Guía del Usuario III

Encriptación de Backup de bibliotecas, objetos y archivos de IFS

Esta traducción está basada en la versión original de Linoma Software:
"Crypto Complete version: 3.30 Publication date: July 30th, 2013"

American Top Tools S.L. Tel. +34 933191612 Fax +34 933191755 att@att.es www.att.es

Nota ATT

La traducción del manual original se ha realizado para facilitar su uso en 4 documentos:

GUIA DEL USUARIO_I_Crypto Complete_Herramienta_de_Encriptación.pdf

GUIA DEL USUARIO_II_Crypto Complete_Encriptación_de_Campos.pdf

GUIA DEL USUARIO_III_Crypto Complete__Backup e IFS encriptados.pdf

GUIA DEL USUARIO_IV_Crypto Complete_Encriptación Automática carpetas IFS.pdf

La primera guía es básica, común y de obligada lectura para la utilización tanto del Módulo de Encriptación de Campos como del Módulo de Encriptación de Backup (de bibliotecas, objetos y archivos de la IFS) como del módulo de Encriptación Automática de carpetas IFS.

Guía del Usuario III - Backup e IFS encriptados

1. Introducción

Crypto Complete ofrece un módulo independiente para la encriptación de **Backup** (cinta) nativa para los usuarios de IBM i (AS/400,iSeries) que desean proteger sus dispositivos de Backup de datos sensibles. La encriptación la proporcionan una serie de mandatos de Crypto Complete que permiten encriptar y salvar bibliotecas completas u objetos individualmente.

El módulo de encriptación de la **IFS** de Crypto Complete permite a los usuarios de IBM i (AS/400) encriptar y desencriptar archivos y directorios de la IFS. Cualquier tipo de archivo de la IFS puede ser encriptado, incluidos los archivos del tipo TXT, PDF, JPG, TIF, CSV y XLS. Crypto Complete proporciona mandatos de encriptación y desencriptación de la IFS nativos, los cuales pueden integrarse fácilmente en las aplicaciones y procesos del IBM i.

En ambos casos, se utilizarán claves simétricas o de passphrase(*) para proteger los datos de la copia de seguridad.

(*) Passphrase: Una cadena de palabras y caracteres que usted introduce para autentificarse. Se diferencian de los passwords en su mayor longitud. A mayor longitud mayor seguridad. Actúa como una contraseña

Se implementa la encriptación AES para proporcionar una mayor seguridad en los Backup. El sistema AES sigue las especificaciones estándar (no propietarias) publicadas por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST). Crypto Complete trabaja con longitudes de clave de AES128, AES192 y AES256. La encriptación de Backup (cinta) del IBMi que proporciona el Crypto Complete permite cumplir adecuadamente con los requisitos del PCI DS, leyes de protección de datos del estado y regulaciones federales como HIPAA y Sarbanes-Oxley.

Otras ventajas son:

- Crypto Complete es una solución de software puro que no requiere de hardware adicional.
- Permite utilizar los dispositivos de cinta actuales.
- Permite alojar la información encriptada en: cinta, dispositivo virtual o físico e IFS.
- Integración rápida de los mandatos de Backup e IFS en sus procesos actuales de Backup.
- Encripta bibliotecas completas u objetos seleccionados individualmente.
- No genera Save Files intermedios ahorrando espacio en disco y tiempo.
- Incorpora un sistema de gestión de claves que reside en el IBM i.
- Las etiquetas de las claves se almacenan conjuntamente con el Backup encriptado, así como en los archivos de IFS encriptados, de modo que no se tiene que recordar que clave se debe utilizar en la desencriptación/restauración del Backup.
- La recuperación de datos en caso de un incidente grave se simplifica al no necesitar de dispositivos especiales para su restauración.
- Sólo los usuarios autorizados pueden tener permiso para desencriptar archivos de la IFS.
- En el caso de la IFS, permite nombres de archivo así como wildcards (*.pdf) para encriptar uno o más archivos de IFS a la vez.

Los mandatos de encriptación y de restauración de Backup o de IFS del Crypto Complete se pueden introducir en la línea de mandatos del AS/400, en un programa CL, incorporados en un BRMS y utilizados en los planificadores de trabajos del IBM i.

A continuación mostramos alguna de las pantallas principales del módulo de Backup.

```
CRYPTO5              Library/Object/File Encryption Menu


Select one of the following:

  1. Encrypt Library         (ENCSAVLIB)
  2. Decrypt Library         (DECRSTLIB)

  3. Encrypt Object          (ENCSAVOBJ)
  4. Decrypt Object          (DECRSTOBJ)

  5. Encrypt Save File       (ENCSAVF)
  6. Decrypt Save File       (DECSAVF)

  7. Encrypt File            (ENCFIL)
  8. Decrypt File            (DECFIL)


 Selection or command
===>_____________________________________________________________________
_____________________________________________________________________

 F3=Exit    F4=Prompt    F9=Retrieve    F12=Cancel
 F13=Information Assistant  F16=AS/400 main menu
```

