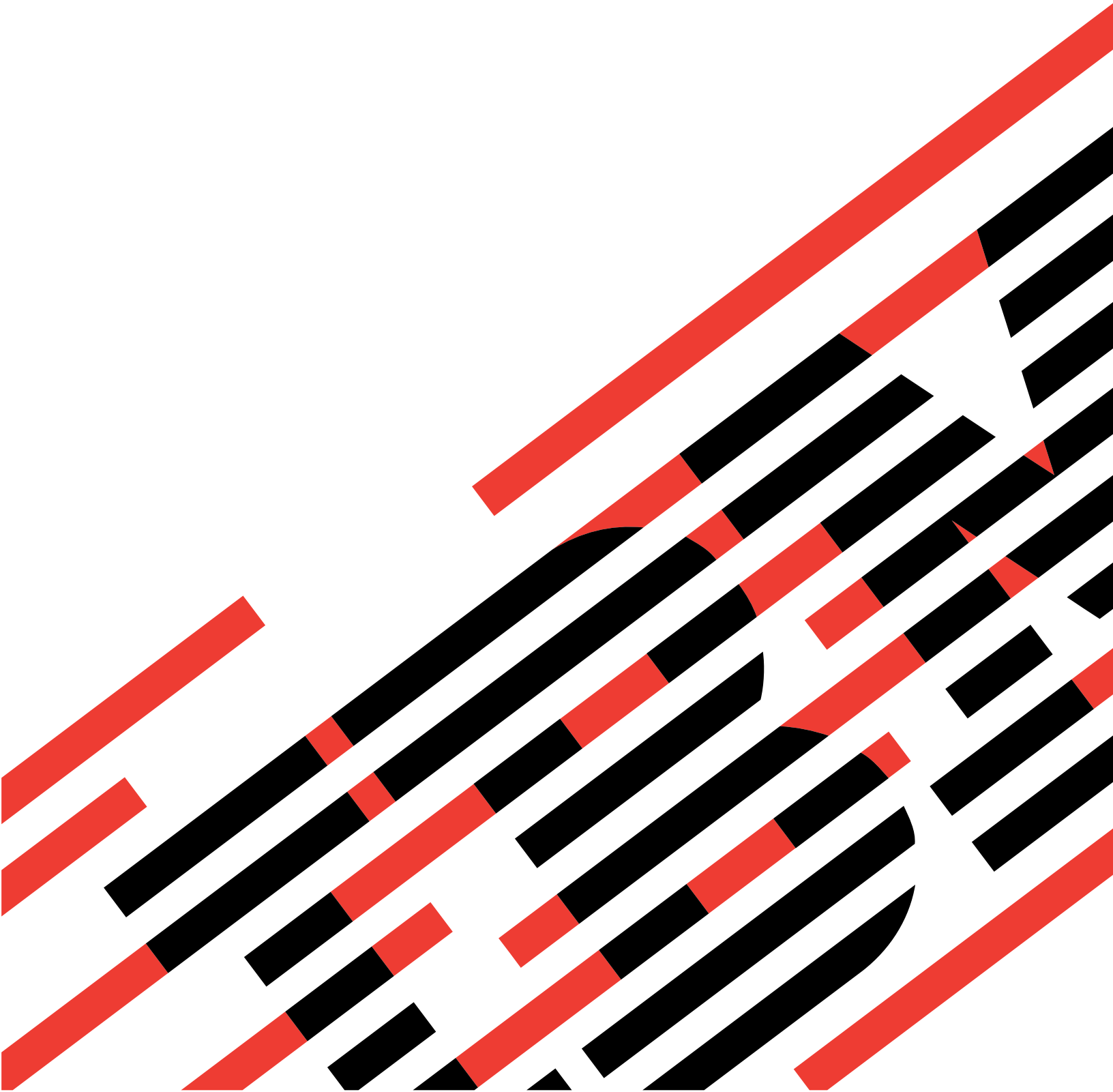
IBM

eserver

iSeries

Firma de objetos y verificación de firmas



IBM

@server

iSeries

Firma de objetos y verificación de firmas

Contenido

Firma de objetos y verificación de firmas

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 de iSeries. 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 no repudiable 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 para iSeries mediante lo siguiente:

- API para firmar objetos y para verificar las firmas de objetos de forma programática.
- Gestor de certificados digitales (Digital Certificate Manager) para firmar objetos y para ver o verificar las firmas de objetos.
- iSeries Navigator Management Central 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:

Novedades de la V5R2
Utilice esta información para aprender sobre las nuevas posibilidades de firma de objetos y verificación de firmas de iSeries, así como los cambios realizados en la documentación para este release.

Imprimir este tema
Utilice esta información para imprimir todo el tema como un archivo PDF.

Casos prácticos de firma de objetos
Utilice esta información para revisar casos prácticos que ilustran algunas situaciones típicas para el uso de las posibilidades de firma de objetos y verificación de firmas de iSeries. Cada caso práctico también proporciona las tareas de configuración que debe llevar a cabo para implementar el caso práctico como se describe.

Conceptos sobre la firma de objetos
Utilice esta información de conceptos y de referencia para aprender más sobre las firmas digitales y sobre como funcionan los procesos de firma de objetos y verificación de firmas.

Requisitos previos para la firma de objetos y la verificación de firmas
Utilice esta información para aprender sobre los requisitos previos de configuración, así como otras consideraciones de planificación para firmar objetos y verificar firmas.

Gestionar objetos firmados
Utilice esta información para aprender sobre los mandatos y los valores del sistema de iSeries que puede utilizar para trabajar con objetos firmados y cómo los objetos firmados afectan a los procesos de copia de seguridad y recuperación.

Resolución de problemas de la firma de objetos y la verificación de firmas
Utilice esta información para aprender a resolver los problemas y errores que pueda encontrar al firmar objetos y verificar firmas.

Información relacionada para la firma de objetos y la verificación de firmas
Utilice esta información para buscar enlaces a otros recursos y así aprender más sobre la firma de objetos y la verificación de firmas de objetos.

