

SecretAgent®

SecretAgent is unsurpassed at ensuring the confidentiality, integrity, and authenticity of sensitive data at-rest and in-transit. Security-conscious government agencies and corporations worldwide rely on SecretAgent to assure that their mission-critical information remains confidential and compartmentalized.

When security matters, SecretAgent is your best choice.

OVERVIEW

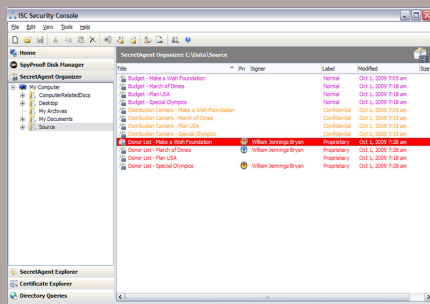
SecretAgent is an encryption program that protects your most sensitive data. It can encrypt and/or digitally sign **any** file or folder stored on your hard drive, removable media, or shared network drive.

A SecretAgent archive is an envelope of encryption and integrity that prevents attackers, Trojans, viruses, and file sharing tools from accessing sensitive plaintext on your computer system or network. Since SecretAgent encrypts at the file level rather than on a specific device, data remains encrypted even when copied to removable media or when transmitted via e-mail.

ARCHIVE CREATION AND ACLS

Archive creation is much like composing an e-mail message: specify the files you wish to encrypt and a list of users who may open (*i.e.*, decrypt) the archive once it is created.

Granting decryption access to other users is simply a matter of adding their certificates (or mutually agreed-upon passwords, if certificates are not available) to an access control list (ACL) embedded in the archive. Archive ACLs may be editing at any time to grant or deny access to specific users or 'communities of interest'.



SIMPLY SECURE

Fully-transparent encryption systems allow all running applications to access everything once the user is logged in. This puts the user's sensitive data at great risk of compromise. SecretAgent, however, takes a more secure, 'semi-transparent' approach: it requires users to grant access to specific files as they work with them, while encrypted archives not in-use remain protected. While still making it effortless for authorized users to access their files.

SecretAgent archives are easily identifiable by their unique icon, and each archive is assigned a color-coded security label allowing users to readily determine document sensitivity. Users are never confused about whether a particular file is protected or its relative value to the organization. Since archives are never transparently decrypted accidental data disclosure is highly unlikely.

SECURE COLLABORATION

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

- archive ACLs persist across editing sessions
- archives opened for editing are viewable, but locked against modification, by others
- archive status and sensitivity level are presented graphically for ease of recognition
- DAS add-on supports ACLs containing community of interest and role-based certificates

STANDARDS-BASED PKI

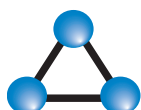
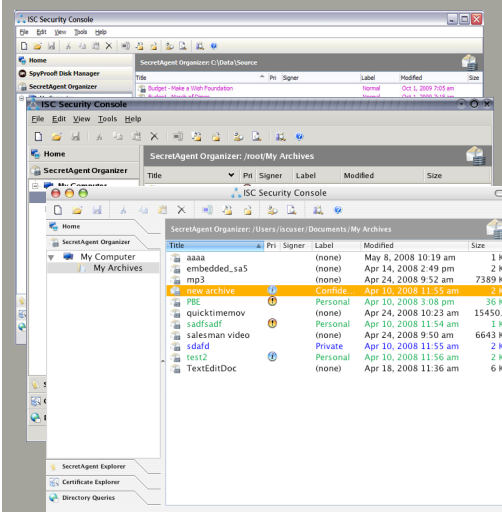
SecretAgent uses X.509 certificates for encryption and access control. The X.509 public key infrastructure (PKI) specification is the most widely-used standard technology for providing access control, authentication, and encryption. It is the basis of trust and security on the Internet and is used to secure e-mail (S/MIME) and web transactions (TLS).

EASE OF ADMINISTRATION

Administrators find SecretAgent easy to pre-configure, install, and support. In many cases users have no configuration tasks to perform themselves.

PLATFORM NEUTRALITY

SecretAgent's design and functionality allows it to perform identically on Windows, OS X, Linux, and Solaris. Maximum performance is achieved using multi-threaded, native, not interpreted, code.



