Latinoamérica

Microsoft TechNet

Capítulo 4: Diseño de la infraestructura de claves públicas

Publicado: octubre 11, aaaa | Actualizado: 24/11/04

En esta página

Introducción

El capítulo anterior ofrecía un diseño lógico para una solución inalámbrica segura que depende de una infraestructura de claves públicas (PKI, Public Key Infrastructure). Este capítulo define el proceso de diseño de una PKI basada en los Servicios de Certificate Server de Microsoft® Windows® 2003. Para que los costos de implementación y administración sean razonables, el diseño de la solución es bastante simple y capaz de emitir certificados para clientes inalámbricos seguros, así como para la infraestructura de red de área local inalámbrica (WLAN).

Sin embargo, aunque el objetivo principal consiste en diseñar una PKI que sea compatible con WLAN seguras, no olvide que una PKI también puede constituir una parte importante de la infraestructura de seguridad global de su organización que otras aplicaciones del entorno podrán utilizar en el futuro. El diseño de la solución puede ampliarse, de modo que la inversión realizada en esta infraestructura queda protegida. Aunque el diseño no sea apropiado para emitir todo tipo de certificados, permitirá agregar funcionalidad y capacidad adicionales más adelante para satisfacer un conjunto más amplio de requisitos de seguridad que los que aquí se tratan.

Este capítulo tiene tres objetivos principales. El primero es presentar las decisiones del diseño de la solución y el razonamiento que hay tras ellas. El segundo es proporcionar información general de planeamiento para ayudarle a decidir si estas decisiones son las apropiadas para su PKI. El tercero es indicar modos en que la solución básica puede extenderse para cubrir necesidades de seguridad que quedan fuera del alcance de esta solución.

Las expresiones como “Esta solución utiliza la opción...” o “Este diseño usa...” que aparecen en este capítulo hacen referencia a decisiones tomadas como parte del diseño de la solución implementadas en los capítulos de las guías de generación y operaciones.

Las expresiones como “Debería considerar...” hacen referencia a contextos en los que debe tomar decisiones según sus propios requisitos. En la mayoría de los casos esto ocurrirá durante la descripción de formas en que podría ampliar la solución para cubrir las necesidades de seguridad generales de su organización. Por esta razón, algunos temas ofrecen consideraciones más detalladas que le ayudarán a comprender las implicaciones de los pasos específicos y evitarán que tenga que consultar otros documentos.

Requisitos previos

Se necesita un entendimiento claro de los principios generales y la terminología específica de PKI. Si no está familiarizado con la tecnología, lea algunos artículos mencionados en la sección “Información adicional” al final de este capítulo.

Antes de continuar, le será de utilidad consultar el capítulo “Designing a Public Key Infrastructure”, dedicado al diseño de infraestructuras de claves públicas, incluido en el *kit de implementación* de *Microsoft Windows Server*™ 2003. En la sección “Información adicional” al final de este capítulo encontrará el modo de obtener esta información. Este capítulo sigue la estructura de dicho capítulo en el kit de implementación para que pueda

consultar más fácilmente la información general y las consideraciones detalladas que le ofrecemos aquí.

La sección “Información adicional” incluye vínculos a información detallada adicional sobre los procesos de planeamiento y diseño de una PKI de Windows Server 2003.

Descripción general del capítulo

Las tareas de planeamiento e implementación de una PKI que se adapte a las necesidades actuales y futuras de su organización requieren un estudio minucioso. Por lo general, una PKI no se utiliza para proporcionar la solución a un problema de seguridad único y aislado. La implementación de PKI en una organización suele llevarse a cabo para cubrir varios requisitos de seguridad interna, así como requisitos de seguridad de negocios a la hora de trabajar con clientes externos o socios.

El diagrama de flujo siguiente ilustra la estructura del capítulo.

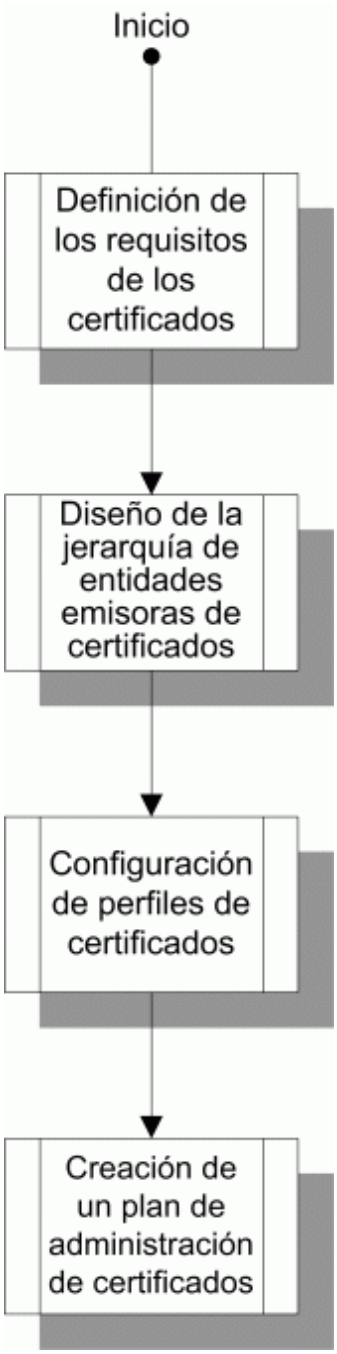

Figura 4.1 Estructura del capítulo para el planeamiento de Servicios de Certificate Server

Los cuatro pasos principales son:

- **Definición de los requisitos de certificados**. Este paso implica la definición de los problemas de seguridad que está intentando resolver. Se basa en los usuarios y aplicaciones específicas que necesitan seguridad mejorada: la ubicación de estos usuarios, el grado de seguridad mejorada requerida, etc. No podrá empezar a crear su PKI hasta que haya definido sus requisitos de seguridad y comerciales.
- **Diseño de la jerarquía de entidades emisoras de certificados**. En consonancia con varios factores, deberá crear una infraestructura de entidades emisoras de certificados (CA). Este paso implica la definición de un modelo de confianza, la determinación de la cantidad de CA necesarias, el modo en que las administrará y la forma en que puede ampliar su PKI mediante la introducción de CA adicionales o el establecimiento de relaciones de confianza con otras organizaciones. Adicionalmente, este paso se ocupa del modo en que la PKI se integra con otras tecnologías en la infraestructura de TI, como el servicio de directorio Active Directory® y Microsoft Internet Information Services (IIS).
- **Configuración de perfiles de certificados**. Este paso incluye decisiones sobre los tipos de certificados que van a utilizarse, el nivel de seguridad de las claves de cifrado asociadas con dichos certificados, la duración de éstos y su capacidad de renovación.
- **Creación de un plan de administración de certificados**. Este paso define el modo en que los certificados se emiten a los usuarios finales, el procesamiento de las solicitudes de certificados y la administración y distribución de las listas de revocación de certificados (CRL, Certificate Revocation List).

Principio de la página

Definición de los requisitos de los certificados

En esta sección se definen los propósitos para los que las PKI emiten certificados y los requisitos de seguridad para cada uno de ellos.

Creación de una orden de prácticas de certificados

Al diseñar la PKI, debe anotar las decisiones que toma acerca de cómo se emitirán los certificados y cómo se utilizarán en la organización. Estas decisiones reciben el nombre de "directivas de certificados", y los documentos que las registran se denominan "declaraciones de directivas de certificados" y "declaraciones de prácticas de certificados".

En términos formales, una *directiva de certificados* (CP, Certificate Policy) es un conjunto de normas que determinan el funcionamiento de la PKI. Por ejemplo, registra la aplicabilidad de un certificado a un grupo determinado de clientes o aplicaciones con requisitos de seguridad comunes. Por otro lado, una *declaración de prácticas de certificados* (CPS, Certificate Practices Statement) es una declaración de las prácticas que una organización utiliza para administrar los certificados que emite. Describe cómo se interpreta la directiva de certificados de una organización en el contexto de la arquitectura del sistema y de los procedimientos operativos de la organización. Una CP constituye un documento aplicable a toda la organización, mientras que una CPS es un documento específico a una entidad emisora, aunque las entidades emisoras pueden tener una CPS común si llevan a cabo la misma tarea (por ejemplo, cuando se intenta distribuir la carga de las entidades emisoras en varios servidores para mejorar el nivel de rendimiento o resistencia).

En lo que respecta a algunas organizaciones y usos de certificados, CP y CPS se consideran documentos o renuncias legales. Normalmente conllevan asesoramiento legal especializado, lo que queda fuera del alcance de este capítulo. Sin embargo, no existe ningún requisito estricto para que deba producir alguno de estos documentos como parte de su PKI. A menos que tenga razones legales o comerciales específicas para ello, no es necesario que emplee el tiempo y los gastos que implica producir y mantener declaraciones formales de directivas y prácticas de certificados.

Aunque no necesite una CP o CPS formal, debería documentar sus directivas de certificados y prácticas operativas de alguna forma. Las directivas de certificados deben formar parte de la directiva de seguridad global de la organización y las prácticas operativas deben formar parte de los procedimientos de administración de seguridad. Puede hacer referencia a esto como CPS informal.

Según los usos que tenga previstos para la PKI deberá decidir si requiere producir una declaración de directivas y una CPS formales. Si requiere una CPS formal, probablemente deberá publicarla e incluir referencias a ella en los certificados de entidad emisora. Aunque en esta solución no se incluyen orientaciones para escribir una CPS formal, las instrucciones acerca de cómo publicarla se encuentran en el capítulo 7, Implementación de la infraestructura de claves públicas. No suele ser necesario publicar CPS informales.

En el resto de este capítulo se hacen referencias frecuentes a la documentación de decisiones en la CPS. Estas instrucciones se aplican por igual a las CPS formales y a las informales.

Algunas fuentes de información adicionales sobre la producción de una CPS se incluyen en la sección “Información adicional” al final de este capítulo.

Identificación de aplicaciones de certificados

El primer paso del proceso de diseño de PKI es identificar la lista de aplicaciones que utilizarán los certificados. Debe documentar los tipos y el número aproximado de certificados que requiere cada aplicación. No es necesario que especifique los detalles de los certificados en esta fase, basta con proporcionar una breve descripción de los mismos.

La solución inalámbrica segura requiere certificados para los clientes inalámbricos y para los servidores Windows Remote Authentication Dial-In User Service (RADIUS). El servidor RADIUS de Microsoft es un componente de Windows Server, el servicio de autenticación de Internet (IAS, Internet Authentication Service).

Los tipos de certificados requeridos se muestran en la tabla siguiente. Aunque no sea estrictamente necesario para esta solución, la PKI también emitirá certificados para los controladores de dominio (éste es el valor predeterminado cuando se instala una entidad emisora de certificados de Windows 2003 Enterprise en el bosque).

Tabla 4.1: Requisitos de los certificados para una solución inalámbrica segura

Aplicación	Tipo de certificado	Número de certificados
WLAN segura	Certificados de autenticación de cliente para usuarios	Todos los usuarios que requieren acceso a la WLAN
	Certificados de autenticación de cliente para equipos	Todos los equipos de la LAN inalámbrica
	Certificados de autenticación de servidor para los servidores IAS	Todos los servidores IAS
Active Directory	Autenticación de controladores de dominio	Todos los controladores de dominio del bosque

En el futuro, la PKI podría ampliarse y emitir certificados para las aplicaciones que aparecen en las tablas siguientes.

Tabla 4.2: Posibles requisitos de certificados futuros

Aplicación	Tipo de certificado	Número de certificados
Acceso de clientes a red privada virtual (VPN)	Autenticación del equipo cliente (IPSec)	Todos los clientes VPN remotos
VPN de sucursal a sucursal	Autenticación de servidor VPN (IPSec)	Todos los enrutadores VPN

Seguridad IP (IPSec)	Autenticación del cliente equipo	Todos los equipos cliente y servidor que requieren IPSec
Seguridad Web	Autenticación de usuarios para aplicaciones Web de intranet	Todos los usuarios
	Servidor Web de intranet	Servidores Web de intranet segura
Sistema de cifrado de archivos (EFS)	Usuario EFS	Todos los usuarios
	Recuperación de datos EFS	Agentes de recuperación
Correo electrónico seguro	Firma y cifrado de Extensiones seguras multipropósito al correo de Internet (S/MIME)	Todos los usuarios de correo electrónico
	Recuperación de claves	Agentes de recuperación
Tarjetas inteligentes	Inicio de sesión de tarjeta inteligente	Usuarios de dominio
Firma de código	Firma de macro y código internos	Administrador de versión de códigos

Definición de clientes de certificados

Para las aplicaciones enumeradas en la sección anterior, debería definir los clientes que utilizarán los certificados. En este contexto, el término “cliente” hace referencia a cualquier persona, proceso de software o dispositivo que utilice los certificados emitidos por la PKI. Por ejemplo, los clientes incluyen usuarios, servidores, estaciones de trabajo y dispositivos de red. Para entender el modo de emisión de los certificados resulta necesario entender dos categorías de clientes principales: el sujeto del certificado (o *entidad final*) y el resto de los usuarios del certificado.

Las entidades finales son clientes que reciben certificados de la PKI. El certificado contará con una o más entradas en los campos de **sujeto** o **nombre alternativo del sujeto** que identifican al cliente (por ejemplo, nombre del host, dirección de correo electrónico o nombre distinguido del directorio) como propietario del certificado. Otros usuarios de certificados son clientes que pueden, por ejemplo, comprobar certificados de entidades finales o buscarlos en un directorio, pero que no han recibido necesariamente certificados de la PKI.

El ejemplo siguiente suele servir para esclarecer la distinción: un usuario de Internet que compra algo en un sitio Web seguro será un usuario del certificado de nivel de sockets seguro (SSL, Secure Sockets Layer) del sitio Web. Sin embargo, el sitio Web es una entidad final de certificados: su identidad, www.woodgrovebank.com, se encuentra codificada en el campo de **sujeto** del certificado. Solamente el sujeto del certificado dispone de acceso para utilizar la clave privada del certificado. Nota: normalmente, los *sujetos* del certificado son además *usuarios* de su propio certificado y de los certificados de otros.

Nota: el término “entidad final” es el término correcto técnicamente hablando pero, en la mayor parte de este capítulo, se utilizará “sujeto del certificado”, que es un término más común.

Debe dividir cada tipo de cliente, tanto para sujetos como usuarios de certificados, en categorías y, para ello, debe responder las siguientes preguntas:

- ¿Es el cliente una persona, un equipo o un dispositivo o bien un proceso de software?
- ¿En qué plataformas (versión de sistema operativo) se utilizarán los certificados?
- ¿Cuál es la ubicación de red del cliente? Por ejemplo, si está conectado a la LAN interna, en una organización asociada, en Internet, etc.
- ¿Es el cliente miembro de un dominio? Si es así, ¿está en un dominio diferente o en un bosque distinto de la

entidad emisora? ¿Se trata de un dominio que no es de confianza?

- ¿Qué tipo de operaciones necesita realizar el cliente? Por ejemplo, inscribir certificados, firmar con certificado, comprobar la confianza de los certificados, buscar certificados en un directorio y comprobar el estado de revocación de certificados.

Esta clasificación tendrá importancia en muchas decisiones de diseño como, por ejemplo, el modo de emisión del certificado, el nivel de confianza que se puede depositar en un certificado determinado y la forma de publicación de la información de revocación del certificado.

Para esta solución, las categorías de cliente se resumen en las tablas siguientes.

Tabla 4.3: Categorías de sujetos de certificados (entidades finales)

Certificado	Tipo de cliente	Plataforma	Ubicación	Dominio	Operaciones del certificado
Autenticación de cliente inalámbrico	User	Windows XP	Red interna	Miembro de dominio	–inscribir –autenticar
Autenticación de cliente inalámbrico	Equipo	Windows XP	Red interna	Miembro de dominio	–inscribir –autenticar
Autenticación de servidor IAS	Equipo	Microsoft Windows Server™ 2003	Red interna	Miembro de dominio	–inscribir –autenticar –canal seguro

En esta aplicación, los usuarios de los certificados serán el mismo conjunto de clientes pero con las funciones invertidas. Por ejemplo, el servidor IAS se convertirá en el usuario de los certificados de cliente y necesitará comprobarlos. Generalmente, la comprobación incluye verificar que el certificado está encadenado a una entidad emisora de certificados raíz y que la firma suministrada por el cliente coincide con la clave pública en el certificado del cliente. Además, es posible que el certificado deba someterse a una comprobación de revocación. Para ver una explicación detallada acerca de la revocación y el estado de certificados, consulte el documento *Troubleshooting Certificate Status and Revocation* .Encontrará la referencia completa en la sección “Información adicional” al final de este capítulo.

Tabla 4.4: Categorías de usuarios de certificados

Certificado	Tipo de cliente	Plataforma	Ubicación	Dominio	Operaciones del certificado
Autenticación de cliente inalámbrico	–equipo	Windows Server 2003	Red interna	Miembro de dominio	–verificar –comprobar revocación
Autenticación de cliente inalámbrico	–equipo	Windows Server 2003	Red interna	Miembro de dominio	–verificar –comprobar revocación
Autenticación de servidor IAS	–usuario	Windows XP	Red interna	Miembro de dominio	–verificar

	–equipo				

En las tablas anteriores puede identificar las plataformas y las clases de operaciones con las que debe ofrecer compatibilidad. Aunque éste no sea el caso en el escenario de WLAN, es posible que para otras aplicaciones necesite admitir la búsqueda o la comprobación de certificados por clientes en Internet, admitir la inscripción desde plataformas ajenas a Windows, etc. Muchos de estos puntos deben decidirse en una fase temprana del proceso de diseño, por lo que es importante considerar los posibles requisitos de certificados futuros.