Menú de Backup Encryption

```
                      Encrypt Library (ENCSAVLIB)

Type choices, press Enter.

Library  . . . . . . . . . . . . > PAYROLL     Name, generic*, *ALL
             + for more values > GLDATA
Device . . . . . . . . . . . . . > TAP01       Name, *IFS
Volume identifier  . . . . . . .   *MOUNTED
Sequence number  . . . . . . . .   *END         1-16777215, *END
Label  . . . . . . . . . . . . .   *LIB
File expiration date . . . . . .   *PERM        Date, *PERM
End of media option  . . . . . .   *REWIND      *REWIND, *LEAVE, *UNLOAD
Target release . . . . . . . . .   *CURRENT     *CURRENT, *PRV, VxRxMx
Update history . . . . . . . . .   *YES         *NO, *YES
Clear  . . . . . . . . . . . . .   *NONE        *NONE, *ALL, *AFTER, *REPLACE
Object pre-check . . . . . . . .   *NO          *NO, *YES
Save active  . . . . . . . . . .   *NO          Name, *NO, *LIB, *SYSDFN
Save active wait time  . . . . .   120          0-99999, *NOMAX
Save active message queue  . . .   *NONE        Name, *NONE, *WRKSTN
  Library  . . . . . . . . . . .     *LIBL      Name, *LIBL, *CURLIB
Save access paths  . . . . . . .   *NO          *NO, *YES
ASP device . . . . . . . . . . .   *            Name, *, *SYSBAS, *CURASPGRP
Algorithm  . . . . . . . . . . .   *AES256      *AES256, *AES192, *AES128
Use key or password  . . . . . .   *KEY         *KEY, *PASS
Key label  . . . . . . . . . . .   BACKUPKEY
Key store name . . . . . . . . .   *DEFAULT     Name, *DEFAULT
  Library  . . . . . . . . . . .     *LIBL      Name, *LIBL
Store key label  . . . . . . . .   *YES         *NO, *YES

F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Ejemplo del mandato ENCSAVLIB para encriptar y salvar bibliotecas

…. y éste es un ejemplo del mandato ENCSTMF para encriptar archivos de la IFS.

```
                    Encrypt IFS Stream File (ENCSTMF)

Type choices, press Enter.

From stream file:
  IFS File . . . . . .  '/sensitivefiles/*'
  Include or omit  . . .  *INCLUDE       *INCLUDE, *OMIT
            + for more values
Name pattern:
  Pattern  . . . . . .  '*'
  Include or omit  . . .  *INCLUDE       *INCLUDE, *OMIT
            + for more values
Directory subtree  . . . . . .  *ALL          *ALL, *DIR, *NONE, *OBJ, *STG
To type  . . . . . .  . . . . .  *DEV         *STMF, *DEV
To device  . . . . . .  . . . .  TAP01        Name
Device volume identifier . . . .  *MOUNTED
Device sequence number . . . . .  *END        1-16777215, *END
Device label . . . . . .  . . .  ENCSTMF
Device file expiration date  . .  *PERM       Date, *PERM
Device end of media option . . .  *REWIND     *REWIND, *LEAVE, *UNLOAD
Target release . . . . . .  . .  *CURRENT    *CURRENT, *PRV, VxRxMx
Update history . . . . . .  . .  *YES        *NO, *YES
Object pre-check . . . . . .  .  *NO         *NO, *YES
Save active  . . . . . .  . . .  *NO         Name, *NO, *LIB, *SYSDFN
Save active wait time  . . . . .  120        0-99999, *NOMAX
Save active message queue  . . .  *NONE
ASP device . . . . . .  . . . .  *           Name, *, *SYSBAS,
Algorithm  . . . . . .  . . . .  *AES256     *AES256, *AES192, *AES128
Use key or password  . . . . . .  *KEY       *KEY, *PASS
Key label  . . . . . .  . . . .  BACKUPKEY
Key store name . . . . . .  . .  *DEFAULT    Name, *DEFAULT
  Library  . . . . . .  . . . .    *LIBL      Name, *LIBL
Store key label  . . . . . .  .  *YES        *NO, *YES
```

Ejemplo mandato para encriptar archivos de la IFS

2. Encriptación de Bibliotecas, Objetos y Archivos IFS

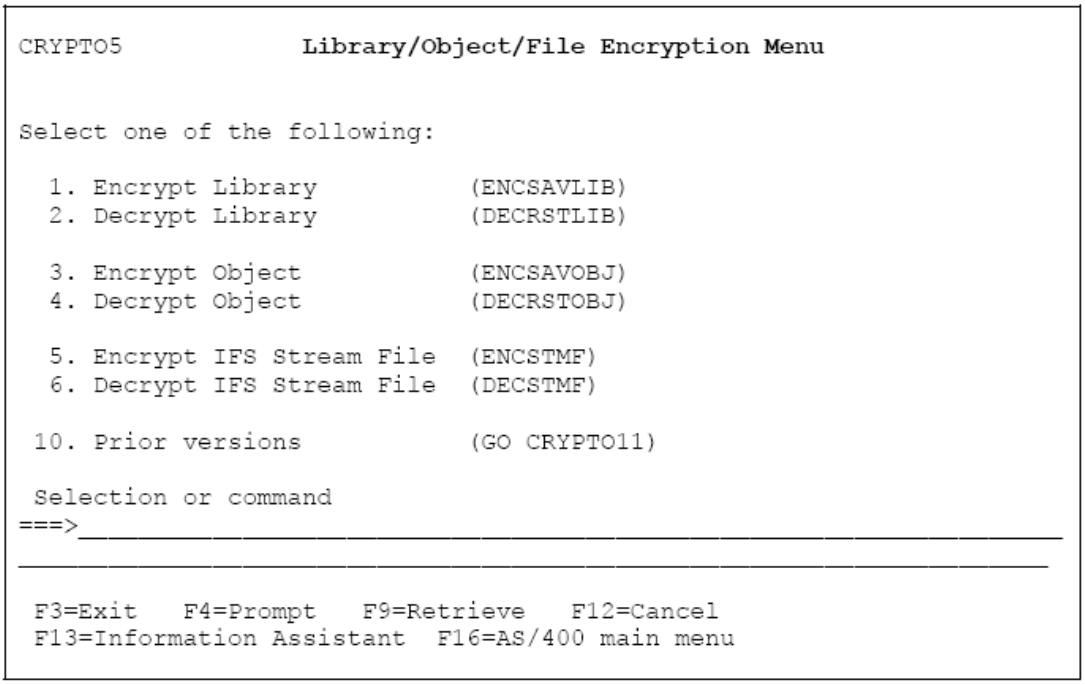
Crypto Complete proporciona mandatos para la encriptación y salvado de bibliotecas, objetos y archivos IFS. Los datos encriptados pueden ser salvados en un dispositivo o disco.

Los usuarios pueden escoger entre los algoritmos de encriptación AES128, AES192 and AES256. Se utilizarán claves simétricas o contraseñas para proteger los datos encriptados.

También se facilitan mandatos para restaurar y desencriptar bibliotecas, objetos y archivos siempre que hayan sido encriptados con mandatos de encriptación de Crypto Complete. Estos mandatos pueden introducirse en la línea de mandatos, en programas CL, en un paquete BRMS(*) y en el planificador de trabajos del IBM i.

Nota: (*) Los clientes de BRMS que deseen incorporar los mandatos de encriptación de Backup a su paquete BRMS, deben contactar con su proveedor para más instrucciones.

Para ver la lista de los mandatos de encriptación y desencriptación disponibles, ejecute el mandato GO CRYPTO/CRYPTO5 y accederá al Menú de Encriptación de Bibliotecas, Objetos y Archivos. Cualquier mandato que aparece puede ser ejecutado mediante la opción de menú o bien ejecutando el mandato que aparece junto a cada opción del menú en la línea de mandatos.



Menú de Encriptación de bibliotecas, objetos y archivos

2.1 Mandatos para Backup de Bibliotecas

a) Encriptar Bibliotecas - (ENCSAVLIB)

El mandato **ENCSAVLIB** permite a los usuarios autorizados encriptar y salvar una copia de una o más bibliotecas a un dispositivo físico o virtual o bien a la IFS.

Los algoritmos de encriptación disponibles son AES128, AES192 y AES256. Puede utilizarse tanto una Clave Simétrica o bien una Contraseña para el proceso de encriptación

Realice los siguientes pasos para **encriptar bibliotecas:**

1. Introduzca el mandato **CRYPTO/ENCSAVLIB** y pulse F4.
2. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line
3. Pulse Intro tras añadir los parámetros.

