Microsoft

Sistema operativo

Operación de red segura con el uso de los servicios de seguridad distribuida de Windows 2000

Resumen

En la actualidad, Microsoft® Windows NT® Server ofrece excelentes servicios de seguridad para la administración de cuentas y autenticación de red dentro de una empresa. Las grandes organizaciones requieren flexibilidad para delegar la administración de cuentas y manejar dominios complejos. La seguridad de Internet está relacionada con el manejo del desarrollo de la tecnología de seguridad de clave pública que debe estar integrada con la seguridad Windows. Para cumplir estas necesidades cada vez mayores, Microsoft ha desarrollado los Servicios de seguridad distribuida de Windows 2000.

Este documento examina los componentes de los Servicios de seguridad distribuida de Windows 2000 y proporciona detalles sobre su implementación.

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

0399

TABLA DE CONTENIDOS

INTRODUCCION

El sistema operativo Microsoft® Windows NT® cuenta con excelentes funciones de seguridad para una empresa. Un solo acceso al dominio de Windows NT permite que el usuario acceda a los recursos que se encuentran en cualquier parte de una red corporativa. Las herramientas del administrador fáciles de utilizar para la política de seguridad y administración de cuentas reducen los costos de implementación de Windows NT. El modelo de dominio Windows NT es flexible y soporta una amplia gama de configuraciones de red, desde un solo dominio en una ubicación a dominios multimaestros que hay en todo el mundo.

Asimismo, Windows NT sienta las bases para una seguridad integrada para la familia BackOffice® de servicios de aplicación, incluyendo Microsoft Exchange, SQL Server™, SNA Server y Microsoft Systems Management Server. El modelo de seguridad de Windows NT brinda una marco sólido para la instalación de aplicaciones cliente/servidor para la empresa. En la actualidad, las empresas utilizan cada vez más Internet. Los negocios necesitan interactuar con socios, proveedores y clientes, utilizando las tecnologías basadas en Internet. La seguridad es un punto muy importante para controlar el acceso a los recursos de una red empresarial, intranets y servidores basados en Internet.

Cada vez más, las Intranets se están convirtiendo en la manera más eficaz de compartir información para las diversas relaciones empresarial. Ahora, el acceso a la información de negocios no pública por partes externas, se controla a través de la creación de cuentas de usuario para aquellos que forman parte de la amplia familia empresarial. Las asociaciones ayudan a definir las relaciones de confianza que alguna vez se aplicaron únicamente a los empleados que utilizaban activos corporativos, pero que ahora incluyen a más personas.

Asimismo, las tecnologías de seguridad también cambian continuamente. Los certificados de clave pública y contraseñas dinámicas son dos áreas de la tecnología que van en aumento con el fin de cumplir con las necesidades de seguridad de nivel más alto del ambiente actual. El acceso remoto sobre las redes públicas y el acceso a Internet para la comunicación de negocios interna están controlando la evolución de la tecnología de seguridad. La arquitectura de seguridad de Windows NT tiene una posición privilegiada para aprovechar estos y otros avances tecnológicos. Windows NT combina la facilidad de uso, excelentes herramientas de administración y una infraestructura de seguridad sólida, que soporta tanto a la empresa como a Internet.

Aspectos importantes

La Seguridad distribuida de Windows 2000 cuenta con varias funciones para simplificar la administración del dominio, mejorar el rendimiento, e integrar la tecnología de seguridad de Internet con base en la criptografía de clave pública. Los aspectos importantes de los Servicios de seguridad distribuida de Windows 2000 incluyen:

- La integración con Windows 2000 Active Directory con el fin de proporcionar una administración de cuenta escalable y flexible para grandes dominios, con control de acceso granular y delegación de administración.
- Protocolo de autenticación Kerberos versión 5, un estándar de seguridad en Internet maduro, el cual ha sido implementado como el protocolo predeterminado para la autenticación de red; sienta las bases para la interoperabilidad de la autenticación.
- Autenticación sólida mediante el uso de certificados de clave pública, canales seguros basados en el Nivel de *sockets* de seguridad (SSL) 3.0 y CryptoAPI para proporcionar protocolos estándar en la industria para la integridad y privacidad de datos a través de redes

públicas.

Este documento describe la siguiente generación de seguridad distribuida de Windows, la cual proporciona las funciones para soportar las demandas empresariales basadas en Internet. La mayor parte del material que aquí se describe se proporciona en Windows 2000, aunque algunas de sus funciones ya han sido implementadas en Windows NT 4.0, como se describe en el texto.

SERVICIOS DE SEGURIDAD DISTRIBUIDA DE WINDOWS 2000

Existen diversas áreas en las cuales se está adaptando la seguridad en Windows 2000 para soportara las empresas basadas en Internet. Algunos de estos cambios reflejan los avances en el soporte que se proporciona a grandes organizaciones por medio del uso de Windows 2000 Active Directory jerárquico. Otros cambios aprovechan la flexibilidad de la arquitectura de seguridad de Windows para integrar la autenticación, utilizando certificados de clave pública de Internet.

A continuación se presenta una lista de las nuevas funciones de seguridad Windows 2000:

- Active Directory proporciona almacenaje para toda la información relativa a políticas de seguridad de dominios e información de cuentas. Active Directory, el cual provee duplicación y disponibilidad de información de cuenta a múltiples Controladores de dominio, está disponible para la administración remota.
- Active Directory soporta un espacio de nombre jerárquico para el usuario, grupo e información de cuenta de la computadora. Las cuentas se pueden agrupar según las unidades organizacionales, en lugar de hacerlo según el espacio del nombre de la cuenta de dominio proporcionado en versiones anteriores de Windows NT.
- Se pueden delegar derechos del administrador para crear y administrar cuentas del usuario o de grupo a nivel de unidades organizacionales. Los derechos de acceso se pueden otorgar a propiedades individuales en objetos del usuario, con el fin de permitir, por ejemplo, que una persona o grupo específicos tenga derecho a restablecer contraseñas, pero no a modificar otra información de la cuenta.
- La duplicación de Active Directory permite actualizaciones a las cuentas en cualquier controlador de dominio, y no únicamente para el controlador de dominio primario (PDC). Se actualizan y sincronizan de manera automática réplicas maestras múltiples de Active Directory en otros controladores de dominio, los cuales se conocen como controladores de dominio de respaldo (BDC).
- Windows 2000 emplea un nuevo modelo de dominio que utiliza Active Directory para soportar un árbol de dominios jerárquico de niveles múltiples. La administración de relaciones de confianza entre dominios se simplifica a través de *trusts* transitorios a lo largo de los árboles que cubren todo el árbol del dominio.
- La seguridad de Windows incluye nueva autenticación basada en los protocolos de seguridad estándar de Internet, incluyendo Kerberos versión 5 y Seguridad de niveles de transporte (TLS) para protocolos de seguridad distribuidos, además de soportar protocolos de autenticación del administrador LAN de Windows NT para compatibilidad.
- La implementación de los protocolos de seguridad de canal seguros (SSL 3.0/TLS) soporta la autenticación sólida del cliente mediante la correlación de credenciales del usuario en la forma de certificados de clave pública para las cuentas Windows NT existentes. Se utilizan herramientas de administración comunes para administrar la información de las cuentas y el control de acceso, ya sea utilizando la autenticación secreta compartida o la seguridad de clave pública.
- Windows 2000 soporta el uso opcional de tarjetas inteligentes para la conexión interactiva, además de las contraseñas. Las tarjetas inteligentes soportan criptografía y almacenaje seguro para claves y certificados privados, habilitando una autenticación sólida desde el escritorio al dominio.
- Windows 2000 incluye Microsoft Certificate Server para que las organizaciones emitan certificados X.509 versión 3 a sus empleados o socios de negocios. Esto incluye la

introducción de CryptoAPI para la administración de certificados y módulos para manejar certificados de clave pública, incluyendo certificados de formato estándar emitidos por cualquier Autoridad de certificado comercial (CA), CA de terceros o Microsoft Certificate Server, incluido en Windows. Los administradores del sistema definen cuáles CAs son confiables en su ambiente y, de esta forma, cuáles certificados se aceptan para la autenticación del cliente y el acceso a los recursos.

- Los usuarios externos que no tienen cuentas Windows 2000 pueden ser autenticados utilizando certificados de clave pública y correlacionados a una cuenta Windows existente. Los derechos de acceso definidos para la cuenta Windows determinan los recursos que los usuarios externos pueden utilizar en el sistema. La autenticación del cliente, utilizando certificados de clave pública, permiten que Windows 2000 autentique usuarios externos, con base en certificados emitidos por Autoridades de certificados acreditadas.
- Los usuarios de Windows 2000 cuentan con herramientas fáciles de usar y diálogos de interfaz comunes para la administración de pares de claves pública/privada y de certificados que se utilizan para acceder a los recursos basados en Internet. El almacenaje de credenciales de seguridad personales, las cuales utilizan el almacenaje basado en disco seguro, se transportan fácilmente con el protocolo estándar en la industria propuesto, Intercambio de información personal. Asimismo, el sistema operativo ha integrado soporte para los dispositivos de tarjeta inteligente.
- La tecnología de encriptación está integrada dentro del sistema operativo en muchas formas, con el fin aprovechar el uso de firmas digitales para proporcionar flujos de datos autenticados. Además de los controles firmados ActiveX™ y Clases Java para Internet Explorer, Windows 2000 utiliza firmas digitales para la integridad de imágenes de una variedad de componentes del programa. Los desarrolladores internos también pueden crear software firmado para distribución y protección de virus.

Además de estos cambios, esperamos que terceros cuenten con servicios de autenticación de contraseña dinámicos en Windows 2000 Server, e integren contraseñas dinámicas con la autenticación de dominio de Windows 2000. Las API y la documentación para soportar estos productos de terceros están disponibles en SDK de la plataforma Microsoft.

Cada una de las nuevas funciones de seguridad de Windows 2000 se describe con más detalle en las secciones siguientes.

ACTIVE DIRECTORY Y LA SEGURIDAD

Actualmente, la información de cuentas de Windows NT se mantiene utilizando una parte de registro segura en los controladores de dominio. Al utilizar *trusts* de dominio y autenticación de pase, una jerarquía de dos niveles de dominios proporciona flexibilidad para organizar la administración de cuentas y los servidores de recursos. Sin embargo, dentro de un dominio, las cuentas se mantienen en un espacio de nombre plano, sin ninguna organización interna.