Novedades de la V5R2

Las posibilidades de firma de objetos y verificación de firmas para iSeries se introdujeron en la V5R1. Sin embargo, la V5R2 ofrece nuevas funciones y mejoras.

Las funciones nuevas o mejoradas de la firma de objetos y la verificación de firmas incluyen:

- **Función de firma de objetos de iSeries Navigator Management Central**
  Ahora puede utilizar el Asistente para la definición del producto Management Central para firmar los objetos que empaquete para su distribución a sistemas de punto final iSeries.
- **Firma de objetos mandato (*CMD)**
  Ahora puede firmar objetos mandato (*CMD). Puede elegir entre firmar un objeto *CMD completo o firmar solamente los componentes del núcleo de un objeto *CMD.
- **Nuevas API de firma y verificación**
  Puede utilizar tres nuevas API para aprovechar de forma programática las mejoras efectuadas en las posibilidades de firma y verificación de OS/400:
  - API Firmar almacenamiento intermedio (QYDOSGNB, QydoSignBuffer)
    Esta API permite al sistema local firmar digitalmente un almacenamiento intermedio para certificar que es fiable. Tras firmar el almacenamiento intermedio, el sistema devuelve la firma digital a quien haya llamado a la API. Por ejemplo, podría utilizar esta API para firmar parte de un archivo XML y almacenar la firma en otra parte del archivo XML, o bien podría leer registros de archivos de base de datos en un almacenamiento intermedio y utilizar la API para firmarlos.
  - Verificar almacenamiento intermedio (QYDOVFYB, QydoVerifyBuffer)
    Esta API permite al sistema local verificar la firma digital en un almacenamiento intermedio firmado anteriormente.
  - API Añadir verificador (QYDOADDV, QydoAddVerifier)
    Esta API añade un certificado al almacén de certificados *SIGNATUREVERIFICATION de un sistema. El sistema puede utilizar entonces el certificado añadido para verificar firmas de objetos que el certificado ha creado. Verificar la firma permite al sistema verificar la integridad de los objetos firmados para asegurar que los objetos no han cambiado desde que se firmaron. Si no existe el almacén de certificados, esta API lo crea al añadir el certificado.

    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, deberá considerar el 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.

Anteriormente, la información sobre las posibilidades de firma de objetos y verificación de firmas de iSeries estaba disponible como parte del tema Digital Certificate Management en Information Center. Ahora existen métodos adicionales que puede utilizar para firmar objetos y verificar firmas. Consecuentemente, este nuevo tema de Information Center está disponible para facilitar el uso de las posibilidades de firma de objetos y verificación de firmas al proporcionar información centralizada sobre el uso de estas posibilidades. El tema ofrece información mejorada y más completa, por ejemplo casos prácticos, para ayudarle a determinar cuándo y cómo utilizar estas posibilidades como suplemento de su política de seguridad.

La información nueva o mejorada para este tema incluye:

- Casos prácticos que puede utilizar como ayuda para determinar el mejor uso de las posibilidades de firma de objetos y verificación de firmas como suplemento de su política de seguridad.
- Nuevas secciones que describen mandatos y valores del sistema que puede utilizar para gestionar objetos firmados en el sistema.
- Nuevas secciones que describen la planificación y otra información conceptual para firmar objetos y verificar firmas.

Para obtener más información sobre las novedades o los cambios de este release, vea Memo to Users

Imprimir este tema

Para ver o bajar la versión PDF, seleccione Firma de objetos y verificación de firmas  (tamaño del archivo 350 kb o 44 páginas aproximadamente).

Para guardar un PDF en la estación de trabajo para verlo o imprimirlo:

1. Abra el PDF en el navegador (pulse en el enlace más arriba).
2. En el menú del navegador, pulse en **Archivo**.
3. Pulse en **Guardar como...**
4. Vaya al directorio en el que desee guardar el PDF.
5. Pulse en **Guardar**.

Si necesita Adobe Acrobat Reader para ver o imprimir el PDF, puede bajar una copia del sitio Web Adobe (www.adobe.com/prodindex/acrobat/readstep.html)  .

Casos prácticos de firma de objetos

El servidor iSeries 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 iSeries de la manera que mejor se adapte a sus necesidades de seguridad y de empresa:

Caso práctico: Utilizar el Gestor de certificados digitales 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 firmar objetos y verificar firmas de objetos.

Caso práctico: Utilizar API para firmar objetos y verificar firmas
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 Firmar objeto y la API Añadir verificador para firmar objetos y habilitar la verificación de firmas.

Caso práctico: Utilizar Management Central para firmar objetos
Este caso práctico describe una empresa que desea firmar los objetos que empaqueta y distribuye a múltiples servidores iSeries. Basándose en las necesidades comerciales y los objetivos de seguridad de la empresa, este caso práctico describe cómo utilizar la función Management Central de iSeries Navigator para empaquetar y firmar objetos que se distribuirán a otros servidores iSeries.

Caso práctico: Utilizar DCM para firmar objetos y verificar firmas

Situación

Como administrador de iSeries para MyCo., Inc. es responsable de la gestión de los dos servidores iSeries de la empresa. Uno de estos servidores iSeries proporciona un sitio Web público para la empresa. Usted utiliza el servidor iSeries 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 OS/400 ha averiguado que existen varios métodos que puede utilizar para firmar objetos y verificar las firmas de objetos. Dado que es usted el responsable de la gestión de un número reducido de servidores iSeries 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 servidores iSeries.

