

Embedded Security Chip and Software - a white paper

Introduction

Security is of utmost importance for a networked PC (or client) that will be used to electronically transfer confidential information. These security requirements can vary from customer to customer. Furthermore, security requirements can vary from client to client within the enterprise of a single customer. Because of the possibilities, the hardware and software components in clients should complement each other to provide progressive, more robust levels of security, locally and across a network.

To achieve this, IBM has equipped select IBM PC 300® PL computers (referred to in this paper as IBM clients) with built-in cryptographic technologies in both the hardware and software components. These components support key-management solutions, such as public key infrastructure (PKI), used to secure the electronic transmission of information.

This paper discusses the components of the IBM client that facilitate and manage secure cryptographic operations. The key topics reviewed in this paper are the embedded Security Chip, the key-management architecture used in the security chip, and the architecture guiding the development of the IBM Client Security Solutions software which includes User Verification Manager (UVM). The topics of this paper have been developed to support Microsoft® Windows® 95, Windows 98, and Windows NT® operating systems.

Note: Although not discussed in this paper, other technologies such as Alert on LAN™, Asset ID¹, chassis-intrusion detection, a physical security U-bolt, Internet Protocol Security (IPSec)² hardware acceleration, and Virtual Private Networks complement the security features described in this paper.

Embedded Security Chip

The embedded Security Chip is a cryptographic microprocessor that is embedded in the system board of the IBM client. The embedded Security Chip supports RSA³ PKI operations such as encryption for privacy and digital signatures for authentication. The embedded Security Chip includes EEPROM memory where RSA key pairs are stored. The chip communicates with the main processor of the computer through the System Management Bus (SMB), a subset of the Phillips I 2 C interface.

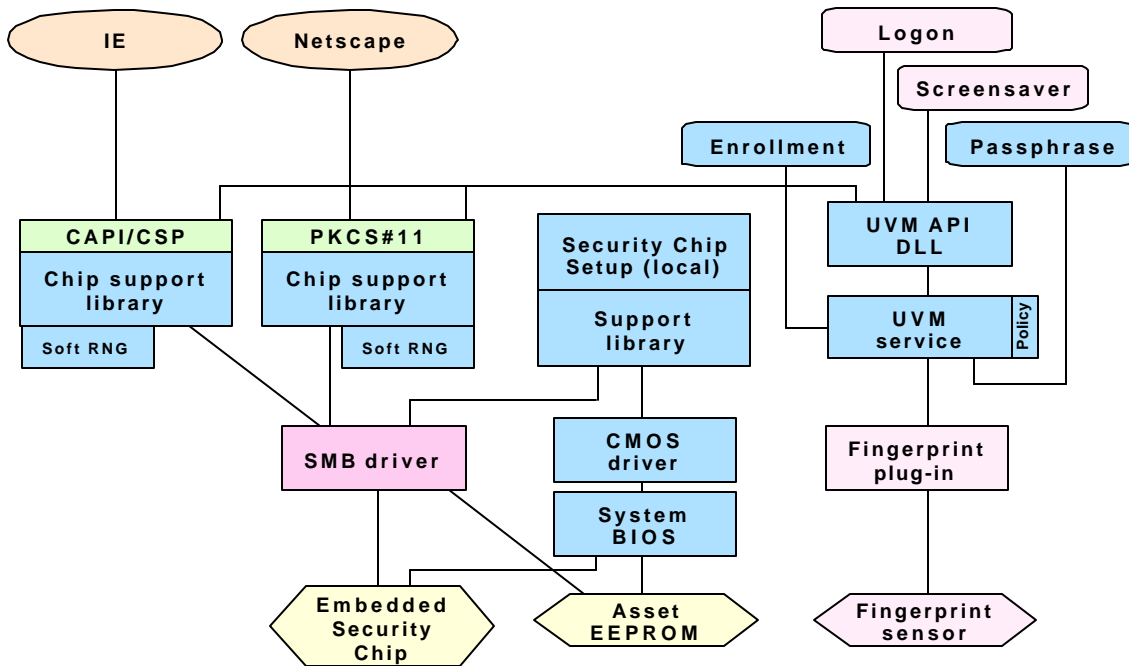
The following diagram shows the interaction between the embedded Security Chip and other security components for the IBM client.