Los Servicios de seguridad distribuida de Windows 2000 utilizan Active Directory como el depósito para la información de cuentas. Active Directory proporciona una mejora importante sobre la implementación basada en el registro en las áreas de rendimiento y escalabilidad, y ofrece un ambiente administrativo rico en funciones.

El siguiente diagrama muestra la estructura jerárquica para un árbol de dominios de Windows 2000 y el contexto de nombre jerárquico dentro de cada dominio que utiliza unidades organizacionales (OU) como contenedores de objetos de directorio.

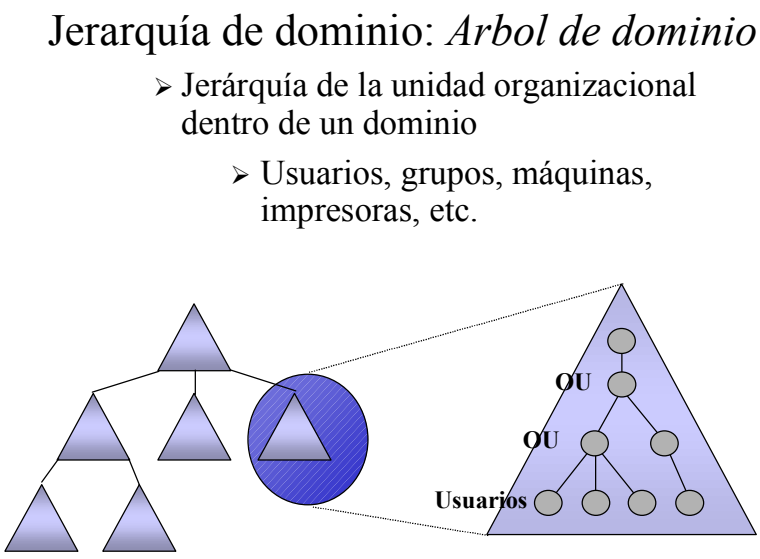

Figura1. Estructura jerárquica de Active Directory

Ventajas de la administración de cuentas de Active Directory

Las ventajas de integrar la administración de cuentas de seguridad con Active Directory son:

- Cuentas para usuarios, grupos y maquinas, que pueden ser organizadas en los contenedores de directorio denominados unidades organizacionales (OU). Un dominio puede tener cualquier número de OU organizadas en espacios de nombre estructurados como un árbol. Las empresas pueden organizar el espacio de nombre para información de cuentas, con el fin de representar los departamentos y organizaciones en la compañía. Asimismo, las cuentas del usuario, al igual que las OU, son objetos de directorio que se pueden renombrar fácilmente dentro de un árbol de dominio, a medida que cambia la organización.

- Active Directory soporta un número mucho mayor de objetos de usuario (más de 1 millón de objetos) con un mejor rendimiento que el registro. La dimensión del dominio individual ya no estará limitada por el rendimiento del depósito de seguridad. Un árbol de dominios conectados puede soportar estructuras organizacionales mucho más grandes y complejas.
- La administración de la información de cuentas se mejora utilizando las herramientas gráficas avanzadas para la administración de Active Directory, así como a través del soporte OLE DS para lenguajes de *script*. Se pueden implementar tareas comunes utilizando *scripts* de lote para automatizar la administración.
- Los servicios de duplicación del directorio permiten realizar múltiples copias de la información de cuentas, en las cuales se pueden realizar actualizaciones en cualquier copia, no únicamente en el controlador de dominio primario designado. El Protocolo de acceso al directorio ligero (LDAP) y el soporte de sincronización de directorio proporcionan los mecanismos para vincular
  el directorio de Windows con los demás directorios de la empresa.

Almacenar la información de la cuenta de seguridad en Active Directory significa que los usuarios y grupos están representados como objetos en el directorio. El acceso de lectura y escritura a los objetos en el directorio se puede otorgar al objeto en su totalidad, o a propiedades individuales del mismo. Los administradores cuentan con un control granular sobre quién puede actualizar la información del usuario o grupo. Por ejemplo, se le puede otorgar a un grupo de operadores de telecomunicaciones el acceso de escritura únicamente para las propiedades de cuenta del usuario relacionadas con el equipo telefónico de oficina, sin requerir privilegios de Operador de cuenta o Administrador.

Asimismo, el concepto de un grupo se simplifica, debido a que los grupos locales y globales están representados por *objetos de grupo* en el directorio. Las interfaces de programación existentes para los accesos a grupos locales aún siguen soportadas para compatibilidad completa hacia atrás. Sin embargo, los grupos definidos en el directorio pueden utilizarse para el control de acceso a los recursos en todo el dominio, o únicamente para fines de administración local en el controlador de dominio.

Relación entre los servicios de directorio y la seguridad

Existe una relación fundamental entre Active Directory y los Servicios de seguridad integrados en el sistema operativo Windows 2000. Active Directory almacena la información de políticas de seguridad de dominio, como son las restricciones de contraseña en todo el dominio y los privilegios de acceso al sistema, que afectan directamente el uso del sistema. Los objetos relacionados con la seguridad en el directorio deben administrarse de manera segura, con el fin de evitar cambios no autorizados que afecten la totalidad de la seguridad del sistema. El sistema operativo Windows 2000 implementa el modelo de seguridad basado en el objeto y el control de acceso a todos los objetos de Active Directory. Cada objeto que se encuentra en Active Directory tiene un descriptor de seguridad único que define las actualizaciones de acceso que se requieren para leer o actualizar las propiedades de un objeto.

El siguiente diagrama muestra la relación fundamental entre Active Directory y los servicios de seguridad del sistema operativo.

Servicios de directorio y seguridad

- Active Directory
  - Almacena la política de seguridad e información de la cuenta
- Sistema operativo
  - Implementa el modelo de seguridad en todos los objetos
  - Información de trusts almacenada de manera segura en el directorio

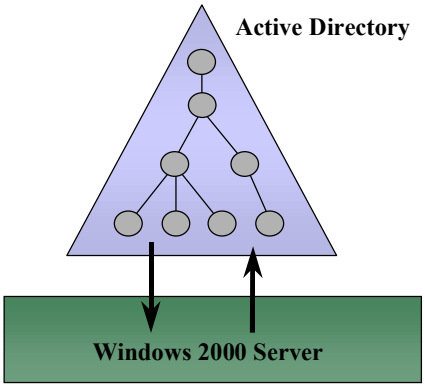

Figura2. Relación entre Active Directory y los Servicios de seguridad

Active Directory utiliza la personificación y verificación de acceso de Windows 2000 para determinar si un cliente de Active Directory puede leer o actualizar el objeto deseado. Esto significa que las solicitudes del cliente LDAP al directorio requieren que el sistema operativo aplique el control de acceso, en lugar de que Active Directory mismo tome las decisiones de control de acceso.

El modelo de seguridad de Windows 2000 proporciona una implementación unificada y consistente de control de acceso a todos los recursos del dominio, con base en membresías de grupo. Los componentes de seguridad de Windows 2000 pueden confiar en la información relacionada con la seguridad almacenada en el directorio. Por ejemplo, el servicio de autenticación de Windows 2000 almacena la información de la contraseña encriptada en una parte segura de los objetos del usuario de directorio. El sistema operativo asegura que la información de la política de seguridad se almacene de manera segura y que las restricciones de cuenta o membresías de grupo no puedan ser cambiadas por nadie sin acceso autorizado. Además, la información de política de seguridad para toda la administración del dominio se mantiene en el directorio.

Esta relación fundamental de Seguridad y Active Directory se logra únicamente mediante la integración completa del directorio con el sistema operativo Windows 2000 y no puede realizarse de otra manera.

Relaciones de confianza entre dominio

Los dominios Windows 2000 se pueden organizar en árboles de dominio jerárquicos. Las relaciones de confianza entre los dominios permiten a los usuarios con cuentas definidas en un dominio que sean autenticadas por los servidores de recursos en otro dominio. En Windows NT 4.0 y versiones anteriores, las relaciones de confianza entre dominios se definen por cuentas de dominio confiables, unidireccionales, entre los controladores de dominio. La administración de

relaciones de confianza entre los dominios de cuenta y los dominios de recursos en una red grande es una tarea compleja.

Active Directory soporta dos formas de relaciones de confianza:

- Las relaciones de confianza unidireccionales explícitas a los dominios Windows NT 4.0.
- Administración transitoria bidireccional entre los dominios que forman parte del árbol de dominios de Windows 2000.

El siguiente diagrama muestra los dos estilos de relaciones administrativas.

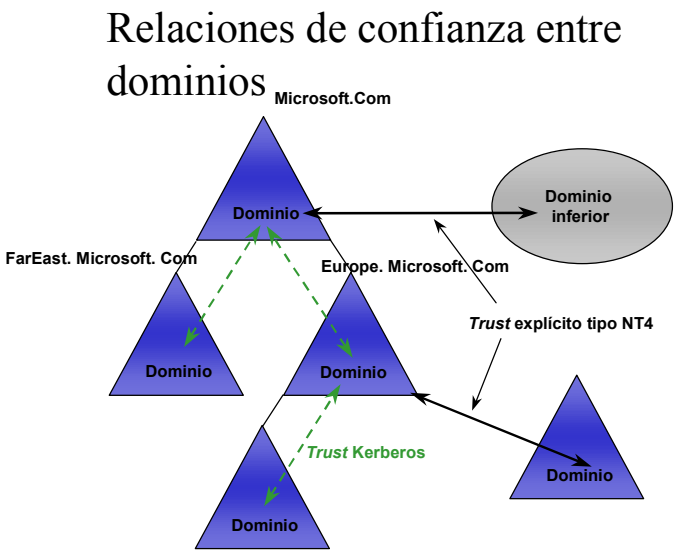

Figura3. Relaciones administrativas de dominio

Los *trusts* transitorios entre los dominios simplifican la administración de cuentas de confianza entre los dominios. Los dominios que son miembros del árbol de dominio definen una relación de confianza bidireccional con el dominio predominante en el árbol. Todos los dominios confían de manera implícita en los demás dominios del árbol. Si existen dominios específicos que no participen en el *trust* bidireccional, se pueden definir cuentas de confianza unidireccional explícitas. Para las organizaciones que cuentan con múltiples dominios, el número total de relaciones de confianza unidireccionales explícitas se reduce en gran medida.

