Glossary

''I know you believe you understand what you think I said, but I am not sure you realize that what you heard is not what I meant.''

Richard Nixon

Authentication
: The positive identification of a network entity such as a server, a client, or a user. In SSL context the server and client *Certificate* verification process.

Access Control
: The restriction of access to network realms. In Apache context usually the restriction of access to certain *URLs*.

Algorithm
: An unambiguous formula or set of rules for solving a problem in a finite number of steps. Algorithms for encryption are usually called *Ciphers*.

Certificate
: A data record used for authenticating network entities such as a server or a client. A certificate contains X.509 information pieces about its owner (called the subject) and the signing *Certificate Authority* (called the issuer), plus the owner's public key and the signature made by the CA. Network entities verify these signatures using CA certificates.

Certification Authority (CA)
: A trusted third party whose purpose is to sign certificates for network entities it has authenticated using secure means. Other network entities can check the signature to verify that a CA has authenticated the bearer of a certificate.

Certificate Signing Request (CSR)
: An unsigned certificate for submission to a *Certification Authority*, which signs it with the *Private Key* of their CA *Certificate*. Once the CSR is signed, it becomes a real certificate.

Cipher
: An algorithm or system for data encryption. Examples are DES, IDEA, RC4, etc.

Ciphertext
: The result after a *Plaintext* passed a *Cipher*.

Configuration Directive
: A configuration command that controls one or more aspects of a program's behavior. In Apache context these are all the command names in the first column of the configuration files.

CONNECT
: A HTTP command for proxying raw data channels over HTTP. It can be used to encapsulate other protocols, such as the SSL protocol.

Digital Signature
: An encrypted text block that validates a certificate or other file. A *Certification Authority* creates a signature by generating a hash of the *Public Key* embedded in a *Certificate*, then encrypting the hash with its own *Private Key*. Only the CA's public key can decrypt the signature, verifying that the CA has authenticated the network entity that owns the *Certificate*.

Export-Crippled
: Diminished in cryptographic strength (and security) in order to comply with the United States' Export Administration Regulations (EAR). Export-crippled cryptographic software is limited to a small key size, resulting in *Ciphertext* which usually can be decrypted by brute force.

Fully-Qualified Domain-Name (FQDN)
: The unique name of a network entity, consisting of a hostname and a domain name that can resolve to an IP address. For example, `www` is a hostname, `whatever.com` is a domain name, and `www.whatever.com` is a fully-qualified domain name.

HyperText Transfer Protocol (HTTP)
: The HyperText Transport Protocol is the standard transmission protocol used on the World Wide Web.

HTTPS
: The HyperText Transport Protocol (Secure), the standard encrypted communication mechanism on the World Wide Web. This is actually just HTTP over SSL.

Message Digest
: A hash of a message, which can be used to verify that the contents of the message have not been altered in transit.

OpenSSL
: The Open Source toolkit for SSL/TLS; see http://www.openssl.org/

Pass Phrase
: The word or phrase that protects private key files. It prevents unauthorized users from encrypting them. Usually it's just the secret encryption/decryption key used for *Ciphers*.

Plaintext
: The unencrypted text.

Private Key
: The secret key in a *Public Key Cryptography* system, used to decrypt incoming messages and sign outgoing ones.

Public Key
: The publically available key in a *Public Key Cryptography* system, used to encrypt messages bound for its owner and to decrypt signatures made by its owner.

Public Key Cryptography
: The study and application of asymmetric encryption systems, which use one key for encryption and another for decryption. A corresponding pair of such keys constitutes a key pair. Also called Asymmetric Crypography.

Secure Sockets Layer (SSL)
: A protocol created by Netscape Communications Corporation for general communication authentication and encryption over TCP/IP networks. The most popular usage is *HTTPS*, i.e. the HyperText Transfer Protocol (HTTP) over SSL.

Session
: The context information of an SSL communication.

SSLeay
: The original SSL/TLS implementation library developed by Eric A. Young <eay@aus.rsa.com>; see http://www.ssleay.org/

Symmetric Cryptography
: The study and application of *Ciphers* that use a single secret key for both encryption and decryption operations.

Transport Layer Security (TLS)
: The successor protocol to SSL, created by the Internet Engineering Task Force (IETF) for general communication authentication and encryption over TCP/IP networks. TLS version 1 and is nearly identical with SSL version 3.

Uniform Resource Locator (URL)
: The formal identifier to locate various resources on the World Wide Web. The most popular URL scheme is `http`. SSL uses the scheme `https`

X.509
: An authentication certificate scheme recommended by the International

Telecommunication Union (ITU-T) which is used for SSL/TLS authentication.