FileAssurity OpenPGP

Encrypt and digitally sign your files, folders, documents, instant messages and emails. Securely delete them beyond US DOD standards. Communicate securely with PGP v5.x+ or any other OpenPGP user.

Protecting Files

Unlike products that use weak password mechanisms to protect your information (easily broken with freely available password crackers on the Internet), FileAssurity uses full strength PKI technology. Your files are encrypted using Government strength industry standard algorithms and your personal protection keys never leave your computer.

Any type of file can be encrypted and/or digitally signed, regardless of its file extension. Encrypting files ensures only the intended recipient can view them. Digitally signing files ensures the recipient knows that they have come from you and have not been tampered with. Files can be encrypted for individuals, multiple recipients or groups.

Secure E-Mails & Instant Messages

Send e-mails and instant messages securely regardless of the messaging client you or your recipients are using. Encrypt, digitally sign and send message text and attachments securely in one simple process. Your default messaging application is automatically opened with the secured files attached and the email address already filled in. For secure message text you can create or paste text into the **Secure Text Editor** and FileAssurity will automatically secure it.

FileAssurity is not integrated tightly into email or instant messaging applications in order to prevent vulnerabilities in the messaging software compromising the security of the system. Your data is never at risk.

Secure File Deletion

FileAssurity securely deletes files beyond the US Government DOD 5220.22-M standard in one easy step using three times the specified number of overwrites. Additional measures prevent even the most dedicated file recovery programs recovering your sensitive documents and files. Just right-click on selected files and folders to securely delete them.

Secure Archives

FileAssurity lets you encrypt multiple files and folders in an archive file using the zip standard for compression. This is a secure alternative to using zip files and provides easy management of your files and folders.

Low cost simple to use alternative to PGP

FileAssurity costs a quarter of the price of PGP and competitor products yet provides strong protection and is much simpler to use. You can generate your own keys just like PGP or import them from the majority of Certificate Authorities. FileAssurity lets you generate, import and export X.509 and PGP keys and encrypt/decrypt, sign/verify OpenPGP compatible files.

There are no algorithms to choose or complex decisions to make. FileAssurity automatically uses the US Government approved algorithm AES at it's greatest strength (256 bit) or for communication with PGP v5.x and v6.x users it uses TDES (192 bit). No user involvement is required.

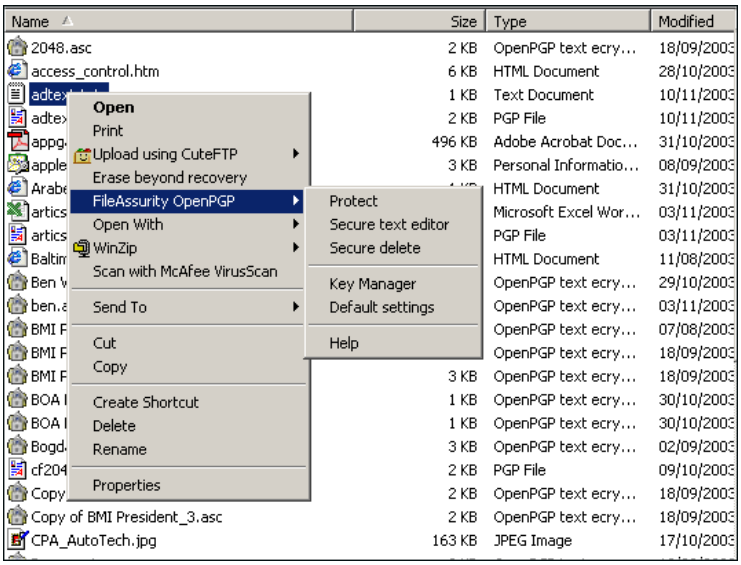

Diagram 1 : Menu options in Windows Explorer and protection options (below)

Simple to use

FileAssurity is incredibly simple to use. Select your files in Windows Explorer, choose who you want to encrypt them for, whether you want to digitally sign them and press the "Protect" button. You can encrypt files, archive files, send files securely via email and create secure message text in one simple operation.

Quick key emailing, quick key recognition, group support for easier encryption management and many other usability features ensures storing, sending and receiving files is a breeze for even the most novice of users. The complexities associated with encryption are now a thing of the past.

