Westpac Institutional Bank

A division of Westpac Banking Corporation ABN 33 007 457 141

Quickstream

Connectivity Options

Date	Description
25-Jun-2003	Initial Version
1-Jul-2003	Added details on HTTPS connections and dial-up
3-July-2003	Changed "Leased Line" to "Frame Relay".
18-July-2003	Updated to include SSL server certificates
18-Aug-2003	Updated to include OPI dial-in
8-Sep-2003	Clarified HTTPS connectivity
19-Sep-2003	Added certificate attribute information
31-Oct-2003	Added FAQ
11-Dec-2003	Added Glossary
23-Feb-2004	Added Dial-up ISDN router option
18-Mar-2004	Updated PGP Options
15-Apr-2005	Updated Connectivity Options
19-Jul-2005	Updated Connectivity Options
26-Sep-2005	Updated Connectivity Options
15-Nov-2006	Added ilink
3-Apr-2008	Clarified connectivity via existing Westpac links.
5-Oct-2009	Updated

Table of Contents

1 Introduction

Westpac is utilising technology developed by our Qvalent subsidiary in conjunction with existing market leading transactional banking products to provide comprehensive receivables management solutions.

This document describes options for connectivity with the **Quickstream** solution offered in Australia. A comparable solution is available in New Zealand.

The Quickstream solution is provided under an Application Service Provider (ASP) service, where the software is hosted externally to your business. This document describes connectivity between your internal applications and Quickstream, in a manner appropriate to your business and in accordance with your own security standards. It does not include details on file formats or API calls as this would be covered in other implementation documents.

1.1 Integration points

Quickstream has a number of integration points that may be grouped as follows:

- Ø **File-based integration**. This is where the majority of Quickstream integration efforts are concentrated, for sending of files to Quickstream (eg invoices/statements) and receiving files from Quickstream (eg cash applied file).

- Ø **Credit Card API integration**. For customers of the credit card API, there is a need for connectivity to the API.

There is also screen-based integration for QuickWeb customers where a link from their web site redirects the browser to a Quickstream-hosted page. This is performed using a standard URL over the Internet and is not discussed further in this document.

Other integration points would be discussed as part of the specific implementation.

1.2 Overview of Connectivity Options

There are a number of connectivity options available between Quickstream and our customers, whether this is for file or API connectivity. These can be separated into connectivity via the Internet, frame relay, Ethernet, ISDN, ADSL or dial-up.

Choosing the appropriate link for connectivity is the first decision to be made in connecting with Quickstream. The following table provides a summary of the available options and how you may choose the connectivity option most appropriate for your business.

Connect via…	Notes	Choose if…
Internet	This is the cheapest and quickest setup method for connectivity. Full public/private key encryption is used over the Internet and therefore information may be safely transmitted, however this does not fit with the security model of all customers. The performance of such a link is also not guaranteed so it is not appropriate for high volume API transactions. Refer to Section 2 for more details on this connectivity option.	Ø Corporate policy does not enforce the use of leased line Ø Guaranteed performance is not required (eg batch file transfers or low volume of Credit Card API calls) Ø Require lowest cost or fastest connectivity option
Frame Relay	This is a standard frame relay link with a guaranteed level of performance. Our preferred supplier is Optus, and we can facilitate the enablement of the connection in order to minimise the difficulty on your side. Refer to Section 3 for more details on this connectivity option.	Ø Corporate policy is to use dedicated line in preference to the Internet Ø Guaranteed performance is required (eg high volume of Credit Card API calls)
Broadband (ADSL)	Though Optus, Qvalent can offer ADSL access. This is the same service that ISP's provide with the exception that you are connecting into Qvalent's private wide area network and not the Internet. Contact Qvalent for more details regarding this configuration.	Ø Corporate policy is to use dedicated line in preference to the Internet Ø High levels of performance (eg high volume of Credit Card API calls) Ø Much cheaper to operate and configure as compared to frame relay
Ethernet	For high availability solutions Qvalent recommends dual Ethernet links connected to Optus's MPLS core. The border gateway protocol (BGP) is then used to propagate routes between the customer site and Qvalent. This solution	Ø Corporate policy is to use dedicated line in preference to the Internet Ø Guaranteed performance is required (eg high volume