Delegación de administración

La delegación de administración es una herramienta valiosa para que las organizaciones confinen la administración de seguridad para que aplique únicamente a subgrupos definidos en el dominio de toda la organización. El requerimiento importante es otorgar los derechos de administrar un grupo pequeño de usuarios o grupos dentro de su área de responsabilidad y, al mismo tiempo, no dar permisos para administrar cuentas en otras partes de la organización.

La delegación de responsabilidad para crear nuevos usuarios o grupos se define en el nivel de una unidad organizacional (OU), o contenedor, donde se crean las cuentas. Los administradores de

grupo para una unidad organizacional no tienen necesariamente la capacidad de crear y administrar cuentas para otra unidad organizacional dentro de un dominio. Sin embargo, las configuraciones de las políticas en todo el dominio y los derechos de acceso definidos en los niveles más altos en el árbol de directorio pueden aplicarse a través del árbol, utilizando la herencia de derechos de acceso.

Existen tres formas de definir la delegación de las responsabilidades de administración:

- Delegar permisos para cambiar propiedades en un contenedor particular, como es LocalDomainPolicies del objeto de dominio mismo.
- Delegar permisos para crear y eliminar objetos hijo de un tipo específico debajo de una OU, tales como usuarios, grupos o impresoras.
- Delegar permisos para actualizar propiedades específicas en objetos hijo de un tipo específico por debajo de una OU; por ejemplo, el derecho de establecer contraseñas en objetos del usuario.

La interfaz de Administración de servicio de directorio facilita la visualización de la delegación de información definida para los contenedores. La adición de una nueva delegación de permisos es fácil de llevar a cabo mediante la selección de la persona a la que se desea delegarle el permiso y posteriormente asignar cuáles permisos son necesarios.

Al integrar el depósito de cuenta de seguridad con Active Directory se logran beneficios reales para administrar una empresa. El resultado directo es el rendimiento, facilidad de administración y escalabilidad para grandes organizaciones. Las empresas basadas en Internet pueden utilizar árboles de dominio y OU jerárquicas para organizar cuentas para socios de negocios, clientes frecuentes o proveedores con derechos de acceso específicos al sistema.

Derechos de acceso granulares

Por lo regular, las grandes organizaciones dependen de varios individuos o grupos para asegurar y administrar la infraestructura de cuentas de la red. Necesitan la capacidad de otorgar derechos de acceso a operaciones específicas, como son la reconfiguración de contraseñas del usuario o la deshabilitación de cuentas para grupos específicos, sin otorgar también permisos para crear nuevas cuentas o cambiar otras propiedades de las cuentas del usuario.

La arquitectura de seguridad de los objetos de Active Directory utiliza los descriptores de seguridad Windows 2000 para controlar el acceso a objetos. Cada objeto que se encuentra en el directorio cuenta con un descriptor de seguridad único. La Lista de control de acceso (ACL) en el descriptor de seguridad es una lista de entradas que otorgan o niegan derechos de acceso específicos a individuos o grupos. Los derechos de acceso pueden ser otorgados o negados con diferentes niveles de enfoque en el objeto. Los derechos de acceso se pueden definir en cualquiera de los siguientes niveles:

- Aplicar a los objetos como un todo, lo cual aplica a todas las propiedades del objeto.
- Aplicar a una agrupación de propiedades definida de acuerdo con los grupos de propiedades que hay dentro de un objeto.
- Aplicar a una propiedad individual del objeto.

El otorgamiento de acceso de lectura/escritura uniforme a todas las propiedades de un objeto es el permiso de acceso predeterminado para el creador del objeto. Otorgar o negar los permisos de acceso al objeto a un grupo de propiedad es una manera conveniente para definir permisos para

un grupo de propiedades relacionadas. La agrupación de propiedades se define de acuerdo con el atributo del grupo de propiedad de una propiedad en el esquema. La relación de grupo de propiedad se puede personalizar cambiando el esquema. Por último, la definición de los derechos de acceso en un nivel según la propiedad, proporciona el nivel más alto de granularidad de permisos. La definición de acceso por propiedad está disponible en todos los objetos de Active Directory.

Asimismo, los objetos del contenedor en el directorio soportan acceso granular con respecto a las personas que tienen permisos para crear objetos hijos y qué tipo de objetos hijos pueden crearse. Por ejemplo, el control de acceso definido en una unidad organizacional (OU) puede definir la persona que tiene autorización para crear objetos de Usuario (cuentas) en este contenedor. Otra entrada en el control de acceso para la OU puede definir quién tiene autorización de crear objetos de impresora. El control de acceso granular en los contenedores de directorio es una manera eficaz de mantener la organización del espacio de nombre del directorio.

Una nueva implementación del Editor de Lista de control de acceso (ACL), el control de diálogo común para la visualización o cambio de autorizaciones de seguridad del objeto, proporciona una interfaz fácil de utilizar para definir derechos de acceso a los objetos Active Directory, según el grupo de propiedades o propiedades individuales. De igual forma, el editor ACL soporta la definición de derechos de acceso, delegados en los objetos del contenedor que fluyen a los subobjetos que se encuentran en alguna parte del árbol del directorio.

Herencia de los derechos de acceso

Heredar los derechos de acceso se refiere a la manera en que la información de control de acceso definida en los niveles más altos de los contenedores del directorio fluye a los subcontenedores y ramas de objetos. Existen, por lo general, dos modelos para la implementación de derechos de acceso heredados: herencia dinámica y estática. La herencia dinámica determina los derechos de acceso efectivos para un objeto mediante la evaluación de permisos definidos de manera explícita en el objeto y aquellos definidos para todos los objetos principales en el directorio. Esto permite flexibilidad para cambiar el control de acceso en algunas partes del árbol del directorio, al realizar cambios a un contenedor específico que afecta de manera automática todos los subcontenedores de los objetos de ramas. A cambio de esta flexibilidad se ofrece el costo de rendimiento para evaluar los derechos de acceso efectivos al momento en que un cliente solicita lectura/escritura a un objeto de directorio específico.

Windows 2000 implementa una forma de herencia estática de los derechos de acceso, conocida como herencia *Crear tiempo*. Se puede definir la información de control de acceso que fluye hasta los objetos hijo del contenedor. Cuando se crea el objeto hijo, los derechos heredados de un contenedor se fusionan con los derechos de acceso predeterminados en el nuevo objeto. Cualquier cambio realizado a los derechos de acceso heredados en los niveles más altos del árbol debe propagarse hacia abajo, hasta todos los objetos hijo afectados. Los nuevos derechos de acceso heredados se propagan mediante Active Directory hasta los objetos para los cuales aplican, en base con las opciones de la manera en que se definen los nuevos derechos.

La verificación del rendimiento para el control de acceso es muy rápida, utilizando el modelo de herencia estático de los derechos de acceso. El sistema operativo está diseñado para optimizar las verificaciones de acceso que son operaciones frecuentes y necesarias, no sólo para el acceso del

objeto de directorio, sino para el objeto del sistema de archivo y todos los demás objetos del sistema Windows 2000.

MULTIPLES PROTOCOLOS DE SEGURIDAD

Windows 2000 soporta múltiples protocolos de seguridad de red, debido a que cada protocolo proporciona ya sea compatibilidad para los clientes existentes, mecanismos de seguridad más efectivos, o funciones de interoperabilidad para redes heterogéneas como Internet. Existen varios protocolos de autenticación actualmente en uso en las redes corporativas y la arquitectura Windows 2000 no limita cuáles protocolos pueden ser soportados. Un protocolo de seguridad que se ajuste a todas las necesidades sería más simple, pero las configuraciones de red desde redes pequeñas de oficina a proveedores de contenido de Internet a gran escala no comparten los mismos requerimientos de seguridad. Los clientes necesitan tener opciones sobre cómo integrar la nueva tecnología de seguridad, como son contraseñas dinámicas o criptografía de clave pública, dentro de su ambiente computacional.

Windows 2000 está diseñado para soportar varios protocolos de seguridad, un elemento esencial para el ambiente de computación distribuida que existe en la actualidad. Al utilizar las API de seguridad Win32® para todo tipo de fines, el sistema operativo aísla las aplicaciones soportadas de los detalles de protocolo de seguridad diferentes disponibles. La interfaz de aplicación de nivel más alto proporcionada por RPC y DCOM autenticados otorgan abstracciones con base en los parámetros de interfaz para utilizar los servicios de seguridad.

La infraestructura de seguridad Windows 2000 soporta los siguientes protocolos de seguridad primarios:

- El protocolo de autenticación Windows NT LAN Manager (NTLM) se utiliza en Windows NT 4.0 y versiones anteriores de Windows NT. NTLM seguirá recibiendo soporte y se utilizará para la autenticación de paso a través de la red, acceso de archivo remoto y conexiones RPC autenticadas para versiones anteriores de Windows NT.
- El protocolo de autenticación Kerberos Versión 5 reemplaza NTLM como el protocolo de seguridad primario para acceder a los recursos dentro o a través de los dominios Windows 2000. El protocolo de autenticación Kerberos es un estándar en la industria ya conocido, que tiene las ventajas de autenticación de red Windows. Algunos de los beneficios del protocolo Kerberos son la autenticación mutua, tanto del cliente como del servidor, carga del servidor reducida durante el establecimiento de la conexión y soporte para la delegación de autorización de clientes a servidores a través del uso de mecanismos *proxy*.
- La Autenticación de contraseña distribuida (DPA) es el protocolo de autenticación secreta distribuida que utilizan las organizaciones de membresía en Internet más grandes, tales como son MSN y CompuServe. Este protocolo de autenticación forma parte de los servicios Microsoft Commercial Internet System (MCIS) y está diseñado de manera específica para que los usuarios utilicen la misma contraseña de membresía en Internet para conectarse a cualquier número de sitios en Internet que forman parte de la misma organización de membresía. Los servidores de contenido de Internet utilizan el servicio de autenticación MCIS como un servicio de Internet *backend*, y los usuarios pueden conectarse a múltiples sitios sin tener que volver a introducir sus contraseñas.
- Los protocolos basados en clave pública proporcionan privacidad y confiabilidad sobre Internet. SSL es el estándar *de facto* actual para las conexiones entre los exploradores de Internet y los servidores de información en Internet. (Una definición próxima del protocolo estándar IETF basado en SSL3 se conoce actualmente como el Protocolo de seguridad de nivel de transporte o TLS.) Estos protocolos, que utilizan certificados de clave pública para autenticar los clientes y servidores, depende de una infraestructura de clave pública para uso

general. Windows NT 4.0 proporciona servicios de seguridad de canal seguros que implementan los protocolos SSL/PCT. La seguridad de Windows 2000 cuenta con soporte de funciones más avanzadas para protocolos de clave pública, los cuales se describen posteriormente en este documento.

