COVIANT Software

DATA SHEET
DIPLOMAT MANAGED FILE TRANSFER
BASIC EDITION

DIPLOMAT® MANAGED FILE TRANSFER
BASIC EDITION

OVERVIEW

Diplomat Managed File Transfer Basic Edition manages secure file transfers to and from your trading partners, including PGP encryption and decryption, without significant IT investments or extensive training.

Organizations today share data with a variety of service providers, vendors, trading partners, customers, regulatory agencies, remote offices, and more. Sensitive data – such as payroll information, human resources benefits, and corporate financials – are transferred to and from entities around the world billions of times each day.

Companies understand the need to protect this data. Security policies requiring encryption are commonplace. And, companies must not only meet their own requirements but the requirements of their trading partners for secure, reliable file transfers.

FAST SET-UP

No one has time to learn new tools. You need to focus on your business – rather than worry about batch scripts or job scheduler syntax. Using Diplomat's intuitive user interface requires no special skills to set up secure file transfer jobs.

You can schedule file transfer jobs and set file transfer parameters using checkboxes and fill-in-the-blank fields. You can control all aspects of a file transfer job, such as which encryption or signature key to use, FTP login data, the location of files to be picked up, whether to delete source files after the transfer, or whether to overwrite existing files.

JOB AUTOMATION

You can use Diplomat's built-in scheduler to run your file transfer jobs with no manual intervention. You can schedule jobs to run in intervals of months, days, hours, or minutes. You can have confidence that file transfers will occur as planned. And, with no manual intervention, you get fewer file transfer errors. In addition to scheduled jobs, you can execute file transfer jobs immediately using Diplomat's *Run Now* feature.

DATA SECURITY

You need to protect your data and your partners' data at all times – in transit and at rest. Diplomat supports OpenPGP encryption and secure file transfer technologies. OpenPGP encryption lets you protect files at rest both inside and outside the firewall. Using secure FTP ensures that FTP login information and data files in transit are protected with your choice of SSH or TLS/SSL encryption.

Other sensitive file transfer job set-up data, such as pass-phrases, passwords, and account logins, need to be protected. Diplomat ensures internal application security by encrypting sensitive job set-up data before storage in a centralized Diplomat database. No more batch files or registry entries with unprotected data.

And, Diplomat uses secure SSL connections for all communication between the Diplomat client and server. No unprotected information is sent over your internal network.

FEWER FAILURES

Successful file transfers rely on your internal network, internet connection, and the source and destination sites being available. A small 'glitch' in any of these systems can cause file transfers to fail.

File transfer failures are usually prevented when using Diplomat Managed File Transfer. When a transient error occurs, like a dropped FTP session, Diplomat automatically attempts to recover and complete the transfer. Most transient file transfer problems are corrected such that a file transfer job succeeds on its first run.

REMOTE SITE MANAGEMENT

Diplomat Basic Edition is easy to deploy at remote offices or other sites that need data encryption and secure file transfer capability. Since all communications between the Diplomat client and server are protected with SSL, you can securely set up file transfer jobs to run from a remote site without leaving your office.

Diplomat makes single-file back-ups of its internal database that can be restored with one-click on any other system running Diplomat. You can set up file transfer jobs with your local copy of Diplomat Basic Edition and restore it at a remote location.

PROBLEM RESOLUTION

When attempting to transfer files, unexpected problems can crop up. You might have outdated FTP account login information. Files might not be ready for pickup. The wrong key may have been used to encrypt a file, so you cannot decrypt it. With Diplomat, these file transfer problems don't become business problems. Your files arrive on time and ready to use.

Diplomat logs all file transfer set-up and run-time events to a log file. Diplomat's built-in log viewer makes it easy to locate the log records you need to diagnose a problem. You can select only the log records associated with a particular file transfer job or search the file for records containing a specific phrase.