	provides automatic failover in the event of a link or router outage. Contact Qvalent for more details regarding this configuration.	of Credit Card API calls) Ø Automatic failover in the event of a link or router failure
Dial-up	This is a dial-up connection via a modem or ISDN router to our service using a provided phone number. Refer to Section 4 for more details on this connectivity option.	Ø Internet option is not feasible due to remote location and frame relay performance is not required Ø Using file-based integration (this option is not recommended for API customers)

Please note: For customers that currently exchange files already with Westpac, it may be possible to send/receive Quickstream files through the same mechanism. If you wish to consider this, please discuss this with your Westpac contact to determine the feasibility of this option. If you are using an IP-based link, you may be able to exchange files directly with Quickstream. If you are using an SNA-based link, you cannot exchange files directly with Quickstream. Any file exchanges, where possible, will be via the Westpac mainframe.

2 Via the Internet

Connectivity to Quickstream is possible via the Internet assuming that the necessary security precautions are put in place. These security precautions include encryption via public / private key and digital signatures for non-repudiation. Please see the following for more details.

2.1 Standard Connectivity

2.1.1 File-based integration

Quickstream can support a number of file-based mechanisms to communicate data between customers and itself. To facilitate data connectivity, Quickstream can accept data in a customer's native format. These formats can include delimited, fixed length or XML based structures.

Security and guaranteed delivery are two key issues when transferring files over the Internet. These are discussed in the following sections.

2.1.1.1 Security

All files transferred must be encrypted and digitally signed between Quickstream and the customer site. This serves two purposes; the first is to ensure that the data cannot be viewed by unauthorised sources. The second is to provide non-repudiation. Through the use of public / private keys, data can be digitally 'signed', by 'signing' the file both Westpac and the customer can be assured that the data originated from a known source and it has not been tampered with. Westpac recommends the following product for encryption and digitally signing of data:

Ø GnuPG (www.gnupg.org). This is a public domain PGP server that may be used free of charge. Obtaining of this product is the responsibility of the customer, however Westpac is able to provide technical assistance to support this.

2.1.1.2 Guaranteed Delivery

Westpac recommends the use of Computer Associates Advantage CA-XCOM, which is available from Westpac. This software may be obtained on request from your Westpac contact and provides guaranteed file delivery. Installation and configuration is the responsibility of the customer's IT staff, however Westpac is able to provide technical assistance to support this.

Additionally, Westpac supports Secure Copy Protocol (SCP) and SFTP. These protocols allow files to be pushed to Westpac or polled from Westpac in a secure manner. Common transport mechanisms such as SMTP or FTP are not supported as they do not meet banking security standards.

2.1.1.3 Via HTTPS

For smaller sized messages, clients may instead use HTTPS to exchange files with Quickstream. In this case, guaranteed delivery is the responsibility of the customer and they must implement retry mechanisms to send/receive files in the event of a network outage.

Security is provided through basic HTTPS authentication through an assigned username/password and a reverse lookup that the request is from a known IP address. All traffic between the customer's server and the Quickstream server is encrypted using the Quickstream 128-bit SSL certificate.

Optionally, for customer's wishing to introduce a further layer of security, data may also be either encrypted and digitally signed (see Section 2.1.1.1) or the customer's HTTPS requests may be verified using a 128-bit SSL certificate installed on the customer's server (similar to the Credit Card API over the Internet, see Section 2.1.2.1).

To send data to Quickstream, the customer must perform a POST to a URL that will be provided.

