System i

Seguridad
Firma de objetos y verificación de firmas

Versión 6 Release 1

System i

Seguridad
Firma de objetos y verificación de firmas

Versión 6 Release 1

Nota

Antes de utilizar esta información y el producto al que hace referencia, lea la información que figura en el apartado “Avisos”, en la página 51.

Esta edición atañe a la versión 6, release 1, modificación 0 de IBM i5/OS (producto número 5761-SS1) y a todos los releases y modificaciones ulteriores hasta que se indique lo contrario en nuevas ediciones. Esta versión no funciona en todos los modelos RISC (reduced instruction set computer) ni tampoco en modelos CISC.

Contenido

Firma de objetos y verificación de firmas

Obtenga información acerca de las posibilidades de seguridad de la firma de objetos y la verificación de firmas de i5/OS que puede utilizar para asegurar la integridad de los objetos. Aprenda a utilizar uno de los diversos métodos de i5/OS para crear firmas digitales en objetos para identificar el origen del objeto y proporciona una manera de detectar los cambios realizados en el objeto. Aprenda también a mejorar la seguridad del sistema mediante la verificación de las firmas digitales de los objetos, incluidos los objetos de sistema operativo, para determinar si se han realizado cambios en el contenido del objeto desde que se firmó.

La firma de objetos y la verificación de firmas son posibilidades de seguridad que puede utilizar para verificar la integridad de una serie de objetos. Se utiliza la clave privada de un certificado digital para firmar un objeto y se utiliza el certificado (que contiene la clave pública correspondiente) para verificar la firma digital. Una firma digital asegura la integridad de hora y contenido del objeto que está firmando. La firma es una prueba de la autenticidad y de la autorización. Puede utilizarse como prueba de origen y para detectar la posible manipulación. Firmando el objeto, identificará el origen del objeto y proporcionará un manera de detectar los cambios realizados en el objeto. Al verificar la firma de un objeto puede determinar si se han realizado cambios en el contenido del objeto desde que se firmó. También puede verificar el origen de la firma para asegurar la fiabilidad del origen del objeto.

Puede implementar la firma de objetos y la verificación de firmas mediante lo siguiente:

- API para firmar objetos y para verificar las firmas de objetos de forma programática.
- Gestor de certificados digitales (DCM) para firmar objetos y para ver o verificar las firmas de objetos.
- Management Central de iSeries Navigator para firmar objetos como parte de la distribución de paquetes para que los utilicen otros sistemas.
- Mandatos CL como, por ejemplo, Comprobar integridad de objeto (CHKOBJITG) para verificar firmas.

Para aprender más sobre estos métodos de firma de objetos y cómo la firma de objetos puede mejorar su política de seguridad actual, revise estos temas:

Nota: Al utilizar los ejemplos de código, acepta los términos de "Información sobre licencia de código y exención de responsabilidad" en la página 49.

Novedades de V6R1

Aquí encontrará la información que ha cambiado en relación con el temario Firma de objetos y verificación de firmas.

Verificar la integridad de la función de comprobación de código

A partir de V6R1, puede verificar el código interno bajo licencia (LIC) utilizando la API Comprobar sistema (QydoCheckSystem) o el mandato Comprobar integridad de objeto (CHKOBJITG).

Cómo localizar lo que es nuevo o lo que ha cambiado

Para ayudarle a localizar dónde se han hecho cambios técnicos, Information Center emplea:

- La imagen » para marcar dónde empieza la información nueva o la que ha cambiado.
- La imagen « para marcar dónde termina la información nueva o la que ha cambiado.

En los archivos PDF, pueden aparecer barras de revisión (|) en el margen izquierdo de la información nueva o de la que ha cambiado.

Para hallar más información sobre las novedades o los cambios de este release, vea el Memorándum para los usuarios.

Archivo PDF de Firma de objetos y verificación de firmas

Utilice esta información para imprimir todo el tema de Firma de objetos y verificación de firmas en i5/OS como un archivo PDF.

Para ver o descargar la versión PDF de este documento, seleccione Firma de objetos y verificación de firmas (tamaño del archivo 605 KB).

Cómo guardar los archivos PDF:

Si desea guardar un archivo PDF en su estación de trabajo para verlo o imprimirlo:

1. En el navegador, pulse el enlace del PDF con el botón derecho del ratón.
2. Pulse la opción destinada a guardar el PDF localmente.
3. Navegue hasta el directorio en el que desea guardar el archivo PDF.
4. Pulse **Guardar**.

Cómo descargar Adobe Acrobat Reader

Necesitará Adobe Acrobat Reader para ver o imprimir estos archivos PDF. Puede descargar una copia del sitio Web Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Conceptos relacionados con la firma de objetos

En este tema se proporciona información conceptual y de consulta sobre las firmas digitales en i5/OS y se explica cómo funcionan los procesos de firma de objetos y verificación de firmas en i5/OS.

Antes de empezar a utilizar las prestaciones de firma de objetos y verificación de firmas, le resultará de utilidad revisar algunos de estos conceptos:

Firmas digitales

Este tema facilita información sobre qué son las firmas digitales del i5/OS y qué protección proporcionan.

El i5/OS proporcionar soporte para utilizar certificados digitales con el fin de ″firmar″ objetos digitalmente. La firma digital en un objeto se crea utilizando una forma de criptografía y es similar a una firma personal en un documento escrito. Una firma digital ofrece pruebas del origen del objeto y un método con el que verificar la integridad del objeto. El propietario de un certificado digital ″firma″ un objeto utilizando la clave privada del certificado. El destinatario del objeto utiliza la clave pública correspondiente del certificado para descifrar la firma, la cuál verifica la integridad del objeto firmado y a la vez verifica al remitente como la fuente de donde procede.

El soporte de firma de objetos incrementa las herramientas tradicionales del sistema para controlar quién puede cambiar objetos. Los controles tradicionales no pueden proteger a un objeto ante manipulaciones no autorizadas mientras el objeto está en tránsito por Internet u otra red no de confianza. Al poder detectar si el contenido de un objeto ha sido modificado desde que se firmó, podrá determinar más fácilmente si puede fiarse de los objetos que obtenga en estos casos.

Una firma digital es un resumen matemático cifrado de los datos de un objeto. La firma digital no hace que el objeto y su contenido queden cifrados y sean privados; sin embargo, el propio resumen está cifrado para impedir que se realicen en él cambios no autorizados. Quien desee asegurarse de que el objeto no ha sufrido cambios en el tránsito y que el objeto se ha originado en una fuente legítima aceptada, puede utilizar la clave pública del certificado de firma para verificar la firma digital original. Si

la firma no coincide, es posible que los datos hayan sido alterados. En ese caso, el destinatario puede evitar utilizar el objeto y puede ponerse en contacto con el firmante para obtener otra copia del objeto firmado.

La firma de un objeto representa al sistema que ha firmado el objeto, no a un usuario específico de ese sistema (aunque el usuario debe tener la autorización adecuada para utilizar el certificado para firmar objetos).

Si decide que utilizar firmas digitales se ajusta a sus necesidades y políticas de seguridad, deberá evaluar si le conviene más utilizar certificados públicos o emitir certificados locales. Si tiene intención de distribuir objetos al público general, considere la posibilidad de utilizar certificados de una Autoridad certificadora (CA) pública conocida para firmar los objetos. El uso de certificados públicos asegura que otras personan pueden verificar de forma económica y fácil las firmas que coloque en los objetos que les distribuye. No obstante, si tiene intención de distribuir objetos únicamente dentro de su organización, puede interesarle más utilizar el Gestor de certificados digitales (DCM) para operar su propia CA local para emitir certificados para firmar objetos. El uso de certificados privados de una CA local para firmar objetos resulta más económico que adquirir certificados de una CA pública conocida.

Tipos de firmas digitales

A partir de la V5R2, puede firmar objetos mandato (*CMD); también puede elegir entre dos tipos de firmas para los objetos *CMD: firmas de núcleo de objeto o firmas de objeto completo.

- **Firmas de objeto completo** Este tipo de firma incluye todos los bytes del objeto excepto unos pocos bytes no esenciales.
- **Firmas de núcleo de objeto** Este tipo de firma incluye los bytes esenciales del objeto *CMD. Sin embargo, la firma no incluye aquellos bytes que están sujetos a cambios más frecuentes. Este tipo de firma permite efectuar algunos cambios en el mandato sin invalidar la firma. Los bytes que la firma de núcleo de objeto no incluye varían según el objeto *CMD específico; las firmas de núcleo no incluyen, por ejemplo, los valores por omisión de parámetros de los objetos *CMD. Los ejemplos de cambios que no invalidarán una firma de núcleo de objeto incluyen:
  - Cambiar valores por omisión de mandatos.
  - Añadir un programa de comprobación de validez a un mandato que no tiene uno.
  - Cambiar el parámetro Dónde se permite ejecutar.
  - Cambiar el parámetro Permitir usuarios limitados.

Conceptos relacionados

"Objetos firmables"
En este tema se facilita información sobre qué objetos puede firmar y sobre las opciones de firma de objetos de tipo mandato (*CMD) del i5/OS.

Información relacionada

Gestor de certificados digitales (DCM)

Objetos firmables

En este tema se facilita información sobre qué objetos puede firmar y sobre las opciones de firma de objetos de tipo mandato (*CMD) del i5/OS.

Puede firmar digitalmente toda una serie de tipos de objetos i5/OS, independientemente del método que utilice para firmarlos. Puede firmar cualquier objeto (*STMF) que tenga almacenado en el sistema de archivos integrado del sistema, excepto los objetos que estén almacenados en una biblioteca. Si el objeto tiene un programa Java adjunto, también se firmará el programa. Puede firmar solamente estos objetos del sistema de archivos QSYS.LIB: programas (*PGM), programas de servicio (*SRVPGM), módulos (*MODULE), paquetes SQL (*SQLPKG), *FILE (solo archivo de salvar) y mandatos (*CMD).

Para firmar un objeto, este debe residir en el sistema local. Por ejemplo, si trabaja en un servidor Windows 2000 situado en un servidor xSeries Server para System i, tiene el sistema de archivos QNTC disponible en el sistema de archivos integrado. Los directorios de este sistema de archivos no se consideran locales porque contienen archivos propiedad del sistema operativo Windows 2000. Además, no puede firmar objetos vacíos ni objetos compilados para un release anterior a V5R1.

Firmas de objetos mandato (*CMD)

Al firmar objetos *CMD, puede elegir entre dos tipos de firmas digitales para aplicarlas al objeto *CMD. Puede elegir firmar el objeto completo o bien firmar solamente la parte núcleo del objeto. Cuando elige firmar el objeto completo, la firma se aplica a todos los bytes del objeto menos a unos pocos bytes no esenciales. La firma del objeto completo incluye los elementos contenidos en la firma del núcleo del objeto.

Cuando elige firmar solamente el núcleo del objeto, la firma protege los bytes esenciales mientras que no se firman los bytes que están sujetos a cambios frecuentes. Qué bytes no se firmarán depende del objeto *CMD, pero pueden incluir bytes que determinen la modalidad en la que el objeto es válido o que determinen dónde se permite al objeto ejecutarse, entre otros. Las firmas de núcleo no incluyen, por ejemplo, los valores por omisión de parámetros de los objetos *CMD. Este tipo de firma permite efectuar algunos cambios en el mandato sin invalidar la firma. Los ejemplos de cambios que no invalidarán estos tipos de firma incluyen:

- Cambiar valores por omisión de mandatos.
- Añadir un programa de comprobación de validez a un mandato que no tiene uno.
- Cambiar el parámetro Dónde se permite ejecutar.
- Cambiar el parámetro Permitir usuarios limitados.

La tabla siguiente describe exactamente qué bytes de un objeto *CMD se incluyen como parte de la firma de núcleo de objeto.

Composición de la firma de núcleo de objeto en objetos *CMD

Parte del objeto	**Relación con la firma de núcleo de objeto**
Valores por omisión de mandatos modificados por CHGCMDDFT	No forma parte de la firma de núcleo de objeto
Programa procesar el mandato y biblioteca	Siempre se incluye como parte de la firma de núcleo de objeto
Archivo fuente REXX y biblioteca	Se incluye si se especifica para el mandato en el momento de firmar, de lo contrario no forma parte de la firma de núcleo de objeto
Miembro fuente REXX	Se incluye si se especifica para el mandato en el momento de firmar, de lo contrario no forma parte de la firma de núcleo de objeto
Entorno de mandatos REXX y biblioteca	Se incluye si se especifica para el mandato en el momento de firmar, de lo contrario no forma parte de la firma de núcleo de objeto
Nombre de programa de salida REXX, biblioteca y código de salida	Se incluye si se especifica para el mandato en el momento de firmar, de lo contrario no forma parte de la firma de núcleo de objeto
Programa de comprobación de validez y biblioteca	Se incluye si se especifica para el mandato en el momento de firmar, de lo contrario no forma parte de la firma de núcleo de objeto
Modalidad en la que es válido	No forma parte de la firma de núcleo de objeto
Dónde se permite ejecutar	No forma parte de la firma de núcleo de objeto

Parte del objeto	Relación con la firma de núcleo de objeto
Permitir usuarios limitados	No forma parte de la firma de núcleo de objeto
Estantería de ayuda	Se incluye si se especifica para el mandato en el momento de firmar, de lo contrario no forma parte de la firma de núcleo de objeto
Grupo de paneles de ayuda y biblioteca	Se incluye si se especifica para el mandato en el momento de firmar, de lo contrario no forma parte de la firma de núcleo de objeto
Identificador de ayuda	Se incluye si se especifica para el mandato en el momento de firmar, de lo contrario no forma parte de la firma de núcleo de objeto
Índice de búsqueda de ayuda y biblioteca	Se incluye si se especifica para el mandato en el momento de firmar, de lo contrario no forma parte de la firma de núcleo de objeto
Biblioteca actual	Se incluye si se especifica para el mandato en el momento de firmar, de lo contrario no forma parte de la firma de núcleo de objeto
Biblioteca del producto	Se incluye si se especifica para el mandato en el momento de firmar, de lo contrario no forma parte de la firma de núcleo de objeto
Programa de alteración temporal de solicitud y biblioteca	Se incluye si se especifica para el mandato en el momento de firmar, de lo contrario no forma parte de la firma de núcleo de objeto
Texto (descripción)	No forma parte de la firma de núcleo de objeto ni de la firma del objeto completo ya que no está almacenado en el objeto
Habilitar interfaz gráfica de usuario (GUI)	No forma parte de la firma de núcleo de objeto

Conceptos relacionados

"Firmas digitales" en la página 2
Este tema facilita información sobre qué son las firmas digitales del i5/OS y qué protección proporcionan.

Proceso de firma de objetos

En este tema se proporciona información sobre cómo funciona el proceso de firmar objetos en el sistema que ejecuta el sistema operativo i5/OS y se indican qué parámetros se pueden establecer para el proceso.

Al firmar objetos puede especificar las siguientes opciones para el proceso de firma de objetos.

Proceso de error
Puede especificar qué tipo de proceso de error deberá utilizar la aplicación al crear firmas en más de un objeto. Puede especificar que la aplicación deje de firmar objetos al producirse un error o que continúe firmando los demás objetos del proceso.

Firma de objeto duplicada
Puede especificar cómo manejará la aplicación el proceso de firma cuando la aplicación firme un objeto de nuevo. Puede especificar dejar la firma original en su lugar o bien sustituirla por la nueva firma.

Objetos de subdirectorios
Puede especificar cómo manejará la aplicación el proceso de firma de objetos de subdirectorios. Puede especificar que la aplicación firme individualmente los objetos de cualquier subdirectorio o bien que la aplicación firme solamente los objetos del directorio principal, ignorando todos los subdirectorios.

Ámbito de la firma de objetos
Al firmar objetos *CMD, puede especificar si debe firmarse el objeto completo o bien firmar solamente el núcleo del objeto.

Proceso de verificación de firmas

Descubra cómo funciona el proceso de i5/OS que permite verificar la firma de un objeto y qué parámetros se pueden establecer para el proceso.

Puede especificar las siguientes opciones para el proceso de verificación de firmas.

Proceso de error
Puede especificar qué tipo de proceso de error deberá utilizar la aplicación al verificar firmas en más de un objeto. Puede especificar que la aplicación deje de verificar firmas al producirse un error o que continúe verificando las firmas de los demás objetos del proceso.

Objetos de subdirectorios
Puede especificar cómo la aplicación manejará la verificación de firmas de objetos de subdirectorios. Puede especificar que la aplicación verifique individualmente las firmas de objetos de cualquier subdirectorio o bien que la aplicación verifique solamente las firmas de los objetos del directorio principal, ignorando todos los subdirectorios.

Verificación de firmas de núcleo frente a firmas de objeto completo
Existen reglas del sistema que determinan cómo deberá manejar el sistema las firmas de núcleo y de objeto completo durante el proceso de verificación. Las reglas son las siguientes:

- Si no hay firmas en el objeto, el proceso de verificación informa de que el objeto no está firmado y continúa verificando los demás objetos del proceso.
- Si el objeto ha sido firmado por una fuente de confianza del sistema (IBM), la firma debe coincidir o de lo contrario el proceso de verificación fallará. Si la firma coincide, el proceso de verificación continúa. La firma es un resumen matemático cifrado de los datos del objeto; por consiguiente, se considera que la firma coincide si los datos del objeto durante la verificación coinciden con los datos del objeto cuando se firmó.
- Si el objeto tiene firmas de objeto completo que son de confianza (basándose en los certificados contenidos en el almacén de certificados *SIGNATUREVERIFICATION), al menos una de esas firmas debe coincidir para que el proceso de verificación no falle. Si coincide al menos una firma de objeto completo, el proceso de verificación continúa.
- Si el objeto tiene firmas de núcleo de objeto que son de confianza, al menos una de ellas debe coincidir con un certificado del almacén de certificados *SIGNATUREVERIFICATION para que no falle el proceso de verificación. Si coincide al menos una firma de núcleo de objeto, el proceso de verificación continúa.

Función de verificación de la integridad del comprobador de código

Este tema facilita información sobre cómo puede verificar la integridad de la función del comprobador de código para verificar la integridad de su sistema al ejecutar el sistema operativo i5/OS.

| En V5R2, i5/OS venía con una función de comprobación de código que le permite verificar la integridad
| de los objetos firmados de su sistema, incluido todo el código del sistema operativo que IBM suministra
| y firma para su sistema. A partir de la V5R3, puede usar la interfaz de programación de aplicaciones
| (API) de Comprobar sistema para verificar la integridad de la propia función de comprobación de código,
| así como la de los objetos clave del sistema operativo. Ahora, IBM firma el código interno bajo licencia
| (LIC) y usted puede usar la API de Comprobar sistema (QydoCheckSystem) o el mandato Comprobar
| integridad de objeto (CHKOBJITG) para verificar el LIC.

La API Comprobar sistema (QydoCheckSystem) proporciona la verificación de la integridad del sistema i5/OS. Esta API se utiliza para verificar los objetos de programa (*PGM), programa de servicio (*SRVPGM) y de mandato (*CMD) seleccionados de la biblioteca QSYS. Además, la API Comprobar

sistema prueba los mandatos Restaurar objeto (RSTOBJ), Restaurar biblioteca (RSTLIB) y Comprobar integridad de objeto (CHKOBJITG), y la API Verificar objeto. Esta prueba garantiza que estos mandatos y la API Verificar objeto informen de los errores de validación de firma cuando proceda; por ejemplo, cuando un objeto suministrado por el sistema no está firmado o contiene una firma no válida.

La API Comprobar sistema notifica mensajes de error relativos a anomalías de verificación y otros errores o anomalías de verificación en las anotaciones de trabajo. Sin embargo, también puede especificar dos métodos adicionales de informe de errores, dependiendo de cómo establezca las siguientes opciones:

- Si el valor del sistema QAUDLVL se establece en *AUDFAIL, la API Comprobar sistema genera registros de auditoría para informar de las anomalías y errores encontrados por los mandatos Restaurar objeto (RSTOBJ), Restaurar biblioteca (RSTLIB) y Comprobar integridad de objeto (CHKOBJITG).
- Si el usuario especifica que la API Comprobar sistema utiliza un archivo de resultados del sistema de archivos integrado, la API crea el archivo si no existe o efectúa adiciones en el archivo para informar de los errores o anomalías que encuentra.

Tareas relacionadas

"Verificar la integridad de la función de comprobación de código" en la página 45
Obtenga información acerca de cómo puede verificar la integridad de la función de comprobación de código utilizada para verificar la integridad del sistema i5/OS.

Casos prácticos de firma de objetos

Revise los casos prácticos que ilustran algunas situaciones típicas en las que se utilicen las prestaciones de firma de objetos y verificación de firmas en i5/OS. En cada caso práctico se proporcionan asimismo las tareas de configuración que debe realizar para implementar el caso práctico tal como se describe.

El sistema proporciona varios métodos distintos para firmar objetos y verificar las firmas de los objetos. La forma en que firme objetos y trabaje con los objetos firmados variará según las necesidades y los objetivos de seguridad de su empresa. En algunos casos, solamente será necesario verificar firmas de objetos en el sistema para asegurar que la integridad del objeto permanece intacta. En otros casos, puede elegir firmar los objetos que distribuya a otras personas. Firmar los objetos permite a otras personas identificar el origen de los objetos y comprobar la integridad de los objetos.

