Sistema operativo

Tarjetas inteligentes

Resumen

La plataforma del sistema operativo Microsoft® Windows® está habilitada para tarjeta inteligente y es la mejor y más rentable plataforma de cómputo para desarrollar e implementar soluciones de tarjeta inteligente. Se han incorporado los requisitos de tarjeta inteligente a las especificaciones de diseño de PC 98 y NetPC y a las futuras versiones del sistema operativo Windows de Microsoft. La compañía ha lanzado su implementación de las especificaciones PC/SC 1.0 para las plataformas del sistema operativo Windows NT 4.0, Windows 95 y Windows 98. Las futuras versiones de la plataforma Windows también darán soporte de tarjeta inteligente como parte de la plataforma base.

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

0399

TABLA DE CONTENIDOS

INTRODUCCION 1

¿POR QUE TARJETAS INTELIGENTES? 2

INTEROPERABILIDAD 3

ISO 7816, EMV y GSM 3

Grupo de trabajo PC/SC 3

El enfoque de Microsoft 4

DESARROLLO DE SOFTWARE 5

Interfaces de programación de aplicación 5

CryptoAPI 5

SCard COM 5

Win32 6

SMART CARD BASE COMPONENTS 7

Los proveedores de servicios 7

Los proveedores de servicios criptográficos (CSPs) 7

Proveedores de servicios de tarjetas inteligentes 7

Tarjetas 8

Administrador de recursos 8

Controladores de dispositivo 9

Estuche del controlador de dispositivos 9

Lectores 10

Programa de logotipo "compatible con Windows" 10

SOLUCIONES MEJORADAS 11

Autenticación del cliente 11

Conexión interactiva de clave pública 11

Correo electrónico seguro 12

REFERENCIAS ADICIONALES 13

Recursos 13

Documentos 13

Para mayores informes 14

INTRODUCCION

La necesidad por una mayor seguridad y privacidad es cada vez más importante a medida que las formas electrónicas de identificación reemplazan las formas físicas y documentales. El surgimiento de Internet global y la expansión de la red corporativa para incluir acceso por parte de clientes y proveedores desde afuera del *firewall*, ha acelerado la demanda de soluciones basadas en tecnología de clave pública. Algunos de estos tipos de servicios que habilitan las tecnologías de clave pública son las comunicaciones de canal seguro sobre una red pública, firmas digitales para asegurar la integridad de la imagen y confidencialidad, y la autenticación de un cliente a un servidor (y viceversa).

¿POR QUE TARJETAS INTELIGENTES?

Las tarjetas inteligentes son un componente clave de la infraestructura de clave pública que Microsoft esta integrando en la plataforma de Windows debido a que las tarjetas inteligentes mejoran las soluciones únicamente de software tales como autenticación, conexión y correo electrónico seguro. Las tarjetas inteligentes son esencialmente un punto de convergencia para certificados de clave pública y claves asociadas, ya que proporcionan:

- Almacenamiento resistente a intromisiones para proteger las claves privadas y otras formas de información personal.
- Aislar cómputos críticos de seguridad que impliquen autenticación, firmas digitales e intercambio de claves de otras partes del sistema que no tengan una necesidad "de saber".
- Permitir la portabilidad de credenciales y de otra información privada entre computadoras en el trabajo, el hogar o el camino.

La tarjeta inteligente será parte integral de la plataforma Windows debido a que habilitará nuevas clases de aplicaciones de la misma forma que el ratón y el CD-ROM lo hicieron cuando se integraron por primera vez con la computadora personal (PC).

INTEROPERABILIDAD

La incompatibilidad entre aplicaciones, tarjetas y lectores ha sido una razón principal en la adopción lenta de las tarjetas inteligentes fuera de Europa. La interoperabilidad entre los productos de diferentes proveedores es un requisito necesario para obtener una amplia aceptación de los consumidores de las tarjetas inteligentes, y para que las empresas implementen tarjetas inteligentes para uso dentro de la empresa.