Esta solución supone lo siguiente acerca de los requisitos futuros:

- probablemente se requerirá la comprobación de certificados de clientes ajenos a Windows.
- Puede requerirse la comprobación de certificados de Internet.
- Se requerirá la compatibilidad de los sujetos y los usuarios de certificados de plataformas que no son Windows XP y Windows Server 2003.

Aunque el diseño no satisface necesariamente estos requisitos en este momento, será fácil acomodarlos.

Definición de los requisitos de seguridad de certificados

La seguridad de un certificado también se conoce como nivel de seguridad. Puede decirse que es la medición de la fuerza que vincula al sujeto del certificado con el certificado en sí. Refleja el nivel de confianza que puede tener en que la persona (o el dispositivo) que utiliza el certificado es realmente la misma que el sujeto nombrado en el certificado. El nivel de seguridad es la medición de dos elementos principales:

- el rigor del proceso de registro e inscripción de certificados. Por ejemplo, ¿tuvo la persona que acudir personalmente y presentar un documento de identificación con fotografía para obtener su certificado o bastó con una dirección de correo electrónico?
- la manera en que se almacena la clave privada. Cuanto más difícil sea copiar o comprometer de otra forma la clave, mayor será la seguridad de que siga en posesión exclusiva del propietario original, el sujeto del certificado.

Los dos están fuertemente vinculados, ya que no existe ninguna razón para invertir en medidas costosas de protección de claves privadas si nunca ha estado verdaderamente seguro de la identidad del propietario de la clave privada. De forma similar, un arduo proceso de registro que implique exhaustivas comprobaciones de antecedentes y pruebas de ADN sirve de poco si, posteriormente, la clave privada se almacena de una forma que no es lo suficientemente segura.

Conseguir una seguridad superior para un certificado cuesta dinero y, con frecuencia, no es necesario para muchos de los usos de los certificados. Si la seguridad que desea de un certificado es que pertenezca a un usuario de dominio autorizado, las credenciales del dominio son totalmente aceptadas como evidencia de registro para inscribir un certificado.

Debe documentar el significado de los niveles de seguridad que utiliza en las directivas de certificados y declaraciones de prácticas.

Para esta solución, la tabla siguiente define tres niveles de seguridad.

Tabla 4.5: Niveles de seguridad de los certificados

Nivel	Requisitos de registro	Requisitos de almacenamiento de claves
Estándar (Baja)	Aprobación automática dependiente del dominio u otra identificación basada en contraseña	Claves de software

Media	Aprobación del administrador de certificados, comprobación visual de identificador (tarjetas inteligentes) o firma de la oficina de inscripción	Claves de software o token de prueba contra manipulaciones de hardware (tarjeta inteligente o token USB)
Alta	Firma del oficial de inscripción nominado y aprobación del administrador de certificados	Token de prueba contra manipulaciones de hardware (tarjeta inteligente o token USB)

Existe cierto grado de superposición entre estas categorías. No se trata de divisiones técnicas estrictas, sino de divisiones de directivas. En su organización, los límites entre ellas se basarán en las decisiones de directivas que tome acerca de cómo desea que se traten los certificados. Por lo general, los certificados de seguridad alta son escasos, mientras que los certificados de seguridad baja son muy comunes.

Importante: en este capítulo se utilizan los términos “certificados de valor estándar” y “certificados de seguridad estándar” en lugar de “certificados de valor bajo” y “certificados de seguridad baja”. Estos últimos ofrecen connotaciones negativas; “estándar” refleja el significado deseado de forma más precisa.

La división de categorías de seguridad definidas en la tabla anterior puede pulirse aún más si se divide cada una en tipos de sujetos diferentes. Las categorías más comunes son las siguientes:

- Equipo: se trata en realidad de cualquier equipo o dispositivo que se encuentre en la organización.
- Usuario interno: representa empleados a tiempo completo o personal que considere equivalente (por ejemplo, personal con contrato).
- Usuario externo: representa cualquier otra entidad que se encuentra fuera de la organización pero con la que realiza algún tipo de actividad comercial o con la que tiene una relación legal (por ejemplo, asociados comerciales y clientes).

La razón de esta distinción es que, a estos tipos de sujetos diferentes, se les aplican normalmente unas directivas de certificado bastante distintas; es decir, las condiciones bajo las cuales se emite, revoca o renueva un certificado. Aunque no haya previsto ningún certificado para una categoría determinada, es aconsejable documentar las directivas de certificado que se aplicarían a dicha categoría de modo que puedan prepararse correctamente las directivas y CPS. En la tabla siguiente se describen los resultados de combinar los niveles de seguridad y las categorías de sujetos.

Tabla 4.6: Categorías de seguridad de los certificados

Categoría de seguridad de certificado	**Características de ejemplo de categoría de seguridad**	**Tipos de certificado de ejemplo**
Certificados de equipo		
Certificados de equipo de seguridad estándar	–aprobación automática basada en las credenciales del dominio del equipo –renovación anual	–equipo WLAN –IPsec
Certificados informáticos de seguridad intermedia	–aprobación necesaria por parte del administrador de certificados –almacenamiento de claves en software –renovación anual	–servidor de Web –autenticación de servidor IAS
Certificados de equipo de seguridad alta	–aprobación por parte del administrador de certificados	–autoridad de certificados

	–almacenamiento de claves en módulo de seguridad de hardware (HSM, Hardware Security Module)	–servicio de tiempo seguro –autoridad de registro
Certificados de usuario interno		
Certificados de usuario interno de seguridad estándar	–aprobación automática basada en las credenciales del dominio del usuario –renovación anual	Usuario EFS
Certificados de usuario interno de seguridad media	–aprobación necesaria por parte del administrador de certificados u oficial de inscripción –almacenamiento de claves en tarjeta inteligente o software –renovación anual	–correo electrónico seguro –autorización financiera de valor bajo-medio –inicio de sesión con tarjeta inteligente –firma de códigos internos –agente de recuperación de datos –agente de recuperación de claves
Certificados de usuario interno de seguridad alta	–comprobación necesaria del identificador físico del sujeto del certificado –aprobación necesaria por parte del administrador de certificados –firma de la oficina de inscripción requerida mediante solicitud –almacenamiento de claves en tarjeta inteligente –renovación semestral	–autorización financiera de valor alto –firma de códigos comerciales
Certificados (de usuarios) externos		
Certificados externos de garantía estándar	–aprobación automática basada en contraseña preasignada –renovación anual	Autenticación de cliente (autenticación en el sitio Web de Internet)
Certificados externos de seguridad media	–aprobación necesaria por parte del administrador de certificados –almacenamiento de claves en tarjeta inteligente –renovación semestral	Autorización financiera de compañía a compañía (B2B)
Certificados externos de seguridad alta	–comprobación necesaria del identificador físico del sujeto del certificado –aprobación necesaria por parte del	Transacción B2B de valor muy alto

	administrador de certificados –firma de la oficina de inscripción requerida mediante solicitud –almacenamiento de claves en tarjeta inteligente –renovación semestral	

Nota: si no necesita utilizar una categoría específica, no tiene por qué crearla. Quizás desee utilizar un sistema de clasificación más simple o más complejo y no todas las combinaciones darán como resultado un tipo de certificado que vaya a emitir.

No existen razones técnicas por las que estos tipos de sujetos de certificados diferentes no puedan tratarse todos de la misma manera. Sin embargo, normalmente se definirán directivas de seguridad diferentes para tipos de sujetos diferentes; por ejemplo, los empleados internos se tratarán de forma diferente que el personal de otras organizaciones. Las distintas directivas de certificados (y su integración a las distintas CPS) pueden afectar a las decisiones de cómo deben estructurarse las entidades emisoras para que emitan estos tipos de certificados diferentes. Esto se explicará más adelante en el capítulo.

También debe plantearse si el mismo administrador será el responsable final de los certificados emitidos a estas tres categorías de usuarios de certificados (o “entidades finales”, en terminología de PKI). En la mayoría de las organizaciones, la persona que puede certificar que un equipo es miembro legítimo del domino no es la misma persona que puede certificar la identidad de una compañía asociada. Debe documentar estas relaciones de responsabilidad en la CPS.

Definición de la seguridad de los certificados de aplicación

Las categorías de seguridad de certificados definidas en la sección anterior pueden utilizarse para clasificar los tipos de certificados para el diseño. Esto se indica en la tabla siguiente.

Tabla 4.7: Requisitos de seguridad de los certificados

Tipo de certificado	Categoría de seguridad	Plataforma	Ubicación lógica	Aprobación	ClaveTamaño	Período de validez
Autenticación de cliente: usuario	Certificados de equipo de seguridad estándar	–Windows XP –Windows Server 2003	Interno	Automático (autenticación de dominio)	Media	Media
Autenticación de cliente: equipo	Certificados de usuario de seguridad estándar	–Windows XP –Windows Server 2003	Interno	Automático (autenticación de dominio)	Media	Media
Autenticación de servidor IAS	Certificados informáticos de seguridad intermedia	–Windows XP –Windows Server 2003	Interno	Manual	Media	Media

Estos amplios requisitos se refinarán en perfiles de certificado específicos en la sección “Configuración de perfiles de certificados”, incluida más adelante en el capítulo.

Combinación de propósitos de certificados

Es posible combinar varias funciones (o usos) de aplicación en un solo certificado a fin de utilizarlo para firmar el correo electrónico, iniciar la sesión en la red y otorgar acceso a una aplicación. La combinación de usos dará como resultado una menor cantidad de tareas de administración y almacenamiento en los servidores de certificados y directorios.

Sin embargo, existen inconvenientes en los certificados de varios propósitos. Por ejemplo, distintas aplicaciones pueden requerir un proceso de aprobación diferente del certificado. La mayoría de las razones para el uso de varios certificados son técnicas pero la principal es que, normalmente, diferentes aplicaciones requieren distintos niveles de seguridad de certificados; es decir, diferentes niveles de seguridad vinculan el certificado al sujeto del certificado. Esto puede incluir diferencias en cualquiera o en todos los puntos siguientes:

- Proceso de aprobación de certificados
- Longitud de clave
- Mecanismo de almacenamiento de claves
- Duración del certificado

Por ello, la estrategia de combinar usos de certificado del mismo nivel de seguridad suele ser la mejor opción. Los certificados de autenticación de cliente utilizados en esta solución incluirán usos para otras aplicaciones estándar, como IPSec y la autenticación de equipos. Según vaya definiendo requisitos para otros usos de certificados, podrá incluirlos y volver a emitir los certificados (esto requerirá la renovación forzada, que puede iniciarse desde la definición de plantilla de certificado).

Sin embargo, los certificados de servidor IAS están considerados como certificados de seguridad media. La amenaza que representa un certificado de servidor no autorizado es muy superior a la planteada por un certificado de cliente ilegítimo. Por esta razón, los certificados de servidor deben tratarse con cuidado, y Microsoft recomienda que no se combinen con usos para aplicaciones de seguridad estándar.

Principio de la página

Diseño de la jerarquía de entidades emisoras de certificados

Para la compatibilidad de las aplicaciones basadas en certificados de la organización, debe establecer una estructura de entidades emisoras vinculadas que sea responsable de emitir, validar, renovar y revocar los certificados según sea necesario. Las entidades emisoras se basan a su vez en la infraestructura de TI subyacente para acciones como la autenticación de sujetos de certificados, la publicación de certificados y la publicación de la información de revocación de certificados.

El objetivo del establecimiento de una infraestructura de entidades emisoras es ofrecer un servicio de confianza a los usuarios, facilidad de uso para los administradores y flexibilidad para satisfacer las necesidades actuales y las futuras, a la vez que seguir manteniendo un nivel óptimo de seguridad para la organización.

Selección de un modelo de confianza

El primer paso en el diseño de la infraestructura de entidades emisoras es determinar el modelo de confianza más adecuado para sus requisitos. Los dos modelos básicos son la confianza de jerarquía y la confianza de red, aunque es posible combinar elementos de los dos en un modelo de confianza híbrida. Si desea obtener más información sobre estos modelos, vea el capítulo sobre el diseño de infraestructuras de claves públicas en el *kit de implementación de Windows Server 2003* al que se hace referencia en la sección “Información adicional”.

Esta solución utiliza el modelo de confianza de jerarquía. Las razones para ello son:

- las entidades emisoras sin conexión pueden tratarse con un nivel de seguridad mayor que las entidades emisoras en línea. Por lo tanto, la creación de una o varias capas de entidades emisoras sin conexión incrementa el nivel global de confianza posible en los certificados emitidos.
- las jerarquías pueden funcionar más fácilmente sin la presencia de un directorio, lo que es importante para la compatibilidad de clientes externos que no tienen acceso al directorio interno. el modelo de confianza de red suele requerir directorios de modo que los usuarios puedan consultar certificados cruzados de entidades

emisoras para crear cadenas de confianza. La cadena de confianza en jerarquías es siempre explícita.

- Hay que mantener y distribuir menos delimitadores de confianza a los clientes: sólo se debe distribuir el certificado de entidad emisora raíz a los usuarios de certificados.
- Incluso en una jerarquía con raíz, siempre existe la opción de incluir varios delimitadores de confianza (o raíces) en el futuro mediante certificaciones cruzadas con otras jerarquías. Esto significa que el diseño puede acomodar elementos como, por ejemplo, fusiones de organizaciones para devolver el control de los certificados a los departamentos para propósitos especiales.

Una sola raíz es adecuada para la solución propuesta.

Raíz de otra empresa frente a raíz interna

Es posible utilizar una raíz interna como delimitador de confianza para la PKI o utilizar los servicios de una entidad emisora comercial para ello. El uso de una raíz de otra empresa implica que las CA emisoras vienen certificadas por la entidad emisora raíz comercial (normalmente a través de una o varias entidades emisoras intermedias). Por lo tanto y en última instancia, todos los certificados que emita tienen sus delimitadores de confianza en esta entidad emisora raíz externa.

Nota: aunque esta opción no se considera explícitamente en esta guía, es posible satisfacer todos los requisitos de certificados de la organización externamente, mediante una entidad emisora comercial. Puede usar un servicio administrado in situ u obtener certificados directamente del proveedor de certificados. Con frecuencia, esto no es económicamente viable, excepto para pequeñas organizaciones o para usos de certificados restringidos. Esta decisión es totalmente independiente de la consideración del uso de una raíz interna o una raíz de otra empresa, aunque suelen confundirse.

Hay varias ventajas en la utilización de una raíz comercial para los certificados emitidos internamente:

- brinda a las empresas externas (por ejemplo, los clientes que visitan el sitio Web seguro o la organización asociada que recibe correo electrónico firmado) un mayor grado de confianza al realizar transacciones seguras con la organización. Normalmente ya confiarán en la entidad emisora raíz de otra empresa y no deberán tomar la decisión de si deben confiar en sus certificados.
- permite a la organización beneficiarse de la experiencia de un proveedor de servicios profesional, lo que incluye el conocimiento que el proveedor tiene de temas técnicos, legales y comerciales asociados al uso de certificados. (Sin embargo, a menos que el proveedor de certificados emita todos los certificados, el usuario seguirá siendo responsable de la manera en que los certificados se emitan y utilicen y deberá documentar esto en la CPS.)

Sin embargo, existen varios inconvenientes relacionados con este enfoque:

- Normalmente implicará un alto costo por certificado.
- El proveedor de certificados puede requerir seguridad estricta y medidas de auditoría para todas las entidades emisoras subordinadas a la entidad emisora raíz comercial.
- Los usuarios y dispositivos internos deben tener acceso a las listas CRL de las entidades emisoras de otras empresas publicadas en Internet.
- algunas aplicaciones pueden requerir la presencia de extensiones o parámetros específicos en los certificados de entidades emisoras intermedias y raíz (por ejemplo, el inicio de sesión con tarjeta inteligente de Microsoft Windows), que pueden no estar disponibles en el proveedor de certificados.
- El acuerdo comercial entre la organización y el proveedor de certificados puede restringir el tipo de certificados que las entidades emisoras subordinadas pueden emitir. Por ejemplo, puede que los certificados de servidor Web no estén permitidos.
- El ámbito de confianza de una entidad emisora raíz comercial puede ser demasiado amplio para las necesidades de seguridad de la organización. Puede que deba introducir comprobaciones especiales o una capa adicional de entidades emisoras interna para distinguir entre los certificados emitidos por la organización y los que ha emitido otra también subordinada a la misma raíz.

A pesar de estos inconvenientes, si debe emitir un número importante de certificados en los que confiarán usuarios externos a la organización, debe plantearse el subordinar como mínimo una parte de la PKI a una raíz comercial (aunque esto puede implicar la creación de dos jerarquías separadas).

Para la mayoría de los certificados utilizados en la organización, esta solución utiliza una jerarquía basada en una entidad emisora raíz interna. Este enfoque ofrece las siguientes ventajas:

- permite a la organización mantener el control directo del delimitador de confianza central, la entidad emisora raíz, y las directivas de seguridad que rigen la emisión y el uso de certificados emitidos por ella.
- Se puede emitir un gran número de certificados desde la PKI interna a un costo relativamente bajo.
- no hay restricciones en los tipos de certificados que pueden emitirse.
- No existe ambigüedad entre la confianza en certificados internos y certificados externos.
- la información de las listas CRL y del acceso a la información de entidad emisora (AIA, Authority Information Accesses) puede publicarse interna o externamente, según sea necesario.