¹ Handheld scanning devices and other hardware and software products that must be used with Asset ID must be purchased through our IBM Asset ID partners. A complete listing of these independent vendors is available at www.ibm.com/pc/us/desktop/assetid.

² IPSec is a standard of the Internet Engineering Task Force.

³ RSA stands for Rivest, Shamir, and Adleman, the developers of the RSA PKI. RSA Data Security, Inc. refers to the company that holds patents for security technologies.

Security components for the IBM client



The embedded Security Chip interacts with the following software:

- Cryptographic application programming interface/cryptographic service provider (CAPI/CSP) and Public-Key Cryptography Standard (PKCS) #11
- IBM chip support library
- Security Chip Setup

CAPI/CSP and PKCS#11

To support the embedded Security Chip, IBM implemented the following application programming interfaces (APIs):

- **CAPI/CSP**, defined by Microsoft and used as the default cryptographic service for Microsoft operating systems and applications
- **PKCS #11**, defined by RSA Data Security, Inc. and used as the cryptographic service for Netscape and other products

Where standard CAPI/CSP and PKCS#11 APIs perform cryptographic operations in software, the APIs implemented by IBM route cryptographic operations through the embedded Security Chip. This routing enables applications that use these APIs to secure cryptographic operations through built-in hardware, which is more secure than a software solution. (Note that no changes in applications need to be made because the cryptographic middleware automatically routes function calls to the hardware.) Also, interoperability between the two APIs is implemented in the IBM client. For example, if a Microsoft application generates a key and its associated certificate, a Netscape application is able to use them. This interoperability is an advantage in present networking environments where multiple applications and configurations are used.

IBM chip support library

The IBM chip support library interfaces with the embedded Security Chip. Key management such as key generation and key encryption are implemented within the IBM chip support library. The following cryptographic functions are contained within the IBM chip support library:

- **1024-bit and 512-bit key generation⁴.** Key generation is a basic function in the IBM client. Applications can call into the IBM chip support library to generate both RSA and symmetric keys.
- **1024-bit and 512-bit key encryption.** Two methods of encrypting information are symmetric and public-key encryption. Symmetric encryption uses the same key to encrypt and decode information. Public-key encryption uses a key pair consisting of a public and a private key to encrypt and decode the information. Symmetric keys can be encrypted using public-key encryption and PKI to secure them during key exchange. The IBM chip support library encrypts all private key information to create virtual private storage.

The following cryptographic functions are implemented in the embedded Security Chip *through* the IBM chip support library:

- **1024-bit and 512-bit digital signature.** The IBM chip support library uses PKI encryption to create digital signatures, which are used for authentication and non-repudiation. The digital signature can be used to prove both the integrity and authenticity of the source of the data.
- **1024-bit and 512-bit RSA key decryption.** Key decryption is for internal use within the embedded Security Chip. This capability enables multiple RSA keys to be stored in an encrypted format on the system without exposing any information about the key. The key information is available only in an unencrypted format when it is inside the embedded Security Chip.
- **Up to 256-bit⁵ decryption of information that was encrypted using 1024-bit and 512-bit keys.** This level of decryption enables symmetric key exchange with the protection of PKI identity and integrity.

Security Chip Setup

Security Chip Setup is a utility that provides an administrator interface to the functions of the embedded Security Chip. Security Chip Setup is used to initialize the security chip and create base levels of keys. Also, the utility is used to establish the administrator credentials (certificate and password). The administrator credentials are used to create archive and migration versions of the platform and user key pairs. (See the "Key-management architecture" box below for more information on key pairs used in the IBM client.) After an administrator password is initialized in the embedded Security Chip, all further administrator level actions must be authenticated by entering the password. Security Chip Setup is used to:

⁴ The figures 1024 bit and 524 bit refer to the RSA key size. Different grades of security are reflected by key size, with 1024-bit keys being more secure than 512-bit keys.