El método que decida utilizar dependerá de diversos factores. Los casos prácticos ofrecidos en este tema describen algunos de los objetivos más corrientes de la firma de objetos y de la verificación de firmas dentro de contextos comerciales típicos. Cada caso práctico también describe los requisitos previos y las tareas que debe llevar a cabo para implementar el caso práctico como se describe. Revise estos casos prácticos como ayuda para determinar cómo puede utilizar las posibilidades de firma de objetos de la manera que mejor se adapte a sus necesidades de seguridad y de empresa:

Caso práctico: utilizar DCM para firmar objetos y verificar firmas

Este caso práctico describe una empresa que desea firmar objetos de aplicaciones vulnerables de su servidor Web público. Desea poder determinar más fácilmente cuándo se efectúan cambios no autorizados en estos objetos. Basándose en las necesidades comerciales y los objetivos de seguridad de la empresa, este caso práctico describe cómo utilizar el Gestor de certificados digitales (DCM) como método principal para utilizar las prestaciones de firma de objetos del i5/OS.

Situación

Como administrador de MyCo, Inc. es responsable de la gestión de dos sistemas de la empresa. Uno de estos sistemas proporciona un sitio Web para la empresa. Usted utiliza el sistema de producción interno de la empresa para desarrollar el contenido de este sitio Web público y transferir los archivos y objetos de programa al servidor Web público después de probarlos.

El servidor Web público de la empresa proporciona un sitio Web de información general de la empresa. El sitio Web también proporciona diversos formularios que los clientes rellenan para registrar productos y para solicitar información sobre productos, avisos de actualización de productos, ubicaciones de distribución de productos y demás. A usted le preocupa la vulnerabilidad de los programas cgi-bin que proporcionan estos formularios; sabe que pueden ser alterados. Por consiguiente, desea poder comprobar la integridad de estos objetos de programa y detectar cuándo se han efectuado cambios no autorizados en ellos. Consecuentemente, ha decidido firmar digitalmente estos objetos para alcanzar este objetivo de seguridad.

Investigando las posibilidades de firma de objetos de i5/OS ha averiguado que existen varios métodos que puede utilizar para firmar objetos y verificar las firmas de objetos. Dado que es el responsable de la gestión de un número reducido de sistemas y no cree que vaya a tener que firmar objetos a menudo, ha decidido utilizar el Gestor de certificados digitales (DCM) para llevar a cabo estas tareas. También ha decidido crear una Autoridad certificadora (CA) local y utilizar un certificado privado para firmar objetos. Utilizar un certificado privado emitido por una CA local para la firma de objetos limita el gasto de utilizar esta tecnología de seguridad, ya que no tiene que adquirir un certificado de una CA pública conocida.

Este ejemplo sirve como introducción útil para los pasos que implica la configuración y el uso de la firma de objetos cuando desea firmar objetos en un número reducido de sistemas.

Ventajas del caso práctico

Este caso práctico tiene las siguientes ventajas:

- Firmar objetos le ofrece una manera de comprobar la integridad de los objetos vulnerables y determinar más fácilmente si los objetos han cambiado después de haber sido firmados. Esto puede reducir parte de las acciones de resolución de problemas que tenga que llevar a cabo en el futuro para descubrir problemas de las aplicaciones y otros problemas del sistema.
- Utilizar la interfaz gráfica de usuario (GUI) de DCM para firmar objetos y verificar firmas de objetos le permite a usted y a otros miembros de la empresa llevar a cabo estas tareas de forma rápida y fácil.
- Utilizar DCM para firmar objetos y verificar firmas de objetos reduce el período de tiempo que debe emplear para comprender y utilizar la firma de objetos como parte de su estrategia de seguridad.
- Utilizar un certificado emitido por una Autoridad certificadora (CA) local para firmar objetos hace que implementar la firma de objetos resulte más barato.

Objetivos

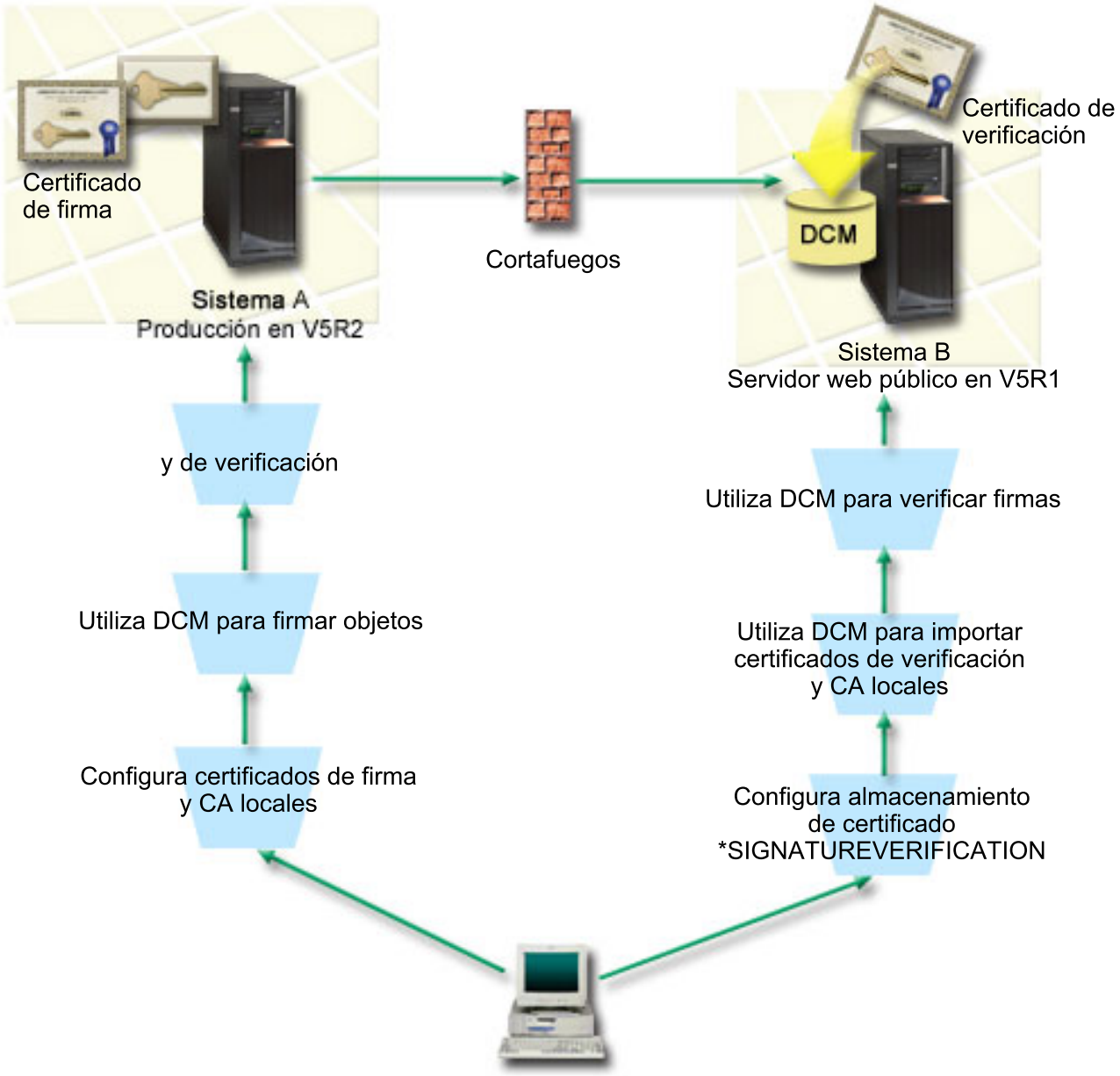
En este caso práctico desea firmar digitalmente objetos vulnerables como, por ejemplo, programas cgi-bin que generan formularios, en el servidor público de su empresa. Como administrador del sistema de MyCo, Inc, desea utilizar el Gestor de certificados digitales (DCM) para firmar estos objetos y verificar las firmas de los objetos.

Los objetivos de este caso práctico son los siguientes:

- Las aplicaciones de empresa y otros objetos vulnerables del servidor Web público (Sistema B) deben firmarse con un certificado de una CA local para limitar los costes de la firma de aplicaciones.
- Los administradores de sistemas y otros usuarios designados deben poder verificar fácilmente las firmas digitales de sistemas para verificar el origen y la autenticidad de los objetos firmados por la empresa. Para lograrlo, cada sistema debe tener una copia del certificado de verificación de firmas de la empresa y una copia del certificado de la Autoridad certificadora (CA) local en el almacén de certificados *SIGNATUREVERIFICATION de cada servidor.
- Verificando las firmas de las aplicaciones de la empresa y de otros objetos, los administradores y otras personas pueden detectar si el contenido de los objetos ha cambiado desde que se firmaron.
- El administrador del sistema debe utilizar DCM para firmar objetos; el administrador del sistema y otras personas deben poder utilizar DCM para verificar firmas de objetos.

Detalles

La siguiente figura ilustra el proceso de firma de objetos y verificación de firmas para implementar este caso práctico:



La figura ilustra los siguientes puntos relevantes de este caso práctico:

Sistema A

- El Sistema A es un modelo de System i que ejecuta OS/400 Versión 5 Release 2 (V5R2).
- El Sistema A es el sistema de producción interno de la empresa y la plataforma de desarrollo para el servidor Web de System i público (Sistema B).
- El System A tiene instalado Cryptographic Access Provider de 128 bits para System i (5722–AC3).
- El Sistema A tiene instalados y configurados el Gestor de certificados digitales (opción 34) e IBM HTTP Server (5722–DG1).

- El Sistema A actúa como Autoridad certificadora (CA) local y el certificado de firma de objetos reside en este sistema.
- El Sistema A utiliza DCM para firmar objetos y es el sistema de firma de objetos principal para las aplicaciones públicas y otros objetos de la empresa.
- El Sistema A está configurado para permitir la verificación de firmas.

Sistema B
- El Sistema B es un modelo de System i que ejecuta OS/400 Versión 5 Release 1 (V5R1).
- El Sistema B es el servidor Web público externo de la empresa fuera del cortafuegos de la empresa.
- El Sistema B tiene instalado un Cryptographic Access Provider de 128 bits (5722–AC3).
- El Sistema B tiene instalados y configurados el Gestor de certificados digitales (opción 34) e IBM HTTP Server (5722–DG1).
- El Sistema B no opera una CA local y el Sistema B no firma objetos.
- El Sistema B está configurado para permitir la verificación de firmas utilizando DCM para crear el almacén de certificados *SIGNATUREVERIFICATION e importar los certificados de verificación y de CA local necesarios.
- DCM se utiliza para verificar las firmas de objetos.

Requisitos previos y presuposiciones

Este caso práctico depende de los siguientes requisitos previos y presuposiciones:
1. Todos los sistemas cumplen los requisitos para instalar y utilizar el Gestor de certificados digitales (DCM).
2. Nadie ha configurado ni utilizado DCM anteriormente en ninguno de los sistemas.
3. Todos los sistemas tienen instalado el nivel más alto del programa bajo licencia Cryptographic Access Provider de 128 bits (5722-AC3).
4. Por omisión se establece el valor del sistema de verificar firmas de objetos durante la restauración (QVFYOBJRST) en todos los sistemas de los casos prácticos como 3 y no se ha cambiado. El valor predeterminado asegura que el sistema puede verificar firmas de objetos a medida que se restauran los objetos firmados.
5. El administrador del sistema para el Sistema A debe tener la autorización especial *ALLOBJ para firmar objetos, o bien el perfil de usuario debe tener autorización sobre la aplicación de firma de objetos.
6. El administrador del sistema u otra persona que cree un almacén de certificados en DCM debe tener las autorizaciones especiales *SECADM y *ALLOBJ.
7. El administrador del sistema u otras personas en todos los demás sistemas deben tener la autorización especial *AUDIT para verificar las firmas de objetos.

Pasos de las tareas de configuración

Existen dos conjuntos de tareas que debe completar para implementar este caso práctico. Un conjunto de tareas le permite configurar el Sistema A como Autoridad certificadora (CA) local así como firmar y verificar firmas de objetos. El segundo conjunto de tareas le permite configurar el Sistema B para verificar las firmas de objetos que crea el Sistema A.

Consulte el tema de detalles del caso práctico que se presenta más abajo para completar estos pasos.

Pasos de las tareas del Sistema A

Debe completar cada una de estas tareas en el Sistema A para crear una CA local privada y para firmar objetos y verificar la firma de objetos como describe este caso práctico:

1. Completar todos los pasos prerrequisito para instalar y configurar todos los productos System i necesarios
2. Utilizar DCM para crear una Autoridad certificadora (CA) local para emitir un certificado de firma de objetos.
3. Utilizar DCM para crear una definición de aplicación
4. Utilizar DCM para asignar un certificado a la definición de aplicación de firma de objetos
5. Utilizar DCM para firmar los objetos de programa cgi-bin
6. Utilizar DCM para exportar los certificados que otros sistemas deben utilizar para verificar firmas de objetos. Debe exportar a un archivo una copia del certificado de CA local y una copia del certificado de firma de objetos como certificado de verificación de firmas.
7. Transferir los archivos de certificado al servidor público de la empresa (Sistema B) para que tanto usted como otras personas puedan verificar las firmas creadas por el Sistema A

Pasos de las tareas del Sistema B

Si tiene previsto restaurar los objetos firmados que transfiera al servidor Web público de este caso práctico (Sistema B), deberá completar estas tareas de configuración de la verificación de firmas en el Sistema B antes de transferir los objetos firmados. La configuración de la verificación de firmas debe completarse para poder verificar firmas satisfactoriamente a medida que restaura los objetos firmados en el servidor Web público.

En el Sistema B, debe completar estas tareas para verificar las firmas de objetos como describe este caso práctico:

1. Utilizar el Gestor de certificados digitales (DCM) para crear el almacén de certificados *SIGNATUREVERIFICATION
2. Utilizar DCM para importar el certificado de CA local y el certificado de verificación de firmas
3. Utilizar DCM para verificar las firmas de los objetos transferidos

   Información relacionada

   Gestor de certificados digitales (DCM)

Detalles del caso práctico: utilizar DCM para firmar objetos y verificar firmas

Complete los pasos de las siguientes tareas para configurar y utilizar el Gestor de certificados digitales con el fin de firmar objetos de i5/OS como se describe en este caso práctico.

Paso 1: completar todos los pasos prerrequisito

Debe completar todas las tareas prerrequisito para instalar y configurar todos los productos de System i necesarios para poder realizar tareas de configuración específicas de implementación de este caso práctico.

Paso 2: crear una Autoridad certificadora local para emitir un certificado de firma de objetos privado

Al utilizar el Gestor de certificados digitales (DCM) para crear una Autoridad certificadora (CA) local, el proceso requiere que complete una serie de formularios. Estos formularios le guían por el proceso de crear una CA y completar otras tareas necesarias para empezar a utilizar certificados digitales para la Capa de Sockets Segura (SSL), la firma de objetos y la verificación de firmas. Aunque en este caso práctico no es necesario configurar certificados para SSL, debe completar todos los formularios de la tarea para configurar el sistema para firmar objetos.

Para utilizar el DCM para crear y operar una CA local, siga estos pasos. Ahora que ha creado una CA local y un certificado de firma de objetos, debe definir una aplicación de firma de objetos para utilizar el certificado y así poder firmar objetos.

1. Inicie DCM. Consulte Iniciar DCM.
2. En el marco de navegación del DCM, seleccione **Crear una Autoridad certificadora (CA)** para ver una serie de formularios.

   Nota: Si tiene preguntas sobre cómo completar un formulario específico en esta tarea guiada, seleccione el botón del signo de interrogación (**?**) en la parte superior de la página para acceder a la ayuda en línea.
3. Complete todos los formularios de esta tarea guiada. A medida que realice esta tarea, debe hacer lo siguiente:
   a. Proporcione información de identificación para la CA local.
   b. Instale el certificado de la CA local en el navegador para que el software pueda reconocer la CA local y validar los certificados que esta CA local emita.
   c. Especifique los datos de política para la CA local.
   d. Utilice la nueva CA local para emitir un certificado de servidor o cliente que sus aplicaciones puedan utilizar para las conexiones SSL.

      Nota: Aunque este caso práctico no utiliza este certificado, debe crearlo para poder utilizar la CA local para emitir el certificado de firma de objetos que necesita. Si cancela la tarea sin crear este certificado, debe crear el certificado de firma de objetos y el almacén de certificados *OBJECTSIGNING en el que se almacena por separado.
   e. Seleccione las aplicaciones que pueden utilizar el certificado de servidor o cliente para las conexiones SSL.

      Nota: En este caso práctico no seleccione ninguna aplicación y pulse en **Continuar** para visualizar el siguiente formulario.
   f. Utilice la nueva CA local para emitir un certificado de firma de objetos que las aplicaciones puedan utilizar para firmar objetos digitalmente. Esta subtarea crea el almacén de certificados *OBJECTSIGNING. Este es el almacén de certificados que se utiliza para gestionar certificados de firma de objetos.
   g. Seleccione las aplicaciones que deben confiar en la CA local.

      Nota: En este caso práctico no seleccione ninguna aplicación y pulse en **Continuar** para finalizar la tarea.

Paso 3: crear una definición de aplicación de firma de objetos

Tras crear el certificado de firma de objetos, debe utilizar el Gestor de certificados digitales (DCM) para definir una aplicación de firma de objetos que pueda utilizar para firmar objetos. No es necesario que la definición de aplicación haga referencia a una aplicación real; la definición de aplicación que cree puede describir el tipo o el grupo de objetos que tiene pensado firmar. Necesita la definición para poder tener un ID de aplicación que pueda asociar con el certificado para habilitar el proceso de firma.

Para utilizar el DCM para crear una definición de aplicación de firma de objetos, siga estos pasos:

1. En el marco de navegación, pulse en **Seleccionar un almacén de certificados** y seleccione ***OBJECTSIGNING** como el almacén de certificados a abrir.
2. Cuando aparezca la página Almacén de certificados y Contraseña, entre la contraseña que haya especificado para el almacén de certificados al crearlo y pulse en **Continuar**.
3. En el marco de navegación, seleccione **Gestionar aplicaciones** para visualizar una lista de tareas.
4. Seleccione **Añadir aplicación** en la lista de tareas para visualizar un formulario para definir la aplicación.
5. Complete el formulario y pulse en **Añadir**.

Ahora debe asignar el certificado de firma de objetos a la aplicación que ha creado.

Paso 4: asignar un certificado a la definición de aplicación de firma de objetos

Para asignar el certificado a la aplicación de firma de objetos, siga estos pasos:

1. En el marco de navegación del DCM, seleccione **Gestionar certificados** para visualizar una lista de tareas.
2. En la lista de tareas, seleccione **Asignar certificado** para visualizar una lista de certificados para el almacén de certificados actual.
3. Seleccione un certificado de la lista y pulse en **Asignar a aplicaciones** para visualizar una lista de definiciones de aplicaciones para el almacén de certificados actual.
4. Seleccione una o varias aplicaciones de la lista y pulse en **Continuar**. Aparecerá una página de mensajes para confirmar la asignación del certificado o proporcionar información de error si se ha producido un problema.

Cuando complete esta tarea estará preparado para utilizar el DCM para firmar los objetos de programa que el servidor Web público de la empresa (Sistema B) va a utilizar.

Paso 5: firmar objetos de programa

Para utilizar el DCM para firmar los objetos de programa para su uso en el servidor Web público de la empresa (Sistema B), siga estos pasos:

1. En el marco de navegación, pulse en **Seleccionar un almacén de certificados** y seleccione ***OBJECTSIGNING** como el almacén de certificados a abrir.
2. Entre la contraseña para el almacén de certificados *OBJECTSIGNING y pulse en **Continuar**.
3. Cuando el marco de navegación se haya renovado, seleccione **Gestionar objetos firmables** para visualizar una lista de tareas.
4. En la lista de tareas, seleccione **Firmar un objeto** para visualizar una lista de definiciones de aplicaciones que pueda utilizar para firmar objetos.
5. Seleccione la aplicación que ha definido en el paso anterior y pulse en **Firmar un objeto**. Aparecerá un formulario que le permitirá especificar la ubicación de los objetos que desee firmar.
6. En el campo suministrado, entre la vía de acceso y el nombre de archivo totalmente calificados del objeto o directorio de objetos que desee firmar y pulse en **Continuar**, o bien entre una ubicación de directorio y pulse en **Examinar** para ver el contenido del directorio para seleccionar los objetos a firmar.

   Nota: El nombre de objeto debe empezar con una barra inclinada, de lo contrario podría encontrar un error. También puede utilizar determinados caracteres comodín para describir la parte del directorio que desea firmar. Estos caracteres comodín son el asterisco (*), que especifica *cualquier número de caracteres* y el signo de interrogación (**?**), que especifica *un único carácter*. Por ejemplo, para firmar todos los objetos de un directorio específico, puede especificar `/mydirectory/*` ; para firmar todos los programas de una biblioteca específica, puede especificar `/QSYS.LIB/QGPL.LIB/*.PGM`. Puede utilizar estos comodines solamente en la última parte del nombre de vía de acceso; por ejemplo, `/mydirectory*/filename` da como resultado un mensaje de error. Si desea utilizar la función **Examinar** para ver una lista del contenido de bibliotecas o directorios, debe especificar el comodín como parte del nombre de vía de acceso antes de pulsar **Examinar**.
7. Seleccione las opciones de proceso que desee utilizar para firmar el objeto u objetos seleccionados y pulse en **Continuar**.

