Guía del Usuario I

Crypto Complete
Herramienta de Encriptación

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.

Omisiones del original

En este manual se ha omitido la traducción del apartado correspondiente al mandato ***IMPPTGKEY el cual permite a usuarios autorizados a importar Claves Simétricas generadas con el software Protegrity Defiance Enteprise Security Administrator una solución para la gestión de claves centralizada.***

En este manual se ha omitido la parte de terminología que se encuentra en el manual en inglés.

Guía del Usuario I - Herramienta de Encriptación

Programa bajo licencia Crypto Complete

Estos índices hacen referencia al material que se encuentra en las otras guías.

Guía del Usuario II - Encriptación de Campos

Guía del Usuario III - Backup e IFS encriptados

Guía del Usuario IV - Encriptación Automática de IFS

1. Introducción

Crypto Complete es una completa herramienta para la protección de los datos sensibles y confidenciales en el System i de IBM (iSeries), a través de una tecnología de encriptación (cifrado) consistente y un sistema de gestión de claves integrado.

La encriptación de datos se ha caracterizado hasta ahora por su difícil, larga y tediosa implantación dentro de nuestras organizaciones. Estas dificultades se multiplicaban en aquellas empresas que además necesitaban encriptar o cifrar campos específicos dentro de una base de datos, por ejemplo, el número de tarjeta de crédito de nuestros clientes. Esta necesidad suponía que debían afrontarse cambios en nuestras aplicaciones para aumentar el tamaño de los campos e implementar complicadas APIs para encriptar y desencriptar datos.

Crypto Complete se ha diseñado con un principal objetivo: **Permitir a las empresas implantar los procesos de encriptación (cifrado), con el máximo grado de protección, de la manera más rápida y sencilla, gracias a pantallas y mandatos intuitivos y de fácil manejo.**

1.1 Características Principales

Crypto Complete reúne un completo abanico de funciones y características necesarias para cumplir con los exigentes requisitos de encriptación y gestión de de claves. A continuación indicamos las principales capacidades novedosas del Crypto Complete:

- Encriptación automatizada de campos de las bases de datos del System i
- Encriptación de bibliotecas y objetos (Encriptación de Backup)
- Encriptación de archivos y directorios del System i (Encriptación de Backup)
- Tokenización, encriptación y almacenamiento de datos de sistemas remotos (IBMi, Windows, Linux, etc…)
- Gestión de claves simétricas integrado
- Rotación de las claves de encriptación sin tener que cifrar los datos de nuevo
- Encriptación de campos de tamaño insuficiente para contener el dato encriptado evitando su modificación
- Encriptación de campos numéricos, alfanuméricos, fecha, hora, timestamp
- Desencripta presentando valores completos y valores con máscara total o parcial
- Robusta encriptación con claves de hasta 256 bits
- Cumple con los estándares AES (Advanced Encryption Standard) y TDES (Data Encryption Standard)
- Menús y mandatos intuitivos del i5/OS con ayuda de texto on-line
- Programas de llamada y procedimientos ILE (APIs) para el cifrado/descifrado de datos de nuestras aplicaciones nativas
- Procedimientos almacenados y funciones SQL para en cifrado/descifrado de datos vía SQL
- Restringir el acceso de los programadores (*ALLOBJ) a los valores desencriptados
- Informes y Auditorías completas, mensajes de alerta.
- Compatible con múltiples entornos
- Compatible con los DB2 Field Procedures (V7R1 y superior)
- Compatible con múltiples entornos

Recomendamos encarecidamente que antes de iniciar la encriptación de sus datos de producción haya leído y comprendido el funcionamiento del producto y como establecer buenas prácticas de gestión de claves. Así se asegurará de que sus datos están siendo correctamente protegidos y que pueden ser únicamente desencriptados por los usuarios autorizados a tal fin.

Revise este manual para aprender a usar correctamente los mandatos y pantallas de Crypto Complete. Si es usted programador, vea la Guía del Programador para aprender a utilizar los programas (API) y procedimientos para encriptar/desencriptar datos desde sus aplicaciones.

1.2 Periodo de validez del Trial

Crypto Complete proporciona un periodo de 30 días de prueba gratuita para que su empresa pueda conocer todas sus posibilidades. Todas las funciones del Crypto Complete estarán disponibles durante este periodo. El periodo de prueba se activará automáticamente la primera vez que utilice cualquiera de los principales mandatos del Crypto Complete.

Con el producto instalado podrá conocer mediante el mandato **CRYPTO/DSPPRDINF**, (opción 10 Menú Principal de Crypto) la fecha de finalización del periodo de prueba.

Si necesitará ampliar el periodo de prueba póngase en contacto con American Top Tools en att@att.es.

Una vez haya tomado la decisión de adquirir Crypto Complete y satisfecho su contraprestación, American Top Tools le facilitará el acceso a una clave permanente para su activación. El producto no tendrá que ser reinstalado y todas sus configuraciones diseñadas durante el periodo de prueba se mantendrán igual.

> **AVISO:** Es muy importante que **durante el periodo de prueba no trabaje en el entorno de producción** ya que finalizado el periodo de prueba todas las funciones del Crypto Complete quedarán inhabilitadas y no podrá descifrar sus datos.

2. Instalación

2.1 Requisitos Mínimos del System i

Sistema operativo: Versión V5R2 o superior
Espacio de disco: 50 MB

Para las versiones del sistema operativo **i5/OS V5R2 o V5R3**, es necesario que el siguiente programa licenciado esté instalado antes de continuar:

Licensed Program: 5722AC3
Product Option: *Base
Description: Crypto Access Provider

IBM proporciona el programa licenciado 5722AC3 de manera gratuita. Contiene funciones fundamentales de encriptación utilizadas por Crypto Complete.

En las versiones de i5/OS iguales o superiores a **V5R4**, las funciones de encriptación 5722AC3 están incluidas en el sistema operativo base y por ello no tiene que ser instalado por separado.

Para comprobar si está instalado en su sistema (solo para versiones V5R2 y V5R3), ejecute el mandato GO LICPGM y seleccione la opción 10 para ver una lista de los programas licenciados instalados. Si el programa 5722AC3 no estuviera en esa lista, entonces debe instalarlo desde su CD del software de i5/OS o contactar con su agente de IBM.

2.2 Notas de Preinstalación

a) Componentes Instalados

Al instalarse, Crypto Complete se restaura en el System i(AS/400) como el programa licenciado llamado 4CRYPTO. Una vez restaurado, los objetos del software se encontrarán en la biblioteca llamada CRYPTO.

b) Requisitos de Autorización

Solo el perfil de usuario QSECOFR o el perfil de usuario con la autorización *SECADM puede instalar Crypto Complete. La instalación de Crypto Complete requiere autorización de acceso a los siguientes mandatos:

RSTLICPGM	Restore Licensed Program	**CRTVLDL**	Create Validation List
CRTLIB	Create Library	**CRTJRN**	Create Journal
CRTDUPOBJ	Create Duplicate Object	**CRTJRNRCV**	Create Journal Receiver

Puede comprobar las autorizaciones a los distintos objetos con el mandato DSPOBJAUT.

2.3 Actualizaciones del Producto

Por favor lea esta sección si va a proceder a **actualizar una versión anterior** de Crypto Complete.

Ejemplo paso a paso

> **PRECAUCIÓN:** NO DEBERIA BORRAR el programa licenciado CRYPTO o su biblioteca CRYPTO antes de la actualización. Si lo hace perderá los datos de usuario de la biblioteca CRYPTO.
> Nota Versión 3.0
> Todos aquellos que actualicen el software anterior a la 3.0 requieren claves nuevas. Contacte con American Top Tools (att@att.es) antes de realizar la actualización. No hacerlo podría hacer que el producto dejará de funcionar.

a) Compruebe que no haya bloqueos

> Antes de la instalación asegúrese de que no existen bloqueos en la biblioteca CRYPTO.

b) Retención de datos de usuario

Si ya dispone de una clave permanente de Crypto Complete, esa clave se mantendrá durante la actualización (Ver Nota Versión 3.0).

Los siguientes datos de usuario definidos por el usuario también se retendrán durante la actualización de Crypto Complete:

- Configuración de Política de claves (Key Policy Settings)
- Configuración de alertas de seguridad (Security Alert Settings)
- Entradas de Oficial de Claves (Key Officer Entries)
- Claves de Encriptación Maestras (Master Encryption Keys)
- Almacenes de Claves (Key Stores)
- Entradas al Registro de Campos Encriptados (Field Encryption Registry Entries)
- Archivos externos que almacenan los valores de campo encriptados

Durante el proceso de instalación, se salvará una copia de los datos de usuario existentes en una biblioteca llamada CRYPTxxxxx donde xxxxx representa un número secuencial que empieza en 00001. Esta biblioteca solo se necesitará si fallara la actualización, en cuyo caso debe contactar con American Top Tools.

Siga los pasos en las páginas siguientes para instalar/actualizar Crypto Complete.

2.4 Instalación del Producto (Nuevas Instalaciones)

*Nota de aquí en adelante “IBM i, iSeries, System i” se representará por “AS/400”.

Si va a actualizar, asegúrese de haber leído el apartado 2.3 Actualización del Producto.

El software de Crypto Complete se aloja en un fichero Save del AS/400 que debe cargarse en su sistema. Siga los siguientes pasos para instalar o actualizar Crypto Complete en su sistema.

1. Identifíquese con el perfil de usuario QSECOFR o con un perfil que tenga autorización *SECADM. Este perfil debería tener la autorización a los siguientes mandatos i5/OS:

   RSTLICPGM CRTLIB CRTDUPOBJ
   CRTVLDL CRTJRN CRTJRNRCV.

2. Cree un archivo Save temporal en su AS/400:

   CRTSAVF FILE(QGPL/CRYPTO)

3. El producto debe cargarse en el AS/400 mediante un FTP. Antes de continuar, compruebe que el servidor FTP funciona en su sistema. Para iniciar el servidor FTP utilice el mandato:

   STRTCPSVR SERVER(*FTP)

4. El archivo de instalación se llama CRYPTO.ZIP. Si aún no dispusiera de él puede descargarlo en http://www.att.es/formcrypto.htm o solicitarlo a American Top Tools (att@att.es).

5. Extraiga los archivos del archivo CRYPTO.zip a un archivo temporal en su PC. Uno de los ficheros extraídos es el archivo Save **CRYPTO.SAVF**

6. Envíe vía FTP el archivo CRYPTO.SAVF desde su PC al archivo Save en su AS/400, creado en el paso 2. A continuación mostramos los pasos a seguir para realizar un envío FTP desde Windows:

   - Abra la ventana DOS (Todos los programas/Accesorios/Símbolo del sistema);
   - Introduzca el mandato FTP <hostname>, donde <hostname> es el nombre host o dirección IP de su Sistema;
   - Identifíquese con su id de usuario (QSECOFR) y contraseña del AS/400 e introduzca los siguientes mandatos FTP:

ftp> **BINARY**	(Cambia la sesión FTP a modo binario)
ftp> **LCD \<tempdir>**	(<tempdir> es el directorio de PC que contiene el archivo CRYPTO.SAVF)
ftp> **CD qgpl**	(Cambia el directorio remoto a la biblioteca QGPL)
ftp> **PUT crypto.savf crypto**	(Envía el archivo CRYPTO.SAVF desde el PC al archivo Save CRYPTO del AS/400)
ftp> **QUIT**	(Finaliza la sesión FTP)

7. De nuevo en el AS/400, restaure el programa licenciado desde el archivo Save ejecutando el mandato i5/OS:

   RSTLICPGM LICPGM(4CRYPTO) DEV(*SAVF) SAVF(QGPL/CRYPTO)

8. Borre el archivo Save temporal ejecutando el mandato i5/OS (opcional):

   DLTF FILE(QGPL/CRYPTO)

9. La biblioteca CRYPTO instalada y todos los objetos contenidos en esta, tendrán inicialmente autorización a los siguientes usuarios:

   QPGMR: *ALL authority *PUBLIC: *USE authority

Si quisiera asignar distintas autorizaciones a la biblioteca y objetos CRYPTO, puede utilizar los mandatos CHGOBJOWN, RVKOBJAUT y GRTOBJAUT para hacer esos cambios.

Se recomienda no dar al usuario *PUBLIC autorizaciones adicionales (Más allá de *USE) a los mandatos y programas de la biblioteca CRYPTO.

3. Visión General

3.1 Menú Principal

Todos los mandatos de Crypto Complete son accesibles desde el menú principal y sus submenús. Para acceder al menú principal de Crypto Complete ejecutar:

GO CRYPTO/CRYPTO

Se verá la siguiente pantalla:

```
CRYPTO                          Main Menu


Select one of the following:

  1. Key Policy and Security Menu          (GO CRYPTO1)
  2. Master Key Menu                       (GO CRYPTO2)
  3. Symmetric Key Menu                    (GO CRYPTO3)
  4. Field Encryption Menu                 (GO CRYPTO4)
  5. Library/Object/File Encryption Menu   (GO CRYPTO5)
  6. Source Examples Menu                  (GO CRYPTO6)
  7. IFS Encryption Menu                   (GO CRYPTO7)
  9. Field Analysis Menu                   (GO CRYPTO9)

 10. Product Information Menu              (GO CRYPTO10)
```

Pantalla del Menú Principal

Los mandatos pueden ejecutarse desde el menú introduciendo la opción correspondiente. También puede ejecutarse utilizando el nombre de mandato (en paréntesis) desde la línea de mandatos.

3.2 Inicio Rápido

La documentación de los mandatos que siguen y otros que aparecerán más adelante la encontrará en este manual. A su vez todos los mandatos de Crypto tienen una ayuda directa a la que puede accederse con el F1 cuando se presenta un mandato.

Siga los pasos mostrados seguidamente y en ese orden, para configurar rápidamente el *Sistema de Gestión de Claves Simétricas* de Crypto Complete y establecer su primera *Clave de Encriptación de Datos (DEK)*.

Con ella podrá encriptar campos, bibliotecas, objetos y/o archivos.

Paso 1.- CHGKEYPCY

Ver y/o cambiar configuraciones de la *Política de Claves*. F4 para opciones.

Paso 2.- WRKKEYOFR

Indicar que usuarios pueden crear y gestionar claves.

Paso 3.- LODMSTKEY

Preparar una Clave de Encriptación Maestra (MEK)
cargando las distintas partes de la passphrase(*)

Paso 4.- CRYTO/SETMSTKEY

Generar la clave MEK
utilizando las partes de la passphrase(*) cargadas

Paso 5.- CRTKEYSTR

Crear un Almacén de Claves
que contendrá las Claves de Encriptación de Datos (DEK).

Paso 6.- CRTSYMKEY

Crear una Clave de Encriptación de Datos (DEK)
y guardarla en el almacén de claves.

(*) 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.

MEK	**Master Encryption Key**	**Clave de Encriptación Maestra**
DEK	**Data Encryption Key**	**Clave de Encriptación de Datos**

Finalmente en la opción 9 del menú, se facilita la búsqueda de campos de la base de datos que pudieran contener datos sensibles, tales como números de tarjetas de crédito, números de seguridad social, etc… Para acceder a este menú también puede ejecutar el mandato:

GO CRYPTO/CRYPTO09

3.3 Encriptación de Campos

Tras completar los pasos anteriores, los campos de la base de datos pueden ser encriptados utilizando las nuevas claves DEK creadas utilizando una o varias de las siguientes aproximaciones:

- Establecer la automatización de encriptación de campos mediante el mandato WRKFLDENC, Work Field Encrytpion (Trabajar la Encriptación de Campos)

- Llamar a procedimientos ILE o programas (APIs) para encriptar/desencriptar datos dentro de nuestras aplicaciones (*)

- Llamar a funciones SQL o procedimientos almacenados para encriptar/desencriptar datos usando SQL (*)

(*) Lea la “GUIA DEL USUARIO_II_Crypto Complete_Encritpación de Campos

3.4 Encriptación de Archivos, Objetos y Bibliotecas

Una vez establecidas las claves DEK (Data Encryption Key) desde su Sistema de Gestión de Claves, puede utilizar cualquiera de los siguientes mandatos para encriptar bibliotecas, objetos y archivos de su AS/400 guardándolos en cinta o disco.

ENCSAVLIB	Encriptar bibliotecas
ENCSAVOBJ	Encriptar objetos específicos dentro de una biblioteca
ENCSTMF	Encriptar archivos stream de IFS y archivos físicos

(*) Lea la “GUIA DEL USUARIO_III_Crypto Complete__Backup e IFS encriptados” para más detalles.

3.5 Crear Alertas de seguridad

Utilizando el mandato **WRKCCALR**, puede establecer Alertas de Seguridad opcionalmente, las cuales pueden enviar notificaciones ante cambios realizados o usos no autorizados relativos a Crypto Complete.

4. Gestión de Claves Simétricas

La Encriptación de Claves Simétricas (también conocida por el cifrado de la clave privada o secreta) es una forma de encriptación en que la misma clave puede ser utilizada para encriptar y desencriptar.

Las claves simétricas deben ser lo suficientemente seguras para la aplicación en cuestión. La fortaleza de una clave simétrica viene determinada por su longitud. Cuanto más larga más difícil será para los superordenadores romper el código. Crypto Complete permite generar claves simétricas de 256 bits de longitud proporcionando mayores niveles de protección.

Los valores de las claves simétricas deben mantenerse secretos para evitar la visualización de datos sensibles no autorizados. Deben pues existir controles para proteger la confidencialidad y el acceso a las claves simétricas. Crypto Complete contempla un sistema integrado de Gestión de Claves Simétricas muy completo para poder establecer esos controles con facilidad.

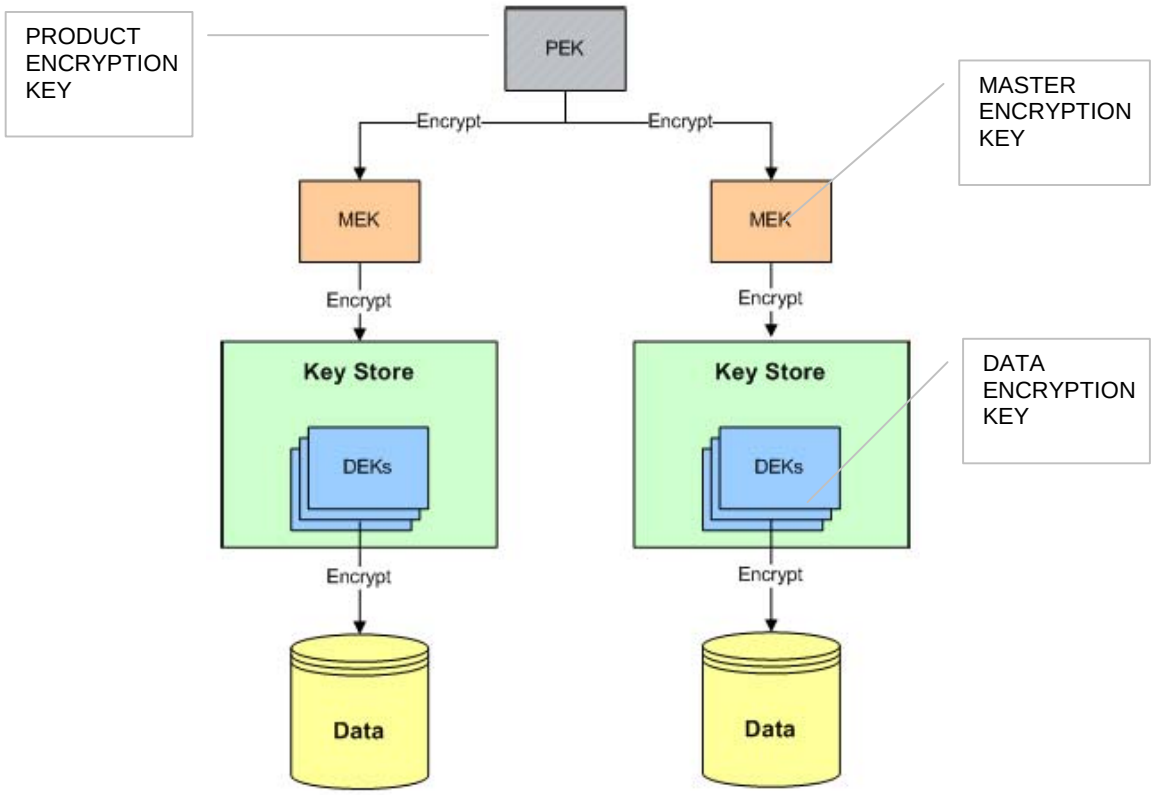
Algoritmo de cifrado (Cipher):
Un par de algoritmos (procesos matemáticos) utilizados para encriptar/desencriptar.
Clave (Key):
La información requerida para controlar las operaciones del algoritmo de cifrado. A diferencia de las contraseñas generadas por el hombre, las claves son más seguras ya que al ser generadas por el ordenador serán representadas por una series no visible de bits (1001110...).

El Sistema de Gestión de Claves Simétricas de Crypto Complete le permitirá:

1. Establecer políticas de cómo pueden crearse y utilizarse las Claves Simétricas
2. Establecer que usuarios pueden crear y generar las Claves Simétricas
3. Generar aleatoriamente Claves Simétricas seguras
4. Proteger sus Claves Simétricas mediante las Claves de Encriptación Maestras
5. Proteger la recreación de una Clave de Encriptación Maestra mediante la solicitud de passphrases de hasta 8 usuarios
6. Organizar en uno o varios Almacenes de Claves todas sus Claves Simétricas
7. Restringir el acceso a estos almacenes de claves mediante las autorizaciones de objetos propias del i5/OS
8. Restringir la búsqueda de los actuales valores de Claves Simétricas
9. Establecer la separación de poderes (Por ejemplo, el creador de una Clave Simétrica puede no tener autorización para utilizar la clave para encriptar o desencriptar)
10. Controlar que usuarios pueden utilizar las Claves para encriptar y desencriptar
11. Obtener audit logs detallados

4.1 Jerarquía de las Claves Simétricas

Crypto Complete proporciona una arquitectura de seguridad multinivel para proteger las Claves Simétricas en el AS/400. A continuación mostramos un sencillo diagrama:



DEK - Data Encryption Key .- Clave de Encriptación de Datos

Una clave DEK es una Clave Simétrica utilizada para encriptar y desencriptar. Pueden crearse un o varias claves DEK. Por ejemplo, podría crearse una clave DEK para cifrar/descifrar números de tarjetas de crédito y una segunda clave DEK para cifrar/descifrar los números de la seguridad social.

