Smart Cards

Microsoft Corporation

Updated March 1999

Summary: The Microsoft® Windows® operating system platform is smart card–enabled and is the best and most cost-effective computing platform for developing and deploying smart-card solutions. Smart-card requirements have been incorporated into the PC98 and NetPC design specifications and into future releases of the Microsoft Windows operating system. Microsoft has released its implementation of the PC/SC 1.0 specifications for the Windows NT® 4.0, Windows 95, and Windows 98 operating system platforms. Future releases of the Windows platform will also contain smart-card support as part of the base platform. (8 printed pages)

Introduction

The need for security and enhanced privacy is increasing as electronic forms of identification replace face-to-face and paper-based ones. The emergence of the global Internet and the expansion of the corporate network to include access by customers and suppliers from outside the firewall have accelerated the demand for solutions based on public-key technology. A few examples of the kinds of services that public-key technology enables are secure channel communications over a public network, digital signatures to ensure image integrity and confidentiality, and authentication of a client to a server (and vice versa).

Why Smart Cards

Smart cards are a key component of the public-key infrastructure that Microsoft is integrating into the Windows platform because smart cards enhance software-only solutions, such as client authentication, logon, and secure e-mail. Smart cards are essentially a point of convergence for public-key certificates and associated keys because they:

- provide tamper-resistant storage for protecting private keys and other forms of personal information.

- Isolate security-critical computations, involving authentication, digital signatures, and key exchange from other parts of the system that do not have a need to know.

- Enable portability of credentials and other private information between computers at work, at home, or on the road.

The smart card will become an integral part of the Windows platform because smart cards provide new and desirable features as revolutionary to the computer industry as the introduction of the mouse or CD.

Interoperability

Incompatibility of applications, cards, and readers has been a major reason for the slow adoption of smart cards outside of Europe. Interoperability among different vendors' products is a necessary requirement to enable broad consumer acceptance of smart cards and for corporations to deploy smart cards for use within the enterprise.

ISO 7816, EMV, and GSM

To promote interoperability among smart cards and readers, the International Standards Organization (ISO) developed the ISO 7816 standards for integrated circuit cards with contacts. These specifications focused on interoperability at the physical, electrical, and data-link protocol levels. In 1996, Europay, MasterCard, and VISA (EMV) defined an industry-specific smart card specification that adopted the ISO 7816 standards and defined some additional data types and encoding rules for use by the financial services industry. The European telecommunications industry also embraced the ISO 7816 standards for their Global System for Mobile Communications (GSM) smart card specification to enable identification and authentication of mobile phone users.

While all of these specifications (ISO 7816, EMV, and GSM) were a step in the right direction, each was either too low-level or application-specific to gain broad industry support. Application interoperability issues, such as device-independent APIs, developer tools, and resource sharing were not addressed by any of these specifications.

PC/SC Workgroup

The PC/SC (Personal Computer/Smart Card) Workgroup was formed in May 1996 in partnership with major computer and smart card companies: Groupe Bull, Hewlett-Packard, Microsoft, Schlumberger, and Siemens Nixdorf. The main focus of the workgroup has been to develop specifications that solve these interoperability problems. In December 1997, the workgroup released the first version of the specifications at http://www.smartcardsys.com/.

The PC/SC specifications are based on the ISO 7816 standards and are compatible with both the EMV and GSM specifications. There is broad industry support for the specifications and a strong desire to move them toward becoming independent standards in the future.

Since its founding and initial publication of the specifications, additional members have joined the PC/SC Workgroup. New members include Gemplus, IBM, Sun Microsystems, Toshiba, and Verifone.

Microsoft Approach

The Microsoft approach is simple and consists of the following:

- A standard model for interfacing smart-card readers and cards with computers.

- Device-independent APIs for enabling smart-card-aware applications.

- Familiar tools for software development.

- Integration with all Windows platforms.

Having a standard model for how readers and cards interface with a computer enforces interoperability among cards and readers from different manufacturers. Device-independent APIs insulate application developers from differences between current and future implementations. Device-independence also reduces software development costs by avoiding application obsolescence due to underlying hardware changes.

Software Development

The Smart Card SDK has been integrated into the Microsoft Platform SDK as part of the Windows Base Services. The Platform SDK now contains the necessary tools and APIs to develop smart-card-enabled and smart-card-aware Windows-based applications. The Platform SDK can be obtained from the Microsoft Developer Network (MSDN) at http://msdn.microsoft.com/developer/sdk/default.asp.