   Nota: Si elige esperar el resultado del trabajo, el archivo de resultados se visualizará directamente en el navegador. Los resultados del trabajo actual se añaden al final del archivo de resultados. Como consecuencia, el archivo puede contener resultados de trabajos anteriores, además de los

del trabajo actual. Puede utilizar el campo de fecha del archivo para determinar qué líneas del archivo corresponden al trabajo actual. El campo de fecha tiene el formato AAAAMMDD. El primer campo del archivo puede ser el ID de mensaje (si se ha producido un error durante el proceso del objeto) o el campo de fecha (indicando la fecha en la que se procesó el trabajo).

8. Especifique la vía de acceso y el nombre de archivo totalmente calificados a utilizar para almacenar los resultados del trabajo para la operación de firma de objetos y pulse en **Continuar**, o bien, entre una ubicación de directorio y pulse en **Examinar** para ver el contenido del directorio para seleccionar un archivo para almacenar los resultados del trabajo. Aparecerá un mensaje indicando que se ha sometido el trabajo para firmar objetos. Para ver los resultados del trabajo, vea el trabajo **QOBJSGNBAT** en las anotaciones de trabajo.

Para asegurar que usted u otras personas podrán verificar las firmas, debe exportar los certificados necesarios a un archivo y transferir el archivo de certificados al Sistema B. También debe completar todas las tareas de configuración de la verificación de firmas en el Sistema B antes de transferir los objetos de programa firmados al Sistema B. La configuración de la verificación de firmas debe completarse para poder verificar firmas satisfactoriamente a medida que restaura los objetos firmados en el Sistema B.

Paso 6: exportar certificados para habilitar la verificación de firmas en el Sistema B

Firmar objetos para proteger la integridad del contenido requiere que usted y otras personan tengan una manera de verificar la autenticidad de la firma. Para verificar las firmas de objetos del mismo sistema que firma los objetos (Sistema A), debe utilizar el DCM para crear el almacén de certificados *SIGNATUREVERIFICATION. Este almacén de certificados debe contener una copia del certificado de firma de objetos y una copia del certificado de CA de la CA que haya emitido el certificado de firma.

Para permitir que otras personas verifiquen la firma, debe proporcionarles una copia del certificado que ha firmado el objeto. Si utiliza una Autoridad certificadora (CA) local para emitir el certificado, también debe proporcionarles una copia del certificado de CA local.

Para utilizar el DCM para poder verificar firmas del mismo sistema que firma los objetos (Sistema A en este caso práctico), siga estos pasos:

1. En el marco de navegación, seleccione **Crear nuevo almacén de certificados** y seleccione ***SIGNATUREVERIFICATION** como el almacén de certificados a crear.
2. Seleccione **Sí** para copiar certificados de firma de objetos existentes al nuevo almacén de certificados como certificados de verificación de firmas.
3. Especifique una contraseña para el nuevo almacén de certificados y pulse en **Continuar** para crear el almacén de certificados. Ahora puede utilizar el DCM para verificar firmas de objetos del mismo sistema que utiliza para firmar objetos.

Para utilizar el DCM para exportar una copia del certificado de CA local y una copia del certificado de firma de objetos como un certificado de verificación de firmas, de forma que puede verificar firmas de objetos en otros sistemas (Sistema B), siga estos pasos:

1. En el marco de navegación, seleccione **Gestionar certificados** y, a continuación, seleccione la tarea **Exportar certificado**.
2. Seleccione **Autoridad certificadora (CA)** y pulse en **Continuar** para visualizar una lista de certificados de CA que puede exportar.
3. Seleccione en la lista el certificado de CA local que ha creado antes y pulse en **Exportar**.
4. Especifique **Archivo** como destino de exportación y pulse en **Continuar**.
5. Especifique una vía de acceso y un nombre de archivo totalmente calificados para el certificado de CA local exportado y pulse en **Continuar** para exportar el certificado.
6. Pulse en **Aceptar** para salir de la página de confirmación de exportación. Ahora puede exportar una copia del certificado de firma de objetos.
7. Vuelva a seleccionar la tarea **Exportar certificado**.

8. Seleccione **Firma de objetos** para visualizar una lista de los certificados de firma de objetos que puede exportar.
9. Seleccione el certificado de firma de objetos correspondiente en la lista y pulse en **Exportar**.
10. Seleccione **Archivo, como certificado de verificación de firmas** como destino y pulse en **Continuar**.
11. Especifique una vía de acceso y un nombre de archivo totalmente calificados para el certificado de verificación de firmas exportado y pulse en **Continuar** para exportar el certificado.

Ahora puede transferir estos archivos a los sistemas de punto final en los que tiene pensado verificar las firmas que ha creado con el certificado.

Paso 7: transferir archivos de certificado al servidor público de la empresa, Sistema B

Debe transferir los archivos de certificados que ha creado en el Sistema A al Sistema B, el servidor Web público de la empresa en este caso práctico, para poder configurarlos para verificar los objetos que firme. Puede utilizar varios métodos distintos para transferir los archivos de certificados. Por ejemplo, puede utilizar el Protocolo de transferencia de archivos (FTP) o la distribución de paquetes de Management Central para transferir los archivos.

Paso 8: tareas de verificación de firmas: crear el almacén de certificados *SIGNATUREVERIFICATION

Para verificar firmas de objetos en el Sistema B (el servidor Web público de la empresa), el Sistema B debe tener una copia del certificado de verificación de firmas correspondiente en el almacén de certificados *SIGNATUREVERIFICATION. Dado que ha utilizado un certificado emitido por una CA local para firmar los objetos, este almacén de certificados también debe contener una copia del certificado de CA local.

Para crear el almacén de certificados *SIGNATUREVERIFICATION, siga estos pasos:

1. Inicie DCM. Consulte Iniciar DCM.
2. En el marco de navegación del Gestor de certificados digitales (DCM), seleccione **Crear nuevo almacén de certificados** y seleccione ***SIGNATUREVERIFICATION** como el almacén de certificados a crear.

   Nota: Si tiene preguntas sobre cómo completar un formulario específico al utilizar el DCM, seleccione el signo de interrogación (**?**) en la parte superior de la página para acceder a la ayuda en línea.
3. Especifique una contraseña para el nuevo almacén de certificados y pulse en **Continuar** para crear el almacén de certificados. Ahora podrá importar certificados al almacén y utilizarlos para verificar firmas de objetos.

Paso 9: tareas de verificación de firmas: importar certificados

Para verificar la firma de un objeto, el almacén *SIGNATUREVERIFICATION debe contener una copia del certificado de verificación de firmas. Si el certificado es privado, este almacén de certificados también deberá tener una copia del certificado de la Autoridad certificadora (CA) local que emitió el certificado para firmas. En este caso práctico, se han exportado ambos certificados a un archivo y se ha transferido dicho archivo a cada sistema de punto final.

Para importar estos certificados al almacén *SIGNATUREVERIFICATION, siga estos pasos. Ahora puede utilizar el DCM en el Sistema B para verificar firmas de objetos que haya creado con el certificado de firmas correspondiente en el Sistema A.

1. En el marco de navegación del DCM, pulse en **Seleccionar un almacén de certificados** y seleccione ***SIGNATUREVERIFICATION** como el almacén de certificados a abrir.
2. Cuando aparezca la página Almacén de certificados y Contraseña, entre la contraseña que haya especificado para el almacén de certificados al crearlo y pulse en **Continuar**.

3. Cuando se haya renovado el marco de navegación, seleccione **Gestionar certificados** para visualizar una lista de tareas.
4. En la lista de tareas, seleccione **Importar certificado**.
5. Seleccione **Autoridad certificadora (CA)** como tipo de certificado y pulse en **Continuar**.

   Nota: Debe importar primero el certificado de CA local para poder importar un certificado de verificación de firmas privado; de lo contrario el proceso de importación del certificado de verificación de firmas resultará anómalo.
6. Especifique la vía de acceso y el nombre de archivo totalmente calificados para el archivo de certificados de CA y pulse en **Continuar**. Aparecerá un mensaje que confirmará que el proceso de importación ha sido satisfactorio o le proporcionará información de error si el proceso falla.
7. Vuelva a seleccionar la tarea **Importar certificado**.
8. Seleccione **Verificación de firmas** como el tipo de certificado a importar y pulse en **Continuar**.
9. Especifique la vía de acceso y el nombre de archivo totalmente calificados para el archivo de certificados de verificación de firmas y pulse en **Continuar**. Aparecerá un mensaje que confirmará que el proceso de importación ha sido satisfactorio o le proporcionará información de error si el proceso falla.

Paso 10: tareas de verificación de firmas: verificar firmas de objetos de programa

Para utilizar el DCM para verificar las firmas de los objetos de programas transferidos, siga estos pasos:

1. En el marco de navegación, pulse en **Seleccionar un almacén de certificados** y seleccione ***SIGNATUREVERIFICATION** como el almacén de certificados a abrir.
2. Entre la contraseña para el almacén de certificados *SIGNATUREVERIFICATION y pulse en **Continuar**.
3. Cuando el marco de navegación se haya renovado, seleccione **Gestionar objetos firmables** para visualizar una lista de tareas.
4. En la lista de tareas, seleccione **Verificar firma de objeto** para especificar la ubicación de los objetos cuyas firmas desea verificar.
5. En el campo suministrado, entre la vía de acceso y el nombre de archivo totalmente calificados del objeto o directorio de objetos cuyas firmas desee verificar y pulse en **Continuar**, o bien entre una ubicación de directorio y pulse en **Examinar** para ver el contenido del directorio para seleccionar los objetos para la verificación de firmas.

   Nota: También puede utilizar determinados caracteres comodín para describir la parte del directorio que desea verificar. Estos caracteres comodín son el asterisco (*****), que especifica *cualquier número de caracteres* y el signo de interrogación (**?**), que especifica *un único carácter*. Por ejemplo, para firmar todos los objetos de un directorio específico, puede especificar `/mydirectory/*` ; para firmar todos los programas de una biblioteca específica, puede especificar `/QSYS.LIB/QGPL.LIB/*.PGM`. Puede utilizar estos comodines solamente en la última parte del nombre de vía de acceso; por ejemplo, `/mydirectory*/filename` da como resultado un mensaje de error. Si desea utilizar la función Examinar para ver una lista del contenido de bibliotecas o directorios, debe especificar el comodín como parte del nombre de vía de acceso antes de pulsar **Examinar**.
6. Seleccione las opciones de proceso que desee utilizar para verificar la firma del objeto u objetos seleccionados y pulse en **Continuar**.

   Nota: Si elige esperar el resultado del trabajo, el archivo de resultados se visualizará directamente en el navegador. Los resultados del trabajo actual se añaden al final del archivo de resultados. Como consecuencia, el archivo puede contener resultados de trabajos anteriores, además de los del trabajo actual. Puede utilizar el campo de fecha del archivo para determinar qué líneas del archivo corresponden al trabajo actual. El campo de fecha tiene el formato AAAAMMDD. El primer campo del archivo puede ser el ID de mensaje (si se ha producido un error durante el proceso del objeto) o el campo de fecha (indicando la fecha en la que se procesó el trabajo).

7. Especifique la vía de acceso y el nombre de archivo totalmente calificados a utilizar para almacenar los resultados del trabajo para la operación de verificación de firma y pulse en **Continuar**, o bien, entre una ubicación de directorio y pulse en **Examinar** para ver el contenido del directorio para seleccionar un archivo para almacenar los resultados del trabajo. Aparecerá un mensaje indicando que se ha sometido el trabajo para verificar firmas de objetos. Para ver los resultados del trabajo, vea el trabajo **QOBJSGNBAT** en las anotaciones de trabajo.

Caso práctico: utilizar las API para firmar objetos y verificar firmas de objetos

Este caso práctico describe una empresa de desarrollo de aplicaciones que desea firmar de forma programática las aplicaciones que comercializa. Desean poder asegurar a sus clientes que las aplicaciones proceden de su empresa y proporcionarles un método para detectar cambios no autorizados en las aplicaciones al instalarlas. Basándose en las necesidades comerciales y los objetivos de seguridad de la empresa, este caso práctico describe cómo utilizar la API de i5/OS Firmar objeto y la API de i5/OS Añadir verificador para firmar objetos y habilitar la verificación de firmas.

Situación

Su empresa (MyCo, Inc.) es un business partner que desarrolla aplicaciones para clientes. Como desarrollador de software de la empresa, usted es responsable de empaquetar estas aplicaciones para la distribución a los clientes. Actualmente utiliza programas para empaquetar una aplicación. Los clientes pueden solicitar un disco compacto (CD-ROM) o pueden visitar el sitio Web y bajar la aplicación.

Está al día de las novedades del sector, especialmente las novedades de seguridad. Consecuentemente, sabe que los clientes están preocupados justificadamente por el origen y el contenido de los programas que reciben o bajan. En ocasiones los clientes piensan que están recibiendo o bajando un producto de una fuente de confianza que resulta no ser la fuente original del producto. A veces esta confusión da como resultado que algunos clientes instalen un producto distinto al que esperaban. A veces el producto instalado resulta ser un programa peligroso o ha sido manipulado y daña el sistema.

Aunque este tipo de problemas no es corriente para los clientes, le interesa asegurar a los clientes que las aplicaciones que obtienen de usted provienen realmente de su empresa. También le interesa proporcionar a los clientes un método para comprobar la integridad de esas aplicaciones para que puedan determinar si han sido alteradas antes de instalarlas.

Basándose en sus investigaciones, ha decidido que puede utilizar las posibilidades de firma de objetos de i5/OS para alcanzar sus objetivos de seguridad. Firmar digitalmente las aplicaciones permite a los clientes verificar que su empresa es la fuente legítima de la aplicación que reciben o bajan. Dado que actualmente empaqueta las aplicaciones de forma programática, ha decidido que puede utilizar API para añadir la firma de objetos fácilmente al proceso de empaquetado existente. También decide utilizar un certificado público para firmar objetos, de forma que pueda hacer que el proceso de verificación de firmas sea transparente para los clientes cuando instalen el producto.

Como parte del paquete de la aplicación incluirá una copia del certificado digital que ha utilizado para firmar el objeto. Cuando un cliente obtiene el paquete de la aplicación, el cliente puede utilizar la clave pública del certificado para verificar la firma de la aplicación. Este proceso permite al cliente identificar y verificar el origen de la aplicación, así como asegurarse de que el contenido de los objetos de la aplicación no ha sido alterado desde que se firmaron.

Este ejemplo sirve como introducción útil para los pasos que implica la firma de objetos de forma programática para las aplicaciones que desarrolle y empaquete para que otros las utilicen.

Ventajas del caso práctico

Este caso práctico tiene las siguientes ventajas:

- Utilizar API para empaquetar y firmar objetos de forma programática reduce el período de tiempo que debe emplear para implementar esta medida de seguridad.
- Utilizar API para firmar objetos a medida que los empaqueta reduce el número de pasos que debe llevar a cabo para firmar objetos porque el proceso de firma forma parte del proceso de empaquetado.
- Firmar un paquete de objetos le permite determinar más fácilmente si los objetos han cambiado después de haber sido firmados. Esto puede reducir parte de las acciones de resolución de problemas que tenga que llevar a cabo en el futuro para descubrir problemas en las aplicaciones para los clientes.
- Utilizar un certificado de una Autoridad certificadora (CA) pública conocida para firmar objetos le permite utilizar la API Añadir verificador como parte de un programa de salida en el programa de instalación del producto. Utilizar esta API le permite añadir automáticamente al sistema del cliente el certificado público que ha utilizado para firmar la aplicación. Esto asegura que la verificación de firmas es transparente para el cliente.

Objetivos

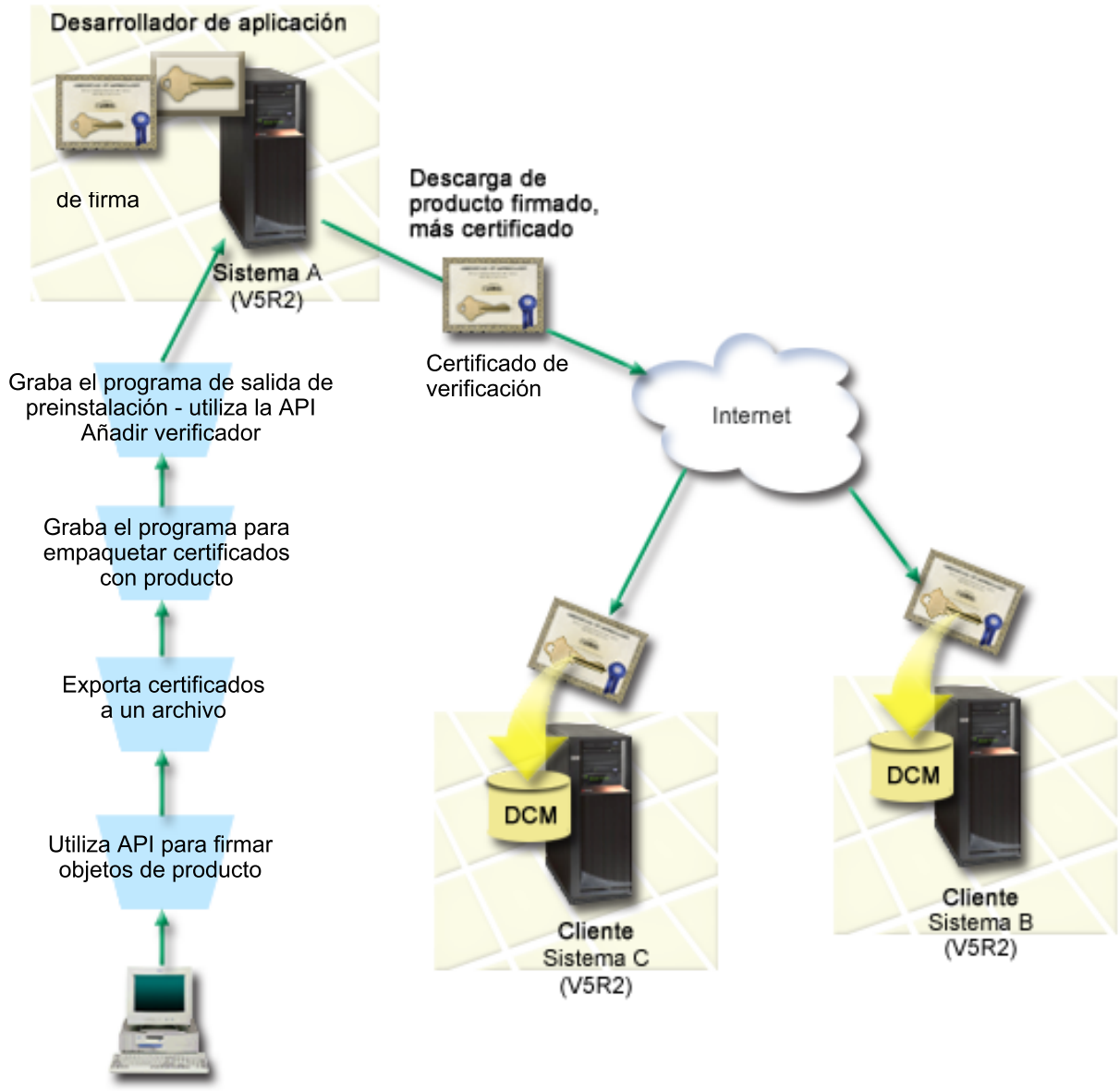
En este caso práctico, MyCo, Inc. desea firmar de forma programática las aplicaciones que empaqueta y distribuye a sus clientes. Como desarrollador de producción de aplicaciones de MyCo, Inc, actualmente empaqueta las aplicaciones de su empresa de forma programática para la distribución a clientes. Consecuentemente, le interesa utilizar las API del sistema para firmar sus aplicaciones y que el sistema del cliente verifique de forma programática la firma durante la instalación del producto.

Los objetivos de este caso práctico son los siguientes:

- El desarrollador de producción de la empresa debe poder firmar objetos utilizando la API Firmar objeto como parte de un proceso programático existente de empaquetado de aplicaciones.
- Las aplicaciones de la empresa deben firmarse con un certificado público para asegurar que el proceso de verificación de firmas es transparente para el cliente durante el proceso de instalación del producto aplicación.
- La empresa debe poder utilizar las API del sistema para añadir de forma programática el certificado de verificación de firmas necesario al almacén de certificados *SIGNATUREVERIFICATION del sistema del cliente. La empresa debe poder crear de forma programática este almacén de certificados en el sistema del cliente como parte del proceso de instalación del producto si aún no existe.
- Los clientes deben poder verificar fácilmente las firmas digitales de la aplicación de la empresa tras la instalación del producto. Los clientes deben poder verificar la firma y así poder asegurarse del origen y la autenticidad de la aplicación firmada, así como determinar si se han efectuado cambios en la aplicación desde que se firmó.

Detalles

La siguiente figura ilustra el proceso de firma de objetos y verificación de firmas para implementar este caso práctico:



La figura ilustra los siguientes puntos relevantes de este caso práctico:

Sistema central A

- El Sistema A es un modelo de System i que ejecuta OS/400 Versión 5 Release 2 (V5R2).
- El Sistema A ejecuta el programa de empaquetado de productos del desarrollador de aplicaciones.
- El System A tiene instalado Cryptographic Access Provider de 128 bits para System i (5722–AC3).
- El Sistema A tiene instalados y configurados el Gestor de certificados digitales (opción 34) e IBM HTTP Server (5722–DG1).
- El Sistema A es el sistema de firma de objetos principal para los productos aplicación de la empresa. La firma de objetos de productos para la distribución a clientes se realiza en el Sistema A mediante estas tareas:
  1. Utilizando API para firmar los productos aplicación de la empresa.
  2. Utilizando el DCM para exportar el certificado de verificación de firmas a un archivo para que los clientes puedan verificar objetos firmados.
  3. Escribiendo un programa para añadir el certificado de verificación al producto aplicación firmado.