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

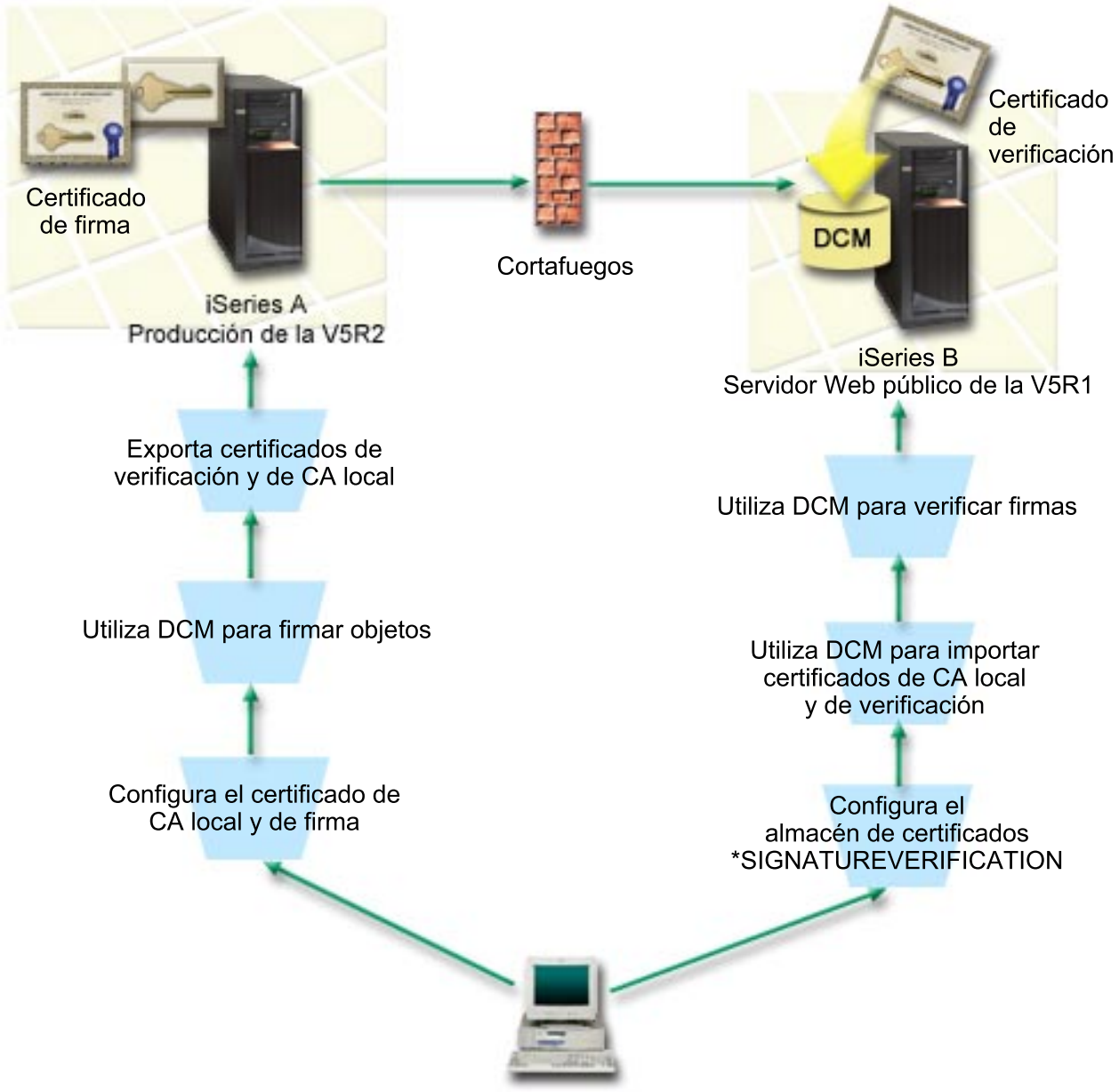
En este caso práctico desea firmar digitalmente objetos vulnerables como, por ejemplo, programas cgi-bin que generan formularios, en el servidor iSeries público de su empresa. Como administrador del sistema en MyCo, Inc., desea utilizar el Gestor de certificados digitales (DCM) para firmar estos objetos 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 (iSeries 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 servidores iSeries para verificar el origen y la autenticidad de los objetos firmados por la empresa. Para logralo, cada servidor iSeries 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 de iSeries 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:

iSeries A

- El iSeries A ejecuta OS/400 Versión 5 Release 2 (V5R2).
- El iSeries A es el servidor de producción interno de la empresa y la plataforma de desarrollo para el sevidor Web iSeries público (iSeries B).
- El iSeries A tiene instalado un Cryptographic Access Provider de 128 bits para iSeries (5722–AC3).
- El iSeries A tiene instalados y configurados el Gestor de certificados digitales (opción 34 de OS/400) y el Servidor HTTP IBM (5722–DG1).
- El iSeries A actúa como Autoridad certificadora (CA) local y el certificado de firma de objetos reside en este sistema.

- El iSeries 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 iSeries A está configurado para permitir la verificación de firmas.

iSeries B

- El iSeries B ejecuta OS/400 Versión 5 Release 1 (V5R1).
- El iSeries B es el servidor Web público externo de la empresa fuera del cortafuegos de la empresa.
- El iSeries B tiene instalado un Cryptographic Access Provider de 128 bits (5722–AC3).
- El iSeries B tiene instalados y configurados el Gestor de certificados digitales (opción 34 de OS/400) y el Servidor HTTP IBM (5722–DG1).
- El iSeries B no opera una CA local y el iSeries B no firma objetos.
- El iSeries 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 servidores iSeries 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 servidores iSeries.
3. Todos los servidores iSeries 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 restauración (QVFYOBJRST) en todos los servidores iSeries de los casos prácticos como 3 y no se ha cambiado. El valor por omisión asegura que el servidor puede verificar firmas de objetos a medida que se restauran los objetos firmados.
5. El administrador del sistema para el iSeries 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 servidores iSeries deben tener autorización especial *AUDIT para verificar las firmas de objetos.

Pasos de las tareas

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

Pasos de las tareas del iSeries A

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

1. Complete todos los pasos prerrequisito para instalar y configurar todos los productos de iSeries necesarios.
2. Utilice el Gestor de certificados digitales (DCM) para crear una Autoridad certificadora (CA) local para emitir un certificado de firma de objetos.

3. Utilice el DCM para crear una definición de aplicación.
4. Utilice el DCM para asignar un certificado a la definición de aplicación de firma de objetos.
5. Utilice el DCM para firmar los objetos de programa cgi-bin.
6. Utilice el 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. Transfiera los archivos de certificados al servidor iSeries público de la empresa (iSeries B) para que tanto usted como otras personas puedan verificar las firmas que cree el iSeries A.