⁵ Up to 256-bit decryption is available in the United States and Canada. 56-bit decryption is available elsewhere to comply with US government export restrictions.

- **Create the base hardware key pair.** The base hardware private key is the basis for all other key information on the client. Rights and ownership of the hardware private key are established through an administrator password.
- **Reset the fail counter for the hardware private key password.** The fail counter for the hardware private key password is incremented each time an incorrect password is entered. To enhance security, the fail counter temporarily locks the security subsystem after three failed attempts.
- **Create the platform key pair.** The platform key pair is generated automatically or imported from a key file. This platform key information is then signed with the administrator private key to ensure authenticity.
- **Create a key archive.** To create a key archive, an administrator public key is used to encrypt the platform and user keys; once encrypted by the administrator public key, they are in a format readable only after the administrator private key is entered. These encrypted keys can then be stored on a diskette. Once a key pair is encrypted and archived through this process, it is never exposed outside the embedded Security Chip.
- **Restore archived keys.** If any of the keys are lost, the keys in the levels above the lost keys are obsolete. If key loss occurs, archived keys can be restored. Some examples where key loss is possible and how those keys can be restored are:
 - **Data loss on the hard disk drive.** Because platform and above keys are stored on the hard disk drive and managed as unprotected data, only those levels of keys are affected by hard-disk data loss. In the event of data loss, a backup tool such as SMART Reaction can be used to restore the

Key-management architecture

A robust key-management architecture is an important requirement for the embedded Security Chip. Functions such as key encryption, key storage, and key restoration are all part of the key-management architecture. With those functions in mind, a hierarchical key ring structure has been developed to manage keys in the embedded Security Chip.

The key ring structure consists of four levels of keys. Each key ring structure level is referred to as a key pair because a pair of keys, private and public, are required to secure each level. Each level is secured through the level below it by encrypting the private key with the public key of the underlying key pair. Encrypted key pairs are then routed through the embedded Security Chip where they are decoded to expose the private key. All private key operations, such as digital signing, take place within the embedded Security Chip and are bound to a specific user through a personal identification number (PIN). At no time is private key information exposed outside the chip.

Level 0 or base hardware key pair - The base hardware key pair resides entirely on the embedded Security Chip. A user creates the hardware private key through Security Chip Setup. The hardware key pair is unique to the client, and it is used as the base key from which all other key information on that client is created.

Level 1 or platform key pair - An administrator creates the platform key pair in Security Chip Setup. The platform key pair is bound to the client as defined by the serial number of the client and does not change with changes to the key information below it. The platform key pair can be created only after the hardware private key is established. Upon creation, the private platform key is installed in the system by encrypting it with the hardware public key. A virtual certificate for the platform key pair is also created during initialization. The platform public key is signed through the hardware private key using the administrator password.

Level 2 or user key pair - User key pairs are associated with a specific user as defined by the operating system logon password. Upon creation, the private user key is encrypted with the public key of the platform key pair.

Level 3 or credential key pair - Credential key pairs are specific to a user and a specific application. During an application key-generation event, the private key associated with the credential is encrypted with the user public key of the user as specified by the operating system logon password. The encrypted credential keys are bound to this user key pair, and only the authorized user can use those credential keys.

User key file integrity and authenticity - All level 2 and level 3 key information is managed by the IBM chip support library as a single user-key file. The integrity and authenticity of the data in this file is maintained by the support library by encrypting and signing the key file through the platform key pair.

data. Security Chip Setup also provides a way to restore the keys if a backup tool such as SMART Reaction is not used.

- **System board replacement.** As previously discussed, the hardware key resides within the embedded Security Chip which is soldered to the system board, and it is the basis for all other keys above it. If the system board needs to be replaced, a new base hardware key pair for the embedded Security Chip on the new system board must be created.

Because the platform key pair was encrypted with the hardware key pair previously installed on that system, the encryption of the platform key pair must be migrated to the new hardware key pair. Security Chip Setup provides a way to restore the archived platform key pair and migrate it from the previous base hardware key to the new base hardware key. This restoration and migration is accomplished by encrypting the platform key information with the public key of a recovery key pair.

