



Secure Internet Fax Services

Protus has implemented both the physical and the technical safeguards necessary to protect the confidentiality and integrity of information being communicated using its Internet Fax services. These safeguards meet the standards set out by the HIPAA.

Protus Physical Safeguards:

All Protus servers are housed in a secure environment that is accessed by approved personnel only. As a result, all information that passes through Protus' internal server environment remains protected and secure.

Protus Technical Safeguards:

For users that want additional safeguards on their emails to Protus, Protus provide public key encryption capabilities. In particular, Protus uses PGP security encryption and decryption software to secure electronic information that is transferred using its Protus Virtual Fax. PGP is based on the use of an asymmetric Public-Key/Private-Key encryption algorithm, which is used to protect the confidentiality of a message, and ensure its authenticity and integrity.

Ensuring Privacy:

PGP software is installed on the end user's computer and automatically manages all of the necessary encryption, decryption and verification processes. A "Key" (a large number used for encryption), is used by the PGP software to convert a message from plain-text (unencrypted) to cipher-text (encrypted). Once encrypted, the cipher-text is impossible to read without decryption using the required Key.

Every user of PGP software, including Protus, is assigned a Key Pair, which consists of both a Public Key and a Private Key. Messages encrypted using a Public Key can only be decrypted using a Private Key, and vice versa.

Protus makes its Public Key available to customers and customers provide Protus with their Public Keys. When a customer sends Protus a message they simply encrypt their message using Protus' Public Key. Only Protus has the corresponding Private Key to decrypt the message. Conversely, when Protus sends a customer a message it is encrypted using the customers Public Key. Only the customer can decrypt the message using their Private Key.

Sending a Secure Fax:

When sending a secure Fax using Protus Virtual Fax, the sender encrypts their document using the Protus Public Key. When Protus receives the email it is able to decrypt the document using its Private Key. The document is then processed and Faxed via secure telephone lines. This ensures total end-to-end security of the document from the

time it leaves the senders computer, to the time it is delivered on the recipient's fax machine.

Receiving a Secure Fax:

For customers to receive a Fax using Protus Virtual Fax, Protus first converts the Fax to a TIFF format file. This file is attached to an email and forwarded to the Fax recipient. If the recipient has provided Protus with their PGP Public Key, Protus automatically encrypts the message using the recipients Public Key before delivery. The recipient's PGP-enabled email software will then decrypt it for viewing. Complete, end-to-end security is provided through a fully automated, widely available, and easy-to-use process.

Ensuring Integrity:

A number called a "Checksum" is included in every sent message. A Checksum is a standard mathematical calculation applied against the entire message before the message is encrypted. Once the recipient decrypts the message successfully, the same Checksum calculation is repeated. If the number obtained matches the number that was sent with the message, the user knows that nothing in the message has been altered. This guarantees integrity.

Ensuring Authenticity:

The sender of a message will typically encrypt a portion of the message, called the signature, using his own private key. The recipient will decrypt that signature using the sender's public key. If this works, it proves that the message did come from the sender. This guarantees the message's authenticity.

Additional Technical Details:

PGP typically uses RSA keys of 1024 bit minimum length. This corresponds to a 309 digit decimal number. In 1998 it was estimated that a 200-digit key would take more than 52,000,000 years for an attacker to crack. This indicates that PGP software offers fully reliable security. (source: <http://senderek.de/security/secret-key.protection.html>).

PGP software is publicly available from a number of sources, including www.pgp.com, www.pgpi.org. It is available on a wide number of platforms including both Unix and Windows. A large number of sources offer this software for free, although some commercial versions may have additional features.



Internet-Based Messaging Solutions for Business

2379 Holly Lane, Suite 210 | Ottawa ON | Canada K1V 7P2
Toll-free: 1-888-733-0000 | (613) 733-0000 | Email: sales@protus.com | www.protus.com

© Protus IP Solutions. All rights reserved. Protus, Virtual Fax and MyFax are trademarks of Protus IP Solutions. All other brands and product names are trademarks or registered trademarks of their respective companies.