Pasos de las tareas del iSeries B

Si tiene pensado restaurar los objetos firmados que transfiera al servidor Web público de este caso práctico (iSeries B), deberá completar estas tareas de configuración de la verificación de firmas en el iSeries 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 iSeries B, debe completar estas tareas para verificar las firmas de objetos como describe este caso práctico:

8. Utilice el Gestor de certificados digitales (DCM) para crear el almacén de certificados *SIGNATUREVERIFICATION.
9. Utilice el DCM para importar el certificado de CA local y el certificado de verificación de firmas.
10. Utilice el DCM para verificar las firmas de los objetos transferidos.

Detalles de la configuración

Complete los siguientes pasos de las tareas para configurar y utilizar el Gestor de certificados digitales 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 iSeries necesarios para poder realizar tareas de configuración específicas para implementar 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:

1. Inicie el 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 deberán confiar en la CA local.

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

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.

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 deberá 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, (iSeries 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 (iSeries 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, podría entrar `/mydirectory/*` ; para firmar todos los programas de una biblioteca específica, podría entrar `/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, deberá entrar el comodín como parte del nombre de vía de acceso antes de pulsar en **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 iSeries B. También debe completar todas las tareas de configuración de la verificación de firmas en el iSeries B antes de transferir los objetos de programa firmados al iSeries B. La configuración de la verificación de firmas debe completarse para poder verificar firmas satisfactoriamente a medida que restaura los objetos firmados en el iSeries B.

Paso 6: Exportar certificados para habilitar la verificación de firmas en el iSeries 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 (iSeries 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 (iSeries 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 (iSeries 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 los 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 iSeries de punto final en los que tiene pensado verificar las firmas que cree con el certificado.

Paso 7: Transferir archivos de certificados al servidor público de la empresa iSeries B

Debe transferir los archivos de certificados que ha creado en el iSeries A al iSeries 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, podría 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 iSeries B (el servidor Web público de la empresa), el iSeries 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 el 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 exportaron ambos certificados a un archivo y se transfirió dicho archivo a cada sistema iSeries de punto final.

Para importar estos certificados al almacén *SIGNATUREVERIFICATION, siga estos pasos:

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.

Ahora puede utilizar el DCM en el iSeries B para verificar firmas de objetos que haya creado con el certificado de firmas correspondiente en el iSeries A.

Paso 10: Tareas de verificación de firmas: Verificar firmas de objetos de programas

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, podría entrar `/mydirectory/*`; para firmar todos los programas de una biblioteca específica, podría entrar `/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, deberá entrar el comodín como parte del nombre de vía de acceso antes de pulsar en **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 API para firmar objetos y verificar firmas de objetos

Situación

Su empresa (MyCo, Inc.) es un business partner de iSeries 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 utilizar programas para empaquetar una aplicación. Los clientes pueden solicitar un compact disc (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 de iSeries, 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 OS/400 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 asegurda que la verificación de firmas es transparente para el cliente.

Objetivos

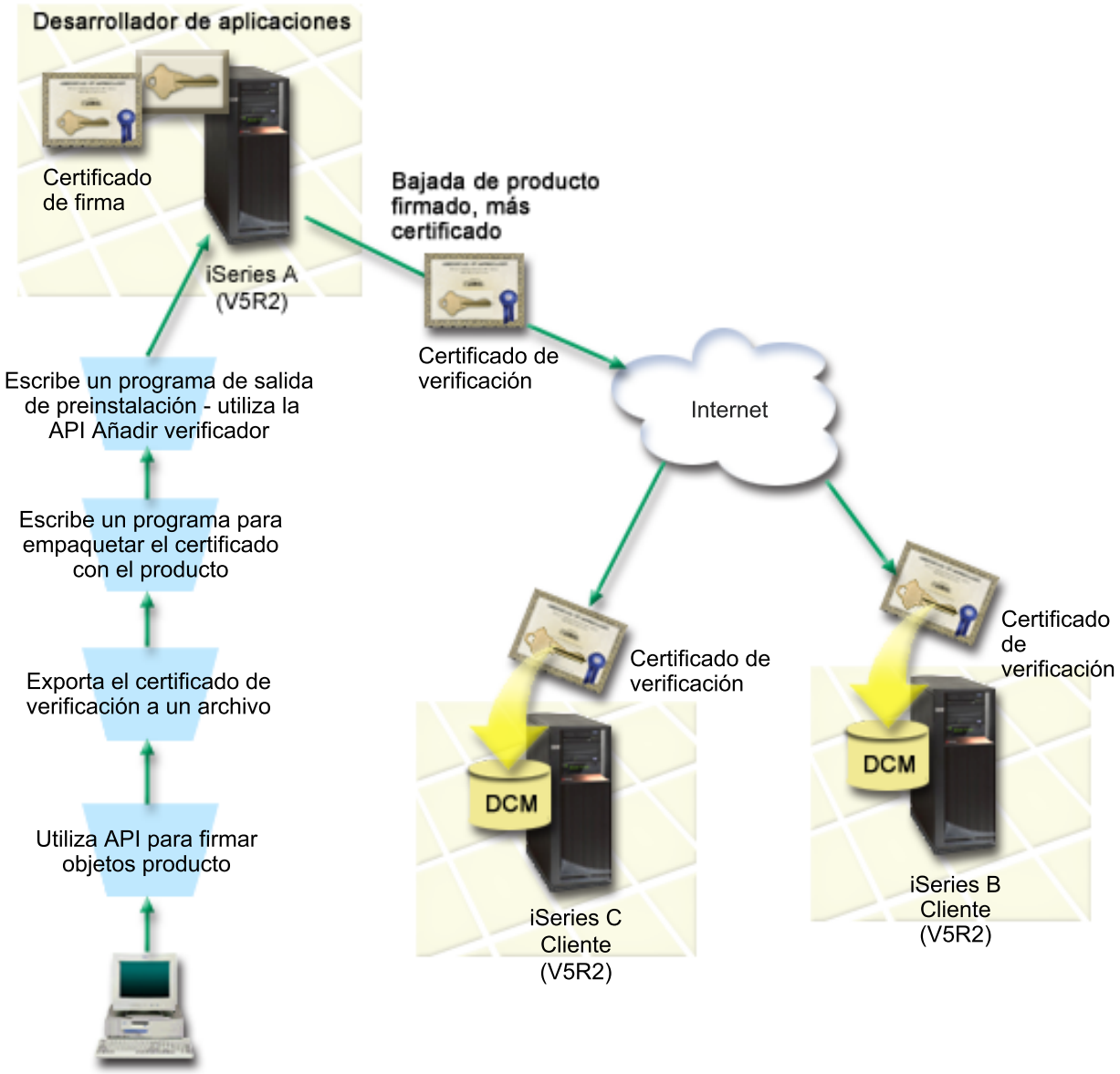
En este caso práctico, MyCo, Inc. desea firmar de forma programática las aplicaciones que empaqueta y distribuye a sus clientes. Como desarrollador de producción de aplicaciones en MyCo, Inc., actualmente empaqueta las aplicaciones de su empresa de forma programática para la distribución a clientes. Consecuentemente, le interesa utilizar las API de iSeries para firmar sus aplicaciones y que el iSeries 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 iSeries para añadir de forma programática el certificado de verificación de firmas necesario al almacén de certificados *SIGNATUREVERIFICATION del servidor iSeries del cliente. La empresa debe poder crear de forma programática este almacén de certificados en el servidor iSeries 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 (iSeries A)

