RSA SecurPC™

Multi-Platform File Protection for the Enterprise

SecurityDynamics

Thinking ahead put us ahead.™

Fast, transparent, secure file encryption for multi-platform environments

Every year hundreds of thousands of portable and desktop computers are stolen – and many more are compromised by hackers and intruders. In almost every case, the most valuable thing lost is not the hardware, but the data stored, such as business plans, customer lists, and confidential correspondence.

RSA SecurPC is the only multi-platform, internationally-compatible encryption solution that protects files against theft, hackers and corporate espionage.

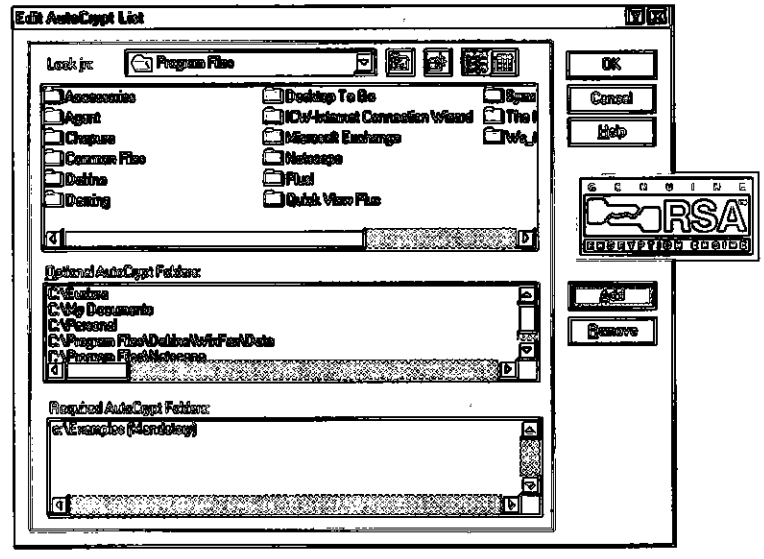
Now available in version 2.0 for Windows 95, RSA SecurPC provides full-strength encryption worldwide. RSA SecurPC v2.0 has been granted unprecedented approval to deploy to U.S. companies and their subsidiaries around the world, at full 128-bit strength.

Highlights

- **High strength security; low impact security administration**
- **Transparent, automatic file protection**
- **Full-strength encryption now available worldwide**
- **Protects corporate data outside the firewall or in transit via email**
- **Emergency Access™ enables file recovery only by multiple trustees**
- **Encrypted files can be easily exchanged with users not equipped with RSA SecurPC**
- **Encrypted files can be shared across platforms: Mac, Windows 3.1, 95, NT**

Easy Enforcement of Security Policy

RSA SecurPC enables the Security Administrator to enforce security policy, from how passphrases are formed, when they expire – even which folders users must encrypt. Once those decisions are made, a master user installation is ready to be loaded. No ongoing security administration is needed. User file recovery, passphrase recovery, even emergency boot access are all exception-based and require no elaborate key management. User installation can be done via network, disk, or CDROM.



Transparent, automatic file protection works full time

Transparent, Automatic Protection Full-Time

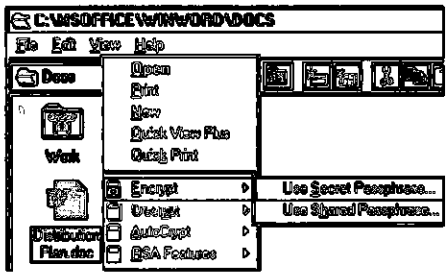
A file encrypted with RSA SecurPC stays encrypted until opened through the application; the file is automatically re-encrypted when closed. Further, AutoCrypt™ folders encrypt everything put into them, immediately. RSA SecurPC works the way you work, enabling you to encrypt files anywhere – even mapped network drives – not just in special "secured folders." The new boot lock and screen lock features in version 2.0 protect users' PCs even more. This means that state-of-the-art security technology may be added without cramping your style or retraining your users. Set it and forget it: RSA SecurPC protects your data.

Integration With the Operating System

RSA SecurPC isn't a separate application – it integrates with the operating system. On a PC, RSA SecurPC actually becomes a part of the Windows 95 Explorer or the Windows 3.1 and NT File Managers, while on the Macintosh, RSA SecurPC integrates with the

RSA SecurPC — The Strongest International Encryption Solution

Finder. Whatever the platform, the place where you move, copy, and manipulate files every day is where you'll find RSA SecurPC. Built in and easy to use, with either on-demand or automatic file protection. Furthermore, once files are chosen for protection, access is direct from your applications through the File Open dialog.



