

OFTP2 (Published by Data Interchange plc – www.dip.co.uk)

Overview

OFTP2 updates the OFTP (ODETTE File Transfer Protocol) in line with market desires to strengthen its position as the premier choice of businesses for performing reliable, automated exchanges of business documents in ALL market sectors. This has been achieved by implementing new security features within OFTP and by adding in other useful features desired by businesses.

The Internet is the network of the future having already displaced both X.25 and ISDN as communications options. Companies are frequently turning to the Internet for communications to take advantage of the lack of call charges and high bandwidth availability. Unfortunately the Internet is inherently insecure with anybody able to look at the packets that are exchanged between computers. It is not a safe environment for companies wishing to exchange business critical data and highly confidential information. Security features in OFTP have not previously been required when X.25 and ISDN networks were commonplace but, with the advent of the Internet, OFTP had to evolve and provide security features to remain as the protocol of choice for businesses.

The new OFTP2 goes head to head with an alternative protocol for secure EDI over the Internet, known as AS2. This whitepaper is intended to provide a comparison of OFTP2 and AS2, both from a commercial perspective and from a technical perspective.

OFTP2 has been developed by the OFTP Security Working Group, working under the ODETTE International banner.

Key Features

- Message encryption
- Digitally signed messages
- Digitally signed message receipts
- Authentication
- File compression
- Automatic file restart
- Works over ISDN, X.25, TCP/IP

OFTP2 Commercial Benefits

- Compression means reduced X.25 and ISDN call charges
- Compression means reduced time to exchange data
- Companies with investments in X.25 and ISDN networks can use OFTP2 Security
- No permanent Internet connections required (Virtually zero networking costs)
- No firewalls required for small companies
- Handling of large files means less delays due to backlogged traffic
- Indirect communications via Value Added Networks (VANs) possible
- Direct communication bypassing VANs
- One protocol for all trading partners regardless of network connection type
- No traffic costs when communicating over the Internet
- Lower overall costs means less supplier resistance
- Lower overall costs means greater take up by suppliers
- Well established base of companies already using OFTP
- No significant investment in new software required for the existing user base of OFTP software
- Built in certificate exchange mechanism allows trading partners to exchange certificates with ease. Possible for applications to auto install these certificates

- Smart cards can be used in conjunction with the protocol to sign files and to decrypt them
- Future proof for tomorrow's file sizes
- Protocol security removes the need for hardware VPNs with their very significant associated costs and setup times

OFTP History

OFTP was first defined in 1986 by ODETTE International Ltd, a membership organisation formed by the automotive industry for the automotive industry, which sets the standards for e-Business communications and engineering data exchange. OFTP is a protocol for exchanging data in an automated environment. It addressed the electronic data interchange requirements of the European automotive industry and was initially designed to work over an X.25 network. Over the last two decades it has evolved to work over ISDN and TCP/IP networks, and is already in use by companies to send EDI data over the Internet.

OFTP is the most prolific protocol inside Europe for the exchange of EDI data, in particular in the automotive sector but is also commonly found in the retail, petrochemical, tax submissions and banking sectors amongst others. It has been proven to provide the necessary levels of file visibility and tracking, robustness and reliability required in critical Just In Time environments.

AS2 History

AS2 (Applicability Statement 2) is a recent American initiative to produce a business protocol. In America there is no common standard for the transmission of EDI data so businesses use VANs (Value Added Networks) to allow them to use a single protocol, network and point of contact for trading with many partners who may be using different protocols and different networks. AS2 was intended primarily as a way to provide a common business protocol for America and hence bypass VANs by having direct communications between trading partners over the Internet.

AS2 is an RFC which was developed by the Internet Engineering Task Force (IETF) and Cyclone Commerce Corporation. The first draft of AS2 was first produced in late 1996. It then took a further decade before finally becoming a RFC standard in July 2005.

Much of the success of AS2 has been confined to America, notably the retail sector. The major driving force behind AS2 is the American retail giant Walmart that dictated that it's 10,000 suppliers must all use AS2 to exchange EDI data with them if they wish to continue supplying Walmart.

Despite being an RFC, AS2 is politically supported and the current environment is such that only Drummond Approved solutions are generally valid. For an AS2 application to become Drummond Approved, a considerable financial investment is required which must be maintained on a yearly basis to ensure the application remains compliant with the AS2 standard.

There are commercial claims by the AS2 evangelists who say that AS2 will kill off the VANs and that AS2 is cheaper than using VANs. There are, however, other hidden costs to AS2 that are not made apparent by the marketing hype which are discussed later.

Security

Both the new OFTP2 and AS2 provide three security levels:

- Session security
- File security
- Secure authentication

Session security encrypts an entire communications session between two trading partners so that it is not possible for a third party to view the original documents being exchanged. All protocol data units

are encrypted so it is not possible to understand what protocol units are being exchanged or to examine their content.

File security provides an additional level of security by allowing a file to also be encrypted. This, in conjunction with session security, means that it is possible for a file to be securely exchanged between two companies, but for the file to remain encrypted until it reaches its ultimate destination such as a specific department or individual inside the recipient company.

The exchanged files can also be signed by the originator to prove the authenticity of the files.

Secure authentication uses X.509 certificates to authenticate two communicating entities to each other. This security prevents malicious users from connecting to an EDI server and attempting to send viruses to it or attempting to hack it. Every trading partner uses a digital certificate, similar to the concept of someone's passport, to identify themselves. The certificate proves that the holder is who they say they are, and it is up to the recipient of the communications session to accept or reject the connection based upon the credentials supplied.