La seguridad empresarial depende de tener la flexibilidad de utilizar los mecanismos de seguridad correctos, cuando sea necesario. La computación empresarial seguirá dependiendo de una amplia gama de servicios de red proporcionados por servidores de archivo e impresión remotos, aplicaciones empresariales y servidores de datos, además de ambientes de *data warehousing* y de procesamiento de transacción. El soporte para protocolos múltiples de seguridad de red permiten que Windows 2000 Professional y Windows 2000 Server alojen una variedad de servicios de red, además de las tecnologías basadas en Internet.

El diagrama siguiente muestra el soporte de arquitectura para múltiples protocolos de seguridad implementados en Windows 2000, utilizando la Interfaz del proveedor de soporte de seguridad (SSPI).

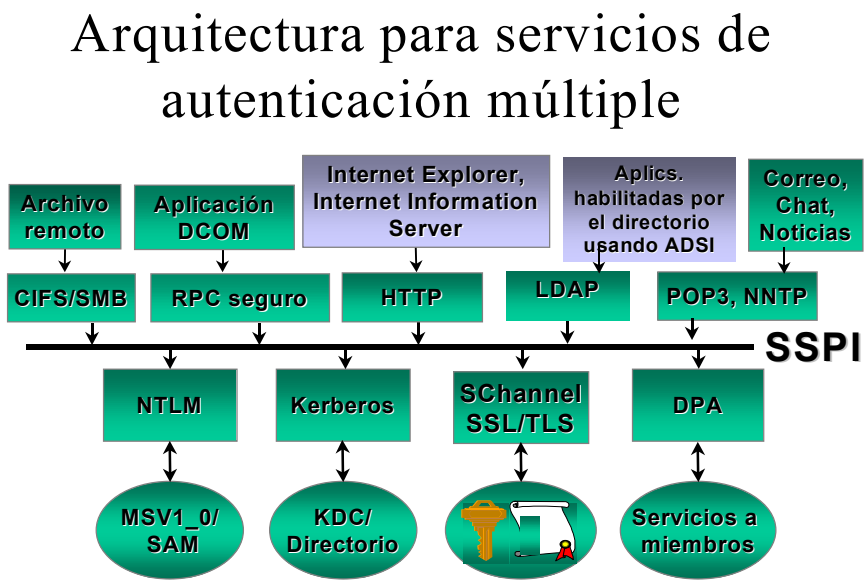

Figura 4. Arquitectura para múltiples servicios de autenticación

La interfaz de proveedor de soporte de seguridad es una API del sistema Win32 utilizada por varias aplicaciones y servicios del sistema, por ejemplo, Internet Explorer (IE) e Internet Information Server (IIS), para aislar los protocolos de nivel de aplicación de los protocolos de seguridad utilizados para la autenticación de red. Los proveedores de seguridad utilizan diferentes credenciales para autenticar al usuario, ya sea con certificados de secreto compartido o clave pública. Los protocolos de seguridad interactúan con diferentes servicios de autenticación y almacenes de información de cuentas.

- El proveedor de seguridad NTLM utiliza el servicio de autenticación MSV1_0 y el servicio NetLogon en un controlador de dominio para autenticación del cliente e información de

autorización.

- El proveedor de seguridad Kerberos se conecta a un Centro de distribución de claves en línea (KDC) y la cuenta Active Directory se almacena para las boletas de sesión.
- DPA utiliza los servicios de seguridad MCIS para la autenticación de membresía e información de acceso específica del servidor.
- Los servicios de canal seguros están basados en certificados de clave pública emitidos por autoridades certificadas confiables; no requieren un servidor de autenticación en línea.

INTERFAZ DEL SERVIDOR DE SOPORTE DE SEGURIDAD

Las APIs de seguridad de Windows para la autenticación de red están definidas a través de la Interfaz del proveedor de soporte de seguridad (SSPI), documentada en la plataforma SDK. La SSPI se comunica con una API de Win32 con base en la Interfaz del programa de aplicación de servicios de seguridad genérico (GSS-API) y proporciona una abstracción de interfaz similar para la administración de contexto de seguridad.[1] Las aplicaciones y servicios Windows 2000 utilizan la SSPI para aislar los protocolos de nivel de aplicación de los detalles de los protocolos de seguridad de red. Windows 2000 soporta la interfaz SSPI para disminuir el código de nivel de aplicación necesario para soportar protocolos múltiples de autenticación. SSPI proporciona una abstracción genérica para soportar múltiples mecanismos de autenticación basados en protocolos de secreto compartido o clave pública. Las aplicaciones que utilizan la seguridad Windows 2000 integrada aprovechan al máximo la modularidad proporcionada por SSPI mediante la solicitud de directorios de rutina SSPI o mediante el uso de protocolos de administración de conexión de red de nivel más alto, proporcionados por RPC o DCOM autenticados.

[1] "Generic Security Services Application Program Interface", J. Linn, Internet RFC 1508, septiembre, 1993.

PROTOCOLO DE AUTENTICACION KERBEROS

El protocolo de autenticación Kerberos define las interacciones entre un cliente y un Servicio de autenticación de red conocido como Centro de distribución de claves (KDC). Windows 2000 implementa un KDC como el servicio de autenticación en cada controlador de dominio. El dominio Windows 2000 es equivalente a un reino Kerberos, pero continúa siendo referido como un dominio. La implementación de Kerberos en Windows 2000 está basada en la definición RFC 1510 de Internet del protocolo Kerberos[2]. El tiempo de ejecución del cliente Kerberos se implementa como un proveedor de seguridad Windows 2000 basado en la SSPI. La autenticación inicial de Kerberos se integra con la arquitectura WinLogon de una sola firma. El servidor Kerberos (KDC), integrado con los servicios de seguridad Windows existentes que se ejecutan en el controlador de dominio, utiliza Active Directory como la base de datos de cuentas para usuarios (principales) y grupos.

El protocolo de autenticación Kerberos mejora las funciones de seguridad subyacentes de Windows 2000 y proporciona las funciones siguientes:

- Rendimiento de autenticación de servidor más rápido durante el establecimiento de la conexión inicial. El servidor de aplicaciones no se tiene que conectar al controlador de dominio para autenticar al cliente. Esto permite a los servidores de aplicaciones escalar mejor, al manejar un mayor número de solicitudes de conexión de clientes.
- Delegación de autenticación para arquitecturas de aplicación cliente/servidor de niveles múltiples. Cuando un cliente se conecta a un servidor, el servidor personifica al cliente en el sistema. Sin embargo, si el servidor necesita realizar una conexión de red a otro servidor *back-end* para completar la transacción del cliente, el protocolo Kerberos permite la delegación de autenticación para que el primer servidor se conecte con otro servidor a nombre del cliente. La delegación permite que el segundo servidor también personifique al cliente.
- Relaciones de administración transitorias para la autenticación entre dominios. Los usuarios pueden autenticar los dominios en cualquier parte del árbol de dominio, ya que los servicios de autenticación (KDC) en cada dominio otorgan confianza a las boletas emitidas por otros KDC en el árbol. La administración transitoria simplifica la administración de dominio para grandes redes con dominios múltiples.

El protocolo de autenticación Kerberos versión 5 definido en RFC 1510 ha pasado por amplios procesos de revisión en la industria y es bien conocido en los grupos de interesados en la seguridad.

Antecedentes de Kerberos

Kerberos es un protocolo de autenticación de secreto compartido, debido a que el usuario y el KDC conocen la contraseña del usuario o, en el caso del KDC, la contraseña encriptada unidireccional. El protocolo Kerberos define una serie de intercambios entre los clientes, el KDC y los servidores, para obtener y utilizar boletas Kerberos. Cuando un usuario inicia una conexión a Windows, el SSP de Kerberos obtiene una boleta Kerberos inicial (TGT) basada en un verificador encriptado de la contraseña del usuario. Windows 2000 almacena la TGT en el caché de la boleta en la estación de trabajo relacionada con el contexto de acceso del usuario. Cuando un programa del cliente trata de tener acceso a un servicio de red, el tiempo real Kerberos verifica el caché de la boleta

[2] "The Kerberos Network Authentication Service (V5)", J. Kohl and C. Neumann, Internet RFC 1510, septiembre, 1993.

para una boleta de sesión válida para el servidor. Si una boleta no está disponible, la TGT se envía en una solicitud al KDC para una boleta de sesión que permita el acceso al servidor.

La boleta de sesión se agrega al caché de la boleta y puede volver a utilizarse para conexiones futuras al mismo servidor hasta que la boleta expire. El período de expiración de la boleta lo define la política de seguridad de dominio y por lo regular se establece para ocho horas. Si la boleta de sesión expira en la mitad de una sesión activa, el proveedor de seguridad Kerberos regresa los valores de error adecuados que permiten que el cliente y el servidor vuelvan a generar la boleta, generar una nueva clave de sesión y reanudar la conexión.

El siguiente diagrama muestra la relación que existe entre el cliente, el KDC y el servidor de aplicaciones utilizando el protocolo de autenticación Kerberos.