```
                        Encrypt Library (ENCSAVLIB)

Type choices, press Enter.

Library  . . . . . . . . . . . . > PAYROLL___     Name, generic*, *ALL
             + for more values > GLDATA____
Device . . . . . . . . . . . . . > TAP01_____     Name, *IFS
Volume identifier  . . . . . . .   *MOUNTED_____________________
Sequence number  . . . . . . . .   *END________  1-16777215, *END
Label  . . . . . . . . . . . . .   *LIB_____________
File expiration date . . . . . .   *PERM_____    Date, *PERM
End of media option  . . . . . .   *REWIND       *REWIND, *LEAVE, *UNLOAD
Target release . . . . . . . . .   *CURRENT      *CURRENT, *PRV, VxRxMx
Update history . . . . . . . . .   *YES          *NO, *YES
Object pre-check . . . . . . . .   *NO           *NO, *YES
Save active  . . . . . . . . . .   *NO_____      Name, *NO, *LIB, *SYSDFN
Save active wait time  . . . . .   120________   0-99999, *NOMAX
Save active message queue  . . .   *NONE_____    Name, *NONE, *WRKSTN
  Library  . . . . . . . . . . .     *LIBL_____  Name, *LIBL, *CURLIB
Save access paths  . . . . . . .   *NO           *NO, *YES
ASP device . . . . . . . . . . .   *_________    Name, *, *SYSBAS, *CURASPGRP
Algorithm  . . . . . . . . . . .   *AES256       *AES256, *AES192, *AES128
Use key or password  . . . . . .   *KEY_         *KEY, *PASS
Key label  . . . . . . . . . . .   BACKUPKEY_____________________
Key store name . . . . . . . . .   *DEFAULT__    Name, *DEFAULT
  Library  . . . . . . . . . . .     *LIBL_____  Name, *LIBL
Store key label  . . . . . . . .   *YES          *NO, *YES

F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Ejemplo del mandato ENCSAVLIB y valores de muestra

El mandato ENCSAVLIB salva:

- Caso General: la **biblioteca completa** incluyendo:
  - la descripción de la biblioteca
  - las descripciones de los objetos
  - los contenidos de los objetos de la biblioteca.

Nota: Las bibliotecas y objetos no resultan afectados para nada en el sistema.

- Caso Particular: De los objetos como colas de trabajo, colas de mensaje, colas de salida y archivos lógicos **sólo se salvan las definiciones del objeto, no los contenidos.** Si bien las rutas de acceso de los archivos lógicos pueden salvarse si se especifica el parámetro ACCPTH.

Nota: Asegúrese de que el subsistema QSYSWRK está activo para que pueda funcionar el mandato ENCSAVLIB.

Control de errores

Si se ejecuta el mandato ENCSAVLIB dentro de un programa CL, puede capturar los errores controlando los ids. de los mensajes. Los ids de mensajes de error para el mandato ENCSAVLIB son:

CRE0712 - Library(s) were not encrypted. Review JOB LOG.
CRE3701 - &1 objects were saved; &2 objects were not saved.
CRE3751- Some Libraries not saved.

Auditoría

Si se utiliza una Clave Simétrica con el mandato ENCSAVLIB y estuviera habilitado el parámetro "Log encryption usage" (Registrar el uso de la encriptación) para la clave simétrica, se generará una entrada en el log de auditoría en el archivo de journal del Crypto Complete cada vez que la clave se utilice para encriptar.

Cada entrada de auditoría indicará la etiqueta y almacén de claves de la clave simétrica utilizada junto con el usuario, fecha, hora, número de trabajo y nombre del trabajo.