ISO 7816, EMV y GSM

Para promover la interoperabilidad entre tarjetas inteligentes y lectores, la organización internacional de normatividad (ISO) desarrolló la norma ISO 7816 para tarjetas de circuito integrado con contactos. Estas especificaciones se enfocaron en la interoperabilidad a nivel físico, eléctrico y protocolo de enlace de datos. En 1996, las empresas Europay, MasterCard y VISA (EMV) definieron una especificación de tarjeta inteligente específica de esa industria que adoptó la norma ISO 7816 y definió algunos tipos de datos adicionales y reglas de codificación a ser utilizados por la industria de servicios financieros. La industria europea de telecomunicaciones también adoptó la norma ISO 7816 con el fin de especificar su tarjeta inteligente del sistema global para comunicaciones móviles (GSM) y permitir así, la identificación y autenticación de usuarios de teléfono móvil.

Mientras que todas estas especificaciones (ISO 7816, EMV y GSM) fueron un paso en la dirección correcta, cada una fue ya sea o muy detallada o específica de una aplicación para obtener amplio soporte de otras industrias. Los asuntos relacionados con la interoperabilidad de las aplicaciones tales como APIs, independientes de dispositivo, herramientas del desarrollador, y compartir recursos no fueron abordados por ninguna de estas especificaciones.

Grupo de trabajo PC/SC

El Grupo de trabajo PC/SC (computadora personal/tarjeta inteligente) se formó en mayo de 1996 con la participación de las principales compañías de tarjetas inteligentes y PCs: Grupo Bull, Hewlett-Packard, Microsoft, Schlumberger y Siemens Nixdorf. El enfoque principal del Grupo de trabajo ha sido desarrollar especificaciones que resuelvan los problemas de interoperabilidad previamente mencionados. En diciembre de 1997, el Grupo de trabajo sacó al mercado la versión 1.0 de las especificaciones en http://www.smartcardsys.com/.

Las especificaciones de PC/SC se basan en la norma ISO 7816 y son compatibles con las especificaciones EMV y GSM específicas de la industria. En virtud de las compañías implicadas en el Grupo de trabajo PC/SC, existe un amplio soporte de industria para las especificaciones y un fuerte deseo de moverlas en el futuro hacia una ruta independiente de normas.

Desde su fundación y publicación inicial de las especificaciones, se han unido miembros adicionales al Grupo de trabajo PC/SC. Los nuevos miembros incluyen Gemplus, IBM, Sun Microsystems, Toshiba y Verifone.

El enfoque de Microsoft

El enfoque de Microsoft es simple y consiste en lo siguiente:

- Un modelo estándar para intercomunicar a los lectores de tarjetas inteligentes y tarjetas con las PCs.
- APIs independientes de los dispositivos para habilitar aplicaciones conscientes de las tarjetas inteligentes.
- Herramientas familiares para el desarrollo de software.
- Integración con las plataformas Windows y Windows NT.

Al tener un modelo estándar de la manera en que los lectores y las tarjetas hacen interfaz con las PCs, se instrumenta la interoperabilidad entre los lectores y las tarjetas de diferentes fabricantes. Las APIs independientes de dispositivo sirven para separar a los desarrolladores de aplicaciones de las diferencias que puedan surgir entre las instalaciones actuales y futuras. La independencia respecto a dispositivos también conserva los costos de desarrollo de software evitando que la aplicación caiga en desuso debido a cambios de hardware fundamentales.

DESARROLLO DE SOFTWARE

El SDK de la tarjeta inteligente se ha integrado al SDK de la plataforma de Microsoft como parte de los servicios básicos de Windows. El SDK de la plataforma ahora contiene las herramientas necesarias y la interfaz de programación de aplicación (API) que se requiere para desarrollar aplicaciones Windows habilitadas y conscientes de la tarjeta inteligente. El SDK de la plataforma se puede obtener de Microsoft Developer Network (MSDN) en http://msdn.microsoft.com/developer/sdk.