Las claves DEK deben ser generadas aleatoriamente por Crypto Complete para así conseguir el mayor nivel de protección. Atendiendo a la política de claves de su empresa, puede hacer que Crypto Complete genera una clave DEK basada en un passphrase creado por el usuario**.**

Key Store.- Almacén de Claves

Las claves DEK son almacenadas en el Almacén de Claves. Puede crear más de un Almacén de Claves en el AS/400 mediante Crypto Complete. Por ejemplo, un Almacén de Claves para almacenar las claves DEK que protegen los datos de pedidos y un segundo almacén para las claves DEK destinadas a la protección de los datos de nómina.

El Almacén de Claves se crea en el AS/400 como un objeto *VLDL (Validation List). El acceso a dicho objeto se puede controlar mediante la seguridad de objetos propia del i5/OS.

MEK – Master Encryption Key.- Clave de Encriptación Maestra

La clave MEK es una Clave Simétrica especial utilizada para proteger (mediante la encriptación) las claves DEK que están almacenadas en un Almacén de Claves.

Puede crear hasta 8 claves MEK para cada entorno en su AS/400. Por ejemplo, una clave MEK podría emplearse para proteger las claves DEK de pedidos almacenadas en un Almacén de Claves y, una segunda MEK podría emplease para proteger las claves DEK de nóminas almacenadas en otro Almacén de Claves (key Store).

Crypto Complete genera la clave MEK usando distintos passphrases introducidos por distintos usuarios autorizados. Atendiendo a su política de claves pueden requerirse hasta 8 passphrases de distintos usuarios para generar una sola MEK.

Las claves MEK se almacenan en un objeto *VLDL (Validation List) del AS/400 llamado CRVL001.

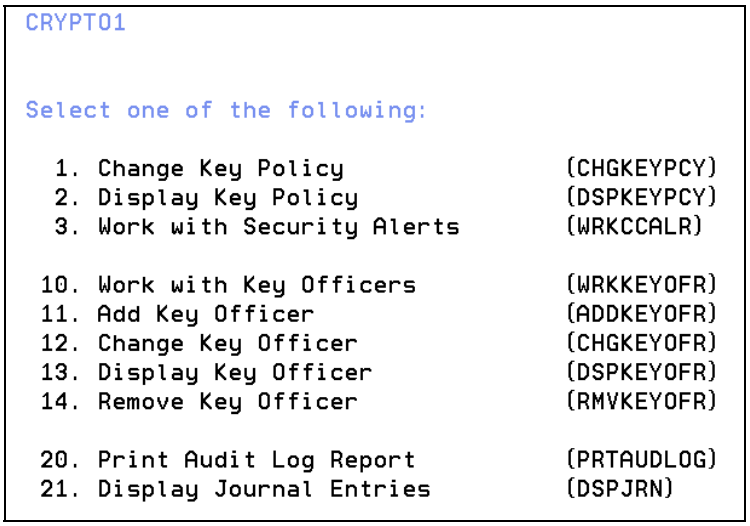
PEK – Product Encryption Key .- Clave de Encriptación del Producto

La clave PEK, como su nombre indica, es propia del producto y la utiliza el propio Crypto Complete para proteger mediante la encriptación las claves MEK y las configuraciones definidas por el usuario encargado de la seguridad (QSECOFR), como son las política de claves, los oficiales de claves, alertas de seguridad…

Crypto Complete genera automáticamente la clave PEK utilizando una combinación del nº de serie del sistema y un valor secreto. El PEK sólo reside en memoria cuando se necesita pero no se almacena nunca.

4.2 Política de Claves

La política de claves le permitirá controlar la configuración del entorno para el Sistema de Gestión de Claves de Crypto Complete. Estas configuraciones estarán encriptadas bajo la clave de encriptación del producto PEK, y se almacenarán en la biblioteca CRYPTO por defecto.



Menú de Política de Claves

a) Cambiar la Política de Claves (CHGKEYPCY)

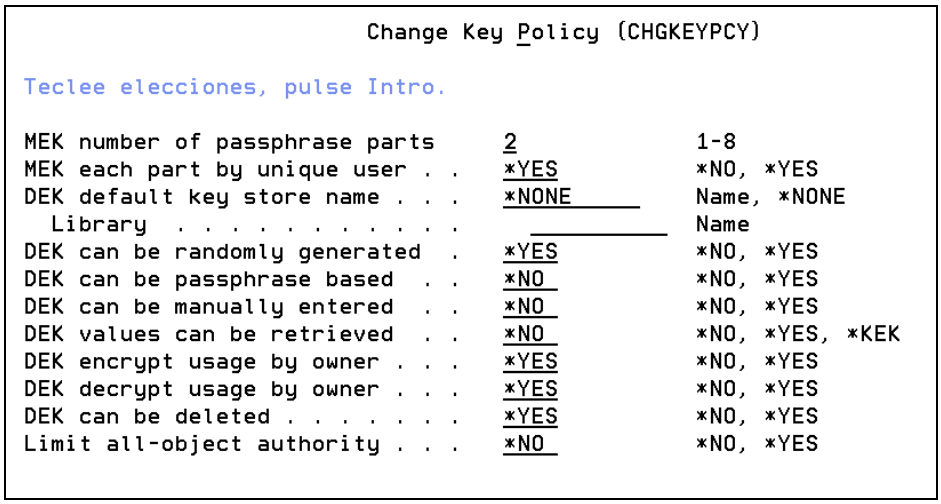
El mandato **CHGKEYPCY** permite especificar la configuración de la política del entorno de Claves Simétricas. Los siguientes usuarios pueden utilizar este mandato:

- Perfil de usuario QSECOFR
- Usuarios con autorización *SECADM (si no se excluye en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain Key Officers” (Mantener Oficiales de Claves) está establecida en *YES

Siga los siguientes pasos para **cambiar la configuración de la política de claves**:

1. Pulse F4 en el mandato **CRYPTO/CHGKEYPCY**
2. Se mostrará la configuración actual de los valores de parámetros
3. Pulse F1 en cualquier parámetro para obtener ayuda on-line
4. Pulse Intro una vez haya introducido los valores de los parámetros.

Nota: Cualquier cambio realizado en las Políticas de Claves (Key Policy) quedará automáticamente registrado en un archivo de auditoría.



```
                    Change Key Policy (CHGKEYPCY)

Teclee elecciones, pulse Intro.

MEK number of passphrase parts     2             1-8
MEK each part by unique user . .   *YES          *NO, *YES
DEK default key store name . . .   *NONE         Name, *NONE
  Library  . . . . . . . . . . .                 Name
DEK can be randomly generated  .   *YES          *NO, *YES
DEK can be passphrase based  . .   *NO           *NO, *YES
DEK can be manually entered  . .   *NO           *NO, *YES
DEK values can be retrieved  . .   *NO           *NO, *YES, *KEK
DEK encrypt usage by owner . . .   *YES          *NO, *YES
DEK decrypt usage by owner . . .   *YES          *NO, *YES
DEK can be deleted . . . . . . .   *YES          *NO, *YES
Limit all-object authority . . .   *NO           *NO, *YES
```

Pantalla del mandato CHGKEYPCY y los valores por defecto

Descripción de los campos del mandato CHGKEYPCY

MEK number of passphrase parts: Número de partes del passphrase de la clave MEK	Indica el número de partes del passphrase que deben introducirse (cargarse) antes de poder generar una clave MEK. Valor recomendado: Se recomiendan al menos 2 o 3 partes. Así ayuda a proteger la seguridad de la clave MEK que solo podrá ser regenerada si todas las partes del passphrase son introducidas.
MEK each part by unique user: Cada parte de MEK por un usuario distinto	Indica si cada parte del passphrase de la clave MEK debe ser introducida por distintos perfiles de usuario. *YES. Para proteger la seguridad de una clave MEK debería requerir que cada parte del passphrase sea introducida por un perfil de usuario distinto. Excepto en casos extremos ningún usuario debería conocer todas las partes del passphrase empleadas para generar la clave MEK.
DEK default key store name: Almacén de Claves que por defecto contiene el DEK	Indica la biblioteca y el nombre de objeto del Almacén de Claves por defecto que contiene las claves DEK. Recomendación: Si especifica un nombre por defecto, entonces el solicitante (por ejemplo, el programador de su aplicación) no tendrá que especificar el nombre del Almacén de Claves cuando tenga que solicitar una clave DEK para utilizar en la encriptación o desencriptación. No es solo una cuestión de conveniencia sino que también puede ayudar a proteger la localización del objeto Almacén de Claves por defecto.
DEK can be randomly generated El DEK puede ser generado aleatoriamente	Indica si las claves DEK pueden ser generadas aleatoriamente mediante el mandato CRTSYMKEY (Crear Clave Simétrica). Valor recomendado: *YES. Para un mayor nivel de seguridad y protección la clave DEK debería ser generada aleatoriamente. Una clave generada aleatoriamente es muy difícil de recrear, por no decir, imposible.

Continuación Descripción de los campos del mandato CHGKEYPCY

DEK can be passphrase based El DEK puede estar basado en passphrase	Indica si una clave DEK puede ser generada con un passphrase creado por el usuario mediante el uso del mandato CRTSYMKEY (Crear Clave Simétrica). Valor recomendado: *NO. Una clave DEK con passphrase puede ser regenerada si la persona en cuestión conoce el passphrase y el algoritmo utilizado para generar la clave DEK. Por ello, una clave DEK con passphrase no es tan segura como una clave DEK generada aleatoriamente. Solo debería utilizar este tipo de claves DEK con passphrase si esas claves DEK tienen que ser regeneradas en otras plataformas.
DEK can be manually entered El DEK puede ser entrado manualmente	Indica si un valor de la clave DEK puede ser introducido manualmente mediante el mandato CRTSYMKEY (Create Symmetric Key). Valor recomendado: *NO. Un valor DEK introducido manualmente es el menos seguro. Dado que el valor DEK podría utilizarse para desencriptar datos sin utilizar las APIs de Crypto Complete y mecanismos de seguridad. Solo debería permitir esta entrada manual de valores DEK cuando necesite almacenar/usar las claves DEK que genere, en otras plataformas.
DEK values can be retrieved Los valores del DEK pueden ser recuperados	Indica si los valores DEK pueden ser recuperados con el mandato EXPSYMKEY (Export Symmetric Key). *NO – No puede recuperarse *YES – Si puede recuperarse *KEK – Solo puede recuperarse si se ha encriptado con una Key Encryption Key (KEK) Valor recomendado: *NO o *KEK. Si un valor DEK es recuperable, entonces el valor actual de la clave DEK podría utilizarse para desencriptar datos sin utilizar las APIs de Crypto Complete y mecanismos de seguridad. Solo debería estar en *YES cuando los valores de clave necesiten compartirse con otro sistema distinto del AS/400, que necesiten encriptar y desencriptar datos utilizando la misma clave.
DEK encrypt usage by owner Utilización del DEK por su creador para encriptar	Indica si el perfil de usuario que creó la clave DEK puede utilizar esa misma clave DEK para encriptar datos.
DEK decrypt usage by owner Utilización del DEK por su creador para desencriptar	Indica si el perfil de usuario que creó la clave DEK puede utilizar esa misma clave DEK para desencriptar datos. Valor recomendado: *NO. Para proporcionar tareas separadas y ayudar a proteger la seguridad en la encriptación de datos, el creador (propietario) de la clave DEK no debería poder utilizar la clave DEK para desencriptar datos.
DEK can be deleted DEK puede ser borrado	Indica si una clave DEK puede ser borrada de un Almacén de Claves. Valor recomendado: *NO. El borrado accidental de una clave DEK puede implicar que los datos encriptados mediante esa clave DEK sean datos irrecuperables.

Continuación Descripción de los campos del mandato CHGKEYPCY

Limit all-object authority	Indica si debe limitarse la autorización sobre los Almacenes de Claves y las listas de autorización del Registro de Campos a aquellos usuarios con autorización especial *ALLOBJ *NO – Si el usuario tiene autorización *ALLOBJ, la API 'QSYCUSRA' de IBM comprobará si el usuario tiene autorización sobre el almacén de claves o lista de autorizaciones solicitada. Por tanto, los usuarios con autorización *ALLOBJ estarán siempre autorizados. Es el valor por defecto. *YES – Si el usuario tiene autorización *ALLOBJ es Crypto Complete quién en este caso hará su propia comprobación al solicitar cualquier almacén de claves o lista de autorizaciones. No se utiliza la API 'QSYCUSRA' de IBM. El usuario de perfil (o perfil de grupo al que pertenezca) tiene que estar específicamente listado con autorización, con al menos *USE, sobre el almacén de claves o lista de autorizaciones. Vea el apéndice "A" para más información sobre cómo tratar los usuarios que tienen autorización *ALLOBJ.

b) Ver la Política de Claves (DSPKEYPCY)

El mandato **DSPKEYPCY** permite a los usuarios autorizados ver la configuración de la política de claves para el entorno de las Claves Simétricas. Siga los siguientes pasos para ver esa configuración:

1. Introduzca el mandato **CRYPTO/DSPKEYPCY**
2. Se mostrará la actual política de claves junto con el id de usuario y hora en que se modificaron por última vez.
3. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line.

```
                    Display Key Policy (DSPKEYPCY)

Type choices, press Enter.

MEK number of passphrase parts     2
MEK each part by unique user . .   *YES
DEK default key store name . . .   PAYROLLDEK
  Library  . . . . . . . . . . .     KEYSTORES
DEK can be randomly generated  .   *YES
DEK can be passphrase based  . .   *NO
DEK can be manually entered  . .   *NO
DEK values can be retrieved  . .   *KEK
DEK encrypt usage by owner . . .   *YES
DEK decrypt usage by owner . . .   *YES
DEK can be deleted . . . . . . .   *NO
Limit all-object authority . . .   *NO
Last modified by user  . . . . .   QSECOFR
Last modified date/time  . . . .   '2011-03-11-10.42.27.179000'
```

Pantalla del Mandato DSPKEYPCY

4.3 Oficiales de Claves

Los Key Officers (Oficiales de Claves) son los usuarios autorizados para crear y gestionar Claves MEK, Almacenes de Claves, Claves DEK y el Registro de la Encriptación de Campos.

a) Trabajar con Oficiales de Claves (WRKKEYOFR)

El mandato **WRKKEYOFR** permite a una organización trabajar con los Oficiales de Claves dentro del entorno de Claves Simétricas.

Los siguientes usuarios pueden utilizar este mandato:

- Perfil de usuario QSECOFR
- Perfiles de usuarios con autorización *SECADM
- Un oficial de claves cuya configuración de autorizaciones “Maintain Key Officers” (Mantener Oficiales de Claves) está establecida en *YES

Los oficiales de claves y su configuración de actualizaciones se almacenan en la biblioteca CRYPTO por defecto. Estas configuraciones están encriptadas con la clave de encriptación de producto (PEK).

Realice los siguientes pasos para **trabajar con los Oficiales de Cla**ves:

1. Ejecute el mandato **CRYPTO/WRKKEYOFR**
2. Se mostrarán los Oficiales de Claves existentes y las autorizaciones correspondientes.

Nota: Un usuario no necesita ser un Oficial de Claves para encriptar y desencriptar datos.

```
6/24/06                    Work with Key Officers                  QSECOFR
21:03:44                                                           CRRM002

Type options, press Enter.
 2=Change  4=Remove  5=Display

                  Key       Key      Load  Set/Clear   Key             Field   IFS
Opt  User       Policy  Officers  MEKs     MEKs     Stores   DEKs     Reg.   Reg.
__   MARY         *NO       *YES   *YES     *YES      *YES    *YES     *YES   *NO
__   JACK         *NO       *NO    *YES     *NO       *NO     *YES     *YES   *YES
__   BILL         *NO       *NO    *YES     *NO       *NO     *YES     *NO    *YES
__   ELLIE        *YES      *YES   *YES     *NO       *NO     *YES     *YES   *NO



F3=Exit    F5=Refresh    F6=Add    F12=Cancel
```

Pantalla del Mandato WRKKEYOFR

Opciones de pantalla: Disponibles por cada Oficial de Clave mostrado en la pantalla.

Opción	Descripción
2	Muestra la opción para cambiar las configuraciones de las autorizaciones del Oficial de Clave utilizando el mandato CHGKEYOFR.
4	Muestra la opción para confirmar la eliminación de un Oficial de Clave mediante el mandato RMVKEYOFR.
5	Muestra la configuración actual de las autorizaciones utilizando el mandato DSPKEYOFR.

Teclas de función: Estas son las teclas de función disponibles en la pantalla WRKKEYOFR:

Función	Descripción
F3	Salir de la pantalla WRKKEYOFR Muestra la opción para cambiar las configuraciones de las autorizaciones del Oficial de Clave utilizando el mandato CHGKEYOFR.
F5	Refrescar la lista de Oficiales de Claves.
F6	Muestra un prompt para añadir un nuevo oficial de seguridad mediante el mandato ADDKEYOFR.

b) Añadir un Oficial de Claves (ADDKEYOFR)

Mediante el mandato **ADDKEYOFR** el usuario autorizado por Crypto Complete podrá añadir un nuevo Oficial de Clave al entorno de Claves Simétricas. Los siguientes usuarios pueden emplear este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain Key Officers” (Mantener Oficiales de Claves) está establecida en *YES

Los Oficiales de Claves y todas sus configuraciones de autorizaciones se almacenan en la biblioteca CRYPTO por defecto. Estas irán encriptadas con la clave PEK.

Siga los siguientes pasos para **añadir un Oficial de Claves**:

1. Introduzca el mandato **CRYPTO/ADDKEYOFR** y haga F4
2. Pulse F1 en cualquier parámetro para obtener información on-line.
3. Pulse Intro después de introducir los valores de los parámetros.

Nota: Cualquier mantenimiento realizado sobre los Oficiales de Claves se registrará en un archivo de auditoría.

```
                        Add Key Officer (ADDKEYOFR)

Type choices, press Enter.

Key officer user profile . . . .  __________    Name
Maintain key policy and alerts .  *YES          *NO, *YES
Maintain key officers  . . . . .  *NO          *NO, *YES
Load MEK passphrase parts  . . .  *YES          *NO, *YES
Set and clear MEKs . . . . . .    *YES          *NO, *YES
Maintain key stores  . . . . . .  *YES          *NO, *YES
Maintain DEKs  . . . . . . . . .  *YES          *NO, *YES
Maintain field enc. registry . .  *YES          *NO, *YES
Maintain IFS enc. registry . . .  *YES          *NO, *YES
```

Pantalla de mandato ADDKEYOFR

Descripción de los campos del mandato ADDKEYOFR

Key officer user profile	Especificar un perfil de usuario existente en el System i.
Maintain key policy and alerts	Indica si el Oficial de Claves puede mantener la Política de claves y Alertas de seguridad del Crypto Complete.
Maintain key officers	Indicar si el Oficial de Claves podrá añadir, cambiar o eliminar a otros Oficiales de Clave.
Load MEK passphrase parts	Indicar si el nuevo Oficial de Claves puede introducir/cargar las partes de los passphrase de la clave MEK.
Set and clear MEKs	Indicar si el nuevo Oficial de Claves puede establecer/generar o borrar una clave MEK.
Maintain key stores	Indicar si el nuevo Oficial de Claves puede crear Almacenes de Claves o reencriptar los Almacenes de Claves bajo otra clave MEK.
Maintain DEKs	Indicar si el Oficial de Claves puede crear, copiar o borrar claves DEK.
Maintain Field Enc. Registry	Indicar si el Oficial de Claves puede mantener el Registro de Encriptación de Campos.
Maintain IFS Enc. Registry	Indicar si el Oficial de Claves puede mantener el registro de Encriptación de archivos en la IFS y otras configuraciones automáticas de la IFS. *Reservado para su uso en un futuro próximo.*

c) Change Key Officer (CHGKEYOFR)

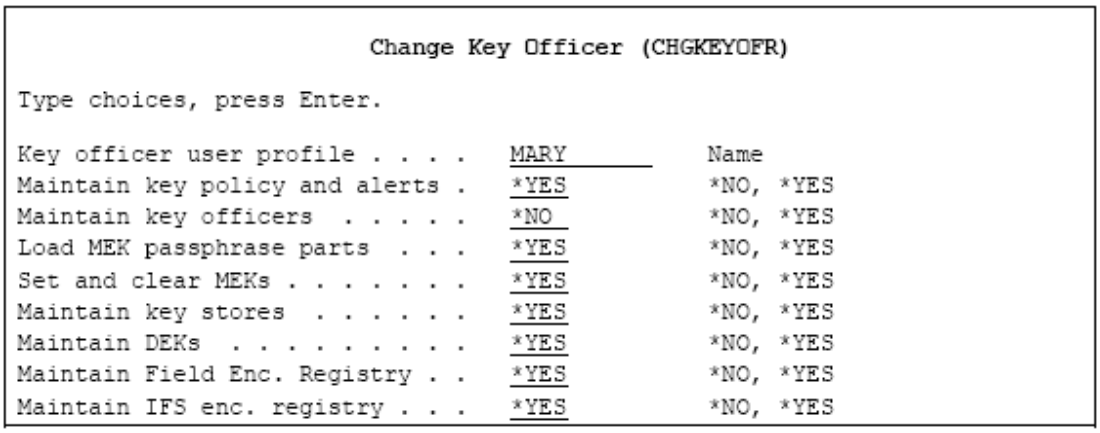
El mandato **CHGKEYOFR** permite a los usuarios autorizados cambiar los parámetros de un Oficial de Claves dentro del entorno de Claves Simétricas. Los siguientes usuarios pueden utilizar este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM si no está excluido en Key Officer Settings)
- Un oficial de claves configuración de autorizaciones “Maintain Key Officers” (Mantener Oficiales de Claves) está establecida en *YES

Realice los siguientes pasos para **cambiar un Oficial de Claves**:

1. Introduzca el mandato **CRYPTO/CHGKEYOFR** y haga F4
2. Introduzca el perfil de usuario del Oficial de Claves y pulse Intro
3. Se mostrará la configuración actual del Oficial de Claves (valores de los parámetros)
4. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line
5. Pulse Intro una vez haya modificado los valores de los parámetros.

Nota: Cualquier mantenimiento o cambio realizado en los Oficiales de Claves serán registrados en el archivo de auditoría.