Si las raíces de confianza de sus usuarios de certificados no pueden administrarse fácilmente, debería considerar el uso de una raíz externa. Esta solución sugiere el uso de certificados de otra empresa y una raíz externa para los servicios siguientes:

- Servidor Web de Internet
- Firma de códigos comerciales
- Firma de documentos comerciales
- correo electrónico seguro de confianza externo.

Definición de confianzas de certificados externos

La sección anterior incidía en la confianza en la infraestructura de certificados de otras organizaciones. Debe considerar este tema de forma más amplia para determinar cómo se controla la confianza en los certificados en la organización. La palabra "confianza" en este contexto tiene tres características importantes:

- la persona o entidad en la que se confía. ¿En quién confía?
- las operaciones o las actividades para las que confía en esa persona o entidad. ¿Qué acciones confía que realicen?
- el período de tiempo durante el que desea mantener esa confianza. ¿Durante cuánto tiempo confiará en ellos?

En lo que respecta a certificados, el “quién” es la raíz de entidad emisora que los emite y el “qué” es los usos y otras características de certificados que desea controlar. El “cuánto tiempo” se define por el período de validez del certificado de la entidad emisora raíz o, en algunos casos, el período de validez de un certificado de confianza cruzada especial que crea.

Es probable que deba cambiar las relaciones de confianza predeterminadas que tiene la organización con empresas externas cuando establezca una nueva relación comercial con otra organización o cuando desee permitir algunas funciones a los usuarios (por ejemplo, confiar en certificados Web para permitir sesiones HTTP seguras). Algunas acciones que es aconsejable realizar son:

- Distribuir el certificado de entidad emisora de una organización asociada (o un nuevo proveedor de certificados comercial) para que algunos o todos los usuarios confíen en los certificados de la entidad emisora asociada o comercial.
- distribuir el certificado de una entidad emisora de propósito especial o en la PKI de la organización cuando no desee que toda la organización confíe en él.
- sustituir las raíces comerciales existentes en el almacén de raíces de los clientes para poder restringir los usos de sus certificados de confianza. Por ejemplo, puede decidir que sólo confía en una raíz comercial determinada para el correo electrónico y los certificados de servidor Web seguro pero no para certificados de inicio de

sesión con tarjeta inteligente, por ejemplo.

Existen varias maneras de conseguir estos objetivos:

- Crear relaciones de subordinación calificadas entre la raíz interna y el certificado de entidad emisora en el que se debe confiar (también conocido como certificación cruzada). Este procedimiento implica que una de las entidades emisoras internas debe volver a firmar el certificado de entidad emisora externa, lo que fundamentalmente agrega la entidad emisora externa a la PKI interna como subordinada de confianza de la entidad emisora que firma. Puede establecer restricciones en el tipo de certificado, lo que limitará de forma precisa los usos y las directivas del certificado, los nombres de tipos de sujetos o las directivas de emisión en los que confiará.

  Importante: el sujeto de certificación cruzada o subordinación calificada es complejo y constituye el método más difícil de implementar satisfactoriamente. Consulte el documento técnico *Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003* sobre el planeamiento y la implementación de certificación cruzada y subordinación calificada con Windows Server 2003, al que se hace referencia en la sección “Información adicional” al final del capítulo.

- Crear una lista de confianza de certificados (CTL). Esta lista permite definir una lista de entidad emisora raíz de confianza y especificar los propósitos para los cuales confiará en estas entidades emisoras (por ejemplo, para el correo electrónico seguro). A continuación las listas CTL se implementan mediante la utilización de los objetos de directiva de grupo (GPO) de Active Directory. Aunque este método sea conveniente, es propiedad de Microsoft. Sólo podrá utilizarse en equipos con Windows 2000 o una versión posterior. Esta opción sólo afecta a los clientes del dominio en los que se aplique el GPO de CTL.

- Instalar el certificado de entidad emisora raíz en el almacén de entidades emisoras de certificados de confianza de Active Directory (en el contenedor Configuración). Esto crea una confianza incondicional en la entidad emisora raíz (y en todas las entidades emisoras subordinadas) para todos los usuarios y dispositivos del bosque. Sin embargo, este tipo de confianza debe otorgarse con precaución. Utilice este método únicamente para las entidades emisoras que se encuentren bajo el control de la organización.

- Implementar un certificado de entidad emisora raíz de confianza en un subconjunto de usuarios o equipos mediante una directiva de grupo. Es similar a la opción anterior pero le permite ser mucho más específico acerca de quién recibirá las raíces de confianza (es decir, los usuarios o los equipos a los que están dirigidos los objetos de directiva de grupo). Esta opción sólo afecta a los usuarios del dominio en el que se aplica el objeto de directiva de grupo.

- Utilizar el servicio de actualización de raíces de Microsoft. Este servicio está indicado para permitir a los proveedores de certificados comerciales distribuir con facilidad nuevas raíces a un gran número de personas. Considere la deshabilitación de este servicio en todos los sistemas de la organización si tiene previsto regular las entidades emisoras raíz de confianza.

- Utilizar la directiva de grupo para deshabilitar raíces de confianza de otras empresas. A diferencia de otros elementos de la lista, este es un medio para restringir la confianza en lugar de incrementarla. Todos los equipos con Windows (y los usuarios que utilizan estos equipos) heredan un conjunto de raíces que se instalan de forma predeterminada. (También es común a otros sistemas operativos y exploradores Web de varias plataformas.) Puede utilizar la directiva de grupo para deshabilitar la confianza automática en estas raíces. Después, puede utilizar uno de los mecanismos descritos previamente para agregar de forma selectiva las raíces de confianza preparadas que necesite (con o sin restricciones, según las necesidades de seguridad).

  Nota: hay determinados certificados raíz que no se pueden deshabilitar. Es así porque el sistema operativo se basa en ellos para elementos como la directiva de firma de controladores. Estas raíces necesarias no se deshabilitan mediante la configuración de la directiva de grupo mencionada.

Esta solución deshabilita el servicio de actualización de certificados raíz en las entidades emisoras. Considere la deshabilitación de este servicio en el resto de los equipos de la organización. Considere además el uso de la directiva de grupo para deshabilitar las raíces predeterminadas de otras empresas para todos los usuarios del dominio. El capítulo 7, Implementación de la infraestructura de claves públicas, se ocupa de estas cuestiones de forma más detallada.

Para distribuir a los clientes el certificado de entidad emisora raíz de la PKI de esta solución, impórtelo en Active Directory, tal y como se describe en la sección siguiente.

Distribución de los certificados de entidad emisora raíz

Los certificados de entidad emisora raíz se distribuyen automáticamente a los miembros del bosque de Active Directory. Mediante la importación del certificado de entidad emisora al contenedor de entidades emisoras de certificados, los miembros (equipos y usuarios) de todos los dominios del bosque instalarán este certificado en sus almacenes de entidad emisora raíz de confianza locales. Éste es el método recomendado para todas las entidades emisoras raíz internas que necesitan un ámbito de confianza con amplitud de bosque.

Normalmente, también deberá distribuir raíces con un ámbito de confianza más limitado junto a las raíces internas. Para obtener más información sobre este tema, consulte la sección sobre la ampliación de la infraestructura de la autoridad de certificados, incluida más adelante en este capítulo.

Para distribuir el certificado de entidad emisora raíz a usuarios y equipos de otras plataformas o que se encuentren fuera del bosque, debe instalar el certificado manualmente o utilizar otro método de distribución del certificado raíz a los mismos.

Definición de las funciones de entidad emisora de certificados

Tras definir el modelo de confianza y seleccionar la estrategia de la entidad emisora raíz, puede planear el resto de la infraestructura de entidades emisoras. Para ello debe definir las distintas funciones que las entidades emisoras realizarán en la organización. Una entidad emisora puede configurarse como entidad emisora raíz o entidad emisora subordinada. Las entidades emisoras subordinadas, a su vez, pueden ser entidades emisoras o entidades emisoras intermedias (que son los pasos de confianza intermedios entre las entidades emisoras y las entidades emisoras raíz).

Entidad emisora raíz

La función de la entidad emisora raíz es muy importante en cualquier organización. Es un punto en el que confían explícitamente todos los usuarios y dispositivos de la organización. Muchas decisiones de seguridad (por ejemplo, permitir que un usuario inicie la sesión, confiar en un correo electrónico o permitir una operación comercial de valores de 10 millones de dólares) descansan en la seguridad de esta raíz y la clave privada que proporciona su identidad. Puesto que hay tantas operaciones que dependen de la raíz, el cambio de una clave y un certificado de la raíz puede ser muy complejo y una operación con probabilidad de errores que puede provocar la interrupción intermitente del servicio para aplicaciones y usuarios durante un período prolongado.

Por esta razón, es altamente aconsejable proteger la clave privada de la entidad emisora raíz lo máximo posible. Una de las mejores formas de hacerlo es desconectar la entidad emisora de la red para que el acceso a ella sea extremadamente limitado (combine esta medida de protección con otras equivalentes para restringir el acceso físico al servidor). Una mejora más para proteger las claves de una entidad emisora es utilizar un Módulo de seguridad de hardware (HSM). Estos módulos ofrecen seguridad de claves adicional a las entidades emisoras de certificados sin conexión, así como un aumento considerable de la seguridad a las entidades emisoras de certificados en línea.

La solución definida en esta guía utiliza una entidad emisora raíz sin conexión.

Importante: debería considerar el uso de un HSM para la entidad emisora raíz con el fin de mejorar la seguridad de las claves de la entidad emisora. Puede agregar HSM tras la instalación de la entidad emisora pero es más sencillo y seguro hacerlo al principio. Si instala un HSM a continuación, deberá renovar la entidad emisora de certificados con una nueva clave aunque muchos proveedores le permitan importar la clave existente.

Entidades emisoras intermedias y CA emisoras

Si se desconecta la entidad emisora raíz, no se podrán emitir certificados desde la misma diariamente. Para crear entidades emisoras que puedan utilizarse para emitir certificados diariamente, la entidad emisora raíz certifica las entidades emisoras subordinadas para que emitan certificados en su nombre. Esto permite a la entidad emisora subordinada heredar la confiabilidad de la entidad emisora raíz sin exponer la clave de la entidad emisora raíz a amenazas de seguridad.

Puede profundizarse aún más en este proceso. En lugar de emitir certificados directamente, la entidad emisora subordinada certifica una capa más de entidades emisoras para que emitan a las entidades finales (usuarios y equipos). Esto no sólo ofrece una capa de seguridad adicional a la clave de la entidad emisora raíz, sino que

permite dividir el riesgo entre las ramas de entidades emisoras subordinadas. Por ejemplo, una entidad emisora intermedia puede certificar CA emisoras internas, mientras que otra entidad emisora intermedia certifica las entidades emisoras que emiten certificados externos. Este enfoque ofrece las siguientes ventajas:

- ayuda a restringir el riesgo de la entidad emisora a una parte menor de toda la jerarquía de la PKI.
- Permite separar las directivas de certificados que deben implementarse para todas las ramas de la jerarquía de entidades emisoras.
- reduce el número de veces que debe utilizarse la clave de entidad emisora raíz y, por lo tanto, reduce los riesgos para la clave.

Aunque el uso de las capas adicionales de entidades emisoras intermedias aumente la seguridad global de la PKI, supone un costo adicional de complejidad y de administración (que normalmente es mucho mayor que el costo de licencias de hardware o software). Por lo tanto, para muchas aplicaciones, los requisitos de seguridad no justifican una jerarquía de tres niveles. En especial, si las claves de la entidad emisora están protegidas con HSM.

La solución definida en esta guía sugiere una jerarquía de dos niveles. El diseño de la solución aporta un equilibrio aceptable entre seguridad y rentabilidad, a la vez que ofrece flexibilidad para aplicaciones de certificados futuras (vea, por ejemplo, los detalles descritos en la sección “Definición de los requisitos de certificados”, incluida anteriormente en el capítulo).

Nota: pueden existir requisitos estatales o legales que indiquen que debe utilizar jerarquías de tres niveles, pero esta consideración queda fuera del alcance de esta guía. Obviamente, estos requisitos anulan otras consideraciones.

Jerarquía de entidades emisoras propuestas

La siguiente figura ilustra la jerarquía propuesta. La implementación actual comprende la entidad emisora raíz y una CA emisora. La entidad emisora distribuirá principalmente certificados de seguridad estándar (técnicos) para equipos o usuarios y certificados de valor más alto para equipos.

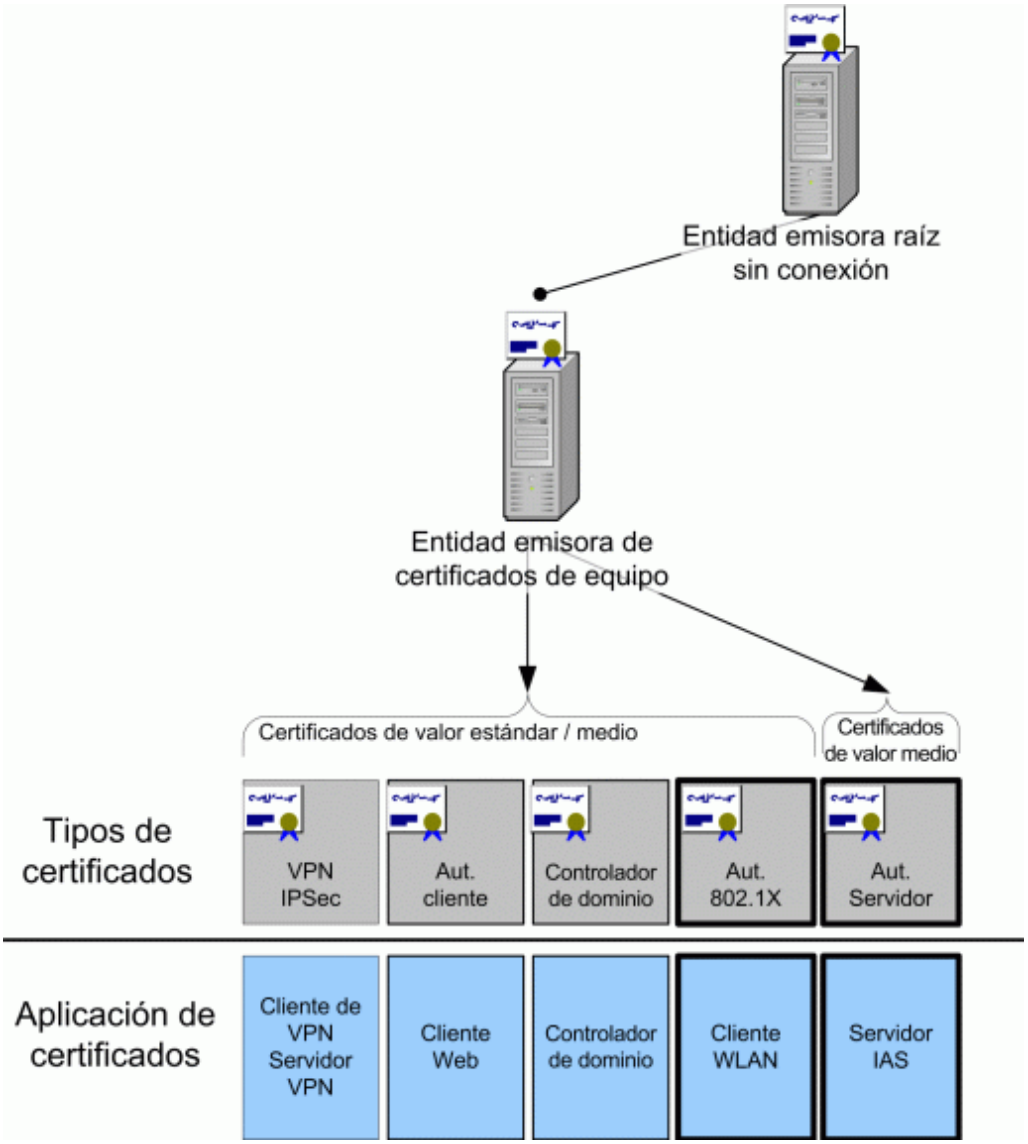

Figura 4.2 Jerarquía de autoridad de certificados
Ver imagen a tamaño completo

Este diseño permite implementar una PKI completamente funcional capaz de compatibilizar la autenticación de LAN inalámbrica segura (802.1X) con una inversión relativamente pequeña en hardware y software y unos costos de administración reducidos.

Nota: este diseño de infraestructura simple puede ampliarse de varias maneras para acomodar distintos requisitos. Esto se explica en la sección “Ampliación de la infraestructura de entidades emisoras”.

La entidad emisora se configurará inicialmente para emitir los siguientes tipos de certificados (en la figura anterior aparecen en cuadros en negrita):

- Autenticación de cliente: usuario
- Autenticación de cliente: equipo
- Autenticación de servidor IAS

Los dos primeros son certificados estándar y se emiten automáticamente basados en las credenciales de dominio del usuario o el equipo. La posesión de estos certificados no indica que exista un vínculo más estrecho con el sujeto que el que ofrece la posesión de un nombre de usuario y una contraseña de dominio válidos. Sin embargo,

es importante recordar que el uso de certificados en lugar de contraseñas y nombres de dominio ofrece ventajas técnicas y de seguridad significativas.

La autenticación de servidor IAS se clasifica como certificado de seguridad media porque los servidores IAS realizan una función de seguridad alta. La emisión de este tipo de certificado normalmente incluirá comprobaciones adicionales en cuanto a la validez de la solicitud y requerirá la aprobación del administrador de certificados.