In addition, a discussion alias SmartCardSDK@DISCUSS.MICROSOFT.COM has been established to allow developers to post questions and receive answers from Microsoft and the community of developers using the Smart Card APIs. Information on how to join the mailing list can be found at http://msdn.microsoft.com/isapi/gomscom.asp?Target=/windowsce/smartcard/default.asp.

APIs

From the application developer's perspective, there are three mechanisms for accessing the services supported by a smart card: CryptoAPI, the Microsoft Win32® API, and SCard COM. The mechanism chosen depends on the type of application and the capabilities of a specific smart card.

CryptoAPI

CryptoAPI is the cryptographic API for writing a Cryptographic Service Provider (CSP) and requires a separate development kit, available from Microsoft. Information on obtaining the CSP development kit can be found at http://msdn.microsoft.com/isapi/gomscom.asp?Target=/security/default.asp in the Technologies section. The CSP development kit is import and export controlled and requires the developer to answer a series of questions to ascertain whether the development kit can be legally obtained from Microsoft.

The benefits of using CryptoAPI are significant because the developer can take advantage of the cryptographic features integrated into the Windows platform without having to know cryptography or how a particular cryptographic algorithm works. For example, a properly programmed smart card CSP would use an existing CSP (such as Microsoft Base Provider) to perform all public- and symmetric-key operations and use the smart card itself to perform all private-key operations.

SCard COM

SCARD COM is a noncryptographic interface implementation provided by Microsoft for accessing generic smart-card-based services from applications written in different languages, such as C, Microsoft Visual C++®, Java, and Microsoft Visual Basic®. It is comprised of a set of base COM interface objects that can be used to build a richer set of interfaces for use by Windows-based applications. The software developer can use standard development tools, such as Visual C++ and Visual Basic, to develop applications and service providers that are smart-card-enabled and smart-card-aware.

In general, the application developer does not need to know the details of how a particular smart card functions in order to access its services through COM. This abstraction speeds up Windows application development, saving both time and development costs, and protects the application from obsolescence caused by subsequent changes to a card's design.

Win32

The Win32 APIs are the base-level APIs for accessing smart cards and require a deeper understanding of the Windows operating system and smart cards in order to be used effectively. They also provide the most flexibility for the application to control readers, cards, and related components. For developers that need maximum control over an application's use of smart cards, this extension to the base Win32 API provides the necessary interfaces for managing interactions with smart-card devices.

Smart Card Base Components

The Microsoft Smart Card Base Components 1.0 have been released for the Windows 95 and Windows NT 4.0 platforms and are available at http://msdn.microsoft.com/isapi/gomscom.asp?Target=/windowsce/smartcard/default.asp. The Smart Card Base Components 1.0 are also included on the Windows 98 CD-ROM as a separate install. Likewise, Windows 2000 integrates the Smart Card Base Components into the operating system to support public-key services, such as logon.

Service Providers

All cards must have at least one service provider for Windows-based applications to access card-based services. There can be multiple service providers, depending on the type of card and the card issuer. In general, there are two categories of Service Providers: cryptographic and noncryptographic. The distinction is necessary due to import and export restrictions on cryptographic technology imposed by governments.

Cryptographic Service Providers

CSPs can be software-only, like the Microsoft Base Provider CSP that ships standard on Windows platforms today, or they can be part of a hardware-based solution where the cryptographic engine resides on a smart card (or some other piece of hardware) attached to the computer. A CSP associated with a smart card is called a Smart Card Cryptographic Provider (SCCP) to distinguish it from a more general CSP. Both SCCPs and CSPs expose cryptographic services— such as random number generation, key generation, digital signature, key exchange,

and bulk encryption—through CryptoAPI.

Smart Card Service Providers

Smart Card Service Providers (SCSP) expose the noncryptographic services of a smart card to an application through interfaces. A smart card interface consists of a predefined set of services, the protocols necessary to invoke the services, and any assumptions regarding the context of the services. This is similar in concept to the ISO 7816-5 Application Identifier, but differs in scope.

A smart card can register support for an interface through association with the interface's globally unique identifier (GUID). This binding between a card and an interface is done at the time the card is first introduced to the system, typically when the SCSP is installed. Once the card is introduced to the system, applications can search for smart cards, based on a specific interface or GUID. For example, a cash card could make itself available to Windows-based applications by registering interfaces to access its purse scheme.

As part of the Smart Card Base Components 1.0 release, Microsoft shipped several base-level service providers for performing generic operations, such as card location, command and reply APDU (Application Protocol Data Unit) management, and card file system access. The Microsoft-supplied service providers are implemented as COM interface objects to enable software developers and card providers to develop higher-level service providers and applications.