To receive data from Quickstream, the customer may poll a separate URL and retrieve the data from the response. Alternatively, Westpac can POST the data directly to a customer-provided site that is accessible from the Internet.

2.1.1.4 Other Mechanisms

In addition to the above products, other open standards such as SOAP can also be considered for integration with Quickstream.

If you wish to consider one of these mechanisms, please indicate this requirement to your Westpac contact.

2.1.2 Credit Card API integration

Quickstream offers an application programming interface (API) that accepts a credit card transaction request and returns a response in real-time. The security and delivery mechanisms for this are described in the following sections.

2.1.2.1 Security

Credit card fraud is a key concern when processing credit card transactions over the Internet. To mitigate this risk, strong security measures need to be implemented. To this end it is mandatory that the Customer use a SSL server-based certificate. An SSL based server certificate has the intended purpose of ensuring the identity of a remote computer. Before the API can be accessed keys must be exchanged between the Client and Westpac.

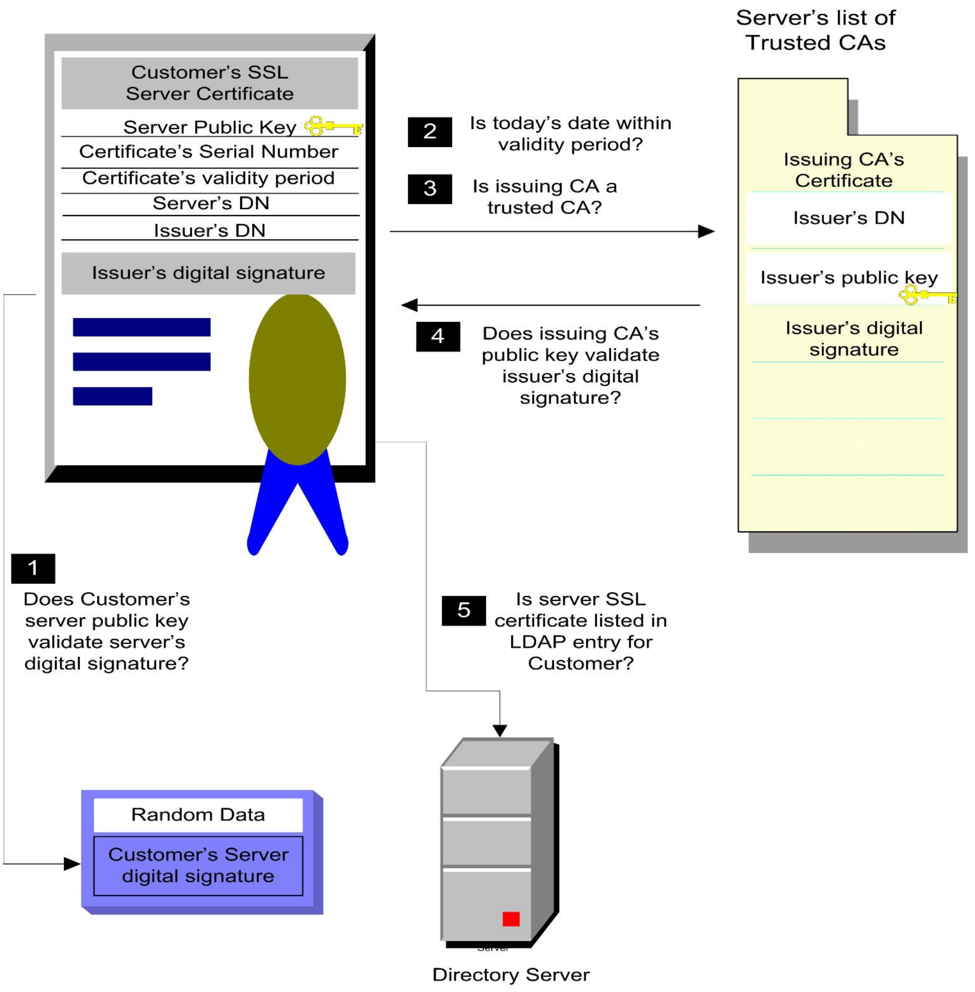
The process of obtaining and registering for a SSL server based certificate is as follows:

1. The Customer must obtain a 128-bit SSL Certificate from a registered Certificate Authority (eg Verisign). This may be purchased or an existing, valid certificate may be used for this purpose. **Note: this SSL certificate must have the property "Proves your identity to a remote computer". Without this property set on the certificate, Westpac will not accept credit card API connection requests.**

2. The public key of the SSL certificate must be provided to Westpac for registration on the Present & Pay server. A method of exchange will be determined during the implementation.

3. The private key of the SSL server certificate must be registered in the customer's key store. If you require assistance in this matter, please indicate this to your Westpac contact.

4. An API call should be tested to ensure that the connection is now working and any outstanding issues resolved. Please note: there are different URLs for the API depending on whether or not SSL certificates are being used.


Customer's SSL Server Certificate
Server Public Key
Certificate's Serial Number
Certificate's validity period
Server's DN
Issuer's DN
Issuer's digital signature
Server's list of Trusted CAs
Issuing CA's Certificate
Issuer's DN
Issuer's public key
Issuer's digital signature
2
Is today's date within validity period?
3
Is issuing CA a trusted CA?
4
Does issuing CA's public key validate issuer's digital signature?
1
Does Customer's server public key validate server's digital signature?
5
Is server SSL certificate listed in LDAP entry for Customer?
Random Data
Customer's Server digital signature
Server
Directory Server

When a customer attempts to use the API the following steps take place:

1. The server uses the customer's server public key (from the certificate) to decrypt the data sent (which was encrypted with the customer's private key). This verifies the client's digital signature, thus ensuring that the provided public key matches the customer's server private key and that the data has not been tampered with during transmission.

2. The server checks that the certificate is valid for the current date – i.e. that the certificate has not yet reached its validity period and has not expired.

3. The server checks that a trusted client Certificate Authority (CA) issued the customer's certificate.

4. The server uses the CA's public key (obtained from Westpac's list of trusted CA certificates) to validate the digital signature of the client's certificate. A CA signs each SSL server certificate, and this step verifies that the SSL server certificate was

indeed signed by this CA and has not been altered since it was issued. If the private key used to sign the client certificate does not match the public key from the server trust database, this step will fail. Note that if there is multiple CAs in the SSL certificate's certification chain, each certificate in the chain will be verified until a trusted CA is reached.

5. The certificate is checked byte for byte in the Quickstream directory server to ensure it is from a registered customer. If a match is found, then access to the API is granted.

All this takes place over a 128bit secure sockets layer (SSL) connection. Once this process is complete, the customer may then issue a credit card request.

Important Note: Refer to the FAQ at the end of this document on certificate chain trusting.

2.1.2.2 Communication Mechanism

Once a customer has been authorised, they may issue a credit card transaction and receive the response back synchronically. Quickstream offers two mechanisms to achieve this. These are via:

- Ø SOAP over HTTPS. A SOAP compliant API is available for the issuing of transactions. All SOAP requests and responses are issued using XML based syntax. The SOAP API is exposed as a standard web service.

- Ø HTTPS POST. A customer may issue a transaction as a HTTPS POST using name / value pairs. In addition to the stand HTTP response code, additional name / value pairs will be returned to the customer containing the outcome of the request.

In the event of a network outage during a transaction, mechanisms are in place to ensure that a transaction can only be processed by the credit card gateway once. For example, if a customer lost network connectivity during a transaction, when connectivity is re-established, and if they are uncertain of the outcome of the transaction, they should reissue it. The credit card gateway in Quickstream will ensure that it is processed only once.

Customers can create their own implementation of the client in any language that supports POST's or SOAP and client certificate based SSL negotiation. Westpac can also provide a Java based client including the source code.