4. Escribiendo un programa de salida de preinstalación para el producto que utiliza la API Añadir verificador. Esta API permite al proceso de instalación del producto añadir de forma programática el certificado de verificación al almacén de certificados *SIGNATUREVERIFICATION en el sistema del cliente (Sistemas B y C).

Sistemas de cliente B y C

- El Sistema B es un modelo de System i que ejecuta OS/400 Versión 5 Release 2 (V5R2) o un release ulterior de i5/OS.
- El Sistema C es un modelo de System i que ejecuta OS/400 Versión 5 Release 2 (V5R2) o un release ulterior de i5/OS.
- Los Sistemas B y C tienen instalados y configurados el Gestor de certificados digitales (opción 34) y el Servidor HTTP IBM (5722–DG1).
- Los Sistemas B y C adquieren y bajan una aplicación del sitio Web de la empresa de desarrollo de aplicaciones (propietaria del Sistema A).
- Los Sistemas B y C obtienen una copia del certificado de verificación de firmas de MyCo cuando el proceso de instalación de la aplicación de MyCo crea el almacén de certificados *SIGNATUREVERIFICATION en cada uno de estos sistemas del cliente.

Requisitos previos y presuposiciones

Este caso práctico depende de los siguientes requisitos previos y presuposiciones:

1. Todos los sistemas cumplen los requisitos para instalar y utilizar el Gestor de certificados digitales (DCM).

   Nota: El cumplimiento de los requisitos previos para instalar y utilizar el DCM es un requisito opcional para los clientes (Sistemas B y C de este caso práctico). Aunque la API Añadir verificador crea el almacén de certificados *SIGNATUREVERIFICATION como parte del proceso de instalación del producto, si es necesario, lo crea con una contraseña por omisión. Los clientes necesitan utilizar el DCM para cambiar la contraseña por omisión para proteger este almacén de certificados de posibles accesos no autorizados.
2. Nadie ha configurado ni utilizado DCM anteriormente en ninguno de los sistemas.
3. Todos los sistemas tienen instalado el nivel más alto del programa bajo licencia Cryptographic Access Provider de 128 bits (5722-AC3).
4. Por omisión se establece el valor del sistema de verificar firmas de objetos durante la restauración (QVFYOBJRST) en todos los sistemas de los casos prácticos como 3 y no se ha cambiado. El valor predeterminado asegura que el sistema puede verificar firmas de objetos a medida que se restauran los objetos firmados.
5. El administrador de la red para el Sistema A debe tener la autorización especial de perfil de usuario *ALLOBJ para firmar objetos, o bien el perfil de usuario debe tener autorización sobre la aplicación de firma de objetos.
6. El administrador del sistema u otra persona (incluso un programa) que cree un almacén de certificados en el DCM debe tener las autorizaciones especiales de perfil de usuario *SECADM y *ALLOBJ.
7. Los administradores de sistemas u otras personas en todos los demás sistemas deben tener la autorización especial de perfil de usuario *AUDIT para verificar las firmas de objetos.

Pasos de las tareas de configuración

Para firmar objetos como se describe en este caso práctico, consulte el siguiente tema de detalles del caso práctico para ver los pasos necesarios para completar cada una de las siguientes tareas en el Sistema A:

1. Completar todos los pasos prerrequisito para instalar y configurar todos los productos System i necesarios

2. Utilizar DCM para crear una petición de certificado a fin de obtener un certificado de firma de objetos de una Autoridad certificadora (CA) pública conocida
3. Utilizar DCM para crear una definición de aplicación de firma de objetos
4. Utilizar DCM para importar el certificado de firma de objetos firmados y asignarlo a la definición de aplicación de firma de objetos
5. Utilizar DCM para exportar el certificado de firma de objetos como un certificado de verificación de firmas a fin de que los clientes puedan utilizarlo para verificar la firma de los objetos de aplicación
6. Actualizar el programa de empaquetado de aplicaciones para utilizar la API Firmar objeto para firmar la aplicación
7. Crear un programa de salida de preinstalación que utilice la API Añadir verificador como parte del proceso de empaquetado de aplicaciones. Este programa de salida le permite crear el almacén de certificados *SIGNATUREVERIFICATION y añadir el certificado de verificación de firmas necesario al sistema de un cliente durante la instalación del producto.
8. Hacer que los clientes utilicen DCM para restablecer la contraseña por omisión para el almacén de certificados *SIGNATUREVERIFICATION en su sistema

Información relacionada

Gestor de certificados digitales (DCM)

Detalles del caso práctico: utilizar las API para firmar objetos y verificar firmas de objetos

Complete las siguientes tareas para utilizar las API de i5/OS para firmar objetos como describe este caso práctico.

Paso 1: completar todos los pasos prerrequisito

Debe completar todas las tareas prerrequisito para instalar y configurar todos los productos de System i necesarios para poder realizar tareas de configuración específicas de implementación de este caso práctico.

Paso 2: utilizar DCM para obtener un certificado de una CA pública conocida

En este caso práctico se presupone que no ha utilizado el Gestor de certificados digitales (DCM) anteriormente para crear y gestionar certificados. Consecuentemente, debe crear el almacén de certificados *OBJECTSIGNING como parte del proceso de creación del certificado de firma de objetos. Una vez creado, este almacén de certificados proporciona las tareas que necesita para crear y gestionar certificados de firma de objetos. Para obtener un certificado de una Autoridad certificadora (CA) pública conocida, utilizará el DCM para crear la información de identificación y el par de claves pública-privada para el certificado y someterá esta información a la CA para obtener el certificado.

Para crear la información de petición del certificado que necesita proporcionar a la CA pública conocida para poder obtener el certificado de firma de objetos, complete estos pasos:

1. Inicie DCM. Consulte Iniciar DCM.
2. En el marco de navegación del DCM, seleccione **Crear nuevo almacén de certificados** para iniciar la tarea guiada y completar una serie de formularios. Estos formularios le guían a través del proceso de crear un almacén de certificados y un certificado que pueda utilizar para firmar objetos.

   Nota: Si tiene preguntas sobre cómo completar un formulario específico en esta tarea guiada, seleccione el botón del signo de interrogación (**?**) en la parte superior de la página para acceder a la ayuda en línea.
3. Seleccione ***OBJECTSIGNING** como el almacén de certificados a crear y pulse **Continuar**.
4. Seleccione **Sí** para crear un certificado como parte de la creación del almacén de certificados *OBJECTSIGNING y pulse en **Continuar**.

5. Seleccione **VeriSign u otra Autoridad certificadora (CA) de Internet** como autoridad que firmará el nuevo certificado y pulse en **Continuar** para visualizar un formulario que le permitirá proporcionar la información de identificación para el nuevo certificado.
6. Complete el formulario y pulse en **Continuar** para visualizar una página de confirmación. Esta página de confirmación muestra los datos de petición de certificado que debe proporcionar a la Autoridad certificadora (CA) pública que va a emitir el certificado. Los datos de la Petición de firma de certificado (CSR) constan de la clave pública y otra información que haya especificado para el nuevo certificado.
7. Copie y pegue con cuidado los datos de CSR en el formulario de petición de certificado, o en un archivo aparte, que la CA pública necesita para solicitar un certificado. Debe utilizar todos los datos de CSR, incluidas las líneas de Iniciar y Finalizar petición de nuevo certificado. Al salir de esta página, se perderán los datos y no podrá recuperarlos.
8. Envíe el formulario de petición a la CA que haya elegido para emitir y firmar el certificado.
9. Espere a que la CA devuelva el certificado firmado y completado antes de continuar con el siguiente paso de la tarea en este caso práctico.

Paso 3: crear una definición de aplicación de firma de objetos

Ahora que ha enviado la petición de certificado a la CA pública conocida, puede utilizar el DCM para definir una aplicación de firma de objetos que pueda utilizar para firmar objetos. No es necesario que la definición de aplicación haga referencia a una aplicación real; la definición de aplicación que cree puede describir el tipo o el grupo de objetos que tiene pensado firmar. Necesita la definición para poder tener un ID de aplicación que pueda asociar con el certificado para habilitar el proceso de firma.

Para utilizar el DCM para crear una definición de aplicación de firma de objetos, siga estos pasos:

1. En el marco de navegación, pulse en **Seleccionar un almacén de certificados** y seleccione ***OBJECTSIGNING** como el almacén de certificados a abrir.
2. Cuando aparezca la página Almacén de certificados y Contraseña, entre la contraseña que haya especificado para el almacén de certificados al crearlo y pulse en **Continuar**.
3. En el marco de navegación, seleccione **Gestionar aplicaciones** para visualizar una lista de tareas.
4. Seleccione **Añadir aplicación** en la lista de tareas para visualizar un formulario para definir la aplicación.
5. Complete el formulario y pulse en **Añadir**.

Una vez la CA le devuelva el certificado firmado, puede asignarlo a la aplicación que ha creado.

Paso 4: importar el certificado público firmado y asignarlo a la aplicación de firma de objetos

Para importar el certificado y asignarlo a la aplicación para permitir la firma de objetos, siga estos pasos:

1. Inicie DCM. Consulte Iniciar DCM.
2. En el marco de navegación, pulse en **Seleccionar un almacén de certificados** y seleccione ***OBJECTSIGNING** como el almacén de certificados a abrir.
3. Cuando aparezca la página Almacén de certificados y Contraseña, entre la contraseña que haya especificado para el almacén de certificados al crearlo y pulse en **Continuar**.
4. Cuando se haya renovado el marco de navegación, seleccione **Gestionar certificados** para visualizar una lista de tareas.
5. En la lista de tareas, seleccione **Importar certificado** para iniciar el proceso de importar el certificado firmado al almacén de certificado.

Nota: Si tiene preguntas sobre cómo completar un formulario específico en esta tarea guiada, seleccione el botón del signo de interrogación (**?**) en la parte superior de la página para acceder a la ayuda en línea.

6. Seleccione **Asignar certificado** en la lista de tareas **Gestionar certificados** para visualizar una lista de certificados para el almacén de certificados actual.
7. Seleccione un certificado de la lista y pulse en **Asignar a aplicaciones** para visualizar una lista de definiciones de aplicaciones para el almacén de certificados actual.
8. Seleccione su aplicación en la lista y pulse en **Continuar**. Aparecerá una página con un mensaje de confirmación para la selección de asignación, o bien un mensaje de error si se ha producido un problema.

Cuando complete esta tarea, estará preparado para firmar aplicaciones y otros objetos utilizando las API de i5/OS. Sin embargo, para asegurar que usted u otras personas pueden verificar las firmas, debe exportar los certificados necesarios a un archivo y transferirlos a cualquier sistema que vaya a instalar las aplicaciones firmadas. Los sistemas de los clientes deberán poder utilizar el certificado para verificar la firma de la aplicación al instalarse. Puede utilizar la API Añadir verificador como parte del programa de instalación de la aplicación para efectuar la configuración de verificación de firmas necesaria para los clientes. Por ejemplo, puede crear un programa de salida de preinstalación que llame a la API Añadir verificador para configurar el sistema del cliente.

Paso 5: exportar certificados para habilitar la verificación de firmas en otros sistemas

Firmar objetos requiere que usted y otras personas tengan un método para verificar la autenticidad de la firma y utilizarlo para determinar si se han efectuado cambios en los objetos firmados. Para verificar las firmas de objetos del mismo sistema que firma los objetos, debe utilizar el DCM para crear el almacén de certificados *SIGNATUREVERIFICATION. Este almacén de certificados debe contener una copia del certificado de firma de objetos y una copia del certificado de CA de la CA que haya emitido el certificado de firma.

Para permitir que otras personas verifiquen la firma, debe proporcionarles una copia del certificado que ha firmado el objeto. Si utiliza una Autoridad certificadora (CA) local para emitir el certificado, también debe proporcionarles una copia del certificado de CA local.

Para utilizar el DCM para poder verificar firmas del mismo sistema que firma los objetos (Sistema A en este caso práctico), siga estos pasos:

1. En el marco de navegación, seleccione **Crear nuevo almacén de certificados** y seleccione ***SIGNATUREVERIFICATION** como el almacén de certificados a crear.
2. Seleccione **Sí** para copiar certificados de firma de objetos existentes al nuevo almacén de certificados como certificados de verificación de firmas.
3. Especifique una contraseña para el nuevo almacén de certificados y pulse en **Continuar** para crear el almacén de certificados. Ahora puede utilizar el DCM para verificar firmas de objetos del mismo sistema que utiliza para firmar objetos.

Para utilizar el DCM para exportar una copia del certificado de firma de objetos como un certificado de verificación de firmas de forma que otras personas puedan verificar las firmas de objetos, siga estos pasos:

1. En el marco de navegación, seleccione **Gestionar certificados** y, a continuación, seleccione la tarea **Exportar certificado**.
2. Seleccione **Firma de objetos** para visualizar una lista de los certificados de firma de objetos que puede exportar.
3. Seleccione el certificado de firma de objetos correspondiente en la lista y pulse en **Exportar**.
4. Seleccione **Archivo, como certificado de verificación de firmas** como destino y pulse en **Continuar**.

5. Especifique una vía de acceso y un nombre de archivo totalmente calificados para el certificado de verificación de firmas exportado y pulse en **Continuar** para exportar el certificado.

Ahora puede añadir este archivo al paquete de instalación de aplicaciones que ha creado para el producto. Utilizando la API Añadir verificador como parte del programa de instalación, puede añadir este certificado al almacén de certificados *SIGNATUREVERIFICATION del cliente. La API también creará este almacén de certificados si aún no existe. El programa de instalación del producto podrá verificar la firma de los objetos de la aplicación a medida que los restaura en los sistemas del cliente.

Paso 6: actualizar el programa de empaquetado de aplicaciones para utilizar las API del sistema para firmar la aplicación

Ahora que tiene un archivo de certificados de verificación de firmas que añadir al paquete de la aplicación, puede utilizar la API Firmar objeto para escribir o editar una aplicación existente para firmar las bibliotecas del producto a medida que las empaqueta para su distribución a los clientes.

Como ayuda para comprender mejor cómo puede utilizar la API Firmar objeto como parte del programa de empaquetado de aplicación, revise el siguiente ejemplo de código. Este fragmento de código de ejemplo, escrito en C, no es un programa de firma y empaquetado completo, sino que es más bien un ejemplo de la parte del programa que llama a la API Firmar objeto. Si elige utilizar este ejemplo de programa, modifíquelo para que se ajuste a sus necesidades específicas. Por motivos de seguridad, IBM recomienda que personalice el ejemplo de programa en vez de utilizar los valores por omisión proporcionados.

Nota: Al utilizar los ejemplos de código, acepta los términos de "Información sobre licencia de código y exención de responsabilidad" en la página 49.

Modifique este fragmento de código para que se ajuste a sus necesidades para utilizar la API Firmar objeto como parte de un programa de empaquetado para su producto aplicación. Es necesario pasar dos parámetros a este programa: el nombre de la biblioteca a firmar y el nombre del ID de aplicación de firma de objetos; el ID de aplicación es sensible a mayúsculas y minúsculas, el nombre de biblioteca no lo es. El programa que escribe puede llamar a este fragmento varias veces si se utilizan varias bibliotecas como parte del producto que va a firmar.

```
/* ------------------------------------------------------------- */
/*                                                               */
/* COPYRIGHT (C) IBM CORP. 2004, 2007                            */
/*                                                               */
/* Utilizar API Firmar objeto para firmar una o varias bibliotecas  */
/*                                                               */
/* La API firmará digitalmente todos los objetos de una biblioteca  */
/*                                                               */
/*                                                               */
/*                                                               */
/* IBM le otorga una licencia de copyright no exclusiva para usar   */
/* los ejemplos de código de programación, desde los que generar    */
/* funciones similares adaptadas a sus necesidades concretas.       */
/* IBM proporciona el código de ejemplo con fines ilustrativos      */
/* solamente. Los ejemplos no se han probado exhaustivamente        */
/* bajo todas las condiciones. Por lo tanto, IBM no puede           */
*/ garantizar ni implicar la fiabilidad, la capacidad de servicio   */
*/ ni el funcionamiento de estos programas. Todos estos programas   */
/* se le proporcionan "TAL CUAL", sin garantías de ningún tipo.     */
/* Se renuncia explícitamente a las garantías implícitas de no      */
/* infracción, comerciabilidad y adecuación para una finalidad      */
/* concreta.                                                     */
/*                                                               */
/*                                                               */
/*                                                               */
/* Los parámetros son:                                           */
/*                                                               */
```

```
/*  char *   nombre de la biblioteca a firmar                      */
/*  char *   nombre del ID de aplicación                           */
/*                                                                 */

#include <qydosgno.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int main (int argc, char *argv[])
{

    /* parámetros:

       char * biblioteca en la que firmar objetos,
       char * identificador de aplicación con el que firmar

     */

    int         lib_length, applid_length, path_length, multiobj_length;
        Qus_EC_t    error_code;
    char        libname[11];
    char        path_name[256];

    Qydo_Multi_Objects_T * multi_objects = NULL;
    multiobj_length = 0;
    error_code.Bytes_Provided = 0;    /* devolver excepciones para errores */


    /* ------------------------------------ */
    /* construir nombre vía dado nombre bibl. */
    /* ------------------------------------ */
    memset(libname, '\00', 11); /* inicializar nombre de biblioteca */
    for(lib_length = 0;
        ((*(argv[1] + lib_length) != ' ') &&
         (*(argv[1] + lib_length) != '\00'));
        lib_length++);
    memcpy(argv[1], libname, lib_length); /* rellenar nombre biblioteca */

    /* crear parámetro nombre vía para llamada API */
    sprintf(path_name, "/QSYS.LIB/%s.LIB/*", libname);
    path_length = strlen(path_name);

    /* --------------------------- */
    /* buscar longitud id aplicación */
    /* --------------------------- */
    for(applid_length = 0;
        ((*(argv[2] + applid_length) != ' ') &&
         (*(argv[2] + applid_length) != '\00'));
        applid_length++);

    /* ------------------------------- */
    /* firmar objetos de la biblioteca  */
    /* ------------------------------- */
    QYDOSGNO  (path_name,             /* nombre vía acceso a objeto  */
               &path_length,          /* longitud de nombre de vía   */
               "OBJN0100",       /* nombre de formato                */
               argv[2],               /* identificador aplicación (ID) */
               &applid_length,        /* longitud de ID aplicación   */
               "1",                   /* sustituir firma duplicada   */
               multi_objects,         /* cómo manejar múltiples
                                         objetos                    */
               &multiobj_length,      /* longitud de estructura de
                                         múltiples objetos a utilizar
                                      (0=no hay estructura múltiples objetos)*/
               &error_code);     /* código de error                  */
```

```
    return 0;

}
```

Paso 7: crear un programa de salida de preinstalación que utilice la API Añadir verificador

Ahora que tiene un proceso programático para firmar la aplicación, puede utilizar la API Añadir verificador como parte del programa de instalación para crear el producto final para su distribución. Por ejemplo, puede utilizar la API Añadir verificador como parte de un programa de salida de preinstalación para asegurar que se añade el certificado al almacén de certificados antes de restaurar los objetos de aplicación firmados. Esto permite al programa de instalación verificar la firma de los objetos de la aplicación a medida que se restauran en el sistema del cliente.

Nota: Por motivos de seguridad, esta API no le permite insertar un certificado de Autoridad certificadora (CA) en el almacén de certificados *SIGNATUREVERIFICATION. Cuando se añade un certificado CA al almacén de certificados, el sistema considera que la CA es una fuente de certificados de confianza. Consecuentemente, el sistema trata un certificado que la CA haya emitido como si se hubiera originado en una fuente de confianza. Por lo tanto, no puede utilizar la API para crear un programa de salida de instalación para insertar un certificado CA en el almacén de certificados. Debe utilizar el Gestor de certificados digitales para añadir un certificado CA al almacén de certificados para asegurar que alguien debe controlar manual y específicamente las CA de confianza del sistema. Efectuando esta operación se evita la posibilidad de que el sistema importe certificados de fuentes que un administrador no haya especificado conscientemente como de confianza.

Si desea impedir que alguien utilice esta API para añadir un certificado de verificación al almacén de certificados *SIGNATUREVERIFICATION sin su permiso, debe considerar la posibilidad de inhabilitar esta API en el sistema. Puede hacerlo utilizando las herramientas de servicio del sistema (SST) para no permitir cambios en los valores del sistema relacionados con la seguridad.

Como ayuda para comprender mejor cómo puede utilizar la API Añadir verificador como parte del programa de instalación de la aplicación, revise el siguiente ejemplo de código de programa de salida de preinstalación. Este fragmento de código de ejemplo, escrito en C, no es un programa de salida de preinstalación completo, sino que es más bien un ejemplo de la parte del programa que llama a la API Añadir verificador. Si elige utilizar este ejemplo de programa, modifíquelo para que se ajuste a sus necesidades específicas. Por motivos de seguridad, IBM recomienda que personalice el ejemplo de programa en vez de utilizar los valores por omisión proporcionados.

Nota: Al utilizar el ejemplo de código, acepta los términos de "Información sobre licencia de código y exención de responsabilidad" en la página 49.