- El iSeries A ejecuta OS/400 Versión 5 Release 2 (V5R2).
- El iSeries A ejecuta el programa de empaquetado de productos del desarrollador de aplicaciones.
- El iSeries A tiene instalado un Cryptographic Access Provider de 128 bits para iSeries (5722–AC3).
- El iSeries A tiene instalados y configurados el Gestor de certificados digitales (opción 34 de OS/400) y el Servidor HTTP IBM (5722–DG1).
- El iSeries 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 consigue en el iSeries A realizando 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 servidor iSeries del cliente (iSeries B y C).

Servidores iSeries de cliente B y C

- El iSeries B ejecuta OS/400 Versión 5 Release 2 (V5R2).
- El iSeries C ejecuta OS/400 Versión 5 Release 2 (V5R2).
- Los iSeries B y C tienen instalados y configurados el Gestor de certificados digitales (opción 34) y el Servidor HTTP IBM (5722–DG1).
- Los iSeries B y C adquieren y bajan una aplicación del sitio Web de la empresa de desarrollo de aplicaciones (propietaria del iSeries A).
- Los iSeries 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 los servidores iSeries de este cliente.

Requisitos previos y presuposiciones

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

1. Todos los servidores iSeries 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 (iSeries 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 servidores iSeries.
3. Todos los servidores iSeries 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 restauración (QVFYOBJRST) en todos los servidores iSeries de los casos prácticos como 3 y no se ha cambiado. El valor por omisión asegura que el servidor puede verificar firmas de objetos a medida que se restauran los objetos firmados.
5. El administrador de la red para el iSeries 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 servidores iSeries deben tener la autorización especial de perfil de usuario *AUDIT para verificar las firmas de objetos.

Pasos de las tareas

Debe completar cada una de estas tareas en el iSeries A para firmar objetos como describe este caso práctico:

1. Complete todos los pasos prerrequisito para instalar y configurar todos los productos de iSeries necesarios.

2. Utilice el DCM para crear una petición de certificado para obtener un certificado de firma de objetos de una Autoridad certificadora (CA) pública conocida.
3. Utilice el DCM para crear una definición de aplicación de firma de objetos.
4. Utilice el DCM para importar el certificado de firma de objetos firmados y asignarlo a su definición de aplicación de firma de objetos.
5. Utilice el DCM para exportar el certificado de firma de objetos como un certificado de verificación de firmas de forma que los clientes puedan utilizarlo para verificar la firma de los objetos de aplicación.
6. Reescriba el programa de empaquetado de aplicaciones para que incluya el archivo de certificados de verificación de firmas como parte del producto y para utilizar la API Firmar objeto para firmar la aplicación al empaquetarla para la distribución a clientes.
7. Cree 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 servidor iSeries de un cliente durante la instalación del producto.
8. Haga que los clientes utilicen el DCM para restablecer la contraseña por omisión para el almacén de certificados *SIGNATUREVERIFICATION en su servidor iSeries.

Detalles de la configuración

Complete los siguientes pasos de las tareas para utilizar las API de OS/400 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 iSeries necesarios para poder realizar tareas de configuración específicas para implementar 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 el 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 en **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 deberá 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, podrá 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 el 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 OS/400. 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 servidor iSeries que vaya a instalar las aplicaciones firmadas. Los servidores iSeries de los clientes deberán poder entonces 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, podría crear un programa de salida de preinstalación que llame a la API Añadir verificador para configurar el servidor iSeries del cliente.

Paso 5: Exportar certificados para permitir la verificación de firmas en otros servidores iSeries

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 (iSeries 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 entonces verificar la firma de los objetos de la aplicación a medida que los restaura en los servidores iSeries del cliente.

Paso 6: Actualizar el programa de empaquetado de aplicaciones para utilizar las API de iSeries 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: IBM le otorga una licencia de copyright no exclusiva para utilizar todos los ejemplos de código de programación, a partir de los cuales puede generar funciones similares adaptadas a sus necesidades específicas. IBM proporciona los códigos de ejemplo con finalidades únicamente ilustrativas. Estos ejemplos no han sido probados exhaustivamente bajo todas las condiciones. IBM, por consiguiente, no puede garantizar ni implicar la fiabilidad, servicio o funcionamiento de estos programas. Todos los programas aquí contenidos se le ofrecen ″TAL CUAL″ sin garantías de ningún tipo. Las garantías implícitas de no vulneración, comercialización e idoneidad para una finalidad determinada se niegan de forma expresa.