Important Note: Refer to the FAQ at the end of this document on certificate chain trusting.

3 Via Private Link

Optus Multi-protocol Label Switching (MPLS) is a secure IP network used to transfer sensitive information between organisations at guaranteed speeds. MPLS is a redundant multi router cloud that offers connectivity options such as Ethernet, DSL, frame relay ISDN and dial-up. A customer connects into the ‘cloud’ which is linked to all Westpac data centres and offering multiple link paths. This removes reliance on point to point links.

The same mechanisms documented in section 2.1.1 apply for file-based transfers over MPLS.

3.1 Credit Card API integration

For the credit card API (refer to section 2.1.1.3), HTTPS is used with optional SSL server certificates.

4 Via Dial-up

For customers requiring a dial-up connection to send and receive files, Quickstream may be accessed using a modem or via an ISDN dial-up router connection. A phone number will be provided as part of the implementation. Please note for dial-up connections Westpac can not push files to customers. Customers must poll Westpac to receive files. Customers may however push files to Westpac.

4.1.1 File-based integration

After establishing a connection to the network using a modem, the customer may transfer files using the methods described in Section 2.1.1, including XCOM and HTTPS.

4.1.2 Credit Card API integration

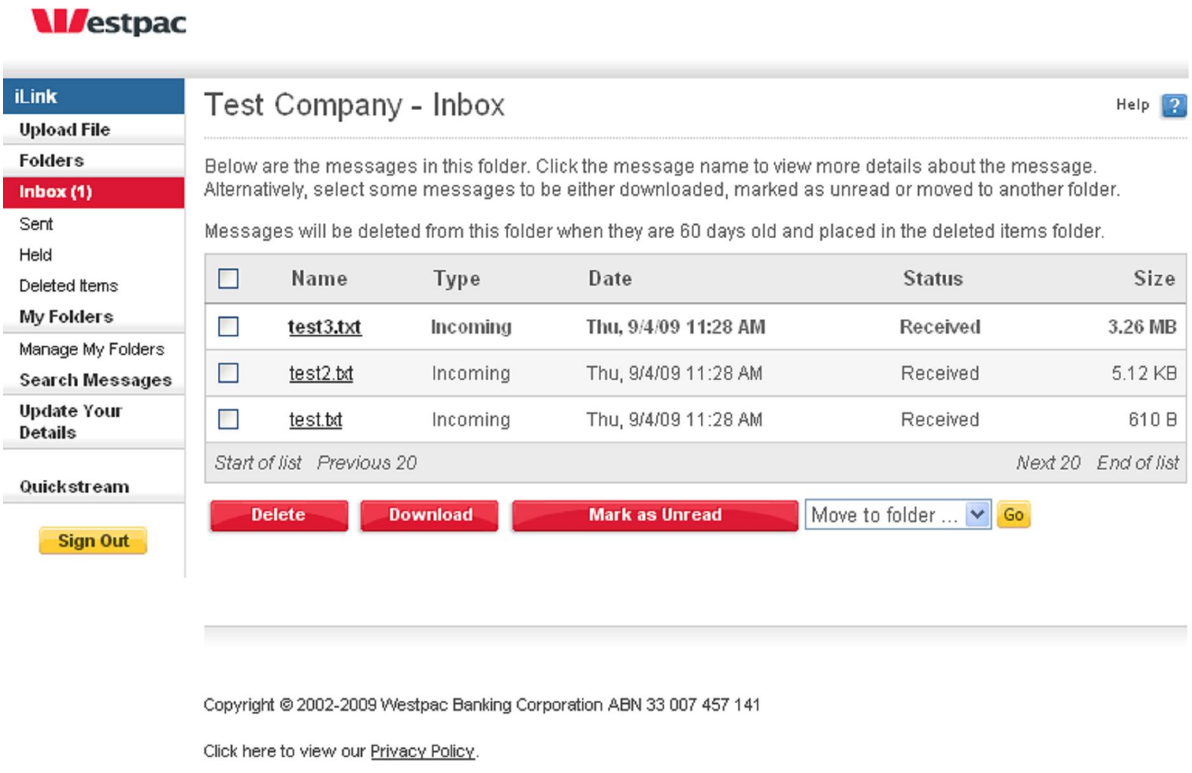
Not recommended for dial-up connections.