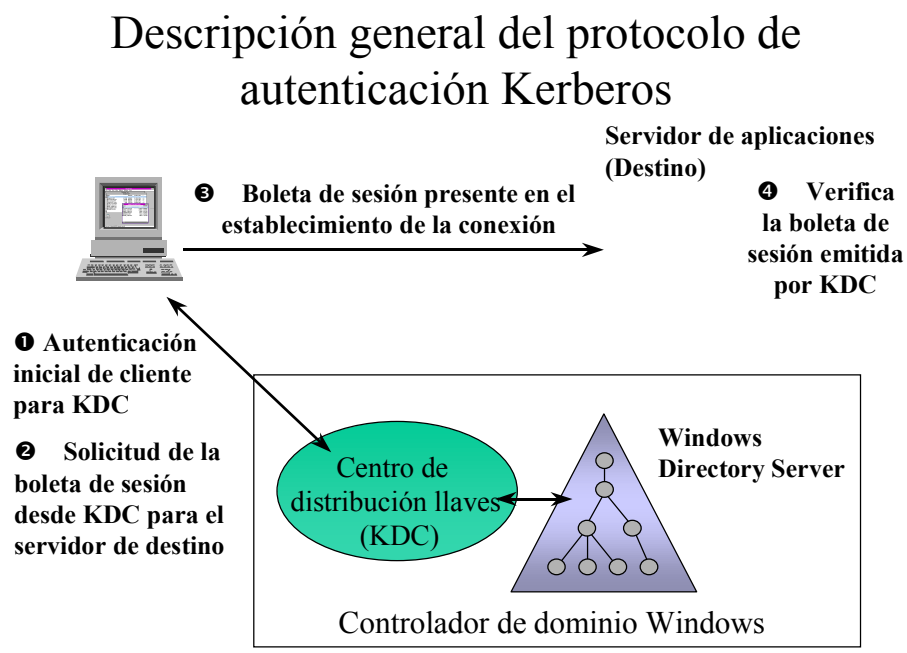

Figura 5. Descripción general del protocolo de autenticación Kerberos

La boleta de sesión Kerberos se presenta al servicio remoto durante el mensaje de conexión inicial. Algunas partes de la boleta de sesión se encriptan utilizando una clave secreta compartida entre el servicio y el KDC. El servidor puede autenticar rápidamente al cliente verificando la boleta de sesión sin ir al servicio de autenticación, ya que el tiempo real Kerberos para el servidor ha guardado una copia en la memoria de la clave secreta del servidor. La configuración de la conexión de sesión es mucho más rápida del lado del servidor que la autenticación NTLM. Con NTLM, el servidor obtendría las credenciales del usuario y después tendría que volver a autenticar al usuario a través del controlador de dominio, como parte del establecimiento de una conexión.

Las boletas de sesión Kerberos contienen una clave de sesión única creada por el KDC para que sea utilizada para la encriptación simétrica de la información de autenticación y los datos transferidos entre el cliente y el servidor. En el modelo Kerberos, se utiliza el KDC como un tercero

confiable en línea para generar una clave de sesión. Los servicios de autenticación en línea son muy eficaces para los servicios de aplicación distribuida disponibles en el ambiente de red semejantes a un *campus.*

Integración de Kerberos

El protocolo Kerberos se integra totalmente con la arquitectura de seguridad Windows 2000 para la autenticación y el control de acceso. La conexión de dominio Windows inicial se proporciona con WinLogon. WinLogon utiliza el proveedor de seguridad Kerberos para obtener una boleta Kerberos inicial. Otros componentes del sistema operativo, como son el redireccionador, utilizan la interfaz SSPI para que el proveedor de seguridad Kerberos obtenga una boleta de sesión para conectarse al servidor SMB para acceso de archivo remoto.

El protocolo Kerberos versión 5 define un campo encriptado en boletas de sesión para portar datos de autorización, pero el uso del campo se deja a las aplicaciones. Windows 2000 utiliza los datos de autorización en las boletas Kerberos para portar los ID de seguridad Windows que representan la membresía del usuario y grupo. El proveedor de seguridad Kerberos del lado del servidor de una conexión utiliza los datos de autorización para crear un registro de acceso de seguridad Windows que representa al usuario en ese sistema. El servidor sigue el modelo de personificación del cliente de seguridad Windows, utilizando el registro de acceso que representa al cliente, antes de intentar acceder a los recursos locales protegidos por las Listas de control de acceso (ACL).

El protocolo Kerberos versión 5 soporta la delegación de autenticación utilizando los indicadores *proxy* y *forwarding* en las boletas de sesión. Windows 2000 utiliza la función de delegación para permitir que los servidores obtengan otra boleta de sesión para conectarse a servidores remotos a nombre del cliente.

Interoperabilidad Kerberos

El protocolo Kerberos versión 5 se implementa para una variedad de sistemas y se utiliza para proporcionar un servicio de autenticación único en una red distribuida. La interoperabilidad Kerberos proporciona un protocolo común que permite una base de datos de cuentas (posiblemente duplicada) para la autenticación de los usuarios en todas las plataformas computacionales de la empresa, para que puedan acceder a todos los servicios en un ambiente heterogéneo. La interoperabilidad Kerberos se basa en las siguientes características:

- Un protocolo de autenticación común utilizado para identificar el usuario o servicio a través del nombre principal en una conexión de red.
- La capacidad de definir relaciones administrativas entre los reinos de Kerberos y de generar boletas referentes a las solicitudes entre reinos.
- Implementaciones que soportan los *Requerimientos de interoperabilidad* que se definen en el RFC 1510, relacionadas con las opciones de encriptar, algoritmos de revisión de suma, autenticación mutua y otras opciones de boleta.
- Soporte para los formatos *token* de seguridad Kerberos versión 5, para el establecimiento del contexto e intercambio por mensaje, como lo define el grupo de trabajo de Tecnología de autenticación común de IETF[3].

[3] RFC 1964 define los formatos de registros de seguridad del mecanismo Kerberos Versión 5 GSS-API.

El nombre principal en una boleta Kerberos se utiliza para autentificar la identidad del usuario, pero la información de autorización adicional puede ser manejada en el sistema local para el control de acceso. La autenticación basada en la identidad proporciona un nivel elevado de interoperabilidad para los sistemas que soportan el protocolo Kerberos versión 5; sin embargo, no soporta la autorización del usuario. El protocolo Kerberos ofrece el transporte de datos de autorización, pero el contenido en este campo se considera específico para el servicio de la aplicación.

La implementación Microsoft del protocolo Kerberos soporta las características de interoperabilidad suficientes para la autenticación basada en la identidad. Además, Microsoft integra datos de autorización en la forma de membresías de grupo Windows 2000 en las boletas Kerberos, para transmitir la información de control de acceso a los servicios Windows 2000. La representación nativa de los datos de autorización se encuentra en los ID de seguridad Windows.

Los servicios de Windows 2000 tienen cuentas de servicio definidas en Active Directory, las cuales definen el secreto compartido que utiliza el KDC para encriptar las boletas de sesión. Los clientes que intentan conectarse a los servicios Windows 2000 obtienen boletas de sesión para el servidor de destino del KDC que se encuentra en el dominio donde se define la cuenta de servicio. El proveedor de seguridad Kerberos que soporta un servicio Windows 2000 espera encontrar datos de autorización en las boletas de sesión que se utilizan para crear un registro de acceso de seguridad. El servicio Windows 2000 personifica el contexto de seguridad del cliente, con base en los datos de autorización proporcionados en la boleta de sesión.

Los clientes que obtienen las boletas TGT Kerberos iniciales del KDC en los sistemas que no son Windows 2000, utilizan el mecanismo de referencia de Kerberos para solicitar una boleta de sesión del KDC en el dominio Windows 2000 Service. La boleta de referencia se crea mediante relaciones de confianza entre reinos entre los KDC. Las solicitudes de boletas que se originan a partir del servicio de autenticación Kerberos MIT en general no contienen datos de autorización. Cuando las boletas de sesión no contienen datos de autorización, el proveedor de seguridad Kerberos en Windows 2000 trata de utilizar el nombre principal de la boleta y crear un registro de acceso de seguridad para una cuenta de usuario designado o utilizar una cuenta predeterminada definida para este fin. actualmente Microsoft sigue investigando algunos aspectos de interoperabilidad con diferentes configuraciones Kerberos y seguirá dicho trabajo con un enfoque en la interoperabilidad total con Kerberos.

Los Servicios de seguridad DCE también están estratificados en el protocolo Kerberos. Los servicios de autenticación DCE utilizan la representación RPC de los mensajes de protocolo Kerberos. Además, DCE utiliza el campo de datos de autorización en las boletas Kerberos para transmitir Certificados de atributos de privilegios extendidos (EPAC) que definen la identidad del usuario y la membresía de grupo. EPAC se utilizan como ID de seguridad Windows para la autorización y control de acceso del usuario. Los servicios Windows 2000 no pueden traducir los EPAC DCE en identificadores de usuario y grupo de Windows 2000. Esto no está relacionado con la interoperabilidad Kerberos, sino con la interoperabilidad que existe entre DCE y la información de control de acceso Windows 2000. Microsoft investigará las maneras de correlacionar la autorización DCE con el modelo de seguridad Windows 2000.

Extensiones Kerberos para clave pública

Asimismo, Windows 2000 implementa extensiones para que el protocolo Kerberos soporte

autenticación basada en pares de clave privada/pública además de claves secretas compartidas. Las extensiones de autenticación de clave pública permiten a los clientes solicitar una TGT inicial utilizando la clave privada, al tiempo que KDC verifica la solicitud utilizando la clave pública obtenida desde un certificado X.509 almacenado en el objeto del usuario en Active Directory. El certificado del usuario podría ser emitido por una Autoridad de certificados de terceros, como Digital ID de VeriSing o Microsoft Certificate Server en Windows 2000. Después de la autenticación de clave privada inicial los protocolos Kerberos estándar para la obtención de boletas de sesión se utilizan para conectarse a los servicios de red.

Una propuesta de ampliar la especificación de protocolo Kerberos con el fin de proporcionar un método para el uso de criptografía de clave pública en la autenticación inicial ha sido presentada al grupo de trabajo IETF para su revisión. Actualmente, Microsoft participa en los procesos de estándares IETF y pretende soportar las extensiones de protocolo estándar para clave pública.

Las extensiones de autenticación de clave pública para el protocolo Kerberos sientan las bases para una autenticación de red, utilizando la tecnología de tarjeta inteligente. Windows 2000 permite a los usuarios conectarse a una estación de trabajo mediante el uso de una tarjeta inteligente. Próximamente existirán varias opciones para obtener certificados para los usuarios, dependiendo de sus afiliaciones a organizaciones o requerimientos de trabajo. Windows 2000 proporciona un Certificate Server a las organizaciones que deseen emitir certificados de clave pública a sus usuarios sin depender de los servicios CA comerciales. La política del certificado es clara y directa: los certificados se emiten a los usuarios que cuentan con autenticación utilizando credenciales de cuenta de dominio válidas. En la sección siguiente se describe la forma en que dichos certificados se pueden utilizar para el acceso a los recursos de Windows 2000 a través de intranet o Internet.

