SecureAge

SecureFile

Digital Signing & DRM

What is SecureFile?

SecureFile is a comprehensive document security solution that secures mission critical files through powerful encryption using the 256-bit AES (Advanced Encryption Standard) algorithm and persistent digital signatures.

Confidentiality
Keep mission critical files secure in any location and inaccessible to unauthorized parties
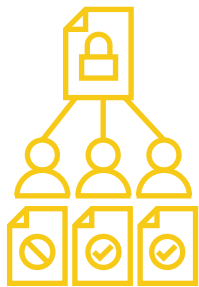
Integrity
Ensure mission critical files are sent as intended and free from unauthorized modification

Authentication
Be assured of the identity of the source of the file with non-repudiable digital signing

Encryption with Sharing in Mind

Designed to protect files from unauthorized use through powerful encryption in just a few clicks, SecureFile also makes possible the sharing of files among multiple authorized users, both internal and external, through standard PKI technology.

Storage Security with Self-Encrypt & WipeFile

For easily storing mission critical files without leaving any plain data residue, SecureFile allows users to self-encrypt files while permanently erasing all traces of the original ones. Once wiped, those plain files are beyond recovery, even with the use of sophisticated file restoration techniques.
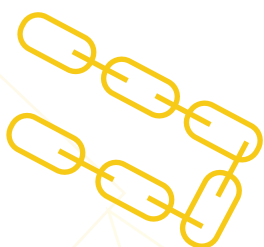
Non-Repudiation with Chain Signing

Digital signatures in SecureFile not only maintain data integrity and allow for reliable authentication, but also provide non-repudiation. It goes even further by allowing multiple authorized users sign a file with chain signing. This offers an essential component for secure approval process workflows within organizations.

Get Any File Encrypted in Just a Few Clicks

SecureFile is intuitively integrated to allow users to encrypt any file, anywhere on your system in as few as two clicks* while also reaping the following benefits in the process:
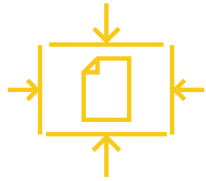
File Compression

Air-Tight Encryption & Signing

Sharing or Wiping of Plain File

* Additional clicks required to select authorized users for sharing use-cases.

Develop Custom Secure Applications With Built-In File Encryption & Signing

The SecureAge COM (Component Object Model) API is a set of application programming interfaces that allow developers to access the SecureAge platform and add PKI-based security functionality within their own applications.

How Does It Work?

It is based on Windows COM interface to allow development through any programming language (i.e. Visual Basic or C++) that can interface with it.

This lets developers easily implement the file encryption and digital signing security features of SecureFile on other enterprise applications with very little development time and effort.

How are User Keys & Certificates Managed?

User keys and certificates are managed within the certificate store of the main SecureAge client software.

Developers can create an application that calls the API to perform an LDAP search for a user's certificate, to download the required certificate not found in the certificate store, and to validate it.
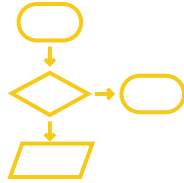
Key SecureFile Features

SecureFile is packed with features to safely secure your files from any unauthorized access without compromising usability.
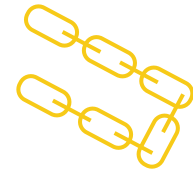
Public & Private Key Encryption/ Decryption
Supports 256-bit AES file encryption algorithms with unlimited key-length RSA digital signature

Customizable Algorithms
Allows integration of user-defined file encryption algorithms to further boost data security

Chain Signing Support
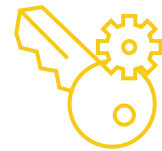Provides chain-signing for secure document workflow control in organizations

WipeFile
Ensures confidential files in plain are permanently erased and unrecoverable once encrypted

Certificate Management
Supports Standard X509 certificates and local caching of peer certificates for enhanced performance
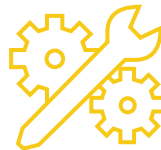
Key Management
Support for standard file encryption algorithms such as AES, triple-DES, RSA, ECDSA, ECDH, MD5, SHA-1, & SHA-2

Two-Factor Authentication
Seamless integration with PKI smart cards and USB tokens

SecureAge COM API
Scalable API for building secure applications with encryption and signing

Need More Information?

www.secureage.com   Contact us