Además, un análisis llamado SmartCardSDK@DISCUSS.MICROSOFT.COM se ha establecido para permitir que los desarrolladores formulen preguntas y reciban respuestas de Microsoft y de la comunidad de desarrolladores que usan las APIs para tarjetas inteligentes. La información de cómo unirse a la lista de correo puede encontrarse en http://www.microsoft.com/smartcard/.

Interfaces de programación de aplicación

Desde la perspectiva del desarrollador de aplicaciones existen tres mecanismos para acceder a los servicios soportados por una tarjeta inteligente: CryptoAPI, Microsoft Win32® API y SCard COM. El mecanismo elegido dependerá del tipo de aplicación y de las capacidades de una determinada tarjeta inteligente.

CryptoAPI

CryptoAPI es una API criptográfica para escribir un Proveedor de servicios criptográficos (CSP) y requiere un estuche de desarrollo separado y disponible en Microsoft. La información para obtener un equipo de desarrollo CSP puede encontrarse en http://www.microsoft.com/security/ en la sección de *Tecnologías*. El estuche de desarrollo CSP esta controlado para exportación/importación y requiere que el desarrollador conteste una serie de preguntas para averiguar si el estuche de desarrollo puede obtenerse legalmente de Microsoft.

Los beneficios de usar CryptoAPI son importantes ya que el desarrollador puede aprovechar las funciones criptográficas que se integran en la plataforma Windows sin tener que saber criptografía o cómo funciona un determinado algoritmo criptográfico. Por ejemplo, una tarjeta inteligente de CSP de buen comportamiento usaría un CSP existente (tal como Microsoft Base Provider) para ejecutar todas las operaciones de clave pública y simétrica y usar la tarjeta inteligente para llevar a cabo todas las operaciones de clave privada.

SCard COM

SCARD COM es una implementación de interfaz no criptográfica proporcionada por Microsoft para acceder a los servicios genéricos de tarjeta inteligente de aplicaciones escritas en diferentes lenguajes tales como C, C++, Java y el sistema de desarrollo Microsoft Visual Basic®. Se compone de un conjunto de objetos base de interfaz COM que puede usarse para construir una serie más completa de interfaces que sean utilizadas por aplicaciones basadas en Windows. El desarrollador de software puede usar herramientas de desarrollo estándar tales como los sistemas de desarrollo Microsoft Visual C++® y Visual Basic para desarrollar aplicaciones y

proveedores de servicio que están habilitados y funcionan con tarjetas inteligentes.

En términos generales, el desarrollador de aplicaciones no necesita saber los detalles de cómo funciona una tarjeta inteligente en particular para acceder a sus servicios a través de COM. Esta abstracción acelera el desarrollo de aplicaciones Windows, ahorrando tanto tiempo como costos de desarrollo, y protege la aplicación de caer en desuso debido a cambios subsecuentes en el diseño de la tarjeta.

Win32

Las APIs de Win32 son las APIs de nivel base para acceder a tarjetas inteligentes y requieren un conocimiento más profundo del sistema operativo Windows y tarjetas inteligentes para poderlas utilizar de manera eficiente. También proporcionan la mayor flexibilidad para que la aplicación controle los lectores, tarjetas y componentes relacionados. Para desarrolladores que necesitan un máximo control sobre el uso de las tarjetas inteligentes por parte de la aplicación, esta extensión a la API Win32 base, proporciona las interfaces necesarias para administrar interacciones con dispositivos de tarjeta inteligente.

SMART CARD BASE COMPONENTS

Microsoft ha salido a la venta para las plataformas Windows 95 y Windows NT 4.0 y están disponibles en http://www.microsoft.com/smartcard/. Smart Card Base Components 1.0 también se incluirán en el CD-ROM Windows 98 como una instalación separada. De la misma manera, Windows 2000 integrará Smart Card Base Components al sistema operativo para soportar los servicios de clave pública tales como colección.

