SecretAgent®/TE

Data Protection

SecretAgent/TE is an add-on to SecretAgent that supports the automatic, on-the-fly encryption and decryption of files without direct user intervention.

Overview

File encryption applications often require the user to manually select sensitive files, click encrypt, select or enter a list of recipients (an ACL), and then click save. This process, requiring the user to be conscious of the encryption process, is error prone and can disrupt the user's normal workflow.

SecretAgent/TE protects sensitive files transparently using preconfigured rules. With SA/TE, encryption just happens, without relying on user interaction.

Rule-Based Encryption

SecretAgent/TE supports rules that trigger encryption based on:

- a file's type (*i.e.,* its file extension)
- a file's location
- the application creating or accessing the file
- keywords or phrases appearing in the file

Each rule specifies the ACL to be applied to its matching files. Sets of rules may be established and managed centrally by one or more administrators and, if permitted, locally by individual users.

Information Security Corporation
+1-847-405-0500
sales@infoseccorp.com
www.infoseccorp.com
infoseccorp
@infoseccorp
/infsec.us

SecretAgent/TE Benefits

- Protects files automatically without user intervention
- Works with all applications and network file systems
- Supports secure file exchange between Windows and Linux
- May be easily deployed with preconfigured rules and then 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®/TE

Data Protection

Use Cases for SecretAgent/TE

Safeguarding Data at Rest

Secures sensitive files with strong encryption, on desktops, laptops, network attached storage, and backup media

Protecting Data in Use

Protects sensitive data in storage even while the files are in use: plaintext is provided in memory and on demand to authorized applications and is never written to disk

Defending against Advanced Persistent Threats, Viruses, and Malware

Prevents unauthorized users and processes from accessing plaintext and exfiltrating data

Enabling Secure Collaboration

Turns existing workflows into a secure collaborative environment

Achieving Compliance

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

TECHNICAL SPECIFICATIONS

Bulk Encryption	128/192/256-bit AES-CBC (FIPS 197)
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)
Message Authentication	SHA-1 (FIPS 180-4; ANSI X9.30) SHA-2 (FIPS 180-4)
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

SUPPORTED PLATFORMS

- Windows 10 or above (x64)
- CentOS 7.4 (Kernel 3.10.0-957) or above (x64)

EXPORT INFORMATION

SecretAgent/TE 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