Modifique este fragmento de código para que se ajuste a sus necesidades para utilizar la API Añadir verificador como parte de un programa de salida de preinstalación para añadir el certificado de verificación de firmas necesario al sistema del cliente al instalar el producto.

```
/* ------------------------------------------------------------ */
/*                                                              */
/* COPYRIGHT (C) IBM CORP. 2004, 2007                           */
/*                                                              */
/* Utilizar la API Añadir verificador para añadir un certificado    */
/* del archivo del sistema de archivos integrado especificado al    */
/* almacén de certificados *SIGNATUREVERIFICATION.                  */
/*                                                              */
/*                                                              */
/* La API creará el almacén de certificados si no existe. Si se     */
/* crea el almacén de certificados, se le otorgará una contraseña   */
/* predeterminada que se debe cambiar con DCM lo antes posible.     */
/* Este aviso se debe dar a los propietarios del sistema que        */
```

```
/* emplean este programa.                                            */
/*                                                                   */
/*                                                                   */
/*                                                                   */
/* IBM le otorga una licencia de copyright no exclusiva para usar    */
/* los ejemplos de código de programación, desde los que generar     */
/* funciones similares adaptadas a sus necesidades concretas.        */
/* IBM proporciona el código de ejemplo con fines ilustrativos       */
/* solamente. Los ejemplos no se han probado exhaustivamente         */
/* bajo todas las condiciones. Por lo tanto, IBM no puede            */
*/ garantizar ni implicar la fiabilidad, la capacidad de servicio    */
*/ ni el funcionamiento de estos programas. Todos estos programas    */
/* se le proporcionan "TAL CUAL", sin garantías de ningún tipo.      */
/* Se renuncia explícitamente a las garantías implícitas de no       */
/* infracción, comerciabilidad y adecuación para una finalidad       */
/* concreta.                                                         */
/*                                                                   */
/*                                                                   */
/*                                                                   */
/* Los parámetros son:                                               */
/*                                                                   */
/*  char *   nombre de vía de acceso al archivo del sistema de       */
/*           archivos integrado que contiene el certificado          */
/*  char *   etiqueta de certificado a otorgar al certificado        */
/*                                                                   */
/*                                                                   */
/*                                                                   */
/* ----------------------------------------------------------------- */

#include <qydoadd1.h>
#include <stdlib.h>
#include <string.h>

int main (int argc, char *argv[])
{

        int         pathname_length, cert_label_length;
        Qus_EC_t    error_code;
        char      * pathname = argv[1];
        char      * certlabel = argv[2];

        /* buscar longitud de nombre de vía */
        for(pathname_length = 0;
                ((*(pathname + pathname_length) != ' ') &&
                  (*(pathname + pathname_length) != '\00'));
                pathname_length++);

        /* buscar longitud de etiqueta de certificado */
        for(cert_label_length = 0;
                ((*(certlabel + cert_label_length) != ' ') &&
                  (*(certlabel + cert_label_length) != '\00'));
                cert_label_length++);


        error_code.Bytes_Provided = 0;    /* devolver excepciones para errores */

        QydoAddVerifier (pathname,         /* nombre vía a archivo con certificado*/
                                          &pathname_length, /* longitud de nombre de vía         */
                                          "OBJN0100",       /* nombre de formato                 */
                                          certlabel,        /* etiqueta de certificado           */
                                          &cert_label_length, /* longitud de etiqueta certificado */
                                          &error_code);     /* código de error                   */

        return 0;
}
```

Con estas tareas completadas, puede empaquetar la aplicación y distribuirla a sus clientes. Cuando instalen la aplicación, los objetos de aplicación firmados se verificarán como parte del proceso de instalación. Posteriormente, los clientes podrán utilizar el Gestor de certificados digitales (DCM) para verificar la firma de los objetos de aplicación. Esto permite a los clientes determinar que la fuente de la aplicación es de confianza y determinar también si se han producido cambios desde que firmó la aplicación.

Nota: El programa de instalación puede haber creado el almacén de certificados *SIGNATUREVERIFICATION con una contraseña por omisión para el cliente. Deberá advertir al cliente de que debe utilizar el DCM para restablecer la contraseña para el almacén de certificados lo antes posible para protegerlo de posibles accesos no autorizados.

Paso 8: hacer que los clientes restablezcan la contraseña por omisión para el almacén de certificados *SIGNATUREVERIFICATION

La API Añadir verificador puede haber creado el almacén de certificados *SIGNATUREVERIFICATION como parte del proceso de instalación del producto en el sistema del cliente. Si la API ha creado el almacén de certificados, también ha creado una contraseña por omisión para él. Consecuentemente, deberá aconsejar a los clientes que utilicen el DCM para restablecer esta contraseña y así proteger el almacén de certificados de posibles accesos no autorizados.

Solicite a los clientes que completen estos pasos para restablecer la contraseña del almacén de certificados *SIGNATUREVERIFICATION:

1. Inicie DCM. Consulte Iniciar DCM.
2. En el marco de navegación, pulse en **Seleccionar un almacén de certificados** y seleccione ***SIGNATUREVERIFICATION** como el almacén de certificados a abrir.
3. Cuando aparezca la página Almacén de certificados y Contraseña, pulse en **Restablecer contraseña** para visualizar la página Restablecer contraseña de almacén de certificados.

   Nota: Si tiene preguntas sobre cómo completar un formulario específico en esta tarea guiada, seleccione el botón del signo de interrogación (**?**) en la parte superior de la página para acceder a la ayuda en línea.
4. Especifique una nueva contraseña para el almacén, vuelva a entrarla para confirmarla, seleccione la política de caducidad de contraseñas para el almacén de certificados y pulse en **Continuar**.

Caso práctico: utilizar Management Central de System i Navigator para firmar objetos

Este caso práctico describe una empresa que desea utilizar las prestaciones de firma de objetos de i5/OS para firmar los objetos que empaqueta y distribuye a múltiples sistemas. Basándose en las necesidades comerciales y los objetivos de seguridad de la empresa, este caso práctico describe cómo utilizar la función Management Central de System i Navigator para empaquetar y firmar objetos que se distribuirán a otros sistemas.

Situación

Su empresa (MyCo, Inc.) desarrolla aplicaciones que luego distribuye a múltiples sistemas en múltiples ubicaciones dentro de la empresa. Como administrador de la red, debe encargarse de asegurar que estas aplicaciones están instaladas y actualizadas en todos los sistemas de la empresa. Actualmente utiliza la función Management Central de System i Navigator para que resulte más fácil empaquetar y distribuir estas aplicaciones y para realizar otras tareas administrativas de las que usted sea responsable. Sin embargo, emplea más tiempo del que desearía localizando y resolviendo problemas de estas aplicaciones debido a cambios no autorizados efectuados en los objetos. Consecuentemente, desea poder asegurar mejor la integridad de esos objetos firmándolos digitalmente.

Ha investigado las prestaciones de firma de objetos de i5/OS y ha averiguado que, a partir de la V5R2, Management Central le permite firmar objetos al empaquetarlos y distribuirlos. Utilizando Management Central puede cumplir los objetivos de seguridad de su empresa de forma eficaz y relativamente fácil. También ha decidido crear una Autoridad certificadora (CA) local y utilizarla para emitir un certificado para firmar objetos. Utilizar un certificado emitido por una CA local para la firma de objetos limita el gasto de utilizar esta tecnología de seguridad, ya que no tiene que adquirir un certificado de una CA pública conocida.

Este ejemplo sirve como introducción útil para los pasos que implica la configuración y el uso de la firma de objetos para aplicaciones que distribuirá a múltiples sistemas de la empresa.

Ventajas del caso práctico

Este caso práctico tiene las siguientes ventajas:

- Utilizar Management Central para empaquetar y firmar objetos reduce el tiempo que debe invertir para distribuir objetos firmados a los sistemas de su empresa.
- Utilizar Management Central para firmar objetos de un paquete reduce el número de pasos que debe llevar a cabo para firmar objetos porque el proceso de firma forma parte del proceso de empaquetado.
- Firmar un paquete de objetos le permite determinar más fácilmente si los objetos han cambiado después de haber sido firmados. Esto puede reducir parte de las acciones de resolución de problemas que tenga que llevar a cabo en el futuro para descubrir problemas en las aplicaciones.
- Utilizar un certificado emitido por una Autoridad certificadora (CA) local para firmar objetos hace que implementar la firma de objetos resulte más barato.

Objetivos

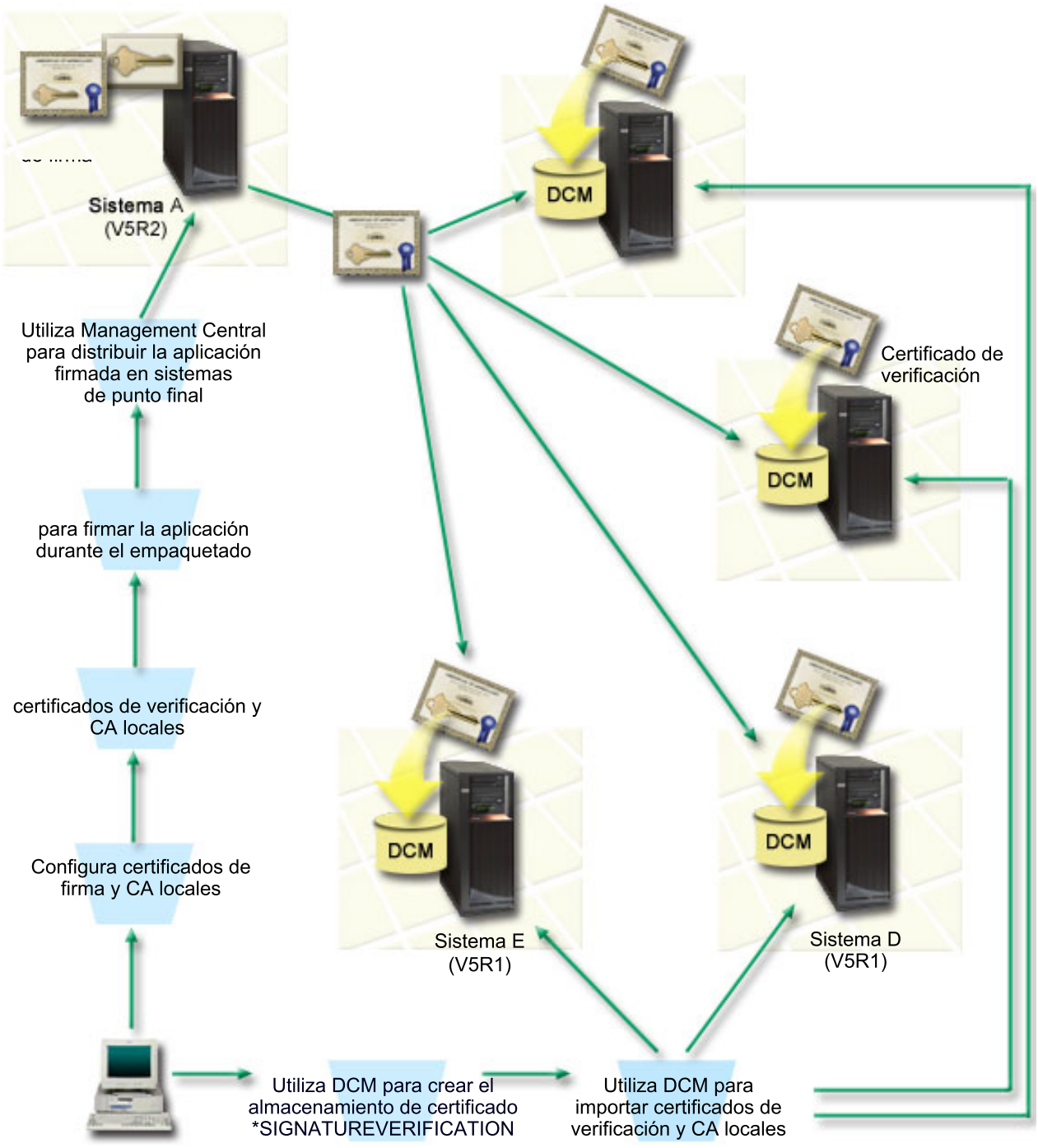
En este caso práctico, MyCo, Inc. desea firmar digitalmente aplicaciones que distribuirá a múltiples sistemas dentro de la empresa. Como administrador de la red en MyCo, Inc, ya utiliza Management Central para diversas tareas administrativas. Consecuentemente, desea ampliar el uso actual de Management Central a la firma de las aplicaciones de la empresa que se distribuyen a otros sistemas.

Los objetivos de este caso práctico son los siguientes:

- Las aplicaciones de la empresa deben firmarse con un certificado emitido por una CA local para limitar los costes de la firma de aplicaciones.
- Los administradores de sistemas y otros usuarios designados deben poder verificar fácilmente las firmas digitales de todos los sistemas para verificar el origen y la autenticidad de los objetos firmados por la empresa. Para lograrlo, cada sistema debe tener una copia del certificado de verificación de firmas de la empresa y una copia del certificado de la Autoridad certificadora (CA) local en el almacén de certificados *SIGNATUREVERIFICATION de cada sistema.
- Verificar las firmas de las aplicaciones de la empresa permite a los administradores y a otras personas detectar si el contenido de los objetos ha cambiado desde que se firmaron.
- Los administradores deben poder utilizar Management Central para empaquetar, firmar y, a continuación, distribuir sus aplicaciones a los sistemas.

Detalles

La siguiente figura ilustra el proceso de firma de objetos y verificación de firmas para implementar este caso práctico:



La figura ilustra los siguientes puntos relevantes de este caso práctico:

Sistema central (Sistema A)

- El Sistema A es un modelo de System i que ejecuta OS/400 Versión 5 Release 2 (V5R2).
- El Sistema A sirve como sistema central desde el que se ejecutan las funciones de Management Central, incluido el empaquetado y distribución de aplicaciones de la empresa.
- El System A tiene instalado Cryptographic Access Provider de 128 bits para System i (5722–AC3).
- El Sistema A tiene instalados y configurados el Gestor de certificados digitales (opción 34) e IBM HTTP Server (5722–DG1).

- El Sistema A actúa como Autoridad certificadora (CA) local y el certificado de firma de objetos reside en este sistema.
- El Sistema A es el sistema de firma de objetos principal para las aplicaciones de la empresa. La firma de objetos de productos para la distribución a clientes se realiza en el Sistema A mediante estas tareas:
  1. Utilizando el DCM para crear una CA local y utilizando la CA local para crear un certificado de firma de objetos.
  2. Utilizando el DCM para exportar una copia del certificado de la CA local y el certificado de verificación de firmas a un archivo para que los sistemas de punto final (Sistema B, C, D y E) puedan verificar objetos firmados.
  3. Utilizando Management Central para firmar objetos de aplicación y empaquetarlos con los archivos de certificados de verificación.
  4. Utilizando Management Central para distribuir aplicaciones firmadas y archivos de certificados a sistemas de punto final.

Sistemas de punto final (Sistemas B, C, D y E)

- Los Sistemas B y C son modelos de System i que ejecutan OS/400 Versión 5 Release 2 (V5R2).
- Los Sistemas D y E son modelos de System i que ejecutan OS/400 Versión 5 Release 1 (V5R1).
- Los Sistemas B, C, D y E tienen instalados y configurados el Gestor de certificados digitales (opción 34) y el Servidor HTTP IBM (5722–DG1).
- Los Sistemas B, C, D y E reciben una copia del certificado de verificación de firmas de la empresa y de la CA local desde el sistema central (Sistema A) cuando los sistemas reciben la aplicación firmada.
- El DCM se utiliza para crear el almacén de certificados *SIGNATUREVERIFICATION e importar los certificados de verificación y de CA local a este almacén de certificados.

Requisitos previos y presuposiciones

Este caso práctico depende de los siguientes requisitos previos y presuposiciones:

1. Todos los sistemas cumplen los requisitos para instalar y utilizar el Gestor de certificados digitales (DCM).
2. Nadie ha configurado ni utilizado DCM anteriormente en ninguno de los sistemas.
3. El Sistema A cumple los requisitos para instalar y utilizar System i Navigator y Management Central.
4. El servidor de Management Central debe ejecutarse en todos los sistemas de punto final.
5. Todos los sistemas tienen instalado el nivel más alto del programa bajo licencia Cryptographic Access Provider de 128 bits (5722-AC3).
6. Por omisión se establece el valor del sistema de verificar firmas de objetos durante la restauración (QVFYOBJRST) en todos los sistemas de los casos prácticos como 3 y no se ha cambiado. El valor predeterminado asegura que el sistema puede verificar firmas de objetos a medida que se restauran los objetos firmados.
7. El administrador de la red para el Sistema A debe tener la autorización especial de perfil de usuario *ALLOBJ para firmar objetos, o bien el perfil de usuario debe tener autorización sobre la aplicación de firma de objetos.
8. El administrador de la red o cualquier otra persona que cree un almacén de certificados en el DCM debe tener las autorizaciones especiales de perfil de usuario *SECADM y *ALLOBJ.
9. Los administradores de sistemas u otras personas en todos los demás sistemas deben tener la autorización especial de perfil de usuario *AUDIT para verificar las firmas de objetos.

Pasos de las tareas de configuración

Existen dos conjuntos de tareas que debe completar para implementar este caso práctico. Un conjunto de tareas le permite configurar el Sistema A para utilizar Management Central para firmar y distribuir aplicaciones. El otro conjunto de tareas permite a los administradores de sistemas y a otras personas

verificar las firmas de estas aplicaciones en todos los demás sistemas. Consulte el tema de detalles del caso práctico que aparece más abajo para completas estas tareas.

Pasos de las tareas de firma de objetos

Para firmar objetos como se describe en este caso práctico, consulte el siguiente tema de detalles del caso práctico para ver los pasos necesarios para completar cada una de las siguientes tareas en el Sistema A:

1. Completar todos los pasos prerrequisito para instalar y configurar todos los productos System i necesarios
2. Utilizar DCM para crear una Autoridad certificadora (CA) local para emitir un certificado de firma de objetos privado.
3. Utilizar DCM para crear una definición de aplicación.
4. Utilizar DCM para asignar un certificado a la definición de aplicación de firma de objetos.
5. Utilizar DCM para exportar los certificados que otros sistemas deben utilizar para verificar firmas de objetos. Debe exportar a un archivo una copia del certificado de CA local y una copia del certificado de firma de objetos como certificado de verificación de firmas.
6. Transferir los archivos de certificado a cada sistema de punto final en el que tenga intención de verificar firmas.
7. Utilizar Management Central de System i Navigator para firmar los objetos de aplicación.

Pasos de las tareas de verificación de firmas

Deberá completar estas tareas de configuración de la verificación de firmas en cada sistema de punto final antes de utilizar Management Central para transferir a ellos los objetos de aplicación firmados. La configuración de la verificación de firmas debe completarse para poder verificar firmas satisfactoriamente a medida que restaura los objetos firmados en los sistemas de punto final.

En cada sistema de punto final, debe completar estas tareas para verificar firmas de objetos como describe este caso práctico:

1. Utilizar DCM para crear el almacén de certificados *SIGNATUREVERIFICATION
2. Utilizar DCM para importar el certificado de CA local y el certificado de verificación de firmas

Información relacionada

Gestor de certificados digitales (DCM)

Detalles del caso práctico: utilizar Management Central de System i Navigator para firmar objetos

Complete los pasos de las siguientes tareas para configurar Management Central para que firme objetos de i5/OS como se describe en este caso práctico.

Paso 1: completar todos los pasos prerrequisito

Debe completar todas las tareas prerrequisito para instalar y configurar todos los productos de System i necesarios para poder realizar tareas de configuración específicas de implementación de este caso práctico.

Paso 2: crear una Autoridad certificadora local para emitir un certificado de firma de objetos privado

Al utilizar el Gestor de certificados digitales (DCM) para crear una Autoridad certificadora (CA) local, el proceso requiere que complete una serie de formularios. Estos formularios le guían por el proceso de crear una CA y completar otras tareas necesarias para empezar a utilizar certificados digitales para la

Capa de Sockets Segura (SSL), la firma de objetos y la verificación de firmas. Aunque en este caso práctico no es necesario configurar certificados para SSL, debe completar todos los formularios de la tarea para configurar el sistema para firmar objetos.

Para utilizar el DCM para crear y operar una CA local, siga estos pasos. Ahora que ha creado una CA local y un certificado de firma de objetos, debe definir una aplicación de firma de objetos para utilizar el certificado y así poder firmar objetos.

1. Inicie DCM. Consulte Iniciar DCM.
2. En el marco de navegación del DCM, seleccione **Crear una Autoridad certificadora (CA)** para ver una serie de formularios.

   Nota: Si tiene preguntas sobre cómo completar un formulario específico en esta tarea guiada, seleccione el botón del signo de interrogación (**?**) en la parte superior de la página para acceder a la ayuda en línea.
3. Complete todos los formularios de esta tarea guiada. A medida que realice esta tarea, debe hacer lo siguiente:
   a. Proporcione información de identificación para la CA local.
   b. Instale el certificado de la CA local en el navegador para que el software pueda reconocer la CA local y validar los certificados que esta CA local emita.
   c. Especifique los datos de política para la CA local.
   d. Utilice la nueva CA local para emitir un certificado de servidor o cliente que sus aplicaciones puedan utilizar para las conexiones SSL.