Nota: en el capítulo sobre generación incluido más adelante, donde se describe la creación de este tipo de certificado, el requisito de la aprobación por parte del administrador de certificados se ha dejado deshabilitado. Esto permite que los servidores IAS renueven automáticamente los certificados que caducan y evita que se deshabilite el servicio cuando caduca el certificado. Siempre que disponga de procesos para vetar y aprobar de forma adecuada la solicitud de certificados, debe considerar la posibilidad de habilitar el requisito de aprobación del administrador de certificados.

Requisitos de hardware y software de las entidades emisoras

Esta sección explica los requisitos de hardware y software de las entidades emisoras.

Entidad emisora raíz

Los requisitos de hardware de la entidad emisora raíz son mínimos. Basta con que la especificación del equipo permita la ejecución de Windows Server 2003. Las características críticas de una entidad emisora raíz son la confianza y el mantenimiento a largo plazo. La entidad emisora raíz suele residir en un equipo de larga duración que está apagado la mayor parte del tiempo. No obstante, cuando *se enciende*, es importante tener la seguridad de que se iniciará sin dificultad alguna. Para hacer frente a posibles fallos de hardware, necesita que sea posible sustituir componentes con facilidad, posiblemente años después de que se haya interrumpido la fabricación del modelo.

Microsoft toma estas consideraciones como base y recomienda:

- elegir un buen fabricante con un buen historial de soporte y mantenimiento de hardware a largo plazo. Consulte durante cuánto tiempo podrá obtener piezas de recambio del proveedor.
- utilizar hardware de servidor en lugar de estación de trabajo o de equipo portátil, ya que el primero tiende a estar más estandarizado y los cambios se producen con menos frecuencia.
- considere la posibilidad de mantener un sistema de reserva que tome el control de la función de entidad emisora raíz si se produce un error en el hardware y no puede repararse en un período de tiempo razonable.
- guarde una copia del medio de instalación original, de los controladores y las revisiones, de modo que pueda reconstruir el sistema en caso de fallos.
- Plantéese utilizar un HSM para seguridad adicional.

La entidad emisora raíz no requiere las capacidades adicionales de la versión Enterprise Edition de Windows Server 2003. Por esta razón, la solución utiliza la versión Standard Edition.

Entidad emisora de certificados

Aunque existen requisitos de rendimiento para la entidad emisora, éstos no son de gran importancia ya que, normalmente, la entidad emisora realizará pocas tareas. Incluso cuando la carga es considerable, las medidas de rendimiento sugieren que, en lo que respecta a una entidad emisora de certificados de empresa, el cuello de botella se encuentra en la interacción con Active Directory (no en la entidad emisora). Los requisitos de rendimiento de hardware son, por lo tanto, bastante modestos. Al igual que ocurre con la entidad emisora raíz, la confianza y el mantenimiento son factores importantes en la elección del hardware.

Los Servicios de Certificate Server utilizan la misma tecnología de base de datos que Active Directory, por lo que se aplican muchas de las mismas directrices de rendimiento. Una buena directriz para la mayoría de las organizaciones es utilizar la misma especificación de hardware que se utiliza para los controladores de dominio de Active Directory.

Para obtener más información acerca de la capacidad, el rendimiento y la escalabilidad de la entidad emisora, consulte la sección “CA Capacity, Performance, and Scalability”, incluida en el documento sobre el diseño de

infraestructuras de claves públicas al que se hace referencia al final de este capítulo.

El capítulo 7, Implementación de la infraestructura de claves públicas, ofrece una sugerencia de perfil de hardware. Además de las directrices anteriores en lo que respecta a la entidad emisora raíz, Microsoft recomienda que tenga en cuenta lo siguiente al especificar el hardware de servidor para la entidad emisora:

- Las tarjetas de interfaz de red (NIC) redundantes que utilizan la formación de equipos NIC.
- Se recomiendan dos matrices redundantes de volúmenes de disco independientes (RAID 1) como mínimo para que los registros de la entidad emisora puedan almacenarse en una unidad de almacenamiento física separada. Esto agrega ventajas de rendimiento así como resistencia a los errores de hardware.
- Debe plantearse utilizar tres volúmenes de RAID 1 (en lugar de dos) para almacenar el sistema operativo, la base de datos de los Servicios de Certificate Server y los registros de los Servicios de Certificate Server, respectivamente, en volúmenes físicos separados para un mejor rendimiento.
- El uso de unidades y controladores SCSI (interfaz estándar de equipos pequeños) de alto rendimiento es preferible a la utilización de sus equivalentes IDE (electrónica integrada de dispositivos) por su mejor rendimiento y características de resistencia. Aparte de la interacción con Active Directory, el rendimiento del subsistema de discos es posiblemente el factor más significativo en la determinación del rendimiento global de la entidad emisora.
- Considere la posibilidad de utilizar un HSM para obtener seguridad adicional y un incremento del rendimiento en las operaciones de firma durante la emisión de certificados.

A diferencia de la entidad emisora raíz, la entidad emisora *requiere* las capacidades adicionales de Windows Server 2003 Enterprise Edition para ofrecer compatibilidad con plantillas de certificados editables y la inscripción automática de certificados de usuarios.

Utilización de varias CA emisoras para resistencia del servicio
En esta sección se explican las razones técnicas por las que puede ser aconsejable instalar varias CA emisoras. También hay razones de seguridad y de directiva por las que es aconsejable que diferentes entidades emisoras inscriban distintos tipos de certificados. Estas razones se consideran en una sección posterior de este capítulo.

Una sola entidad emisora con hardware muy modesto es adecuada para satisfacer los requisitos de emisión de los tipos de certificado descritos previamente a miles de clientes, por lo que no es probable que necesite varias entidades emisoras sólo por razones de rendimiento. Sin embargo, debe plantearse si sus requisitos de disponibilidad de las CA emisoras le obligarán a implementar varias entidades emisoras para inscribir los mismos tipos de certificados.

Una entidad emisora no tiene el mismo tipo de problemas de disponibilidad que muchos servicios. Los clientes no necesitan ponerse en contacto con la entidad emisora para utilizar o comprobar un certificado. Solamente se requiere el contacto directo con una entidad emisora para:

- Inscribir un nuevo certificado.
- Renovar un certificado.
- Revocar un certificado.
- Publicar una nueva lista CRL.
- Renovar el certificado de entidad emisora.

Los requisitos de disponibilidad de cada una de ellas se detallan en la tabla siguiente.

Tabla 4.8: Requisitos de disponibilidad del servicio de entidad emisora

Servicio de entidad emisora	Requisito de disponibilidad
Servicios de inscripción: certificado nuevo	Éste podría ser un factor significativo, ya que puede evitar que usuarios nuevos obtengan acceso a la red o a otros servicios que requieren un certificado. Debe

	evaluar si el tiempo requerido para recuperar la entidad emisora a partir de la copia de seguridad es mayor de lo que la organización puede esperar para que un nuevo usuario inscriba un certificado. La mayoría de las organizaciones consideran que el costo de la espera por la recuperación de la entidad emisora es menor que el costo de administración de entidades emisoras adicionales. De lo contrario, necesitará varias entidades emisoras para los tipos de certificados existentes.
Servicios de inscripción: renovar certificado	Si se utiliza la renovación automática con un tipo de certificado determinado, se produce de forma predeterminada seis semanas antes de que caduque el certificado. Por otro lado, normalmente el tiempo de recuperación de una entidad emisora a partir de la copia de seguridad se mide en horas. La renovación manual de los certificados se deja en manos del propietario. Si lo desea, puede instituir un sistema de advertencia automatizado que alertará al propietario cuando deban renovarse certificados importantes. De lo contrario, los criterios de disponibilidad son los mismos que para inscribir un certificado nuevo.
Revocación de un certificado	Normalmente, un certificado sólo puede revocarse mediante la entidad emisora que lo ha emitido, por lo que una segunda entidad emisora no serviría de gran ayuda. Si la revocación tiene una gran dependencia del tiempo (es decir, debe realizarse antes de que la entidad emisora pueda recuperarse), puede insertar entradas de revocación en las listas CRL actuales, siempre que disponga del número de serie del certificado que debe revocarse y la clave privada de la entidad emisora (restaurada en un equipo diferente). Debe recordar que las listas CRL tienen normalmente una latencia de uno o varios días. A menos que el tiempo de recuperación de la entidad emisora sea superior al intervalo hasta la siguiente publicación de la lista CRL, se ganará poco tiempo con la actualización manual de la lista CRL.
Publicación de una lista CRL	Una lista CRL es exclusiva a una entidad emisora; una segunda entidad emisora no hará que la publicación de la lista CRL sea más resistente, sólo minimizará el impacto de un error en la publicación de la lista CRL (ya que menos del 100% de los certificados emitidos dependerán de la CRL errónea). El acceso al estado de revocación actual es esencial para muchas aplicaciones de certificados, lo que significa que una lista CRL que no ha caducado debe estar disponible en los puntos de distribución CRL (CDP). Si esto no ocurre, se producirán errores en las aplicaciones de certificados en las que influye la revocación. El período de recuperación de la entidad emisora no debe ser nunca superior al intervalo comprendido entre la caducidad de la lista CRL anterior y la emisión de la lista CRL nueva. Incluso en los casos donde lo es, se puede volver a firmar una lista CRL y ampliar su período de validez. Este procedimiento se explica en la guía de operaciones.
Renovación del certificado de entidad emisora	Una segunda CA emisora no serviría de nada en este caso. Esta operación nunca debe retrasarse tanto en el proceso que el tiempo de recuperación de una entidad emisora se convierta en un problema. Aunque lo sea, el certificado de entidad emisora puede volverse a firmar con la clave de entidad emisora primaria, lo que amplía su período de validez.

Nota: en la tabla anterior, el tiempo de recuperación de la entidad emisora y la disponibilidad de la misma deben tomarse en relación con cualquier punto que afecte a la capacidad de la entidad emisora para prestar servicio a los usuarios finales. No se confina al error del servidor. De hecho, una interrupción entre sitios de la red es un ejemplo mucho más probable de causa de error en el sistema. Debe tener en cuenta todos los factores que pueden afectar la entrega de servicio a los usuarios al decidir el nivel de disponibilidad de servicio que requiere.

Siempre y cuando administre la copia de seguridad y la recuperación de las entidades emisoras de forma apropiada, únicamente la inscripción y algunos requisitos de renovación afectarán a la decisión de utilizar varias entidades emisoras de certificados para ofrecer resistencia de servicio. Debe sopesar el costo que supone que estos servicios no estén disponibles en contraposición con el costo de la instalación y administración de entidades emisoras de certificados adicionales.

Además de ofrecer un nivel de disponibilidad mayor, la opción de contar con varias entidades emisoras proporciona un rendimiento de emisión de certificados mejorado y reducen a la mitad el tamaño de las listas CRL. Estos factores no son de importancia en la solución para esta guía. En esta solución, los problemas de resistencia se tratan mediante una administración cuidadosa de las entidades emisoras de certificados y la inclusión de procedimientos adecuados de copia de seguridad y recuperación. Por lo tanto, sólo se requiere una entidad emisora.

Protección de las claves de entidad emisora de certificados con HSM

Una mejora significativa que puede incrementar el nivel de seguridad de la solución básica que se presenta aquí es utilizar HSM para proteger las claves privadas de todas las entidades emisoras. Aunque estos módulos de hardware suelen ser caros (seguramente cuesten más que un servidor de entidad emisora), el nivel de seguridad adicional que brindan al entorno es significativo. Esta medida le permitirá restringir el acceso a las operaciones clave de la entidad emisora a usuarios autorizados. Operaciones importantes (por ejemplo, la exportación y copia de seguridad de las claves) suelen presentarse protegidas por varias tarjetas inteligentes. Esto es más seguro que confiar únicamente en claves basadas en software que cualquier miembro de los grupos de administradores locales o responsables de copias de seguridad puede copiar de la entidad emisora.

Además de las enormes ventajas de seguridad que ofrecen, los HSM pueden acelerar las operaciones de las entidades emisoras mediante la descarga de tareas de la CPU a procesadores de aceleración de cifrado dedicados.

Seguridad de la entidad emisora de certificados

En esta sección se examina la seguridad de las entidades emisoras de certificados, incluida la seguridad física y del sistema operativo, la auditoría y supervisión de la seguridad y el uso de funciones para delegar las responsabilidades de administración a la entidad emisora.

Seguridad del sistema operativo

La entidad emisora se protege utilizando las directivas de seguridad de Windows. La configuración se basa en la función del servidor de entidad emisora de certificados de la publicación *Guía de seguridad de Windows Server 2003*.

Para obtener más detalles sobre las configuraciones utilizadas en esta función, consulte el capítulo 7, Implementación de la infraestructura de claves públicas.

La configuración de seguridad para la entidad emisora raíz se aplica directamente con las plantillas de seguridad, mientras que la configuración de la CA emisora se aplica con la directiva de grupo.

Seguridad física

La seguridad física de los servidores de entidad emisora es primordial. A menos que se pueda controlar el acceso físico básico a los servidores, no será efectiva ninguna medida de seguridad de red o de sistema operativo.

La entidad emisora raíz debe alojarse en una ubicación en la que el acceso al servidor esté estrictamente controlado. El acceso a la entidad emisora sólo se requiere en contadas ocasiones (dos o tres veces al año) y no es necesario activar el servidor en ninguna otra situación. Esto significa que el servidor puede almacenarse en una sala protegida aunque no tenga los recursos de equipo estándar de una sala de servidor. Por ejemplo, no se necesita red, alojamientos de servidor sofisticados ni administración de energía y temperatura.

La entidad emisora también debe estar alojada en una ubicación en la que el acceso físico esté estrictamente controlado. La seguridad física es importante, ya que hay varias maneras de comprometer la seguridad de un

sistema de equipo si un atacante cuenta con acceso físico al mismo (además de los posibles ataques en la red). Este servidor debe estar continuamente en línea y debe almacenarse en una ubicación con recursos de sala de servidor de equipos estándar (control de temperatura, administración de energía, filtrado de aire y capacidad de extinción de incendios).

En la medida en que sea posible, la ubicación de ambos servidores debe estar lo más libre posible de riesgos externos que puedan dañar los servidores, como incendios, inundaciones, etc.

También es importante controlar el acceso físico a las copias de seguridad, al material de claves y a otros datos de configuración, y garantizar la seguridad física de los mismos. Esta información debe almacenarse en una ubicación diferente a la de los servidores para permitir la recuperación de las entidades emisoras en caso de que el sitio entero deje de estar disponible (por ejemplo, después de una catástrofe natural o un incendio).

Administración de la seguridad de las entidades emisoras de certificados

Una infraestructura de certificados es en potencia un activo de valor muy alto. Este valor dependerá del uso que la organización haga de los certificados, no sólo ahora, sino en los próximos cinco años o más. Por ello, debe utilizar medidas de seguridad y de comprobación más estrictas en la instalación, la configuración y la administración de las entidades emisoras que en la instalación de otras infraestructuras de TI. Estas medidas deben ser, como mínimo, equivalentes a las diseñadas para un controlador de dominio. En algunos casos es posible que necesite un nivel de seguridad incluso mayor.

La seguridad que ofrece una entidad emisora dependerá de la seguridad con que se haya configurado y administrado. Si no puede garantizar que la clave privada de la entidad emisora no se ha copiado de forma furtiva, nunca podrá estar realmente seguro de que el certificado supuestamente emitido por esa entidad emisora no sea una falsificación.

Esta seguridad o nivel de confianza no puede incrementarse fácilmente de forma retroactiva; este estado especial debe crearse en todas las interacciones con la entidad emisora desde el principio. La confianza de la organización en la seguridad de la clave privada de la entidad emisora será muy superior si dispone de una pista de auditoría u otra evidencia de que todo acceso a la entidad emisora ha sido legítimo. Por ejemplo, si se han grabado en vídeo todas las operaciones administrativas llevadas a cabo en las entidades emisoras o las ha presenciado otra persona además del administrador. En el caso de una entidad emisora sin conexión, gran parte de la garantía de seguridad de la misma depende de que no haya estado nunca conectada a una red.

La necesidad de este alto nivel de seguridad puede ser especialmente importante si la organización se ve involucrada en una controversia legal sobre la validez de un certificado que ha emitido. En estos casos, si dispone de pruebas de que las entidades emisoras no se han visto comprometidas, tendrá muchas más oportunidades de que el resultado de la controversia sea satisfactorio. Este tema queda fuera del ámbito de esta guía y debería consultar a sus auditores y asesores legales para examinarlo en mayor profundidad.

Algunos ejemplos de los pasos que puede seguir para aumentar significativamente el nivel de seguridad de las entidades emisoras son:

- Garantice la seguridad física de la entidad emisora para que las personas no autorizadas no puedan obtener acceso al hardware o medio de copia de seguridad de la misma.
- Realice todos los pasos de instalación y configuración con un testigo presente; anote los pasos principales de la instalación y solicite la refrenda por parte del testigo para comprobar que se han llevado a cabo satisfactoriamente. (Alternativamente podría grabar la instalación en vídeo y confiar una copia de la misma a un tercero.)
- Realice todas las operaciones de emisión y revocación de certificados en la entidad emisora raíz bajo condiciones similares. Lo ideal sería que todo acceso a la entidad emisora raíz se realizara con la presencia de un testigo.
- Asegúrese de que todas las personas que tienen acceso administrativo a las entidades emisoras tengan cuentas que se puedan seguir de forma exclusiva. Audite todas las operaciones de la entidad emisora.
- Piense en la posibilidad de permitir la separación de funciones en la entidad emisora. (Esto se trata de forma detallada más adelante en el capítulo.)

