

IBM Embedded Security Subsystem



Highlights

- **Easily engage cutting-edge security, thanks to the IBM Embedded Security Subsystem, featuring intuitive interfaces, sophisticated authentication techniques and automated encryption functionality.**
- **Simplify security with an innovative utility for creating, storing and managing passwords.**
- **NEW! The subsystem supports an integrated fingerprint reader for out-of-the-box functionality that puts your passwords at the tip of your finger (select IBM ThinkPad models).**
- **Enjoy the protection of advanced IBM Client Security Software and Password Manager, available via a single download for easy configuration.**
- **Boost mobile workforce security. This standards-based application enhances secure wireless access and remote authentication for employees on the go.**

Big risks. Bigger solution.

According to the *Eighth Annual Computer Crime and Security Survey* published by the Computer Security Institute and the FBI, 2003 was another expensive year for the victims of computer crime. Theft of notebook computers, for example, resulted in losses of more than US\$6.8M for the 530 companies that responded to the survey. And, for the same 530 companies, theft of proprietary information caused the greatest financial loss—with an average loss of US\$2.7M, and more than US\$70M in total.

IBM can help. The Embedded Security Subsystem is an IBM ThinkVantage™ Technology that helps turn your computer into a highly protected vault. Available on select IBM ThinkPad® notebooks and ThinkCentre™ desktops, this subsystem offers advanced technology for user authentication—including support for the integrated fingerprint reader on select ThinkPad notebooks—plus enhanced security for wired and wireless networking through the use of digital certificates (third-party digital certificate, not included).

Call **1 888 SHOP IBM** or go to **ibm.com** (U.S.) or **ibm.ca** (Canada) to buy direct, to locate an IBM reseller or for more information.

Secure to the core.

The Embedded Security Subsystem helps you gain more extensive control over enterprise security. Here's how:

An embedded cryptographic microprocessor works in conjunction with IBM Client Security Software to manage encryption keys and processes that help secure data, communications and digital identity. The chip itself is isolated from the operating system using patented IBM tamper-resistant technology. To initialize the integrated chip after taking possession of a machine, users or administrators simply download the Client Security Software and run a single setup wizard to install all necessary drivers. The software creates a set of master encryption keys and uses them to authenticate users.

Lock data—and lock out thieves.

After activating the security chip, the Client Security Software also enables users to lock valuable data with file and folder encryption. This useful feature helps protect data and

“We can break into just about anything, but that IBM [embedded security] chip is still a challenge to us.”

—Technology Crime Investigator, *The Edmonton Journal*, February 2003

simplify security by encrypting data automatically. Only a verified user can unlock the encrypted data, so sensitive information can be better protected if a computer is stolen.

Identify yourself with secure flexibility.

Flexible authentication techniques—such as passphrases, fingerprints and smart cards—are supported to help secure logon procedures according to your specific security policy requirements (optional fingerprint or card readers required).

In addition, the subsystem offers support for integrated fingerprint readers on select IBM ThinkPad notebooks. By using the integrated reader, users can bypass the need for peripheral components while adding the convenience and security of fingerprint authentication.

When using the integrated fingerprint reader built into the palm rest on select IBM ThinkPad notebooks, users can go from power up to Windows desktop with one swipe of their finger.

Multiple passwords? No problem.

Hardware, software and even Web-based services frequently require unique sign-on codes to gain secured access. The Embedded Security Subsystem helps eliminate the hassle—and can reduce help desk calls for password resets—through the intuitive IBM Client Security Password Manager utility.

Password Manager allows users to replace multiple passwords with authentication through a single passphrase, fingerprint or smart card. An easy-to-use interface simplifies the creation and management of



many unique passwords, while the integrated chip encrypts stored passwords for improved security. When prompted for a sign-on to an application, users can simply open the Password Manager and authenticate.

If using the integrated fingerprint reader built into the palm rest on select IBM ThinkPad notebooks, users simply swipe their fingerprints to recall passwords. Password Manager then automatically decrypts user credentials and places the data in the correct fields on the sign-on screen.

Wireless and remote security you can afford.

Don't be afraid to let your workforce go mobile. The Embedded Security Subsystem, in conjunction with IBM Access Connections, enhances security for existing wired and wireless standards-based (802.1x) networks. For those IBM systems featuring Cisco's Light Extensible Authentication Protocol (LEAP), authentication is based on user's ID and password. The Embedded Security Subsystem helps to protect a user's ID and password

by concealing them cryptographically through the security chip. Another example is 802.1x EAP-TLS security which uses a certificate for client authentication. ESS can enhance this security by cryptographically protecting the certificate.