      Nota: Aunque este caso práctico no utiliza este certificado, debe crearlo para poder utilizar la CA local para emitir el certificado de firma de objetos que necesita. Si cancela la tarea sin crear este certificado, debe crear el certificado de firma de objetos y el almacén de certificados *OBJECTSIGNING en el que se almacena por separado.
   e. Seleccione las aplicaciones que pueden utilizar el certificado de servidor o cliente para las conexiones SSL.

      Nota: En este caso práctico no seleccione ninguna aplicación y pulse en **Continuar** para visualizar el siguiente formulario.
   f. Utilice la nueva CA local para emitir un certificado de firma de objetos que las aplicaciones puedan utilizar para firmar objetos digitalmente. Esta subtarea crea el almacén de certificados *OBJECTSIGNING. Este es el almacén de certificados que se utiliza para gestionar certificados de firma de objetos.
   g. Seleccione las aplicaciones que deben confiar en la CA local.

      Nota: En este caso práctico no seleccione ninguna aplicación y pulse en **Continuar** para finalizar la tarea.

Paso 3: crear una definición de aplicación de firma de objetos

Tras crear el certificado de firma de objetos, debe utilizar el Gestor de certificados digitales (DCM) para definir una aplicación de firma de objetos que pueda utilizar para firmar objetos. No es necesario que la definición de aplicación haga referencia a una aplicación real; la definición de aplicación que cree puede describir el tipo o el grupo de objetos que tiene pensado firmar. Necesita la definición para poder tener un ID de aplicación que pueda asociar con el certificado para habilitar el proceso de firma.

Para utilizar el DCM para crear una definición de aplicación de firma de objetos, siga estos pasos:

1. En el marco de navegación, pulse en **Seleccionar un almacén de certificados** y seleccione ***OBJECTSIGNING** como el almacén de certificados a abrir.

2. Cuando aparezca la página Almacén de certificados y Contraseña, entre la contraseña que haya especificado para el almacén de certificados al crearlo y pulse en **Continuar**.
3. En el marco de navegación, seleccione **Gestionar aplicaciones** para visualizar una lista de tareas.
4. Seleccione **Añadir aplicación** en la lista de tareas para visualizar un formulario para definir la aplicación.
5. Complete el formulario y pulse en **Añadir**.

Ahora debe asignar el certificado de firma de objetos a la aplicación que ha creado.

Paso 4: asignar un certificado a la definición de aplicación de firma de objetos

Para asignar el certificado a la aplicación de firma de objetos, siga estos pasos:

1. En el marco de navegación del DCM, seleccione **Gestionar certificados** para visualizar una lista de tareas.
2. En la lista de tareas, seleccione **Asignar certificado** para visualizar una lista de certificados para el almacén de certificados actual.
3. Seleccione un certificado de la lista y pulse en **Asignar a aplicaciones** para visualizar una lista de definiciones de aplicaciones para el almacén de certificados actual.
4. Seleccione una o varias aplicaciones de la lista y pulse en **Continuar**. Aparecerá una página de mensajes para confirmar la asignación del certificado o proporcionar información de error si se ha producido un problema.

Cuando complete esta tarea, estará preparado para firmar objetos utilizando Management Central al empaquetarlos y distribuirlos. Sin embargo, para asegurar que usted u otras personas pueden verificar las firmas, debe exportar los certificados necesarios a un archivo y transferirlos a todos los sistemas de punto final. También deberá completar todas las tareas de configuración de la verificación de firmas en cada sistema de punto final antes de utilizar Management Central para transferir a ellos los objetos de aplicación firmados. La configuración de la verificación de firmas debe completarse para poder verificar firmas satisfactoriamente a medida que restaura los objetos firmados en los sistemas de punto final.

Paso 5: exportar certificados para habilitar la verificación de firmas en otros sistemas

Firmar objetos para proteger la integridad del contenido requiere que usted y otras personan tengan una manera de verificar la autenticidad de la firma. Para verificar las firmas de objetos del mismo sistema que firma los objetos, debe utilizar el DCM para crear el almacén de certificados *SIGNATUREVERIFICATION. Este almacén de certificados debe contener una copia del certificado de firma de objetos y una copia del certificado de CA de la CA que haya emitido el certificado de firma.

Para permitir que otras personas verifiquen la firma, debe proporcionarles una copia del certificado que ha firmado el objeto. Si utiliza una Autoridad certificadora (CA) local para emitir el certificado, también debe proporcionarles una copia del certificado de CA local.

Para utilizar el DCM para poder verificar firmas del mismo sistema que firma los objetos (Sistema A en este caso práctico), siga estos pasos:

1. En el marco de navegación, seleccione **Crear nuevo almacén de certificados** y seleccione ***SIGNATUREVERIFICATION** como el almacén de certificados a crear.
2. Seleccione **Sí** para copiar certificados de firma de objetos existentes al nuevo almacén de certificados como certificados de verificación de firmas.
3. Especifique una contraseña para el nuevo almacén de certificados y pulse en **Continuar** para crear el almacén de certificados. Ahora puede utilizar el DCM para verificar firmas de objetos del mismo sistema que utiliza para firmar objetos.

Para utilizar el DCM para exportar una copia del certificado de CA local y una copia del certificado de firma de objetos como un certificado de verificación de firmas, de forma que puede verificar firmas de objetos en otros sistemas, siga estos pasos:

1. En el marco de navegación, seleccione **Gestionar certificados** y, a continuación, seleccione la tarea **Exportar certificado**.
2. Seleccione **Autoridad certificadora (CA)** y pulse en **Continuar** para visualizar una lista de certificados de CA que puede exportar.
3. Seleccione en la lista el certificado de CA local que ha creado antes y pulse en **Exportar**.
4. Especifique **Archivo** como destino de exportación y pulse en **Continuar**.
5. Especifique una vía de acceso y un nombre de archivo totalmente calificados para el certificado de CA local exportado y pulse en **Continuar** para exportar el certificado.
6. Pulse en **Aceptar** para salir de la página de confirmación de exportación. Ahora puede exportar una copia del certificado de firma de objetos.
7. Vuelva a seleccionar la tarea **Exportar certificado**.
8. Seleccione **Firma de objetos** para visualizar una lista de los certificados de firma de objetos que puede exportar.
9. Seleccione el certificado de firma de objetos correspondiente en la lista y pulse en **Exportar**.
10. Seleccione **Archivo, como certificado de verificación de firmas** como destino y pulse en **Continuar**.
11. Especifique una vía de acceso y un nombre de archivo totalmente calificados para el certificado de verificación de firmas exportado y pulse en **Continuar** para exportar el certificado.

Ahora puede transferir estos archivos a los sistemas de punto final en los que tiene pensado verificar las firmas que ha creado con el certificado.

Paso 6: transferir archivos de certificados a sistemas de punto final

Debe transferir los archivos de certificados que ha creado en el Sistema A a los sistemas de punto final de este caso práctico para poder configurarlos para verificar los objetos que firme. Puede utilizar varios métodos distintos para transferir los archivos de certificados. Por ejemplo, puede utilizar el Protocolo de transferencia de archivos (FTP) o la distribución de paquetes de Management Central para transferir los archivos.

Paso 7: firmar objetos utilizando Management Central

El proceso de firma de objetos para Management Central forma parte del proceso de distribución de paquetes de software. Debe completar todas las tareas de configuración de verificación de firmas en cada sistema de punto final para poder utilizar Management Central para transferir a ellos los objetos de aplicación firmados. La configuración de la verificación de firmas debe completarse para poder verificar firmas satisfactoriamente a medida que restaura los objetos firmados en los sistemas de punto final.

Para firmar una aplicación que vaya a distribuir a sistemas de punto final como describe este caso práctico, siga estos pasos:

1. Utilice Management Central para empaquetar y distribuir productos de software.
2. Cuando llegue al panel **Identificación** del asistente de **Definición de productos**, pulse en **Valores avanzados** para visualizar el panel **Identificación avanzada**.
3. En el campo **Firma digital**, entre el ID de aplicación de la aplicación de firma de objetos que ha creado anteriormente y pulse en **Aceptar**.
4. Complete el asistente y continúe el proceso para empaquetar y distribuir productos de software con Management Central.

Paso 8: tareas de verificación de firmas: crear el almacén de certificados *SIGNATUREVERIFICATION en los sistemas de punto final

Para verificar firmas de objetos en los sistemas de punto final de este caso práctico, cada sistema debe tener una copia del certificado de verificación de firmas correspondiente en el almacén de certificados *SIGNATUREVERIFICATION. Si se han firmado los objetos mediante un certificado privado, este almacén de certificados también debe contener una copia del certificado de CA local.

Para crear el almacén de certificados *SIGNATUREVERIFICATION, siga estos pasos:

1. Inicie DCM. Consulte Iniciar DCM.
2. En el marco de navegación del Gestor de certificados digitales (DCM), seleccione **Crear nuevo almacén de certificados** y seleccione ***SIGNATUREVERIFICATION** como el almacén de certificados a crear.

   Nota: Si tiene preguntas sobre cómo completar un formulario específico en esta tarea guiada, seleccione el botón del signo de interrogación (**?**) en la parte superior de la página para acceder a la ayuda en línea.
3. Especifique una contraseña para el nuevo almacén de certificados y pulse en **Continuar** para crear el almacén de certificados. Ahora podrá importar certificados al almacén y utilizarlos para verificar firmas de objetos.

Paso 9: tareas de verificación de firmas: importar certificados

Para verificar la firma de un objeto, el almacén *SIGNATUREVERIFICATION debe contener una copia del certificado de verificación de firmas. Si el certificado es privado, este almacén de certificados también deberá tener una copia del certificado de la Autoridad certificadora (CA) local que emitió el certificado para firmas. En este caso práctico, se han exportado ambos certificados a un archivo y se ha transferido dicho archivo a cada sistema de punto final.

Para importar estos certificados al almacén *SIGNATUREVERIFICATION, siga estos pasos. Ahora, su sistema podrá verificar las firmas de objetos que se han creado con el certificado de firma correspondiente cuando restaura los objetos firmados.

1. En el marco de navegación del DCM, pulse en **Seleccionar un almacén de certificados** y seleccione ***SIGNATUREVERIFICATION** como el almacén de certificados a abrir.
2. Cuando aparezca la página Almacén de certificados y Contraseña, entre la contraseña que haya especificado para el almacén de certificados al crearlo y pulse en **Continuar**.
3. Cuando se haya renovado el marco de navegación, seleccione **Gestionar certificados** para visualizar una lista de tareas.
4. En la lista de tareas, seleccione **Importar certificado**.
5. Seleccione **Autoridad certificadora (CA)** como tipo de certificado y pulse en **Continuar**.

   Nota: Debe importar primero el certificado de CA local para poder importar un certificado de verificación de firmas privado; de lo contrario el proceso de importación del certificado de verificación de firmas resultará anómalo.
6. Especifique la vía de acceso y el nombre de archivo totalmente calificados para el archivo de certificados de CA y pulse en **Continuar**. Aparecerá un mensaje que confirmará que el proceso de importación ha sido satisfactorio o le proporcionará información de error si el proceso falla.
7. Vuelva a seleccionar la tarea **Importar certificado**.
8. Seleccione **Verificación de firmas** como el tipo de certificado a importar y pulse en **Continuar**.
9. Especifique la vía de acceso y el nombre de archivo totalmente calificados para el archivo de certificados de verificación de firmas y pulse en **Continuar**. Aparecerá un mensaje que confirmará que el proceso de importación ha sido satisfactorio o le proporcionará información de error si el proceso falla.

Prerrequisitos de la firma de objetos y la verificación de firmas

En este tema se ofrece información sobre los prerrequisitos de configuración y se exponen otras consideraciones de planificación para firmar objetos y verificar las firmas en un sistema que ejecute el sistema operativo i5/OS.

Las prestaciones de firma de objetos y verificación de firmas de i5/OS le proporcionan potentes medios adicionales para controlar los objetos del sistema. Para aprovechar estas prestaciones, debe cumplir los prerrequisitos que permiten utilizarlas.

Prerrequisitos de la firma de objetos

Existe una serie de métodos que puede utilizar para firmar objetos, dependiendo de sus necesidades de empresa y de seguridad:

- Puede utilizar el Gestor de certificados digitales (DCM).
- Puede escribir un programa que utilice la API Firmar objeto.
- Puede utilizar la función Management Central de iSeries Navigator para firmar objetos al empaquetarlos para su distribución a sistemas de punto final.

El método que elija para firmar objetos dependerá de sus necesidades de empresa y de seguridad. Independientemente del método que piense utilizar para firmar objetos, debe asegurarse de que se cumplen ciertas condiciones prerrequisito:

- Debe cumplir los requisitos previos para instalar y utilizar el Gestor de certificados digitales (DCM).
  - Debe utilizar el DCM para crear el almacén de certificados *OBJECTSIGNING. Este almacén de certificados se crea como parte del proceso de crear una Autoridad certificadora (CA) local o como parte del proceso de gestionar certificados de firma de objetos desde una CA pública de Internet.
  - El almacén de certificados *OBJECTSIGNING debe contener al menos un certificado, ya sea uno que haya creado utilizando una CA local o uno que haya obtenido de una CA pública de Internet.
  - Debe utilizar el DCM para crear al menos una definición de aplicación de firma de objetos a utilizar para firmar objetos.
  - Debe utilizar el DCM para asignar un certificado específico a la definición de aplicación de firma de objetos.
- El perfil de usuario que firme los objetos debe tener la autorización especial *ALLOBJ. El perfil de usuario que cree el almacén de certificados *SIGNATUREVERIFICATION debe tener las autorizaciones especiales *SECADM y *ALLOBJ.

Prerrequisitos de la verificación de firmas

Existe una serie de métodos que puede utilizar para verificar firmas de objetos:

- Puede utilizar el Gestor de certificados digitales (DCM).
- Puede escribir un programa que utilice la API Verificar objeto (QYDOVFYO).
- Puede utilizar uno entre diversos mandatos, por ejemplo Comprobar integridad de objeto (CHKOBJITG).

El método que elija para verificar firmas dependerá de sus necesidades de empresa y de seguridad. Independientemente del método que piense utilizar, debe asegurarse de que se cumplen ciertas condiciones prerrequisito:

- Debe cumplir los requisitos previos para instalar y utilizar el Gestor de certificados digitales (DCM).
- Debe crear el almacén de certificados *SIGNATUREVERIFICATION. Puede crear este almacén de certificados de dos maneras distintas, dependiendo de sus necesidades. Puede crearlo utilizando el Gestor de certificados digitales (DCM) para gestionar los certificados de verificación de firmas, o bien,

si está utilizando un certificado público para firmar objetos, puede crear este almacén de certificados escribiendo un programa que utilice la API Añadir verificador (QYDOADDV).

Nota: La API Añadir verificador crea el almacén de certificados con una contraseña por omisión. Es necesario utilizar el DCM para restablecer esta contraseña por omisión a una de su elección para evitar el acceso no autorizado al almacén de certificados.

- El almacén de certificados *SIGNATUREVERIFICATION debe contener una copia del certificado que firmó los objetos. Puede añadir este certificado al almacén de certificados de dos maneras distintas. Puede utilizar el DCM en el sistema que firma para exportar el certificado a un archivo y, a continuación, utilizar el DCM en el sistema de verificación destino para importar el certificado al almacén de certificados *SIGNATUREVERIFICATION, o bien, si está utilizando un certificado público para firmar objetos, puede añadir el certificado al almacén de certificados del sistema de verificación destino escribiendo un programa que utilice la API Añadir verificador.
- El almacén de certificados *SIGNATUREVERIFICATION debe contener una copia del certificado de CA que emitió el certificado que firmó los objetos. Si está utilizando un certificado público para firmar objetos, el almacén de certificados que está en el sistema de verificación destino ya debe tener una copia del certificado de CA necesario. Sin embargo, si está utilizando un certificado emitido por una CA local para firmar objetos, debe utilizar el DCM para añadir una copia del certificado de la CA local al almacén de certificados del sistema de verificación destino.

  Nota: Por motivos de seguridad, la API Añadir verificador no le permite insertar un certificado de Autoridad certificadora (CA) en el almacén de certificados *SIGNATUREVERIFICATION. Cuando se añade un certificado CA al almacén de certificados, el sistema considera que la CA es una fuente de certificados de confianza. Consecuentemente, el sistema trata un certificado que la CA haya emitido como si se hubiera originado en una fuente de confianza. Por lo tanto, no puede utilizar la API para crear un programa de salida de instalación para insertar un certificado CA en el almacén de certificados. Debe utilizar el Gestor de certificados digitales para añadir un certificado CA al almacén de certificados para asegurar que alguien debe controlar manual y específicamente las CA de confianza del sistema. Efectuando esta operación se evita la posibilidad de que el sistema importe certificados de fuentes que un administrador no haya especificado conscientemente como de confianza.

  Si está utilizando un certificado emitido por una CA local para firmar objetos, debe utilizar el DCM en el sistema de hospedaje de la CA local para exportar una copia del certificado de la CA local a un archivo. Luego puede utilizar el DCM en el sistema de verificación destino para importar el certificado de la CA local al almacén de certificados *SIGNATUREVERIFICATION. Para evitar un posible error, debe importar el certificado de CA local al almacén de certificados antes de utilizar la API Añadir verificador para añadir el certificado de verificación de firmas. Consecuentemente, si está utilizando un certificado emitido por una CA local, resultará más fácil utilizar el DCM para importar el certificado de CA y el certificado de verificación al almacén de certificados.

  Si desea impedir que alguien utilice esta API para añadir un certificado de verificación al almacén de certificados *SIGNATUREVERIFICATION sin su permiso, debe considerar la posibilidad de inhabilitar esta API en el sistema. Puede hacerlo utilizando las herramientas de servicio del sistema (SST) para no permitir cambios en los valores del sistema relacionados con la seguridad.
- El perfil de usuario de sistema que verifica firmas debe tener la autorización especial *AUDIT. El perfil de usuario de sistema que crea el almacén de certificados *SIGNATUREVERIFICATION o cambia la contraseña del mismo debe tener las autorizaciones especiales *SECADM y *ALLOBJ.

Gestionar objetos firmados

Utilice esta información para aprender más cosas sobre los mandatos del sistema i5/OS y los valores del sistema que puede utilizar para trabajar con objetos firmados y para saber cómo afectan los objetos firmados a los procesos de copia de seguridad y recuperación.

A partir de V5R1, IBM empezó a firmar programas bajo licencia y PTF de i5/OS como una forma de marcar el sistema operativo oficialmente como procedente de IBM y como un método para detectar si se producen cambios no autorizados en los objetos del sistema. Además, los business partners y otros proveedores pueden estar firmando las aplicaciones que adquiera. Consecuentemente, aunque no firme objetos personalmente, deberá aprender a trabajar con objetos firmados y comprender cómo estos objetos firmados afectan a las tareas administrativas corrientes del sistema.

Los objetos firmados afectan principalmente a las tareas de copia de seguridad y recuperación, específicamente a cómo salvar objetos y restaurar objetos en el sistema.

Valores del sistema y mandatos que afectan a los objetos firmados

En este tema se facilita información sobre los valores del sistema y los mandatos de i5/OS que se pueden usar para gestionar los objetos firmados o que pueden afectar a los objetos firmados cuando se ejecutan.

Para gestionar objetos firmados de forma eficaz, es necesario comprender cómo los valores del sistema y los mandatos afectan a los objetos firmados. El valor del sistema **Verificar firmas de objeto durante la restauración** (QVFYOBJRST) determina cómo determinados mandatos de restaurar afectan a objetos firmados y cómo el sistema maneja los objetos firmados durante las operaciones de restauración. No hay mandatos CL que estén diseñados exclusivamente para trabajar con objetos firmados en un sistema. Sin embargo, existe una serie de mandatos CL comunes que se utilizan para gestionar objetos firmados (o para gestionar los objetos de la infraestructura que hacen posible la firma de objetos). Otros mandatos pueden afectar negativamente a los objetos firmados del sistema eliminando la firma de los objetos y, por consiguiente, eliminando la protección que la firma proporciona.

Valores del sistema que afectan a objetos firmados

El valor del sistema **Verificar firmas de objeto durante la restauración** (QVFYOBJRST), un miembro de la categoría de restauración de los valores del sistema i5/OS, determina cómo los mandatos afectan a los objetos firmados del sistema. Este valor del sistema, disponible a través de iSeries Navigator, controla cómo el sistema maneja la verificación de firmas durante las operaciones de restauración. El valor que defina para este valor del sistema, en conjunción con la definición de otros dos valores del sistema, afectará a las operaciones de restauración del sistema. Dependiendo de cómo defina este valor, puede permitirse o no que los objetos se restauren según el estado de las firmas. (Por ejemplo, si el objeto no está firmado, si tiene una firma no válida, si está firmado por una fuente de confianza y demás.) El valor por omisión para este valor del sistema permite que se restauren objetos no firmados, pero asegura que los objetos firmados puedan restaurarse solamente si tienen una firma válida. El sistema define un objeto como firmado solamente si el objeto tiene una firma en la que el sistema confíe; el sistema ignora otras firmas ″no de confianza″ en el objeto y lo trata como si no estuviera firmado.

Hay diversos valores que puede utilizar para el valor del sistema QVFYOBJRST, que van desde ignorar todas las firmas a requerir firmas válidas para todos los objetos que el sistema restaura. Este valor del sistema solamente afecta a los objetos ejecutables que se están restaurando, por ejemplo programas (*PGM), mandatos (*CMD), programas de servicio (*SRVPGM), paquetes SQL (*SQLPKG) y módulos (*MODULE). También es aplicable a objetos archivo continuo (*STMF) que tengan programas Java asociados creados por el mandato Crear programa Java (CRTJVAPGM). No es aplicable a los archivos de salvar (*SAV) ni a los archivos del sistema de archivos integrado.