Pantalla de mandato CHGKEYOFR

Descripción de los campos del mandato CHGKEYOFR

Key officer user profile	Especificar un perfil de usuario existente en el IBM i.
Maintain key policy and alertas	Indicar si el Oficial de Claves puede mantener la política de claves y las alertas de Crypto Complete.
Maintain key officers	Indicar si el Oficial de Claves que estamos creando podrá añadir, cambiar o eliminar a otros Oficiales de Clave.
Load MEK passphrase parts	Indicar si el nuevo Oficial de Claves puede introducir/cargar las partes de los passphrase de la clave MEK.
Set and clear MEKs	Indicar si el nuevo Oficial de Claves puede establecer/generar o borrar una clave MEK.
Maintain key stores	Indicar si el nuevo Oficial de Claves puede crear Almacenes de Claves o reencriptar los Almacenes de Claves bajo otra clave MEK.
Maintain DEKs	Indicar si el Oficial de Claves puede crear, copiar o borrar claves DEK.
Maintain Field Enc. Registry	Indicar si el Oficial de Claves puede mantener el Registro de Encriptación de Campos.
Maintain IFS Enc. Registry	Indicar si el Oficial de Claves puede mantener el registro de Encriptación de archivos en la IFS y otras configuraciones automáticas de la IFS. *Reservado para su uso en un futuro próximo.*

d) Ver Oficial de Claves (DSPKEYOFR)

El mandato **DSPKEYOFR** permite a un usuario autorizado ver las configuraciones de las autorizaciones de los Oficiales de Claves. Siga los siguientes pasos para ver las autorizaciones de los Oficiales de Claves:

1. Teclee **CRYPTO/DSPKEYOFR** y haga F4. ()
2. Introduzca el perfil de usuario del Oficial de Clave y pulse Intro
3. Se mostrarán las autorizaciones de los Oficiales de Claves junto con quien modificó o añadió a ese oficial y la hora en que se hizo
4. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line.

```
                        Display Key Officer (DSPKEYOFR)

Type choices, press Enter.

Key officer user profile . . . .   MARY
Maintain key policy and alerts .   *YES
Maintain key officers  . . . . .   *NO
Load MEK passphrase parts  . . .   *YES
Set and clear MEKs . . . . . .     *YES
Maintain key stores  . . . . . .   *YES
Maintain DEKs  . . . . . .         *YES
Maintain Field Enc. Registry . .   *YES
Maintain IFS enc. registry . . .   *YES
Last modified by user  . . . . .   QSECOFR
Last modified date/time  . . . .   '2011-06-24-19.53.50.751000'
```

Pantalla del mandato DSPKEYOFR

e) Eliminar un Oficial de Claves (RMVKEYOFR)

El mandato **RMVKEYOFR** permite a los usuarios autorizados eliminar un Oficial de Claves del entorno de las Claves Simétricas.

Los siguientes usuarios pueden emplear este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Perfil de Usuario y autorización *SECADM (si no está excluido en Key Officer Settings)
- Un Oficial de Claves configuración de autorizaciones “Maintain Key Officers” (Mantener Oficiales de Claves) está establecida en *YES

El mandato RMVKEYOFR no eliminará el perfil de usuario actual. Solo eliminará las autorizaciones de este perfil de usuario como Oficial de Claves del Sistema de Gestión de Claves.

Siga los siguientes pasos para **eliminar a un Oficial de Seguridad**:

1. Teclee **CRYPTO/RMVKEYOFR** y haga F4.
2. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line

3. Pulse Intro una vez haya modificado los valores de los parámetros

Nota: Cualquier mantenimiento realizado sobre los Oficiales de Claves se registrará en un archivo de auditoría.

```
                        Remove Key Officer (RMVKEYOFR)

Type choices, press Enter.

Key officer user profile . . . .   MARY_____     Name
```

Pantalla del mandato RMVKEYOFR

Descripción del campo del mandato RMVKEYOFR:

Key officer user profile Perfil de usuario del Oficial de Seguridad	Especificar el perfil de usuario que le corresponde a este Oficial de Claves en el IBM i o As/400, el cual desea eliminar como Oficial de Claves del sistema de gestión de claves.

4.4 Master Encryption Keys

Una clave MEK (Master Encryption Key) es una Clave Simétrica AES256 **bit utilizada para proteger (encriptando) las claves DEK** (Data Encryption Key) contenidas dentro de un Almacén de Claves. Puede crear hasta 8 claves MEK para cada entorno en su AS/400.

Por ejemplo, una clave MEK podría emplearse para proteger las claves DEK almacenadas en un Almacén de Claves y, una segunda MEK podría emplearse para proteger las claves DEK de nóminas almacenadas en otro Almacén de Claves.

Crypto Complete genera la clave MEK usando distintos passphrases introducidos por distintos oficiales de claves. Atendiendo a la política de su empresa pueden requerirse hasta 8 passphrases de distintos usuarios para generar una sola MEK. Las claves MEK se almacenan en un objeto *VLDL (Validation List) del System i (AS/400). Las claves MEK estarán encriptadas con la clave PEK (Clave de Encriptación del Producto).

```
CRYPTO2                    Master Encryption Key Menu


Select one of the following:

  1. Load Master Encryption Key       (LODMSTKEY)
  2. Set Master Encryption Key        (SETMSTKEY)
  3. Display Master Key Attributes    (DSPMSTKEY)
  4. Clear Master Encryption Key      (CLRMSTKEY)
```

Menú de Claves Master Key

a) Versiones de la Master Encryption Key (MEK)

Cada clave MEK puede tener hasta tres versiones con los siguientes nombres:

***NEW**	La versión *NEW es la versión de la clave MEK en que los usuarios mediante el mandato LODMSTKEY (Load Master Key) han introducido los passphrases. Esta clave *NEW **no puede utilizarse** para encriptar las claves DEK sitas en un Almacén de Claves. Es necesario convertir la versión *NEW a la versión *CURRENT. Esto solo puede hacerlo un Oficial de Claves con el mandato SETMSTKEY (Configurar Clave Master).
***CURRENT**	Es la versión actual de la clave MEK que puede asociarse a los Almacenes de Claves.
***OLD**	Es la clave *CURRENT anterior a la actual clave *CURRENT. No puede asociarse a los nuevos Almacenes de Claves. Pero puede suceder que las claves DEK en un Almacén de Claves actual todavía estén encriptadas bajo esta versión *OLD hasta que se traduzcan con el mandato (TRNKEYSTR).

b) Cargar Master Encryption Key (LODMSTKEY)

El mandato **LODMSTKEY** permite a los usuarios autorizados especificar las partes del passphrase para una versión *NEW de la clave MEK.

Nota: Las versiones *OLD y *CURRENT de la clave MEK no se verán afectadas por el mandato LODMSTKEY

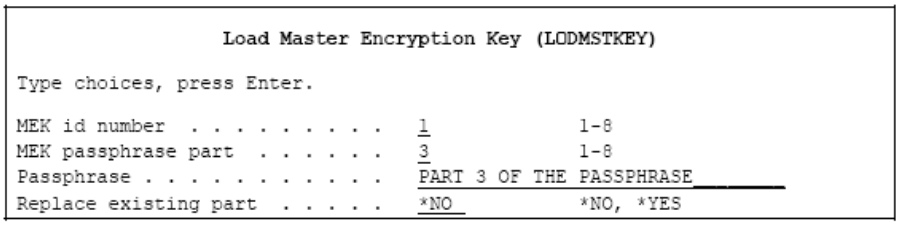
Los siguientes usuarios pueden utilizar este mandato:

- Perfil de usuario QSECOFR si no está excluido en Key Officer Settings)
- Perfil de usuario con autorización *SECADM si no está excluido en Key Officer Settings)
- Un Oficial de Claves que tenga la configuración de autorizaciones “Load MEK passphrase parts” (Cargar partes del passphrase de la Clave MEK) establecida en *YES

La política por defecto de claves requiere que CADA PARTE DEL PASSPHRASE SEA INTRODUCIDO POR UN PERFIL DE USUARIO DISTINTO.

Siga los siguientes pasos para **cargar la clave MEK**:

1. Introduzca el mandato **CRYPTO/LODMSTKEY** y haga F4
2. Pulse F1 sobre cualquier parámetro para obtener información on-line.
3. Pulse Intro después de introducir los valores de los parámetros.



```
                  Load Master Encryption Key (LODMSTKEY)

Type choices, press Enter.

MEK id number  . . . . . .  1              1-8
MEK passphrase part  . . . .  3            1-8
Passphrase . . . . . . . . .  PART 3 OF THE PASSPHRASE_______
Replace existing part  . . . .  *NO        *NO, *YES
```

Pantalla del Mandato LODMSTKEY

Descripción de claves del mandato LODMSTKEY

MEK id number	Indique el número de id de la clave versión *NEW de la clave MEK para cargar con un passphrase nuevo.
MEK passphrase part	Indique qué parte del passphrase, de cuantas partes determino en la Política de Claves, correspondiente a ese número de id (de ocho posibles) está introduciendo. El orden de introducción de las partes no altera el resultado. Por ejemplo, puede introducir la tercera parte y luego la primera para finalmente introducir la segunda.
Passphrase	Escriba aquí el passphrase (frase corta) con un máximo de 32 caracteres. RECUERDE: El passphrase es sensible a las mayúsculas y nunca puede ser igual a otro passphrase ya introducido para otra parte de la misma clave *NEW MEK que estamos creando.
Replace existing part	Indicar si el passphrase introducido sustituirá al passphrase existente para esa parte especificada. Es muy útil si el passphrase se introdujo equivocadamente.

PRECAUCIÓN:

- Las distintas partes del passphrase empleadas para cargar la clave MEK deberían guardarse en un sitio seguro (no su propio sistema).
- Una clave MEK no puede simplemente restaurarse bajo otro Número de Serie de otro sistema o copiarse a otro sistema con número de serie distinto.
- Si necesita recrear la misma clave MEK en una máquina con otro Número de Serie (recuperación en caso de emergencia) se deberán reintroducir y cargar las mismas partes del passphrase con el mismo número de partes y mismo orden.

c) Establecer la Master Encryption Key (SETMSTKEY)

PRECAUCIÓN:
El mandato SETMSTKEY reemplazará la versión *OLD de la clave MEK (si ya existe una clave *OLD anterior) con la versión *CURRENT. Antes de ejecutar este mandato debería utilizar el mandato TRNKEYSTR para reencriptar (traducir) las claves DEK contenidas en sus Almacenes de Claves que aún están encriptadas con la clave *OLD.

Una vez se hayan introducido todos los passphrases utilizados para crear una clave MEK, ya podemos configurar la versión *CURRENT con el mandato SETMSTKEY. Este mandato realiza los siguientes pasos:

1. Efectúa un Back Up del objeto *VLDL lista de validación CRVL001 que contiene las claves MEK encriptadas, en un SAVF (nombrados secuencialmente)
2. Se genera la versión *NEW de la clave MEK (mediante los passphrases cargados)
3. La versión *OLD se elimina
4. La versión *CURRENT, la actual, se copia donde estaba la versión *OLD
5. La versión *NEW se copia donde estaba la clave *CURRENT
6. La versión *NEW se elimina

Los siguientes usuarios pueden utilizar el mandato SEMSTKEY:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Perfil de usuario con autorización *SECADM si no está excluido en Key Officer Settings)
- Un Oficial de Claves que tenga la configuración de autorizaciones “Set and Clear MEKs” (Configurar y borrar MEKs) establecida en *YES

Siga los siguientes pasos para **configurar la clave MEK**:

1. Introduzca el mandato **CRYPTO/SETMSTKEY** y haga F4
2. Pulse F1 sobre cualquier parámetro para obtener información on-line.
3. Pulse Intro después de introducir los valores de los parámetros.

Nota: El mantenimiento de las Claves Maestras de Encriptación quedará registrado en un log.

```
                Set Master Encryption Key (SETMSTKEY)

Type choices, press Enter.

MEK id number  . . . . . .   1            1-8
```

Pantalla del mandato SETMSTKEY

Descripción de campos del mandato SETMSTKEY:

MEK id number	Indica el número de id de la clave MEK a configurar.

⚠ **PRECAUCIÓN:** Después de ejecutar el mandato SETMSTKEY, si tuviéramos claves DEK en Almacenes de Claves encriptados con la MEK, debería reencriptar las claves DEK del Almacén de claves con el mandato TRNKEYSTR

d) Ver Atributos de la Clave de Encriptación (DSPMSTKEY)

El mandato **DSPMSTKEY** permite ver a los usuarios autorizados los atributos de las Claves Maestras. En el caso de una Clave Maestra *NEW, los atributos visibles serán el número total de partes del passphrase especificadas para la Clave Maestra, junto con los perfiles de usuario (y fecha de creación) que definieron esas partes.

Para las claves Maestras *CURRENT y *OLD se mostrará el valor de verificación de la clave junto con el perfil de usuario (y fecha de creación) que establecieron la Clave Maestra con el mandato SETMSTKEY.

Realice los siguientes pasos para **ver los atributos de la Clave Maestra**:

1. Introduzca el mandato **CRYPTO/DSPMSTKEY** y haga F4
2. Introduzca el id de la Clave Maestra y la versión que quiera ver y pulse Intro
3. Se mostrarán los atributos de la Clave Maestra

Nota: El valor actual de la Clave de Encriptación Maestra (MEK) no puede verse.

```
                Display Master Key Attributes (DSPMSTKEY)

Type choices, press Enter.

MEK id number  . . . . . .   5
Version  . . . . . .  . . .  *NEW
Total parts required . . . . .   3
Total parts specified  . . . . .   2
Part 1 user  . . . . . .  . . .  MARY
Part 1 date/time . . . . . .  .  '2006-06-21-01.13.53.760000'
Part 2 user  . . . . . .  . . .
Part 2 date/time . . . . . .  .
Part 3 user  . . . . . .  . . .  QSECOFR
Part 3 date/time . . . . . .  .  '2006-06-24-20.25.36.968000'
```

Ejemplo de una clave maestra *NEW:

```
                Display Master Key Attributes (DSPMSTKEY)

Type choices, press Enter.

MEK id number  . . . . . .   5
Version  . . . . . .  . . .   *CURRENT
Key verification value . . . . .   92205F1E356E93D144132E172D4F08DC49EC8E39

Last modified by user  . . . . .   QSECOFR
Last modified date/time  . . . .   '2007-10-15-15.09.38.257000'
```

Ejemplo de una Clave Maestra *CURRENT:

Nota: Por cada Clave Maestra Crypto Complete genera un valor de verificación de clave (KEYVV). Este valor es distinto (y tiene un propósito distinto) al valor actual de la Clave Maestra. Este valor KEYVV se almacenará junto con cada Almacén de Claves creado utilizando esa clave maestra.

Cuando una aplicación o usuario trate de acceder a un Almacén de Claves, Crypto Complete comparará los valores KEYVV del Almacén de Claves y su correspondiente Clave Maestra. Si coinciden, entonces la Clave Maestra será considerada como válida para ese Almacén de Claves.

e) Borrar la Clave Maestra de Encriptación (CLRMSTKEY)

El mandato **CLRMSTKEY** permite a los usuarios autorizados borrar las claves *NEW y *OLD de una Clave de Encriptación Maestra (MEK). Antes de que se borre la clave MEK, se efectúa un backup a un objeto SAVE FILE (Nombrado secuencialmente) del objeto *VLDL lista de validación CRVL001 que contiene las claves MEK encriptadas.

> **PRECAUCIÓN:** NO BORRE una clave *OLD de una clave MEK si existen aún Almacenes de Claves que fueron encriptados con esta clave *OLD. Debería primero utilizar el mandato TRNKEYSTR para volver a encriptar las claves DEK de los almacenes de claves que continúan encriptadas con la versión *OLD de la clave MEK.

Los siguientes usuarios pueden utilizar este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Perfil de usuario con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un Oficial de Claves que tenga la configuración de autorizaciones “Set and Clear MEKs” (Configurar y borrar claves MEK) establecida en *YES

Realice los siguientes pasos para **eliminar la Clave de Encriptación Maestra**:

1. Introduzca el mandato **CRYPTO/CLRMSTKEY** y haga F4
2. Pulse F1 sobre cualquier parámetro para obtener información on-line.
3. Pulse Intro después de introducir los valores de los parámetros.

```
                    Clear Master Encryption Key (CLRMSTKEY)

Type choices, press Enter.

MEK id number  . . . . . .  1            1-8
Version  . . . . . . . . .  *NEW         *OLD, *NEW
```

Pantalla del mandato CLRMSTKEY

Descripción de campos del mandato CLRMSTKEY:

MEK id number	Indica el número de id de la clave MEK a borrar.
Versión	Especificar la versión a eliminar: *NEW o *OLD.

Nota i/OS V6R1: Los mandatos SETMSTKEY y CLRMSTKEY coinciden en la V6R1 con mandatos de IBMi, por lo que para llamar a los de Crypto, es necesario hacerlo a través del menú o bien añadir la biblioteca CRYPTO delante del mandato. (CRYPTO/SETMSTKEY).

4.5 Almacén de Claves

Las claves DEK (Data Encryption Key) se encuentran alojadas en los Almacenes de Claves. Usted puede crear uno o más Almacenes de Claves en su AS/400-IBM i. Por ejemplo, un Almacén de Claves puede utilizarse para contener las claves DEK que protegen datos de Entrada de Pedidos y un segundo Almacén de Claves para contener las claves que protegen los datos de las nóminas.

Cada Almacén de Claves se crea como un objeto (*VLDL) de lista de validación en el AS/400-IBM i. El nombre del objeto *VLDL se especifica con el mandato CRTKEYSTR, (Create Key Store) . Las claves DEK alojadas en el Almacén de claves son encriptadas utilizando la Clave de Encriptación Maestra (MEK) especificada por el usuario.

```
CRYPTO3                  Symmetric Encryption Key Menu


Select one of the following:

  1. Create Key Store                (CRTKEYSTR)
  2. Display Key Store Attr.         (DSPKEYSTR)
  3. Translate Key Store             (TRNKEYSTR)

 10. Work with Symmetric Keys        (WRKSYMKEY)
 11. Create Symmetric Key            (CRTSYMKEY)
 12. Change Symmetric Key            (CHGSYMKEY)
 13. Display Symmetric Key Attr.     (DSPSYMKEY)
 14. Copy Symmetric Key              (CPYSYMKEY)
 15. Export Symmetric Key            (EXPSYMKEY)
 16. Delete Symmetric Key            (DLTSYMKEY)
 20. Import Protegrity Key(s)        (IMPPTGKEY)
```

Menú de Gestión de Almacén de Claves y Claves Simétricas

a) Crear un Almacén de Claves (CRTKEYSTR)

El mandato **CRTKEYSTR** puede ser utilizado por los usuarios autorizados para crear un Almacén de Claves nuevo. Este se creará como un objeto *VLDL (Lista de Validación) de AS/400-IBM i.

Los siguientes usuarios pueden utilizar este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Perfil de usuario con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un Oficial de Claves que tenga la configuración de autorizaciones “Maintain Key Stores” (Mantener Almacenes de Claves) establecida en *YES

El mandato CRTKEYSTR, requiere que el perfil de usuario tenga autorización al mandato CRTVLDL(Crear lista de validación) de IBM.

Realice los siguientes pasos para **crear un nuevo Almacén de Claves** (Key Store):

1. Introduzca el mandato **CRYPTO/CRTKEYSTR** y haga F4
2. Pulse F1 sobre cualquier parámetro para obtener información on-line.
3. Pulse Intro después de introducir los valores de los parámetros.

PRECAUCIÓN: Se recomienda NO crear sus Almacenes de Claves en la biblioteca CRYPTO. Sería mejor crear una biblioteca (por ejemplo, KEYSTORES) solo para contener sus Almacenes de Claves. Asegúrese que esta biblioteca forma parte de sus procesos habituales de backup.

```
                    Create Key Store (CRTKEYSTR)

Type choices, press Enter.

Key store name . . . . . .   PAYROLLDEK      Name
  Library  . . . . . . . .     KEYSTRLIB      Name
MEK id number  . . . . . .   1               1-8
Description  . . . . . . .   Key Store for Payroll Data Encryption Keys
Public authority . . . . .   *EXCLUDE   *EXCLUDE, *USE, *CHANGE, *ALL
```

Pantalla del mandato CRTKEYSTR

Descripción de campos del mandato CRTKEYSTR:

Key store name	Indicar el nombre del Almacén de Claves, que se crea como un objeto *VLDL de lista de validación en su AS/400.
Library	Indicar la biblioteca que contiene el Almacén de Claves.
MEK id number	Indicar el número de id de la clave MEK que se utilizará para encriptar las claves DEK guardadas en el Almacén de Claves. Debe existir una versión *CURRENT de la clave MEK.
Description	Indicar una descripción para el Almacén de Claves.
Public authority	Indicar los derechos de autorización *PUBLIC de ese Almacén de Claves. Por defecto *EXCLUDE.

b) Traducir el Almacén de Claves (TRNKEYSTR)

El mandato TRNKEYSTR permite a los usuarios autorizados reencriptar las claves DEK dentro de un Almacén de Claves con la nueva versión *CURRENT de la clave MEK.

Antes de que se lleve a cabo esa traducción o reencriptación, el objeto *VLDL de lista de validación, que contiene el Almacén de Claves será salvado con un Backup en un objeto Save File (nombrado secuencialmente) dentro de la biblioteca de Crypto Complete.

> **PRECAUCIÓN:** Es muy recomendable ejecutar el mandato TRNKEYSTR INMEDIATAMENTE DESPUES de ejecutar el mandato SETMSTKEY utilizado para reemplazar la versión *CURRENT con la nueva versión *NEW de la calve MEK.

Los siguientes usuarios pueden utilizar este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Perfil de usuario con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un Oficial de Claves que tenga la configuración de autorizaciones “Maintain Key Stores” (Mantener Almacenes de Claves) establecida en *YES

```
                    Translate Key Store (TRNKEYSTR)

Type choices, press Enter.

Key store name . . . . . .   PAYROLLDEK     Name
  Library  . . . . . .         KEYSTRLIB     Name

To MEK id number . . . . . .   2             1-8
```

Pantalla del mandato TRNKEYSTR

Descripción de campos del mandato TRNKEYSTR:

Key store name	Indicar el nombre del Almacén de Claves a traducir (Reencriptar).
Library	Indicar el nombre de la biblioteca que contiene el Almacén de Claves.
To MEK id number	Indicar el número de id de la clave MEK que será utilizada para traducir (Reencriptar) las claves DEK contenidas en el Almacén de Claves indicado. Recuerde que la versión *CURRENT de la MEK especificada debe existir.

Importante: Después de ejecutar el mandato TRNKEYSTR, debería comprobar que los valores de verificación de claves coinciden entre el Almacén de Claves y el de la clave Maestra, viendo esos valores mediante los mandatos DSPMSTKEY y DSPKEYSTR

Notas: - El mandato TRNKEYSTR puede ejecutarse mientras los usuarios y aplicaciones están activos en el sistema.
- Este mandato NO MODIFICARA ningún dato contenido en sus archivos de base de datos.
- Los datos existentes NO NECESITARAN ser reencriptados una vez hecha la traducción.

c) Autorizaciones del Almacén de Claves

Dado que el Almacén de Claves se crea como un objeto *VLDL (Validation List) del AS/400-IBM i, usted puede controlar las autorizaciones de acceso al Almacén de Claves mediante el mandato de IBM, **EDTOBJAUT** (Edit Object Authority) para editar autorizaciones del objeto.

