Definitions (What is TLS, SSL, SSH, SFTP, HTTPS, PGP etc ...)

- What is encryption/decryption, cipher
- What is TLS/SSL and IPSec
- What is IMAPs/POPs, SMTPs
- What is HTTPs
- What is SSH, SCP/SFTP
- What is a Security Certificate
- What is a 'dummy' / 'self signed' Security Certificate
- What is a CA (Certificate Authority)
- What is PGP (Pretty Good Privacy), OpenPGP, GnuPG and why is different from TLS/SSL
- What is a PGP public key
- What is PGP en/decryption and when is used
- What is PGP Email Integration
- What is a PKS (Public Key Server)
- What is a PKI (Public Key Infrastructure)

What is encryption/decryption, cipher

encryption is the process of converting something readable into something completely unreadable with out loosing the content.

decryption is the process by which the encryption is reversed and the encrypted content is restore to a readable form with out loss.

cipher: The mechanism applied to an encryption/decryption process, the mechanism is a well defined mathematical process

XSecHosting uses the ciphers provided by the OpenSSL library, implementing both the SSL and TLS security protocols used by the IMAPs, POPs, SMTPs, HTTPs, SSH, SFTP, and SCP services. The ciphers provided by the Linux Kernel are used for file system and system resources (en)/(de)cryption, and for implementing the kernel level part of the IPSec Protocols. The ciphers and libraries provided by GnuPG are used by the XSecHosting WebMail service for both digitaly signing and (en)/(de)crypting email. GnuPG is also used by the system to digitaly sign and (en)/(de)crypt system objects and documentation. What is TLS/SSL and IPSecSSL Secure Sockets Layer is a security protocol that provides communications privacy over the Internet. See draft302.txt for the SSL 3.0 specification

TLS: Transport Layer Security is the replacement for SSL. See RFC 2246 for the TLS 1.0 specification.

IPSec: Internet Protocol Secured is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPSec IPsec has been deployed widely to implement Virtual Private Networks (VPNs).

The protocols allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. XSecHosting uses the OpenSSL library to provide the SSL (v2/v3) and TLS (v1) implemention. IPSec is implemented in the Linux Kernel with kernel encryption and the FreeS/WAN, and the replacement OpenS/WAN libraries What is IMAPs/POPs, SMTPs

IMAPs: The SSL secured version of the Internet Message Access Protocol (IMAP), a protocol for accessing electronic messages kept on a mail server. The protocol can be used access messages in the system 'Inbox' and in 1 or more other folders. IMAPs allows the message headers to be downloaded independantly from the message body. XSecHosting supports email access with the IMAPs protocool.

POPs: The SSL secured version of the Post Office Protocol (POP), a protocol for accessing electronic messages kept on a mail server. The protocol can only access messages in the system 'Inbox' and downloads all messages stored there, deleting the messages after transmission. There is an option to keep the messages on the mail server after transmission.

SMTPs: The TLS secured version of the Simple Mail Transfer Protocol (SMTP), a protocol for sending e-mail messages between servers, and from clients to servers for further transmission (relaying). If a mail server does not implemet some kind of authentication relaying (Open Relay), the server can be abused to retransmit messages to other servers easily obscuring the location of the original sender, a techinique often used by spammers to 'hide' the origin of the messages. XSecHosting implements the relay part by authentication (requiring a login and password) the channel is TLS secured to ensure that not only the authentication details, but the content as well is not transmitted in plain text between the client and the server What is HTTPs

HTTPs: Secure HyperText Transfer Protocol (or S-HTTP) is a protocol for transmitting data securely over the World Wide Web. Unlike SSL which creates a secure connection between a client and a server, over which any amount of data can be sent securely, HTTPs is designed to transmit individual messages securely. SSL and HTTPs, therefore, can be seen

as complementary rather than competing technologies. See RFC 2660 for the HTTPs specification

XSecHosting provides HTTPs using the Apache web server which in turn uses the ciphers and functions provided by the OpenSSL library to implement the protocol. What is SSH, SCP/SFTP

SSH: Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist

SCP: Secure Copy is the secure replacement for the remote copy protocol or rcp

SFTP: Secure FTP is the secure replacement for the file transfer protocol or ftp

XSecHosting provides access to the Hosted Websites source folders/directories via SFTP or SCP using the OpenSSH library. However the SSH itself has been disabled as shell access to accounts is not required. All functionality for user administration is provided by the web based [UserMin Client] control interface.

The following free SFTP/SCP Open Source clients are available form our [Downloads] section

Windows
- WinSCP

MAC OS X
- Fugu
- Cyberduck

Linux
- Kbear
- Gftp What is a Security Certificate

A Security Certificate is not a piece of paper rubber stamped by a usually rather large uniformed person at the gate of some barbed wire surrounded location, but it is something simular 'electronicly' speaking. A security certicate is the part of the TLS/SSL type of secure communications protocols presented by the service initiator which contain ing a verifiable identification, a cipher type, and a cipher key to be use in setting up the secured communications session.

There are several types of security certificates, There are the 'dummy/self signed certificates' (see below) used in experimental situations and not recommendated for use with public services. There are authenticated or digitaly signed certificates, authenticated by a certifcate authority (see below) security certificates. And there are the 'On the fly' or 'one off' certificates generated on a per session basis.

XSecHosting uses the latter 2 types of security certificates. However it should be noted that the authenticated certificates are signed by XSecHosting's own certificate authority, and not by one of the so called 'recognised' certificate authorities. It is not a requirement for the presented certificate to be authenticated by a 'recognised' cerficate authority for the secure protocols to work. The protocol mearly requires any 'non authenticated' certifcates to be verified/accepted by the user. Protocols using 'one off' certifcates do not suffer this inconvenience. Mail /Web servers hosted XSecHosting may be used with a client's own (purchased) certificates, see our [services] section for further details. What is a 'dummy' / 'self signed' Security Certificate

A 'dummy' Security Certificate is a security cerificate signed by a fictitious certifcate authority (see below). It may even be in complete or invalid and is used for test purposes only.

