IBM Personal Computing Division
July 2001

Information Brief

These IBM® NetVista™ and ThinkPad® Security Solutions help protect your data, hardware, network access and communications:

- ***The IBM Embedded Security Subsystem, featuring the IBM embedded security chip and IBM Client Security Software 2.0, helps protect your data locally and from network intrusion.***
- ***Partnerships with Entrust and RSA ensure that select IBM NetVista desktops and ThinkPad notebooks are compatible with industry-leading security options.***
- ***Physical security options include hardware locking solutions for NetVista desktops and ThinkPad notebooks.***
- ***The IBM Backup and Restore utility helps protect against the devastating loss of data and applications.***

NetVista and ThinkPad Security Solutions

Security is essential in today's networked world. Organizations must protect their sensitive data, hardware and transactions. Threats include theft, corruption and network security breaches such as viruses and online intrusions.

Rock-solid security depends on the ability to establish that data transmissions are authentic, confidential, and intact.

To address these top priorities on NetVista desktops and ThinkPad notebooks, IBM Client Security Solutions present a unique suite of hardware- and software-based security solutions. These solutions complement one another to provide individualized and progressively robust levels of security locally and across a network.

This information brief addresses four categories of IBM Client Security Solutions:

- **IBM Secure Client**
- **Physical Security**
- **IBM Backup and Restore**
- **Norton AntiVirus**

IBM Secure Client

Select IBM NetVista desktops and ThinkPad notebooks feature the IBM Embedded Security Subsystem and are designed for use with IBM Client Security Software—two solutions that comprise the heart of the IBM Secure Client.

- **IBM Embedded Security Subsystem**
  The IBM Embedded Security Subsystem consists of a cryptographic microprocessor designed to interface with common security protocols.

  Built into the system board of an IBM NetVista desktop or ThinkPad notebook, the cryptographic microprocessor is an advanced chip that employs encryption keys and processes to help secure your data, communications and identity. The chip stores your encrypted keys and supports public key infrastructure (PKI) operations, such as encryption for privacy and digital signatures for authentication, within the protected environment of the chip.

  Two industry-standard interfaces enable access to protected functions: the Cryptographic Application Programming Interface/Cryptographic Service Provider (CAPI/CSP) and Public-Key Cryptography Standard (PKCS) #11. These interfaces link to industry-standard security protocols, such as Secure Multipurpose Internet Mail Extension (S/MIME), Secure Socket Layer (SSL), and Internet Protocol Security (IPSec).

  The Embedded Security Subsystem helps protect electronic transmissions generated by applications such as Microsoft® Outlook®, Lotus® Notes®, Microsoft Internet Explorer and Netscape Navigator. And it works immediately, because it's enabled through CAPI and PKCS#11. Unlike software solutions alone, the Embedded Security Subsystem is physically located on the motherboard and protects PKI operations and other functions within a secure and separate hardware environment. The encryption functions are more secure because the operations are not performed in main memory and the keys are not stored on the hard disk drive.

The Embedded Security Subsystem is a result of the IBM commitment to developing trust and security in the PC industry. IBM was instrumental in defining the security standard adopted by the Trusted Computing Platform Alliance as the basis for future PC design. Formed by IBM, Compaq, HP, Intel and Microsoft, the alliance today includes more than 170 computer, chip and security device manufacturers; cell-phone companies; security-software developers, and security consulting-service providers. These companies work together to develop specifications that improve trust and security through hardware and software solutions.

- **IBM Client Security Software**
  IBM Client Security Software 2.0 is available to download from the Internet for IBM NetVista and ThinkPad models equipped with the Embedded Security Subsystem. By downloading the software after the systems have been shipped, the customer can be assured that no unauthorized parties have knowledge of the keys and pass phrases designated by the customer.

  An administrator utility allows administrators to activate or deactivate the Embedded Security Subsystem and generate, archive and regenerate keys and pass phrases. The software includes a library of drivers for interface with industry-standard security applications and devices, including RSA and Entrust solutions. A major asset of Client Security Software 2.0 and the embedded security chip is the ability to encrypt files and folders located on the system's hard disk drive. This encryption protects valuable data from intrusion when the system is connected to a network or in the event of physical theft of a system. Given the ease and frequency with which mobile computers are stolen, the importance of safeguarding data on a notebook computer is critical. Without the correct password or authentication controls, which are safely stored through the embedded security chip, the files remain encrypted and inaccessible.

  IBM Client Security Software also includes User Verification Manager (UVM). UVM manages the security policy for NetVista and ThinkPad

computers equipped with the IBM Embedded Security Subsystem.Once installed, UVM manages:

- Means of authentication—mechanisms or devices, such as pass phrases, tokens or biometric devices, used to gain access to a secure client or network.
- PKI activities—functions that use public-key cryptography to encrypt sensitive data and authenticate users. IBM Client Security solutions are EntrustReady for industry-leading Entrust PKI solutions.
- UVM-aware applications—special applications, such as the UVM logon and the UVM screen saver, that are provided with IBM Client Security Software and developed to conform to the UVM application programming interface.
- UVM security policy—the access hierarchy in which each level can be managed by the level above—from a client user managed locally at the client system to a global policy in which UVM interactions can be dynamically managed across an enterprise. It is compatible with Tivoli® Policy Director, serving as a key feature for implementing security plans for large corporations.