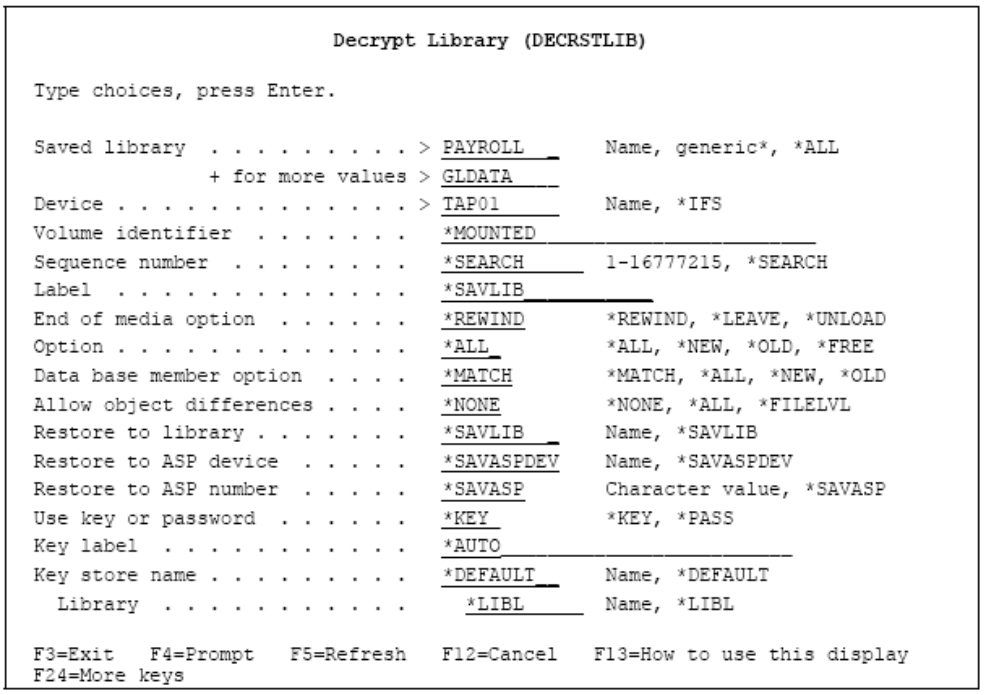
b) Desencriptar Bibliotecas - (DECRSTLIB)

El mandato **DECRSTLIB** permite a los usuarios autorizados **restaurar y desencriptar una o más bibliotecas** que fueron encriptadas con el mandato ENCSAVLIB.

Las bibliotecas pueden ser restauradas desde un dispositivo físico o virtual o de la IFS. Puede especificarse una clave simétrica o contraseña para el proceso de desencriptación.