A 'self signed' Security Certificate is a security certifcate signed with the key presented in the certificate, and is also only for testing purposes.

XSecHosting does not use 'dummy' or 'self signed' Security Certificates. All XSecHosting security certificates are digitaly signed by XSecHosting's own certificate authority maintained with the same rigorous standards applied by the so called 'recognised' commercial certificate authorities. What is a CA (Certificate Authority)

A Certificate Authority is the owner of a key used to digitaly sign or authenticate a security certificate.

There are 2 types of certificate authorities. The 'non recogised' authority and the 'recognised' authority the difference being the 'recognised' authority will have its own certificate installed in common software eg browsers, mail clients, having paid a fortune for the privilege in return for getting the software to complain (usually very vocaly and with dire warnings) that it does not know the signing authority. A security certifcate is not required to be signed by a 'recognised' authority. It is mearly required to be signed by a certificate authority 'recognised' or 'non recognised' for the protocols to

work.

XSecHosting maintains its' own certificate authority to sign/authenticate its own security certicates the installable XSecHosting root certificate is available on request. What is PGP (Pretty Good Privacy), OpenPGP, GnuPG and why is different from TLS/SSL

PGP (Pretty Good Privacy) a technique developed by Philip Zimmerman for encrypting messages. PGP is based on the public-key method, which uses two keys. One is a public key (see beow) that is made public, it is used to encrypt message to be received by the public key owner. The other is a private key (see below) used to decrypt messages encrypted with the corresponding public key.

OpenPGP is the ietf rfc 2440 standard for PGP describing security services for electronic communications (meaning content as in an email, not protocols) and data storage. These services include confidentiality, key management, authentication, and digital signatures.

GnuPG: The GNU Privacy Guard is an OpenPGP complient complete and free replacement for PGP. Because it does not use the patented IDEA algorithm (which is optional according to the OpenPGP standard) it can be used without any restrictions.

PGP is a set of services used in electronic communications and data storage. TLS and SSL are protocols used to establish secure communications. PGP does not use an ASN1 encoded security certificate to initiate (en)/(de)cryption. PGP encrypts using just a public key, and decrypts using an associated private key, keys mays stored may be in a key ring (a set of known keys). Public keys may also be stored on a Public Key Server or PKS (see below).

XSecHosting uses the GnuPG library in the XsecHosting [WebMail Client] to provide client PGP services, and to provide internal system PGP services. What is a PGP public key

A PGP public key is the key part used in PGP to verify a digitaly signed, or encrypt a document/email. The PGP public key is usually made public to a Public Key Server (PKS) or by other means such as inclusion in an email. What is a PGP Digital Signature and when is used

A PGP Digital Signature is used to provide a means of authenticating a document/email. A Digital Signiture also provides a means of ensuring document/email has not been tampered with during transit.

Even if email transmitted within and between domains hosted by XSecHosting can be seen as end-to-end secure (all clients access/send email using TLS/SSL secured protocols). In terms of accountability XSecHosting recommends digitaly signing all emails as a standard practice. What is PGP en/decryption and when is used

PGP encryption is used to encrypt a message with a known Public Key. Messages encrypted with a Public Key can only be decrypted with a matching Private Key.

Please remember PGP encryption is illegal in certain parts of the world, and using PGP encryption may attract unnecessary attention. PGP encryption is subject to private key integrety. Current UK Law does not make PGP illegal, but does however require PGP keys to be released on demand by law enforcement and may a carry stiff penality for non compliance.

XSecHosting only recommends using PGP encryption if the message path is not end-to-end secure and the recipient is not exposed to the above warnings. Generaly speaking end-to-end secured messaging does not require PGP encryption. E-Mail messages transmitted within and between domains hosted by XSecHosting may be seen as end-to-end secure (all clients access/send email using TLS/SSL secured protocols, where content is encryted for the duration of transport). However XSecHosting recommends using Digital Signitures, for message authentication and integrety checking, as a standard practice. What is PGP Email Integration

PGP Email Integration is the seamless integration of PGP services and functions into an email client. Providing among other things

* Public Key import to PGP key rings
* Encryption to a known public key
* Message decryption
* Message Digital Signiture verification
* Digitaly Sign a message

The free Open Source GnuPG library is available for each of the platforms listed below from our Downloads section, along with the following email client plugins.

Windows
- Enigmail for Mozilla
- G-Data for Outlook
- WinPT Outlook Express Plugin
- WinPT Eudora Plugin
- QDGPG for Pegasus Mail

Mac OS X
- Enigmail for Mozilla
- GPGMail for Apple's Mail
- Eudora-GPG
- Entourage-GPG
- Mailsmith-GPG

Linux
- Enigmail for Mozilla

Note: These Linux email clients have native GnuPG Support
- KMail
- Kontakt
- Evolution
- Sylpheed
- Mew
- Mut What is a PKS (Public Key Server)

A PKS (Public Key Server) is a service provided to store and provide access to PGP Public Keys.

XSecHosting is currently testing a PKS provided by the OpenPGP Public Key Server project and will make the service generaly available soon. What is a PKI (Public Key Infrastructure)

A PKI (Public Key Infrastructure) is defined as a set of procedures for maintaining and accesing Public and private Keys, not necessarily just PGP Public keys. Certificate Authorites (see above) also maintain a PKI to manage the Private and Public keys used in producing , authenticating, and signing Security Certificates.

XSecHosting uses the OpenCA and the OpenSSL libraries to implement and maintain its' own Certificate Authority and PKI.