5 Via iLink

ilink is a secure web based interface that allows you to upload files to Westpac or download files from Westpac via the Internet. ilink can function as your daily mechanism to communicate with Westpac, or it can provide you with a business continuity process in the event that your links or hardware stop functioning.

5.1.1 How does ilink work?

ilink uses a simple mailbox concept to allow you to manage the files between yourself and Westpac. Any files sent to you from Westpac will appear in you 'inbox' just like your email. A simple to use wizard will lead you through the file upload process. Messages you upload to Westpac will appear in your 'sent' mailbox. ilink will automatically accept files that have been compressed using industry standard ZIP format to speed the upload of large files. For sensitive files you can specify that dual authorisation is required before the file is moved from ilink to Westpac for processing.



Test Company - Inbox

Below are the messages in this folder. Click the message name to view more details about the message. Alternatively, select some messages to be either downloaded, marked as unread or moved to another folder.

Messages will be deleted from this folder when they are 60 days old and placed in the deleted items folder.

□	Name	Type	Date	Status	Size
□	test3.txt	Incoming	Thu, 9/4/09 11:28 AM	Received	3.26 MB
□	test2.txt	Incoming	Thu, 9/4/09 11:28 AM	Received	5.12 KB
□	test.txt	Incoming	Thu, 9/4/09 11:28 AM	Received	610 B

Start of list   Previous 20   *Next 20   End of list*

Copyright © 2002-2009 Westpac Banking Corporation ABN 33 007 457 141

Click here to view our Privacy Policy.

Figure 1, ilink Web Interface

6 FAQ

This section provides the answers to a number of questions that are commonly in relation to connectivity and digital certificates.

What type of digital certificate do I need to obtain to communicate with the Westpac credit card API or post data via HTTPS?

You need to obtain a standard 128bit SSL certificate. This certificate must have the property “Proves your identity to a remote computer” set on it.

Can I install my certificate on my proxy server?

No, while SSL will work via a proxy server, the actual certificate must be installed on the server that is instigating communications with Westpac.

Can I use a self-signed certificate?

Yes, provides that Westpac can verify the source of your public key.

When I try and connect to the Westpac test environment I get the following error “The certificate authority is invalid or incorrect”. What does this mean?

Westpac uses self signed certificates in its test environment. Please contact Westpac to obtain a copy of their public key. You will then need to embed this key into your key store.

Can I FTP data to Westpac?

Westpac does not recommend FTP due to it not providing a guaranteed delivery mechanism and security concerns around the FTP protocol.

What Level in the Qvalent certificate chain should I trust?

Where a customer system exchanges information with Qvalent either via credit card API, PNPnet or HTTPS post, the customer system **must trust the root level certificate (ie that issued by Verisign) and not the certificate issued to Qvalent**. The Qvalent certificates expire and are replaced each year, whereas the Verisign certificates have a much longer life (i.e. expiry in 2028). Any customers that trust the Qvalent certificates directly will cease to operate as replacement certificates are installed and therefore this must be avoided.

7 Glossary

CA-XCOM
CA-XCOM is a cross-platform, value-added data transport solution, providing high-performance unattended file transfer with complete audit trails and reporting. CA-XCOM provides a single solution for sending and receiving files, as well as sending reports and jobs, to a wide range of platforms. This is Qvalent's standard file transfer mechanism.

Certificate
An electronic document that identifies an entity (e.g. a person, computer or company). Each certificate contains the entity's public key, along with details about which encryption algorithms the entity can use. Certificates are issued by Certificate Authorities (CAs) when the CA verifies the entity requesting the certificate.