Estos tipos de medidas son especialmente importantes para el servidor de entidad emisora raíz. La CA emisora puede tener un nivel de seguridad mucho menor según los tipos de certificados que deba emitir. Por ejemplo, si los certificados que emite la entidad son de valor relativamente bajo (como la autenticación de red de usuarios y equipos), no necesitará más seguridad para esta entidad emisora que la utilizada para un controlador de dominio.

Siempre que la entidad emisora raíz tenga un nivel de seguridad alto, tendrá flexibilidad para agregar una CA emisora de seguridad superior para emitir certificados de valor superior más adelante. Puede mantener entidades emisoras de seguridad alta junto con la entidad emisora estándar existente. Sin embargo, si la entidad emisora raíz se instala y configura en un entorno de seguridad relativamente baja, probablemente deberá volver a instalarla o crear una nueva entidad emisora raíz si más adelante desea emitir certificados de valor alto.

Supervisión y auditoría de seguridad
La auditoría del sistema operativo y de los Servicios de Certificate Server se utiliza en todas las entidades emisoras. Para que sea efectiva, deberá supervisar e investigar cualquier elemento sospechoso. Consulte el capítulo 11, “Administración de la infraestructura de claves públicas” para obtener una explicación del significado de las entradas de sucesos de auditoría de los Servicios de Certificate Server.

Funciones de administración
Los Servicios de Certificate Server proporcionan gran nivel de control sobre la delegación de funciones administrativas. Esta capacidad se ofrece en esta solución para proporcionar flexibilidad óptima en la administración de la PKI. Cada una de las funciones administrativas principales definidas en los Servicios de Certificate Server se ha implementado mediante la utilización de un grupo de seguridad del dominio o, en las entidades emisoras de certificados fuera de línea, un grupo de seguridad local. Además, se han definido dos grupos adicionales de funciones y seguridad para ayudar en la delegación de obligaciones administrativas a los componentes de PKI de Active Directory.

Es importante comprender que no existe necesariamente una asignación uno a uno entre estas funciones y los miembros del equipo de TI de la organización. En la mayoría de las organizaciones, la misma persona realizará muchas de las funciones. Esto es posible si se incluye a esa persona en cualquiera o en todos los grupos de seguridad indicados en la tabla siguiente. Por otro lado, si la organización cuenta con una separación más compleja de las responsabilidades administrativas, es importante saber que existe la posibilidad de hacer lo mismo.

Las funciones implementadas y sus asignaciones a los grupos de seguridad (donde están implementadas) se muestran en la tabla siguiente.

Tabla 4.9: Funciones importantes de Servicios de Certificate Server

Nombre de la función	Grupo de seguridad	Ámbito	Descripción
Administrador de la PKI de la empresa	Administradores de PKI de empresa	Bosque de Active Directory	Responsable de la PKI global: define para la empresa los tipos de certificados, las directivas de aplicación, las rutas de confianza, etc.
Publicador de la PKI de la empresa	Editores de PKI de empresa	Bosque de Active Directory	Responsable de publicar certificados raíz de confianza, certificados de subentidades emisoras de certificados y listas CRL en el directorio.
Administrador de entidad emisora	Administradores de entidad emisora	Entidad emisora	Responsable de la configuración de entidades emisoras. Generalmente se trata de las mismas personas que actúan como administradores o administradores de PKI de empresa. Es posible que existan diferentes administradores de entidades emisoras a cargo de diferentes entidades emisoras si el uso del certificado así lo indica.
Administrador	Administradores	Entidad emisora	Administra el sistema operativo y el servidor de

	locales		entidades emisoras de certificados. También es responsable de instalar la entidad emisora y renovar el certificado de la misma. Normalmente se comparte con la función de administrador de entidad emisora de certificados.
Auditor de entidad emisora	Auditor de entidad emisora	Entidad emisora	Administra el registro de sucesos de auditoría y la directiva de los sucesos que se pueden auditar de las entidades emisoras de certificados.
Administrador de certificados	Administrador de certificados	Entidad emisora	Aprueba solicitudes de certificado que requieren la aprobación manual y revoca certificados. Puede haber varios administradores de certificados a cargo de aprobaciones de diferentes entidades emisoras de certificados si el uso del certificado lo requiere.
Autoridad de registro o bien Oficial de inscripción	No está definido	Perfil de certificado	Es una extensión de la función del administrador de certificados. Es responsable de aprobar y firmar las solicitudes de certificado siguiendo la comprobación de Id. fuera de banda. Puede ser una persona, un proceso de TI o un dispositivo (por ejemplo, un escáner de huellas dactilares y base de datos). Se pueden especificar diferentes autoridades de registro para distintos perfiles de certificados (plantillas) y pueden abarcar múltiples entidades emisoras de certificados.
Agente de recuperación de claves	No está definido	Entidad emisora	Contiene la clave para descifrar claves privadas archivadas en la base de datos de la entidad emisora de certificados.
Operador de copia de seguridad de la entidad emisora	Operador de copia de seguridad de la entidad emisora	Entidad emisora	Responsable de la copia de seguridad y recuperación de los servidores de entidad emisora y el almacenamiento seguro de los medios de copia de seguridad.

Estos grupos de seguridad se implementan como grupos universales del dominio y se aplican a la CA emisora y al directorio. Para la entidad emisora raíz, se implementan grupos equivalentes como grupos locales (aunque no hay equivalente para los administradores de PKI de empresa y editores de PKI de empresa para una entidad emisora fuera de línea). La solución supone que se utilizarán los mismos grupos de seguridad para todas las entidades emisoras de la empresa. Si no es válido para su organización, debe implementar grupos separados para cada entidad emisora para todas las funciones con ámbito de entidad emisora. (Obviamente, debe cambiarse el nombre en consonancia, por ejemplo, Administradores de entidad emisora: CA emisora 1.)

Puesto que las autoridades de registro (u oficiales de inscripción) y el archivado y la recuperación de claves no se han implementado para esta solución, las funciones no tienen un grupo de seguridad definido.

Es posible obligar la separación entre las funciones de entidad emisora de una entidad emisora. Cuando se habilita, se deniega el acceso de cualquier usuario miembro de más de un grupo de funciones a los privilegios de todos los grupos de funciones. Esta separación de funciones no se ha implementado en esta solución.

Integración en Active Directory

Las entidades emisoras de certificados pueden instalarse de dos modos: modo de empresa (o integrada en Active Directory) o modo independiente. Las principales diferencias entre estos modos son que las entidades emisoras de certificados de empresa se basan en Active Directory para almacenar la información de configuración, pueden utilizar Active Directory como autoridad de registro y pueden publicar automáticamente los certificados emitidos en el directorio. Por otro lado, las entidades emisoras de certificados independientes pueden publicar los certificados y las listas CRL en el directorio pero no dependen de la presencia de Active Directory.

Consulte la sección “Información adicional” incluida al final del capítulo para ver los recursos que ofrecen una explicación más detallada de este tema.

Puesto que se presenta sin conexión, la entidad emisora raíz sólo puede configurarse como servidor independiente. Lo mismo podría decirse de las entidades emisoras intermedias sin conexión, en caso de que tenga previsto implementarlas en el entorno.

La entidad emisora de certificados se configurará como una entidad emisora de certificados de empresa por las razones siguientes:

- Se requiere la inscripción y la aprobación automática de los certificados para los tipos de certificados que se utilizan en la solución.
- La solución requiere plantillas de certificados; éstas ofrecen ventajas considerables, ya que facilitan la administración de varios tipos de certificados (con frecuencia en varias entidades emisoras).
- IAS requiere que Active Directory realice la asignación de certificados de confianza para autenticar los clientes inalámbricos. La entidad emisora debe estar registrada en el almacén NTAuth para permitirlo.
- Es posible la publicación automática de certificados para los objetos de usuario y equipo correspondientes (aunque no se requiere en esta solución).
- La entidad emisora requiere una fuente de confianza para obtener la información de nombre de sujeto que debe utilizarse en las solicitudes de certificados y en los certificados emitidos. Active Directory puede proporcionarla a partir de los atributos de usuario y equipo almacenados en el directorio.
- Es posible que en el futuro se requieran certificados de inicio de sesión con tarjeta inteligente; la implementación de estos certificados resulta mucho más sencilla si se utilizan entidades emisoras de certificados de empresa.

  Nota: la entidad emisora de certificados de empresa ofrece estas posibilidades de forma predeterminada pero también puede ofrecerlas una entidad emisora independiente configurada correctamente. (Esto se describe de forma más detallada en la documentación del producto Servicios de Certificate Server.) Consulte la sección de referencia al final de este capítulo.

Instalación de entidades emisoras en dominios

Si su empresa dispone de un bosque con varios dominios (o incluso de varios bosques), debe seleccionar los dominios en que instalará las entidades emisoras de certificados. La decisión puede verse afectada por muchos factores como, por ejemplo, la necesidad de delegar el control a diferentes administradores de dominio o por la legislación nacional o local que afecta a la provisión de certificados en diferentes zonas de la organización.

Los procedimientos más comunes son instalar las entidades emisoras en el dominio raíz del bosque o en un dominio dedicado a la administración. Debe instalarlas en un dominio que vaya a permanecer estable durante un largo período de tiempo. (El nombre de una entidad emisora de certificados, la pertenencia a un dominio y el nombre de dominio DNS no pueden cambiarse después de la instalación.) Debe evitar la instalación de entidades emisoras de certificados en dominios en los que no pueda garantizar la seguridad o la integridad de la cuenta del equipo. No es necesario instalar las entidades emisoras en el mismo dominio, aunque hacerlo puede facilitar la administración centralizada.

En esta solución, las cuentas de servidor de entidad emisora de certificados (sólo de entidad emisora de certificados de empresa) se instalan en el dominio raíz del bosque o, si se trata de un bosque de un solo dominio, se instalan en este dominio.

Asignación de órdenes de prácticas de certificados a las entidades emisoras de certificados

Si tiene previsto publicar la CPS, debe determinar el ámbito de la misma. Puede crear una CPS para toda una jerarquía de entidades emisoras de certificados o para parte de ella, o puede disponer de una CPA por cada entidad emisora de certificados.

La última opción le brinda más flexibilidad, pero también aumenta las tareas de administración de varias CPS. La práctica general es crear una CPS distinta para cada entidad emisora o grupo de entidades emisoras que tengan en común la directiva de certificados, los tipos de sujetos y los niveles de seguridad. Cuando éstos difieran de forma notable entre entidades emisoras, probablemente deberá utilizar varias CPS. Obviamente, si ha implementado muchas entidades emisoras de certificados idénticas por razones de resistencia o de rendimiento, éstas deberán tener CPS idénticas.

Como mencionamos anteriormente, no hay ninguna razón por la que no pueda crearse una CPS sin intenciones de publicarla. Por ejemplo, es aconsejable evitar la publicación externa de la CPS si contiene información operativa y de seguridad de naturaleza interna. También puede publicar una versión abreviada de la CPS que indique las directivas operativas importantes de la entidad emisora sin desvelar ningún detalle operativo interno.

Si decide publicar la CPS y desea anunciar su ubicación en el certificado de la entidad emisora, deberá obtener un identificador de objeto (OID, Object Identifier) para su directiva de certificados del espacio de nombres OID oficial asignado a la organización por International Standards Organization (ISO). La directiva de certificados es exclusiva de la organización, de modo que requiere un OID exclusivo globalmente para identificarla.

Este OID de la CP está codificado en cada certificado de la organización como extensión del certificado. Una "*extensión de certificado*" es un tipo de campo de datos de certificado. La extensión incluye una URL, que apunta a la CPS para la entidad emisora que emitió un certificado específico.

Es común incluir también un aviso para el usuario en formato de texto que ofrezca algunas indicaciones del propósito u origen del certificado (aunque está limitado a 200 caracteres, por lo que obviamente no es una alternativa a un documento CPS separado).

Si desea obtener detalles precisos sobre la codificación en certificados de OID de directivas y URL de CPS, vea RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, en la sección "Información adicional" al final de este capítulo.

Tras obtener el OID de la CP y decidir la URL donde se publicará la CPS, puede incluirlo en los certificados de la entidad emisora. Este procedimiento se describe en el capítulo 7, "Implementación de la infraestructura de claves públicas".

Compatibilidad de la infraestructura de IT

La PKI de esta solución se basa en otros servicios de infraestructura para funcionar correctamente. El diagrama siguiente ilustra los principales, IIS y Active Directory, y su modo de interacción con las entidades emisoras y los clientes de certificados.

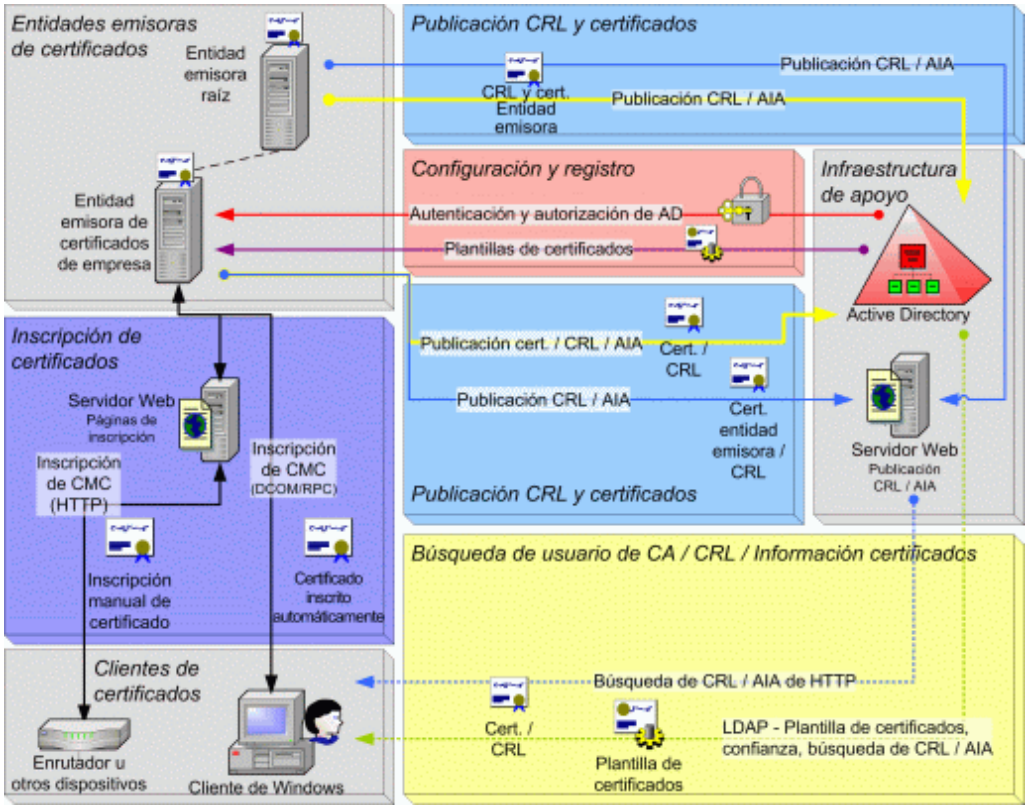

Figura 4.3 Interacción de entidad emisora con la infraestructura de TI
Ver imagen a tamaño completo

La supervisión, los servicios de alerta y la administración son imprescindibles para el funcionamiento correcto de los Servicios de Certificate Server, aunque estos componentes no se ilustran en el diagrama. El capítulo 11, “Administración de la infraestructura de claves públicas” describe esta infraestructura con más detalle. Las secciones siguientes describen los servicios que ofrecen Active Directory e IIS a la PKI.

Active Directory

Tal como se explica en la sección anterior, “Integración en Active Directory”, Active Directory ofrece varios servicios diferentes que son esenciales para la PKI. Éstos incluyen la publicación de certificados, el registro de certificados, la asignación de cuentas de certificados y el almacenamiento de la información de configuración y de confianza.

Todos estos servicios se proporcionan automáticamente para las entidades emisoras de certificados de empresa. Las entidades emisoras de certificados independientes en línea también pueden utilizar algunos de estos servicios. Sin embargo, las entidades emisoras sin conexión no pueden interactuar directamente con Active Directory para almacenar y recuperar información.

En esta solución, el certificado de la entidad emisora raíz sin conexión se publica en el almacenamiento raíz de confianza de Active Directory. El resultado es que el certificado de entidad emisora raíz se distribuirá automáticamente al almacén raíz de confianza de todos los clientes Active Directory del mismo bosque.

Además, la entidad emisora raíz podría utilizar Active Directory para los siguientes servicios de publicación (aunque éstos no se utilizan en la solución):

- Publicación de listas CRL: los clientes del dominio (de todo el bosque) pueden recuperar listas CRL publicadas en Active Directory desde un controlador de dominio local.
- Distribución de certificados cruzados a clientes del dominio: los certificados cruzados publicados en Active Directory se distribuirán automáticamente al almacén de certificados local de todos los clientes Active Directory del mismo bosque.

La entidad emisora de certificados utiliza Active Directory para todos los servicios descritos en la sección "Integración en Active Directory".

Utilización de Active Directory para clientes que no son Active Directory
Hay unas cuantas consideraciones sobre la compatibilidad de clientes PKI que son miembros de un bosque de Active Directory que no es de confianza o que no son miembros de ningún bosque de Active Directory.

Si desea permitir que este tipo de clientes externos recuperen certificados de la entidad emisora y las listas CRL mediante el Protocolo ligero de acceso a directorios (LDAP), debe plantearse los puntos siguientes:

- Los clientes externos requieren la configuración de un nombre de host LDAP explícito para rutas de acceso CDP y AIA. Para obtener más información, consulte la sección "Configuración de rutas de acceso CDP y AIA", que aparece más adelante en este capítulo.
- Los clientes externos no podrán realizar consultas LDAP anónimas en Active Directory de forma predeterminada. Debe cambiar el valor de **dsHeuristics** del bosque y otorgar permisos de acceso explícitos a la cuenta anónima. Para obtener más información sobre este tema, consulte la sección "Información adicional" que aparece al final de este capítulo.