Mandatos CL que afectan a objetos firmados

Existen diversos mandatos CL que le permiten trabajar con objetos firmados o que afectan a los objetos firmados en el sistema. Puede utilizar diversos mandatos para ver información de firmas de los objetos, verificar las firmas de objetos y salvar y restaurar objetos de seguridad necesarios para verificar firmas. Adicionalmente, hay un grupo de mandatos que, al ejecutarlos, pueden eliminar la firma de objetos y así negar la seguridad que proporciona la firma.

Mandatos para ver información de firmas para un objeto

- El mandato Visualizar descripción de objeto (DSPOBJD). Este mandato muestra los nombres y los atributos de objetos especificados en la biblioteca especificada o en las bibliotecas de la lista de bibliotecas de la hebra. Puede utilizar este mandato para determinar si un objeto está firmado y para ver información sobre la firma.
- Mandatos del sistema de archivos integrado Visualizar enlaces de objeto (DSPLNK) y Trabajar con enlaces de objeto (WRKLNK). Puede utilizar cualquiera de estos dos mandatos para visualizar información de firma para un objeto del sistema de archivos integrado.

Mandatos para verificar firmas de objeto

- Mandato Comprobar integridad de objeto (CHKOBJITG). Este mandato le permite determinar si hay objetos en el sistema que hayan sufrido violaciones de la integridad. Puede utilizar este mandato para verificar firmas de la misma manera que utiliza un buscador de virus para determinar si un virus ha afectado a archivos u otros objetos del sistema. Para conocer más detalles sobre el uso de este mandato con objetos firmados y firmables, consulte Mandatos de comprobador de código para asegurar la integridad de las firmas.
- Mandato Comprobar opción de producto (CHKPRDOPT). Este mandato informa de las diferencias entre la estructura correcta y la estructura real de un producto de software. Por ejemplo, el mandato informa de un error si se suprime un objeto de un producto instalado. Puede utilizar el parámetro CHKSIG para especificar cómo el mandato debe manejar e informar de posibles problemas de firmas para el producto. Para conocer más detalles sobre el uso de este mandato con objetos firmados y firmables, consulte Mandatos de comprobador de código para asegurar la integridad de las firmas.
- Mandato Salvar programa bajo licencia (SAVLICPGM). Este mandato guarda una copia de los objetos que forman un programa bajo licencia. Salva el programa bajo licencia en un formato que puede restaurarse mediante el mandato Restaurar programa bajo licencia (RSTLICPGM). Puede utilizar el parámetro CHKSIG para especificar cómo el mandato debe manejar e informar de posibles problemas de firmas para el producto. Para conocer más detalles sobre el uso de este mandato con objetos firmados y firmables, consulte Mandatos de comprobador de código para asegurar la integridad de las firmas.
- Mandato Restaurar (RST). Este mandato restaura una copia de uno o varios objetos que pueden utilizarse en el sistema de archivos integrado. Este mandato también le permite restaurar almacenes de certificados y su contenido al sistema. Sin embargo, no puede utilizar este mandato para restaurar el almacén de certificados *SIGNATUREVERIFICATION. La manera en que el mandato de restaurar manejará los objetos firmados y firmables estará determinada por cómo se defina el valor del sistema Verificar firmas de objeto durante la restauración (QVFYOBJRST).
- Mandato Restaurar biblioteca (RSTLIB). Este mandato restaura una biblioteca o un grupo de bibliotecas que se haya salvado mediante el mandato Salvar biblioteca (SAVLIB). El mandato RSTLIB restaura toda la biblioteca, que incluye la descripción de biblioteca, descripciones de objetos y el contenido de los objetos de la biblioteca. La manera en que el mandato manejará los objetos firmados y firmables estará determinada por cómo se defina el valor del sistema Verificar firmas de objeto durante la restauración (QVFYOBJRST).
- Mandato Restaurar programa bajo licencia (RSTLICPGM). Este mandato carga o restaura un programa bajo licencia, ya sea para la instalación inicial o la instalación de un nuevo release. La manera en que el mandato manejará los objetos firmados y firmables estará determinada por cómo se defina el valor del sistema Verificar firmas de objeto durante la restauración (QVFYOBJRST).

- Mandato Restaurar objeto (RSTOBJ). Este mandato restaura uno o varios objetos de una sola biblioteca que se guardaron en disquete, cinta, volumen óptico o en un archivo de salvar utilizando un único mandato. La manera en que el mandato manejará los objetos firmados y firmables estará determinada por cómo se defina el valor del sistema Verificar firmas de objeto durante la restauración (QVFYOBJRST).

Mandatos para salvar y restaurar almacenes de certificados

- Mandato Salvar (SAV). Este mandato le permite salvar una copia de uno o varios objetos que pueden utilizarse en el sistema de archivos integrado, incluidos los almacenes de certificados. Sin embargo, no puede utilizar este mandato para salvar el almacén de certificados *SIGNATUREVERIFICATION.
- Mandato Salvar datos de seguridad (SAVSECDTA). Este mandato le permite salvar toda la información de seguridad sin necesidad de tener el sistema en estado restringido. Utilizar este mandato le permite salvar el almacén de certificados *SIGNATUREVERIFICATION y los certificados que contenga. Este mandato no salva ningún otro almacén de certificados.
- Mandato Salvar sistema (SAVSYS). Este mandato le permite salvar una copia del código interno bajo licencia y la biblioteca QSYS en un formato compatible con la instalación del sistema. No salva objetos de ninguna otra biblioteca. Además, le permite salvar los objetos de seguridad y de configuración que también puede salvar utilizando los mandatos SAVSECDTA y SAVCFG. Utilizar este mandato le permite salvar el almacén de certificados *SIGNATUREVERIFICATION y los certificados que contenga.
- Mandato Restaurar (RST). Este mandato le permite restaurar almacenes de certificados y su contenido al sistema. Sin embargo, no puede utilizar este mandato para restaurar el almacén de certificados *SIGNATUREVERIFICATION.
- Mandatos Restaurar perfiles de usuario (RSTUSRPRF). Este mandato le permite restaurar los componentes básicos de un perfil de usuario o de un conjunto de perfiles de usuario salvados mediante los mandatos Salvar sistema (SAVSYS) o Salvar datos de seguridad (SAVSECDTA). Puede utilizar este mandato para restaurar el almacén de certificados *SIGNATUREVERIFICATION y las contraseñas guardadas para este y para todos los demás almacenes de certificados. Puede restaurar el almacén de certificados *SIGNATUREVERIFICATION sin restaurar información del perfil de usuario especificando *DCM como el valor para el parámetro SECDTA y *NONE para el parámetro USRPRF. Para utilizar este mandato para restaurar información del perfil de usuario y almacenes de certificados y sus contraseñas, especifique *ALL para el parámetro USRPRF.

Mandatos que pueden eliminar o perder firmas de los objetos

Al utilizar los siguientes mandatos en un objeto firmado, puede hacerlo de forma que se podría eliminar o perder la firma del objeto. Eliminar la firma podría provocar problemas en el objeto afectado. Como mínimo, ya no podrá verificar el origen del objeto como de confianza ni podrá verificar la firma para detectar cambios en el objeto. Utilice estos mandatos solamente en los objetos firmados que haya creado personalmente y no en los objetos firmados que haya obtenido de otros, como por ejemplo IBM o proveedores). Si el hecho de que el mandato elimine o pierda la firma de un objeto es motivo de preocupación, puede utilizar el mandato Visualizar descripción de objeto (DSPOBJD) para ver si la firma sigue ahí y volver a firmar si fuera necesario.

Nota: Para verificar si un mandato Salvar ha perdido la firma de un objeto, debe restaurar el objeto en una biblioteca distinta de la biblioteca de la que lo salvó (por ejemplo, QTEMP). Entonces puede utilizar el mandato DSPOBJD para determinar si el objeto que está en el soporte de salvar ha perdido la firma.

- Mandato Cambiar programa (CHGPGM). Este mandato cambia los atributos de un programa sin necesidad de recompilarlo. Además, puede utilizar este mandato para forzar la recreación de un programa incluso si los atributos que se especifican son los mismos que los actuales.
- Mandato Cambiar programa de servicio (CHGSRVPGM). Este mandato cambia los atributos de un programa de servicio sin necesidad de recompilarlo. Además, puede utilizar este mandato para forzar la recreación de un programa de servicio incluso si los atributos que se especifican son los mismos que los actuales.

- Mandato Borrar archivo de salvar (CLRSAVF). Este mandato borra el contenido de un archivo de salvar; borra todos los registros existentes del archivo de salvar y reduce la cantidad de almacenamiento que el archivo utiliza.
- Mandato Salvar (SAV). Este mandato salva una copia de uno o varios objetos que puede utilizarse en el sistema de archivos integrado. — Al utilizar este mandato podría perder la firma de los objetos mandato (*CMD) en el soporte de salvar si especifica un valor anterior a la V5R2M0 para el parámetro TGTRLS. La pérdida de firmas se produce debido a que los objetos mandato no pueden firmarse en releases anteriores a V5R2.
- Mandato Salvar biblioteca (SAVLIB). Este mandato le permite salvar una copia de uno o varias bibliotecas. Al utilizar este mandato podría perder la firma de los objetos mandato (*CMD) en el soporte de salvar si especifica un valor anterior a la V5R2M0 para el parámetro TGTRLS. La pérdida de firmas se produce debido a que los objetos mandato no pueden firmarse en releases anteriores a V5R2.
- Mandato Salvar objeto (SAVOBJ). Este mandato salva una copia de un solo objeto o de un grupo de objetos ubicados en la misma biblioteca. Al utilizar este mandato podría perder la firma de los objetos mandato (*CMD) en el soporte de salvar si especifica un valor anterior a la V5R2M0 para el parámetro TGTRLS. La pérdida de firmas se produce debido a que los objetos mandato no pueden firmarse en releases anteriores a V5R2.

Conceptos relacionados

"Consideraciones sobre salvar y restaurar para objetos firmados"
En este tema se proporciona información sobre cómo afectan los objetos firmados a la manera de realizar las tareas de salvar y restaurar en un sistema que ejecute el sistema operativo i5/OS.

Información relacionada

Buscador de valores del sistema

Consideraciones sobre salvar y restaurar para objetos firmados

En este tema se proporciona información sobre cómo afectan los objetos firmados a la manera de realizar las tareas de salvar y restaurar en un sistema que ejecute el sistema operativo i5/OS.

Existen varios valores del sistema que pueden afectar a las operaciones de restauración de su sistema. Solamente uno de estos valores del sistema, el valor del sistema **Verificar firmas de objeto durante la restauración (QVFYOBJRST)**, determina cómo el sistema maneja objetos firmados al restaurarlos. El valor que elija para este valor del sistema le permitirá determinar cómo el proceso de restauración manejará la verificación de objetos sin firmas o con firmas no válidas.

Algunos mandatos de salvar y restaurar afectan a objetos firmados o determinan cómo el sistema maneja los objetos firmados y los no firmados durante las operaciones de salvar y restaurar. Debe tener en cuenta estos mandatos y la repercusión que pueden tener en los objetos firmados, de forma que pueda gestionar mejor el sistema y evitar los posibles problemas que podrían producirse.

Estos mandatos pueden verificar firmas de objetos durante operaciones de salvar y restaurar:
- El mandato Salvar programa bajo licencia (SAVLICPGM).
- El mandato Restaurar (RST).
- El mandato Restaurar biblioteca (RSTLIB).
- El mandato Restaurar programa bajo licencia (RSTLICPGM).
- El mandato Restaurar objeto (RSTOBJ).

Estos mandatos le permiten salvar y restaurar almacenes de certificados; los almacenes de certificados son objetos sensibles a la seguridad que contienen los certificados que utilizará para firmar objetos y verificar firmas:
- El mandato Salvar (SAV).
- El mandato Salvar datos de seguridad (SAVSECDTA).

- El mandato Salvar sistema (SAVSYS).
- El mandato Restaurar (RST).
- El mandato Restaurar perfiles de usuario (RSTUSRPRF).

Algunos mandatos de salvar, dependiendo de los valores de parámetros que utilice, podrían perder la firma de un objeto en el soporte de salvar, eliminando así la seguridad que la firma proporciona. Por ejemplo, *cualquier* operación de salvar que haga referencia a un objeto mandato (*CMD) con un release destino anterior a V5R2M0 provoca que los mandatos se salven sin firmas. Eliminar la firma podría provocar problemas en los objetos afectados. Como mínimo, ya no podrá verificar el origen del objeto como de confianza ni podrá verificar la firma para detectar cambios en el objeto. Utilice estos mandatos solamente en los objetos firmados que haya creado personalmente y no en los objetos firmados que haya obtenido de otros, como por ejemplo IBM o proveedores).

Nota: Para verificar si un mandato Salvar ha perdido la firma de un objeto, debe restaurar el objeto en una biblioteca distinta de la biblioteca de la que lo salvó (por ejemplo, QTEMP). Entonces puede utilizar el mandato DSPOBJD para determinar si el objeto que está en el soporte de salvar ha perdido la firma.

Debe tener en cuenta este potencial para los siguientes mandatos de salvar específicos, así como para los mandatos de salvar en general:

- El mandato Salvar (SAV).
- El mandato Salvar biblioteca (SAVLIB).
- El mandato Salvar objeto (SAVOBJ).

Conceptos relacionados

"Valores del sistema y mandatos que afectan a los objetos firmados" en la página 39
En este tema se facilita información sobre los valores del sistema y los mandatos de i5/OS que se pueden usar para gestionar los objetos firmados o que pueden afectar a los objetos firmados cuando se ejecutan.

Mandatos del comprobador de código para asegurar la integridad de las firmas

Aquí aprenderá a utilizar los mandatos de i5/OS para verificar firmas de objetos con el fin de determinar su integridad.

Puede utilizar el Gestor de certificados digitales (DCM) o las API para verificar firmas de los objetos. También puede utilizar varios mandatos para comprobar firmas. Utilizar este mandato le permite verificar firmas de la misma manera que utiliza un buscador de virus para determinar si un virus ha afectado a archivos u otros objetos del sistema. La mayoría de firmas se comprueban al restaurarse o instalarse el objeto en el sistema, por ejemplo utilizando el mandato RSTLIB.

Puede elegir entre tres mandatos para comprobar firmas de objetos que ya están en el sistema. De ellos, el mandato Comprobar integridad de objeto (CHKOBJITG) está diseñado específicamente para verificar firmas de objetos. La comprobación de firma para cada uno de estos mandatos está controlada por el parámetro CHKSIG. Este parámetro le permite buscar firmas en todos los tipos de objeto que pueden firmarse, ignorar todas las firmas o comprobar solamente los objetos que tengan firmas. Esta última opción es el valor por omisión para el parámetro.

Mandato Comprobar integridad de objeto (CHKOBJITG)

El mandato Comprobar integridad de objeto (CHKOBJITG) le permite determinar si hay objetos en el sistema que hayan sufrido violaciones de la integridad. Puede utilizar este mandato para buscar violaciones de la integridad en objetos propiedad de un perfil de usuario específico, objetos que coincidan

con un nombre de vía de acceso específico o todos los objetos del sistema. Aparecerá una entrada en las anotaciones de violación de la integridad cuando se cumpla de estas condiciones:

- Un mandato, un programa, un objeto módulo o los atributos de una biblioteca han sufrido alteraciones.
- Se ha determinado que la firma digital de un objeto no es válida. La firma es un resumen matemático cifrado de los datos del objeto; por consiguiente, se considera que la firma coincide y es válida si los datos del objeto durante la verificación coinciden con los datos del objeto cuando se firmó. Se determina que una firma no es válida basándose en una comparación del resumen matemático cifrado que se crea al firmarse el objeto y el resumen matemático cifrado realizado durante la verificación de la firma. El proceso de verificación de firmas compara los dos valores de resumen. Si los valores no son los mismos, significa que el contenido del objeto ha cambiado desde que se firmó y se considera que la firma no es válida.
- Un objeto tiene un atributo de dominio incorrecto para el tipo de objeto.

Si el mandato detecta una violación de la integridad en un objeto, añade el nombre de objeto, el nombre de biblioteca (o nombre de vía de acceso), el tipo de objeto, el propietario de objeto y el tipo de anomalía a un archivo de anotaciones de base de datos. El mandato también crea una entrada de anotaciones en otros casos, aunque estos casos no sean violaciones de la integridad. Por ejemplo, el mandato crea una entrada de anotaciones para los objetos que pueden firmarse pero que no tienen una firma digital, los objetos que no ha puede comprobar y los objetos que están en un formato que requiere cambios para poder utilizarlos en la implementación actual del sistema (conversión de IMPI a RISC).

El valor del parámetro CHKSIG controla cómo el mandato maneja las firmas digitales de los objetos. Puede especificar uno de tres valores para este parámetro:

- *SIGNED – Al especificar este valor, el mandato comprueba los objetos con firmas digitales. El mandato crea una entrada en las anotaciones para cualquier objeto con una firma que no sea válida. Este es el valor por omisión.
- *ALL – Al especificar este valor, el mandato comprueba todos los objetos firmables para determinar si tienen una firma. El mandato crea una entrada en las anotaciones para cualquier objeto firmable que no tenga una firma y para cualquiera objeto con una firma que no sea válida.
- *NONE – Al especificar este valor, el mandato no comprueba las firmas digitales de los objetos.

Mandato Comprobar opción de producto (CHKPRDOPT)

El mandato Comprobar opción de producto (CHKPRDOPT) informa de las diferencias entre la estructura correcta y la estructura real de un producto de software. Por ejemplo, el mandato informa de un error si se suprime un objeto de un producto instalado.

El valor del parámetro CHKSIG controla cómo el mandato maneja las firmas digitales de los objetos. Puede especificar uno de tres valores para este parámetro:

- *SIGNED – Al especificar este valor, el mandato comprueba los objetos con firmas digitales. El mandato verifica las firmas de los objetos firmados. Si el mandato determina que la firma de un objeto no es válida, el mandato envía un mensaje a las anotaciones de trabajo y se identifica al producto como en estado erróneo. Este es el valor por omisión.
- *ALL – Al especificar este valor, el mandato comprueba todos los objetos firmables para determinar si tienen una firma y verifica la firma de esos objetos. El mandato envía un mensaje a las anotaciones de trabajo por cada objeto firmable que no tenga una firma; sin embargo, el mandato no identifica el producto como erróneo. Si el mandato determina que la firma de un objeto no es válida, envía un mensaje a las anotaciones de trabajo y define el producto como erróneo.
- *NONE – Al especificar este valor, el mandato no comprueba las firmas digitales de objetos de producto.

Mandato Salvar programa bajo licencia (SAVLICPGM)

El mandato Salvar programa bajo licencia (SAVLICPGM) le permite salvar una copia de los objetos que forman un programa bajo licencia. Salva el programa bajo licencia en un formato que puede restaurarse mediante el mandato Restaurar programa bajo licencia (RSTLICPGM).

El valor del parámetro CHKSIG controla cómo el mandato maneja las firmas digitales de los objetos. Puede especificar uno de tres valores para este parámetro:

- *SIGNED – Al especificar este valor, el mandato comprueba los objetos con firmas digitales. El mandato verifica las firmas de los objetos firmados pero no comprueba los objetos no firmados. Si el mandato determina que la firma de un objeto no es válida, el mandato envía un mensaje a las anotaciones de trabajo para identificar el producto y la operación de salvar fallará. Este es el valor por omisión.
- *ALL – Al especificar este valor, el mandato comprueba todos los objetos firmables para determinar si tienen una firma y verifica la firma de esos objetos. El mandato envía un mensaje a las anotaciones de trabajo por cada objeto firmable que no tenga una firma; sin embargo, el proceso de salvar no finaliza. Si el mandato determina que la firma de un objeto no es válida, envía un mensaje a las anotaciones de trabajo y la operación de salvar fallará.
- *NONE – Al especificar este valor, el mandato no comprueba las firmas digitales de objetos de producto.

Verificar la integridad de la función de comprobación de código

Obtenga información acerca de cómo puede verificar la integridad de la función de comprobación de código utilizada para verificar la integridad del sistema i5/OS.

Para utilizar la nueva función de verificación de la integridad de la comprobación de código utilizada para verificar la integridad del sistema, debe tener la autorización especial *AUDIT.

Para verificar la función de comprobación de código, ejecute la API Comprobar sistema (QydoCheckSystem) para determinar si algún objeto clave del sistema operativo ha cambiado desde que se firmó. Al ejecutar la API, esta comprueba objetos clave del sistema, incluidos los programas y programas de servicio y objetos de mandato (*CMD) seleccionados de la biblioteca QSYS, de la forma siguiente:

1. Comprueba todos los objetos de programa (*PGM) a los que señala la tabla de puntos de entrada del sistema.
2. Comprueba todos los objetos de programa de servicio (*SRVPGM) de la biblioteca QSYS y verifica la integridad de la API Verificar objeto.
3. Ejecuta la API Verificar objeto (QydoVerifyObject) para verificar la integridad de los mandatos Restaurar objeto (RSTOBJ), Restaurar biblioteca (RSTLIB) y Comprobar integridad de objeto (CHKOBJITG).
4. Utiliza los mandatos RSTOBJ y RSTLIB en un archivo de salvar especial (*SAV) para asegurarse de que se informa correctamente de los errores. Una falta de mensajes de error o la presencia de mensajes de error incorrectos indican un problema potencial.
5. Crea un objeto de mandato (*CMD) diseñado para fallar a fin de realizar una verificación correcta.
6. Ejecuta el mandato CHKOBJITG y la API Verificar objeto en este objeto de mandato especial para asegurarse de que el mandato CHKOBJITG y la API Verificar objeto informan correctamente de los errores. Una falta de mensajes de error o la presencia de mensajes de error incorrectos indican un problema potencial.
7. Comprueba la firma de cada módulo de código interno bajo licencia (LIC) y verifica que los errores se notifiquen con módulo LIC no firmado y firmado sin validez.