Realice los siguientes pasos para **desencriptar bibliotecas:**

1. Introduzca el mandato **CRYPTO/DECRSTLIB** y pulse F4.
2. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line
3. Pulse Intro tras añadir los parámetros.



```
                        Decrypt Library (DECRSTLIB)

Type choices, press Enter.

Saved library  . . . . . > PAYROLL __    Name, generic*, *ALL
             + for more values > GLDATA___
Device . . . . . > TAP01_____    Name, *IFS
Volume identifier  . . . . . *MOUNTED_____________________
Sequence number  . . . . . *SEARCH_____  1-16777215, *SEARCH
Label  . . . . . *SAVLIB_____________
End of media option  . . . . . *REWIND       *REWIND, *LEAVE, *UNLOAD
Option . . . . . *ALL_          *ALL, *NEW, *OLD, *FREE
Data base member option  . . . . *MATCH        *MATCH, *ALL, *NEW, *OLD
Allow object differences . . . . *NONE         *NONE, *ALL, *FILELVL
Restore to library . . . . . *SAVLIB __    Name, *SAVLIB
Restore to ASP device  . . . . . *SAVASPDEV    Name, *SAVASPDEV
Restore to ASP number  . . . . . *SAVASP       Character value, *SAVASP
Use key or password  . . . . . *KEY_          *KEY, *PASS
Key label  . . . . . *AUTO_____________________
Key store name . . . . . *DEFAULT__    Name, *DEFAULT
  Library  . . . . . *LIBL_____  Name, *LIBL

F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Ejemplo del mandato DECRSTLIB y valores de muestra

El mandato DECRSTLIB restaura:

- Caso General: **la biblioteca completa** incluyendo:
  - la descripción de la biblioteca
  - la descripción de los objetos
  - los contenidos de los objetos de esa biblioteca.

Consideraciones:

- Si el perfil propietario ya no existiera en el sistema, el perfil de usuario QDFTOWN del sistema se convierte en el propietario por defecto de cualquier objeto que se haya restaurado en el sistema.
- Si un objeto ya existe en la biblioteca en que se va a restaurar, las autorizaciones públicas y privadas del objeto existente son retenidas. Si el objeto no existe en la biblioteca, todas las autorizaciones públicas son restauradas, pero las autorizaciones privadas se deben conceder de nuevo.
- Si un objeto se está restaurando sobre un objeto existente en el sistema, el valor de auditoría del objeto que corresponde al objeto existente se mantiene. Si el objeto está siendo restaurando como nuevo en el sistema, el valor de auditoría del objeto se restaurará con el valor que viene del dispositivo externo. Adicionalmente, si el objeto es una biblioteca, el valor de auditoría por defecto de cada objeto creado en la biblioteca será restaurado si la biblioteca se está restaurando como nueva, de otro modo, el valor de auditoría por defecto se restaurará con el valor que viene del dispositivo externo.

Nota: Asegúrese de que el subsistema QSYSWRK está activo para que pueda funcionar el mandato DECRSTLIB.

Control de Errores

Si se ejecuta el mandato DECRSTLIB dentro de un programa CL, puede capturar los errores controlando los ids. de los mensajes. Los ids de mensajes para el mandato DECRSTLIB son:

CRE0714 - Library(s) were not decrypted. Review JOB LOG.
CRE3773 - &1 objects restored. &2 not restored to &3.
CRE3779 - &1 Library(s) restored. &2 Library(s) were partially restored. &3 not restored.

Auditoría

Si se utiliza una Clave Simétrica con el mandato DECRSTLIB y estuviera habilitado el parámetro "Log decryption usage" (Registrar el uso de la desencriptación) para la clave simétrica, se generará una entrada en el log de auditoría en el archivo de journal del Crypto Complete cada vez que la clave se utilice para desencriptar.

Cada entrada de auditoría indicará la etiqueta y almacén de claves de la clave simétrica utilizada junto con el usuario, fecha, hora, número de trabajo y nombre del trabajo

2.2 Mandatos para Backup de Objetos

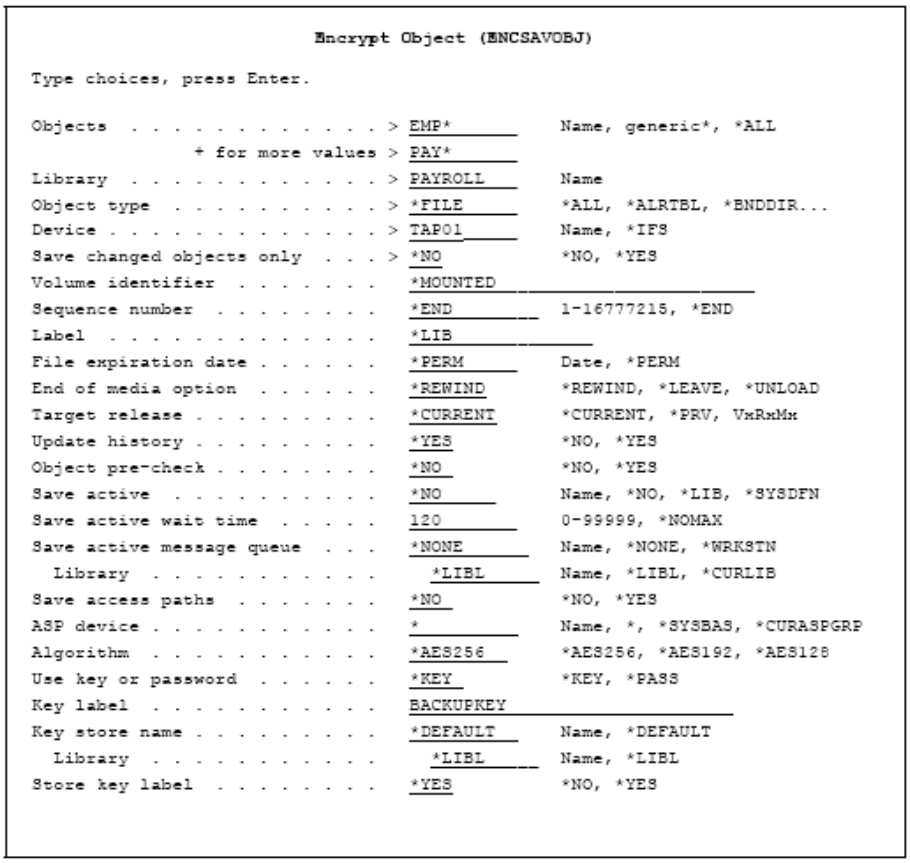
a) Encriptar Objetos - (ENCSAVOBJ)

El mandato **ENCSAVOBJ** permite a los usuarios autorizados encriptar y salvar uno o más objetos a un dispositivo físico o virtual o de la IFS.

Los algoritmos de encriptación disponibles son AES128, AES192 y AES256. Puede utilizarse tanto una Clave Simétrica o bien una contraseña para el proceso de encriptación

Realice los siguientes pasos para **encriptar objetos:**

1. Introduzca el mandato **CRYPTO/ENCSAVOBJ** y pulse F4.
2. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line
3. Pulse Intro tras añadir los parámetros.



```
                        Encrypt Object (ENCSAVOBJ)

Type choices, press Enter.

Objects  . . . . . > EMP*          Name, generic*, *ALL
             + for more values > PAY*
Library  . . . . . > PAYROLL       Name
Object type  . . . . . > *FILE     *ALL, *ALRTBL, *BNDDIR...
Device . . . . . > TAP01           Name, *IFS
Save changed objects only  . . . > *NO          *NO, *YES
Volume identifier  . . . . . *MOUNTED
Sequence number  . . . . . *END    1-16777215, *END
Label  . . . . . *LIB
File expiration date . . . . . *PERM       Date, *PERM
End of media option  . . . . . *REWIND     *REWIND, *LEAVE, *UNLOAD
Target release . . . . . *CURRENT  *CURRENT, *PRV, VxRxMx
Update history . . . . . *YES      *NO, *YES
Object pre-check . . . . . *NO     *NO, *YES
Save active  . . . . . *NO         Name, *NO, *LIB, *SYSDFN
Save active wait time  . . . . . 120       0-99999, *NOMAX
Save active message queue  . . . *NONE     Name, *NONE, *WRKSTN
  Library  . . . . . *LIBL         Name, *LIBL, *CURLIB
Save access paths  . . . . . *NO   *NO, *YES
ASP device . . . . . *             Name, *, *SYSBAS, *CURASPGRP
Algorithm  . . . . . *AES256       *AES256, *AES192, *AES128
Use key or password  . . . . . *KEY  *KEY, *PASS
Key label  . . . . . BACKUPKEY
Key store name . . . . . *DEFAULT  Name, *DEFAULT
  Library  . . . . . *LIBL         Name, *LIBL
Store key label  . . . . . *YES    *NO, *YES
```

Ejemplo del mandato ENCSAVOBJ y valores de muestra

- Caso General: El sistema salvará los objetos especificados realizando una copia de cada objeto. Los objetos no son alterados en el sistema. Sin embargo, la descripción de cada objeto se actualiza con la fecha, hora y lugar en que se salvó por última vez, a menos que se especifique *NO en el prompt de Update History (Actualizar historial), del parámetro UPDHST.

- Caso Particular: De los objetos como colas de trabajos, colas de mensajes, colas de salida y archivos lógicos, sólo se salvan las definiciones del objeto, no los contenidos. Las rutas de acceso de los archivos lógicos pueden salvarse si se utiliza el parámetro output ACCPTH.

Nota: Asegúrese de que el subsistema QSYSWRK está activo para que pueda funcionar el mandato ENCSAVOBJ.

Control de errores

Si se ejecuta el mandato ENCSAVOBJ dentro de un programa CL, puede capturar los errores controlando los ids. de los mensajes. Los ids de mensajes de error para el mandato ENCSAVOBJ son:

CRE0713 - Object(s) were not encrypted. Review JOB LOG.
CRE3701 - &1 objects were saved; &2 objects were not saved.

Auditoría

Si se utiliza una Clave Simétrica con el mandato ENCSAVOBJ y estuviera habilitado el parámetro “Log encryption usage” (Registrar el uso de la encriptación) para la clave simétrica, se generará una entrada en el log de auditoría en el archivo de journal del Crypto Complete cada vez que la clave se utilice para encriptar.

Cada entrada de auditoría indicará la etiqueta y almacén de claves de la clave simétrica utilizada junto con el usuario, fecha, hora, número de trabajo y nombre del trabajo.

b) Desencriptar Objetos - (DECRSTOBJ)

El mandato **DECRSTOBJ** permite a los usuarios autorizados **restaurar y desencriptar uno o más objetos** que fueron encriptados con el mandato ENCSAVOBJ o ENCSABLIB.

Los objetos pueden ser restaurados desde un dispositivo físico o virtual o de la IFS. Puede especificarse una clave simétrica o contraseña para el proceso de desencriptación.

Realice los siguientes pasos para **desencriptar objetos:**

1. Introduzca el mandato **CRYPTO/DECRSTOBJ** y pulse F4.
2. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line
3. Pulse Intro tras añadir los parámetros.