  Advertencia: esto permite LDAP anónimo en todos los controladores de dominio del bosque (aunque los clientes no autenticados sólo podrán obtener acceso a los elementos con permisos explícitos para la cuenta anónima). Considere todas las implicaciones de permitir el acceso no autenticado al directorio antes de continuar.
- Los clientes externos no heredarán la información raíz de confianza configurada en el directorio, de modo que deberá configurar esta información de algún otro modo.

Consideraciones para clientes de Internet
Hay algunas consideraciones importantes para la configuración de CDP y AIA para clientes que se encuentran fuera de la organización (por ejemplo, clientes de Internet). Éstas se explican en la sección "Configuración de rutas de acceso CDP y AIA", incluida más adelante en este capítulo.

Si necesita proporcionar la búsqueda de certificados a clientes de Internet para la compatibilidad, por ejemplo, la búsqueda de certificados de correo electrónico, es posible que deba crear un directorio LDAP aparte para que lo utilicen los clientes de Internet. Debido a las implicaciones de seguridad que esto conlleva, se recomienda no utilizar el método descrito previamente para habilitar LDAP anónimo del bosque de Active Directory interno. En su lugar, cree un bosque de Active Directory aparte y replique la información del bosque interno mediante la herramienta de metadirectorio LDIFDE (como, por ejemplo, Microsoft Metadirectory Services) u otro producto de sincronización de directorios.

Servicios de Internet Information Server
IIS ofrece dos servicios para la PKI en este diseño:

- Publica información de entidad emisora de certificados como, por ejemplo, las listas CRL, los certificados de entidades emisoras y, posiblemente, documentos CPS.
- Ofrece la posibilidad de inscribir certificados mediante una interfaz Web, lo que resulta especialmente útil para clientes ajenos a Windows, aunque esta capacidad no se utiliza en esta solución.

Utilización de IIS para publicar información de entidad emisora de certificados
En esta solución, la información de CDP y AIA para las entidades emisoras raíz y emisora se publicará en un servidor Web. La publicación HTTP permite a un número más amplio de clientes recuperar la información requerida.

Es común la instalación de IIS en la entidad emisora para este propósito, pero puede que no sea el mejor procedimiento. Si hay otro servidor IIS disponible y puede utilizarse para publicar la lista CRL y la información de entidad emisora, debería utilizarlo. Intente limitar las formas en que los usuarios pueden obtener acceso a las entidades emisoras de certificados porque cada protocolo y servicio adicional que haya en la entidad emisora de certificados ofrecerá a posibles atacantes otro posible punto de entrada al servidor. La utilización de IIS en la entidad emisora de certificados también impide que la entidad emisora de certificados se desactive para mantenimiento, ya que puede ser la única ubicación de CRL válida para muchos clientes.

En la publicación Build Guide, la CA emisora se utiliza para alojar IIS para la publicación de listas CRL y entidad emisora de certificados, lo que simplifica el proceso de creación y reduce los requisitos de hardware adicional. Sin embargo, Microsoft recomienda que se utilicen ubicaciones diferentes.

Utilización de páginas IIS para inscribir certificados
Las páginas de inscripción IIS resultan útiles en variedad de escenarios: para la inscripción de clientes que no son de dominio, la inscripción de clientes ajenos a Windows o para clientes de exploradores que no sean Microsoft Internet Explorer.

Sin embargo, las páginas de inscripción Web no se requieren en una entidad emisora de certificados. En esta solución, se instalan en las entidades emisoras de forma predeterminada, aunque pueden instalarse en un servidor Web aparte (para ofrecer compatibilidad con páginas ASP, el servidor debe contar con IIS 5.0 o una versión posterior). Las páginas de inscripción facilitan algunas tareas, pero no es necesario que las instale si no las necesita. Para obtener más información acerca de la instalación y el uso de las páginas de inscripción Web, consulte la sección “Información adicional” al final de este capítulo.

Configuración de rutas de acceso CDP y AIA

Los clientes necesitan acceso a listas CRL actualizadas para determinar la revocación de certificados. Además, los clientes deben recuperar certificados de la entidad emisora para comprobar que un certificado de entidad final se encadena con una raíz de confianza. Cada entidad emisora debe codificar en sus certificados una o varias direcciones URL que indiquen ubicaciones que los clientes puedan usar para obtener esta información sobre los certificados.

La configuración de CDP y AIA para cada entidad emisora dependerá de los tipos de clientes que usarán sus certificados. ¿Están destinados únicamente para su uso por parte de usuarios y equipos miembros del bosque de Active Directory, por ejemplo? ¿O también necesitarán utilizarlos los usuarios o dispositivos externos? La definición de clientes de certificados se ha explicado anteriormente en este capítulo.

Entidad emisora raíz

La entidad emisora raíz se configurará para esta solución de la forma siguiente:

- Las rutas de acceso CDP y AIA principales (se indican primero) serán las direcciones URL HTTP. La lista CRL de la entidad emisora raíz suele ser muy pequeña (1- 2 KB) y el intervalo de publicación muy largo (seis meses), por lo que si sólo se publica en una ubicación, no provocará cuellos de botella significativos cuando los clientes recuperen la CRL.
- Las rutas secundarias se configurarán como direcciones URL LDAP para crear una copia de seguridad de las ubicaciones HTTP. No se utilizará ningún nombre de host LDAP, por lo que los clientes del mismo bosque recuperarán la información de sus controladores de dominio locales. Los clientes fuera del bosque no podrán obtener acceso a esta ubicación.

Esta configuración permite que clientes que se encuentran fuera del bosque de Active Directory utilicen los certificados de esta entidad emisora de certificados y de las entidades emisoras de certificados subordinadas, ya que de forma predeterminada utilizarán las rutas HTTP.

Entidad emisora de certificados

Se optimizará la CA emisora de esta solución para que los clientes Active Directory internos la utilicen. La entidad emisora se configurará de la siguiente manera:

- Las rutas de acceso principales de las direcciones URL de CDP y AIA serán las rutas de acceso de directorios LDAP.
- No se especificará ningún nombre de host LDAP en las direcciones URL de CDP y AIA, lo que permitirá que el cliente utilice el servidor LDAP predeterminado. En el caso de clientes Active Directory, los controladores de dominio locales constituyen el servidor LDAP predeterminado. Sin embargo, otros clientes LDAP pueden fallar al consultar estas rutas LDAP.

Esta configuración es óptima para los clientes del mismo bosque que las entidades emisoras. Las listas CRL básicas se publican semanalmente y las diferencias entre CRL se publican diariamente. Puesto que la ubicación predeterminada para las dos es Active Directory, los clientes las recuperarán de sus controladores de dominio

más cercanos, lo que ofrece resistencia, así como optimización del tráfico de red.

Configuración de CDP y AIA para clientes externos
La organización anterior no será óptima para los clientes que son miembros de otro bosque de Active Directory o que no son miembros de ningún bosque de Active Directory (por ejemplo, un enrutador). Puesto que estos clientes foráneos no pueden obtener acceso a los CDP y AIA de LDAP, los usuarios externos pueden experimentar retrasos significativos al intentar comprobar la información de revocación y de AIA. Estos retrasos pueden provocar errores en las aplicaciones para estos clientes externos.

Si existe la posibilidad de que los certificados vayan a utilizarse fuera del bosque de Active Directory, deberá configurar los valores CDP y AIA para usar URL de HTTP como rutas primarias en lugar de URL de LDAP.

Para incluir URL de LDAP que puedan usar los clientes externos, debe hacer lo siguiente:

- Configure un nombre de host LDAP explícito para rutas CDP y AIA; no puede usar la ruta nula predeterminada (LDAP:///). La modificación de una ruta CDP o AIA para una entidad emisora requiere la repetición de emisión (renovación) del certificado de la entidad emisora.
- Debe habilitar el acceso LDAP anónimo, tal como se describe previamente en este capítulo.

Consideraciones para clientes de Internet
Si tiene previsto distribuir certificados fuera de la organización para que se utilicen en Internet, existen unas cuantas consideraciones adicionales a tomar en cuenta.

Los certificados que contienen direcciones URL LDAP internas pueden ofrecer información acerca de la estructura y los nombres internos de Active Directory y la entidad emisora de certificados. Para evitarlo, debe:

- Utilizar solamente direcciones URL HTTP para los valores de CDP y AIA de la entidad emisora raíz y para las entidades emisoras subordinadas de la cadena.
- Emita certificados que van a utilizarse externamente desde una entidad emisora aparte. Esta entidad emisora de certificados sólo utilizará los URI de CDP y AIA HTTP.

En ambos casos, debe ofrecer una ubicación HTTP secundaria para la recuperación de listas CRL a la que los clientes puedan recurrir en caso de que la ubicación principal no esté disponible.

Para obtener una explicación más profunda sobre el uso de las listas CRL y CDP, consulte las referencias de la sección “Información adicional”, incluida al final del capítulo.

Ampliación de la infraestructura de la entidad emisora de certificados

La sección “Definición de los requisitos de seguridad de los certificados” explica la clasificación de los certificados por nivel de seguridad y también por tipo de sujeto. La razón principal para separar los distintos tipos de sujetos es que probablemente se aplicarán diferentes directivas de certificados y prácticas operativas (tal como se documenta en las CPS) a estos tipos de sujetos.

Normalmente, se aplica una CPS por cada entidad emisora de certificados. Es posible acomodar diferentes directivas que rijan diferentes tipos de sujetos en una sola entidad emisora de certificados, pero la CPS será más compleja y, con frecuencia, difícil de implementar correctamente. La estrategia para ampliar esta PKI de modo que emita certificados cubiertos por diferentes directivas y requisitos de seguridad es crear CA emisoras adicionales para los tipos de sujetos principales. Esta configuración se ilustra en la figura siguiente.

Nota: esta figura sólo indica cómo puede ampliarse la jerarquía de entidad emisora de certificados anterior. Puede que la organización requiera una ampliación mucho más compleja o mucho más simple para cubrir necesidades futuras. Cree el diseño de entidades emisoras adicionales y capacidad de certificados según sus requisitos de seguridad: no hay un diseño absolutamente correcto o incorrecto para una PKI. Cuando se plantee la ampliación de la PKI para cubrir el resto de sus requisitos de certificados, debería seguir un enfoque similar al indicado aquí para el diseño de la PKI simple.

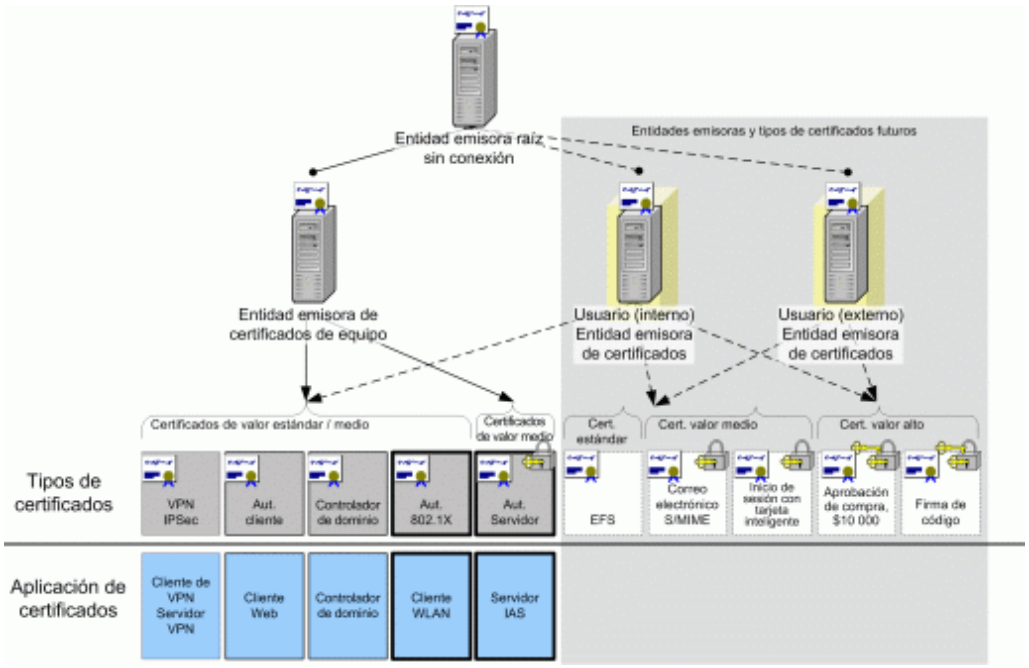

Figure 4.4 Ampliación de la jerarquía de entidad emisora
Ver imagen a tamaño completo

Esta figura muestra cómo puede ampliarse la jerarquía de entidades emisoras de certificados simple presentada anteriormente, de modo que satisfaga una variedad más amplia de requisitos de certificados. Las nuevas entidades emisoras de certificados y capacidades de certificados aparecen con un fondo gris. La figura ilustra también el uso de certificados de alto valor (símbolo de llave y candado) y cómo a medida que las entidades emisoras de certificados (internas y externas) entran en conexión, toman el control de la función de emitir certificados de usuario de valor estándar de la primera entidad emisora de certificados.

Esta estrategia para ampliar la infraestructura de entidades emisoras de certificados incluye algunas suposiciones:

- La administración de la infraestructura de las entidades emisoras se llevará a cabo de forma centralizada, es decir, no existen requisitos de delegación del control de las entidades emisoras de certificados por división geográfica u organizativa.
- Se utilizan estándares de certificado comunes en toda la organización, es decir, un certificado de un tipo determinado ha aceptado y admitido comúnmente usos y directivas de toda la organización.
- No se requiere ninguna interoperabilidad con una PKI existente.
- Se requieren niveles de seguridad y directivas diferentes para los distintos tipos de certificados mostrados (y cualquier otro que se pueda requerir).

Si estas suposiciones no son válidas para su organización, requerirá una estructura más compleja que ésta. Para obtener una explicación detallada de las opciones y enfoques diferentes respecto a la ampliación de la infraestructura de entidades emisoras, consulte el documento “Designing a Public Key Infrastructure” sobre el diseño de infraestructuras de claves públicas, al que se hace referencia al final de este capítulo.

Subordinación calificada

Las definiciones de los certificados que ha creado pueden utilizarse para definir plantillas de certificados y emitir certificados sin necesidad de personalizarlas más. Sin embargo, al ampliar la PKI, es aconsejable limitar el ámbito de los certificados que las entidades emisoras pueden emitir mediante la limitación de la delegación de certificados de su entidad emisora.

Puede utilizarse la subordinación calificada, que se ha explicado en una sección anterior, para controlar el ámbito y el propósito de las confianzas de la organización mediante la creación de certificados cruzados entre su

infraestructura de entidad emisora y las de organizaciones externas. Puede utilizar esta misma técnica para limitar los tipos de certificado y determinados atributos de certificados dentro de su propia jerarquía de entidades emisoras. Una explicación más detallada de este tema queda fuera del alcance de este capítulo. Consulte el documento técnico *Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003* sobre el planeamiento y la implementación de certificación cruzada y subordinación calificada con Windows Server 2003, al que se hace referencia al final del capítulo.

Para la PKI en esta solución, no se requiere el uso de la subordinación calificada dentro de la jerarquía de entidades emisoras.

Principio de la página

Configuración de perfiles de certificado.

Esta sección explica cómo se configuran los certificados para satisfacer los requisitos definidos previamente en el capítulo.

Definición de los parámetros de los certificados

Para cada tipo de certificado que necesite, deberá especificar el perfil de certificado para dicho tipo. Seguidamente podrá configurar los parámetros de perfiles en plantillas de certificados que controlan los tipos de certificados emitidos por su entidad emisora.

Nota: las entidades emisoras de certificados independientes no utilizan plantillas de certificados. Deberá crear la solicitud mediante procesos de programación; alternativamente, puede utilizar una herramienta como Certreq.exe o el formulario de las páginas de inscripción Web. Aunque use una entidad emisora independiente, debería definir perfiles de certificados para cada tipo de certificado y utilizarlos en la creación de solicitudes de certificados a una entidad emisora independiente.

Una definición de perfil de certificado incluye todos los elementos siguientes:

- Nombre de plantilla y nombre de visualización (debe definir un estándar de denominación para estos)
- Longitud de clave de certificado
- Período de validez del certificado
- Extensiones de certificado opcionales
- Directivas de inscripción y renovación
- Directivas relacionadas con los períodos de validez
- Directivas relacionadas con el uso de aplicaciones
- Directivas relacionadas con el uso de claves
- Directivas relacionadas con el archivado de claves
- Autorización de certificados
- Creación de nombre de asunto
- Agentes de inscripción de certificados
- Creación de claves
- Claves y tipos de CSP

Las opciones de longitud de clave, período de validez y creación de claves, así como las directivas de inscripción y autorización, se determinan por el nivel de seguridad de los certificados requerido y los requisitos de aplicación identificados previamente en el capítulo.

Definición de la vigencia de certificados y claves

Son varios los factores que afectan a la vigencia de los certificados como, por ejemplo, el tipo de certificado, los requisitos de seguridad de la organización, las prácticas estándar del sector y la legislación estatal. En general, las claves más largas admiten una vigencia de certificados y de claves más larga.