RSA SecurPC integrates easily into the operating system

Encrypted File Sharing Across Platforms, Across Borders, Among Versions

RSA SecurPC is cross-compatible among all Windows platforms (95, NT, 3.1) and on the Macintosh platform. Files encrypted on one platform can be decrypted on another, whether from version 2.0 or the original version. This interoperability applies to the full-strength U.S. version and the export-strength worldwide version. RSA SecurPC also enables users to encrypt files to be shared with non-RSA SecurPC users – anyone with the same platform can be sent a self-extracting encrypted file. All a recipient needs is the special passphrase that the user created for that file, which can be communicated via telephone, pre-arrangement, etc.

How are current users taking advantage of this capability?

- Delivering confidential reports from the U.S. to international clients (without export restrictions and with full-strength encryption)
- Broadcasting corporate directories worldwide – even to employees who don't have RSA SecurPC
- Sending electronic mail with confidential attachments (sales figures, policy documents, employee evaluations)
- Exchanging confidential email with overseas business partners – without concern over compatibility of key length

Fast, Secure, Encryption Technology

In the security business, RSA is synonymous with encryption. For bulk encryption, RSA SecurPC uses our well-known RC4™ Symmetric Stream Cipher. That's the same RC4 used by professional security developers at Microsoft, Netscape, Apple, and Novell. This implementation, which uses 128-bit RC4 keys for U.S. and Canadian companies and their subsidiaries around the world, provides security that is orders of magnitude greater than 56-bit DES-based systems. "Cracking" a single 128-bit RC4 key is estimated to be an effort costing over half a billion dollars and taking over six months to set up – and every file has a separate key. In addition, RSA-quality security is available without waiting hours to encrypt or decrypt files: RSA SecurPC achieves throughputs of over 25MB per minute on a typical 75MHz Pentium® PC or comparable Macintosh.

Exclusive Threshold-Based Emergency Access™

Most disk-locking systems use simple "master key/slave key" systems to allow system administrators access to users' encrypted files or private passphrases. This type of system is an invitation to abuse. One crooked insider can compromise the entire network. RSA SecurPC provides for safe recovery of a user's encrypted files and lost passphrases, and even provides for emergency boot access when the user's passphrase is lost or forgotten.

Using the patented RSA Public Key Cryptosystem™ along with advanced key storage and secret-splitting technologies, RSA SecurPC enables the security administrator to split emergency decryption authority among as many as 255 trustees. The administrator determines the threshold number of trustees (say, any 3 out of 7) that must enter their passphrases and "key disks" to decrypt a user's files in an emergency. This is similar to the protections for large corporate checking accounts, which require multiple signatures, but stronger, since these passphrases can't be forged.

RSA SecurPC puts the control over this process completely into the hands of the security administrator; the trustees need only know their passphrases and have their key disks in order to run the recovery process. The safeguards are in the hands of the trustees and the process is simple for the administrator.

Take Your Business with You

Face it. In the 90's, your electronic records are your business. Previously, using networked PCs or remote laptops meant either sacrifice of productivity or risk of loss. Traveling copies of important business databases were out of the question – but not any more. Now, with RSA SecurPC, you can take your business with you – anywhere – with confidence and security.

Technical Requirements

For all platforms, RSA SecurPC's "footprint" is small. The hard disk space requirement is just over 1MB. The upper memory for the DLL is approximately 75K. For Macintosh, the minimum requirement is 2MB of RAM and System 7.0 or above, with System 7.1.1 for drag and drop support. The hard disk usage and memory usage is similar to Windows. On all platforms, a mouse is not required, but is recommended.

For more information

For more information on RSA SecurPC or on the full range of Security Dynamics enterprise security solutions, please call 800 SECURID or visit our Web site at www.securitydynamics.com.

SecurityDynamics

Headquarters: 20 Crosby Drive, Bedford, MA 01730 USA Tel. 800 SECURID or 781 687 7000 Fax: 781 687 7010 Email: info@securitydynamics.com Internet: www.securitydynamics.com

Canada: 416 368 9980 United Kingdom: 44 118 936 2600 France: 33 1 46 94 75 58 Germany: 49 6173 924 40 Norway: 47 67 56 95 99 Singapore: 65 334 5070 Hong Kong: 852 2887 7847 Japan 81 3 3539 7517