Cards

The term *smart card* has been used to describe a class of credit-card-sized devices with varying capabilities: stored-value cards, contactless cards, and integrated circuit cards (ICC). All of these cards differ in functionality from each other and from the more familiar magnetic stripe cards used by standard credit, debit, and ATM cards. It is the ICC that is of most interest to the computer industry because it is able to perform more sophisticated operations, including signing and key exchange.

To work under the Windows implementation of the PC/SC 1.0 specifications, a smart card must conform physically and electrically to the ISO 7816-1, 7816-2, and 7816-3 standards.

A smart card must first be introduced to Windows, using a vendor-supplied installation program because there is no Plug and Play model for smart cards. There is no standard for encoding a unique identifier within the Answer-to-Reset (ATR) string used to uniquely identify cards of the same type. The card installation software typically installs an associated card service provider that registers its interfaces with the Resource Manager. The Resource Manager then binds the card to the registered interfaces, enabling applications to access card-based services, based on their supported interfaces. A card can also bind to previously registered interfaces of an existing service provider.

Resource Manager

The Resource Manager runs as a trusted service in a single process. All requests for smart-card access go through the Resource Manager and are routed to the smart-card reader containing the requested card. Therefore, the Resource Manager is responsible for managing and controlling all

application access to any smart card inserted into any reader attached to a Windows-based computer. The Resource Manager provides a given application with a virtual direct connection to the requested smart card.

The Resource Manager performs three basic tasks in managing access to multiple readers and cards. First, it identifies and tracks resources. Second, it controls the allocation of readers and resources across multiple applications. Finally, it supports transaction primitives for accessing services available on a specific card. This is important because current cards are single-threaded devices that often require execution of multiple commands to complete a single function. Transaction control allows multiple commands to be executed without interruption, ensuring that intermediate state information is not corrupted.

Device Drivers

A device driver for a specific reader maps the functionality of that reader to the native services provided by the Windows platform and the smart card infrastructure. The reader device driver communicates card insertion and removal events to the Resource Manager and provides data communications capabilities to and from the card by either the T=0 or the T=1 protocols.

A common driver library is included with the Smart Card Base Components 1.0 release for use by developers to simplify device driver development. This shared library supports ISO 7816 and common system functions required for data communication between a smart card and a reader. This is a significant improvement over how smart-card reader device drivers were developed in the past because there are now standard interfaces for developers to rely upon. These common interfaces enable a smart-card reader device driver to be developed in a uniform manner and be accessible to all Windows applications, as opposed to only a select few applications that know how to communicate with a specific reader.

Device Driver Kits

The type of device driver (for example, .vxd or .sys) depends on the targeted Windows platform. Using the standard Device Driver Kit (DDK) for the targeted Windows platform, an OEM or independent hardware vendor (IHV) can develop a device driver for its reader much like it does for any other peripheral. There are separate Smart Card DDKs for each Windows-based platform. They can be obtained from MSDN™ on CD-ROM but cannot be downloaded from the Microsoft Web site. See http://msdn.microsoft.com/default.asp for more information on subscribing to MSDN.

The device driver model for RS-232, PS/2, and PC Card readers varies according to the targeted Windows platform and bus type. With the release of Windows 2000, the device driver model for USB and IEEE 1394 devices will be unified. This device driver model is referred to as the Windows Driver Model (WDM). For more information on WDM, see http://msdn.microsoft.com/isapi/gomscom.asp?Target=/hwdev/desinit/wdm.htm.

Readers

Smart-card readers attach to standard peripheral interfaces, such as RS-232, PS/2, PCMCIA, and Universal Serial Bus (USB). Readers are considered standard Windows devices and carry a security descriptor and Plug and Play identifier. They are controlled through standard Windows

device drivers and are introduced to and removed from the system using the Hardware Wizard that is standard with Windows.

Windows-compatible Logo Program

Readers must conform to the PC97 or PC98 hardware design requirements and to the Microsoft implementation of the PC/SC Workgroup 1.0 specifications. There is a Windows-compatible logo program for smart-card readers available from the Windows Hardware Quality Lab (WHQL), as there is for other peripheral devices. The smart-card reader test kit can be downloaded from the WHQL Web site at http://msdn.microsoft.com/isapi/gomscom.asp?Target=/hwtest/default.asp. The test kit includes several test smart cards (distributed separately) that are used to determine whether a reader meets the requirements to receive the Windows-compatible logo. Smart-card readers must also meet Windows platform requirements including Plug and Play and Power Management requirements to qualify for the Windows-compatible logo.

