either e-mail messages or users' keys, storage costs and operational overhead are avoided.

With plug-in application support for Blackberry, Android, and iOS devices, e-mails remain encrypted on these devices at all times. Mobile users can reply or create encrypted e-mail from the mobile device. Other devices without software installed can still read and send encrypted e-mail by using the Zero Download Manager (ZDM), which is a web-based key delivery system. ZDM provides full SecureMail functionality in a web-based interface, enabling anyone to send, receive, forward, and reply to secure messages with no special software required.

SecureMail offers a large file attachment capability. With this feature, the software will strip large files from an e-mail and send a notification message to the recipient that describes how to download the file through a secure web connection. The notification provides the recipient with an expiration date for the file, which will be automatically deleted if not downloaded by that date.

SecureMail offers options for user-initiated and policy-based encryption. Users can choose to "send secure" from e-mail client applications and Microsoft Office programs such as Word and Excel. Policies for encrypting e-mails can be set at the desktop or gateway using message content, mail domains, and other attributes to encrypt if the user forgets to press the "send secure" button. SecureMail also works with data loss prevention programs to scan encrypted or unencrypted outbound content as well as inbound encrypted e-mail. Many archiving systems work compatibly with SecureMail to store encrypted or decrypted e-mails. SecureMail logs key requests and administrator functions and creates logging reports.

SecureMail licenses can be purchased for \$99 per user. This is a one-time-only cost. Maintenance and support are provided through an annual maintenance contract. The vendor can provide additional details. Customer support is provided through a toll free number and e-mail. On site and remote training is available.

4. VENDOR CONTACT INFORMATION

Additional information on the products included in this market survey report can be obtained from the vendors of encryption software tools.

Table 4-1. Vendor Contact Information

Company	Product	Address/Phone Number	E-Mail/Website
Cryptzone U.S., Inc.	Simple Encryption Platform Secured eMail	185 Alefewife Brook Parkway Suite 410 Cambridge, MA 02138 (919) 469-5066	sales@cryptzone.com www.cryptzone.com
Cypherix	Secure IT	None provided on vendor website	www.cypherix.com
Dekart	Keeper	Compania-Dekart, SRL 85, M Kogalniceanu MD2009, Chisinau Republic of Moldova (+1 321) 549-5415	sales@dekart.com www.dekart.com
East-Tec	Invisible Secrets SafeBit	Balogh Istvan Nr. 17 Oradea, Romania 410238 0040 770 160969	sales@east-tec.com www.east-tec.com
Entrust, Inc.	Entelligence Messaging Server	3 Lincoln Center 5430 LBJ Freeway Suite 1250 Dallas, TX 75240 1-888-690-2424	entrust@entrust.com www.entrust.com
Intercrypto, Ltd.	Advanced Encryption Package Professional	Pacific Business Center P.O. Box 34069 #381 Seattle, WA 98124-1069	sales@aeppro.com www.aeppro.com
Lux Scientiae, Inc.	SecureLine	P.O. Box 326 Westwood, MA 02026 1-800-441-6612	sales@luxsci.com www.luxsci.com
Midwest Research Corporation	KetuFile	P.O. Box 2256 Fairfield, IA 52556 (641) 472-5005	salesdept@ketufile.com www.ketufile.com
Privato Security	PrivateMail PrivateMail Plus	395 Del Monte Center Suite 275 Monterey, CA 93940 (831) 372-2600	sales@privatosec.com www.privatosec.com
Ranquel Technologies	CryptoForge	Adolfo Alsina 1779 Buenos Aires, C.A.B.A 1088 Argentina 1-832-736-8316	sales.1@ranquel.com www.ranquel.com
Symantec	Encryption Management Server	350 Ellis Street Mountain View, CA 94043 1-800-745-6054	www.symantec.com
Voltage Security, Inc.	SecureMail	20400 Stevens Creek Boulevard Cupertino, CA 95014 (410) 292-8391	www.voltage.com

5. SUMMARY

This market survey includes 15 encryption software products from 12 different vendors. These products give the reader a good overview of the encryption software products on the commercial marketplace.