SEGURIDAD DE INTERNET PARA WINDOWS 2000

Microsoft está desarrollando una infraestructura de seguridad de clave pública a fin de integrar la seguridad de clave pública con la seguridad de Windows 2000. La criptografía de clave pública es la tecnología de seguridad que permite una seguridad sólida para las comunicaciones empresariales y de Internet. Las tecnologías de seguridad de Internet de Microsoft incluyen un Certificate Server, un proveedor de seguridad de canal seguro que implementa los protocolos SSL/TLS, el protocolo de pago seguro SET para las transacciones de tarjeta de crédito y componentes CryptoAPI para la administración y manejo de certificados.

Los componentes de la infraestructura de seguridad de clave pública de Microsoft se muestran a continuación.

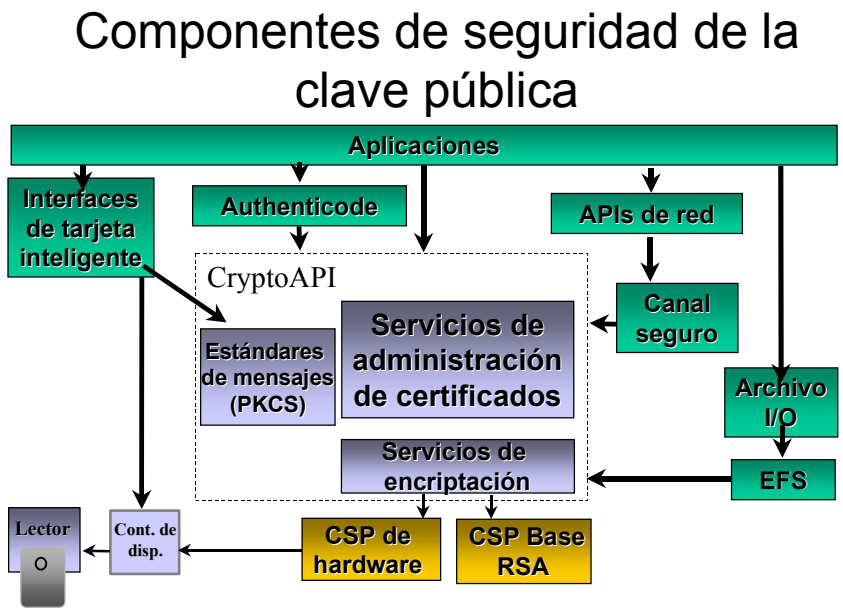

Figure 6: Componentes de seguridad de llave pública de Microsoft

La infraestructura de seguridad de Internet de Microsoft se basa en los estándares de la industria para la seguridad de clave pública, incluyendo el soporte para los formatos de certificado *Public-key Cipher* de RSA, X.509 y estándares PKCS.

La versión 4.0 de Windows NT proporcionó los primeros componentes para la utilización de la seguridad de clave pública, entre ellos:

- CryptoAPI, con soporte de programador para la generación e intercambio de claves, firmas digitales y encriptación de datos, con el uso de una arquitectura de proveedor con el fin de soportar los Proveedores de servicio criptográfico instalables.
- Soporte CryptoAPI de certificados X509 y PKCS, los cuales fueron emitidos en el paquete de servicio 3 para Windows NT 4.0 y se utilizan en Internet Explorer 4.0 y Windows 2000.
- Implementación de canal seguro de los protocolos de seguridad de clave pública *Secure Socket Layer* (SSL) versión 2.0, soporte del lado del cliente en la versión 3.0 y *Private Communications Technology* (PCT) versión 1.0.
- Authenticode™, una solución estándar en la industria, que utiliza firmas digitales para verificar

la integridad del software descargado de Internet y la identificación del editor de software.

La infraestructura de seguridad de Internet de Microsoft se crea en estos componentes y proporciona funcionalidad adicional para soportar la seguridad de clave pública para plataformas Windows, incluyendo Windows 2000. Muchos de los componentes de seguridad de Internet se utilizan en Microsoft Internet Explorer e Internet Information Server. Las nuevas funciones de la infraestructura de seguridad de Internet de Microsoft para Windows 2000 Distributed Security Services incluyen:

- Autenticación del cliente con SSL 3.0 basado en certificados de clave pública.
- Certificate Server para la emisión de certificados para cuentas de dominios Windows 2000.

La seguridad Windows 2000 utiliza los estándares de Internet para la seguridad de clave pública con funciones incorporadas en el sistema operativo.

Autenticación del cliente con SSL 3.0

Secure Socket Layer y *Transport Layer Security* son protocolos de seguridad basados en clave pública implementados por el proveedor de seguridad Secure Channel (Schannel). Estos protocolos de seguridad los utilizan los exploradores y servidores de Internet para autenticación mutua, integridad de mensajes y confidencialidad. La autenticación de Internet Server se realiza a través de Internet Explorer (el cliente) cuando se presenta el certificado del servidor como parte del establecimiento de canal seguro SSL/TLS. El programa del cliente acepta el certificado del servidor a través de la verificación de las firmas criptográficas en el certificado y cualquier certificado CA intermedio, para uno o más de los CA de raíz configurados o conocidos.

Asimismo, la autenticación del cliente está soportada por SSL 3.0 y TLS. La autenticación del cliente que utiliza certificados de clave pública se complementa como parte de este establecimiento de sesión de canal seguro.

La Figura 7 muestra los mensajes de saludo SSL 3.0 entre el cliente y servidor para el establecimiento de una conexión segura.

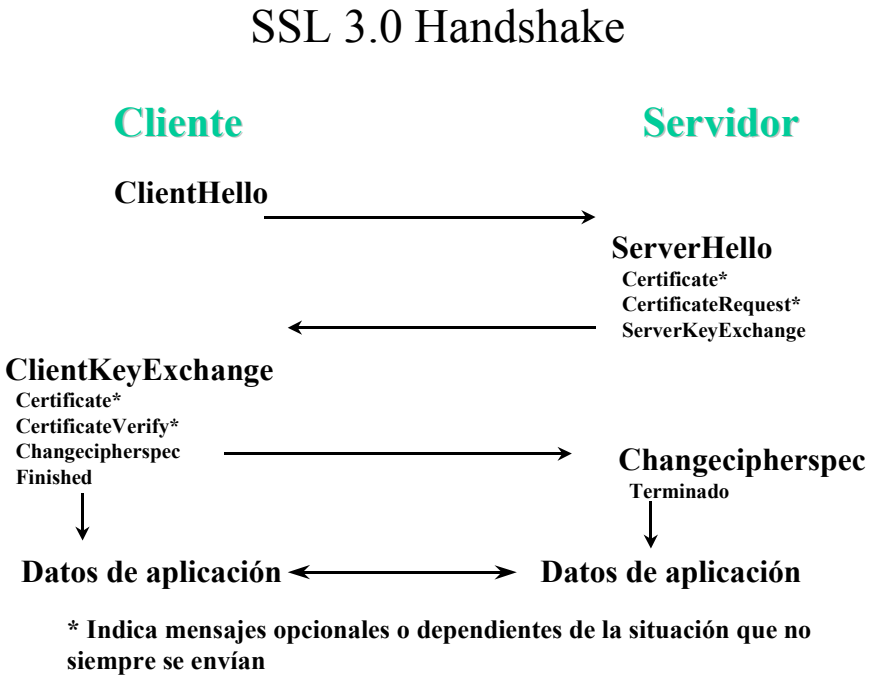

Figura 7. Saludo SSL 3.0

La autenticación del cliente por el servidor es el mismo proceso que se sigue con la autenticación del servidor. El servidor verifica las firmas criptográficas en el certificado del cliente y cualquier certificado CA intermedio, a un CA de origen conocido o verdadero. Sin embargo, una vez que se ha verificado la identidad del cliente a través de la verificación de certificado (autenticación del cliente), el servidor de la aplicación necesita establecer un contexto de seguridad con los derechos de acceso correspondientes definidos para el cliente. La información de control de acceso determina qué recursos se le permite utilizar al cliente en este servidor. En la arquitectura de seguridad Windows 2000, el control de acceso lo definen las membresías y privilegios de grupo en el registro de acceso de seguridad.

La autenticación del cliente de clave pública utiliza la información que se encuentra en el certificado del mismo, para correlacionarla con la información de control de acceso local. Esta correlación determina qué *autorización* tiene el cliente para acceder a los recursos en el sistema de servidor. El soporte inicial para la autenticación del cliente a través de Microsoft Internet Information Server está disponible mediante la administración de la base de datos de autorización para correlacionar al sujeto de certificado o al emisor de información con las cuentas Windows 2000. La base de datos de autorización puede ser tan simple o complicada, según sea necesario, para cumplir con los requerimientos de la aplicación.

Windows 2000 proporciona soporte en el extranjero para la autenticación del cliente mediante la implementación y de un servicio de seguridad que utiliza Active Directory para correlacionar la información de certificado con las cuentas Windows existentes. La correlación se puede realizar utilizando una búsqueda del nombre del tema de certificado en el directorio Windows, o mediante la búsqueda de las propiedades de directorio que identifican el certificado del cliente.

El soporte Windows 2000 para la autenticación del cliente integra certificados de clave pública con la arquitectura de seguridad Windows 2000. No se requiere una base de datos separada para definir el acceso a los derechos relacionados con los certificados de clave pública. La información de control de acceso la mantiene una membresía de grupo almacenada en el directorio Windows. Las herramientas de administración de servicio de directorio común de Windows se utilizan para otorgar derechos de acceso mediante la adición de usuarios Windows a los grupos.

Autenticación de usuarios externos

El soporte para la autenticación de certificados de clave pública en Windows 2000 permite que las aplicaciones del cliente se conecten a servicios seguros a nombre de los usuarios que no tienen una cuenta de dominio en Windows 2000. Los usuarios que están autenticados con base en un certificado de clave pública emitido por una Autoridad certificada confiable, pueden recibir acceso a los recursos Windows 2000. Las herramientas de administración de servicio de directorio permiten a los administradores o autoridades delegadas asociar a un usuario externo, o más, con una cuenta Windows 2000 existente para el control de acceso. El nombre del tema en el certificado X.509 versión 3 se utiliza para identificar al usuario externo que está relacionado con la cuenta.