```
                        Decrypt Object (DECRSTOBJ)

Type choices, press Enter.

Objects  . . . . . > EMP*_____     Name, generic*, *ALL
             + for more values > PAY*_____
Saved library  . . . . . > PAYROLL___   Name
Object type  . . . . . *ALL_____    *ALL, *ALRTBL, *BNDDIR...
Device . . . . . > TAP01_____    Name, *IFS
Volume identifier  . . . . . *MOUNTED_____________________________
Sequence number  . . . . . *SEARCH_____  1-16777215, *SEARCH
Label  . . . . . ENCOBJ_____
End of media option  . . . . . *REWIND       *REWIND, *LEAVE, *UNLOAD
Option . . . . . *ALL        *ALL, *NEW, *OLD, *FREE
Data base member option  . . . . *MATCH      *MATCH, *ALL, *NEW, *OLD
Allow object differences . . . . *NONE       *NONE, *ALL, *FILELVL
Restore to library . . . . . *SAVLIB___   Name, *SAVLIB
Restore to ASP device  . . . . . *SAVASPDEV   Name, *SAVASPDEV
Restore to ASP number  . . . . . *SAVASP      Character value, *SAVASP
Use key or password  . . . . . *KEY          *KEY, *PASS
Key label  . . . . . *AUTO_____________________________
Key store name . . . . . *DEFAULT___   Name, *DEFAULT
  Library  . . . . . *LIBL_____   Name, *LIBL

F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Ejemplo del mandato DECRSTOBJ y valores de muestra

Los tipos de objeto que pueden restaurarse con este mandato están listados en el prompt de tipos de objeto (OBJTYPE parameter).

El mandato DECRSTOBJ restaura:

- Caso General: las descripciones del objeto y sus contenidos.

- Caso particular: Si se hubieran salvado rutas de acceso a archivos lógicos (Se especificó ACCPTH(*YES) cuando se salvaron los objetos) , estas rutas de acceso serán restauradas si:

  (1) todos los archivos físicos relacionados están siendo también restaurados con el mismo mandato de restauración
  (2) el archivo lógico también está siendo restaurado con el mismo mandato de restauración o bien el archivo lógico ya existe en el sistema (el mismo archivo, no una nueva versión)
  (3) MAINT(*IMMED o *DLY) está aún vivo para ese archivo lógico si todavía existe en el sistema.

Consideraciones:

- El perfil de usuario por defecto QDFTOWN se convertirá en propietario de aquellos objetos restaurados al sistema cuyo propietario original sea desconocido para el sistema.

- Si el objeto está siendo restaurado sobre un objeto ya existente en el sistema, el valor de auditoría del objeto del objeto existente se mantendrá. Si el objeto está siendo restaurado como nuevo para el sistema, el valor de auditoría del objeto será restaurado desde el dispositivo en que se salvó.

- Si se utiliza para restaurar un programa, la copia del programa que está actualmente en el sistema no debe estar ejecutándose cuando se realiza la restauración. Si se intentará, el programa en funcionamiento no sería restaurado.

Nota: Asegúrese de que el subsistema QSYSWRK está activo para que pueda funcionar el mandato DECRSTLIB.

Control de errores

Si se ejecuta el mandato DECRSTOBJ dentro de un programa CL, puede capturar los errores controlando los ids. de los mensajes. Los ids de mensajes de error para el mandato DECRSTOBJ son:

CRE0715 - Object(s) were not decrypted. Review JOB LOG.
CRE3773 - &1 Object(s) restored. &2 not restored to &3.

Auditoría

Si se utiliza una Clave Simétrica con el mandato DECRSTOBJ y estuviera habilitado el parámetro “Log decryption usage” (Registrar el uso de la desencriptación) para la clave simétrica, se generará una entrada en el log de auditoría en el archivo de journal del Crypto Complete cada vez que la clave se utilice para desencriptar.