For users working remotely, on the road, or with wireless connectivity, the latest version of IBM Client Security Software also supports the use of Virtual Private Networking (VPN) to achieve secure connections. VPN software helps safeguard the transmissions of employees who are connecting to internal company networks through the public Internet or are using wireless connections. The VPN software authentication functions are conducted within the secure environment of the IBM embedded security chip, preventing any unauthorized users from gaining access to data transmitted wirelessly or accessing the company network through the wireless transmission.

RSA Secured, SecurID Ready

The IBM Embedded Security Subsystem has been certified as an RSA Secured, SecurID Ready Partner, which means the technology has been designed and tested to comply and be compatible with industry-leading VPN solutions from RSA.

The RSA SecurID software and the IBM Embedded Security Subsystem work together to offer more secure user authentication and more secure VPN access to your corporate network. Using the SecurID software, the user passcode is generated within the protected confines of the Embedded Security Subsystem and is used to create safer wired or wireless connections. This secure solution eliminates the need for the users to carry, maintain and manage hardware tokens, such as key fobs.

Entrust Ready

The IBM Embedded Security Subsystem has been certified to be Entrust Ready, which means the technology has been designed and tested to ensure compatibility with industry-leading PKI security solutions from Entrust.

Client Security Software 2.0 includes the PKCS #11 Library to support Entrust PKI functions. The Entrust/PKIsoftware allows people to encrypt, digitally sign and authenticate electronic transactions across intranets, extranets and the public Internet. As PKI functions are handled within the secure environment of the chip, the IBM Embedded Security Subsystem affords more protection than software alone.

Physical security

When it comes to physical security, IT managers can choose from a variety of options. Each contributes to this essential layer of protection for your technology investment.

- **Asset ID**
  Asset ID[1] technology enables compatible security and asset-tracking systems, including handheld devices, to wirelessly read or write vital system and user information on an EEPROM chip inside select IBM NetVista personal computers and ThinkPad notebooks. The information can be read or recorded even when the system is powered down or still packed in its carton. Asset ID can eliminate many of the costly, time-consuming manual steps involved in today's system deployment, inventory and tracking processes.

  - Asset ID allows you to take accurate physical inventories of systems and their components without searching for a label or opening the chassis.
  - Used in conjunction with a compatible RFID security system, the Asset ID feature can be used to assist security personnel in preventing unauthorized removal of computers and notebooks.
  - Asset ID is part of IBM Universal Manageability, which delivers innovative, standards-based technologies to simplify systems management.

- **Locks**
  Select IBM NetVista desktops come with a key lock built into the chassis to deter potential thieves. A number of IBM desktop systems also have slots for padlocks or other locking devices for customers who want to bolt the system into place.

  Physical security options are also available for ThinkPad notebooks. The ThinkPad Dock provides a key lock for notebook security, plus security functions to help protect the Ultrabay™ 2000, slots and hard disk drive. ThinkPad Proven™ partner Compu-Lock offers cable locks for ThinkPad notebooks, the ThinkPad Dock and the ThinkPad Port Replicator.

- **Chassis-intrusion switch**
  Select NetVista models feature a chassis-intrusion switch inside which may be set to alert the system administrator each time the computer cover is removed.

IBM Backup and Restore

IBM Backup and Restore is a client application that helps protect you from computer data disasters. Benefits include:

- Quick backups of the primary partition on your computer's hard disk drive on a regularly scheduled or as-needed basis (attended or unattended).
- Better protection of the Microsoft Windows® operating system, important data files, registry settings, desktop settings and Internet productivity files.
- Backups stored in a special, locked partition on your hard disk drive or on an optional second installed hard disk drive.
- Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) alerts to predict imminent hard disk drive failures and send notifications.

Norton AntiVirus

Norton AntiVirus software(OEM edition)[2] builds a solid defense to protect against computer viruses. Preloaded on select NetVista systems, the Norton startup check examines memory, boot records and system files. Then, the AutoProtect scan continuously monitors memory, master boot records, system files and diskette boot records upon access, shutdown or when you restart your computer. If either scan detects a virus code, it can alert the system and remove the virus either automatically or at your prompt.

Plus, the Norton LiveUpdate feature lets you download new virus definitions created by the Symantec AntiVirus Research Center with a single mouse click, or automatically using the Scheduler function.

For more information

ibm.com/pc/ww/ibmpc/security/index

Ibm.com/pc/ww/ibmpc/security/newsandref

Buy Direct: **1 888 SHOP IBM** (746-7426)

Locate Dealer: 1 800 426-7235 U.S.

1 800 426-2255 Canada

1. Asset ID technology allows your personal computer to be scanned by various radio-frequency emitting devices supplied by independent companies.
2. Some software may differ from its original version (in any) and may not include user manuals or all program functionality. Warranty, service and support for non-IBM products are provided directly to you by third parties, not IBM. IBM makes no representations or warranties regarding non-IBM products. For non-IBM software, applicable third-party software licenses may apply.

IBM reserves the right to alter product offerings and specifications at any time without prior notice. This publication could include technical inaccuracies or typographical errors. References herein to IBM products and services do not imply that IBM intends to make them available in other countries. IBM PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this disclaimer may not apply to you.

IBM Personal Computing Division, USA

GK20 5858 00