Así pues, para poder editar las autorizaciones del Almacén de Claves debe tener:

- Autorización para uso del mandato EDTOBJAUT
- Derechos de *OBJMGT sobre el objeto Lista de Validación

Realice los siguientes pasos para **editar las autorizaciones de acceso al objeto Lista de Validación que contiene el Almacén de Claves**:

1. Introduzca el mandato, EDTOBJAUT OBJ(*library* / *vldlist*) OBJTYPE(*VLDL) donde *library* es la biblioteca que contiene la Lista de Validación y *vldlist* es el nombre de la Lista de Validación del Almacén de Claves
2. Especifique las autorizaciones para ese objeto
3. Pulse Intro una vez haya introducido todas las autorizaciones

Recomendación: Estas son nuestras recomendaciones para la autorización de los objetos (*VLDL) Lista de Validación del Almacén de Claves:

- Excluya la autorización *PUBLIC de este objeto.
- Solo garantice la autorización *USE a aquellos usuarios que necesiten usar las claves DEK del Almacén de Claves (Lista de Validación) para cifrar y descifrar datos.
- Solo garantice la autorización *CHANGE a aquellos usuarios que siendo Oficiales de Claves estén autorizados para crear nuevas claves DEK en el Almacén de Claves.

Nota: La autorización de objetos dentro de un Almacén de Claves controlará que usuarios pueden gestionar claves en dicho almacén así como que usuarios pueden utilizar las claves dentro del Almacén de Claves para encriptar y desencriptar datos.

Si un usuario intenta acceder a un almacén de claves para el cual no tiene autorización a través de las pantallas de Crypto Complete o de las APIs, el error de autorización será auditado en el log.

Consejo: Las Estrategias de Gestión de Claves Avanzadas se discuten en el apéndice A.

d) Ver Atributos del Almacén de Claves (DSPKEYSTR)

El mandato **DSPKEYSTR** permite a los usuarios autorizados ver los atributos de un Almacén de Claves. Es muy útil para ver el número de id y versión de la clave MEK bajo la cual se están encriptando las entradas en el Almacén de Claves.

Realice los siguientes pasos para **ver los atributos del almacén de claves**:

1. Introduzca el mandato **CRYPTO/DSPKEYSTR** y haga F4
2. Introduzca el nombre del almacén y biblioteca
3. Se mostrarán los atributos
4. Pulse F1 sobre cualquier parámetro para obtener información on-line

```
                Display Key Store Attributes (DSPKEYSTR)

Type choices, press Enter.

Key store name . . . . . .   PAYROLLDEK
  Library  . . . . . .         KEYSTRLIB
MEK id number  . . . . . .   5
MEK version  . . . . . .     *CURRENT
MEK key verification value . . .   92205F1E356E93D144132E172D4F08DC49EC8E39

Last modified by user  . . . . .   QSECOFR
Last modified date/time  . . . .   '2006-06-27-10.27.06.678000'
```

Pantalla del mandato DSPKEYSTR

Nota: El valor de verificación KEYVV de la clave Maestra se almacena junto con cada Almacén de Claves creado mediante esa Clave Maestra. Cuando un usuario o aplicación trata de acceder al Almacén de Claves, Crypto Complete comparará el valor KEYVV existente con el de su Clave Maestra correspondiente. Si coinciden, entonces la Clave Maestra es considerada como buena para el Almacén de Claves.

e) Borrar un Almacén de Claves

Dado que el Almacén de Claves se crea como un objeto (*VLDL) Lista de Validación en su System i (AS/400), puede borrar un Almacén de Claves con el mandato DLTVLDL (Borrar Lista de Validación) de IBM.

Para borrar un Almacén de Claves, el usuario debe tener:

- Autorización al mandato DLTVLDL
- Derechos *OBJEXIST sobre el objeto Lista de Validación.

Precaución:
- NO BORRE un Almacén de Claves que contenga claves DEK necesarias para desencriptar datos existentes.
- SIEMPRE realice un BACKUP del almacén de claves antes de borrarlo.

Realice los siguientes pasos para **borrar un Almacén de Claves**:

1. **Haga un Backup** del objeto (*VLDL) Lista de Validación a un soporte externo o un objeto Save File
2. Introduzca el mandato DLTVLDL y haga F4
3. Especifique el nombre del Almacén de Claves y biblioteca que contiene el objeto lista de validación y pulse Intro

```
                    Delete Validation List (DLTVLDL)

Type choices, press Enter.

Validation list  . . . . . .   PAYROLLDEK    Name, generic*
  Library  . . . . . . . . .     KEYSTRLIB   Name, *LIBL, *CURLIB...
```

Pantalla del mandato DLTVLDL

Descripción de campos del mandato DLTVLDL:

Validation list	Indicar el nombre del objeto VLDL Lista de Validación que contiene el Almacén de Claves que quiere borrar.
Library	Indicar la biblioteca que contiene el objeto Lista de Validación.

4.6 Claves de Encriptación de Datos DEK

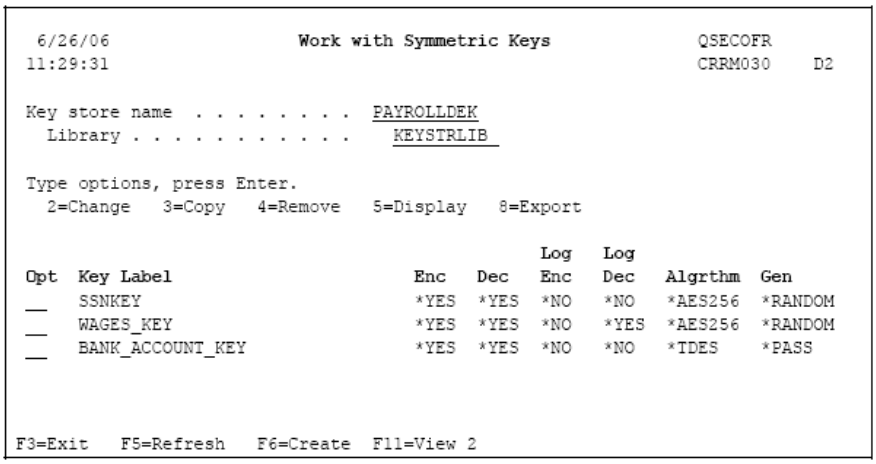
Una clave DEK (Data Encryption Key), es una clave simétrica que sirve tanto para encriptar y desencriptar datos. Cualquier usuario autorizado puede crear una o más claves DEK que se almacenarán en los Almacenes de Claves. Por ejemplo, podría crearse una clave para encriptar/desencriptar números de tarjetas de crédito y una segunda clave para encargada de encriptar/desencriptar números de la seguridad social.

a) Trabajar con Claves Simétricas (WRKSYMKEY)

El mandato **WRKSYMKEY** permite a los usuarios autorizados trabajar con las Claves de Encriptación de Datos (DEK) (claves simétricas) almacenadas en el Almacén de Claves (Key Store). Este mandato incluye funciones para crear, cambiar y borrar claves.

Realice los siguientes pasos para **trabajar con claves simétricas DEK alojadas en el Almacén de Claves**:

1. Introduzca el mandato **CRYPTO/WRKSYMKEY** y pulse F4
2. Especifique el nombre y biblioteca del Almacén de Claves y pulse Intro
3. Se mostrarán las Claves Simétricas que existen actualmente en el Almacén de Claves



Pantalla del mandato WRKSYMKEY

Opciones de la pantalla: Disponibles por cada clave mostrada en la pantalla.

Opción	Descripción
2	Ver un prompt para cambiar los atributos de la llave mediante el mandato CHGSYMKEY.
3	Ver un prompt para copiar los atributos de la clave con el mandato CPYSYMKEY.
4	Ver un prompt para confirmar la eliminación de una clave con el mandato DLTSYMKEY.
5	Ver los atributos de la clave. No se mostrará el valor actual de la clave.
8	Exportar el valor de la clave actual con el mandato EXPSYMKEY (si lo permite la Política de Claves previamente establecida).

Teclas de función de la pantalla WRKSYMKEY:

Opción	Descripción
F3	Salir de la pantalla WRKSYMKEY.
F5	Actualizar la lista de Claves del Almacén de Claves.
F6	Ver un prompt para crear una nueva clave con el mandato CRTSYMKEY.

b) Crear un Clave Simétrica (CRTSYMKEY)

El mandato **CRTSYMKEY** permite a los usuarios autorizados crear NUEVAS claves DEK (Claves Simétricas) y almacenarlas en el Almacén de Claves elegido.

Los siguientes usuarios pueden utilizar el mandato CRTSYMKEY:

- Perfil de usuario QSECOFR si no está excluido en Key Officer Settings)
- Perfil de usuario con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un Oficial de Claves que tenga la configuración de autorizaciones “Maintain DEKs” (Mantener DEKs) establecida en *YES

El usuario debe tener: Autorización *CHANGE para acceder al objeto (*VLDL) Lista de Validación que contiene el Almacén de Claves en que se crearán las claves.

Realice los siguientes pasos para **crear una nueva clave simétrica DEK**:

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

```
                  Create Symmetric Key (CRTSYMKEY)

Type choices, press Enter.

Key label  . . . . . .  SSNKEY

Key store name . . . . . .  PAYROLLDEK    Name, *DEFAULT
  Library  . . . . . .  KEYSTRLIB   Name
Encryption allowed with key  . .  *YES      *YES, *NO
Decryption allowed with key  . .  *YES      *YES, *NO
Log encryption usage . . . . . .  *NO       *YES, *NO
Log decryption usage . . . . . .  *NO       *YES, *NO
Key algorithm  . . . . . .  *AES256    *AES256, *AES192, *AES128...
Key generation option  . . . . .  *RANDOM    *RANDOM, *PASS, *MANUAL
```

Pantalla del mandato CRTSYMKEY

Descripción de campos del mandato CRTSYMKEY:

Key label	Indicar un nombre único (etiqueta) para la clave de hasta 30 caracteres. No permite espacios ni algunos caracteres especiales. Si puede contener el guión bajo (underscore). No es sensible a mayúsculas ni minúsculas. Se almacenará en mayúsculas.
Key store name Library	Indicar el nombre y biblioteca del Almacén de Claves que contendrá las claves creadas. Especifique *DEFAULT para utilizar, por defecto, el nombre de Almacén de Claves especificado en la Política de Claves. Debe tener autorización *CHANGE sobre el objeto *VLDL.
Encryption allowed with key	Indica si la llave se puede utilizar para encriptar.
Decryption allowed with key	Indica si la clave se puede utilizar para desencriptar.
Log encryption usage	Indicar si el uso de la Clave de Encriptación se almacenará en el archivo de auditoría (audit journal log). Nota: La auditoría implica un impacto adicional en el rendimiento y en el consumo de disco.
Log decryption usage	Indicar si el uso de la Clave de Desencriptación se almacenará en el archivo de auditoría (audit journal log). Nota: La auditoría implica un impacto adicional en el rendimiento y en el consumo de disco.
Key algorithm	Indicar el algoritmo utilizado para crear la clave. Los valores permitidos son *AES256, *AES192, *AES128 y *TDES.
Key generation option	Indicar como se generará la clave: *RANDOM.-Crypto Complete la genera aleatoriamente. La opción más segura. *PASS.- Se genera basándose en un passphrase del usuario y otra parte aleatoria definida en un “iteration count” y “salt”.- Utiliza la función PBKDF2 pseudorandom detallada en RFC2898) *MANUAL.- El usuario introduce la clave manualmente.

Nota: El valor salt son datos aleatorios que pueden utilizarse junto con los datos cifrados o hash para aumentar las defensas necesarias para proteger los datos de ataques de diccionario por fuerza bruta. Se suele colocar delante de los datos cifrados o hash.

Un hash es un valor numérico de longitud fija que identifica datos de forma unívoca. Los valores hash se utilizan para comprobar la integridad de los datos que se envían a través de canales no seguros.

Parámetros adicionales.... si se especifica la opción *PASS en Key Generation Option

Passphrase	Especificar un passphrase de hasta 256 caracteres de longitud.
Salt	Indicar un valor “salt” (aleatorio) para alterar el algoritmo.
Iteration count	Indicar una valor para la cuenta iterativa entre 1-50000 para alterar el algoritmo de generación de claves.
ASCII input format	Indica el código de caracteres para el passphrase y salt: *YES – Utilizará el ASCII *NO – Utilizará el EBCDIC

Parámetros adicionales…. si se especifica la opción *MANUAL en Key Generation Option:

Key value format	Indicar el formato del valor de la clave que se va a introducir: *HEX - El valor de la clave introducido es hexadecimal *CHAR - El valor de la clave se introduce en formato de caracteres *BASE64 - El valor de la clave se introduce en formato BASE64
Key value	Especifica el valor de la clave.
KEK Key Label	Indica la etiqueta de la Key Encrytpion Key (KEK) con que la llave simétrica es encriptada.
KEK key store name	Indica el nombre del objeto y biblioteca del Almacén de Claves que contiene la Key Encryption Key (KEK).

c) Cambiar Claves Simétricas (CHGSYMKEY)

El mandato **CHGSYMKEY** permite a los usuarios autorizados cambiar los atributos de una clave DEK (Clave simétrica).

Los siguientes usuarios pueden utilizar el mandato CHGSYMKEY:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Perfil de usuario con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un Oficial de Claves que tenga la configuración de autorizaciones “Maintain DEKs” (Mantener DEKs) establecida en *YES

El usuario debe tener autorización *CHANGE para acceder al objeto *VLDL (Lista de Validación) que contiene el Almacén de Claves.

Realice los siguientes pasos para **cambiar los atributos de la clave simétrica DEK:**

1. Introduzca el mandato **CRYPTO/CHGSYMKEY** y pulse F4
2. Introduzca los nombres del Almacén de Claves y la Etiqueta de la Clave y pulse Intro
3. Se mostrarán los atributos de la Clave Simétrica actual (valores de parámetros)
4. Pulse F1 para sobre cualquier parámetro para obtener ayuda on-line
5. Pulse Intro tras introducir los valores para los parámetros.

```
                    Change Symmetric Key (CHGSYMKEY)

Type choices, press Enter.

Key label  . . . . . . . . . . .   SSNKEY
Key store name . . . . . . . . .   PAYROLLDEK     Name, *DEFAULT
  Library  . . . . . . . . . . .     KEYSTRLIB    Name
Encryption allowed with key  . .   *YES           *YES, *NO
Decryption allowed with key  . .   *YES           *YES, *NO
Log encryption usage . . . . . .   *NO            *YES, *NO
Log decryption usage . . . . . .   *NO            *YES, *NO
```

Pantalla del Mandato CHGSYMKEY

Descripción de campos del mandato CHGSYMKEY

Key label	Indicar el nombre de la etiqueta de la Clave a cambiar.
Key store name Library	Indicar el nombre y biblioteca del Almacén de Claves que contiene la Clave. Especifique *DEFAULT, para usar el nombre de Almacén de Claves establecido por defecto en la Política de Claves. Debe tener autorización *CHANGE para el objeto *VLDL del Almacén de Claves.
Encryption allowed with key	Indicar si la Clave puede ser utilizada para encriptar.
Decryption allowed with key	Indicar si la Clave puede ser utilizada para desencriptar.
Log encryption usage	Indicar si el uso de la Clave de encriptación se guardará en un log.
Log decryption usage	Indicar si el uso de la Clave de desencriptación se guardará en un log.

d) Copiar Claves Simétricas (CPYSYMKEY)

El mandato **CPYSYMKEY** permite a los usuarios autorizados copiar las claves DEK entre distintos Almacenes de Claves.

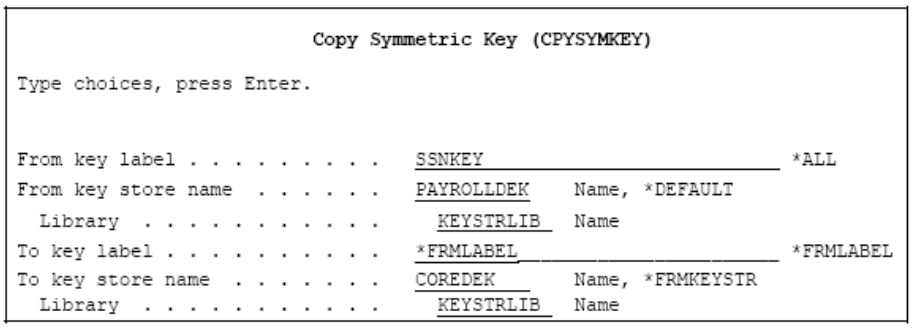
Los siguientes usuarios pueden utilizar el mandato CPYSYMKEY:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Perfil de usuario con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un Oficial de Claves que tenga la configuración de autorizaciones “Maintain DEKs” (Mantener DEKs) establecida en *YES

El usuario debe tener autorización *CHANGE para acceder al objeto *VLDL (Lista de Validación) del Almacén de Claves al que se quieren copiar las Claves.

Realice los siguientes pasos para **copiar una nueva clave simétrica DEK**:

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



Pantalla del mandato CPYSYMKEY

Descripción de los campos del mandato CPYSYMKEY:

From key label	Indicar la etiqueta de la Clave. Especifique *ALL para copiar todas las claves.
From key store name Library	Indicar el nombre y biblioteca del almacén de claves que contiene la clave. Especifique *DEFAULT para utilizar el Almacén de Claves especificado por defecto en la Política de Claves.
To key label	Indicar el nombre de la etiqueta nueva para la clave copiada. Especificar *FRMLABEL para utilizar el nombre que tuviera en el campo "From key label".
To key store name - Library	Indicar el nombre y biblioteca del Almacén de Claves en que se copiará la Clave. Especifique *FRMKEYSTR para copiar en un Almacén de Claves que utilizará el nombre de "From key store name". Debe tener autoridad *CHANGE para el objeto *VLDL Almacén de Claves.

e) Ver Atributos de las Claves Simétricas (DSPSYMKEY)

El mandato **DSPSYMKEY** permite a los usuarios autorizados ver los atributos de las Claves Simétricas (DEK)

Realice los siguientes pasos para **ver los atributos de la clave simétrica DEK**:

1. Introduzca el mandato **CRYPTO/DSPSYMKEY** y pulse F4
2. Introduzca los nombres del almacén de claves y la etiqueta de la clave y pulse Intro
3. Se mostrará los atributos de la Clave Simétrica junto a la fecha y hora (timestamp) en que se produjo el último cambio o se añadió y que usuario lo hizo.
4. Pulse F1 para sobre cualquier parámetro para obtener ayuda on-line

```
                  Display Symmetric Key Attr. (DSPSYMKEY)

Type choices, press Enter.

Key label  . . . . . . . . . . .   SSNKEY
Key store name . . . . . . . . .   PAYROLLDEK
  Library  . . . . . . . . . . .     KEYSTRLIB
Encryption allowed with key  . .   *YES
Decryption allowed with key  . .   *YES
Log encryption usage . . . . . .   *NO
Log decryption usage . . . . . .   *NO
Key algorithm  . . . . . . . . .   *AES256
Key generation option  . . . . .   *RANDOM
Last modified by user  . . . . .   QSECOFR
Last modified date/time  . . . .   '2009-06-27-11.27.21.017000'
Key owner  . . . . . . . . . . .   MARY
```

Pantalla del mandato DSPKEYSTR

f) Exportar Claves Simétricas (EXPSYMKEY)

El mandato **EXPSYMKEY** permite a los usuarios autorizados ver el valor actual de la Clave Simétrica (DEK) contenida en un Almacén de Claves. Este mandato es muy útil si el valor de la clave debe ser compartido con otro ordenador (distinto de un AS/400 - IBM i) que necesita encriptar y desencriptar utilizando la misma clave.

Se recomienda especificar una clave KEK (Key Encryption Key) que proteja la clave simétrica exportada.

La política de claves debe permitir la recuperación de valores de claves con el parámetro DEKRTVVAL(*YES) o(*KEK)

PRECAUCIÓN: Si un valor de una clave puede ser exportado (recuperado), entonces el valor podría ser utilizado para desencriptar datos sin necesidad de utilizar las APIs de Crypto Complete ni sus mecanismos de seguridad. Este riesgo puede ser eliminado si se mantiene el parámetro DEKRTVVAL de la política de claves en *NO.

Los siguientes usuarios pueden utilizar este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Perfil de usuario con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un Oficial de Claves que tenga la configuración de autorizaciones “Maintain DEKs” (Mantener Claves DEK) establecida en *YES

Realice los siguientes pasos para **exportar (ver) un valor de clave simétrica**:

1. Introduzca el mandato **CRYPTO/EXPSYMKEY** y haga F4
2. Introduzca la etiqueta de la clave y el nombre de almacén de claves y luego pulse Intro
3. Se mostrará el valor actual de la clave simétrica

```
                  Export Symmetric Key (EXPSYMKEY)

Type choices, press Enter.

Key label  . . . . . .  SSNKEY
Key store name . . . . .  PAYROLLDEK    Name, *DEFAULT
  Library  . . . . . .    KEYSTRLIB     Name, *LIBL
KEK key label  . . . . .  *NONE
KEK key store name . . . .  *DEFAULT     Name, *DEFAULT
  Library  . . . . . .      _________     Name, *LIBL
Key value format . . . . .  *HEX         *BASE64, *CHAR, *HEX
Key value  . . . . . .  C2D6C240D3E4C5C2C2C540C1E340D3C9D5D6D4C1
40E2D6C6E3E6C1D9C5404040
```

Pantalla del mandato EXPSYMKEY

Descripción de campos del mandato EXPSYMKEY:

Key label	Indicar el nombre de etiqueta (único) de la Clave a exportar.
Key store name Library	Indica el nombre de la biblioteca y del Almacén de Claves que contienen la Clave. Especifique *DEFAULT para utilizar el nombre del Almacén de Claves especificado en la política de claves por defecto. Debe tener la autorización *USE para acceder al objeto *VLDL Almacén de Claves.
KEK Key Label	Indica el nombre de etiqueta de la clave KEK (Key Encryption Key) a usar para encriptar la clave Simétrica que será exportada. La clave Simétrica será encriptada con el modo CBC y sin espacios (padding).
KEK Key store name Library	Indica el nombre y biblioteca del almacén de claves que contiene la clave KEK. Especifique *DEFAULT para utilizar el nombre del Almacén de Claves especificado en la política de claves por defecto. Debe tener la autorización *USE para acceder al objeto *VLDL Almacén de Claves.
Key value format	Indicar si la Clave debería mostrarse en hexadecimal, BASE64 o formato de caracteres. Normalmente la clave debería ser siempre exportada en *HEX o BASE64 para asegurar la compatibilidad con otros sistemas. El formato *CHAR debe usarse solo si la clave se introdujo manualmente en formato de caracteres (en el mandato CRTKEYSYM).
Key value	El valor de la clave recuperado.

g) Borrar Claves Simétricas (DLTSYMKEY)

El mandato **DLTSYMKEY** permite a los usuarios autorizados borrar una clave DEK (clave simétrica) del Almacén de Claves.