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. 2002                                  */
/*                                                               */
/* Utilizar API Firmar objeto para firmar una o varias bibliotecas  */
/*                                                               */
/* La API firmará digitalmente todos los objetos de una biblioteca  */
/* especificada                                                  */
/*                                                               */
/*                                                               */
/* Este material contiene código fuente de programación para su     */
/* consideración.  Este ejemplo no se ha probado exhaustivamente    */
/* bajo todas las condiciones. IBM, por consiguiente, no puede      */
/* garantizar ni implicar la fiabilidad, servicio o funcionamiento  */
/* de estos programas. Todos los programas aquí contenidos se le    */
/* proporcionan "TAL CUAL". LAS GARANTÍAS IMPLÍCITAS DE             */
/* COMERCIALIZACIÓN E IDONEIDAD PARA UNA FINALIDAD DETERMINADA SE   */
/* NIEGAN DE FORMA EXPRESA. IBM no proporciona servicios de         */
/* programa para estos programas y archivos.                     */
/*                                                               */
/*                                                               */
/*                                                               */
/* 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 parametro 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 una 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, podría 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 servidor iSeries 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, deberá considerar el 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: IBM le otorga una licencia de copyright no exclusiva para utilizar todos los ejemplos de código de programación, a partir de los cuales puede generar funciones similares adaptadas a sus necesidades específicas. IBM proporciona los códigos de ejemplo con finalidades únicamente ilustrativas. Estos ejemplos no han sido probados exhaustivamente bajo todas las condiciones. IBM, por consiguiente, no puede garantizar ni implicar la fiabilidad, servicio o funcionamiento de estos programas. Todos los programas aquí contenidos se le ofrecen ″TAL CUAL″ sin garantías de ningún tipo. Las garantías implícitas de no vulneración, comercialización e idoneidad para una finalidad determinada se niegan de forma expresa.