Cada entrada de auditoría indicará la etiqueta y almacén de claves de la clave simétrica utilizada junto con el usuario, fecha, hora, número de trabajo y nombre del trabajo

2.3 Mandatos para archivos/directorios IFS

a) Encriptar Archivos Stream de la IFS - (ENCSTMF)

El mandato **ENCSTMF** permite a los usuarios autorizados encriptar archivos stream de la IFS a un dispositivo físico o virtual o a la IFS.

Los algoritmos de encriptación disponibles son AES128, AES192 y AES256. Puede utilizarse tanto una Clave Simétrica o bien una Contraseña para el proceso de encriptación

Realice los siguientes pasos para **encriptar archivos:**

1. Introduzca el mandato **CRYPTO/ENCSSTMF** y pulse F4.
2. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line
3. Pulse Intro tras añadir los parámetros.

```
                    Encrypt IFS Stream File (ENCSTMF)

Type choices, press Enter.

From stream file:
  IFS File . . . . . .  '/sensitivefiles/*'
  Include or omit  . . .  *INCLUDE       *INCLUDE, *OMIT
            + for more values
Name pattern:
  Pattern  . . . . . .  '*'
  Include or omit  . . .  *INCLUDE       *INCLUDE, *OMIT
            + for more values
Directory subtree  . . . . .  *ALL         *ALL, *DIR, *NONE, *OBJ, *STG
To type  . . . . . .  *DEV         *STMF, *DEV
To device  . . . . . .  TAP01       Name
Device volume identifier . . . .  *MOUNTED
Device sequence number . . . . .  *END         1-16777215, *END
Device label . . . . . .  ENCSTMF
Device file expiration date  . .  *PERM        Date, *PERM
Device end of media option . . .  *REWIND      *REWIND, *LEAVE, *UNLOAD
Target release . . . . . .  *CURRENT     *CURRENT, *PRV, VxRxMx
Update history . . . . . .  *YES         *NO, *YES
Object pre-check . . . . . .  *NO          *NO, *YES
Save active  . . . . . .  *NO          Name, *NO, *LIB, *SYSDFN
Save active wait time  . . . . .  120         0-99999, *NOMAX
Save active message queue  . . .  *NONE
ASP device . . . . . .  *           Name, *, *SYSBAS,
Algorithm  . . . . . .  *AES256      *AES256, *AES192, *AES128
Use key or password  . . . . . .  *KEY         *KEY, *PASS
Key label  . . . . . .  BACKUPKEY
Key store name . . . . . .  *DEFAULT     Name, *DEFAULT
  Library  . . . . . .  *LIBL        Name, *LIBL
Store key label  . . . . . .  *YES          *NO, *YES
```

Ejemplo del mandato ENCSTMF y valores de muestra

Control de errores

Si se ejecuta el mandato ENCSTMF dentro de un programa CL, puede capturar los errores controlando el id de mensaje CRE0700

Auditoría

Si se utiliza una Clave Simétrica con el mandato ENCSTMF y estuviera habilitado el parámetro “Log encryption usage” (Registrar el uso de la encriptación) para la clave simétrica, se generará una entrada en el log de auditoría en el archivo de journal del Crypto Complete cada vez que la clave se utilice para encriptar.

Cada entrada de auditoría indicará la etiqueta y almacén de claves de la clave simétrica utilizada junto con el usuario, fecha, hora, número de trabajo y nombre del trabajo

b) Desencriptar Archivos Stream de la IFS - (DECSTMF)

El mandato **DECSTMF** permite a los usuarios autorizados **desencriptar los archivos stream de la IFS** que fueron encriptados con el mandato ENCSTMF. Los archivos pueden ser restaurados/desencriptados desde un dispositivo físico o virtual o de la IFS. Puede especificarse una clave simétrica o contraseña para el proceso de desencriptación.

Realice los siguientes pasos para **desencriptar archivos:**

1. Introduzca el mandato **CRYPTO/DECSTMF** y pulse F4.
2. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line
3. Pulse Intro tras añadir los parámetros.

```
                    Decrypt IFS Stream File (DECSTMF)

Type choices, press Enter.

From type  . . . . . .  *DEV          *STMF, *DEV
From device  . . . . . .  TAP01       Name
From stream file:
  Name . . . . . .  '/Sensitivefiles/*'
  Include or omit  . . . . . .  *INCLUDE      *INCLUDE, *OMIT
  New object name  . . . . . .  *SAME
            + for more values
Name pattern:
  Pattern  . . . . . .  '*'
  Include or omit  . . . . . .  *INCLUDE      *INCLUDE, *OMIT
            + for more values
Directory subtree  . . . . . .  *ALL          *ALL, *DIR, *NONE, *OBJ, *STG
Volume identifier  . . . . . .  *MOUNTED
Sequence number  . . . . . .  *SEARCH       1-16777215, *SEARCH
Device label . . . . . .  ENCSTMF
Device end of media option . . .  *REWIND       *REWIND, *LEAVE, *UNLOAD
Allow object differences . . . .  *NONE        *NONE, *ALL, *FILELVL
Use key or password  . . . . . .  *KEY         *KEY, *PASS
Key label  . . . . . .  BACKUPKEY
Key store name . . . . . .  *DEFAULT     Name, *DEFAULT
 Library  . . . . . .    *LIBL       Name, *LIBL
```

Ejemplo del mandato DECSTMF y valores de muestra

Control de errores

Si se ejecuta el mandato DECSTMF dentro de un programa CL, puede capturar los errores controlando el id de mensaje CRE0701

Auditoría

Si se utiliza una Clave Simétrica con el mandato DECSTMF y estuviera habilitado el parámetro “Log decryption usage” (Registrar el uso de la desencriptación) para la clave simétrica, se generará una entrada en el log de auditoría en el archivo de journal del Crypto Complete cada vez que la clave se utilice para encriptar.