Los siguientes usuarios pueden utilizar este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Perfil de usuario con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un Oficial de Claves que tenga la configuración de autorizaciones “Maintain DEKs” (Mantener Claves DEK) establecida en *YES

El usuario debe tener autorización *CHANGE al objeto *VLDL Lista de validación el cual contiene el(los) Almacén(es) de Claves del que se quiere borrar una clave.

Antes de borrar una Clave se hará un Backup del objeto *VLDL Lista de Validación, que contiene el Almacén de Claves, en un objeto SAVE File (nombrado secuencialmente), dentro de la biblioteca de Crypto Complete.

PRECAUCIÓN: NO BORRE claves que pueda necesitar para desencriptar datos existentes.
Asegúrese de haber desencriptado todos los datos, ya sean campos de base de datos, archivos de salvado, objetos salvado o archivos de la IFS, que hubiera encriptado anteriormente con la clave DEK que pretende borrar.

Realice los siguientes pasos para **borrar el Almacén de Claves (Key Store):**

1. Introduzca el mandato **CRYPTO/DLTSYMKEY** y haga F4
2. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line
3. Introduzca los valores de los parámetros y pulse Intro

Nota: La Política de Claves por defecto no permite el borrado de claves.

```
                    Delete Symmetric Key (DLTSYMKEY)

Type choices, press Enter.

Key label  . . . . . . . . . . .   SSNKEY          _   _____________
Key store name . . . . . . . . .   PAYROLLDEK      Name, *DEFAULT
  Library  . . . . . . . . . . .     KEYSTRLIB     Name
```

Pantalla del mandato DLTSYMKEY

Descripción de campos del mandato DLTSYMKEY:

Key label	Indicar el nombre(etiqueta) de la Clave a borrar.
Key store name Library	Indicar el nombre y biblioteca del Almacén de Claves que contienen la Clave que desea borrar. Especifique *DEFAULT para utilizar el nombre del Almacén de Claves especificado por defecto en la Política de Claves. Debe tener autorización *CHANGE para acceder al objeto *VLDL del Almacén de Claves.

5. Alertas de Seguridad

Puede configurar alertas de seguridad para enviar notificaciones cuando se realicen actividades relacionadas con la Gestión de Claves. Esto puede incluir:

- Configuración de la Política de Claves
- Configuración de los Oficiales de Claves
- Master Encryption Keys (MEK)
- Data Encryption Keys (DEK)
- Entradas del Registro de Encriptación de Campos (si disponible).
- Configuración de las alertas

También, cuando se produzcan errores de autorización en Crypto Complete, como por ejemplo, si un usuario no autorizado intenta acceder al almacén de claves.

Nota: Las actividades relacionadas con la gestión de claves, así como los errores de autorización serán siempre registrados en el archivo de journal de auditoría de Crypto Complete, aún cuando no haya configurado ninguna alerta.

Para acceder a la configuración de alertas desde el menú principal, entre en la opción 1, "Key Policy and Security Menu" y también mediante el mandato:

GO CRYPTO1

Desde esta nueva pantalla, podrá empezar a configurar las alertas de seguridad desde la opción 3 "Work with Security Alerts". También puede acceder con el mandato WRKCCALR.

a) Trabajar con Alertas (WRKCCALR)

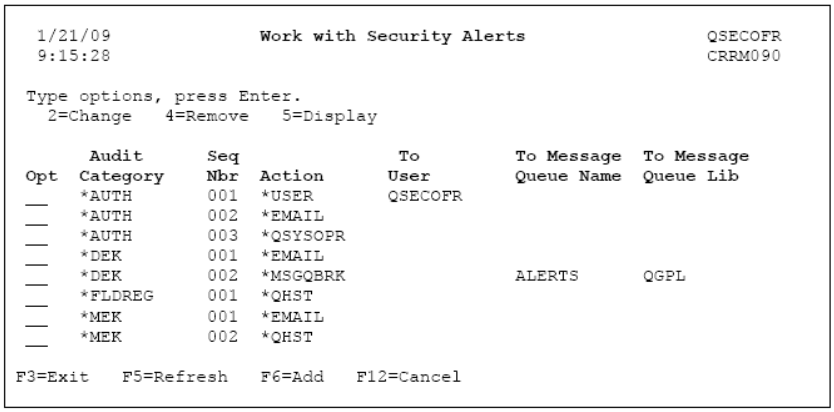
El mandato **WRKCCALR** permite a los usuarios autorizados configurar y ver las Alertas de Seguridad configuradas.

Los siguientes usuarios pueden utilizar este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones "Maintain Key Policy and Alerts" (Mantener Política de Claves y Alertas) está establecida en *YES

Siga los siguientes pasos para **trabajar con las Alertas de Seguridad**:

1. Pulse F4 en el mandato **CRYPTO/WRKCCALR**
2. Se mostrarán las Alertas de Seguridad que configuradas actualmente



Pantalla del mandato WRKCCALR con valores de ejemplo

Opciones de pantalla: Disponibles por cada alerta configurada mostrada en la pantalla.

Opción	Descripción
2	Muestra la opción para **cambiar** la configuración de la Alerta con el mandato CHGCCALR.
4	Muestra la opción para **borrar** la configuración de la Alerta con el mandato DLTCCALR.
5	Muestra la configuración actual de la Alerta con el mandato DSPCCALR.

Teclas de función: Estas son las teclas de función disponibles en la pantalla WRKCCALR.

Opción	Descripción
F3	Salir de la pantalla WRKCCALR.
F5	Refrescar la lista de Alertas.
F6	Muestra un prompt para añadir una nueva Alerta con el mandato ADDCCALR.

b) Añadir alerta (ADDCCALR)

El mandato **ADDCCALR** permite a un usuario autorizado añadir una nueva Alerta de Seguridad.

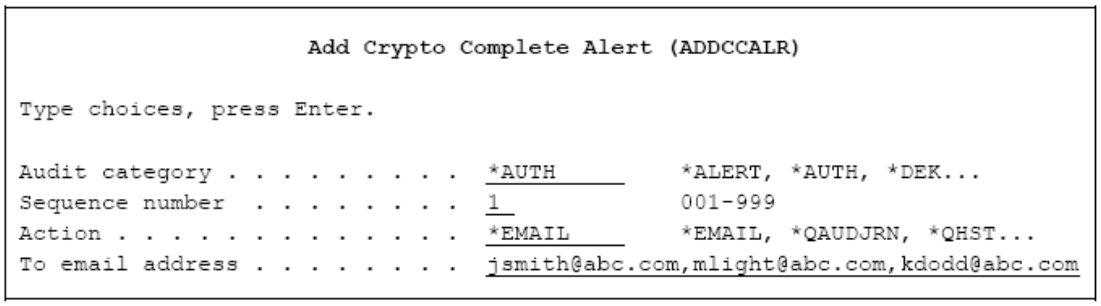
Los siguientes usuarios pueden utilizar este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain Key Policy and Alerts” (Mantener Política de Claves y Alertas) está establecida en *YES

Siga los siguientes pasos para **añadir una nueva Alerta de Seguridad**:

1. Pulse F4 en el mandato **CRYPTO/ADDCCALR**
2. Pulse F1 en cualquier parámetro para obtener ayuda
3. Pulse Intro cuando haya terminado de introducir los parámetros

Nota: Cualquier mantenimiento realizado sobre las Alertas de Seguridad será registrado en el archivo de journal de auditoría.



Pantalla del mandato ADDCCALR con valores de ejemplo

Descripción de campos del mandato ADDCCALR:

Audit Category	Indicar la categoría a auditada a controlar. Las categorías válidas para las cuales se controlará las actividades de mantenimiento o errores de autorización son:	
	*ALL	Todas
	*ALERT	Alertas de seguridad
	*AUTH	Errores autorización en Crypto Complete
	*DEK	Data Encryption Keys
	*FLDREG	Entradas del Registro de Campos
	*IFSREG	Entradas en el Registro de IFS
	*KEYOFR	Configuración del Oficial de Claves
	*KEYPCY	Configuración de la Política de Claves
	*MEK	Master Encryption Keys
Sequence number	Indica el número de secuencia de 1 a 999. Esto permite enviar múltiples alertas para cada Categoría Auditada.	
Action	Indicar la acción a realizar de entre las siguientes:	
	*EMAIL	Enviar e-mail a uno o más receptores con el mandato SNDDST.
	*MSGQBRK	Enviar mensajes a una cola de mensajes especificada con el mandato SNDBRKMSG.
	*MSGQINF	Enviar mensajes a una cola de mensajes especificada con el mandato SNDMSG.
	*QAUDJRN	Escribir entradas en el archivo de journal QAUDJRN.
	*PTGLOG	Solo válido para usuarios de Protegrity Defiance Enterprise Security Administrator (ESA).

Continuación Descripción de los campos ADDCCALR

Continúa valores Action	*QHST	Enviar mensajes al log QHST mediante el mandato SNDMSG.
	*QSYSOPR	Enviar mensajes al QSYSOPR mediante el mandato SNDMSG.
	*SYSLOG	Enviar mensajes un servidor de logs externo mediante el protocolo SYSLOG.
	*USER	Enviar mensajes a un Usuario mediante el mandato SNDMSG.
To email address	Si ACTION es *EMAIL, especificar las direcciones de correo electrónico. Separar con coma.	
To user profile	Si ACTION es *USER, especifique el Perfil de Usuario al que enviar el mensaje.	
To message queue name Library	Si ACTION es *MSGBRK o *MSGQINF, especifique el nombre y biblioteca de la Cola de Mensajes que recibirá los mensajes.	
Log host	Si ACTION es *SYSLOG o *PTLOG, especifique el nombre host o dirección IP del servidor de log.	
Log source port	Si ACTION es *SYSLOG, especifique el puerto local a utilizar cuando se conecte al servidor de log. El puerto por defecto de syslog es 514.	
Log destination port	Si ACTION es *SYSLOG o *PTLOG, especifique el puerto del servidor log.	

Nota: Si una Alerta de Seguridad configurada no funcionará, se enviará un mensaje al QSYSOPR y se registrará una entrada en el archivo de log de auditoría.

Alertas de Email

Si desea enviar Alertas vía E-mail utilizando el servidor SMTP del IBM i, debe asegurarse de configurar su sistema adecuadamente. A continuación mostramos un ejemplo.

Ejecute el siguiente mandato:

```
ADDDIRE USRID(INTERNET GATEWAY) USRD('Allow SNDDST to send INTERNET Mail')
SYSNAME(INTERNET) MSFSRVLVL(*USRIDX) PREFADR(NETUSRID *IBM ATCONTXT)
```

Cambie los atributos de distribución de email con el mandato:

```
CHGDSTA SMTPRTE(INTERNET GATEWAY)
```

Se requiere un directorio de entradas para cada usuario que pudiera enviar e-mail (con el mandato SNDDST) como Alerta de seguridad. Ejemplo:

```
ADDDIRE USRID(USERNAME SYSTEMNAME) USRD('User name') USER(USERNAME)
```

Ejecute el mandato SNDDST para enviar un e-mail de prueba y verificar que se recibió correctamente. Ejemplo:

```
SNDDST TYPE(*LMSG) TOINTNET(username@abc.com) DSTD('Test Email Subject')
LONGMSG('Test Message Text') SUBJECT(*DOCD)
```

Nota: Consulte con el administrador del Sistema antes de realizar cambios.

c) Cambiar alerta (CHGCCALR)

El mandato **CHGCCALR** permite a los usuarios autorizados cambiar la configuración de la Alerta de Seguridad.

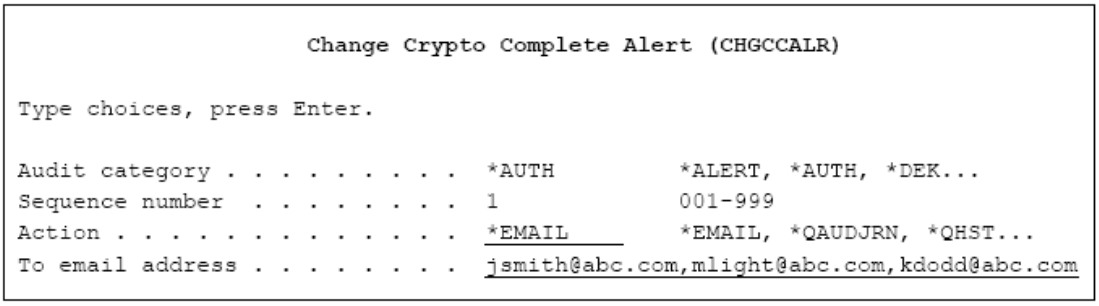
Los siguientes usuarios pueden utilizar este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain Key Policy and Alerts” (Mantener Política de Claves y Alertas) está establecida en *YES

Siga los siguientes pasos para **cambiar una Alerta de Seguridad**:

1. Pulse F4 en el mandato **CRYPTO/CHGCCALR**
2. Introduzca la categoría auditada y en número de secuencia y pulse Intro
3. Se mostrará la configuración de alertas (valores de los parámetros).
4. Pulse F1 en cualquier parámetro para obtener ayuda
5. Pulse Intro cuando haya terminado de introducir los parámetros

Nota: Cualquier mantenimiento realizado sobre las Alertas de Seguridad será registrado en el archivo de journal de auditoría.



Pantalla del mandato CHGCCALR con valores de ejemplo

Vea la descripción de campos del mandato ADDCCALR mostrada anteriormente para más información sobre los parámetros.

d) Visualizar Alertas (DSPCCALR)

El mandato **DSPCCALR** permite a un usuario autorizado ver la configuración de una Alerta de Seguridad.

Siga los siguientes pasos para **ver una Alerta de Seguridad**:

1. Pulse F4 en el mandato **CRYPTO/DSPCCALR.**
2. Introduzca la categoría auditada y el número de secuencia y pulse Intro.

3. Se mostrará la configuración de la Alerta (valores de los parámetros) además del usuario y hora en que se añadió o modificó por última vez.
4. Pulse F1 en cualquier parámetro para obtener ayuda.

```
                Display Crypto Complete Alert (DSPCCALR)

Type choices, press Enter.

Audit category . . . . . .  *AUTH
Sequence number  . . . . . .  1
Action . . . . . .  *EMAIL
To email address . . . . . .  jsmith@abc.com,mlight@abc.com
Last modified by user  . . . . .  QSECOFR
Last modified date/time  . . . .  '2011-03-24-19.53.50.751000'
```

Pantalla del mandato DSPCCALR con valores de ejemplo

e) Borrar Alerta (DLTCCALR)

El mandato **DLTCCALR** permite a los usuarios autorizados borrar las Alertas de Seguridad creadas.

Los siguientes usuarios pueden utilizar este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain Key Policy and Alerts” (Mantener Política de Claves y Alertas) está establecida en *YES

Siga los siguientes pasos para **cambiar una Alerta de Seguridad**:

1. Pulse F4 en el mandato **CRYPTO/DLTCCALR**
2. Introduzca la categoría auditada y en número de secuencia
3. Pulse Intro para borrar la Alerta de Seguridad

Nota: Cualquier mantenimiento realizado sobre las Alertas de Seguridad será registrado en el archivo de journal de auditoría.

```
                Delete Crypto Complete Alert (DLTCCALR)

Type choices, press Enter.

Audit category . . . . . .  *AUTH       *ALERT, *AUTH, *DEK...
Sequence number  . . . . . .  1         001-999
```

Pantalla del mandato DLTCCALR con valores de ejemplo

6. Auditoría

6.1 Audit Trails del producto

Crypto Complete incluye un amplio sistema de auditoría que permite satisfacer los requisitos de seguridad más estrictos. Se registran entradas en el log de auditoría cuando se produzcan eventos o acciones sobre:

Elementos Auditados	Acciones Controladas
Política de Claves	Cambio
Oficiales de Claves	Añadir, Cambiar, Borrar
Alertas de Seguridad	Añadir, Cambiar, Borrar
Master Encryption Keys (MEKs)	Carga o Configurar
Almacenes de Claves	Crear o Traducir
Data Encryption Keys (DEKs)	Crear, Cambiar, Borrar, Exportar
Data Encryption Keys (DEKs)	Cambios o Traducción en entradas del Registro de encriptación de campos
Entradas Registro Encriptación de Campos	Añadir, Cambiar, Copiar, Eliminar, Activar, Desactivar
Entradas Registro Encriptación IFS	Añadir, Cambiar, Copiar, Eliminar, Activar, Desactivar
SQL Triggers	Añadir, Borrar
Autorización denegada	Funciones denegadas por falta de autorización
Registro de encriptación	Si la clave especifica realizar el registro
Registro de desencriptación	Si la clave especifica realizar el registro

Las entradas del log de auditoría se registran a través del journal CRJN001, el cual se encuentra en la biblioteca CRYPTO por defecto. El receptor de journal inicial se llama CRJR001, adjunto al journal para almacenar las entradas iniciales de auditoría. El journal utiliza la opción MNGRCV(*SYSTEM) para que el sistema pueda gestionar automáticamente los receptores de journal.

Cada entrada registrada en el journal, es asignada con un "Entry Type", el cual indica el evento controlado que generó la entrada en el log de auditoría. Los "Entry Types" válidos son:

Entry Type	Descripción	Mandato Lanzado
01	Key Policy setting(s) changed	CHGKEYPCY
02	Key Officer added	ADDKEYOFR
03	Key Officer changed	CHGKEYOFR
04	Key Officer removed	RMVKEYOFR
05	Master Key passphrase part loaded	LODMSTKEY
06	Master Key was Set	SETMSTKEY
07	Master Key cleared	CLRMSTKEY
08	Key Store created	CRTKEYSTR

Entry Type	Descripción	Mandato Lanzado
09	Key Store translated	TRNKEYSTR
10	Symmetric Key created	CRTSYMKEY
11	Symmetric Key changed	CHGSYMKEY
12	Symmetric Key copied	CPYSYMKEY
13	Symmetric Key deleted	DLTSYMKEY
14	Field Encryption Registry – Entry added	ADDFLDENC
15	Field Encryption Registry – Encryption Key changed	CHGFLDKEY
16	Field Encryption Registry – Entry removed	RMVFLDENC
17	Field Encryption Registry – Entry activated	ACTFLDENC
18	Field Encryption Registry – Entry changed	CHGFLDENC
19	Field Encryption Registry – Entry deactivated	DCTFLDENC
21	Symmetric Key exported	EXPSYMKEY
22	Field Encryption Registry – Unable to Activate Entry	ACTFLDENC
23	Field Encryption Registry – Unable to Deactivate Entry	DCTFLDENC
24	Field Encryption Registry – Entry copied	CPYFLDENC
25	Field Encryption Registry – SQL Triggers added to file	ADDFLDTRG
26	Field Encryption Registry – SQL Triggers removed from file	RMVFLDTRG
27	Field Encryption Registry – Field keys translated	TRNFLDKEY
30	Unable to encrypt/decrypt field using stored procedure	TRIGGER
31	Trigger exit program – Error occurred or return code of ‘E’rror	TRIGGER
32	Trigger exit program – Return code of ‘I’gnore	TRIGGER
33	Trigger exit program – Return code of ‘P’rocess with message	TRIGGER
34	Unable to send Security Alert	
35	Security Alert added	ADDCCALR
36	Security Alert changed	CHGCCALR
37	Security Alert deleted	DLTCCALR
40	Data encrypted with Key that requires logging	
41	Data decrypted with Key that requires logging	
50	Authority error	
60	IFS Encryption Registry – Entry added	ADDIFSENC
61	IFS Encryption Registry – Entry key changed	CHGIFSKEY
62	IFS Encryption Registry – Entry removed	RMVIFSENC
63	IFS Encryption Registry – Entry activated	ACTIFSENC
64	IFS Encryption Registry – Entry changed	CHGIFSENC
65	IFS Encryption Registry – Entry deactivated	DCTIFSENC

Entry Type	Descripción	Mandato Lanzado
66	IFS Encryption Registry – Unable to Activate Entry	
67	IFS Encryption Registry – Unable to Deactivate Entry	
68	IFS Encryption Field	
69	IFS Decryption Field	
70	IFS General Error	
71	IFS Exit Point Program added	
72	IFS Exit Point Program removed	
73	IFS Server Program started	
74	IFS Server Program stopped	
75	IFS Debug Mode was changed	
76	IFS Debug Mode was cleared	

Las entradas del log de auditoría pueden imprimirse mediante el mandato PRTAUDLOG. Se explica en el próximo apartado. Adicionalmente puede ver las entradas del log de auditoría en el journal CRJN001 mediante el mandato DSPJRN. A continuación mostramos un ejemplo de cómo ver las entradas del journal de los errores de autorización ocurridos entre el 1 de Junio de 2008 y el 30 de Junio de 2008:

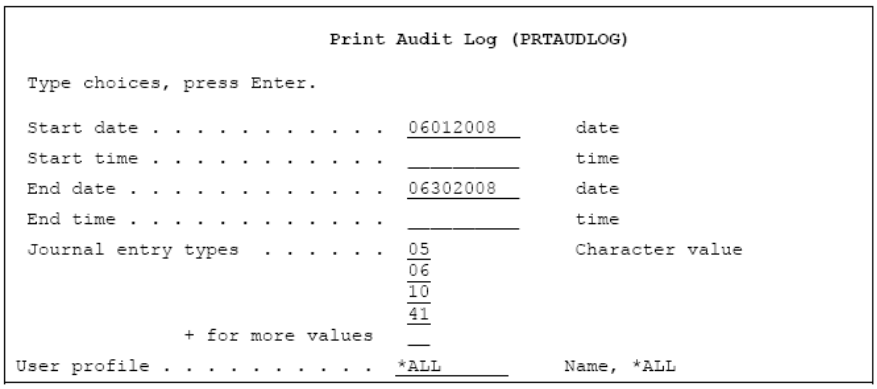
```
DSPJRN JRN(CRYPTO/CRJN001) FROMTIME('06/01/08') TOTIME('06/30/08') ENTTYP(50)
```

a) Print Audit Log (PRTAUDLOG)

El mandato PRTAUDLOG permite a los usuarios autorizados imprimir las entradas del log de auditoría de Crypto Complete. Permite aplicar criterios de selección según la fecha, hora, tipos de auditoría e id. de usuarios.

