C.P.A. Secure Versus Secure FTP Servers

C.P.A. Secure is a secure file transfer and storage service product that offers many security and operational capabilities not typically found in most 'secure' ftp servers.

FIPS 140-2 Validation. Files, messages, passwords and other sensitive data handled by C.P.A. Secure technologies are protected by its built-in FIPS 140-2 validated cryptography, which has been inspected by a US and Canadian government-approved testing lab to insure that its algorithms are securely implemented, all sensitive data is securely erased, and there are no hidden "back doors". Almost no secure ftp servers include FIPS 140-2 cryptography.

Multi-Factor Authentication. C.P.A. Secure supports usernames plus one, two or three authentication factors, including passwords, SSH Public keys ("fingerprints") as well as SSL software and hardware-based client certificates and/or IP addresses/address ranges. US financial institutions face a December 2006 two-factor authentication requirement.

File Integrity Checking. C.P.A. Secure does cryptographically valid SHA1 integrity checks on each file when uploaded and downloaded. This is a requirement for providing file Non-Repudiation and Guaranteed Delivery. Many secure ftp servers still use the outdated cyclical redundancy check method (called CRC, CRC-32 or XCRC) which produces errors,
is easily subverted, and thus cannot be used for Non-Repudiation or Guaranteed Delivery.

Encrypted Storage. Every file and message uploaded to C.P.A. Secure server is securely stored, until downloaded or deleted, with its built-in, FIPS validated 256-bit key AES encryption. Encryption/decryption is done in tiny pieces so the file or message is never exposed, and each has its own separate key — which is also encrypted. Few secure ftp servers have encrypted storage, even though data in files is more vulnerable "at rest" than in transit. This means most secure ftp servers only protect data in transit, but fail to protect the data during its most vulnerable state, when stored on the server.

End-to-End Encryption. The combination of encrypted transfer and storage means that files exchanged through C.P.A. Secure will be safely encrypted from sender to recipient. Most secure ftp servers cannot provide this because they do not have encrypted storage. This means users must acquire expensive third-party encryption programs such as PGP.

OS Security Independence. In addition to encrypted storage, C.P.A. Secure has its own built-in permissions system. This combination means the safety of C.P.A. Secure settings and the files and messages that it handles, does not depend on the security (or lack thereof) of the underlying operating system of the physical servers. This OS security ndependence is in marked contrast to the OS security dependence of virtually all secure ftp servers. Hackers can exploit flaws in the OS to gain access to systems, applications and files.

No Push Vulnerability. By design, C.P.A. Secure cannot push files to other systems. Hackers can exploit push capabilities to send malware to remote file transfer servers, and into the local trusted network. Despite these vulnerabilities, a surprising number of secure ftp servers feature scriptable Move/Copy file transfer client capabilities.

Firewall Friendly. Unlike C.P.A. Secure, some secure file transfer products require that firewall ports be open from the publicly accessible DMZ into the local trusted network. Hackers can use such ports to bypass the firewall and gain entry into the local network. C.P.A. Secure's virtual interface and its 'least privilege' permissions policy also help protect the data it handles (and the privacy of its users) by providing tight administrative control over exactly what each user can and cannot see and do in terms of command options, files, messages, folders, logs, etc.

Web Browser Support. Firefox, Internet Explorer, Mozilla, Netscape, Opera and Safari can securely exchange files and messages via C.P.A. Secure, and be used to administer it. (Secure FTP SSL (FTPS), SSH2 (SFTP/SCP2) and CPA Secure HTTPS clients are also supported.)

Free Clients. CPA Secure includes the CPA Secure Wizard plugins for Web browsers. These commercially supported Java and Windows clients use firewall friendly HTTPS encrypted transport and provide

automatic SHA1 file integrity checking, transfer retry, resume of interrupted transfers, and many other features.

File Non-Repudiation. This is the ability to prove who sent and received a specific file, and that the file sent and the file received are identical (requires use of CPA Secure clients, including any of the above Web browsers with a CPA Secure Wizard plugin).

Guaranteed Delivery. This requires file transfer retry, resume and File Non-Repudiation.

Email Notification. C.P.A. Secure can alert users when files or messages arrive or have been viewed/deleted/downloaded — or not. C.P.A. Secure will also alert administrators about important system and user events, including password expirations, lockouts, etc.

Comprehensive Audit Trail. Based on secure user, file, message, Web form posting, and administrative action records in the ODBC accessible database in C.P.A. Secure.

Extensive Reporting. C.P.A. Secure includes over 90 pre-defined, customizable reports. Data can also be automatically extracted and exported in CSV, fixed-width, and XML file formats for use by a variety of third-party reporting and billing/tracking applications.

User Interface Language Options. Enables users to select English, French or Spanish versions of the C.P.A. Secure Web user interfaces.