Las empresas pueden compartir información de manera segura con personas seleccionadas de otras organizaciones sin tener que crear varias cuentas individuales Windows 2000. La correlación de muchos a uno de los certificados para los objetos de usuario Windows 2000 proporciona una autenticación sólida con base en los certificados de clave pública y las autorizaciones de control de acceso común. La autenticación de cliente de usuarios externos sigue requiriendo que el administrador del sistema configure la Autoridad de certificado para los certificados de usuarios externos como un CA confiable. Esto evita que alguna persona que tenga un certificado emitido por una autoridad desconocida reciba autenticación en el sistema como alguien más.

Microsoft Certificate Server

Microsoft Certificate Server, incluido en Windows 2000 e IIS 4.0, proporciona servicios personalizables para la emisión y administración de certificados, para aplicaciones que utilizan criptografía de clave pública. Certificate Server puede desempeñar un papel central en la administración de dicho sistema para proporcionar comunicaciones seguras a través de Internet, intranets corporativas y otras redes no seguras. Microsoft Certificate Server es personalizable para soportar los requerimientos de las aplicaciones de diferentes organizaciones.

Certificate Server recibe una solicitud de nuevos certificados sobre transportes, tales como RPC, HTTP o correo electrónico. Cada solicitud se verifica contra las políticas personalizadas específicas del sitio, grupos de propiedades opcionales del certificado que va a ser emitido y emisiones del certificado. De igual forma, permite que los administradores agreguen elementos a la lista de revocación de certificados (CRL) y publiquen una CRL firmada constantemente. Se incluyen interfaces programables para que sean utilizadas por los desarrolladores con el fin de crear soporte a transportes, políticas, propiedades de certificados y formatos adicionales.

El módulo de políticas para Certificate Server utiliza la autenticación de red de solicitudes de certificado para emitir certificados a los usuarios que tengan cuentas de dominio Windows 2000. El módulo de política puede ser personalizado para satisfacer las necesidades de las publicaciones de la organización. Certificate Server genera certificados en un formato estándar X.509. Los

certificados en formato X.509 se utilizan normalmente para autenticar servidores y clientes involucrados en comunicaciones seguras, utilizando ya sea los protocolos TLS o SSL. Las siguientes secciones describen los usos y algunas de las funciones clave de Certificate Server.

En una intranet corporativa o en Internet, los servidores tales como Microsoft Internet Information Server pueden realizar la autenticación del cliente para comunicaciones seguras, utilizando los certificados generados por Certificate Server. De igual forma, Certificate Server genera certificados de servidor utilizados por IIS y otros servidores de Web para proporcionar la autenticación del servidor y asegurar a los clientes (exploradores) que se están comunicando con la entidad pretendida.

CryptoAPI

Windows NT 4.0 proporcionó el soporte de criptografía de nivel bajo y proveedores de servicio criptográfico modulares en CryptoAPI. Windows 2000 se beneficia por la introducción de la administración de certificado CryptoAPI para soportar la seguridad de clave pública.

Entre algunas de las principales funciones de CryptoAPI se incluyen:

- Soporte a los certificados X.509 versión 3 y CRLs X.509 versión 2.0 a través de funciones de codificación/decodificación común, análisis de certificado y verificación.
- Soporte a solicitudes de certificado PKCS#10 y PKCS #7 para datos firmados y envueltos.
- Agregar y recuperar certificados y CRL en los almacenes de certificados, localizar certificados por sus atributos y asociarlos con claves privadas.
- Firma y verificación digital; así como soporte de encriptación de datos utilizando las funciones de nivel más alto disponibles para las aplicaciones en HTML, Java, Visual Basic® Scripting Edition (VBScript) y C/C++.

Las funciones CryptoAPI se utilizan en los componentes del sistema operativo Windows 2000, como son Software Publisher Trust Provider para la verificación Authenticode. Otras aplicaciones y servicios del sistema utilizan CryptoAPI versión 2.0 para permitir que la funcionalidad común habilite la tecnología de seguridad de clave pública.

ACCESO ENTRE EMPRESAS: SOCIOS DISTRIBUIDOS

Las empresas basadas en Internet ya están realizando negocios con clientes y socios a través de Internet. Los *resellers*, proveedores, distribuidores y cualquier persona que forme parte de un negocio amplio se puede conectar a intranets corporativas y acceder a información importante de la compañía. Los empleados y representantes en el campo utilizan cada vez más el acceso local a redes públicas y después se conectan a las fuentes de información corporativas remotas. La seguridad Windows NT está evolucionando con el fin de soportar las necesidades cambiantes de la computación distribuida a través de Internet.

La computación distribuida entre empresas no está limitada a una arquitectura única y la tecnología de seguridad no deberá limitar a las compañías a una sola forma de acceder a la información. A medida que la tecnología de seguridad cambia rápidamente están disponibles muchos enfoques. Windows 2000 integra soporte para los protocolos de seguridad y modelos del usuario que se adapten mejor a las necesidades de la aplicación o de negocios. Lo que es más importante, Windows 2000 proporciona una migración de la seguridad empresarial actual con la oportunidad de utilizar totalmente la seguridad de clave pública de Internet, a medida que la infraestructura madura.

A continuación se presentan algunas opciones que la seguridad Windows 2000 proporciona para la administración y soporte de relaciones entre empresas:

- Un enfoque inicial que se utiliza ampliamente hoy es la creación de cuentas de usuario para que los socios de negocios puedan acceder a los servicios de información corporativa. Al integrar la seguridad Windows 2000 con Active Directory se facilita la administración de estas cuentas especiales. Las unidades organizacionales que se encuentran en el directorio se pueden utilizar para agrupar cuentas relacionadas según el socio, proveedor u otras relaciones de negocios. La administración de estas cuentas se puede delegar a personas en la organización que administran tales relaciones con los socios. Las Redes privadas virtuales se establecen entre las organizaciones para encriptar tráfico de red a través de la red pública. Al utilizar este enfoque, los socios de negocios pueden utilizar acceso remoto a los servicios para obtener información corporativa, de la misma forma que cualquier otro empleado remoto. El acceso a las bases de datos o depósitos de información se puede controlar con un control de acceso Windows 2000.
- Las relaciones administrativas de dominio son otra herramienta para el establecimiento de relaciones entre las empresas. Active Directory proporciona mucho más flexibilidad para administrar un árbol de dominios jerárquicos. Con los nombres de dominio Windows 2000 integrados con la denominación DNS, el enrutamiento de Internet de la información entre dos dominios es fácil de configurar. Si así lo requiere la relación de negocios, el dominio se puede utilizar como una manera de configurar las aplicaciones de cliente/servidor que también tienen las funciones de privacidad e integridad necesarias para comunicarse sobre Internet. Los usuarios pueden utilizar ya sea los protocolos Kerberos o los de autenticación de clave pública para acceder a recursos compartidos en dominios remotos.
- Las organizaciones pueden utilizar la infraestructura de seguridad Microsoft Internet para resolver problemas de seguridad en Internet. Las compañías pueden emitir certificados de clave pública para socios específicos que necesitan acceder a recursos de información específicos. En lugar de crear una cuenta de usuario o definir una relación de confianza de dominios, los certificados se pueden utilizar como una manera de proporcionar identificación y autorización al usuario. Los certificados de clave pública, así como la infraestructura

necesaria para soportar la emisión de certificados y la verificación de revocación de certificado, son las maneras más eficaces para soportar las relaciones de empresa a empresa sobre Internet. Windows 2000 soporta certificados X.509 versión 3 emitidos por cualquier sistema de emisión de certificados. Los administradores del sistema en Windows 2000 definen qué Autoridades certificadas son confiables. Asimismo, pueden relacionar usuarios externos autenticados a través de certificados de clave pública con cuentas de usuario Windows 2000 para definir los permisos de acceso relacionados con dichos usuarios.

REGISTRO UNICO FRIMA ÚNICA PARA EMPRESAS Y PARA INTERNET

Windows 2000 administra las credenciales de seguridad de red del usuario de manera transparente después de un registro único satisfactorio. Al usuario no le preocupa si una conexión a un servidor de red utiliza NTLM, Kerberos o un protocolo de seguridad basado en una clave pública. Desde el punto de vista del usuario, se ha registrado en el sistema y ahora puede acceder a una amplia variedad de servicios de red.

Dentro de la empresa, el acceso a los recursos se determina mediante los derechos otorgados a las cuentas del usuario, o a través de membresías de grupo. A través de Internet, un acceso del usuario se basa en su identidad probada por una operación de firma de clave privada y el certificado de clave pública correspondiente. Todos los protocolos de seguridad dependen en alguna forma de las credenciales del usuario, las cuales se presentan a un servidor cuando se establece la conexión. Windows 2000 administra esas credenciales del usuario y utiliza de manera automática el grupo de credenciales adecuado, basado en el protocolo de seguridad involucrado.

Windows 2000 Active Directory soporta múltiples credenciales de seguridad como parte del uso seguro de la información de cuenta del usuario. Estas credenciales se utilizan para los servicios de autenticación empresarial que utilizan al controlador de dominio para la autenticación del usuario en línea. Los servidores de aplicaciones avanzadas pueden soportar la autenticación Windows 2000 integrada mediante el uso de la Interfaz del proveedor de servicio de seguridad para la autenticación de red.

Credenciales NTLM

El protocolo de autenticación NTLM es utilizado por los clientes Windows 2000 para conectarse a los servidores que ejecutan versiones anteriores de Windows NT. Por ejemplo, la autenticación NTLM se utiliza para conectarse a un componente compartido de archivo remoto en Windows NT 4.0 Server, o para conectar a un cliente Windows NT 4.0 con un componente compartido de archivo Windows 2000. Las credenciales NTLM consisten en el nombre de dominio, el nombre del usuario y la contraseña encriptada introducida una vez durante el registro inicial.

Los servicios de seguridad en un controlador de dominio administran una copia segura de las credenciales del usuario NTLM en Active Directory que se utilizarán para la autenticación NTLM. Un cliente Windows 2000 administra las credenciales NTLM introducidas en el registro del sistema del lado del cliente, para que se utilicen cuando el cliente se conecte a los servidores Windows NT 4.0 utilizando la autenticación NTLM. El soporte para las credenciales NTLM en la seguridad Windows 2000 es el mismo que se utiliza para la compatibilidad con Windows NT 4.0.

