# SECRETAGENT®

## *Data Protection*

**SecretAgent is unsurpassed at ensuring the confidentiality, integrity, and authenticity of data at rest and data in transit. When security matters, SecretAgent is the only choice.**

**Information Security** CORPORATION

**+1-847-405-0500**

sales@infoseccorp.com
**www.infoseccorp.com**

in  infoseccorp

🐦  @infoseccorp

f  /infsec.us

## Overview

SecretAgent is the world's leading file encryption and digital signature utility. Interoperable across a wide range of platforms (Windows, Linux, OS X, and most other UNIX-like systems) and with a variety of interfaces (app, command line, and API), it's the perfect solution for your data at rest or data in transit security requirements, regardless of the size of your organization.

Administrators find SecretAgent easy to pre-configure, deploy, and support. In most cases users have zero configuration tasks.

## Secure Collaboration

File security is paramount, but the ability to safely and easily work with the files is also important. SecretAgent's secure collaboration framework ensures confidentiality while supporting cooperative work flows:

- vault ACLs persist across editing sessions
- vaults opened for editing are viewable, but locked against modification, by others
- vault status and sensitivity level are presented graphically for ease of recognition
- DAS adds support for ACLs containing community of interest and role-based certificates

### SecretAgent Benefits

- Supports 'in-place' editing of encrypted documents
- Works with all applications and file systems
- Supports secure file exchange between all supported operating systems
- May be easily deployed and centrally managed
- Appropriate for organizations of any size, scaling up to millions of users
- Uses NIST CMVP-validated FIPS 140-2 cryptography and proven security standards, including ANSI X.509 and IETF PKIX, TLS, and S/MIME

⊞ Windows

FIPS VALIDATED 140-2 ™
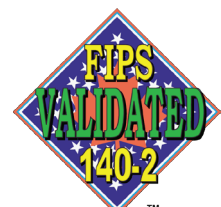
# SECRETAGENT®

## *Data Protection*

## Use Cases for SecretAgent

### Protecting Data at Rest and Data in Transit

Secures sensitive files with strong encryption, on desktops, laptops, network attached storage, and backup media and enables secure B2B information exchange by providing end-to-end encryption (E2EE) of files sent via e-mail, FTP, web, removable media, or any other means for internal or external users

### Safeguarding Data in the Cloud

Provides end-to-end encryption (E2EE) of files shared on Dropbox, Google Drive, Microsoft OneDrive, Slack, and other file sharing services

### Achieving Compliance

Helps meet data privacy compliance regulations such as HIPAA, PCI, and GDPR

### Signing Documents

Digitally signs files of any type with or without encryption

### Securely Erasing Data

Deletes files securely and wipes free space in compliance with NIST SP800-88

## TECHNICAL SPECIFICATIONS

| | |
|---|---|
| Bulk Encryption | 128/192/256-bit AES-CBC (FIPS 197) |
| | TDES/DES-CBC (FIPS 46-3; decrypt-only for backwards compatibility) |
| | 128/192/256-bit AES-CTR (FIPS 197; password-based archives only) |
| Key Exchange | RSA (up to 16384-bit keys; FIPS 186-4; ANSI X9.31) |
| | ECDH (233/283/409/571-bit NIST curves in char. 2, 256/384/521-bit NIST curves in char. p; NIST SP800-56A; ANSI X9.63; IEEE 1363) |
| Digital Signature | RSA (up to 16384-bit keys; FIPS 186-4; ANSI X9.31; RFC 3447/PKCS#1 v.2.1) |
| | ECDSA (NIST curves up to 571-bits in char. 2, 521-bits in char. p; FIPS 186-4; ANSI X9.62; IEEE 1363) |
| Message Authentication | SHA-1 (FIPS 180-4; ANSI X9.30) |
| | SHA-2 (FIPS 180-4) |
| Compression & Encoding | LZSS compression and base64-encoding (both optional) |
| DBRG | NIST SP800-90A HMAC DRBG SHA2-256 (256-bit) |
| Hardware Support | Supported APIs: PKCS#11, Microsoft CAPI, Microsoft CNG |
| | Supported Tokens: DOD CAC, PIV, other smart cards, USB tokens, hardware security modules and biometric devices |
| Secure Erasure | NIST SP800-88 Clear |

## SUPPORTED PLATFORMS

- Windows 7, 8, 8.1, 10, or above (x64)
- Apple OS X 10.10 or higher (x64)
- CentOS 6.7 (Linux Kernel 2.6.32-573) or above (x64)

## EXPORT INFORMATION

SecretAgent may be freely exported to all but a handful of embargoed countries and denied parties under License Exception ENC:

ECCN 5D002; CCATS: G016161

## Information Security CORPORATION