Los proveedores de servicios

Todas las tarjetas deben tener por lo menos un proveedor de servicio para que las aplicaciones basadas en Windows accedan a los servicios de tarjeta. Puede haber múltiples proveedores de servicio dependiendo del tipo de tarjeta y del emisor de tarjeta. En general, hay dos categorías de proveedores de servicios: el criptográfico y el no criptográfico, la distinción es necesaria debido a las restricciones de exportación/importación sobre tecnología criptográfica impuesta por los gobiernos.

Los proveedores de servicios criptográficos (CSPs)

Los CSPs pueden ser únicamente de software como el Microsoft Base Provider CSP que se incluye en forma estándar en todas las plataformas Windows actuales, o puede ser parte de una solución basada en hardware donde el motor criptográfico reside en la tarjeta inteligente (o alguna otra pieza del hardware) agregada a la PC. Un CSP asociado con una tarjeta inteligente se llama Proveedor criptográfico de tarjeta inteligente (SCCP) para distinguirlo de un CSP general. Los SCCPs y los CSPs exponen servicios criptográficos a través de CriptoAPI tales como generación al azar del número, generación de clave, firma digital, intercambio de claves y encriptación a destajo.

Proveedores de servicios de tarjetas inteligentes

Los proveedores de servicios de tarjetas inteligentes (SCSP) exponen los servicios no criptográficos de una tarjeta inteligente a una aplicación a través de *interfaces*. La interfaz de una tarjeta inteligente consiste en una serie de servicios predefinidos, los protocolos necesarios para llamar los servicios y cualquier aseveración con respecto al contexto de los servicios. El término *interfaz* se usa de manera muy similar a la forma en que se utiliza en COM. Note que este concepto es similar al identificador de aplicación ISO 7816-5 pero difiere en alcance.

Una tarjeta inteligente puede registrar soporte para una interfaz a través de la asociación con el identificador único global (GUID) de la interfaz. Esta unión entre la tarjeta y la interfaz se realiza al momento en que la tarjeta se introduce por primera vez en el sistema cuando generalmente el SCSP se instala. Un proveedor de servicios de tarjeta registra sus interfaces en el momento que se introduce la tarjeta al sistema, habilitando entonces a las aplicaciones para registrar las tarjetas inteligentes basadas en la interfaz específica o GUID. Por ejemplo, una tarjeta de efectivo podría hacerse disponible en las aplicaciones basadas en Windows al registrar interfaces para acceder a su esquema de monedero.

Como parte de la versión Smart Card Base Components 1.0, Microsoft incluye varios proveedores de servicio a nivel base para llevar a cabo operaciones genéricas tales como la ubicación de tarjeta, administración de la APDU (Unidad de datos de protocolo de aplicación) de comando/respuesta y acceso al sistema de archivos de tarjeta. Los proveedores de servicio proporcionados por Microsoft se implementan como objetos de interfaz COM para permitir a los desarrolladores de software y proveedores de tarjetas desarrollar aplicaciones y proveedores de servicio de más alto nivel.

Tarjetas

El término *tarjeta inteligente* se ha usado para describir una clase de dispositivos del tamaño de una tarjeta de crédito con diferentes capacidades: tarjetas de valor almacenado, tarjetas sin contacto y tarjetas de circuito integrado (ICC). Todas estas tarjetas difieren en funcionalidad entre sí y de las tarjetas de cinta magnética más familiares utilizadas por las tarjetas estándar de crédito, débito y cajero automático. El ICC es la parte más interesante para la PC debido a que puede llevar a cabo operaciones más sofisticadas que incluyen intercambio de claves y firmas.

Para trabajar bajo la implementación de Windows de las especificaciones PC/SC 1.0, una tarjeta inteligente debe ajustarse física y eléctricamente a las normas ISO 7816-1, 7816-2 y 7816-3.