Existen restricciones en la longitud de clave y el tipo de clave:

- Compatibilidad: es posible que algunas aplicaciones de certificados no sean compatibles con claves de una longitud superior a 2048 bits. El tipo de clave también puede afectar a la compatibilidad; generalmente, las claves RSA ofrecen una compatibilidad óptima pero algunas aplicaciones pueden requerir otro tipo de claves. Debe tener en cuenta la compatibilidad de longitud y tipo de clave de todas las entidades emisoras de certificados de la cadena, ya que se requerirán aplicaciones para procesar todos los certificados de la cadena.
- Rendimiento: las operaciones de firma y de cifrado requieren una capacidad de procesamiento mayor para las claves grandes que para las pequeñas. Por esta razón, generalmente no deben utilizarse claves superiores a 2048 bits en las entidades emisoras con alta velocidad de emisión de certificados.
- Almacenamiento: las claves grandes crean certificados grandes que requieren un almacenamiento mayor en la base de datos de certificados. Si los certificados se publican en Active Directory, sus requisitos de almacenamiento también aumentarán. El tamaño y el tipo de las copias de seguridad se incrementarán proporcionalmente.

Al elegir la vigencia de los certificados y las claves, debe tener en cuenta la vulnerabilidad de estas últimas frente a posibles ataques y las consecuencias de este riesgo. Los factores siguientes afectan a la vigencia que elija para los certificados y las claves:

- Longitud de clave privada: las claves largas son más difíciles de averiguar, por lo que se justifica que su vigencia sea más larga.
- Seguridad de entidad emisora de certificados: cuanto más seguras sean la entidad emisora y su clave privada, más larga será la vigencia segura.
- Uso de hardware de cifrado especializado: las tarjetas inteligentes y los HSM protegen la clave privada de forma más eficaz y justifican una vigencia más larga.
- Confianza en los sujetos de los certificados: puede permitir una vigencia de certificados más larga para los empleados y los equipos internos que para los usuarios y los equipos externos.
- El número de certificados firmados con una clave de entidad emisora: cuantas más veces se obtenga acceso a la clave y más amplio sea el ámbito al que se distribuya la clave pública de la entidad emisora, más probable será que la clave se vea atacada y posiblemente comprometida.

La vigencia de esta clave y los períodos de renovación para las entidades emisoras de certificados y las entidades finales utilizadas en esta solución se muestran en la tabla siguiente.

Tabla 4.10: Vigencia de certificados y claves

Sujeto de certificado	Longitud de clave	Vigencia de clave	Intervalo de renovación
Entidad emisora raíz	4096 bits	16 años	Ocho años
Entidad emisora de certificados	2048 bits	Ocho años	Cuatro años
Entidad final	De 1024 a 2048 bits	De seis meses a dos años	90 por ciento de período de validez

En lo que respecta a longitud de clave, se considera que las claves de 1024 bits no se pueden descifrar mediante un análisis criptográfico. Deben tener una vigencia de clave segura muy superior al valor propuesto de entidad final de 2 años. El uso de claves de 512 bits ya no se considera seguro, excepto quizás para aplicaciones con muy

pocos requisitos de seguridad. Por este motivo no se utilizan claves de 512 bits en esta solución.

La fortaleza de la clave de la CA emisora es un compromiso entre los requisitos de seguridad y de rendimiento. Una clave de este tamaño tiene actualmente una vigencia superior al período de renovación de cuatro años.

La entidad emisora raíz no tiene restricciones de rendimiento reales, por lo que la fortaleza de la clave debe establecerse en el máximo de 16 kilobits. Por razones de compatibilidad, en esta solución se establece en un nivel muy inferior. De todos modos, las claves de 4096 bits tienen una vigencia de clave segura superior al período de renovación de ocho años.

Todas las entidades emisoras de certificados utilizan claves RSA, aunque el tipo de clave para las entidades finales quedará determinado por los requisitos de la aplicación.

Es posible renovar un certificado con la misma clave pero no se recomienda que lo haga bajo circunstancias normales. En esta solución se genera un nuevo par de claves con cada renovación de certificado.

Los certificados emitidos por las entidades emisoras no pueden tener un período de validez que sobrepase los períodos de validez restantes de la entidad emisora y de todas las entidades emisoras de certificados superiores hasta llegar a la raíz. Por ejemplo, si el certificado de entidad emisora va a caducar en seis meses, sólo puede emitir certificados con una vigencia máxima de seis meses. Por lo tanto, esta solución obliga a que los certificados de entidad emisora se renueven cuando haya transcurrido la mitad de la vigencia de los certificados. Todos los certificados emitidos por una entidad emisora de certificados tienen un período de validez que no supera la mitad de la vigencia de los certificados de la CA emisora.

Esto ofrece períodos de validez máximos anidados de cuatro, ocho y dieciséis años para las entidades finales, las CA emisoras y las entidades emisoras raíz, respectivamente. En esta solución, los certificados de entidad final se mantienen hasta un período de validez máximo de dos años. Esto permite introducir una capa de entidad emisora de certificados intermedia adicional sin provocar un impacto excesivo en la jerarquía de vigencias de certificados.

Asignación de requisitos de seguridad a los parámetros de certificados

En la tabla siguiente se indican los tipos de certificados identificados previamente en el capítulo y el modo en que se asigna la categoría de seguridad de cada tipo a los parámetros de perfil de certificado.

Tabla 4.11: Parámetros de certificados

Tipo de certificado	Directiva de emisión	Método de aprobación	Clave	Período de validez	Almacenamiento de claves	Exportación de claves	CSP
Autenticación de cliente: usuario	Baja	Automática (autenticación de dominio)	1024	Un año	Software	No	Denominado
Autenticación de cliente: equipo	Baja	Automático (autenticación de dominio)	1024	Un año	Software	No	Denominado
Autenticación de servidor IAS	Media	Manual (Administrador de certificados)	1024	Un año	Software	No	Denominado

Notas:
La directiva “Baja” en la columna **Directiva de emisión** hace referencia a la directiva de certificados de “Seguridad baja” predefinida en Servicios de Certificate Server. Equivale al nivel de seguridad o garantía estándar mencionado anteriormente en este capítulo.

El valor “Denominado” en la columna de la tabla que muestra los **CSP** (proveedores de servicios de cifrado) indica que deben especificarse los CSP permitidos por esta plantilla. Los certificados de equipo cliente y servidor tienen requisitos de CSP específicos.

Asignación de requisitos de certificados a parámetros de plantillas de certificados

Las aplicaciones esperan con frecuencia que los certificados estén configurados de manera precisa. Pueden requerir que el nombre de asunto tenga un formato determinado, que se incluyan OID de directiva de aplicación específicos o que el certificado se haya emitido con una directiva de emisión concreta. Como mínimo, la aplicación requerirá que el uso de claves se haya definido correctamente. El propietario (o proveedor) de la aplicación debe proporcionarle todos estos parámetros para definir el perfil de certificados.

Los requisitos de aplicación para la lista de certificados requeridos en esta solución se muestran en las tablas siguientes. Estas tablas ilustran las propiedades de los certificados y los parámetros de la entidad emisora de certificados (tal como se configuran en las plantillas de certificados). No aparecen todas las propiedades posibles.

Nota: todos los tipos de certificados que se muestran a continuación se basan en uno de los tipos de plantilla integrada. En lugar de modificar las plantillas originales, haga copias de las plantillas integradas y edite dichas copias para obtener la configuración requerida. Esto le permitirá revertir fácilmente a las plantillas integradas si fuera necesario, ya que no se han modificado.

Tabla 4.12: Autenticación de cliente: usuario

Parámetro del certificado	Valor obligatorio
Nombre de plantilla de certificado	Autenticación de cliente: usuario
Publicación de Active Directory	No
Uso de claves	Firma digital
Almacenamiento de claves	No
Tamaño mínimo de la clave	1024
Nombre de asunto	Nombre común
Nombre alternativo del sujeto	Nombre principal de usuario
Directivas de aplicación/Uso de clave ampliada	Autenticación de cliente
Proveedores de servicios de cifrado (CSP)	Microsoft Base Cryptographic Provider v1.0 Microsoft Enhanced Cryptographic Provider v1.0
Derivado de plantilla	Sesión de autenticación

Tabla 4.13: Autenticación de cliente: equipo

Parámetro del certificado	Valor obligatorio
Nombre de plantilla de certificado	Autenticación de cliente: equipo
Publicación de Active Directory	No
Uso de claves	Firma digital Cifrado de clave

Almacenamiento de claves	No
Tamaño mínimo de la clave	1024
Nombre de asunto	Nombre común
Nombre alternativo del sujeto	Nombre DNS
Directivas de aplicación/Uso de clave ampliada	Autenticación de cliente
Proveedores de servicios de cifrado (CSP)	Proveedor de cifrado RSA SChannel de Microsoft
Derivado de plantilla	Autenticación de estación de trabajo

Tabla 4.14: Autenticación de servidor 802.1X

Parámetro del certificado	**Valor obligatorio**
Nombre de plantilla de certificado	Autenticación de servidor 802.1X
Publicación de Active Directory	No
Uso de claves	Firma digital Cifrado de clave
Almacenamiento de claves	No
Tamaño mínimo de la clave	1024
Nombre de asunto	Nombre común
Nombre alternativo del sujeto	Nombre DNS
Directivas de aplicación/Uso de clave ampliada	Autenticación de servidor
Proveedores de servicios de cifrado (CSP)	Proveedor de cifrado RSA SChannel de Microsoft
Derivado de plantilla	Servidores IAS y RAS

Creación de plantillas de certificado

Active Directory de Windows Server 2003 contiene definiciones de plantillas de certificados predefinidas para muchas funciones habituales. Cuando se instala una CA de empresa, se configura de forma predeterminada para que emita varios de estos tipos de certificados integrados. Puede encontrar descripciones de todas las plantillas integradas en la documentación del producto Windows Server 2003 Enterprise Edition. (Consulte la sección “Información adicional” al final del capítulo para ver una referencia precisa.)

En la solución presentada en esta guía, la mayoría de estas plantillas predeterminadas se eliminan de la entidad emisora; es decir, se eliminan de la carpeta de plantillas en la consola de administración de la entidad emisora de certificados (no debería suprimir las definiciones de plantillas del directorio).

Puede optar por utilizar las plantillas predefinidas si coinciden con sus necesidades; la mayoría de aplicaciones basadas en certificados de Windows (como EFS y autenticación de VPN, entre otras) quedan cubiertas por estas plantillas. Si necesita emitir otros tipos de certificados, normalmente resulta mejor crear plantillas específicamente alineadas a los requisitos. Si utiliza las plantillas predefinidas sin comprender sus posibilidades, se arriesga a habilitar una funcionalidad no prevista. Por ejemplo, el certificado de equipo, diseñado para la

autenticación de cliente simple, también puede utilizarse como certificado de servidor Web.

Para crear plantillas nuevas, debe buscar una plantilla predefinida similar a sus requisitos de perfil de certificado y crear un duplicado de dicha plantilla en el que basará las nuevas. La configuración de plantillas es un proceso sencillo de selección de atributos aplicables a los perfiles de certificados definidos en esta sección.

Nota: no puede crear una plantilla nueva desde cero; debe hacer una copia de una plantilla existente y editarla según sea necesario. Las plantillas de equipo siempre deben derivarse de plantillas de equipo y las plantillas de usuario, de plantillas de usuario; no se pueden intercambiar.

A medida que va creando y modificando las plantillas, mantenga un registro detallado de los parámetros de las plantillas como parte del sistema de administración de la configuración.

Principio de la página

Creación de un plan de administración de certificados

Tras configurar los certificados para la organización, debe crear un plan para administrarlos durante su vigencia. La creación de un plan de administración de certificados implica la toma de decisiones sobre lo siguiente:

- la forma en que se procesan las solicitudes de certificados nuevos y de renovación de certificados.
- la forma en que se asignan certificados a cuentas de usuario.
- la forma en que se administran y se distribuyen las listas CRL.
- las estrategias que se utilizan para la recuperación de los datos cifrados.

Selección de los métodos de inscripción y de renovación

Para realizar la inscripción de certificados puede utilizar varios métodos distintos (la renovación también se puede efectuar con estos métodos):

- inscripción automática de Windows.
- inscripción en línea con el Asistente para la inscripción de certificados (normalmente se inicia desde la consola de administración de certificados).
- inscripción en línea mediante las interfaces CryptoAPI o CAPICOM desde aplicaciones o secuencias de comandos.
- mediante la utilización de la herramienta Certreq.exe para crear y enviar solicitudes y recuperar certificados emitidos.

  Nota: los cuatro métodos anteriores sólo son interfaces diferentes de la misma interfaz de inscripción en línea básica.
- inscripción en página Web.
- Inscripción manual fuera de línea (implica la generación de la solicitud como un archivo con uno de los métodos definidos anteriormente, la colocación de este archivo en la entidad emisora, su envío a través de la consola de administración de entidades emisoras de certificados y su recuperación a través de la consola de administración).

Todos estos métodos son válidos y adecuados según las circunstancias. Esta solución utiliza los siguientes métodos de inscripción:

- inscripción automática de Windows. Es el método preferido siempre que sea posible, ya que reduce la administración de certificados. Puede utilizar la inscripción automática aunque un certificado requiera la aprobación manual (pero no cuando requiera la firma de un agente de inscripción). Aunque el certificado no se emitirá inmediatamente, se enviará una solicitud a la entidad emisora y la inscripción se completará cuando se apruebe la solicitud.

  Inscripción manual fuera de línea. Este método se utiliza para todas las inscripciones y renovaciones de

- certificados en la entidad emisora raíz.

Ninguno de estos métodos es adecuado para situaciones más complejas, por ejemplo, cuando una solicitud de certificado requiere la firma de un tercero antes de enviarla a la entidad emisora. La inscripción en línea basada en la llamada a procedimiento remoto (RPC) tampoco es compatible con la mayoría de plataformas ajenas a Windows (por ejemplo, enrutadores). Además, la inscripción automática no es posible si se debe definir el nombre del sujeto o un nombre de sujeto alternativo en la solicitud de certificado (en lugar de generarlo Active Directory).

Para adaptarse a requisitos avanzados como estos, considere el uso de uno de los métodos siguientes:

- crear una secuencia de comandos CAPICOM para ejecutarla en el equipo independiente cliente, por ejemplo, como parte de una secuencia de comandos de inicio de sesión.
- Utilizar certreq.exe en un archivo de comandos o por lotes para generar y enviar solicitudes y para recuperar e instalar el certificado emitido.
- crear una página Web (ASP o Microsoft ASP.NET) personalizada utilizando CAPICOM para crear y enviar la solicitud. Con esta última técnica, es posible ofrecer servicios de inscripción a un amplio conjunto de clientes e incluir sofisticados procesos de fases múltiples (por ejemplo, cuando se requieren varias firmas para aprobar una solicitud).

Asignación de certificados a identidades

La asignación entre certificados y sujetos nombrados en los certificados es un tema de explicación amplia y se encuentra fuera del ámbito de este capítulo. Sin embargo, hay que tener en cuenta dos aspectos importantes:

- ¿Cómo se confirma la identidad del sujeto del certificado antes de emitir éste?
- ¿Cómo se descubre la identidad del sujeto del certificado a partir de la información facilitada en el directorio?

La primera de estas preguntas está relacionada con la forma en que se ha llevado a cabo el proceso de registro del certificado. Este aspecto se explica en la sección siguiente, “Creación de directivas de certificados”. La segunda pregunta explica la forma en que los usuarios de certificados (aplicaciones y servicios) asignan correctamente la identidad del sujeto de certificado a otra identidad que puedan utilizar. Serían ejemplos de este último aspecto:

- ¿Cómo identifica un controlador de dominio a un usuario a partir del certificado de tarjeta inteligente para iniciar la sesión del usuario en el dominio y crear un token de acceso?
- ¿Cómo descubre un usuario de correo electrónico el certificado de una persona a la que desea enviar un correo electrónico seguro?

La mayoría de los certificados se asignan automáticamente a las entidades principales de seguridad de Active Directory (usuarios y equipos) como parte del proceso de inscripción. Active Directory define el nombre del sujeto y el nombre del sujeto alternativo) del certificado para crear una asignación implícita entre el certificado y el principal de seguridad nombrado en el certificado. Normalmente, el nombre del sujeto alternativo contendrá el nombre principal de usuario (UPN, User Principal Name) o el nombre de correo electrónico si se trata de un usuario y el nombre principal de servicio (SPN, Service Principal Name) o el nombre de host DNS si se trata de un equipo. Los valores de UPN y SPN serán siempre únicos en un bosque de Active Directory. Los nombres de correo electrónico y DNS deben ser únicos globalmente (aunque Active Directory no obligue a ello). Otros servicios de Windows, como IIS y IAS, pueden llevar a cabo la asignación de certificados también para identidades de equipos o usuarios.

Nota: la asignación de certificados no guarda ninguna relación con la publicación de certificados. La asignación de certificados implica que hay algún atributo del certificado (normalmente el nombre alternativo del sujeto) que identifica exclusivamente a un objeto en el directorio. El servidor IAS lo utiliza para determinar la identidad de un usuario o equipo desde un certificado presentado. IAS usa esta asignación implícita en lugar de buscar certificados en el directorio. La publicación y la búsqueda de certificados describen la ubicación donde se almacenan los certificados en el directorio como atributos de objetos de usuario o equipo. Esto permite que los usuarios puedan buscar a personas en el directorio y recuperar los certificados que les pertenecen.

También se puede importar manualmente o asignar otros certificados a los objetos de usuario o equipo mediante la consola de administración de usuarios y equipos de Active Directory.