Siga los siguientes pasos para **imprimir las entradas del log de auditoría**:

1. Pulse F4 en el mandato **CRYPTO/PRTAUDLOG**
2. Pulse F1 sobre cualquier parámetro para obtener ayuda en línea.
3. Pulse Intro una vez haya introducido los parámetros



Pantalla del mandato PRTAUDLOG con valores de ejemplo

Se generará un informe con las entradas del log de auditoría. Por cada entrada impresa, incluirá:

• Fecha de la auditoría • Hora • Usuario • Nombre del trabajo	• Número del trabajo • Tipo de auditoria • Mensaje.

```
11/13/08  13:14:38                Crypto Complete Audit Log

 Date        Time      Type  User        Job Name    Job #   System
 ----------  --------  ----  ----------  ----------  ------  --------
 06/01/2008  15:21:01  06    MSMITH      QPADEV0001  657766  PRD64
       CRA0018 AUDIT: Key store PRODDATA/KS1 was created.

 06/02/2008  15:22:35  10    MSMITH      QPADEV0001  657766  PRD64
       CRA0020 AUDIT: Key CREDIT_CARD_KEY created in Key Store PRODDATA/KS1.

 06/03/2008  15:45:12  41    MARYJ       QPADEV0006  657766  PRD64
       CRA0043 AUDIT: Key SSN_KEY in PRODDATA/KS2 used to DECRYPT data. SSN for cust. 837626

 06/03/2008  15:45:12  41    MARYJ       QPADEV0006  657766  PRD64
       CRA0043 AUDIT: Key BA_KEY in PRODDATA/KS2 used to DECRYPT data. Bank# for cust. 837626

 06/03/2008  15:45:12  41    MARYJ       QPADEV0006  657766  PRD64
       CRA0043 AUDIT: Key CREDIT_CARD_KEY in PRODDATA/KS1 used to DECRYPT data. Credit Card
                      Number for cust. 837626

 06/15/2008  09:33:58  05    JSCHMIT     QPADEV0008  659540  PRD64
       CRA0011 AUDIT: Master Key 1 passphrase part 1 loaded.

 06/15/2008  09:34:09  05    JSCHMIT     QPADEV0008  659540  PRD64
       CRA0011 AUDIT: Master Key 1 passphrase part 2 loaded.
```

Ejemplo de informe

6.2 Audit Trails del sistema

La Política de Claves, las Master Keys, los Oficiales de Seguridad y las Alertas de Seguridad se almacenan en un objeto lista de validación *VLDL llamado CRVL001. Este objeto se encuentra por defecto en la biblioteca CRYPTO.

El objeto CRVL001 está protegido con la clave PEK y otros mecanismos internos que previenen los cambios no autorizados. Sin embargo, puede querer establecer un sistema de auditoría adicional sobre el objeto CRVL001 para rastrear los cambios realizados sobre este objeto.

Sistema adicional de auditoría sobre CRVL001

Siga los siguientes pasos:

1. Establezca la auditoría del sistema sobre el objeto CRVL001 mediante el mandato:

```
CHGOBJAUD OBJ(CRYPTO/CRVL001) OBJTYPE(*VLDL) OBJAUD(*ALL)
```

Compruebe que la auditoría de objetos está habilitada a nivel de sistema viendo que el valor del sistema contiene el valor especial *OBJAUD con el mandato:

```
DSPSYSVAL QAUDCTL
```

2. Si el valor de sistema QAUDCTL no contiene el valor especial *OBJAUD, entonces ejecute el mandato:

```
CHGSECAUD QAUDCTL(*OBJAUD)
```

Este mandato establecerá el valor del sistema QAUDCTL con el valor *OBJAUD y creará el journal de auditoría QSYS/QAUDJRN.

Ejemplo que muestra entradas del journal para cualquier cambio en las listas de validación entre el 5 de junio de 2009 y 11 de junio de 2009.

```
DSPJRN JRN(QAUDJRN) FROMTIME('06/05/09') TOTIME('06/11/09') ENTTYP(VO)
```

7. Configurar Múltiples Entornos de Producción

Su empresa puede que almacene datos de producción de diferentes compañías o divisiones en el mismo sistema. Para cada compañía o división, podría haber una biblioteca única (un entorno) propia de cada compañía o división. La lista de bibliotecas del usuario se utilizará casi seguro para controlar que entorno de bibliotecas está disponible al usuario.

Puede establecer diferentes configuraciones de Crypto Complete para cada entorno mediante la ubicación en esos entornos de bibliotecas de ciertos objetos del producto. Veamos dos escenarios posibles.

7.1 Escenario 1

- **Diferentes Registros de Encriptación de Campos por cada entorno**
- **Compartir las mismas Política de Claves, Oficiales de Claves, Master Keys, Alertas de Seguridad, y Almacenes de Claves en ambos entornos.**

A) Para implementar este escenario siga estos pasos:

1. Compruebe que ninguna aplicación este actualmente utilizando las funciones o programas de Crypto Complete.
2. El Registro de Encriptación de Campos (objeto CRVL002) NO PUEDE ESTAR en la biblioteca CRYPTO, cuando se necesitan diferentes entornos. Establezca el **primer entorno** moviendo el objeto CRVL002 desde la biblioteca CRYPTO a la biblioteca de ese nuevo entorno:

   MOVOBJ OBJ(CRYPTO/**CRVL002**) OBJTYPE(*VLDL) TOLIB(datalib1)

3. Por cada **entorno adicional**, necesitará crear el Registro de Encriptación de Datos (CRVL002) en la biblioteca de ese entorno mediante el mandato:

   CRTVLDL VLDL(datalib2/**CRVL002**) TEXT('Field Encryption Registry')

4. Si se utiliza la opción de archivo físico para almacenar los Last Index Numbers (parámetro LSTINDSTG(*PF) en el Registro), entonces el archivo físico (llamado CRPF002) no puede estar en la biblioteca CRYPTO cuando existen múltiples entornos. Debe seguir estos pasos para establecer el CRPF002:

   a. Establezca el **primer entorno** moviendo el archivo CRPF002 desde la biblioteca del producto CRYPTO a la biblioteca de ese entorno con el mandato:

      MOVOBJ OBJ(CRYPTO/**CRPF002**) OBJTYPE(*FILE) TOLIB(datalib1)

   b. Por cada entorno adicional, necesitará crear un archivo físico CRPF002 (para almacenar los last index numbers) en la biblioteca de ese entorno con el mandato:

      CRTPF FILE(datalib2/**CRPF002**) SRCFILE(CRYPTO/QDDSSRC)

B) Para configurar el Registro de Encriptación de Campos de cada entorno siga esto pasos:

1. Situé la biblioteca del entorno en la parte superior de la lista de bibliotecas:

   ADDLIBLE LIB(datalib1) POSITION(*FIRST)

2. Configure el Registro de Encriptación de Campos para ese entorno

   CRYPTO/WRKFLDENC

SUGERENCIA: Si el estado del id. de campo esta *INACTIVE, entonces puede utilizar el mandato CPYFLDENC para copiar les entradas de campo de un registro de encriptación de campos de un entorno al de otro entorno.

7.2 Escenario 2

- **Diferentes Política de Claves, Oficiales de Claves, Master keys, Alertas de Seguridad y Almacenes de Claves para cada entornos.**
- **Diferente Registro de Encriptación de Campos para cada entorno.**

A) Para implementar este escenario siga estos pasos:

1. Compruebe que ninguna aplicación este actualmente utilizando las funciones o programas de Crypto Complete.
2. Ciertos objetos NO pueden permanecer en la biblioteca CRYPTO. Establecer el **Primer Entorno** moviendo los siguientes objetos y su contenido desde la biblioteca CRYPTO a la biblioteca del entorno deseado:

Objeto a mover	Contenido	Tipo de Objeto
CRVL001	Política de Claves Oficiales de Claves Master Keys	Lista Validación
CRVL002	Registro de Encriptación de Campos	Lista Validación
CRPF002	Para almacenar los “last index number” utilizados	Archivo Físico

Mandatos a utilizar:

MOVOBJ OBJ(CRYPTO/**CRVL001**) OBJTYPE(*VLDL) TOLIB(datalib1)

MOVOBJ OBJ(CRYPTO/**CRVL002**) OBJTYPE(*VLDL) TOLIB(datalib1)

MOVOBJ OBJ(CRYPTO/**CRPF002**) OBJTYPE(*FILE) TOLIB(datalib1)

3. Por cada **entorno adicional,** necesitará crear los objetos CRVL001, CRVL002 y CRPF002 en la biblioteca del entorno adicional con los siguientes mandatos:

   CRTVLDL VLDL(datalib2/**CRVL001**) TEXT(‘Settings and Master Keys') CRTVLDL

   VLDL(datalib2/**CRVL002**) TEXT(‘Field Encryption Registry’)

   CRTPF FILE(datalib2/**CRPF002**) SRCFILE(CRYPTO/QDDSSRC)

B) Ahora siga los siguientes pasos para configurar la Política de Claves, Oficiales de Claves, Master Keys, Alertas de Seguridad y Registros de Encriptación de Campos para cada entorno:

1. Situé la biblioteca del entorno en primera posición el la lista de bibliotecas:

   ADDLIBLE LIB(datalib1) POSITION(*FIRST)

2. Establezca las Políticas de Claves para el entorno.

   CRYPTO/CHGKEYPCY (pulse F4)

3. Establecer los Oficiales de Claves para el entorno.

   CRYPTO/WRKKEYOFR

4. Cargar los passphrases para la Master Key para el entorno:

   CRYPTO/LODMSTKEY MEKID(1) MEKPRT(?) PASSPHRASE(??)

5. Establezca la Master Key para el entorno:

   CRYPTO/SETMSTKEY MEKID(1)

6. Cree el Almacén de Claves para el entorno:

   CRYPTO/CRTKEYSTR KEYSTR(datalib1/KEYSTR) MEKID(1) TEXT('Key Store')

7. Establezca las Claves de Encriptación de Datos DEK en el nuevo almacén de claves:

   CRYPTO/WRKSYMKEY KEYSTR(datalib1/KEYSTR)

8. Configure el Registro de Encriptación de Campos para el entorno

   CRYPTO/WRKFLDENC

9. Configure las Alertas de Seguridad para el entorno:

   CRYPTO/WRKCCALR

Consejo: Si el estado del id. de campo en el registro de encriptación de campos original es *INACTIVE, entonces puede utilizar el mandato CPYFLDENC para copiar las entradas de campos de un Registro de Encriptación de Campos al del otro entorno.

Las claves y configuraciones de Crypto Complete están listas para ser utilizadas en cada entorno. Asegúrese de situar la biblioteca del entorno apropiada en la lista de bibliotecas del usuario para que utilice las claves y configuraciones apropiadas a ese entorno.

8. Configuración de un Entorno de Desarrollo y Pruebas

Quizás su empresa quiera utilizar entornos (bibliotecas) de desarrollo para trabajar y probar la encriptación de campos. Puede establecer diferentes configuraciones Crypto Complete para un entorno de desarrollo colocando ciertos objetos propios del producto en esas bibliotecas del entorno. **Siga los siguientes pasos para establecer un entorno de desarrollo.**

1. Compruebe que ninguna aplicación este actualmente utilizando las funciones o programas de Crypto Complete.
2. El Registro de Encriptación de Campos (objeto CRVL002) NO PUEDE ESTAR en la biblioteca CRYPTO, cuando se necesitan diferentes entornos. Establezca el **entorno de producción** moviendo el objeto CRVL002 desde la biblioteca CRYPTO a la biblioteca de ese nuevo entorno:

   MOVOBJ OBJ(CRYPTO/**CRVL002**) OBJTYPE(*VLDL) TOLIB(prodlib)

3. Por cada **entorno de desarrollo**, necesitará crear el Registro de Encriptación de Datos (CRVL002) en la biblioteca de ese entorno mediante el mandato:

   CRTVLDL VLDL(devlib/**CRVL002**) TEXT('Field Encryption Registry')

4. Si se utiliza la opción de archivo físico para almacenar los "Last Index Numbers" (parámetro LSTINDSTG(*PF) en el Registro), entonces el archivo físico (llamado CRPF002) no puede estar en la biblioteca CRYPTO cuando existen múltiples entornos.

   Debe seguir estos pasos para establecer el CRPF002:

   a. Establezca el **entorno de producción** moviendo el archivo CRPF002 desde la biblioteca del producto CRYPTO a la biblioteca de ese entorno con el mandato:

      MOVOBJ OBJ(CRYPTO/**CRPF002**) OBJTYPE(*FILE) TOLIB(prodlib)

   b. Por cada **entorno de desarrollo**, necesitará crear un archivo físico CRPF002 (para almacenar los "Last Index Numbers") en la biblioteca de ese entorno con el mandato:

      CRTPF FILE(devlib/**CRPF002**) SRCFILE(CRYPTO/QDDSSRC)

5. Copie las entradas de campos del Registro de Encriptación de campos del entorno de producción al entorno de desarrollo:

   CRYPTO/CPYFLDENC FRMLIB(prodlib) FRMFLDID(fieldid) TOLIB(devlib)

6. Si no existiera el archivo de la base de datos de prueba, cree el archivo de la base de datos sin copiar los datos. O bien elimine los datos una vez copiada.

   CRTDUPOBJ OBJ(filename) FROMLIB(prodlib) OBJTYPE(*FILE) TOLIB(devlib) DATA(*NO) TRG(*NO)

7. Copie los datos de prueba del archivo de producción al archivo creado en el entorno de desarrollo:

```
CPYF FROMFILE(prodlib/filename) TOFILE(devlib/filename) MBROPT(*ADD) FROMRCD(*START)
TORCD(100) REPLACE(*YES)
```

8. Si los valores encriptados están almacenados en un archivo externo, entonces realice los siguientes pasos:

   a. Si el fichero externo de pruebas no existe entonces cree el archivo externo de prueba en el entorno de desarrollo sin copiar los datos.

   ```
   CRTDUPOBJ OBJ(extfilename) FROMLIB(prodlib) OBJTYPE(*FILE) TOLIB(devlib) DATA(*NO)
   ```

   b. Si un archivo lógico estuviera siendo utilizado sobre el archivo externo, entonces cree el archivo lógico externo en el entorno de desarrollo.

   ```
   CRTDUPOBJ OBJ(extlogicalfilename) FROMLIB(prodlib) OBJTYPE(*FILE) TOLIB(devlib)
   ```

   c. Copie los datos de prueba del archivo externo de producción al archivo externo de desarrollo. Solo copie los registros externos que coincidan con los números índice en su archivo de base de datos de prueba.

9. Sitúe la biblioteca de desarrollo en la parte superior de la lista de bibliotecas.

   ```
   ADDLIBLE LIB(devlib) POSITION(*FIRST)
   ```

10. Si se utilizan Triggers SQL en el identificador de campos, añada los Triggers SQL al archivo de desarrollo mediante el mandato:

    ```
    CRYPTO/ADDFLDTRG FLDID(fieldid)
    ```

El Registro de Encriptación de Campos y los archivos de Crypto Complete ya están listos para ser utilizados en la biblioteca de desarrollo. Asegúrese de situar la biblioteca del entorno apropiada en la lista de bibliotecas del usuario para que utilice el Registro de Encriptación de Campos y archivos apropiados a ese entorno.

Refrescando Datos

Si necesita refrescar los datos de la biblioteca de desarrollo y si el archivo de la base de datos de prueba está utilizando Triggers SQL para encriptar datos automáticamente, debería hacer lo siguiente para refrescar los datos:

1. Situé la biblioteca de desarrollo en la parte superior de la lista de bibliotecas
2. Elimine los Triggers del archivo de la base de datos de prueba mediante el mandato RMVFLDTRG de Crypto Complete.
3. Refresque los datos en el archivo de la base de datos de prueba.
4. Si se está utilizando un archivo externo para almacenar valores encriptados, entonces refresque los datos del archivo externo de pruebas.
5. Recree los Triggers del archivo de la base de datos de prueba mediante el mandato ADDFLDTRG de Crypto Complete.

9. Backup de Claves y Recuperación de Claves

9.1 Backup Automático preventivo a disco de Crypto Complete

Crypto Complete realiza copias de Backup automáticamente en Save Files antes de que ciertas acciones de mantenimiento se realicen con el producto. Esto permite recuperar los valores anteriores en caso de cambios accidentales.

Acciones que activan el Backup automático:

- Traducción del Almacén de Claves.
- Creación de una Master Key.

a) Almacenes de Claves

Las claves DEK están alojadas dentro del Almacén de Claves que son objetos *VLDL - Lista de Validación. Los nombres (y ubicación de las bibliotecas) de estos objetos *VLDL son los nombres que se especificaron con el mandato CRTKEYSTR (Create Key Store), a menos que se renombraran o movieran posteriormente.

Antes de que se produzca la traducción de un almacén de claves con la nueva MEK, se realiza un Backup automático del objeto *VLDL del almacén de claves a un Save File con nombre propio. Su nombre se forma con el prefijo BACKUP y el sufijo xxxx, siendo este un número secuencial entre 1 y 9999. Se creará en la misma biblioteca que el objeto *VLDL.

b) Master Encrytion Keys (MEKs)

Las claves MEK se almacenan en un objeto *VLDL - Lista de Validación llamado CRVL001, en la biblioteca CRYPTO por defecto.

Antes de que se cree una Master Key (MEK) se realiza un Backup automático del objeto *VLDL CRVL001 en un Save File con nombre propio. Su nombre se forma con el prefijo BACKUP y el sufijo xxxx, siendo este un número secuencial entre 1 y 9999. Se creará en la misma biblioteca que el objeto *VLDL.

c) Eliminar los Save Files de Backup automático

Estos objetos Save Files creados con el nombre BACKUPxxxx deberían eliminarse periódicamente para optimizar el uso del disco y que no queden en el sistema claves y datos antiguos. **Solo elimínelas si está seguro de que sus aplicaciones están funcionando correctamente.**

9.2 Estrategia de Backup Obligatorio a medios externos

Importante: Es fundamental tener previsto un plan de contingencias para volver a recrear las Master Encryption Keys (MEKs) y recuperar los Almacenes de Claves, Registro de Encriptación de Campos y Archivos Externos (los que contienen valores de campos encriptados). No hacer esto podría hacer imposible la desencriptación de los datos.

Esta es una lista de los **objetos que DEBE incluir en su sistema de Backup** y realizar frecuentemente:

- Programa bajo licencia Crypto Complete (4CRYPTO) que contiene la biblioteca CRYPTO
- CRVL001 objects type *VLDL (uno por cada entorno)
- CRVL002 objects type *VLDL (uno por cada entorno)
- CRPF002 object type *FILE (uno por cada entorno si corresponde)
- Almacenes de Claves objects type *VLDL, creados por el usuario.
- Archivos Externos (prefijo por defecto del objeto CRXX tipo *FILE) utilizados para almacenar los valores de los campos de la base de datos encriptados.
- Listas de Autorización del sistema utilizadas para asegurar los objetos Almacén de Claves y las usadas para asegurar campos en el Registro de Encriptación de Campos.

Precaución NO UTILICE los mandatos de encriptación de Backup (ENCxxx) de CRYPTO COMPLETE para realizar el Backup de la biblioteca CRYPTO o los objetos *VLDL. Utilice los mandatos propios del sistema IBM i.

	Objeto	Ubicación x defecto (*)	Incluir en Backup	Proceso Salvado
Programa Crypto Complete	4CRYPTO		Si	**SAVLICPGM LICPGM(4CRYPTO)**
MEKs Master Encryption Key	CRVL001 *VLDL	Biblioteca CRYPTO	Si	**Backup con mandatos propios del sistema.** No utilizar los mandatos de Crypto Complete
Política de Claves				
Oficiales de Claves				
Alertas de Seguridad				
Los valores dentro de este objeto CRVL001 están encriptados con la clave PEK (Product Encryption Key). Esta clave deriva parcialmente del número de serie del sistema. Por eso cada máquina tendrá una PEK diferente. Si este objeto se restaura bajo otro número de serie diferente no será válido. La política de claves, Master Keys, Oficiales de Claves y Alertas de Seguridad tendrán que ser recreadas manualmente. (Ver recuperación en caso de emergencia). **Nota sobre los Passphrases:** Las partes del passphrase utilizadas para cargar una MEK DEBEN GUARDARSE en un lugar seguro fuera del sistema. Serán NECESARIAS para recrear la MEK en caso de tener que instalar el producto en otra máquina con diferente número de serie. Recuerde: son sensibles a mayúsculas/minúsculas y el orden de las partes de la MEK.				

(continuación…)	Objeto	Ubicación x defecto (*)	Incluir en Backup	Proceso Salvado
Registro de Encriptación de Campos (1)	CRVL002 *VLDL	Biblioteca CRYPTO	Si	**Backup con mandatos propios del sistema.** No utilizar los mandatos de Crypto Complete
Registro de Encriptación de directorios IFS (ATT)	CRVL003 *VLDL	Biblioteca CRYPTO	Si	
Last Index Numbers	CRPF002	Biblioteca CRYPTO	Si (**)	
Archivos Externos (2)	CRXX*	Biblioteca archivo original	Si	
Almacenes de Claves (3)	*VLDL	Biblioteca y nombre especificados	Si	
Listas de Autorización	*AUTL	QSYS	Si (***)	**SAVSECDTA or SAVSYS**

(*) Biblioteca por defecto: Es CRYPTO, salvo que se hayan creado diferentes entornos de pruebas, desarrollo o de producción. Entonces será la biblioteca que se haya determinado al crearlos. Los archivos externos por defecto se almacenan en la biblioteca que aloja el archivo que contiene los campos que estamos encriptando. Los almacenes de claves se almacenan con el nombre y biblioteca especificados. Se recomienda crear una biblioteca particular. Las listas de autorización se encuentran el biblioteca QSYS.

(**) Si utiliza archivos externos para almacenar los valores encriptados de los campos de la base de datos y el Registro de Encriptación de Campos y se ha especificado que los “last index number used” se almacenen en la opción del archivo físico (parámetro LSTINDSTG(*PF) de registro) debe salvarse el objeto CRPF002.

(***) Si se han utilizado listas de autorización para asegurar los Almacenes de claves o asegurar campos en el Registro de campos, incluir en Backup.

(1) El objeto CRVL002, contiene información importante sobre los campos que se han registrado para su encriptación: nombres de campos, pointers a las etiquetas de claves para encriptar y desencriptar, números índices para los datos de campos encriptados almacenados en archivo externo, etc…

(2) Para averiguar los nombres de los archivos externos utilice el mandato CRYPTO/WRKFLDENC y seleccione la opción 5 junto a cada campo.

(3) Las claves DEK están alojadas en los Key Stores (Almacenes de Claves). Los nombres y bibliotecas donde se alojan se especificaron con el mandato CRTKEYSTR a menos que se hayan cambiado o renombrado. Dado que el almacén de claves se encripta con la Master Key (la cual está encriptada por la PEK), los almacenes estarán protegidos en su dispositivo de Backup de usos no autorizados.