Una tarjeta inteligente debe introducirse primero a Windows usando un programa de instalación proporcionado por el proveedor ya que no hay modelo *Plug-and-Play* para tarjetas inteligentes. No hay modelo *Plug-and-Play* para tarjetas inteligentes debido a que no existe una norma para codificar un identificador único dentro de la extensión *Answer To Reset* (ATR) que se utiliza para identificar de manera exclusiva a tarjetas que son del mismo tipo. El software de instalación de tarjeta normalmente instalaría un proveedor de tarjetas asociado que registre sus interfaces con el administrador de recursos. El administrador de recursos relacionaría la tarjeta a las interfaces registradas, permitiendo que las aplicaciones tengan acceso a los servicios basados en tarjeta en sus interfaces que soportan. También es posible que una tarjeta se conecte a interfaces previamente registradas de un proveedor de servicios existente.

Administrador de recursos

El Administrador de recursos se ejecuta como un servicio confiable en un proceso simple. Todas las peticiones para el acceso de la tarjeta inteligente pasan a través del Administrador de recursos y se enrutan al lector de tarjeta inteligente que contiene la tarjeta solicitada. Por lo tanto, el Administrador de recursos es responsable de controlar y administrar todo el acceso de las aplicaciones a cualquier tarjeta inteligente que se inserte en cualquier lector conectado a una PC basada en Windows. El Administrador de recursos proporciona una aplicación determinada con una conexión directa *virtual* a la tarjeta inteligente solicitada.

El Administrador de recursos soluciona tres problemas básicos al administrar el

acceso a múltiples tarjetas y lectores. Primero, es responsable de identificar y rastrear los recursos. Segundo, es responsable de controlar la distribución de lectores y recursos a través de las múltiples aplicaciones. Finalmente, soporta primitivas de transacciones para acceder a los servicios disponibles en una tarjeta determinada. Este es un punto importante porque las tarjetas actuales son dispositivos de un solo hilado que frecuentemente requieren ejecución de múltiples comandos para completar una sola función. El control de transacción permite que varios comandos se ejecuten sin interrupción, asegurando que la información de estado intermedio no se dañe.

Controladores de dispositivo

Un controlador de dispositivo para un lector específico correlaciona la funcionalidad del lector con los servicios nativos proporcionados por la plataforma Windows y la infraestructura de tarjeta inteligente. Es responsabilidad del controlador de dispositivo del lector comunicar los eventos de remoción e inserción de la tarjeta al Administrador de recursos, y proporcionar capacidades de comunicaciones de datos desde y hacia la tarjeta por los protocolos de T=0 ó T=1.

Una biblioteca de controlador común se incluye con Smart Card Base Components 1.0 para uso por los desarrolladores con el objeto de simplificar el desarrollo de controladores de dispositivo. Esta biblioteca compartida soporta ISO 7816 y las funciones de sistema comunes que se requieren para la comunicación de datos entre una tarjeta inteligente y un lector. Esta es una mejora importante sobre la forma en que se han desarrollado en el pasado los controladores de dispositivos de lectores de tarjetas inteligentes ya que ahora existen *interfaces* estándar en las que pueden depender los desarrolladores. Tales interfaces comunes habilitan a un controlador de dispositivo de lectores de tarjetas inteligentes para que se desarrollen de manera uniforme y sean accesibles a todas las aplicaciones Windows, a diferencia de únicamente unas cuantas aplicaciones seleccionadas que saben cómo comunicarse con un lector determinado.