In a network environment, an administrator usually has the private key of this recovery key pair. To migrate the platform key data to a new system board, the administrator enters the private key of this recovery key pair (in the Security Chip Setup utility) to decrypt the platform key data and then re-encrypt it with the new base hardware key. Because all other key information on the hard disk drive had been encrypted with this platform key pair, this key information remains valid.

- **Install administrator virtual certificate.** The administrator virtual certificate is created to provide a means for verifying the authenticity of the administrator signature without requiring a full certificate authority association. During initialization, Security Chip Setup enables an administrator to provide the public key of the administrator key pair and the administrator password that has been initialized into the chip. The administrator public key is then signed through the chip using the base hardware private key. The administrator password is required for the embedded Security Chip to perform the signature operation with the hardware private key. This administrator signature is then appended to the platform public key to form a virtual certificate. The chip support library can then authenticate the platform public key before each use by using the hardware (level 0) public key (read from the chip) to decrypt the appended signature and then comparing the result to the digest of the current platform public key. Because only the administrator should have knowledge of the hardware password (which is needed to create a signature using the base hardware private key), the authenticity of the platform public key is validated. The integrity of the hardware password serves as the link to the administrator authenticity.

IBM Client Security Solutions software

IBM has developed security software designed to be used with the embedded Security Chip. This software is available for downloading and installation from the World Wide Web. The security software includes different layers that support cryptographic and identification services. UVM is the software used to manage identification services. Note that some of the security software is discussed in more detail in the previous section, "Embedded Security Chip."

Cryptographic services

The following software layers provide cryptographic support in the IBM client:

- **CAPI/CSP and PKCS#11** provide support for Microsoft applications, such as Internet Explorer and Outlook Express, and Netscape applications.
- The **IBM chip support library** provides support for management services, such as key encryption, password association, and key hierarchy management.
- The **smart card software layer** provides a standardized command interface to a smart card reader. Options by IBM (OBI) offers a smart card security kit that includes a smart-card reader and a smart card. The smart card reader attaches to the serial port of the computer. The smart card contains a chip with

secure memory and hardware support for security functions, including identification and authentication. The chip on the smart card can be used to store data and a variety of programs, and can be updated whenever necessary.

User Verification Manager

A primary function in client security is end-user identification and authentication. Once the user is identified, client software must assist in the management and enforcement of the access rights and privileges for that user, as defined by the security policy for the client.

The IBM security software includes UVM which is used to identify an individual and to determine access rights and privileges. UVM is a central control function that can determine the type and application of the identification service under policy control. For example, UVM can enforce the policy of a client so that one user is required to enter a password to access the computer, while another user is required to enter a password and also use another identification service such as a smart card. The identification services that UVM manages are knowledge tokens (for example, passwords) and smart cards.

Providing safe key storage is another requirement in client security. In the IBM client, access to this storage is most often protected with a PIN either directly or indirectly through UVM. This safe storage can be virtualized through the embedded Security Chip or be implemented through an external device such as a smart card.

UVM interacts with authentication applications. Authentication applications run on the IBM client and control access to functions on the computer or provide ease-of-use features to the client. Examples of these authentication applications include:

- **Logon** identifies a user so that the user can log on to the operating system.
- **Screen saver** identifies a user in order to unlock the screen saver.
- **Application execution manager** encrypts the main executable file of a program in order to prevent unauthorized use of the program. If the user is allowed to run the program, application execution manager decrypts the executable and runs it.

UVM does not take the place of the authentication application in performing any actions (such as logon). Instead, UVM determines what authentication is needed to perform the requested action, and then ensures that the required authentication is provided. It is up to the application that makes calls to UVM to perform the actual task.

Summary

The IBM client security hardware and software components provide the user with a means to set up and control cryptographic operations for that client. The IBM client includes the embedded Security Chip where PKI cryptographic operations for the client can be routed. The security software, which can be downloaded from the World Wide Web, is needed to enable and exploit the security hardware. This security software includes support for CAPI/CSP and PKCS#11 cryptographic services; support for initialization and administration of the embedded Security Chip; support for key creation, archiving, and restoration; and support for the management of the security policy for a client through UVM.