(ATT) Si está utilizando el módulo de Encriptación Automático de las carpetas de la IFS compuebe que en sus backup se están salvando los siguientes objetos propios de ese módulo: CRVL003 (Registro directorios IFS), los archivos CRPFIFS, CRPFIFS2, CRPFIFSLOG y las áreas de datos CRDEBUG, CRLSTSEQ. Finalmente compruebe que dispone de las listas de autorizaciones utilizadas con este módulo.

9.3 Recuperación en caso de Emergencia

Si se ha producido una situación de crisis y se tiene que restaurar el producto Crypto Complete, las configuraciones del usuario, Master Keys y Almacenes de Claves siga los siguientes pasos. Hay unos pasos comunes y otros solo según el módulo o módulos contratados.

a) Restaurar en una máquina con el mismo número de serie

Pasos Comunes a los usuarios de todos los módulos de Crypto Complete

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 que fueron salvadas con el mandato SAVLIB de IBM. Por ejemplo: RSTLIB SAVLIB(*NONSYS) DEV(TAP01).
3. Localice su copia del programa bajo licencia Crypto Complete en su dispositivo de Backup. Si no estuviera disponible contacte con su proveedor.
4. Restaure el programa Crypto Complete 4CRYPTO con el mandato RSTLICPGM.
5. Restaure los Almacenes de Claves creados por el usuario (Key Stores) de su dispositivo de Backup. Los almacenes de claves son objetos (*VLDL).
6. Restaure el objeto CRVL001 *VLDL de su dispositivo de Backup. Contiene la Política de Claves, Master Encryption Keys, Oficiales de Claves y Alertas de Seguridad. Por defecto, se encuentra en la biblioteca CRYPTO, salvo que se hubieran creado diferentes entornos.

(Sólo si utiliza el módulo de Encriptación de Campos, además realice pasos 7, 8 y 9)

7. Si utiliza el Registro de Encriptación de Campos de Crypto Complete, restaure el objeto CRVL002 *VLDL de su dispositivo de Backup. Por defecto, se encuentra en la biblioteca CRYPTO, salvo que se hubieran creado otros entornos.
8. Si utiliza el Registro de Encriptación de Campos y está usando archivos externos para almacenar valores encriptados de los campos de la base de datos y los “last index numbers” se almacenan en la opción de archivo físico (parámetro del registro LSTINDSTG(*PF)), entonces restaure el archivo llamado CRPF002 de su dispositivo de Backup. Por defecto, el archivo CRPF002 se encuentra en la biblioteca CRYPTO, salvo que se hubieran creado otros entornos.
9. Si utiliza los archivos externos para almacenar los valores encriptados de los campos de la base de datos, restaure los archivos externos. Su prefijo por defecto es CRXX.

(Sólo si utiliza el módulo de Backup de Crypto Complete de Bibliotecas, Objetos y archivos IFS, además realice pasos 10 y 11)

10. Restaure mediante los mandatos DECRSTLIB o DECRSTOBJ de Crypto Complete, todas las bibliotecas y objetos que fueron salvados y encriptadas con Crypto Complete.
11. Restaure mediante el mandato DECSTMF de Crypto Complete, todos los archivos de la IFS que fueron salvados y encriptados con Crypto Complete.

Nota att: Sólo si utiliza el módulo de Encriptación Automática de IFS ver nota ATT en apartado 9.2.

b) Restaurar en una máquina con distinto número de serie

Nota: El objeto CRVL001 *VLDL NO se puede restaurar en esta máquina por tener un número de serie distinto, ya que el objeto se encripta bajo la PEK (Product Encryption Key) directamente vinculada al número de serie de la máquina en que se instala Crypto Complete.

Pasos Comunes a los usuarios de todos los módulos de Crypto Complete

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 que fueron salvadas con el mandato SAVLIB de IBM. Por ejemplo: RSTLIB SAVLIB(*NONSYS) DEV(TAP01).
3. Localice su copia del programa bajo licencia Crypto Complete en su dispositivo de Backup. Si no estuviera disponible contacte con su proveedor.
4. Restaure el programa Crypto Complete 4CRYPTO con el mandato RSTLICPGM.

   Si no tuviera una clave autorizada para la nueva máquina, Crypto Complete se activará automáticamente con una clave provisional de 30 días. Solicite su nueva clave definitiva a través de su proveedor.
5. Restaure los Almacenes de Claves creados por el usuario (Key Stores) de su dispositivo de Backup. Los almacenes de claves son objetos (*VLDL).

(Sólo si utiliza el módulo de Encriptación de Campos, además realice pasos 6,7,8)

6. Si utiliza el Registro de Encriptación de Campos de Crypto Complete, restaure el objeto CRVL002 *VLDL de su dispositivo de Backup. Por defecto, se encuentra en la biblioteca CRYPTO, salvo que se hubieran creado otros entornos.
7. Si utiliza el Registro de Encriptación de Campos y está usando archivos externos para almacenar valores encriptados de los campos de la base de datos y los “last index numbers” se almacenan en la opción de archivo físico (parámetro del registro LSTINDSTG(*PF)), entonces restaure el archivo llamado CRPF002 de su dispositivo de Backup. Por defecto, el archivo CRPF002 se encuentra en la biblioteca CRYPTO, salvo que se hubieran creado otros entornos.
8. Si utiliza los archivos externos para almacenar los valores encriptados de los campos de la base de datos, restaure los archivos externos. Su prefijo por defecto es CRXX.

Pasos Comunes a los usuarios de todos los módulos de Crypto Complete

9. Restablezca la misma Política de Claves que tenía con el mandato CHGKEYPCY.
10. Restablezca las Alertas de Seguridad con el mandato WRKCCALR.
11. Restablezca los Oficiales de Claves con el mandato WRKKEYOFR
12. Genere las mismas claves MEK. Introduzca exactamente las mismas partes del passphrase y en el mismo orden que utilizaba actualmente en su sistema de producción, mediante el mandato LODMSTKEY. Recuerde que son sensibles a mayúsculas y minúsculas. Realice este paso por cada MEK que tuviera creadas en el sistema de producción.

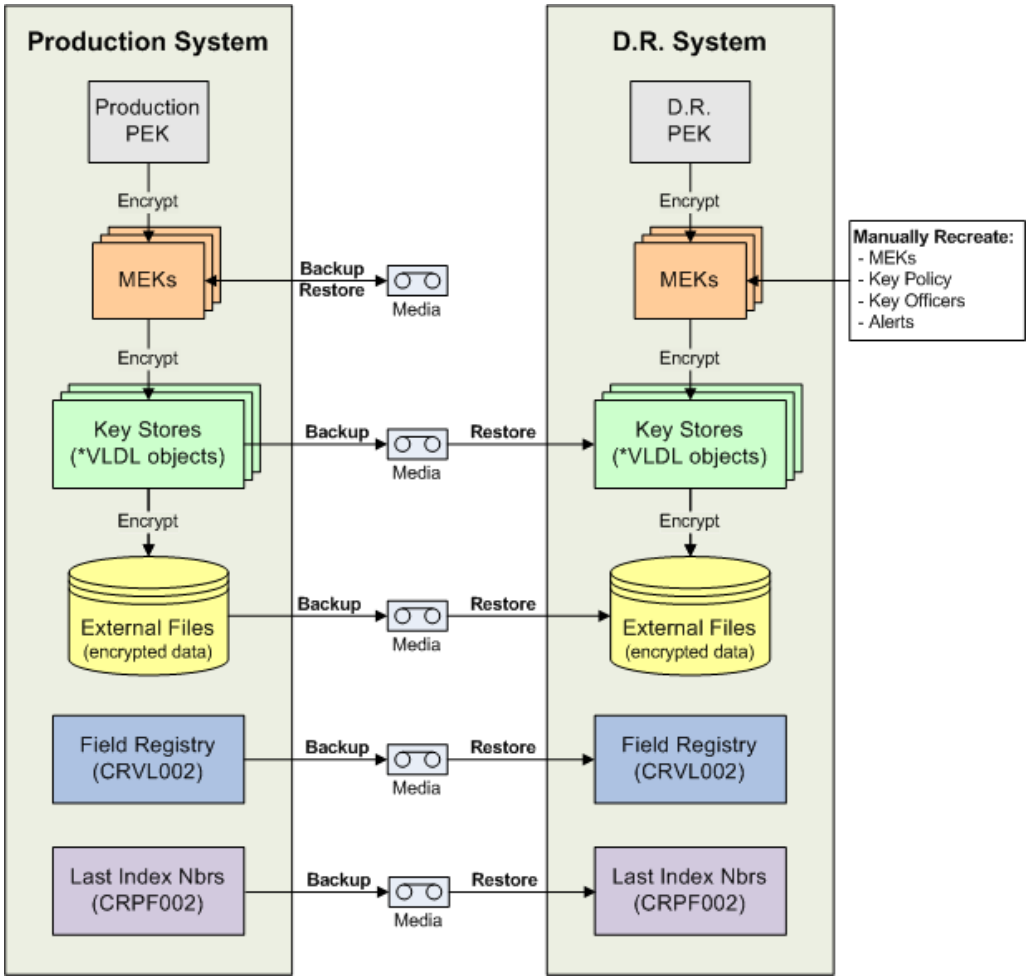
13. Establezca las claves MEK generadas mediante el mandato SETMSTKEY.

(Sólo si utiliza el módulo de Backup de Crypto Complete de Bibliotecas, Objetos y archivos IFS, además realice pasos 14 y 15)

14. Restaure mediante los mandatos DECRSTLIB o DECRSTOBJ de Crypto Complete, todas las bibliotecas y objetos que fueron salvados y encriptadas con Crypto Complete.
15. Restaure mediante el mandato DECSTMF de Crypto Complete, todos los archivos de la IFS que fueron salvados y encriptados con Crypto Complete.

Nota ATT: Sólo si utiliza el módulo de Encriptación Automática de IFS ver nota ATT en apartado 9.2.

Los Almacenes de Claves y las claves que contienen deberían estar disponibles para su uso. A continuación vemos un diagrama del sistema de copias que debe llevarse y los pasos a realizar en una recuperación en caso de emergencia y si el número de serie de la máquina de emergencia es diferente al de la máquina de producción.



Ejemplo de restauración de emergencia en máquina con diferente número de serie

9.4 Sistemas de Alta Disponibilidad

En caso de instalar Crypto Complete en una máquina de Alta Disponibilidad (High Availability) (HA) siga las siguientes instrucciones para replicar correctamente las configuraciones establecidas en su máquina de producción y los datos de usuario relacionados.

a) Configuración Inicial

Instale una copia del producto bajo licencia de Crypto Complete en su máquina de alta disponibilidad siguiendo las instrucciones de instalación de Crypto Complete que encontrará al inicio de este manual.

La primera vez que utilice Crypto Complete se activará una clave temporal de 30 días. Se recomienda que obtenga una clave permanente de Crypto Complete al mismo tiempo que realice la compra de la copia de producción. Contacte con American Top Tools para facilitarle el número de serie y grupo de procesador de la máquina de HA y obtener la clave.

b) Replicación Manual

Pasos Comunes a los usuarios de todos los módulos de Crypto Complete

El objeto CRVL001 *VLDL - Lista de Validación - se encuentra por defecto en la biblioteca CRYPTO (salvo que se hubiera cambiado a otro entorno) del sistema de producción. Contiene la configuración de la Política de Claves, los Oficiales de Claves, las Alertas de Seguridad y las Master Keys (MEKs) que ha definido en el sistema de producción.

Este objeto CRVL001 *VLDL se encripta con la clave PEK (Product Encryption Key), la cual es única para cada máquina según el número de serie.

En consecuencia, cualquier cambio realizado sobre estas configuraciones del producto en la máquina de producción, tendrán que ser aplicadas manualmente en la máquina de alta disponibilidad (HA) mediante las pantallas y mandatos de Crypto Complete.

Precaución: NO incluya en la replicación automática el objeto CRVL001 *VLDL de su máquina de Producción en la máquina de alta disponibilidad. Las configuraciones contenidas en el objeto CRVL001 (Política de Claves, Oficiales de Claves, Alertas de Seguridad y Master Keys) deben ser recreadas MANUALMENTE en la máquina de HA desde las pantallas de Crypto Complete

Siga los siguientes pasos (1 a 9) para recrear manualmente las mismas configuraciones de la máquina de producción en su sistema de alta disponibilidad. Algunos pasos sólo son necesarios según el módulo de Crypto Complete contratado.

1. Política de Claves (Key Policy)

Si se cambia la Política de Claves en el sistema de producción, también se tiene que cambiar manualmente en la máquina de alta disponibilidad.

Sistema de Producción	Sistema de Alta Disponibilidad / Replicación
• Visualice la Política de Claves con CRYPTO/DPSKEYPCY • Tome nota de los valores mostrados de la Política de Claves.	• Actualice la Política de Claves **con** CRYPTO/**CHGKEYPCY**. • **Introduzca los mismos valores del sistema de producción** que acaba de anotar.

2. Oficiales de Claves (Key Officers)

Si se producen modificaciones, añaden o borran Oficiales de Claves en el sistema de producción, debe actualizarse manualmente las configuraciones de los Oficiales de Claves del sistema de alta disponibilidad.

Sistema de Producción	Sistema de Alta Disponibilidad / Replicación
• Visualice los Oficiales de Claves con CRYPTO/WRKKEYOFR • Tome nota de los valores mostrados sobre los Oficiales de Claves.	• **Actualice los Oficiales de Claves con** CRYPTO/**WRKKEYOFR**. • **Introduzca los mismos valores del sistema de producción** que acaba de anotar.

3. Alertas de Seguridad

Si se añaden Alertas de Seguridad, o se modifican o borran de la máquina de producción, debe actualizarse manualmente las configuraciones de las Alertas de Seguridad del sistema de alta disponibilidad.

Sistema de Producción	Sistema de Alta Disponibilidad / Replicación
• Visualice las Alertas de Seguridad con CRYPTO/WRKCCALR • Tome nota de los valores mostrados sobre las Alertas de Seguridad	• **Actualice las Alertas de Seguridad con** CRYPTO/**WRKCCALR**. • **Introduzca los mismos valores del sistema de producción** que acaba de anotar.

4. Master Keys

Si se configuran las Master keys en la máquina de producción, debe actualizarse manualmente las configuraciones las Master Keys del sistema de alta disponibilidad.

Sistema de Producción	Sistema de Alta Disponibilidad / Replicación
• Recupere las distintas partes que componen la passphrase que introdujo en el sistema de producción por cada Master Key • Estas deberían estar guardadas aparte fuera del sistema.	• Introduzca **las mismas partes del passphrase y en el mismo orden** para cada **Master Key con LODMSTKEY**, respetando mayúsculas y minúsculas. • **Genere las MEK** mediante el mandato **SETMSTKEY.**

b) Replicación Automática

Configure su producto de Alta disponibilidad (HA) para que replique los siguientes objetos de manera automatizada y continua:

Pasos Comunes a los usuarios de todos los módulos de Crypto Complete

5. Almacenes de Claves

Los **Almacenes de Claves** creadas por el usuario son objetos *VLDL- Lista de Validación. Los nombres (y su biblioteca de ubicación) de estos objetos *VLDL son aquellos nombres que se especificaron con el mandato CRTKEYSTR, a menos que se hayan movido o cambiado de nombre. Estos objetos *VLDL, **deben replicarse** por su producto de alta disponibilidad desde la máquina de producción a su máquina HA.

(Sólo si utiliza el módulo de Encriptación de Campos realice pasos 6, 7 y 8)

6. Archivos Externos

Si está utilizando **archivos externos para almacenar valores encriptados** de campos de la base de datos, **debe replicar** esos archivos externos desde su máquina de producción a su máquina de alta disponibilidad. Puede averiguar los nombres de los archivos externos mediante el mandato CRYPTO/WRKFLDENC y seleccionar la opción 5 junto a cada entrada de campo *ACTIVE.

7. Registro de Encriptación de Campos

Replique el **objeto CRVL002** *VLDL de su máquina de producción en su máquina de alta disponibilidad. Este objeto contiene el Registro de Encriptación de Campos.

8. Archivo CRPF002

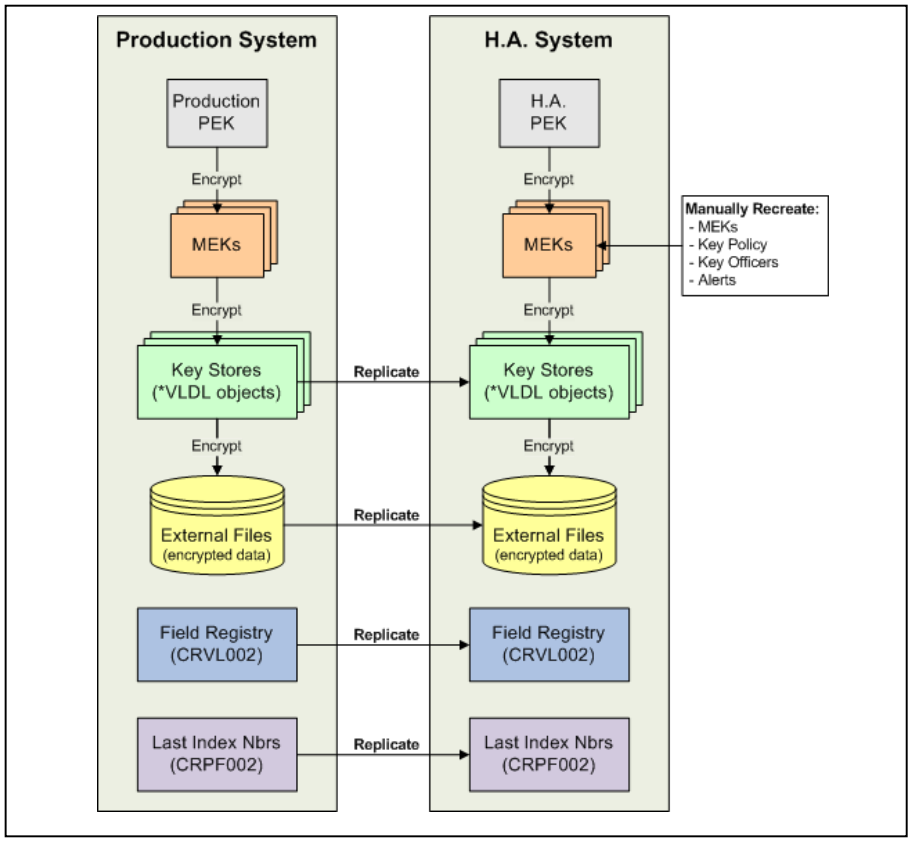
Si utiliza el Registro de Encriptación de Campos y está usando archivos externos para almacenar valores encriptados de los campos de la base de datos y los “last index numbers” se almacenan en la opción de archivo físico (parámetro del Registro LSTINDSTG(*PF)), entonces replique el archivo físico llamado CRPF002 de su sistema de producción en su máquina de alta disponibilidad.

Pasos Comunes a los usuarios de todos los módulos de Crypto Complete

9. Listas de autorizaciones

Replique cualquier Lista de Autorizaciones del sistema que se esté utilizando para proteger Almacenes de Claves, proteger campos en el Registro de Encriptación de Campos o autorizar usuarios a desencriptar carpetas y archivos del Registro de Encriptación de IFS.

Precaución: NO incluya en la replicación automática el objeto CRVL001 *VLDL de su máquina de Producción en la máquina de alta disponibilidad. Las configuraciones contenidas en el objeto CRVL001 (Política de Claves, Oficiales de Claves, Alertas de Seguridad y Master Keys) deben ser recreadas MANUALMENTE en la máquina de HA desde las pantallas de Crypto Complete. Este objeto esta encriptado con la clave PEK (Product Encryption Key) que es única según el número de serie de cada máquina.



Ejemplo de funcionamiento en un entorno de Alta Disponibilidad (HA)

9.5 Verificar la configuración de CRVL001

El **mandato VFYCRVL001** permite verificar que el objeto CRVL001 es correcto en su instalación. Esta verificación normalmente debería hacerse después de una restauración del sistema.

El objeto CRVL001 contiene la configuración de la Política de Claves, de Alertas de Seguridad, de Oficiales de Claves y de las Master Keys de su organización.

Si el mandato VFYCRVL001 falla, probablemente sea porque el objeto fue copiado de otra máquina con un número de serie distinto.

NO DEBERÍA COPIAR el objeto CRVL001 *VLDL entre máquinas con número de serie distinto ya que el objeto CRVL001 y sus contenidos están encriptados con la PEK (Product Encryption Key) la cual es única para cada número de serie.

10. Preguntas y Respuestas

1.- ¿Puedo utilizar un campo encriptado como campo clave en un archivo? (Para búsquedas/cadenas).

Si. Si estuviera utilizando un Procedimiento de Campo DB2 (desde V7R1) en el campo encriptado, el sistema operativo encriptará automáticamente el argumento de búsqueda y utilizará ese valor encriptado para realizar la búsqueda. No debería hacerse ningún cambio sobre la aplicación.

Si no estuviera utilizando los Procedimientos de Campo DB2, también puede buscar un registro en la base de datos por el campo clave encriptado, pero primero tiene que encriptar el valor buscado o argumento de búsqueda. Por ejemplo, una vez el usuario haya introducido el valor buscado en la pantalla, puede encriptar ese valor (mediante una API de Crypto Complete), y luego, utilizar ese valor encriptado para enlazarlo con el archivo. El tipo de programación que realice dependerá de si los valores encriptados son almacenados dentro de su campo existente o son almacenados en un archivo externo separado. Vea los ejemplos de miembro fuente CAHININT Y CHAINEXT en el archivo de fuentes CRYPTO/QRPGLESRC.

2.- ¿Se salvan los Triggers SQL junto con el objeto del archivo físico?

Si. Cuando se establece una entrada en el Registro de Encriptación de campos, puede especificar si los Triggers SQL deberían utilizarse para encriptar datos automáticamente cuando se añaden o cambian valores del campo. Al activar una entrada de campo en el Registro de Encriptación de campos, Crypto Complete creará los triggers sobre el archivo físico mediante el mandato SQL “CREATE TRIGGER”.

Al contrario que los Triggers externos tradicionales, los Triggers SQL se salvan en el objeto del archivo físico cuando realiza un mandato SAVLIB, SAVOBJ o SAVCHGOBJ. Consecuentemente no necesita realizar el backup de los Triggers SQL separadamente.

3.- ¿Pueden interferir los Triggers SQL de Crypto Complete con otros Triggers que ya tuviera el archivo?