Credenciales Kerberos

El protocolo de autenticación primario para el dominio Windows 2000 es la autenticación Kerberos. Las credenciales Kerberos consisten en el nombre de dominio y de su área (los cuales pueden estar en forma de sobrenombres en Internet, como son BobbyB@microsoft.com) y contraseñas encriptadas estilo Kerberos. Cuando el usuario se registra en un sistema, Windows 2000 obtiene una o más boletas Kerberos para conectar a los servicios de red. Las boletas Kerberos representan las credenciales de red del usuario en la autenticación basada en Kerberos.

Windows 2000 administra de manera automática el *caché* de la boleta Kerberos para las conexiones con todos los servicios de red. Las boletas tienen hora de expiración y tienen que ser

renovadas con cierta frecuencia. La expiración y renovación de la boleta las maneja el proveedor de seguridad Kerberos y los servicios de aplicación asociados. La mayoría de los servicios, tales como el redireccionador del sistema de archivo, mantienen actualizadas automáticamente las boletas de sesión. La renovación regular de una boleta agrega seguridad a la sesión, mediante el cambio de clave de sesión periódicamente.

Pares de claves privadas/públicas y certificados

El usuario es quien administra las credenciales de Internet en forma de pares de claves privadas/públicas y certificados. Active Directory se utiliza para publicar los certificados de clave pública para los usuarios y los protocolos de acceso al directorio estándar se utilizan para ubicarlos. Las claves privadas y los certificados emitidos para los usuarios se mantienen en un almacén seguro, ya sea en el sistema local o en una tarjeta inteligente. El almacenamiento seguro se proporciona con la tecnologías de seguridad de Internet y se conoce como Almacén protegido.

La implementación del Almacén protegido se basa en la arquitectura CryptoAPI para Windows NT. CryptoAPI proporciona la funcionalidad de administración de claves así como otras capacidades criptográficas para la creación de un almacén seguro, guardando los certificados en el Almacén de certificados. La implementación de Windows 2000 de protocolos de seguridad basados en clave pública utilizan claves y certificados accesados desde un Almacén protegido y Almacén de certificados como credenciales de usuario para el acceso a servidores basados en Internet. En muchos casos, las propiedades definidas por el usuario de los certificados en el Almacén de certificados permiten que los protocolos de seguridad seleccionen y utilicen de manera automática el certificado correcto y la clave de firma. Los avances que existen en los protocolos de seguridad de Internet (SSL3/TLS) permiten que un servidor solicite credenciales específicas a un cliente, que se utilizan de manera automática desde el Almacén de certificados en caso de que estén disponibles.

La información que se encuentra en el Almacén protegido y el Almacén de certificados está disponible para los usuarios *roaming*, ya que han sido implementadas de manera segura como parte del perfil del usuario. Cuando un usuario se conecta por primera vez al cliente Windows, la información del perfil del usuario se copia en esta computadora. Si el usuario obtiene claves y certificados nuevos durante esa sesión, se actualiza el perfil del usuario en el servidor central cuando el usuario sale del sistema.

Transición sin fallas

La transición de una autenticación NTLM utilizada en Windows NT 4.0 (y versiones anteriores de Windows NT) a la autenticación de dominio Kerberos será muy transparente. Los servicios Windows 2000 soportan las conexiones cliente o servidor utilizando ambos protocolos de seguridad. La negociación de seguridad, ya sea mediante el nivel SSPI u otro protocolo de aplicación, proporciona otra opción para seleccionar la mejor correspondencia de las opciones de protocolo de seguridad disponibles.

La transición desde los servicios basados en una empresa que utiliza la autenticación Kerberos a servicios basados en Internet que utilizan autenticación de clave privada es completamente transparente para el usuario. El soporte Windows 2000 para múltiples credenciales del usuario hace posible que se utilice la tecnología de autenticación de clave secreta para los servicios de

aplicación empresarial con un rendimiento muy alto y la tecnología de seguridad de clave pública al conectarse a servidores basados en Internet. La mayoría de los protocolos de aplicación, tales como LDAP, HTTP/HTTPS o RPC, soportan la autenticación y están diseñados para soportar múltiples servicios de autenticación y seleccionar dichos servicios durante el establecimiento de una conexión.

En lugar de depender de una sola tecnología de autenticación y un solo protocolo de autenticación, Windows 2000 utiliza múltiples protocolos, según sea necesario, para ajustar la aplicación y los requerimientos de comunidad del usuario para una computación de red segura.

PROPORCIONAR UNA MIGRACION TRANSPARENTE A LA PROXIMA GENERACION DE DOMINIOS

La migración desde un ambiente Windows NT 4.0 a los dominios Windows 2000 es sencilla, debido a la compatibilidad hacia atrás con los protocolos de duplicación de seguridad y cuentas de Windows. Una migración sin problemas está disponible, ya que Windows 2000 cuenta con las siguientes funciones de interoperabilidad:

- Un controlador de dominio Windows 2000 puede desempeñar el papel de Windows NT 4.0 BDC y recibir la duplicación de la cuenta de dominio desde un Windows NT 4.0 PDC existente.
- Las estaciones de trabajo Windows NT 4.0 pueden enviar solicitudes de autenticación de red utilizando el protocolo de autenticación NTLM al controlador de dominio Windows 2000, actuando como un BDC en el dominio Windows NT 4.0.
- Los controladores de dominio Windows 2000 pueden establecer relaciones de confianza con los dominios Windows NT 4.0 y soportar la autenticación de pase entre los dominios. Esto significa que no se requiere que todos los dominios que existen en una empresa se actualicen a la seguridad de dominio Windows 2000 al mismo tiempo.

A la larga, los controladores de dominio Windows 2000 pueden reemplazar a los controladores de dominio Windows NT 4.0 en una actualización gradual de los Windows NT 4.0 BDC a los controladores de dominio Windows 2000. Las herramientas de administración de cuentas de Windows NT 4.0 se utilizan en el controlador de dominio primario siempre que PDC se ejecute en Windows NT 4.0. Finalmente, se pueden actualizar todos los controladores de dominio para utilizar Active Directory para la administración de cuentas y la duplicación de cuenta multimaestra.

El soporte Windows 2000 para los protocolos de autenticación múltiple significa que desde un dominio único de acceso en el escritorio, los usuarios pueden acceder a los servicios Windows 2000 en cualquier ambiente de dominio mezclado, como:

- Un servidor Windows 2000 en la conexión o dominio local, utilizando boletas de sesión Kerberos emitidas por el Centro de distribución de claves (KDC) en el controlador de dominio.
- Un servidor Windows 2000 en un dominio confiable, utilizando una referencia Kerberos para el KDC en el dominio confiable, para emitir una boleta de sesión al servidor remoto, o
- Un servidor Windows NT 4.0 en un dominio utilizando una autenticación de pase NTLM entre el cliente, el servidor Windows NT 4.0 y el controlador de dominio confiable.

Debido a que Windows 2000 sigue soportando la autenticación NTLM, los clientes Windows NT 4.0, que no utilizan la autenticación Kerberos, también pueden conectarse a los servidores de aplicación Windows 2000.

Estas funciones de interoperabilidad permiten flexibilidad para que las organizaciones planeen e implementen una estrategia de migración a servidores Windows 2000 que se ajusten mejor con sus necesidades de crecimiento empresarial.

RESUMEN

Los Servicios de seguridad distribuidas de Windows 2000 proporcionan soluciones flexibles para la creación de aplicaciones seguras, distribuidas y escalables. La administración de seguridad y administración cuentan con funciones más ricas para la delegación y control de cuenta granular. Active Directory soporta dominios con un mayor número de cuentas en un ambiente de nomenclatura estructurado en unidades organizacionales. La administración de confianza entre dominios es más simple, ya que proporciona mayor flexibilidad para utilizar los dominios en forma que refleje las necesidades de la empresa.

Las API de seguridad Windows para la autenticación de red, privacidad de datos, firmas digitales y soporte de encriptación aseguran el desarrollo de la aplicación para la empresa e Internet. Las interfaces SSPI y CryptoAPI, así como las abstracciones de interfaz COM y de DCOM de nivel más alto, hacen que todas las funciones de seguridad integradas en Windows 2000 estén disponibles para su uso por todas las aplicaciones. La arquitectura sólida de seguridad de Windows NT se utiliza de manera consistente a través de todos los componentes del sistema y será ampliada para soportar la autenticación sólida y la seguridad de clave pública. Estas funciones no tienen comparación con cualquier otra plataforma de aplicación distribuida disponible en la actualidad.

Windows 2000 Distributed Security integra los estándares maduros de Internet para la autenticación, al tiempo que presenta la nueva tecnología de seguridad de clave pública basada en la dirección de la industria y estándares disponibles. La gran mayoría de los estándares de seguridad de clave pública en Internet aún se están creando. Microsoft participa en el desarrollo de estos estándares, pero reconoce que tienen que cambiar con el paso del tiempo. La arquitectura de seguridad Windows 2000 está diseñada específicamente para incorporar nueva tecnología de seguridad en forma de protocolos, proveedores de servicio criptográficos o tecnología de autenticación de terceros. Los clientes que implementan Windows 2000 tienen opciones sobre qué tecnología de seguridad desean utilizar, cómo integrar la seguridad en su ambiente de aplicaciones con el mínimo impacto y cuándo migrar a la nueva tecnología, a medida que esté disponible.

En conjunto, todo esto convierte los Servicios de seguridad distribuida de Windows 2000 en las mejores bases para la computación segura y distribuida sobre Internet.

PARA MÁS INFORMACION

Para obtener la información más reciente de Windows 2000 y Windows NT Server, visite los sitios Web en http://www.microsoft.com/ntserver y el Windows NT Server Forum en Microsoft Network (GO WORD: MSNTS).

Para obtener más información de Windows 2000 Active Directory, consulte el documento estratégico adjunto, *Resumen técnico de Microsoft Windows NT Active Directory*.

Información adicional sobre seguridad Microsoft Internet está disponible en el sitio Web en http://www.microsoft.com/security.

Información adicional sobre la arquitectura de seguridad Windows NT, interfaz de proveedor de soporte de seguridad, CryptoAPI y las API de seguridad Windows NT está disponible en las referencias en línea para el SDK de la plataforma Microsoft.