De forma inversa, hay muchos ejemplos de casos en que no se requiere la asignación directa a un objeto de directorio; entre ellos se incluyen los siguientes:

- Los servidores Web en los que el identificador principal es el nombre de host DNS del sitio Web.
- Cuando se emiten certificados a entidades que no tienen equivalente de Active Directory (por ejemplo, un enrutador o un usuario de otra organización).

Todas las entidades finales de la solución en esta guía tienen una asignación directa (e implícita) a usuarios y equipos de Active Directory.

Las entidades emisoras son casos especiales que no se asignan necesariamente a objetos de equipo. Sin embargo, normalmente se asignarán a objetos de entidades emisoras de certificados en los contenedores de entidades emisoras de certificados de confianza y AIA de Active Directory.

Creación de directivas de certificados

Como mínimo, debe definir el método de aprobación de certificados para cada categoría de seguridad de certificado (alta, media y baja) y Microsoft recomienda que lo haga también para cada categoría de sujeto de certificado (equipo, usuario interno, usuario externo). No es probable que tenga que definir directivas a un nivel más específico que éste. Documente estas decisiones de directivas como parte de la declaración de directivas de certificados y CPS.

Las diferentes directivas de certificados se usan como indicación del tipo de proceso de aprobación de certificados y del nivel de seguridad de la clave privada utilizados en la inscripción de un certificado. Puede codificarla (aunque no es necesario) en el certificado mediante OID para representar las diferentes directivas. El rigor del proceso de aprobación debe reflejar el valor del certificado que se aprueba. El objetivo del proceso de aprobación (o registro) es ofrecer un nivel adecuado de confianza de que el solicitante del certificado es la misma entidad que el sujeto del certificado. La fuerza de seguridad de la clave es una medida de la confianza que puede depositarse en el hecho de que la clave privada permanecerá privada y en la sola posesión del sujeto de certificado.

Los niveles de seguridad de certificados que se utilizan en esta solución se han definido anteriormente, en la sección “Definición de los requisitos de seguridad de los certificados” de este capítulo. Puede indicar el nivel de seguridad de los certificados que emite mediante la inclusión de un OID de directiva de certificado correspondiente al nivel de seguridad de estos certificados. Las aplicaciones (y los usuarios) pueden utilizar la directiva para determinar el nivel de confianza de un certificado determinado.

Los tres niveles de seguridad definidos anteriormente corresponden a las tres directivas de certificados predefinidas en Windows Server 2003 (“directivas de seguridad” en la consola de administración de plantillas de certificados de Microsoft). La tabla siguiente explica el uso de las diferentes directivas de certificados en esta solución. Debe incluir OID de directiva en las plantillas de certificados (al menos para las directivas de seguridad media y alta) a fin de que sea fácil identificar los certificados de seguridad alta. Se supone que los certificados sin directiva de certificado son de seguridad estándar.

Tabla 4.15: Niveles de directivas de emisión de certificados

Directiva (de emisión) de certificados	Requisitos de registro	Requisitos mínimos de almacenamiento de claves
Baja (Estándar)	Aprobación automática dependiente de la autenticación satisfactoria del dominio Para las entidades emisoras independientes, se trata de un nivel de aprobación no autenticada, es decir, la entidad emisora emite el certificado sin realizar ninguna (o una mínima) comprobación del	Claves de software

	solicitante.	
Media	Aprobación del administrador de certificados. Se deben definir en la directiva los tipos de comprobaciones que debe realizar el administrador de certificados antes de aprobar la solicitud de certificado.	Claves de software y claves de hardware. Si utiliza claves de software, considere la utilización de protección de alta seguridad de las claves, a menos que la aplicación no pueda utilizarla. (Por ejemplo, los certificados de equipo no pueden utilizar protección de alta seguridad de claves).
Alta	Firmas nombradas del oficial de inscripción y aprobación del administrador de certificados. Debe definir los tipos de comprobaciones que el oficial de inscripción y el administrador de certificados deben realizar antes de aprobar la solicitud.	Token de prueba contra manipulaciones de hardware. Por ejemplo, token criptográfico de tarjeta inteligente o bus serie universal (USB) para los usuarios o HSM para los equipos.

Nota: no hay ninguna razón por la que no pueda definir más o menos directivas de emisión y niveles de seguridad si resulta conveniente a la hora de cumplir los requisitos de la organización.

Definición de directivas de revocación de certificados

En algunas situaciones, puede que deba invalidar un certificado antes de que llegue el final de su vigencia. La creación de directivas para la revocación de certificados implica las tareas siguientes:

- definición de las condiciones que garantizan la revocación de un certificado.
- selección de una ubicación de publicación de la lista CRL.
- selección del tipo o tipos de listas CRL que tiene previsto utilizar.
- establecimiento de programaciones para la publicación de listas CRL.

La definición de las condiciones que garantizan la revocación del certificado formarán parte de la directiva del certificado. Puede variar según los diferentes tipos de certificados y probablemente variará para los certificados de diferentes niveles de seguridad y tipos de sujetos de diferentes entidades emisoras.

También debería documentar el uso de los códigos de razón de revocación que deben darse según sea adecuado al revocar un certificado. La tabla siguiente describe los distintos códigos de razón.

Tabla 4.16: Códigos de revocación de certificados

Código de razón	Descripción
Compromiso de clave	La clave privada del certificado ha quedado comprometida (o se sospecha que ha quedado comprometida).
Compromiso de entidad emisora	La clave privada de la entidad emisora ha quedado comprometida (o se sospecha que ha quedado comprometida).
Cambio de afiliación	El sujeto se ha pasado a una organización diferente.
Reemplazadas	Se ha emitido un nuevo certificado que ocupa el lugar de éste.

Cese de operaciones	La entidad emisora ya no está operativa.
Certificado retenido	Debe suspenderse temporalmente el uso de certificados (por ejemplo, si un usuario no encuentra su tarjeta inteligente pero no está seguro de si la ha perdido).
Sin especificar	Cualquier razón que no cubran los demás códigos.

Importante: debe evitar el uso del código de razón de retención de certificado a menos que esté estrictamente justificado. Cuando se retiene un certificado y seguidamente se libera, no es posible determinar el estado de revocación de un certificado (y, por lo tanto, la validez de cualquier firma realizada por ese certificado) en un momento determinado.

Como parte del procedimiento de revocación, debe asegurarse de que documenta las respuestas a las siguientes preguntas. Normalmente, se almacenan en un registro de administración de cambios o de incidentes:

- ¿Cuál es la razón para revocar este certificado?
- ¿Quién ha solicitado la revocación de este certificado?
- ¿Volverá a necesitar este certificado (por ejemplo, para la verificación de firmas o para descifrar mensajes)? Si es así, ¿para que será necesario (por ejemplo, para comprobar firmas, descifrar mensajes, uso normal)?
- ¿Existen requisitos especiales para la persona que revoca el certificado (por ejemplo, que sea el administrador de certificados) que deba satisfacer como administrador?
- ¿Hay algún procedimiento operativo documentado para la organización que deba seguir al revocar certificados (por ejemplo, copia de seguridad)?

También hay varios parámetros técnicos que rigen la revocación de certificados. Microsoft recomienda que se documenten también como parte de la directiva de entidad emisora. Los parámetros de las tablas siguientes son para las entidades emisoras raíz y emisora de esta solución.

Tabla 4.17: Parámetros de revocación de certificados de entidad emisora raíz

Parámetro	Valor seleccionado	Motivo
Ubicaciones de publicación de CRL (CDP)	Ruta de acceso HTTP a servidor Web interno	La publicación en un servidor Web permite la creación de una copia de seguridad en la ubicación LDAP y el acceso a la CRL de clientes no pertenecientes a LDAP.
	Ruta de acceso LDAP para el contenedor de CDP de Active Directory	La publicación en todos los controladores del dominio permite un acceso local fácil para todos los usuarios del dominio.
Tipo de CRL	Sólo la lista CRL base	Debido al pequeño número de certificados que se emiten, no hay ninguna ventaja en utilizar listas diferencias entre listas CRL.
Programa de publicación	Seis meses	Esto dificulta la revocación de certificados de la entidad emisora, por lo que requiere confianza en la seguridad de la entidad emisora. Sin embargo, este período largo mantiene al mínimo la administración de la entidad emisora raíz.
Período de coincidencia de listas CRL (intervalo entre la publicación de la lista CRL nueva publicada y la lista CRL	10 días	Permite un margen de error para recuperar la nueva lista CRL de la entidad emisora raíz.

caducada)		

Tabla 4.18: Parámetros de revocación de certificados de entidad emisora

Parámetro	Valor seleccionado	Motivo
Ubicaciones de publicación de CRL (CDP)	Ruta de acceso LDAP al contenedor de CDP de Active Directory (tanto para listas CRL base como para diferencias entre listas CRL)	La publicación en todos los controladores del dominio permite un acceso local fácil para todos los usuarios del dominio. (Consulte la nota siguiente sobre la publicación de diferencias entre listas CRL en Active Directory.)
	Ruta de acceso HTTP a servidor Web interno	La publicación en un servidor Web permite la creación de una copia de seguridad en la ubicación LDAP y el acceso a la CRL de clientes no pertenecientes a LDAP.
Tipo de CRL	Lista CRL base Diferencia entre listas CRL	Las diferencias entre listas CRL son útiles para optimizar el tráfico de recuperación de listas CRL a la vez que proporcionar un tiempo relativamente breve para la publicación de la información de revocación.
Programa de publicación	Lista CRL base: siete días	Este intervalo debe ser lo suficientemente frecuente para que los sistemas que no comprenden la diferencia entre listas CRL sigan recibiendo información de revocación relativamente reciente.
	Diferencia entre listas CRL: un día	Para clientes modernos que pueden utilizar diferencias entre listas CRL, ofrece un tiempo de revocación relativamente pequeño.
Período de coincidencia de listas CRL base (intervalo entre la publicación de la nueva lista CRL y la caducidad de la anterior)	Cuatro días	Esto permite un margen de error para la recuperación de la entidad emisora en caso de que no se pueda publicar a tiempo una lista CRL base. Se han elegido cuatro días en previsión del peor caso que se puede dar: error en la entidad emisora un viernes por la noche de un fin de semana largo (lunes fiesta) y que nadie se dé cuenta hasta el martes siguiente.
Período de coincidencia de diferencia entre listas CRL	1 día	Las diferencias entre CRL no son críticas para el servicio, por lo que no es catastrófico si se produce un error en la publicación de la diferencia entre listas CRL. Se establece para que la coincidencia sea mayor que la latencia de replicación de Active Directory.

Nota: puesto que se utilizan diferencias entre listas CRL de vigencia relativamente corta (un día), debe asegurarse de que la latencia máxima de replicación de Active Directory sea inferior al 50 por ciento del período de publicación de la diferencia entre listas CRL. De lo contrario, podría certificar clientes utilizando información de revocación obsoleta, así como posiblemente producir un efecto negativo en el tráfico de replicación de directorios para sitios con ancho de banda de red restringido. El tiempo de coincidencia de diferencia entre listas CRL debe establecerse en un valor mayor que el período de tiempo más largo que tarda la replicación de la información de directorio en el bosque.
Si la latencia de Active Directory es mayor o si no desea tráfico de replicación de directorio adicional, debe alargar el período de publicación de la diferencia entre listas CRL o evitar la publicación de diferencia entre listas CRL en el directorio. Si cambia las ubicaciones de la diferencia entre listas CRL, debe emitir una nueva lista CRL

base.
La latencia de replicación suele ser mucho menos preocupante al utilizar ubicaciones HTTP en lugar de URL de LDAP para publicar diferencias entre CRL.

Planeamiento de la recuperación de claves y datos

La recuperación de claves y datos se encuentra fuera del ámbito de esta solución. Si requiere una de las dos o ambas, debe planear y administrarlas con cuidado para evitar la pérdida de datos e impedir la divulgación inadvertida de datos cifrados.

Lea las secciones “Planning for Data Recovery and Key Recovery” y “Designing a Public Key Infrastructure”, sobre la recuperación de datos y claves y el diseño de una infraestructura de claves públicas respectivamente, incluidas en el *kit de implementación de Windows Server 2003*, y las notas del producto técnicas de Microsoft “Key Archival and Management in Windows Server 2003”, sobre la administración y archivo de claves en Windows Server 2003.

Principio de la página

Resumen

Este capítulo se ha ocupado del proceso de diseño de una PKI para una solución de WLAN segura. La PKI detallada en esta guía se ha diseñado teniendo en cuenta la posibilidad de que las organizaciones la utilicen en aplicaciones futuras. El diseño presentado en este capítulo es lo suficientemente flexible como para adaptarse a una amplia gama de requisitos futuros. Puede utilizar la información proporcionada para diseñar una PKI que sea lo suficientemente segura como para servir criterios de seguridad mucho más estrictos que los requeridos por la aplicación WLAN.

Las decisiones de diseño que se describen aquí se utilizarán en las guías de generación y operaciones para implementar la PKI. Esta información se detalla en los capítulos 7 y 11 de la guía de la solución.

En el resto de los capítulos de esta guía de planeamiento, aprenderá a diseñar los demás componentes principales de esta solución: la infraestructura de RADIUS (implementada con IAS) y la infraestructura de seguridad de WLAN.

Información adicional

Los recursos siguientes proporcionan información de referencia detallada y datos relacionados sobre muchos de los temas cubiertos en este capítulo:

- El capítulo “Designing a Public Key Infrastructure”, sobre el diseño de infraestructuras de claves públicas, incluido en el *kit de implementación de Windows Server 2003*, en http://go.microsoft.com/fwlink/?LinkId=4735.
- Para obtener una introducción a los conceptos de PKI y el uso de Servicios de Certificate Server de Windows 2000, consulte *An Introduction to the Windows 2000 Public-Key Infrastructure* en http://www.microsoft.com/technet/archive/windows2000serv/evaluate/featfunc/pkiintro.mspx.
- Para ver una descripción detallada de la funcionalidad mejorada de PKI en Windows Server 2003 y Windows XP PKI, consulte *PKI Enhancements in Windows XP Professional and Windows Server 2003*, en http://www.microsoft.com/technet/prodtechnol/winxppro/plan/pkienh.mspx
- La documentación del producto Windows 2003 Server Enterprise Edition Public Key Infrastructure explica los conceptos clave y las tareas de administración de los servicios de Certificate Server; está disponible en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/SE_PKI.mspx.
- Para obtener más información acerca de cómo escribir una declaración de prácticas de certificados, consulte RFC2527, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* en www.ietf.org/rfc/rfc2527.txt.
- Si desea consultar un ejemplo de CPS, vea la página VeriSign Certification Practice Statement (CPS) en

www.verisign.com/repository/CPS/.

- Si desea obtener detalles precisos sobre la codificación en certificados de OID de directivas y URL de CPS, vea RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, en www.ietf.org/rfc/rfc3280.txt.
- Consulte el documento técnico *Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003* sobre el planeamiento y la implementación de certificación cruzada y subordinación calificada con Windows Server 2003, en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx.
- Para ver una explicación detallada de las diferencias entre las entidades emisoras de certificados de empresa y las entidades emisoras de certificados independientes, consulte la sección sobre entidades emisoras en la documentación del producto de los servicios de Certificate Server en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_CSCAs.mspx.
- Para obtener más información acerca de la habilitación del acceso LDAP anónimo en Windows Server 2003, consulte el artículo Q326690 de Microsoft Knowledge Base, "Anonymous LDAP operations to Active Directory are disabled on Windows Server 2003 domain controllers" en http://support.microsoft.com/default.aspx?scid=326690.
- Para ver una explicación detallada acerca de la revocación de certificados, consulte *Troubleshooting Certificate Status and Revocation*, en http://www.microsoft.com/technet/prodtechnol/winxppro/support/tshtcrl.mspx. La sección sobre las extensiones de CDP es especialmente importante para algunas de las explicaciones en este capítulo.
- Para obtener más información acerca de la instalación y el uso de las páginas de inscripción Web de los servicios de Certificate Server, consulte la página Web de la documentación del producto Windows Server 2003 en http://www.microsoft.com/windowsserver2003/proddoc/default.mspx, y realice una búsqueda sobre seguridad, PKI, servicios de Certificate Server, Cómo... y configuración de entidades emisoras de certificados.
- Si desea consultar una guía detallada de las plantillas de certificado predeterminadas, consulte *Implementing and Administering Certificate Templates in Windows Server 2003* en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03crtm.mspx.
- Puede encontrar las descripciones de todas las plantillas de certificados integradas en la documentación del producto Windows Server 2003, en la sección de solución de problemas incluida en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/ctcon_tshoot.mspx.
- Si desea consultar información sobre la inscripción automática de certificados, consulte *Certificate Autoenrollment in Windows Server 2003* en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx.
- Para obtener información sobre la administración y el archivo de claves en Windows Server 2003, consulte el documento técnico *Key Archival and Management in Windows Server 2003* en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/kyacws03.mspx.
- Si desea consultar información sobre escenarios de inscripción de certificados avanzados, consulte *Advanced Certificate Enrollment and Management* en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/advcert.mspx.
- Para obtener información sobre la inscripción de certificados mediante páginas de inscripción Web, consulte *Configuring and Troubleshooting Windows 2000 and Windows Server 2003 Certificate Services Web Enrollment* en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/

technologies/security/webenroll.mspx.

- Si desea información detallada sobre la implementación de una PKI de Windows Server 2003, consulte Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx.
- Puede encontrar información adicional en la guía de implementación de Microsoft Systems Architecture 2.0, disponible para descargar desde la página Windows Server System Reference Architecture en http://www.microsoft.com/resources/documentation/msa/2/all/solution/en-us/msa20ik/vmhtm1.mspx.

Principio de la página

Administre su perfil