Diplomat makes it easy to know when file transfer set-up data has been changed. Diplomat's log file captures comprehensive user activity, such as user ID and IP address, for each update to the Diplomat database. And, each screen in Diplomat displays a timestamp, user ID, and IP address that reflect the last time any data on the screen was modified.

DATA RECOVERY

Sometimes you may need to resend a file because a business partner deleted the file before it was processed. Diplomat automatically archives each file you send or receive for 30 days. You have a copy on hand for your own records or to resend to a partner. And, after 30 days, Diplomat automatically deletes the archived files, so no manual clean-up is required.

INTEROPERABILITY

Your secure file transfer solution needs to interoperate seamlessly with your partners' current applications. Diplomat works with existing technologies by using industry standards, such as OpenPGP and secure FTP. Your business partners can continue to use the encryption and file transfer products they have in place. And, if you already have OpenPGP keys, they can be imported into the Diplomat database for use whenever OpenPGP encryption is needed.

OPENPGP MANAGEMENT CONSOLE

You don't need to replace pre-existing PGP command line encryption tools to get the other benefits of Diplomat Managed File Transfer. Diplomat includes a management console that lets owners of OpenPGP command line products (such as PGP® Command Line Server or McAfee® E-Business Server) continue to use these tools when performing file encryption or decryption tasks as part of a Diplomat file transfer job. You no longer need to spend time and resources developing and maintaining batch scripts for your PGP command line tools.

TECHNICAL SPECIFICATIONS

PLATFORM SUPPORT

DIPLOMAT SERVER

- Windows XP SP3 (32-bit)
- Windows 7 (32-bit, 64-bit)
- Windows Server 2003 R2 (32-bit)
- Windows Server 2008 R2 (64-bit)
- Red Hat Linux (32-bit, 64-bit; x86)

DIPLOMAT CLIENT

- Windows XP SP3 (32-bit)
- Windows 7 (32-bit, 64-bit)
- Windows Server 2003 R2 (32-bit)
- Windows Server 2008 R2 (64-bit)

FILE TRANSFER SUPPORT

FTP

- FTP (RFC 959)
- FTPS (RFC 2228 with Secure FTP Using TLS)
- SFTP (RFC 4253)

OPENPGP ENCRYPTION SUPPORT

SYMMETRIC ALGORITHMS

- AES (up to 256-bit keys)
- Blowfish (up to 448-bit keys)[1]
- CAST5 (RFC2144)
- DES (56-bit keys)[1]
- IDEA (128-bit keys)[1]
- Safer (128-bit keys)[1]
- Triple DES (56-bit keys)[1]
- Twofish (up to 256-bit keys)[1]

ASYMMETRIC ALGORITHMS

- RSA (up to 4096-bit keys)
- DSA (1024-bit key only)
- El Gamal (up to 4096-bit keys)

HASHES

- SHA-256[1], SHA-384[1], SHA-512[1], SHA-24[1], SHA-1
- MD2[1], MD5[1]
- RIPEMD-160[1]

[1] Only supports decrypting existing messages encrypted with algorithm or encrypting to existing keys specifying algorithm as preferred cipher.

OPENPGP PRODUCT INTEROPERABILITY (RFC2440/4880)

- Authora Edge v3.6
- McAfee E-business Server v8.0 - v8.5.2
- PGP Command Line v9.0 - v10.0
- Veridis FileCrypt v3.6
- Any other RFC 2440 or RFC 4880 compliant product

ABOUT COVIANT SOFTWARE

Coviant® Software delivers file transfer management products that secure data in transit and improve compliance with industry and government mandates. Built on open technologies, such as OpenPGP encryption, secure FTP and SQL, Coviant's Diplomat® Transaction Manager suite is an easy to implement, cost-effective solution for automating your secure file transfer process.

COVIANT Software
ASSURED FILE DELIVERY

209 West Central Street / Suite 204 / Natick, MA 01760
781.210.3310 T / 781.210.3313 F / www.coviantsoftware.com