File Compression

OFTP2 has been designed to handle extremely large files (in the petabytes), way beyond anything that is currently considered realistic. However large files consume bandwidth and take a very long time to send or receive, potentially causing other files to be delayed in their transmission. OFTP2 caters for this by providing file level compression which can significantly reduce the size of a file, in some cases down to as little as 10% of their original size. This is particularly relevant for companies exchanging CAD/CAM data where file sizes are in the hundreds of megabytes and take significant amounts of time to exchange using the slow X.25 and ISDN networks. Not only will the data be transferred faster but also the call duration will be shorted and hence significant cost savings can be achieved.

File Restart

One of the biggest drawbacks of AS2 is the lack of a restart capability. When sending large files, it is important to note that connections can drop. Machines have a habit of hanging when put under high traffic volumes, and the Internet is reliably unreliable. If a company is 90% through transmitting a 500Mb file when the connection drops, having spent three hours previously transmitting it, it is a waste of time and communications bandwidth to start sending the file all over again. Resending the file could potentially delay other data that needs to get through. AS2 does not support restart and so if a connection were to be dropped halfway through a communications session, the file would have to be resent from the very beginning. OFTP2 has restart built in to the protocol, so if a connection is dropped then the communication of the file restarts at a point just before the connection was dropped.

Reliability

OFTP2 is a protocol that is designed to work reliably regardless of the reliability of the underlying network. It has built in flow control, variable buffer sizes and check pointing. File restart allows transmission of a file to restart at the last known check point, so if a connection drops then the file transmission does not have to begin again from the beginning.

The performance of OFTP2 is such that it is actually possible to transfer a file via OFTP2 in less time than it takes to perform a DOS copy file command on the same file.

AS2 is fundamentally a very simple HTTP POST to a web server. There is no flow control or buffer size to be setup. The file is simply streamed in one go to the web server.

Network Support

OFTP2 works with X.25, X.25 over ISDN and TCP/IP based networks. All of the security features and compression are fully supported on all networks so companies do not need to move to the Internet to take advantage of compression, or to benefit from the new security features.

AS2 by comparison only works over a TCP/IP based network because it utilises HTTP. Companies that use ISDN connections for example would be unable to take advantage of AS2 without a costly migration plan to change their networking.

VANs

OFTP2 can be used to exchange message directly between trading partners or indirectly via a number of intermediaries, typically VANs. It makes no difference. There is special support within OFTP2 for indirect communications so that a trading partner knows when a message has reached its ultimate destination.

AS2 is not designed to work with VANs and is instead hailed as the VAN killer because it can bypass VANs. OFTP2 can also bypass VANs.

However VANs serve a very useful commercial purpose, which are very beneficial to AS2 when its deficiencies are fully realised. AS2 is limited to working over a TCP/IP based network, typically the Internet, which means that large OEMs, who have invested heavily in X.25 and ISDN networks, must ditch these in order to use AS2. OFTP2 works with X.25, ISDN and TCP/IP so companies that already have in place X.25 or ISDN can benefit from the increased security and compression options immediately without having to ditch their existing networks with the inherent migration projects and associated costs.

Permanent Internet Connections

OFTP2 is a full duplex protocol which means that it is possible for files to be exchanged in both directions regardless of which party made the connection. So A can connect to B and send files to B and also receive files from B. The result of this is that smaller suppliers can use a dialup connection to exchange files with a trading partner. The cost savings are obvious, with dialup connections costing virtually zero in today's environment. A dialup connection is not permanently connected to the Internet and so the threat from hackers is limited to the time taken for a communications session, hence firewalls and expertise are not necessarily required.

AS2 is a half duplex protocol which means that files can only be sent by the party that makes the connection. It is not possible for a trading partner A to connect to a trading partner B and receive files from B. For A to receive files from B, B must connect to A. This dictates a requirement for both A and B to have 'always on' Internet connections with static IP addresses assigned to the AS2 machines. For many small suppliers the costs of the Internet connection alone are significant. Further problems present themselves with a permanent Internet connection such as the threat from hackers which necessitates firewalls and the necessary skill sets to administer them. It also requires that the EDI machine for a small supplier, which typically sits in the corner next to a standard telephone phone line, be permanently switched on and connected to the company's network.

No Certification Costs

There are no certification costs associated with OFTP2 software, in exactly the same way that there are no certification costs required to implement FTP, SMTP, or HTTP.

AS2 is often synonymous with the words "Drummond Certification" which means that often an OEM / Hub requires that an AS2 solution is Drummond Certified. This certification costs tens of thousands of dollars each year which is expensive for software development companies and hence has a consequential impact on the cost of AS2 software and the number of solutions available. Certification is an inhibiting factor in the number of AS2 solutions available, and with AS2 now having the status of a full RFC standard there is little real requirement for interoperability testing to be required (unless

the RFC is so complicated and overly flexible that there hundreds of different permutations of options to test).

Summary

AS2 filled a gap that existed in the market for a small period of time for the secure exchange of business data. OFTP2 has leap-frogged AS2 and is superior from a technical perspective, a commercial viability perspective and from an installed user base perspective. The security features inside OFTP2 make it workable over the Internet and over existing legacy networks. Whereas AS2 has been labelled "The VAN Killer", OFTP2 can unreservedly be labelled "The AS2 Killer".

Companies which have already invested in ISDN and X.25 networks, as well as OFTP software, can now take full advantage of the Internet with next to no hardware, software or networking costs. For OEMs that already have OFTP software, the decision as to whether to continue to use OFTP2 or switch to AS2 is obvious. For suppliers, where cost is everything, then the decision to use OFTP2 rather than AS2 is also a no-brainer.