ARTICSOFT

FileAssurity OpenPGP

Key Generation & Management
FileAssurity's in-built key manager lets you generate your own X.509 and OpenPGP compliant certificates and keys, or you can import them from any Certificate Authority (VeriSign, GeoTrust, etc.) or OpenPGP compliant product. It's backup and restore facility and password changer ensure you have full control over the management of your keys. For the more technically minded, advanced key information is just a single click away.

In addition, FileAssurity automatically recognizes keys signed by all the major Certificate Authorities. It's unique Trusted Authorities system shields you from the complexities of importing Root Certificates in order to verify keys. Notes can be added to every key you generate or import to help you identify keys or to store additional information that you want associated with them.

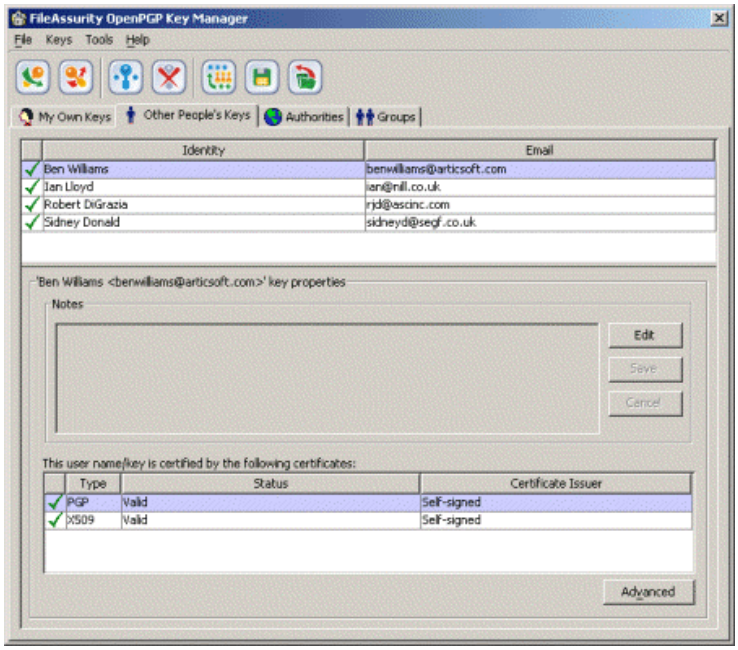

Diagram 2 : FileAssurity OpenPGP Key Manager

FREE Decryption & Verification software
Other people do not have to purchase FileAssurity in order to verify and decrypt the files and secure text you send them – they can do this for FREE by downloading FileAssurity OpenPGP Reader from the ArticSoft web site.

Our free reader software lets recipients generate, import, export and manage their keys and is much more secure than password protected EXE files.

Features & Benefits

- Encrypt and Digitally Sign any type of file – ensuring full confidentiality, accountability & integrity
- Secure storage and sending of files, folders, archives
- Send e-mails and instant messages securely (both message text and attachments)
- Securely delete files, documents & folders beyond recovery above US DOD standards
- Secure zip archives – easy management of files/folders
- Built in key generation & key / certificate manager – no need to purchase any other software
- Group support for easy encryption management
- Full integration with Windows Explorer
- Automatic space saving compression for every file
- Free Reader software - file decryption/verification
- Simple to use, low cost, Government strength

Available Options

Command line scripting support. Control FileAssurity from the command line and let it automatically encrypt, sign, decrypt, verify, securely delete and email files without any user intervention. Specify the date and time when actions should occur and what folders/files to work on. Audit reports.

Central Key Management. Deploy FileAssurity from a central location. Determine the keystores users will have and where they are located. Specify policy rules (what users can do), perform remote password recovery, key recovery + more.

Technical Information	
Signing Algorithm	RSA (2048 bit), DH/DSS (2048/1024 bit)
Hashing Algorithm	SHA-1 (160 bit), MD5 supported
Encryption Algorithm	AES (256 bit) – FIPS 197 CAST, TDES and Twofish supported
Platforms supported	Windows 95, 98, ME, NT, 2000, XP
Client requirements	PII Processor, 128MB RAM, 42MB disk space
File and Certificate formats supported	.P7B (PKCS#7), .CER, .P12 (PKCS#12), .PFX, .ASC, .PGP, .GPG, X.509, .SKR, .PKR
OpenPGP compatibility	FileAssurity works with all OpenPGP compliant products including PGP v5 + and uses the IETF OpenPGP standard (RFC 2440)
Other options	Unix/Linux/MAC & Token support available on request

ARTICSOFT