

Appendix
A

GLOSSARY

*Get on the
Fast Track!*



TM

**SYS-ED/
COMPUTER
EDUCATION
TECHNIQUES, INC.**

Term(s)	Description
Authentication	The positive identification of a network entity such as a server, a client, or a user.
Access Control	The restriction of access to network realms.
APache eXtension Tool - apxs	A perl script that aids in compiling module sources into Dynamic Shared Objects (DSOs) and helps install them in the Apache Web server.
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 (subject) and the signing Certificate Authority (issuer), plus the owner's public key and the signature made by the CA. Network entities verify these signatures using CA certificates.
Certification Authority	A trusted third party whose purpose is to sign certificates for network entities it has authenticated using secure means.
Certificate Signing Request	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.
Ciphertext	The result after Plaintext is passed through a Cipher.
Common Gateway Interface	A standard definition for an interface between a web server and an external program that allows the external program to service requests.
Configuration File	A text file containing Directives that control the configuration of Apache.
CONNECT	An HTTP method for proxying raw data channels over HTTP. It can be used to encapsulate other protocols, such as the SSL protocol.
Context	An area in the configuration files where certain types of directives are allowed.
Digital Signature	An encrypted text block that validates a certificate or other file.
Directive	A configuration command that controls one or more aspects of Apache's behavior.
Dynamic Shared Object	Modules compiled separately from the Apache httpd binary that can be loaded on-demand.
Environment Variable - env-variable	Named variables managed by the operating system shell and used to store information and communicate between programs.
Export-Crippled	Diminished in cryptographic strength and security in order to comply with the United States' Export Administration Regulations (EAR).
Filter	A process that is applied to data that is sent or received by the server. Input filters process data sent by the client to the server, while output filters process documents on the server before they are sent to the client.
Fully-Qualified Domain-Name	The unique name of a network entity, consisting of a hostname and a domain name that can resolve to an IP address.

Term(s)	Description
Handler	An internal Apache representation of the action to be performed when a file is called.
Header	The part of the HTTP request and response that is sent before the actual content, and that contains meta-information describing the content.
.htaccess	A configuration file that is placed inside the web tree and applies configuration directives to the directory where it is placed and all sub-directories.
httpd.conf	The main Apache configuration file. The default location is /usr/local/apache2/conf/httpd.conf.
HyperText Transfer Protocol - HTTP	The standard transmission protocol used on the World Wide Web. Apache implements version 1.1 of the protocol, referred to as HTTP/1.1 and defined by RFC 2616.
HTTPS	The HyperText Transport Protocol (Secure), the standard encrypted communication mechanism on the World Wide Web.
Method	In the context of HTTP, an action to perform on a resource, specified on the request line by the client.
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.
MIME-type	A way to describe the kind of document being transmitted. Its name is derived from the Multipurpose Internet Mail Extensions.
Module	An independent part of a program. Much of Apache's functionality is contained in modules that which can be included or excluded. The modules types are static, dynamic, base, and third party.
Plaintext	The unencrypted text.
Private Key	The secret key in a Public Key Cryptography system, used to decrypt incoming messages and sign outgoing ones.
Proxy	An intermediate server that sits between the client and the origin server. It accepts requests from clients, transmits those requests on to the origin server, and then returns the response from the origin server to the client.
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.
Regular Expression - Regex	A way of describing a pattern in text. Regular expressions are useful in Apache because they let you apply certain attributes against collections of files or resources in very flexible ways.

Term(s)	Description
Reverse Proxy	A proxy server that appears to the client as if it is an origin server. This is useful to hide the real origin server from the client for security reasons, or to load balance.
Server Side Includes - SSI	A technique for embedding processing directives inside HTML files.
SSLey	The original SSL/TLS implementation library developed by Eric A. Young
Symmetric Cryptography	The study and application of Ciphers that use a single secret key for both encryption and decryption operations.
Tarball	A package of files gathered together using the tar utility. Apache distributions are stored in compressed tar archives or using pkzip.
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.
Uniform Resource Locator - URL	The name/address of a resource on the Internet.
Uniform Resource Identifier	A compact string of characters for identifying an abstract or physical resource. It is formally defined by RFC 2396.
X.509	An authentication certificate scheme recommended by the International Telecommunication Union (ITU-T) which is used for SSL/TLS authentication.