Each certificate contains a subject, describing who the certificate is for, and an issuer, describing the organisation that signed the certificate.

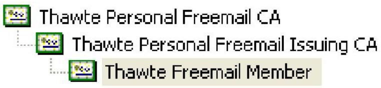
The certificate contains the entity's public key, as well as the digital signature of the CA. This signature is like a hologram on a credit card, verifying that the CA has authenticated the entity's identity.

Certificates can be marked for various purposes, including SSL client, SSL server and CA. See also *Certificate Authority*, *Digital Signature*, *SSL* and *Public Key Encryption*.

Certificate Authority
A trusted third party that signs certificates for other parties. Often in internet communications, the two parties will not trust each other, but will trust a third party. Party A can trust party B's certificate if it is signed by that third party (the certificate authority or CA).

Certain CAs (e.g. Verisign, Thawte) are automatically trusted by all certificate software. See also *Certificate* and *Certificate Hierarchy*.

Certificate Hierarchy
The chain of certificates for an entity consisting of that entity's certificate and any CAs which signed the certificate. All certificates are signed by another certificate, generating a hierarchy. This hierarchy terminates at a root certificate, which is **self-signed**. This type of certificate contains an identical issuer and subject.



Thawte Personal Freemail CA
Thawte Personal Freemail Issuing CA
Thawte Freemail Member

A certificate is trusted by a party if the certificate chain terminates at a CA which is trusted by that party. Each party maintains a list of trusted root CAs. See also *Certificate*, *Certificate Authority and Self-signing*.

Digital Signature
A process of signing a message electronically. Normally, the sender of a message will calculate a message digest, then encrypt that digest value with the sender's private key. This resulting value is the digital signature.

The receiver can verify the signature by calculating the message digest, and comparing it to the value obtained by decrypting the digital signature with the sender's public key. See also *Message Digest* and *Public Key Encryption*.

Encryption / Decryption
The process of scrambling a message so that it cannot be read by a third party while in transit. The sender encrypts a message before sending, and the receiver decrypts the received message before reading it.

Many algorithms are available to encrypt data. Examples include RSA, RC4 and DES. The algorithm is generally well-known, but a number (called a **key**) must be used with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption with the correct key is simple, whereas without the key, decryption is almost impossible.

HTTP
Hypertext Transfer Protocol: The application level protocol that is used to transfer data on the web. A client sends a request message to the server, and the server sends a response message.

Each message consists of a start line (which is either a request line or a status line as appropriate), followed by a set of message headers and finally an optional message body.

The request line contains the method (usually GET or POST) used for the request. GET is a simple request for information, whereas POST allows the client to send data to the server in the request.

A web browser generally sends a GET request to the server for information, and the server responds with a HTML document in the response for the browser to display.

The HTTP protocol uses the TCP/IP protocol to transport the information between client and server. HTTP uses TCP port 80 by default. See also *TCP/IP*.

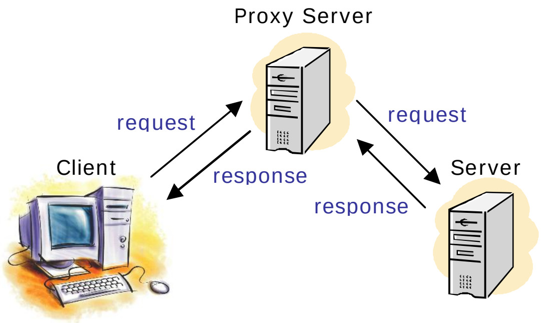
HTTPS
Hypertext Transfer Protocol, Secure: The HTTP protocol using the Secure Sockets Layer (SSL), providing encryption and non-repudiation. HTTPS uses TCP port 443 by default. See also *HTTP* and *SSL*.