Information Security
CORPORATION

+1 847 405-0500
sales@infosecorp.com
http://www.infosecorp.com

SecretAgent®

Additional Features

- **archive search:** find all archives that contain a specific search term in the header, filename, or inside the archive
- **data erasure:** securely delete files and wipe free space in compliance with US Department of Defense sanitization requirements
- **digital signatures:** digitally sign files while encrypting or create signed only archives
- **data labeling:** assign archives a color coded security label and priority
- **auditing:** system wide and per archive audit trails provide complete information for administrative and forensic purposes
- **key rollover:** automatically employs the user's prior credentials to decrypt archives created in the past
- **data recovery:** supports administrative private key password or per-archive symmetric key recovery; specify one or more recovery certificates in PolicyAgent
- **server-mediated private key operations:** with ISC's Document Access Servlet, available separately, users can encrypt files for frequently changing communities of interest or use SecretAgent in a role-based manner
- **NSA Suite B:** NSA Suite B algorithms for digital signatures, key wrapping, and integrity are supported
- **file formats:** supports native SA5/SA6, SA6 password-protected, and S/MIME CMS (RFC5652) files; SA5 auto-encrypted files (.saa; decrypt-only)
- **scalability:** no central servers required; a distributed configuration policy scheme scales to millions of users while providing centralized control
- **simple certificate distribution:** included LDAP and Active Directory support allows individual certificates or groups of certificates to be retrieved from a remote repository; directory queries may be pre-configured by an administrator
- **centralized policy management:** administrative editions include PolicyAgent which generates digitally signed configuration policies that ensure SecretAgent conforms to organizational guidelines.
- **extensibility:** applications or scripts may leverage SecretAgent's capabilities by utilizing the same extensibility API that ISC uses for the Microsoft Office application macros, Windows Explorer integration, and e-mail plug-ins for Microsoft Outlook and Lotus Notes

PKI Support

- **certifications and standards:** certified by DISA's JITC PKE Lab as interoperable with the U.S Department of Defense PKI. Interoperable with the U.S. Intelligence Community PKI. Internal Path validation module passes the stringent NIST PKITS Certificate Path Validation Test and is "(Federal) Bridge-Enabled."
- **certificate authorities:** functions with any X.509 Certificate Authority. Additional functionality is available when used with ISC's CertAgent, Entrust's Authority, or Microsoft's CA
- **PKI tools:** includes private key, certificate, and CRL management components with integrated certificate and private key storage
- enforces standard IETF PKIX certificate extensions, including keyUsage, basic constraints, and policy constraints
- imports X.509 version 3 certificates from binary, PEM- or base64-encoded ASN.1 DER, PKCS#7 and PKCS#12 files
- generates self-signed RSA, DSA, and ECC certificates for use without a formal PKI
- **private keys:** utilizes Microsoft CAPI/CNG, PKCS #11, Entrust, or its own integrated key store (either on your PC, or on your Windows Mobile device) for private key operations

Regulatory Compliance

- utilizes ISC's CDK, a FIPS 140-2 compliant (#347) cryptographic module, for all cryptographic operations except for private key operations performed when used with smart cards or third-party private key stores
- satisfies NSTISSP 11, OMB, and GSA acquisition requirements for COTS security and information assurance products
- available through the DAR ESI BPA and GSA SmartBuy programs
- complies with Section 508 of the ADA
- meets HIPAA requirements for securing sensitive medical information

Export Information

SecretAgent is freely exportable to all but a handful of embargoed countries and denied parties under unrestricted License Exception ENC. ECCN: 5D002; CCATS: G016161.

Technical Specifications

Bulk Encryption Algorithms	128/192/256-bit AES-CBC (FIPS 197) TDES/DES-CBC (FIPS 46-3/81; decrypt-only for backwards compatibility) 128-bit AES-CTR (FIPS 197; password-based archives only)
Key Exchange Mechanisms	RSA (up to 16384-bit keys; ANSI X9.31; IEEE 1363; RFC2313) Diffie-Hellman (up to 4096-bit keys; ANSI X9.42-1998; IEEE P1363) ECDH (163/233/ 283/409/571-bit NIST curves in char. 2, 192/224/256/384/521-bit NIST curves in char. p; FIPS 186-3; ANSI X9.42-1998; IEEE P1363)
Digital Signature Schemes	DSA (up to 4096-bit keys; FIPS 186-3; ANSI X9.30-1997) RSA (up to 16384-bit keys; ANSI X9.31-1998; PKCS#1 v.1.5) ECDSA (NIST curves up to 571-bits in char. 2, 521-bits in char. p; FIPS 186-3; ANSI X9.42-1998; IEEE 1363)
Message Authentication Codes	SHA-1 (FIPS 180-3; ANSI X9.30-1997) SHA-2 (FIPS 180-3; for certificate path validation and CMS signature verification only) MD2 and MD5 (RFC1319/RFC1321; only for certificate path validation)
Compression & Encoding Options	LZSS compression and base64-encoding (both optional)
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 Delete Mechanism	Conforms to DoD 5220.22-M, Section 8-306 method d
Platform Support (GUI and CLI)	Microsoft Windows 2000, XP, 2003, 2008, Vista, 7 (x86, x64) Microsoft Windows Mobile (ARM) Macintosh OS X 10.4 or higher (Universal) Sun Solaris 8 or higher (SPARC, x86) RedHat, CentOS, Ubuntu, and SUSE Linux Kernel 2.6 (x86, x64, IA64)
Platform Support (CLI only)	HP-UX 11.x (PA-RISC, IA64), HP Tru64 (Alpha), HP OpenVMS/AXP, IBM AIX 4.3 or higher, Cray T3E/C90/T90