Conceptos relacionados

"Función de verificación de la integridad del comprobador de código" en la página 6
Este tema facilita información sobre cómo puede verificar la integridad de la función del comprobador de código para verificar la integridad de su sistema al ejecutar el sistema operativo i5/OS.

Referencia relacionada

"Interpretar los mensajes de error de verificación del comprobador de código" en la página 47
En este tema se proporciona información sobre qué mensajes devuelve la función de verificación de integridad del comprobador de código en un sistema que ejecute el sistema operativo i5/OS y se explica cómo usar los mensajes para asegurar que la función del comprobador de código no está dañada, así como las posibles soluciones si los mensajes indican que la función o los objetos clave del sistema operativo pueden haberse dañado.

Resolución de problemas relacionados con objetos firmados

En este tema se facilita información sobre los mandatos y valores del sistema i5/OS que le permiten trabajar con objetos firmados y se explica cómo pueden afectar los objetos firmados a los procesos de copia de seguridad y recuperación.

Al firmar objetos y trabajar con objetos firmados, puede encontrar problemas que le impidan realizar sus tareas y alcanzar sus objetivos. Muchos de estos errores y problemas habituales que puede experimentar se engloban en las siguientes categorías:

Resolución de errores relacionados con la firma de objetos

En este tema se facilita información sobre cómo resolver algunos de los problemas más comunes que pueden surgir al firmar objetos en un sistema que ejecute el sistema operativo i5/OS.

Problema	Posible solución
Al utilizar la API Firmar objeto para firmar un objeto con un release destino V4R5 o anterior, el proceso de firmar falla y no se firma el objeto (mensaje de error CPFB721).	El sistema no proporciona el soporte de firma de objetos hasta la V5R1. Para los objetos que devuelven un mensaje de error CPFB721, debe volver a crear los programas con un release destino V5R1 o posterior para poder firmarlos.

Resolución de errores relacionados con la verificación de firmas

En este tema se facilita información sobre cómo resolver algunos de los problemas más comunes que pueden surgir al verificar las firmas digitales de i5/OS en los objetos.

Problema	Posible solución
El proceso de restauración falla para los objetos sin firmas.	Si la falta de firma no es motivo de preocupación, compruebe si el valor del sistema QVFYOBJRST está establecido en 5. El valor 5 especifica que los objetos sin firma no pueden restaurarse. Cambie el valor a 3 y vuelva a intentar la restauración.
El proceso de restauración falla para los objetos con firmas.	Esto puede suceder si se ha transferido el almacén de certificados *SIGNATUREVERIFICATION al sistema y no se utilizado el DCM para cambiar la contraseña. En tal caso, los certificados contenidos en el almacén no pueden utilizarse para verificar las firmas de los objetos durante el proceso de restauración. Utilice el DCM para cambiar la contraseña para el almacén de certificados. Si no conoce la contraseña, tendrá que suprimir el almacén de certificados, volver a crearlo y utilizar el DCM para cambiar la contraseña.

Problema	Posible solución
Al restaurar o instalar un producto, obtendrá un error al no poder verificarse una firma.	Cuando la firma de un objeto no consigue verificarse correctamente, la anomalía puede indicar que el objeto ha sido modificado desde que se firmó. Si el problema es la integridad del objeto, no cambie el valor del sistema QVFYOBJRST ni lleve a cabo otras acciones que puedan permitir que el objeto cuestionable se restaure. Al permitirlo se eludiría la seguridad que proporciona la verificación de firmas, dejando así entrar un objeto peligroso en el sistema. En lugar de ello, póngase en contacto con quien haya firmado el objeto para determinar la acción adecuada a llevar a cabo para resolver el problema.

Interpretar los mensajes de error de verificación del comprobador de código

En este tema se proporciona información sobre qué mensajes devuelve la función de verificación de integridad del comprobador de código en un sistema que ejecute el sistema operativo i5/OS y se explica cómo usar los mensajes para asegurar que la función del comprobador de código no está dañada, así como las posibles soluciones si los mensajes indican que la función o los objetos clave del sistema operativo pueden haberse dañado.

La tabla siguiente proporciona una lista de los mensajes generados por la función de verificación de comprobación de código durante el proceso. Esta tabla no ofrece una lista exhaustiva de todos los mensajes que puede recibir. En lugar de ello, la tabla lista aquellos mensajes que muy probablemente indican que la verificación de comprobación de código ha sido satisfactoria o que ha encontrado un problema grave. Consulte la documentación de la API Comprobar sistema (QydoCheckSystem) para obtener una lista detallada de los mensajes de error.

Del mismo modo, diversos mensajes generados por la función de verificación de comprobación de código durante el proceso son informativos, y no figuran en esta lista. Para obtener más información acerca del funcionamiento del proceso de verificación de la comprobación de código, consulte la sección Verificar la integridad de la función de comprobación de código.

Tabla 1. Mensajes de error de verificación de la comprobación de código

Mensaje de error	Posible problema y solución
CPFB729	Indica que el proceso de verificación de la comprobación de código no ha podido realizarse según lo esperado. Esta anomalía puede deberse a un amplio espectro de problemas. Consulte las anotaciones de trabajo por si existen mensajes de error más detallados a fin de determinar la naturaleza exacta de la anomalía y la posible causa. Si determina que la comprobación de integridad no ha podido realizarse en objetos clave del sistema operativo, esta anomalía puede indicar que el objeto ha cambiado desde que se firmó al suministrar el sistema operativo. Puede que sea necesario reinstalar el sistema operativo para garantizar la integridad del sistema.

Tabla 1. Mensajes de error de verificación de la comprobación de código (continuación)

Mensaje de error	Posible problema y solución
Al consultar las anotaciones de trabajo, verá mensajes tales como CPFB723, CPD37A1 o CPD37A0 relativos a estos objetos específicos: • Objetos de programa (*PGM): – QYDONOSIG de la biblioteca QTEMP – QYDOBADSIG de la biblioteca QTEMP • Objetos de mandato (*CMD): – QYDOBADSIG de la biblioteca QTEMP – SIGNOFF de la biblioteca QTEMP	Indica que el conjunto especial de objetos que la función de verificación de la comprobación de código utiliza para la prueba de integridad ha fallado según lo esperado. Esta anomalía indica que los mandatos RSTOBJ, RSTLIB y CHKOBJITG, y la API Verificar objeto informan correctamente de los errores. No es necesario realizar otras acciones.
CPFB723 para cualquier objeto distinto a los mencionados anteriormente en esta tabla.	Indica que la firma de un objeto clave del sistema operativo no ha podido verificarse. Esta anomalía puede indicar que el objeto ha cambiado desde que se firmó al suministrar el sistema operativo. Puede que sea necesario reinstalar el sistema operativo para garantizar la integridad del sistema.
CPFB722 para cualquier objeto distinto a los mencionados anteriormente en esta tabla.	Indica que un objeto clave del sistema operativo no tiene firma, cuando se esperaba que fuera así. Esta falta de firma puede indicar que el objeto ha cambiado desde que se firmó al suministrar el sistema operativo. Puede que sea necesario reinstalar el sistema operativo para garantizar la integridad del sistema.
CPFB72A para cualquier objeto distinto de los mencionados anteriormente en esta tabla.	Indica que no ha podido realizarse la comprobación de integridad en un objeto clave del sistema operativo. Esta anomalía puede indicar que el objeto ha cambiado desde que se firmó al suministrar el sistema operativo. Puede que sea necesario reinstalar el sistema operativo para garantizar la integridad del sistema.

Si alguna vez necesita reinstalar el código que verifica la integridad de la función de comprobación de código, debe obtenerlo de una fuente conocida y fiable. Por ejemplo, puede cargar el soporte de instalación que ha utilizado para instalar el release actual. Para restaurar la función de verificación de la comprobación de código, siga estos pasos desde un indicador de mandatos de i5/OS:

1. Ejecute el mandato `QSYS/DLTPGM QSYS/QYDOCHKS`. Este mandato suprime la API Comprobar sistema (OPM, QYDOCHKS; ILE, QydoCheckSystem).
2. Ejecute el mandato `QSYS/DLTSRVPGM QSYS/QYDOCHK1`. Este mandato suprime el programa de servicio de comprobación de código con la API Comprobar sistema (OPM, QYDOCHKS; ILE, QydoCheckSystem).
3. Ejecute el mandato `QSYS/DLTF QSYS/QYDOCHKF`. Este mandato suprime el archivo de salvar que contiene los objetos utilizados por la función de comprobación de código para probar los objetos con firmas incorrectas y sin firmas.
4. Ejecute el mandato `QSYS/RSTOBJ OBJ(QYDOCHK*) SAVLIB(QSYS) DEV(OPT01) OBJTYPE(*ALL) OPTFILE('Q5722SS1/Q5200M_/Q00/Q90')`. Este mandato restaura todos los objetos necesarios para la función de verificación de la comprobación de código desde el soporte de instalación cargado.

Tareas relacionadas

"Verificar la integridad de la función de comprobación de código" en la página 45
Obtenga información acerca de cómo puede verificar la integridad de la función de comprobación de código utilizada para verificar la integridad del sistema i5/OS.

Información relacionada con la firma de objetos y la verificación de firmas

En algunos sitios Web y libros rojos de IBM (Redbooks) en formato PDF hallará información relacionada con el temario Firma de objetos y la verificación de firmas. Puede ver y descargar cualquiera de los archivos PDF.

La firma de objetos y la verificación de firmas son tecnologías de seguridad relativamente nuevas. A continuación se ofrece una breve lista de otros recursos que pueden ser de ayuda si está interesado en obtener conocimientos más amplios sobre estas tecnologías y cómo funcionan:

- **Sitio Web VeriSign Help Desk** El sitio Web VeriSign proporciona una amplia biblioteca sobre temas relacionados con los certificados digitales, tales como la firma de objetos, así como una serie de otros temas de seguridad de Internet.
- **IBM eServer iSeries Wired Network Security: i5/OS V5R1 DCM and Cryptographic Enhancements**

  SG24-6168 Esta publicación de IBM Redbooks se centra en las mejoras de seguridad de red de la V5R1. La publicación Redbooks consta de muchos temas, incluido el que explica cómo utilizar prestaciones de firma de objetos, el Gestor de certificados digitales (DCM), etcétera,

Información sobre licencia de código y exención de responsabilidad

IBM le otorga una licencia de copyright no exclusiva para utilizar todos los ejemplos de código de programación, a partir de los que puede generar funciones similares adaptadas a sus necesidades específicas.

SUJETO A LAS GARANTÍAS ESTATUTARIAS QUE NO PUEDAN EXCLUIRSE, IBM Y LOS DESARROLLADORES Y SUMINISTRADORES DE PROGRAMAS DE IBM NO OFRECEN NINGUNA GARANTÍA NI CONDICIÓN, YA SEA IMPLÍCITA O EXPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS O CONDICIONES IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN PROPÓSITO DETERMINADO Y NO VULNERACIÓN CON RESPECTO AL PROGRAMA O AL SOPORTE TÉCNICO, SI EXISTE.

BAJO NINGUNA CIRCUNSTANCIA, IBM Y LOS DESARROLLADORES O SUMINISTRADORES DE PROGRAMAS DE IBM SE HACEN RESPONSABLES DE NINGUNA DE LAS SIGUIENTES SITUACIONES, NI SIQUIERA EN CASO DE HABER SIDO INFORMADOS DE TAL POSIBILIDAD:

1. PÉRDIDA DE DATOS O DAÑOS CAUSADOS EN ELLOS;
2. DAÑOS ESPECIALES, ACCIDENTALES, DIRECTOS O INDIRECTOS, O DAÑOS ECONÓMICOS DERIVADOS;
3. PÉRDIDAS DE BENEFICIOS, COMERCIALES, DE INGRESOS, CLIENTELA O AHORROS ANTICIPADOS.

ALGUNAS JURISDICCIONES NO PERMITEN LA EXCLUSIÓN O LA LIMITACIÓN DE LOS DAÑOS DIRECTOS, ACCIDENTALES O DERIVADOS, POR LO QUE PARTE DE LAS LIMITACIONES O EXCLUSIONES ANTERIORES, O TODAS ELLAS, PUEDE NO SER PROCEDENTE EN SU CASO.

Apéndice. Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en los Estados Unidos.

Es posible que en otros países IBM no ofrezca los productos, los servicios o los dispositivos que se describen en este documento. Póngase en contacto con el representante local de IBM que le informará sobre los productos y servicios disponibles actualmente en su área. Las referencias hechas a productos, programas o servicios de IBM no pretenden afirmar ni dar a entender que únicamente puedan utilizarse dichos productos, programas o servicios de IBM. Puede utilizarse en su lugar cualquier otro producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y comprobar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes de aprobación que cubran alguno de los temas tratados en este documento. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por correo, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
Estados Unidos

Para realizar consultas relacionadas con los caracteres de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM de su país o bien envíe su consulta por escrito a:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japón

El párrafo que sigue no se aplica en el Reino Unido ni en ningún otro país en el que tales disposiciones entren en contradicción con las leyes locales: INTERNATIONAL BUSINESS MACHINES CORPORATION SUMINISTRA ESTA PUBLICACIÓN “TAL CUAL”, SIN GARANTÍAS DE NINGUNA CLASE, YA SEAN EXPLÍCITAS O IMPLÍCITAS, INCLUIDAS LAS GARANTÍAS IMPLÍCITAS DE NO VULNERABILIDAD, COMERCIALIZACIÓN O ADECUACIÓN A UN PROPÓSITO DETERMINADO, PERO SIN LIMITARSE A ELLAS. Algunos estados no permiten la declaración de limitación de responsabilidad con respecto a las garantías explícitas o implícitas en determinadas transacciones; por tanto, esta información puede no ser aplicable en su caso.

Esta documentación puede incluir inexactitudes técnicas o errores tipográficos. La información que contiene está sujeta a modificaciones periódicas, que se incorporarán en sucesivas ediciones de la publicación. IBM puede efectuar mejoras y/o cambios en los productos y/o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Las referencias efectuadas en esta documentación a sitios Web no IBM se suministran solo a efectos de comodidad, y no implican ninguna garantía con respecto a los mismos. Los materiales de estos sitios Web no forman parte de los materiales de IBM para este producto y el uso que se haga de estos sitios Web es de la entera responsabilidad del usuario.

IBM puede utilizar o distribuir la información que usted le suministre del modo que IBM considere conveniente sin incurrir por ello en ninguna obligación para con usted.

Los licenciatarios de este programa que deseen recibir información acerca del mismo con la finalidad de permitir: (i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido este) y (ii) la utilización mutua de la información intercambiada, deben ponerse en contacto con:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
Estados Unidos

Tal información puede estar disponible, sujeta a los términos y condiciones adecuados, incluido en algunos casos el pago de una tasa.

El programa bajo licencia descrito en esta información y todo el material bajo licencia disponible para el mismo, se proporciona bajo los términos del Acuerdo de Cliente IBM, el Acuerdo de Licencia de Programa Internacional IBM, el Acuerdo de Licencia de Código Máquina IBM o cualquier otro acuerdo equivalente entre ambas partes.

Los datos de rendimiento contenidos en esta documentación se han determinado en un entorno controlado. Por tanto, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Algunas de las mediciones pueden haberse efectuado en sistemas a nivel de desarrollo, y no existe garantía alguna de que dichas mediciones sean las mismas en sistemas disponibles a nivel general. Además, algunas mediciones pueden haberse estimado por extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información concerniente a productos no IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha comprobado los productos y no puede confirmar la exactitud en cuanto a rendimiento, compatibilidad u otras características relativas a productos no IBM. Las cuestiones relativas a las capacidades de productos no IBM deben dirigirse a los proveedores de dichos productos.

Todas las afirmaciones relativas a planes futuros de IBM están sujetas a modificación o retirada sin previo aviso, y solo representan metas y objetivos.

Todos los precios de IBM mostrados son precios actuales de venta al por menor sugeridos por IBM y están sujetos a modificaciones sin previo aviso. Los precios de los concesionarios pueden ser diferentes.

Esta información está pensada únicamente a efectos de planificación. La información que aquí se incluye está sujeta a cambios antes de que los productos descritos estén disponibles.

Esta documentación contiene ejemplos de datos e informes utilizados en operaciones diarias de gestión. Para ilustrarlos de la forma más completa posible, incluyen los nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios, y cualquier parecido con nombres y direcciones utilizados por empresas reales es pura coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene ejemplos de programas de aplicación en lenguaje fuente, que ilustran técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de la forma deseada sin tener que efectuar ningún pago a IBM, con el objetivo de desarrollar, utilizar, comercializar o distribuir programas de aplicación conformes a la interfaz de programación de aplicaciones para la plataforma operativa para la que se han escrito los programas de ejemplo. Estos ejemplos no han sido probados exhaustivamente bajo todas las condiciones. IBM, por lo tanto, no puede garantizar ni dar por supuesta la fiabilidad, la posibilidad de servicio, ni el funcionamiento de estos programas.

SUJETO A LAS GARANTÍAS ESTATUTARIAS QUE NO PUEDAN EXCLUIRSE, IBM Y LOS DESARROLLADORES Y SUMINISTRADORES DE PROGRAMAS DE IBM NO OFRECEN NINGUNA GARANTÍA NI CONDICIÓN, YA SEA IMPLÍCITA O EXPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS O CONDICIONES IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN PROPÓSITO DETERMINADO Y NO VULNERACIÓN CON RESPECTO AL PROGRAMA O AL SOPORTE TÉCNICO, SI EXISTE.

BAJO NINGUNA CIRCUNSTANCIA, IBM Y LOS DESARROLLADORES O SUMINISTRADORES DE PROGRAMAS DE IBM SE HACEN RESPONSABLES DE NINGUNA DE LAS SIGUIENTES SITUACIONES, NI SIQUIERA EN CASO DE HABER SIDO INFORMADOS DE TAL POSIBILIDAD:

1. PÉRDIDA O DAÑO DE LOS DATOS;
2. DAÑOS ESPECIALES, FORTUITOS O INDIRECTOS O DAÑOS ECONÓMICOS CONSECUENTES O
3. PÉRDIDAS DE BENEFICIOS, COMERCIALES, DE INGRESOS, CLIENTELA O AHORROS ANTICIPADOS.

ALGUNAS JURISDICCIONES NO PERMITEN LA EXCLUSIÓN O LIMITACIÓN DE DAÑOS FORTUITOS O DERIVADOS POR LO QUE ES POSIBLE QUE LAS LIMITACIONES O EXCLUSIONES ANTERIORES O PARTE DE ELLAS NO LE SEAN APLICABLES.

Cada copia o parte de estos programas de ejemplo o cualquier trabajo derivado de estos debe incluir una nota de derechos de copia como esta:

Si visualiza esta documentación en soporte software, puede que no aparezcan las fotografías y las ilustraciones en color.

Marcas registradas

Los siguientes términos son marcas registradas de International Business Machines Corporation en los Estados Unidos y/o en otros países:

Adobe
eServer
i5/OS
IBM
iSeries
OS/400
Redbooks
system i
xSeries

| Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe
| Systems Incorporated en Estados Unidos y/o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

Java y todas las marcas basadas en Java son marcas registradas de Sun Microsystems, Inc. en los Estados Unidos y/o en otros países.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y/o en otros países.

UNIX es una marca registrada de The Open Group en los Estados Unidos y/o en otros países.

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o marcas de servicio de terceros.

Términos y condiciones

Los permisos para utilizar estas publicaciones están sujetos a los siguientes términos y condiciones.

Uso personal: puede reproducir estas publicaciones para uso personal (no comercial) siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede distribuir ni visualizar estas publicaciones ni ninguna de sus partes, como tampoco elaborar trabajos que se deriven de ellas, sin el consentimiento explícito de IBM.

Uso comercial: puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de su empresa, siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede elaborar trabajos que se deriven de estas publicaciones, ni tampoco reproducir, distribuir ni visualizar estas publicaciones ni ninguna de sus partes fuera de su empresa, sin el consentimiento explícito de IBM.

Aparte de la autorización que se concede explícitamente en este permiso, no se otorga ningún otro permiso, licencia ni derecho, ya sea explícito o implícito, sobre las publicaciones, la información, los datos, el software o cualquier otra propiedad intelectual contenida en ellas.

IBM se reserva el derecho de retirar los permisos aquí concedidos siempre que, según el parecer del fabricante, se utilicen las publicaciones en detrimento de sus intereses o cuando, también según el parecer del fabricante, no se sigan debidamente las instrucciones anteriores.

No puede bajar, exportar ni reexportar esta información si no lo hace en plena conformidad con la legislación y normativa vigente, incluidas todas las leyes y normas de exportación de Estados Unidos.

IBM NO PROPORCIONA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN ″TAL CUAL″, SIN GARANTÍA DE NINGUNA CLASE, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO VULNERACIÓN E IDONEIDAD PARA UN FIN DETERMINADO.

Impreso en España