Estuche del controlador de dispositivos

El tipo de controlador de dispositivo (por ejemplo: .vxd, .sys) dependerá de la plataforma Windows objetivo: Windows o Windows NT. Al utilizar el estuche de controlador de dispositivos estándar (DDK) para la plataforma Windows objetivo, un fabricante de equipo original (OEM) o proveedor de hardware independiente (IHV) pueden desarrollar un controlador de dispositivo para su lector de la misma manera que lo hace para cualquier otro periférico de la PC. Existe un DDK de tarjeta inteligente separado para Windows y otro para Windows NT. Ambos se pueden obtener de MSDN™ en CD-ROM mas no se pueden descargar del sitio Web de Microsoft. Visite http://www.microsoft.com/developer para mayores informes sobre cómo suscribirse a MSDN.

El modelo de controlador de dispositivo para lectores RS-232, PS/2 y PC Card varía de acuerdo con la plataforma Windows objetivo y el tipo de *bus*. Con la nueva versión de Windows y Windows NT, se unificará el modelo de controlador de

dispositivo para dispositivos USB e IEEE 1394. Este modelo de controlador de dispositivo se conoce como el Modelo de controlador Win32 (WDM). Para mayores informes sobre WDM, consulte http://www.microsoft.com/hwdev/pcfuture/wdm.htm.

Lectores

Los lectores de tarjeta inteligente se unen a las interfaces periféricas estándar de la PC tales como RS-232, PS/2, PCMCIA, y (en el futuro) el Bus serial universal (USB). Los lectores se consideran dispositivos Windows estándar, y como tales incluyen un identificador *Plug-and-Play* y un descriptor de seguridad. Se controlan a través de los controladores de dispositivos Windows estándar y se introducen y remueven del sistema utilizando el Asistente de hardware, que es estándar, con el sistema operativo Windows y Windows 2000.

Programa de logotipo "compatible con Windows"

Los lectores deben ajustarse a los requisitos de diseño de hardware PC 97 ó PC 98 y a la implementación de Microsoft de las especificaciones PC/SC Workgroup 1.0. Existe un programa de logotipo "compatible con Windows" para los lectores de tarjeta inteligente disponible del laboratorio de calidad de hardware para Windows (WHQL), al igual que para otros dispositivos periféricos. El estuche de prueba para lectores de tarjeta inteligente se puede descargar del sitio Web WHQL en http://www.microsoft.com/hwtest/. Este estuche de prueba incluye varias tarjetas inteligentes de prueba (distribuidas por separado) que se usan para determinar si el lector cubre los requisitos para recibir el logotipo "compatible con Windows". Los lectores de tarjetas inteligentes también deben satisfacer los requisitos de plataforma de Windows incluyendo *Plug and Play* de administración de energía para poder calificar para el logotipo "compatible con Windows".

SOLUCIONES MEJORADAS

Al mejorar las soluciones únicamente de software como mensajería segura y autenticación de cliente, las tarjetas inteligentes permiten que una nueva generación de aplicaciones se posicionen para aprovechar las oportunidades futuras en la economía digital global emergente. Las tarjetas inteligentes ofrecen un mecanismo seguro a los desarrolladores de aplicaciones para mejorar soluciones dirigidas al espacio de consumidor y empresarial.

Autenticación del cliente

La autenticación del cliente implica la identificación y validación del mismo a un servidor para establecer un canal seguro de comunicaciones. Un protocolo seguro tal como el Nivel de Socket seguro (SSL) o Seguridad en el nivel de transporte (TLS) se utiliza generalmente junto con un certificado de clave pública confiable proporcionado por el cliente que identifica a éste con el servidor. El cliente podría ser Internet Explorer ejecutándose en Windows o Windows NT y el servidor podría ser Internet Information Server (o algún otro servidor del Web que soporte SSL/TLS).

La sesión segura se establece usando la autenticación de clave pública con el intercambio de claves para derivar una clave de sesión única la cual puede usarse después para asegurar la integridad de los datos y la confidencialidad durante la sesión. Se puede lograr autenticación adicional al correlacionar la información del certificado con una cuenta de usuario o grupo con privilegios de control de acceso previamente establecidos. La tarjeta inteligente mejora el proceso de autenticación de clave pública al fungir como un almacén seguro para el material de clave privada y un motor criptográfico para llevar a cabo la firma digital o la operación de intercambio de claves.

