

SECRETAGENT[®] MOBILE

Working with confidential documents on your Pocket PC? If so, you'll appreciate the security and user-friendliness of SecretAgent Mobile.

With SecretAgent Mobile it's a snap to encrypt sensitive files to be stored on your mobile device or transmitted to confidants.

SecretAgent Mobile conforms with all Federal and industry cryptographic standards and is interoperable with SecretAgent for Windows, Linux, Mac OS X, Solaris, and other popular UNIX-based platforms!



System Requirements:

A handheld running Microsoft Pocket PC 2002, 2003, 2003 SE, or Windows Mobile 5 (please specify when ordering)

A Windows desktop system with at least 1.5 MB free disk space running ActiveSync 3.7 or above

Export Regulations:

The U.S. Bureau of Industry and Security has eased restrictions on cryptographic products. Please contact ISC for up-to-date information regarding the export status of SecretAgent and other ISC products.

Note: Specifications quoted herein are subject to change without notice. For the latest information visit:

<http://www.infosecorp.com>

©1991-2006 Information Security Corporation. All rights reserved.

All trademarks and registered trademarks are the properties of their respective owners.



1141 Lake Cook Rd., Suite D
Deerfield, IL 60015

Phone: (847) 405-0500
Fax: (847) 405-0506
E-mail: sales@infosecorp.com
Web: www.infosecorp.com

Overview

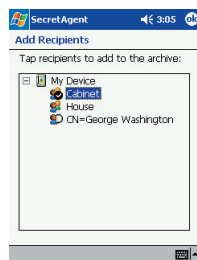
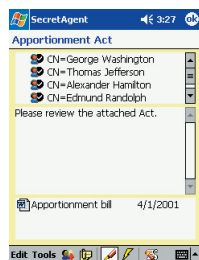
SecretAgent Mobile is the premier file encryption and digital signature utility for your handheld device. It makes protecting your sensitive files as easy as composing an e-mail message. FIPS 140-validated encryption and digital signature algorithms ensure the confidentiality and authenticity of your critical data, whether it's "at rest" on your handheld device or in transmission to another system.

How It Works

Create a new encrypted archive just as you compose an e-mail message:

1. select recipients (yourself and others to whom you wish to grant decryption rights)
2. enter text into the message body (optional)
3. add file attachments (also optional)

When you save the archive, the message body and all file attachments are encrypted for the specified list of recipients (and your original plaintext files are optionally securely erased).



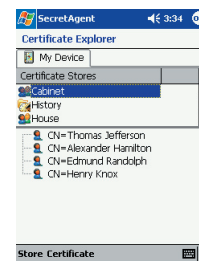
Any designated recipient can open an encrypted archive on their Pocket PC by simply entering their password. The contents of an open archive are displayed in a window similar to that used by Inbox for e-mail messages. You may read and/or edit the message body, or open an attachment in its associated Windows application. And if you change the archive in any way, when you close it SecretAgent Mobile will automatically offer to re-encrypt and/or re-sign it for you, preserving its original list of recipients.

Simplified Key Management

In addition to managing individual certificates, SecretAgent Mobile allows you to create named groups of certificates that simplify the frequent encryption of documents for one or more communities of interest. SecretAgent Mobile also maintains a history of your private keys and automatically applies the correct decryption key to an archive when you enter your password.

Share Sensitive Data

Transmit your encrypted and/or signed archives as e-mail attachments or beam them to a correspondent's PDA. Archives created by SecretAgent Mobile are fully compatible with SecretAgent on other platforms.



Enterprise Policy Enforcement

An administrator can impose the same security policy settings on all SecretAgent users in their organization. In particular, an administrator can ensure that:

- only approved symmetric and public key algorithms are used
- (optional) specified data recovery agents can decrypt any archive in an emergency
- all users receive the same set of initial software configuration settings (including default archive type, preset RDN values for self-signed certificate generation, password strength requirements, etc.); individual settings can be locked against user tampering, if desired

Technical Specifications

To promote maximum interoperability with SecretAgent on other platforms, SecretAgent Mobile supports the following standards:

- Credentials:
RSA, DSA, and ECC X.509 recipient certificates and a standard PFX/PKCS#12 file (or ASN.1 DER-encoded certificate and associated PKCS#8 private key) for user's own key pair
- Encryption Ciphers:
128/192/256-bit AES-CBC (FIPS 197)
192-bit TDES-CBC (FIPS 46-3; ANSI X9.52-1998)
- Decryption Ciphers:
128/192/256-bit AES-CBC (FIPS 197)
192-bit TDES-CBC (FIPS 46-3; ANSI X9.52-1998)
56-bit DES-CBC (FIPS 46-3/81; ANSI X3.106) (DESX and EA2 are also provided)
- Message Digest:
SHA-1 (FIPS 180-2)

SecretAgent Mobile uses ISC CDK 7.0 which has been awarded NIST FIPS 140-1 Level 1 Certificate No. 347. For further information contact ISC.