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 servidor iSeries del cliente al instalar el producto.

```
/* ------------------------------------------------------------- */
/*                                                               */
/* COPYRIGHT (C) IBM CORP. 2002                                  */
/*                                                               */
/* Utilizar la API Añadir verificador para añadir un certificado    */
/* del archivo IFS 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   */
/* por omisión que deberá cambiarse mediante DCM lo antes posible.  */
/* Debe darse este aviso a los propietarios del sistema que utiliza */
/* este programa.                                                   */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Este material contiene código fuente de programación para su     */
/* consideración.  Este ejemplo no se ha probado exhaustivamente    */
/* bajo todas las condiciones. IBM, por consiguiente, no puede      */
/* garantizar ni implicar la fiabilidad, servicio o funcionamiento  */
/* de estos programas. Todos los programas aquí contenidos se le    */
/* proporcionan "TAL CUAL". LAS GARANTÍAS IMPLÍCITAS DE             */
/* COMERCIALIZACIÓN E IDONEIDAD PARA UNA FINALIDAD DETERMINADA SE   */
/* NIEGAN DE FORMA EXPRESA. IBM no proporciona servicios de         */
/* programa para estos programas y archivos.                        */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Los parámetros son:                                              */
/*                                                                  */
/*  char *   nombre de vía al archivo IFS que tiene 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 servidor iSeries 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 el 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 para firmar objetos

Situación

Su empresa (MyCo, Inc.) desarrolla aplicaciones que luego distribuye a múltiples servidores iSeries en múltiples ubicaciones dentro de la empresa. Como administrador de la red, usted es responsable de asegurar que estas aplicaciones están instaladas y actualizadas en todos los servidores iSeries de la empresa. Actualmente utiliza la función Management Central de iSeries Navigator para empaquetar y distribuir más fácilmente estas aplicaciones y para realizar otras tareas administrativas de las que es 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.

Investigando las posibilidades de firma de objetos de OS/400 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 servidores iSeries.

Ventajas del caso práctico

Este caso práctico tiene las siguientes ventajas:

- Utilizar Management Central para empaquetar y firmar objetos reduce el período de tiempo que debe emplear para distribuir objetos firmados a los servidores iSeries 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

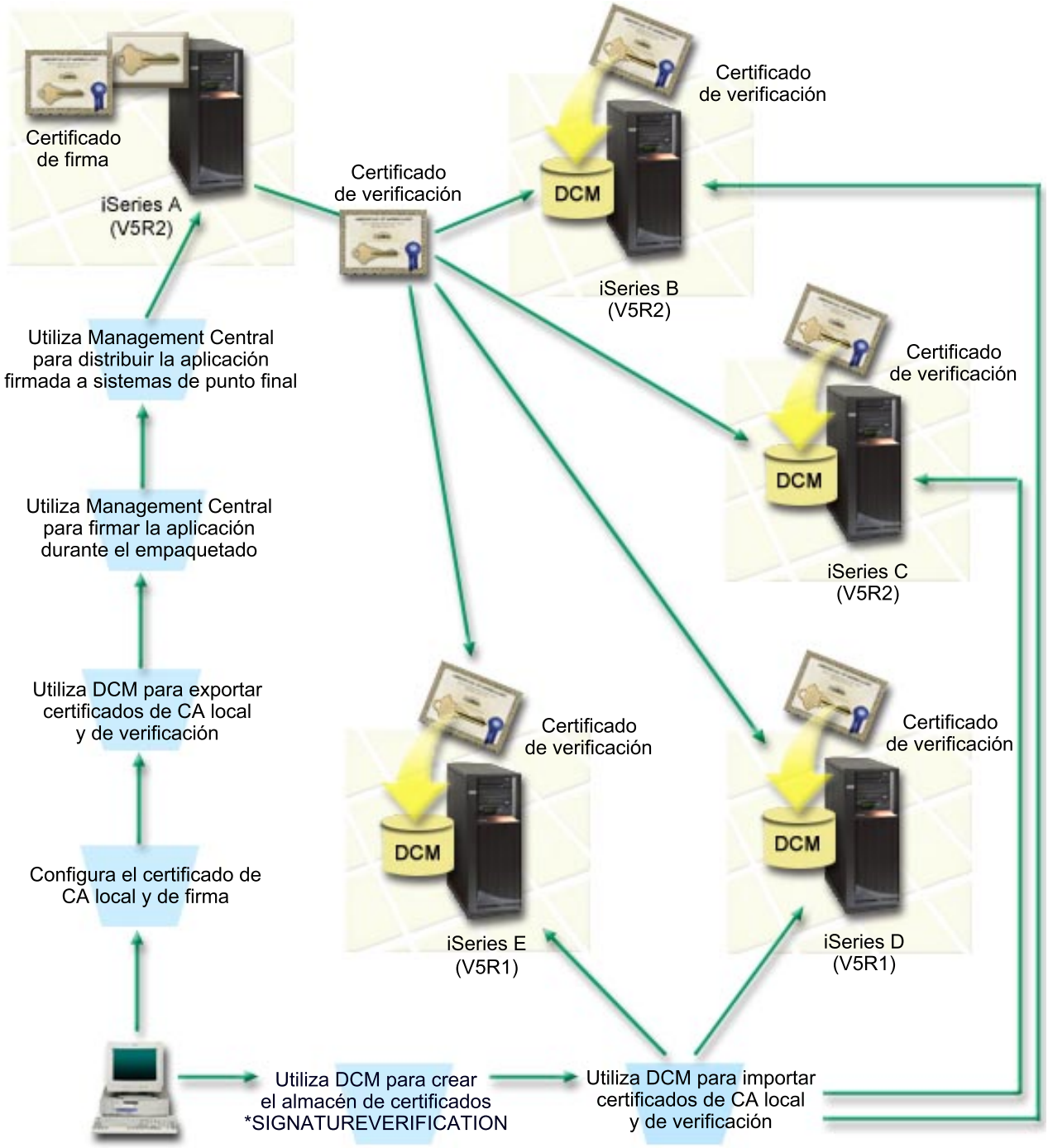
En este caso práctico, MyCo, Inc. desea firmar digitalmente aplicaciones que distribuirá a múltiples servidores iSeries dentro de la empresa. Como administrador de la red en MyCo, Inc., ya utiliza Management Central para diversas tareas administrativas del iSeries. Consecuentemente, desea ampliar el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

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 servidores iSeries para verificar el origen y la autenticidad de los objetos firmados por la empresa. Para logralo, cada servidor iSeries 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.
- Verificar las firmas de las aplicaciones de la empresa permite a los administradores de iSeries 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 servidores iSeries.

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(iSeries A)

- El iSeries A ejecuta OS/400 Versión 5 Release 2 (V5R2).
- El iSeries 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 iSeries A tiene instalado un Cryptographic Access Provider de 128 bits para iSeries (5722–AC3).

- El iSeries A tiene instalados y configurados el Gestor de certificados digitales (opción 34 de OS/400) y el Servidor HTTP IBM (5722–DG1).
- El iSeries A actúa como Autoridad certificadora (CA) local y el certificado de firma de objetos reside en este sistema.
- El iSeries 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 consigue en el iSeries A realizando 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 (iSeries 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 (servidores iSeries B, C, D y E)

- Los iSeries B y C ejecutan OS/400 Versión 5 Release 2 (V5R2).
- Los iSeries D y E ejecutan OS/400 Versión 5 Release 1 (V5R1).
- Los iSeries B, C, D y E tienen instalados y configurados el Gestor de certificados digitales (opción 34) y el Servidor HTTP IBM (5722–DG1).
- Los iSeries 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 (iSeries 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 servidores iSeries 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 servidores iSeries.
3. El iSeries A cumple los requisitos para instalar y utilizar iSeries Navigator y Management Central.
4. El servidor de Management Central debe ejecutarse en todos los sistemas iSeries de punto final.
5. Todos los servidores iSeries 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 restauración (QVFYOBJRST) en todos los servidores iSeries de los casos prácticos como 3 y no se ha cambiado. El valor por omisión asegura que el servidor puede verificar firmas de objetos a medida que se restauran los objetos firmados.
7. El administrador de la red para el iSeries 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 servidores iSeries deben tener la autorización especial de perfil de usuario *AUDIT para verificar las firmas de objetos.

Pasos de las tareas

Existen dos conjuntos de tareas que debe completar para implementar este caso práctico: Un conjunto de tareas le permite configurar el iSeries 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 servidores iSeries.

Pasos de la tareas de firma de objetos

Debe completar cada una de estas tareas en el iSeries A para firmar objetos como describe este caso práctico:

1. Complete todos los pasos prerrequisito para instalar y configurar todos los productos de iSeries necesarios.
2. Utilice el Gestor de certificados digitales (DCM) para crear una Autoridad certificadora (CA) local para emitir un certificado de firma de objetos privado.
3. Utilice el DCM para crear una definición de aplicación.
4. Utilice el DCM para asignar un certificado a la definición de aplicación de firma de objetos.
5. Utilice el 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. Transfiera los archivos de certificados a cada sistema iSeries de punto final en el que tenga intención de verificar firmas.
7. Utilice Management Central para firmar los objetos de aplicaciones.

Pasos de las tareas de verificación de firmas

Deberá completar estas tareas de configuración de la verificación de firmas en cada sistema iSeries 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 iSeries de punto final, debe completar estas tareas para verificar firmas de objetos como describe este caso práctico:

8. Utilice el Gestor de certificados digitales (DCM) para crear el almacén de certificados *SIGNATUREVERIFICATION.
9. Utilice el DCM para importar el certificado de CA local y el certificado de verificación de firmas.

Detalles de la configuración

Complete los siguientes pasos de las tareas para configurar Management Central 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 iSeries necesarios para poder realizar tareas de configuración específicas para implementar 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:

1. Inicie el 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 deberán confiar en la CA local.

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

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.

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 deberá 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 iSeries de punto final. También deberá completar todas las tareas de configuración de la verificación de firmas en cada sistema iSeries 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 permitir la verificación de firmas en otros sistemas iSeries

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 (iSeries 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 los 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 iSeries de punto final en los que tiene pensado verificar las firmas que cree con el certificado.

Paso 6: Transferir archivos de certificados a sistemas iSeries de punto final

Debe transferir los archivos de certificados que ha creado en el iSeries A a los sistemas iSeries 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, podría 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 la verificación de firmas en cada sistema iSeries 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 iSeries 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 iSeries de punto final