Eight file and folder encryption software tools are described in this report. These products range in price from \$29.95 to \$125.00. Seven of these programs use the AES cipher that is approved by NIST and meets the FIPS 140-2 standard. Most programs give users the option to encrypt with their choice of several different symmetric-key ciphers that are considered secure by the cryptography community. Key sizes for these ciphers range from 128 to 512 bits. Users also have the option to encrypt with at least 256 bits in all eight programs. This is important because 256-bit symmetric-key encryption is considered very strong and will not be broken even if the computer is lost or stolen. One program allows encryption with multiple ciphers simultaneously, and one program allows for asymmetric encryption, so that encrypted files can be shared securely with multiple parties. Many of the programs meet HIPAA, GLBA, or PCI regulatory requirements for protecting sensitive information in the health care, financial, and payment card industries, respectively. Emergency responders who deal with these types of data may need to store it in encrypted form to meet these requirements.

Seven e-mail encryption software tools are described in this report. Licenses for these products range in price from \$48.00 to \$129.95 per user per year. Most of these programs reside on computers within an organization's network, while some reside on the cloud and operate as a service in which users connect securely through the Internet. Whether operating in house or on the cloud, most of these programs centrally manage e-mail encryption and other security measures based on policy rules set by IT administrators. Many of them integrate into standard e-mail applications such as Outlook and Thunderbird and allow employees to send and receive encrypted e-mails from various mobile devices. Recipients that do not subscribe with the same vendor can usually download free software to read encrypted e-mails or go to a web service where they can register and then read and reply to encrypted e-mails. As with the file encryption programs, these e-mail encryption programs have options for many different encryption ciphers. However, they generally use a combination of symmetric and asymmetric encryption. Long messages are usually encrypted symmetrically, and the symmetric key is encrypted with an asymmetric cipher such as RSA. Key sizes for asymmetric ciphers range from 1024 to 2048 bits. A wide variety of key management schemes are used by these tools. Many of the programs meet HIPAA and other regulatory requirements.

APPENDIX A. REQUEST FOR INFORMATION

U. S. Department of Homeland Security
National Urban Security Technology Laboratory
201 Varick Street, New York, NY 10014-7447



Document Type: Special Notice

Title: Market Survey – Software Encryption Tools

Posted Date: September 23, 2013

Contracting Office Address:

Office of the Chief Procurement Officer
Washington, District of Columbia 20528
United States

Description:

Request for Information (RFI) – SOFTWARE ENCRYPTION TOOLS

DUE: October 11, 2013

I. BACKGROUND AND OBJECTIVES

The U.S. Department of Homeland Security, National Urban Security Technology Laboratory (NUSTL), a SAVER Technical Agent, is seeking information on commercially available software encryption tools, particularly software applications for file encryption and e-mail encryption.

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercial equipment and systems, and provides those results along with other relevant equipment information to the emergency response community in an operationally useful form. Information provided by the SAVER Program will be shared nationally with the responder community, providing a life- and cost-saving asset to DHS, as well as to Federal, state, and local responders. For more information on the SAVER Program, visit the SAVER website at <https://www.rkb.us/saver>.

SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL). The AEL item numbers for the subject equipment is 05EN-00-ECRP. The target audience for this information is public safety providers and their purchasing agents.

www.dhs.gov

- 2 -

II. SUBMISSION OF INFORMATION

Respondents are required to complete a written Product Summary Questionnaire for each product. The questionnaire may be obtained via email from the technical point of contact, [redacted], at [redacted] (see below). The Product Summary Questionnaire includes questions seeking the following specific information:

1. Company's name
2. Company's address
3. Point(s) of contact (name, title, e-mail, and phone number)
4. Business type and size (manufacturer or distributor, small or large business)
5. Product name, type, description, and specifications
6. Cost information (purchase price and General Services Administration [GSA] schedule information).

All information received will be treated as public knowledge and may be used in SAVER Program documentation; therefore, vendors should not submit proprietary information in response to this RFI.

Responses to this *Request for Information* must be submitted to [redacted] not later than 4:00 PM EST, March 8, 2013. All technical comments, inquiries and responses should be directed to [redacted] via email at [redacted]; all non-technical questions should be directed to [redacted], DHS Contracting Officer, via email at [redacted].

III. OTHER

The submitted information will be evaluated for inclusion in SAVER projects and reports. Determination as to an individual product's suitability will be made by NUSTL based on the objectives of this request. Therefore, requests for feedback should not be made through the Federal Business Opportunities posting agency. Vendors may be contacted following submission for more detailed product information. Vendor provided information may be reformatted for publication in SAVER Program documents.

This RFI is for information gathering and planning purposes only, and should not be construed as a Request for Proposal (RFP) or solicitation of an offer. The Government does not intend to award a contract on the basis of this RFI or otherwise pay for the information solicited. Submission of vendor information constitutes consent to publication of that information in SAVER Program documentation.