Microsoft ha establecido un servidor de certificado de prueba disponible en Internet en http://sectest.microsoft.com/ para que los desarrolladores lo utilicen para propósitos de prueba y muestra. Además, hay información en http://www.microsoft.com/security dentro de la pestaña Recursos que describe el uso de los certificados y los lineamientos para las autoridades de certificados públicos de Microsoft.

Conexión interactiva de clave pública

En el pasado, la conexión interactiva significaba la habilidad de autenticar un usuario a una red usando una forma de credencial compartida tal como una contraseña verificada. Windows 2000 soportará la conexión interactiva de clave pública usando un certificado X.509v3 que esta almacenado en una tarjeta inteligente junto con la clave privada. En lugar de una contraseña, el usuario registra un número de identificación personal (NIP) en la identificación gráfica y autenticación (GINA) que se usa subsecuentemente para autenticar al usuario con la tarjeta.

El certificado de clave pública del usuario se recupera de la tarjeta a través de un proceso seguro y se verifica su validez y que sea de un emisor confiable. Durante el proceso de autenticación se emite un *challenge,* basado en la clave pública

contenida en el certificado, a la tarjeta para verificar que la tarjeta en realidad posea la clave privada correspondiente y pueda utilizarla con éxito. Después de una verificación minuciosa del par de claves privada y pública, la identidad del usuario contenida en el certificado se utiliza para hacer referencia al objeto de usuario almacenado en Active Directory para construir una contraseña y regresar al cliente *Ticket Granting Ticket* (TGT). La conexión de clave pública ha sido integrada con la implementación de Kerberos v5 de Microsoft que es compatible con la extensión de clave pública especificada en el esquema RFC-1510 de IETF.

Correo electrónico seguro

El correo electrónico seguro es una de las aplicaciones más emocionantes y habilitadas por la clave pública debido a que permite que los usuarios compartan información de manera confidencial y confíen en que la integridad de la información se mantuvo durante el tránsito. Al utilizar Microsoft Outlook™ Express o el cliente de colaboración y mensajes de Outlook 98, un usuario puede seleccionar un certificado de clave pública emitido por una autoridad de certificados de confianza que se use para firmar digitalmente y descifrar mensajes seguros. Al publicar el certificado del usuario en un directorio público en la empresa o en Internet, otros usuarios dentro de una compañía o en Internet pueden enviar correo electrónico encriptado al usuario, y viceversa.

Una tarjeta inteligente agrega un nivel de integridad a aplicaciones de correo electrónico seguro ya que almacena la clave privada en la tarjeta, la cual es protegida por un NIP. Para comprometer la clave privada y enviar correo electrónico firmado como otra persona, uno necesitaría obtener la tarjeta inteligente del usuario y el NIP. En el futuro, uno podría imaginar que el NIP será reemplazado algún día con una plantilla biométrica de la huella digital del usuario, por lo tanto mejoraría a su vez los aspectos de correo electrónico digitalmente firmado que no sean repudiados.

REFERENCIAS ADICIONALES

Recursos

Microsoft Test Certificate Server:

http://sectest.microsoft.com/

Documentos

Microsoft CryptoAPI y otras tecnologías de clave pública:

http://www.microsoft.com/security/

Iniciativa de Cero administración de Microsoft para Windows:

http://www.microsoft.com/windows/platform/info/zawmb.htm

NetPC:

http://www.microsoft.com/windows/netpc/default.htm

Guía de diseño de PC98:

http://www.microsoft.com/hwdev/

Miembros del Grupo de trabajo PC/SC

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://www.microsoft.com

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

Para mayores informes

Para la información más reciente de Windows 2000 o Windows NT Server, verifique nuestro sitio en el World Wide Web en http://www.microsoft.com/ntserver o en el Foro de Windows NT Server de Microsoft (GO WORD: MSNTS).