Para verificar firmas de objetos en los sistemas iSeries 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 el 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 exportaron ambos certificados a un archivo y se transfirió dicho archivo a cada sistema iSeries de punto final.

Para importar estos certificados al almacén *SIGNATUREVERIFICATION, siga estos pasos:

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.

Ahora, su sistema iSeries podrá verificar las firmas de objetos que se crearon con el certificado de firma correspondiente cuando restaura los objetos firmados.

Conceptos sobre la firma de objetos

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

Firmas digitales
Descubra qué son las firmas digitales y qué protección proporcionan.

Objetos firmables
Descubra qué objetos de iSeries puede firmar y las opciones de firma de objetos mandato (*CMD).

Proceso de firma de objetos
Descubra cómo funciona el proceso de firma de objetos y qué parámetros puede definir para el proceso.

Proceso de verificación de firmas
Descubra cómo funciona el proceso de verificar la firma de un objeto y qué parámetros puede definir para el proceso.

Firmas digitales

OS/400 proporciona soporte para el uso de certificados digitales para ″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 amplía las herramientas tradicionales del servidor iSeries para controlar quién puede modificar 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 el utilizar certificados de una Autoridad certificadora (CA) pública conocidad 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.

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 cubre todos los bytes del objeto excepto unos pocos bytes no esenciales.
- **Firmas de núcleo de objeto**
  Este tipo de firma cubre los bytes esenciales del objeto *CMD. Sin embargo, la firma no cubre 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 cubre varían según el objeto *CMD específico; las firmas de núcleo no cubren, 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.

Para aprender más cosas sobre los objetos de iSeries que puede firmar y qué bytes de un objeto *CMD cubre una firma de núcleo de objeto, vea Objetos firmables.

Objetos firmables

Puede firmar digitalmente toda una serie de tipos de objetos OS/400, 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 (sólo archivo de salvar) y mandatos (*CMD).

Para firmar un objeto, éste debe residir en el sistema local. Por ejemplo, si opera un servidor Windows 2000 en un servidor xSeries integrado para iSeries, tendrá disponible el sistema de archivos QNTC en el sistema de archivos integrado. No se considera que los directorios de este sistema de archivos sean 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 a aplicar 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 cubre 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 cubren, 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 és 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
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

Parte del objeto	Relación con 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

Proceso de firma de objetos

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 la aplicación manejará 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

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, 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.

Requisitos previos de la firma de objetos y la verificación de firmas

Las posibilidades de firma de objetos y verificación de firmas de OS/400 le proporcionan un método potente adicional para controlar los objetos de su servidor iSeries. Para aprovechar estas posibilidades, debe cumplir los requisitos previos para poder utilizarlas.

Requisitos previos 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 iSeries 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 de iSeries que firme los objetos debe tener la autorización especial *ALLOBJ. El perfil de usuario de iSeries que cree el almacén de certificados *SIGNATUREVERIFICATION debe tener las autorizaciones especiales *SECADM y *ALLOBJ.

Requisitos previos 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 deberá 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 servidor principal iSeries de CA local para exportar una copia del certificado de CA local a un archivo. Entonces puede utilizar el DCM en el servidor iSeries de verificación destino para importar el certificado de 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 conocimiento, considere el 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 iSeries que verifica firmas debe tener la autorización especial *AUDIT. El perfil de usuario de iSeries que crea el almacén de certificados *SIGNATUREVERIFICATION o cambia la contraseña del mismo debe tener las autorizaciones especiales *SECADM y *ALLOBJ.

Gestionar objetos firmados

A partir de la V5R1, IBM ha empezado a firmar los programas bajo licencia y los PTF de OS/400. 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 objetos firmados
Aprenda acerca de los valores del sistema y mandatos que puede utilizar para gestionar objetos firmados o que tienen un efecto sobre los objetos firmados al ejecutarlos.

Consideraciones sobre salvar y restaurar para objetos firmados
Descubra cómo los objetos firmados afectan a la manera de realizar las tareas de salvar y restaurar del sistema.

Mandatos de comprobador de código para asegurar la integridad de las firmas
Conozca detalles sobre el uso de mandatos para verificar firmas de objetos para determinar la integridad de los objetos.

Valores del sistema y mandatos que afectan a objetos firmados

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 iSeries. 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 OS/400, determina cómo los mandatos afectan a 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 de serie (*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 IFS.

Para conocer más detalles sobre el uso de este y otros valores del sistema, consulte System Value Finder en Information Center.

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 servidor iSeries. 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 manejará e informará 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 manejará e informará 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 (IFS). 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 servidor iSeries. 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. Deberá utilizar 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 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 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.

Consideraciones sobre salvar y restaurar para objetos firmados

Existen varios valores del sistema que pueden afectar a las operaciones de restauración de su servidor iSeries. 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. Deberá utilizar 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.

Deberá 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).

Para obtener más información sobre cómo afectan estos mandatos a los objetos firmados y a las firmas de objetos durante las operaciones de salvar y restaurar, consulte Valores del sistema y mandatos que afectan a objetos firmados.

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

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 han podido comprobarse 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.

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 se interrumpe. 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.

Resolución de problemas de objetos firmados

Puede utilizar las tablas siguientes para buscar información que le ayude a resolver algunos de los problemas más corrientes que puede encontrarse al trabajar con las posibilidades de firma de objetos y verificación de firmas de iSeries.

Problemas corrientes de firma de objetos

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).	iSeries 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.

Problemas corrientes de verificación de firmas

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. Un valor de 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 vez de ello, póngase en contacto con quien haya firmado el objeto para determinar la acción adecuada a llevar a cabo para resolver el problema.

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

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: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  Este libro rojo de IBM se centra en las mejoras de la seguridad de red de la V5R1. El libro rojo trata muchos temas, incluido cómo utilizar las posibilidades de firma de objetos de iSeries, el Gestor de certificados digitales (DCM) y otros.

Impreso en España