Message Digest
A mathematical function which generates a number from a message (also called a one-way hash). The generated number is unique for the message, in that changing any part of the message changes the resulting number. The function is one-way in that it is, for all practical purposes, impossible to determine the message from the number. Common algorithms are MD5 and SHA-1.

Non-repudiation
Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Proxy Server
An intermediate server on the client side of a HTTP transaction which makes requests on behalf of the client. Proxy servers improve corporate security by only exposing the proxy server to the internet, rather than each individual computer in the organisation.

The client sends its request to the proxy server, which then sends the request (with any modifications) to the server. The server responds to the proxy, which then passes the response to the client.



System administrators can restrict which servers are accessible simply by configuring the proxy server. See also *HTTP*.

Public Key Encryption
An encryption method where different keys are used for encryption and decryption. Each party has two keys – a public key and a private key. Messages encrypted with the public key can only be decrypted with the private key, and messages encrypted with the private key can only be decrypted by with the public key. Each party publishes their public key and keeps their private key secret.

Encryption is accomplished by the sender encrypting the message with the receiver's public key. The message can then only be decrypted by the receiver with his private key.

Non-repudiation is accomplished by the sender encrypting the message with her private key. The message can then be decrypted by anyone with the sender's public key (which is published), but the receiver can be assured of the message's origin. See also *Symmetric Key Encryption* and *Encryption*.

Self-Signing
Self-signing occurs when the owner of a key uses his private key to sign his public key. Self-signing a key establishes some authenticity for the key, at least for the user IDs. The user ID of the signature must match the user ID of the key. (Where there are multiple user IDs, the ID of the signature must match the primary ID of the key.) Also, the key ID of the signature matches the key ID of the key. This verifies that whoever placed a user ID on a public key also possesses the private key and passphrase. Of course, this does not verify that the owner of the key is really who she says she is. That is done by the signatures of others on the public key (such as a root CA like Verisign).

SOAP
Simple Object Access Protocol: An XML-based protocol allowing remote procedure calls and asynchronous messaging. SOAP generally uses HTTP to transport the messages between computers. SOAP is becoming popular because of its use of standard internet protocols as its basis. See *XML* and *HTTP*.

SSL
Secure Sockets Layer: A protocol designed by Netscape to encrypt data, authenticate the client and server and ensure message integrity. SSL sits between the application layer protocol (e.g. HTTP) and above the TCP/IP network protocol.

The SSL handshake establishes the SSL connection, setting up the secure channel. In this process, the server presents its certificate to the client for authentication:

- The server encrypts some data with its private key and the client then checks this signature with the public key from the server's certificate.
- The client checks that the server DNS name is the same as that in the certificate.
- The client checks that the server certificate has not expired.
- The client checks that the server's certificate is signed by a trusted CA.

The server can also optionally require the client to present its certificate to the server for authentication.

The handshake also allows the client and server to agree on an encryption algorithm (a symmetric key algorithm for speed), and securely exchange the session key. This session key is used in the encryption algorithm which encrypts the data exchanged between the client and server after the handshake is finished. The session key length can be 40-bit, 56-bit or 128-bit, with the longer keys being more difficult to break. See also *TCP/IP*.

Symmetric Key Encryption
An encryption method where the sender and receiver use the same key to encrypt and decrypt the message. This method relies on the key being kept secret between the two parties. If the key is discovered, anyone can read the messages in transit, or send false messages to the receiver.

This type of encryption is often used for bulk encryption because it is much faster than public key encryption. See also *Encryption* and *Public Key Encryption*.

TCP/IP
Transmission Control Protocol over Internet Protocol. IP allows packets of data to be sent across the internet from one computer to another. TCP provides a reliable communication stream between the two computers, using the Internet Protocol.

XML
eXtensible Markup Language: A document formatting language which describes a standard syntax, but allowing many different document types. Business partners can then agree on the specific documents they will exchange, using the standard syntax. XML documents contain a hierarchical list of tags, some of which contain values.