Enhanced Solutions

By enhancing software-only solutions, such as client authentication and secure messaging, smart cards enable a new breed of applications positioned to take advantage of future opportunities in the emerging global digital economy. Smart cards offer application developers a secure mechanism for enhancing solutions aimed at both enterprise and the consumer.

Client Authentication

Client authentication involves identification and validation of a client to a server to establish a secure communications channel. A secure protocol, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), is typically used in conjunction with a trusted public-key certificate provided by the client that identifies the client to the server. The client could be the Internet Explorer running on a Windows platform, and the server could be Microsoft Internet Information Service (or some other Web server that supports SSL/TLS).

The secure session is established using public-key authentication with key exchange to derive a unique session key that can then be used to ensure data integrity and confidentiality throughout the session. Additional authentication can be achieved by mapping the certificate to a user or group account with previously established access-control privileges. The smart card enhances the public-key authentication process by serving as a secure store for the private-key material and as a cryptographic engine for performing a digital signature or key-exchange operation.

Microsoft has provided information at http://msdn.microsoft.com/isapi/gomscom.asp?Target=/security/default.asp under Resources that describes the use of certificates and guidelines for public certificate authorities.

Public Key Interactive Logon

In the past, interactive logon has meant the ability to authenticate a user to a network, using a form of shared credential, such as a hashed password. Windows 2000 supports public-key interactive logon, using a X.509 version 3 certificate stored on a smart card along with the

private key. Instead of a password, the user inputs a Personal Identification Number (PIN) to the Graphical Identification and Authentication (GINA) ; the PIN is used to authenticate the user to the card.

The user's public-key certificate is retrieved from the card through a secure process and verified to be valid and from a trusted issuer. During the authentication process, a challenge, based on the public key contained in the certificate, is issued to the card to verify that the card is indeed in possession of and can successfully use the corresponding private key. After successful verification of the public-private key pair, the user's identity contained in the certificate is used to reference the user object stored in the Active Directory to build a token and return a Ticket-Granting Ticket (TGT) to the client. Public key logon has been integrated with the Microsoft implementation of Kerberos version 5 that is compatible with the public-key extension specified in the IETF draft RFC-1510

Secure E-mail

Secure e-mail is one of the more exciting public-key-enabled applications because it allows users to share information confidentially and to trust that the integrity of the information was maintained during transit. Using Microsoft Outlook™ Express or Outlook 98, a user can select a public-key certificate issued by a trusted certificate authority to use for digitally signing and decrypting secure messages. By publishing the user's certificate to a public directory in the enterprise or on the Internet, other users within a company or on the Internet can send encrypted e-mail to the user, and visa-versa.

A smart card adds a level of integrity to secure e-mail applications because it stores the private key on the card, protected by a PIN. In order to compromise the private key and send signed e-mail as someone else, someone would have to obtain the user's smart card and the PIN. The PIN could someday be replaced with a biometric template of the user's fingerprint, thus enhancing the nonrepudiation aspects of digitally signed e-mail.

Additional References

Documents

Microsoft CryptoAPI and other public-key technologies:
http://msdn.microsoft.com/isapi/gomscom.asp?Target=/security/default.asp

"Microsoft 'Zero Administration' Initiative for Windows":
http://msdn.microsoft.com/isapi/gomscom.asp?Target=/windows/platform/info/zawmb.htm

NetPC:
http://msdn.microsoft.com/isapi/gomscom.asp?Target=/Windows/platform/Innovate/NetPC/default.asp

PC98/99 Design Guide:
http://msdn.microsoft.com/isapi/gomscom.asp?Target=/HWDEV/xpapers/PC99/default.htm

PC/SC Workgroup Members

Bull CP8:
http://www.bull.com

Gemplus:
http://www.gemplus.com

Hewlett-Packard:
http://www.hp.com

IBM:
http://www.chipcard.ibm.com

Microsoft:
http://msdn.microsoft.com/isapi/gomscom.asp?Target=/ms.htm

Schlumberger:
http://www.slb.com

Siemens Nixdorf:
http://www.sni.de

Sun Microsystems:
http://www.sun.com

Toshiba:
http://www.toshiba.com

Verifone:
http://www.verifone.com

For More Information

For the latest information on Windows 2000 or Windows NT Server, visit the Web site at http://msdn.microsoft.com/isapi/gomscom.asp?Target=/ntserver/default.asp or the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

Microsoft Corporation · One Microsoft Way · Redmond, WA 98052-6399 · USA