

ALTERNATIVE SOLUTIONS IN A POST PGP-WORLD

PGP has been virtually the de facto standard for e-mail encryption since Phil Zimmermann released it as shareware many years ago. Since Network Associates has decided to cease actively supporting the product, consumers are left scrambling for a new secure e-mail solution. Mr. Zimmermann himself has several suggestions at his web site: <http://www.philzimmermann.com/findpgp.shtml> .

There are other options, however. First, there are several web-based services, mail client plug-ins, full-fledged secure e-mail clients, and secure mail systems. Also, there are a number of file encryption products and "steganographic" secure systems. Since there are no real standards, however, you must arrange to exchange both a common application as well as any public keys or other needed keying material. Please contact IT GlobalSecure, Inc. Toll Free at (1-866-IT-ARMOR in the U.S) or at 1-202-332-5878 internationally to acquire more information and prices on these products.

Web-based Services – there are several web-based services that offer secure e-mail. They either work by using SSL to encrypt the communication between the users of the system or use a downloaded Java applet to provide encryption. This latter function tends to claim that the data is only accessible between the end-users since the data is always encrypted. However, since the applet is provided by the web-mail company, it is as secure as they choose it to be. The control of security is out of the hands of the user.

Mail-client plug-ins – these products integrate with standard e-mail applications such as MS Outlook™ or Eudora™. They are often interoperable with PGP (and, in fact, the commercial version of PGP could act as a plug-in). They have the advantage of allowing a user to work in their familiar e-mail environment. Problems usually stem from poor integration and interface design.

Full Secure Mail Clients – have the advantage of having security integrated as a native element of the mail system. The downside is that these are often smaller companies and they are competing both with traditional e-mail applications and with security applications. We do recommend and sell the **SoftClan e-Cryptor** product, which requires only that the sender have the secure mail client. Any mail recipient may receive the encrypted "envelope" and decrypt it with a password that has been exchanged out-of-band, such as by phone or fax.

SoftClan e-cryptor uses symmetric key-based encryption and by default the encryption algorithm used is AES (Advanced Encryption Standard), 128-bit encryption. Unlike other programs, however, ALL encryption is sent with 128-bit encryption even if the password used is less than 16 characters.

Also, since the encryption algorithm is contained in the envelope, as new encryption standards and levels become available, new envelopes will be provided and can be used with the existing version of your software. SoftClan e-cryptor uses fast and strong integrity checking using the RSA MD5 algorithm to guarantee the encrypted envelope

and its contents are exactly the same as they were before being encrypted and sent and have not been altered in any way during transit.

Call 1-866-IT-ARMOR toll free to receive pricing and technical literature on the exciting e-Cryptor product, or visit our Partners Page¹ at www.itglobalsecure.com

Standalone Secure E-mail Systems – these complete secure e-mail systems provide both the mail client application (or plug-in) as well as the common infrastructure for exchanging keys (typically a Public Key Infrastructure). These are particularly good for corporate environments. The value of these environments must be weighed against the pre-existing investment a company may have made in placing other security measures into their IT environment.

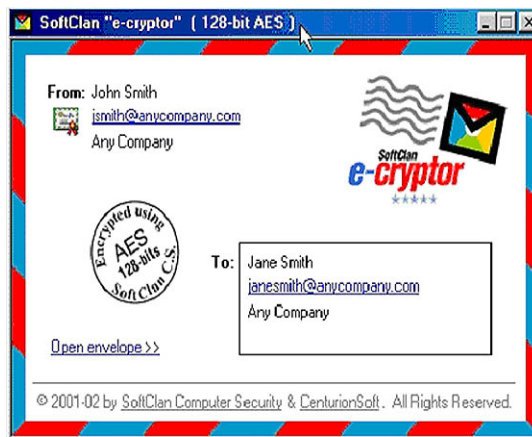
Integration work is involved in connecting these closed systems to external network users, but a solid enterprise-wide secure email system results. IT GlobalSecure carries the TOVARIS secure e-mail solutions, based on the Mithril Server, that supports the OpenPGP (PGP-interoperable) standard interface. We also carry the Authentica MailRecall product that provides outstanding control over who can read mail, its encryption, and privileges associated with the mail message (who can read it, its duration, delete privileges, and so forth).

File Encryption is an adequate solution and does not affect the operation of the mail system. However, it does not handle encrypting base messages easily, but does secure the encryption of attachments. Obviously, the file encryption product must be available to all e-mail recipients, and file decrypting occurs after mail transmission. IT GlobalSecure carries file encryption products from Authentica, Baltimore Technologies, and Eracom manufacturers.

Steganography, in its purest sense, is not encryption but encoding. A message of interest is concealed within a much larger binary file (typically an image). Cryptography can be used to determine where the data is hidden as well as to encrypt the sensitive data. This is much more of a covert communication system than a means of ensuring privacy. It is also very bandwidth inefficient as it requires the transmission of the large image.

IT GlobalSecure provides several secure e-mail solutions and can provide advice on a case-by-case basis for preferred options based on your needs.

If you already have PGP, or are intending to use a version of it, a security vulnerability has been identified. You may download the patch at:
<http://www.nai.com/naicommon/download/upgrade/patches/patch-pgphoffix.asp>



Available at More than 25% below List Prices from IT GlobalSecure, Call Toll Free at 1-866-IT-ARMOR for help in Selecting Your Best Desktop or Enterprise E-mail Security Solution. Content filtering also available.

¹ SoftClan will join or online list of Partners on or about May 16, 2002.