Your Trusted Solution in Document Security

SecureAge

SecureAge SecureFile

SecureAge SecureFile is a powerful, PKI-based document security solution that secures mission-critical files with its encryption and digital signing capabilities. It protects file from unwanted tampering and interception, thereby, ensuring its privacy, integrity and authenticity. It is an ideal solution for the government, banking, legal or procurement sector where digital signing and verification of confidential electronic document is part of a crucial decision-making and approval process. It also supports a programmatic module, SecureAge COM API which allows developers to easily and seamlessly integrate SecureAge SecureFile into their existing applications.

How does SecureAge SecureFile work?

1. Encryption

SecureAge SecureFile allows users to encrypt or self-encrypt sensitive documents with 256-bit AES (Advanced Encryption Standard) in just a few simple clicks. When encrypting or self-encrypting a file, the content of the file is first compressed to reduce storage space and then scrambled using the user's encryption key. Any intruder, without the proper decryption key, is unable to access and decipher the content of the encrypted files. With PKI technology support, the file can be encrypted for any selected group of users using their corresponding public keys. The sensitive document can then be securely shared with colleagues, partners, customers and other parties.

2. Digital Signature

A digital signature is recognized as a digital equivalent of handwritten signature in many countries and it cannot be forged. It authenticates a user's identity so that no one can tamper with the digitally signed document. With SecureAge SecureFIle, a user can establish his/her identity by putting his/her digital signature in any electronic document. The recipient will then be able to verify the validity of the signature with the sender's digital certificate which is also embedded in the signed document.

3. Encryption and Digital Signature

In many cases, the user would like to both sign and encrypt their document. In this case, the document is first signed and then encrypt with his/her preferred recipient's encryption key. The authorized recipient willthen be able to use his/her corresponding decryption key to decrypt the document and to verify the validity of the sender's signature. This not only authenticates the sender's identity but also ensure that only the intended recipient is privy to the content of the document.

4. Chain-signing Capability

SecureAge SecureFile supports chain-signing capability to secure document work flow control in a decision-making and approval process. More than one authorized user can add his/her unique digital signature to the confidential document as an authenticated proof that he/she had viewed and approve the document. This is to prevent non-repudiation, whereby any of the signers cannot deny having approved the document.

5. Wipe File

Wipe File, another feature of SecureAge SecureFile, allows a user to completely and permanently erase those confidential documents without leaving any trace in the computer hard disk. There is no way anyone can recover these files from the hard disk even when using very sophisticated data recovery techniques.

6. SecureAge COM API

SecureAge COM (Component Object Model) API is a set of application programming interfaces (APIs) built on top of SecureAge platform. It provides full PKI functionalities for data security as well as full key and certificate management for the users. It allows developer to access SecureAge platform directly, add PKI-based security to their application and embed SecureAge services into their own applications seamlessly. This greatly reduces a developer's development and programming effort.

SecureAge COM API provides a comprehensive set of data protection utility. Developers can use this utility to either add security features or build and create their own applications on SecureAge platform easily, seamlessly and hassle-free.

- How does SecureAge COM API work?

SecureAge COM API is based on Windows COM interface. Hence, the application calling the APIs can be developed in any programming language (like Visual Basic or C++) that can interface with COM. For example, developers can develop the application that calls the data security APIs to add security to the application data. The security configurations can be set based on a company's policy and requirements, eg. data is signed and/or encrypted before storage, signing and/or encryption is performed at file-level on the file system and so on.

- How are user' keys and certificate managed?

The user's key and certificates are managed within the certificate store of SecureAge Client Software. Developers can develop an application that calls the API to perform an LDAP search for a user's certificate, download the required certificate not found in the certificate store the validity of the certificate.

Figure 1: Encrypted files with .sfm extension

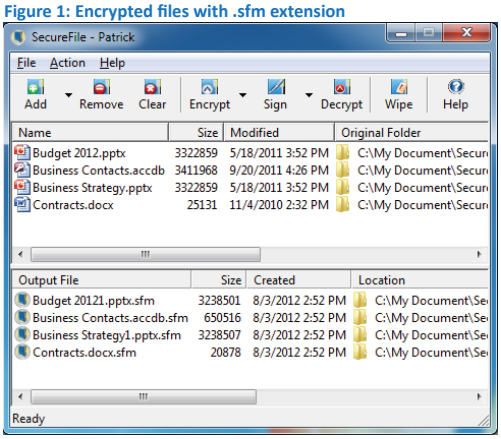
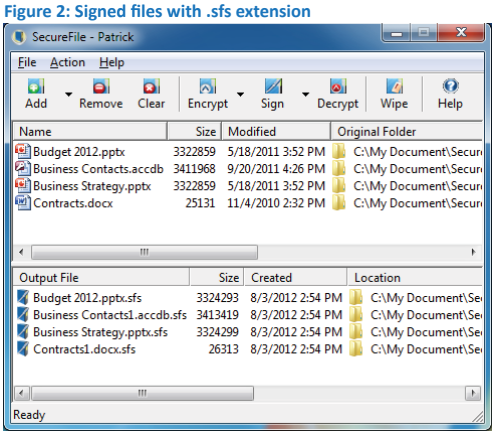


Figure 2: Signed files with .sfs extension



Key Features

1. SecureAge COM API

- Provides a scalable API for building secure applications.

2. Data Security

- Data security functions are provided in memory and on files.
- Data hash checking and verification.
- Public/private key encryption/decryption.
- Supports 256-bit AES encryption algorithms, with unlimited key-length RSA digital signature.
- Allows integration of user-defined encryption algorithms to further boost data security.
- Provides digital signature that allows signing and encrypting of any type of desktop document like text file, image file and binary file.
- Provides chain-signing for secure document work flow control.
- Provides Wipe File capability to ensure that confidential files are permanently erased from the computer hard disk and can never be recovered.

3. Built-in Key and Certificate Management

- Provides Key Management and supports wide range of standard algorithms including AES, triple-DES, RSA, ECDSA, ECDH, MD5, SHA-1, SHA-2, etc.
- Support standard X509 certificates.
- Local caching of peer certificates for performance enhancement.

4. Two-factor Authentication

- Provides two-factor authentication and seamless integration with PKI smart cards and USB tokens.

Need More Information?

Sales: biz@secureage.com
Public Relations / Marketing: pr@secureage.com
General Enquiry: contactus@secureage.com
Technical Support: support@secureage.com

www.secureage.com
www.lockcube.com

Asia Pacific
SecureAge Technology Pte Ltd
3, Fusionopolis Way
#05-21, Symbiosis
Singapore 138633

Japan
SecureAge K.K.
Barbizon 18, 7F
5-18-18 Shirokanedai
Minato-ku, Tokyo 108-0071
Japan

North America
SecureAge Technology Inc
3 Twin Dolphin Drive Suite 150
Redwood City CA 94065
U.S.A.