The Embedded Security Subsystem is certified RSA SecurID-ready for enhanced remote access protection, and can function as an RSA SecurID authenticator. As a result, mobile users can employ cost-efficient SecurID software tokens to carry one less piece of equipment while on the road—without sacrificing security or budget.

The innovations go on and on.

Looking for more efficiency-improving, business-building technologies? IBM has them. They're called IBM ThinkVantage Technologies. They have been developed to help businesses increase efficiency. To learn more about the Embedded Security Subsystem or other IBM ThinkVantage Technologies, visit **ibm.com/thinkvantage**

A security solution you can manage with ease.

Administrators can help set and promote broad adherence to critical security policies—even across virtual private networks—with built-in functionality for unique user verification, e-mail protection and digital certificate management. After security policies have been set, administrators can push these policies to the client using optional file communication tools such as Tivoli® Access Manager.

ThinkVantage Technologies Service and Support.

Rollouts of even the most user-friendly new technology can be challenging at times. To help you get the most out of ThinkVantage Technologies, IBM has specialists who can provide everything from on-site analysis to installation assistance. Help ensure a successful and efficient deployment. Ask about ThinkVantage Technologies Service and Support today.

The Embedded Security Subsystem has been tested to interoperate with select security and authentication offerings from these organizations	
Adobe for secure digital documents	www.adobe.com
Checkpoint for networking	www.checkpoint.com
Cisco for networking	www.cisco.com
Entrust for PKI solutions	www.entrust.com
Gemplus for smart card devices	www.gemplus.com
RSA for authentication devices	www.rsa.com
Targus for biometric devices	www.targus.com
Utimaco for full hard drive encryption	www.utimaco.com
VeriSign for PKI solutions	www.verisign.com

Check the Web.

- **Embedded Security Subsystem**
ibm.com/pc/us/think/thinkvantagetech/security.html
- **ThinkVantage Technologies**
U.S. **ibm.com**/thinkvantage
Canada **ibm.ca**/think
- **ThinkPad**
U.S. **ibm.com**/thinkpad
Canada **ibm.ca**/thinkpad
- **ThinkCentre**
U.S. **ibm.com**/thinkcentre
Canada **ibm.ca**/thinkcentre
- **Accessories and upgrades**
U.S. **ibm.com**/pc/options
Canada **ibm.ca**/options
- **eSupport**
U.S. **ibm.com**/support
Canada **ibm.com**/support/ca/en
- **Presentations and 3D tours**
U.S. **ibm.com**/pc/webcast
Canada **ibm.com**/ca/webcast
- **PC services**
U.S. **ibm.com**/pc/services
Canada **pc.ibm.com**/ca/migration
can.ibm.com/snd/
solutioncentre
can.ibm.com/helpware
- **Financing**
ibm.com/pc/financing
- **PC product training**
U.S. **ibm.com**/pc/training
Canada **ibm.com**/ca/education

Read on.

Download product literature



- ThinkPad
ibm.com/pc/us/thinkpad/literature
- ThinkCentre
ibm.com/pc/us/desktop/literature

Call us.

Request an IBM PC catalog or buy direct
1 888 SHOP IBM

Reseller locator
U.S.
1 800 IBM-4968
Canada
1 800 IBM-2255



PCD HelpCenter®
U.S. 1 800 426-7378
Canada 1 800 565-3344

IBM Asset Recovery Solutions for disposal and recycling of your systems (U.S. only)
1 888 SHOP IBM (option 1, enter 7615)



© 2004 IBM Corporation

Produced in the U.S.A.
10-04
All Rights Reserved

Availability: All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time, without notice. IBM is not responsible for photographic or typographic errors.

Warranty: For a copy of applicable product warranties, write to: Warranty Information, P.O. Box 12195, RTP, NC, 27709, Attn: Dept JDJA/B203. IBM makes no representation or warranty regarding third-party products or services.

This publication was developed for products and services offered in the United States. IBM may not offer the products, services or features discussed in this document in other countries. Information is subject to change without notice. Consult your local IBM representative for information on offerings available in your area.

Trademarks: IBM, the IBM logo, HelpCenter, ThinkCentre, ThinkPad, ThinkVantage and Tivoli are trademarks of IBM Corporation in the U.S. and other countries. Other company, product and service names may be trademarks or service marks of others.

Made in Japan, Korea, Mexico, Scotland and Taiwan.

Visit ibm.com/pc/safecomputing periodically for the latest information on safe and effective computing.