Cada entrada de auditoría indicará la etiqueta y almacén de claves de la clave simétrica utilizada junto con el usuario, fecha, hora, número de trabajo y nombre del trabajo

3. Comprobar el Proceso de Restauración de los Backup Encriptados

Es muy aconsejable que se realicen comprobaciones de la restauración de los Backup encriptados. **Especialmente importante cuando se de cualquiera de las siguientes condiciones**:

1. Cuando se utilizan los mandatos ENCxxx por primera vez.
2. Si se modifica algún parámetro de los mandatos ENCxxx.
3. Si se cambia la clave o contraseña utilizada con los mandatos ENCxxx.
4. Si se realiza una actualización del sistema operativo del IBMi.
5. Si se realiza una actualización del software de Crypto Complete.
6. Si recibe algún parche o arreglo para el producto Crypto Complete.

4. Mantenimiento de Contraseñas y Claves de Encriptación

PRECAUCIÓN: Su proveedor NO PODRÁ recuperar los datos encriptados de su empresa si se pierde la contraseña o clave.

4.1 Contraseñas

Si se utiliza una contraseña para la encriptación con los mandatos ENCxxx, es muy importante MANTENER UNA COPIA DE LA CONTRASEÑA, para casos de recuperación de desastres. Esta contraseña será necesaria para desencriptar los datos en el proceso de restauración con los mandatos DECxxx.

Debería registrar esta contraseña en su documentación de recuperación de desastres o en su caja fuerte. AL MENOS DOS PERSONAS DE SU COMPAÑÍA DEBERIAN SABER EL VALOR DE LA CONTRASEÑA.

4.2 Claves

Si se utiliza una clave para encriptar con los mandatos ENCxxx, es muy importante HACER UNA COPIA DE SEGURIDAD del ALMACÉN DE CLAVES que contiene la clave, así como HACER UNA COPIA DE SEGURIDAD de la MASTER KEY utilizada para encriptar el almacén de claves.

El Almacén de Claves y la Master Key tienen que estar disponibles en el sistema antes de poder realizar una operación de restauración con los mandatos DECxxx.

Las passphrases necesarios para recrear una Master Key deben también mantenerse en un lugar seguro. Vea la sección de “Backup y Recuperación de Claves” de la guía del usuario I apartado 9.

5. Preguntas más frecuentes sobre Encriptación de Backup

¿Puedo encriptar y salvar objetos Document Library Objects (DLO) ?

Si. Primero necesita salvar DLO en un Save file mediante el mandato SAVDLO de IBM con el parámetro DEV(*SAVF). Luego puede utilizar el mandato ENCSAVOBJ de Crypto Complete para encriptar/salvar el archivo SAVE al dispositivo de Backup.

¿Cómo puedo optimizar mi Backup?

A continuación se muestran varios consejos de cómo reducir el tiempo empleado en los procesos de Backup encriptado.

- Intente encriptar solo aquellas bibliotecas u objetos que contengan datos sensibles. No es necesario encriptar bibliotecas IBM (ejem. QSYS) u otras bibliotecas que no contengan datos confidenciales.
- Los mandatos ENCSAVLIB y ENCSAVOBJ de Crypto Complete permiten salvar las bibliotecas y objetos aún cuando estén activas. Esto permite a los usuarios continuar trabajando en una biblioteca mientras se está salvando.
- Si dispone de espacio suficiente en su disco, puede salvar cada biblioteca (que realmente requiera encriptación) en su propio objeto Save File mediante el mandato SAVLIB de IBM. Cuando sea conveniente, puede encriptar y salvar esos objetos Save File en el dispositivo de Backup utilizando el mandato ENCSAVOBJ (Encrypt Object) de Crypto Complete.

¿Dónde puedo utilizar los mandatos de Crypto Complete?

Los mandatos de encriptación pueden ejecutarse desde la línea de mandatos del sistema, en programas CL, incorporarse en el paquete BRMS de IBM o en el planificador de trabajos de IBM. Si su empresa utiliza BRMS, póngase en contacto con su proveedor para más instrucciones.

Normalmente realizamos un Backup completo de nuestro sistema desde el menú de Backup de IBM. ¿Cómo podemos continuar haciendo un Backup completo mientras se encriptan ciertas bibliotecas de usuario?

En lugar de utilizar el menú de Backup de IBM para ejecutar un Backup completo, podría escribir un programa CL que realice un Backup completo mediante la combinación de los mandatos de Backup de IBM para salvar aquellas bibliotecas del sistema o bibliotecas no sensibles y de los mandatos de Crypto Complete para encriptar y salvar bibliotecas de usuario sensibles. Revise el miembro fuente BACKUPALL en el archivo fuente CRYPTO/QCLSRC para ver un ejemplo de cómo realizar un Backup completo parcialmente encriptado.

¿Cómo realizar una restauración completa en nuestra máquina de recuperación de desastres?

Durante una recuperación total del sistema.

1. Restaure las bibliotecas del sistema de IBM, perfiles de usuario, autorizaciones y configuraciones que fueron salvadas con el mandato SAVSYS.
2. Restaure todas las bibliotecas de usuario no encriptadas que fueron salvadas con el mandato SAVLIB de IBM. Por ejemplo: RSTLIB SAVLIB(*NONSYS) DEV(TAP01).
3. Restaure el programa bajo licencia Crypto Complete. Por ejemplo, RSTLICPGM LICPGM(4CRYPTO) DEV(TAP01)
4. Restaure o recree las Master Keys.
5. Restaure los almacenes de claves (si se han utilizado claves para proteger los Backups).
6. Restaure todas las bibliotecas encriptadas y objetos encriptados mediante los mandatos DECRSTLIB o DECRSTOBJ de Crypto Complete.
7. Restaure todos los archivos encriptados de la IFS con el mandato DECSTMF de Crypto Complete.

Vaya el miembro fuente llamado RESTOREALL en el archivo fuente CRYPTO/QCLSRC para ver un ejemplo de una restauración completa.