

# Glossary

**3G** ? 3rd generation GSM.

**A/A** - Active/Active.

**A/P** - Active Passive.

**Active/Active** Where both PINsafe servers are active at the same time and may both respond to authentication requests.

**Active/Passive** Where one PINsafe server only is active, the other taking over upon failure of the first.

**AD** ? Active Directory, windows user management system, similar to a phone book.

**Apache** ? Linux Web Server.

**API** ? Application Program Interface, a set of protocols and method for communicating with a program.

**AES** ? Advanced Encryption Standard.

**CA** ? Certificate Authority.

**CAPTCHA** - Text presented to the user in a form to prevent automated reading by computer OCR software. The digits are often varied, run together, coloured or animated.

**ChangePIN** - A self help tool allowing a user to change their PIN

**CHAP** ? Challenge Handshake Authentication Protocol, uses one way MD5 hashes to encrypt data and check usernames and passwords.

**CMI** - Command Management Interface, used to manage and configure the PINsafe appliance

**Data Store** ? Where PINsafe data is Stored, either an internal or External database.

**DC** ? Domain Controller in Active Directory.

**DES** ? Double Encryption Standard.

**Dual Channel** ? 2 channels are used for communications, e.g. Internet and mobile phones. This helps to increase security as both channels would have to be compromised.

**Dual Factor Authentication** ? Two methods of providing login credentials, typically something you have such as a fingerprint and something you know, such as a password.

**FTP** - File Transfer Protocol

**GIF** - Graphics Interchange Format, an image format

**GINA** ? Graphical Identification and Authentication, a replaceable DLL that allows a windows logon to be altered. This is used for Windows XP, 2000, and 2003. later versions do not use the Windows GINA.

**GPRS** ? General Packet Radio Service, used for transmitting data by mobile phones.

**GSM** ? Global System for Mobile communications.

**Hash** ? a unique string generated against a file to indicate if tampering has occurred.

**HTTP** - The Hypertext Transfer Protocol.

**IAG** - Intelligent Application Gateway. A Microsoft VPN and Application firewall.

**IIS** - Internet Information Services, a Microsoft web server.

**ISAPI** ? Internet Server API, an IIS API allowing web applications to be added.

**ISA** ? Internet Security and Acceleration server, a Microsoft product.

**J2ME** ? Java 2 platform Micro Edition, allowing development for wireless and mobile devices

**JSP** ? Java Server Pages.

**Key Logger** - Software on a PC or Hardware attached to a PC that will allow information entered on a keyboard to be captured. Often used for capturing passwords as part of a Trojan or virus.

**LDAP** ? Lightweight Directory Access Protocol ? contains user information, similar to a phone book.

**M2F** ? Mobile 2 Factor.

**Man in the middle attack** ? a user is redirected to another fake site that records their information for connecting.

**MIDP** ? Mobile Information Device Profile.

**MD5** ? A one way has function to produce a unique string of digits.

**MSISDN** - Mobile Station Integrated Services Digital Network, The number used to call a mobile subscriber. An MSISDN consists of a country code, a national destination code and a subscriber number.

**Multicast** - Used for session sharing between PINsafe servers. Requires that the PINsafe servers are able to send and receive multicast traffic between the PINsafe appliances.

**NAS** ? Network Access Server.

**Obfuscation/Obfuscated** ? hidden from view.

**OCR** ? Optical Character Recognition.

**OS** ? Operating System.

**OTC** ? One Time Code, a one time password, once the code is used it cannot be used again.

**OWA** ? Outlook Web Access.

**PAP** ? Password Authentication Protocol, whereby usernames and passwords are checked, PAP data is transmitted without encryption. The database of passwords and usernames may be encrypted.

**Phishing** ? A social engineering attack, whereby a user is tricked into giving away their login, passwords and other details to those masquerading as legitimate organisations. Often carried out by email, asking users to enter their details on a fake website.

**PIN** - A unique number remembered by a user for extracting an OTC from a security string.

**PIN Extraction** - The process of extracting an OTC from a Security String.

**PINless** - An OTC that is sent directly to the user without the need for PIN extraction.

**PINsafe** - A method of providing an OTC through the use of a PIN and a security string.

**RADIUS** ? Remote Authentication Dial In User Service, usernames and passwords are checked against the RADIUS server before being allowed access.

**ResetPIN** - A self service tool, allowing a user to be sent a new PIN if it has been forgotten.

**sAMAccountName** - The logon name that is used to support clients and servers in earlier versions of Windows

**Security String Index** - When a user receives multiple security strings by SMS or email, each one is given a number known as the security string index. PINsafe can tell the user which security string to use by telling them the security string number

**Session Sharing** - Where information is shared across a pair of PINsafe servers allowing the graphical Single Channel image to be requested from one server and the authentication made against another server.

**Single Factor Authentication** ? Where only one identification is used for gaining access to a system, this could be just a username and password, or just a token.

**SNMP** - Simple Network Management Protocol, a UDP protocol used for monitoring hardware and software

**Tomcat** ? An Apache Java Container.

**Transport** - A method of transmitting information to a user. This can be information such as an alert, or a security string such as a Turing image, an SMS message, an email.

**Trojan** - Software that hides within other software programs to hide it from detection. Key loggers may be put onto machines in this way.

**UPN** ? User Principle Name, for Active Directory.

**VM** - Virtual Machine.

**Positive ID** ? A mechanism to uniquely identify a computer or other such device.

**SCP** - Secure Copy, used for copying files between computers over an encrypted link.

**Security String** - A 10 digit sequence of numbers or letters from which an OTC can be extracted by using a PIN number.

**SMS** ? Simple Messaging System. Allows text messages to be sent to mobile phones.

**SMTP** ? Simple Mail Transfer Protocol (email).

**Social Engineering** ? Obtaining passwords or other information by persuading users to give them up.

**SSH** - Secure Shell, allows command line access through an encrypted link. Other protocols may be tunneled through SSH.

**SSL** ? Secure Sockets Layer, a method of encrypting web communications. SSL can be run on almost any port.

**Swivel** - A connector allowing free rotation

**Swivlet** ? A Mobile Phone Client Java application for providing authentication strings to a user.

**TCP** - Transmission Control Protocol, is a network transmission used for transferring data reliably between two network hosts.

**TMG** - Threat Management Gateway, A Microsoft product and is a follow on to the ISA server.

**Tomcat** ? official reference container for the Java servlet.

**Turing Image** ? An image designed to give a number or character that is difficult for computer software to read. Named after a pioneer of computing.

**Two Factor Authentication** ? 2 forms of identification, such as username and password, or biometric and pin number.

**Two Way Authentication** - The ability of the authentication mechanism to respond back to the server. For example an SMS text message sent to a user and the user responds with a SMS text message.

**UAG** - Unified Access Gateway - A Microsoft VPN and Application level firewall. This is a follow on to the IAG.

**UDP** - User Datagram Protocol, a simple transmission control protocol without error checking present in TCP.

**VIP** - Virtual IP Address, used for fail over whereby the VIP moves from one server to another

**Virus** - software that transmits itself from one computer to another, the purpose of which may be for gathering information such as usernames and passwords, or to delete or manipulate files and data.

**VM** - Virtual Machine, a guest OS run on another OS.

**W3C** ? World Wide Web Consortium.

**WAI** ? Web Accessibility Interface, to allow ease of use for disabled users.

**WAR** - Web application ARchive, a file format used to package Java applications

**XML** ? Xtensible Markup Language ? programming language understood by web browsers.