Los Triggers SQL pueden colocarse en un archivo físico incluso si ya existen otros Triggers en el archivo. Cuando se configura una entrada en el Registro de Encriptación de Campos, puede especificar los nombres de los Triggers SQL o bien, utilizar la opción *GEN para que el propio Crypto Complete genere los nombres de los Triggers. Para la opción *GEN, la convención de nomenclatura utilizada para los Triggers SQL es:

“**FILE**NAME_**FIELD**NAME_CryptoInsert” para el Trigger Insert
“**FILE**NAME_**FIELD**NAME_CryptoUpdate” para el Trigger Update
“**FILE**NAME_**FIELD**NAME_CryptoInsert” para el Trigger Delete

Donde FILENAME es el nombre del archivo físico y FIELDNAME es el nombre del campo en el archivo físico.

Los Triggers se crean de modo que funcionen como Triggers BEFORE, lo que significa que se ejecutan antes del INSERT, UPDATE o DELETE actual del registro del archivo. Los Triggers de Insert y Update cambiarán el valor del campo de la base de datos (en que se basan los Triggers) para que contenga un valor encriptado (si no se utilizan archivos externos) o para que contenga un número de índice (si el valor encriptado se almacena externamente).

4.- ¿Cómo se muestran los datos encriptados en la pantalla?

Los datos encriptados están representados por números, letras y caracteres especiales. Este sería un ejemplo de un texto encriptado con el algoritmo AES256:

Texto: "The quick brown fox jumped over the lazy dog"
Texto Encritpado "„OE \ËKä°BBY ý\åê·Ñ,C‹Ÿ^{F+rÀJ[1]Ï(¾Y½i›"®t"

Estos valores encriptados pueden contener delimitadores de fin de campo u otros caracteres especiales, que confunden a los terminales y emuladores 5250. Estos datos pueden hacer que los emuladores muestren un extraño comportamiento o bloqueo.

Si esta almacenando valores encriptados en el espacio del campo existente en la base de datos, debería evitar mostrar esos valores en las pantallas 5250. Modifique el programa si no quiere que muestre el valor encriptado. Si no, puede llamar a una de las APIs de Crypto Complete para que desencripte el valor del campo y lo muestre en la pantalla (si el usuario está autorizado).

Si esta almacenando los valores encriptados en un archivo externo, entonces el usuario verá el número de índice numérico del registro del archivo externo. Puede que esto sea suficiente para su empresa. Si no, puede cambiar el programa de su aplicación para que no muestre el número de índice o bien, llamar al procedimiento GetEncFld para que recupere y desencripte el valor del campo, el cual puede mostrar en la pantalla (si el usuario está autorizado).

5.- ¿Puedo rotar las claves en cualquier momento?

Si. Si utiliza el Registro de Encriptación de Campos y elige almacenar los valores del campo encriptados en un archivo externo, entonces un Identificador de Campo es almacenado junto con cada registro en el archivo externo. Si se cambia la clave de un campo, entonces se almacenará un nuevo Identificador de Clave con cualquier registro que sea añadido o actualizado en el archivo externo. No será necesaria una reencriptación masiva de los valores de los campos.

Cuando se recupere un valor encriptado desde un archivo externo, Crypto Complete utilizará el Identificador de Clave del registro del archivo externo para recuperar la Etiqueta de Clave correcta para desencriptar ese valor. Está técnica permite cambiar la calve de un campo en el Registro en cualquier momento, aún cuando los usuarios estén activos en esa aplicación. Se pueden rotar hasta 99.999 claves por cada campo.

6.- ¿Qué tipo de mantenimiento puedo realizar en un archivo de base de datos que contiene Triggers SQL?

1. El sistema operativo NO permite ejecutar el mandato CLRPFM (Clear Physical File Member) sobre el archivo de la base de datos si tiene un Trigger DELETE. Este existe en su archivo si usted eligió almacenar valores de campo encriptados en un archivo externo cuando lo definió en el Registro de Encriptación de Campos. Si desea eliminar todos los registros del archivo, debería realizar un borrado masivo mediante un lenguaje de programación o el mandato SQL Delete.

2. NO renombre o mueva un archivo de la base de datos si uno o más de los campos están ACTIVOS en el Registro de Encriptación de Campos. Para que el Registro de Encriptación de Campos mantenga la "sincronización" con la nueva ubicación del archivo, debe seguir estos pasos:
   a) Desactive el campo en el Registro de Encriptación de Campos
   b) Renombre o mueva el objeto del archivo de la base de datos
   c) Cambie la entrada en el Registro de Encriptación de Campos con la nueva ubicación del archivo.
   d) Active el campo en el Registro de Encriptación de Campos

3. NO realice un CRTDUPOBJ (Create Duplicate Objetct) con el parámetro especificado TRG(*YES). Está acción duplicaría los Triggers al objeto nuevo, lo que confundiría al Registro de Encriptación de Campos y a los procesos de encriptación. PODRIAN PERDERSE DATOS.

7.- ¿Puedo encriptar valores de campo solo para algunos registros específicos de un archivo de base de datos?

Existen dos aproximaciones que pueden utilizarse para encriptar SOLO los valores de CIERTOS registros seleccionados:

Aproximación 1:

A. Cree un archivo lógico con criterios Select/Omit para elegir los registros (del archivo físico) que deben ser encriptados.
B. Cuando añada el campo al Registro de Encriptación de Campos con el mandato ADDFLDENC, especifique el nombre de ese archivo lógico en el parámetro DBFILE.
C. Cuando active el campo en el Registro de Encriptación de Campos mediante el mandato ACTFLDENC, solo encriptará masivamente los valores de campo de los registros seleccionados por el archivo lógico.
D. NO PODRÁ utilizar Triggers para encriptar automáticamente los valores ya que los Triggers no están permitidos en los archivos lógicos. En su lugar, necesitará las APIs de encriptación de campos de Crypto Complete (EncFld, InsEncFld, UpdEncFld, etc…) para encriptar los valores. Están documentadas en la Guía del Programador de Crypto Complete.

Aproximación 2:

A. En lugar de utilizar el Registro del campo y un archivo lógico, utilice las APIs EncAES dentro de su aplicación para encriptar los valores de los campos de solo aquellos registros que reúnan los criterios de selección de su aplicación. Estas APIs están documentadas en la Guía del Programador de Crypto Complete.

B. Para desencriptar valores utilice los procedimientos DecAES*.

11. Apéndice A - Autorización All-Object

Por defecto, la autorización especial *ALLOBJ permite al usuario acceder a cualquier recurso del sistema tenga o no tenga ese recurso autorización privada para ese usuario. Aún cuando el usuario tenga autorización *EXCLUDE sobre un objeto, la autorización especial *ALLOBJ permite a ese usuario acceder al objeto. **Un usuario con autorización especial *ALLOBJ puede ver, cambiar o borrar cualquier objeto.** Estos usuarios pueden también dar autorización sobre un objeto a otros usuarios del sistema.

Cuando se encriptan o desencriptan datos, se producen comprobaciones de autorización propias de IBM para determinar si un usuario tiene autorización sobre el objeto del Almacén de Claves *VLDL, que contiene la clave de encriptación/desencriptación. Si el usuario tiene autorización *ALLBOJ, entonces el sistema IBM dirá que el usuario está autorizado, lo que permite al usuario acceder a la clave para encriptar y desencriptar datos. (Vea el cuadro contiguo para saber cómo el sistema IBM realiza las comprobaciones de autorización).

Adicionalmente, cuando se determina si el usuario está autorizado sobre un valor enmascarado o completo (en una operación de desencriptación), el sistema IBM comprueba los permisos del usuario sobre las Listas de Autorización que pueden especificarse para el campo en el registro de Encriptación de Campos. Si el usuario tiene autorización *ALLOBJ, entonces el sistema IBM indicará que el usuario está autorizado sobre la Lista de Autorización, lo que permitirá al usuario acceder al valor entero del campo desencriptado.

Como una buena práctica de seguridad, sería conveniente que no hubiera usuarios en el sistema con autorización especial *ALLOBJ. Quizás no sea posible si algunas de sus aplicaciones antiguas pueden fallar cuando se elimina la autorización especial *ALLOBJ. Por ello, proponemos dos opciones a nuestros clientes para tratar el problema de la autorización especial *ALLOBJ.

COMPROBACION DE AUTORIZACION SOBRE OBJETOS REALIZADOS POR EL SISTEMA IBM i

1.- ¿El perfil de usuario está definido con autorización *ALLOBJ? Si la tiene definida, tiene autorización para utilizar el objeto.

2.- ¿El perfil de usuario tiene autorización individual sobre el objeto? El acceso sobre el objeto dependerá sobre las autorizaciones que posea sobre el objeto.

3.- ¿El perfil de usuario tiene autorización a través de una lista de autorizaciones externa que está asociada al objeto? Si está presente en la lista de autorizaciones, entonces tiene acceso o no según lo que especifique esa lista de autorizaciones.

4.- ¿Pertenece el usuario a un perfil de grupo que tiene autorización *ALLOBJ? Si es así, tiene acceso garantizado al objeto.

5.- El perfil de grupo asociado, al que está asociado el perfil de usuario, ¿tiene autorización sobre el objeto? Tendrá acceso o no sobre el objeto según las autorizaciones sobre el objeto que tenga el perfil de grupo.

6.- El perfil de grupo, al que está asociado el perfil de usuario, ¿tiene autorización a través de una lista de autorizaciones externa asociada a un objeto? Si está presente en la lista de autorizaciones, tendrá o no acceso según sean las autorizaciones para ese grupo en la lista de autorizaciones.

7.- ¿Tiene el objeto autorización *PUBLIC suficiente para permitir que el usuario pueda acceder al objeto? El usuario tiene acceso o no según sea la autorización pública del usuario para ese objeto.

OPCIÓN 1 – Cambiar la autorización *ALLOBJ del usuario a un perfil de grupo

Por como IBM i comprueba la autorización de los objetos (ver cuadro página anterior), podría mover la autorización especial *ALLOBJ desde el nivel de perfil de usuario individual a un perfil de grupo (al cual asignará luego el usuario). De este modo, el usuario obtiene la autorización *ALLOBJ del perfil de grupo, dando al usuario (por defecto) acceso a todos los objetos del sistema. Así ahora podría excluir al usuario de ciertos objetos (con *EXCLUDE) tales como el Almacén de Claves y las Listas de Autorización empleadas por Crypto Complete.

Siga los siguientes pasos para configurar esta opción:

1. Cree un Perfil de Grupo (Group User Profile) con la autorización especial *ALLOBJ mediante el mandato CRTUSRPFR.

2. Con el mandato CHGUSRPRF, cambie el perfil de usuario individual para eliminar la autorización especial *ALLOBJ y asociarlo (mediante el parámetro GRPPRF) con el Perfil de Grupo creado en el paso 1. Este usuario todavía tendrá autorización *ALLOBJ, pero solo a través del Perfil de Grupo.

3. Edite las autorizaciones del objeto que contiene el Almacén de Claves (key Store) mediante el mandato EDTOBJAUT. Añada el perfil de usuario individual (que quiere excluir) al objeto y especifique *EXCLUDE en la Autorización del Objeto (Object Authority).

OPCIÓN 2 – Que Crypto Complete realice sus propias comprobaciones para los usuarios *ALLOBJ

Existe una opción en la Política de Claves de Crypto Complete, la cual permite indicar como manejar los usuarios con autorización *ALLOBJ. Esta opción llamada “Limit all-object authority” y el parámetro LMTALLOBJ. Las opciones válidas son *NO y *YES.

*YES - Crypto Complete realizará su propia comprobación de autorizaciones sobre cualquier solicitud sobre el Almacén de Claves o Listas de Autorización para aquellos usuarios con autorización *ALLOBJ. El perfil de usuario, o perfil de grupo al que pertenezca, debe estar específicamente listado como una entrada autorizada (con al menos autorización *USE) en el Almacén de Claves o en la Lista de Autorizaciones.

Comprobación de Autorización en el Almacén de Claves (Key Store)

Si en la Política de Claves de Crypto Complete se ha especificado LMTALLOBJ(*YES) y el usuario tiene autorización especial *ALLOBJ, se producirán los siguientes pasos para determinar si el usuario tiene autorización sobre el objeto *VLDL Almacén de Claves que contiene la clave solicitada en las operaciones de encriptación y desencriptación:

1. ¿Tiene el perfil de usuario la entrada autorizada definida en el objeto? Si tiene autorización *USE definida en el objeto, entonces el usuario está autorizado sobre el objeto. En caso

contrario, si no tiene como mínimo *USE, entonces el usuario no estará autorizado sobre el objeto.

2. ¿Pertenece el usuario a un perfil de grupo u otros perfiles de grupo suplementarios que tienen la entrada autorizada definida en el objeto? Si el perfil de grupo tiene autorización *USE definida en el objeto, entonces el usuario está autorizado sobre el objeto. En caso contrario, si no tiene como mínimo *USE, entonces el usuario no estará autorizado sobre el objeto.
3. Comprobar la autorización *PUBLIC del objeto. Si tiene autorización *USE definida para el perfil *PUBLIC como mínimo, entonces el usuario está autorizado sobre el objeto. En caso contrario, si no tiene como mínimo *USE y tampoco existe una Lista de Autorizaciones sobre el objeto, entonces el usuario no estará autorizado sobre el objeto.
4. ¿Existe una Lista de Autorización sobre el objeto Almacén de Claves (Key Store) y está el perfil de usuario en esa Lista? Si tiene autorización *USE definida en el objeto para la lista de autorización, entonces el usuario está autorizado sobre el objeto. En caso contrario, si no tiene como mínimo *USE, entonces el usuario no estará autorizado sobre el objeto.
5. ¿Existe una Lista de Autorización sobre el objeto Almacén de Claves (Key Store) y el usuario pertenece a un perfil de grupo u otros perfiles de grupo suplementarios que existen en esa Lista? Si la autorización es *USE como mínimo en la lista de autorizaciones para cualquiera de los perfiles de grupo, entonces el usuario estará autorizado sobre el objeto. En caso contrario, y ninguna de esos perfiles de grupo tienen*USE como mínimo definido en la lista de autorizaciones, el usuario no estará autorizado sobre el objeto.
6. Si existe una Lista de Autorización sobre el objeto Almacén de Claves (key Store), compruebe la autorización *PUBLIC de esa lista. Si *PUBLIC tiene autorización *USE como mínimo definida en la Lista de Autorización, entonces el usuario está autorizado sobre el objeto. En caso contrario, y la entrada *PUBLIC no es *USE como mínimo, entonces el usuario no estará autorizado.

Lista de Autorización del Registro de Campos

Las Listas de Autorizaciones pueden asignarse a un campo dentro del Registro de Encriptación de Campos para indicar que usuarios están autorizados a los valores enmascarados o valores completos. Si se ha especificado LMTALLOBJ(*YES) en la Política de Claves y el usuario tiene autorización especial *ALLOBJ y se ha especificado lista de autorización para el campo, se realizarán los siguientes pasos para comprobar si el usuario está autorizado:

1. ¿Existe el perfil de usuario en la Lista de Autorizaciones? Si tiene autorización *USE, entonces el usuario está autorizado sobre el objeto. En caso contrario, si no tiene como mínimo autorización *USE, entonces el usuario no estará autorizado sobre el objeto.
2. ¿Pertenece el usuario a un perfil de grupo u otros perfiles de grupo suplementarios y existe alguna entrada del perfil de grupo o lo perfiles de grupo suplementarios en la Lista de Autorizaciones? Si tiene autorización *USE para una o más de las entradas del grupo, entonces el usuario está autorizado sobre el objeto. En caso contrario, si no tiene como mínimo autorización *USE, entonces el usuario no estará autorizado sobre el objeto.

3. Compruebe la entrada *PUBLIC de la Lista de Autorizaciones. Si tiene autorización *USE, entonces el usuario está autorizado sobre el objeto. En caso contrario, si no tiene como mínimo autorización *USE, entonces el usuario no estará autorizado sobre el objeto.

Precaución:

- Un usuario con autorización *ALLOBJ puede cambiar la autorización de cualquier objeto del sistema, incluidos los objetos *VLDL del Almacén de Claves (Key Store) y las Listas de Autorización. De modo que si un usuario *ALLOBJ es limitado por Crypto Complete con LMTALLOBJ(*YES), podría DARSE AUTORIZACIÓN a si mismo sobre el Almacén de Claves y Las Listas de Autorizaciones. Dado que no puede restringir que un usuario con *ALLOBJ pueda cambiar las autorizaciones, la única opción es auditar los cambios de autorización con el mandato CHGOBJAUD.
- La autorización adoptada de programas no será reconocida para los usuarios con autorización *ALLOBJ cuando se especifica LMTALLOBJ(*YES). Por ejemplo, si un usuario *ALLOBJ está ejecutando un programa que adopta autorización del propietario del programa, este usuario *ALLOBJ no adoptará la autorización sobre el Almacén de Claves (key store) si el propietario del programa si tuviera autorización sobre el Key Store.

12. Apéndice B - Procedimientos de Campo DB2 (DB2 Field Procedures

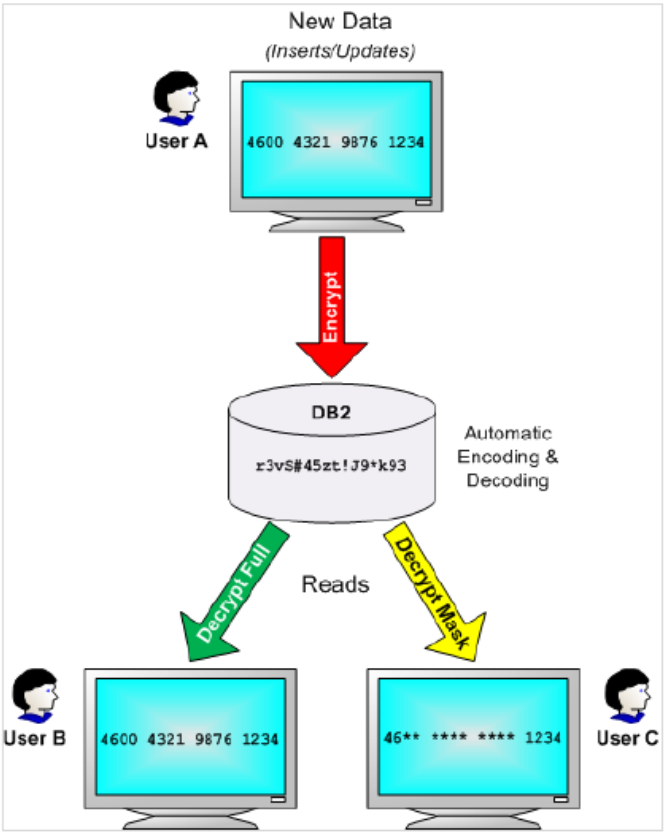
Solo para usuarios del Módulo de Encriptación de Campos de Crypto Complete

Los FieldProcs (DB2 Field Procedures - Procedimientos de Campo DB2) fueron introducidos en la versión 7.1 de IBM i, para simplificar la encriptación de campos. Un FieldProc puede situarse en un campo de la base de datos, lo que llamará a un exit program especficado por el usuario cuando se lean datos del campo, se añadan o actualicen. De algún modo, los FieldProcs son similares a los Triggers de base de datos, pero que aportan dos ventajas significativas.

A. Los FieldProcs permiten que los datos sean modificados (por el exit program) en una operación READ. Esto permite que el exit program desencripte automáticamente el valor del campo antes de que sea devuelto al usuario o a la aplicación. Por tanto, no deben realizarse cambios en la aplicación para poder desencriptar datos, lo cual reduce drásticamente el tiempo de implementación de la encriptación a nivel de campos.

B. Los FieldProcs proporcionan un espacio interno aparte en el fichero existente para almacenar la versión encriptada de los valores de los campos. Este espacio interno permite encriptar otros tipos de campo (numéricos, fecha, hora) sin tener que almacenar los valores alfanuméricos encriptados en un archivo separado.

Si bien IBM proporciona este "enganche" a la base datos con los FieldProcs, se necesitan soluciones de terceros, como Crypto Complete, para que creen los exit programs de los FieldProc y realizar las funciones de encriptación / desencriptación.



Crypto Complete simplifica la creación y gestión de FieldProcs gracias a las pantallas y mandatos del Registro de Encriptación de Campos. Encripta y desencripta los valores de los campos (dentro de los FieldProcs) adaptándose totalmente a la política y controles de seguridad de Crypto Complete, gestión de claves y controles de auditoría, cumpliendo así con los requerimientos de cumplimiento obligado.

Dependiendo de las listas de autorización asignadas a los campos, los usuarios podrán tener acceso a los valores completos del campo, al valor enmascarado o tener el acceso denegado.

12.1 Implementar los DB2 Field Procedures- FieldProcs

Siga los siguientes pasos para añadir un Procedimiento de Campo DB2 (FieldProc) a un campo de la base de datos para su encriptación:

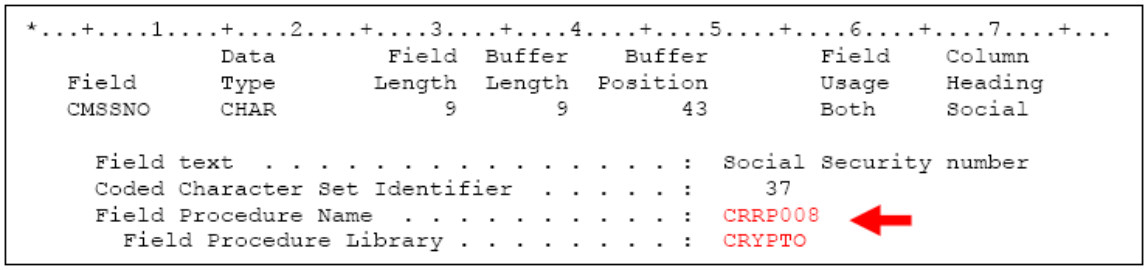
1. Añada el campo de la base de datos al Registro de Encriptación de Campos de Crypto Complete mediante el mandato CRYPTO/ADDFLDENC y F4. Especifique el nombre del campo, el archivo en el que se encuentra, su longitud, la clave de encriptación a utilizar, el formato de enmascaramiento (si es un campo alfanumérico), así como las listas de autorización que controlaran el acceso a los valores desencriptados. Elija a continuación utilizar un FieldProc especificando un *YES en el parámetro USEFLDPROC. Pulse F1 sobre cualquier parámetro para obtener más ayuda. Vea un ejemplo del mandato ADDFLDENC:

```
CRYPTO/ADDFLDENC
FLDID(SOCIAL_SECURITY_NUMBER)
DBFLD(CMSSNO)
DBFILE(PRDATA/EMPLOYEE)
DBFLDTYP(*CHAR)
DBFLDLEN(9)
NCKEYLBL(SS_KEY)
ENCKEYSTR(LIB/KEYSTORE)
FLDMASK('*****9999')
AUTLDEC(SSFULL)
AUTLMASK(SSMASK)
USEFLDPROC(*YES)
FLDPROCOPT(*AUTH)
```

El mandato ADDFLDENC solo añadirá la entrada del campo al Registro de Encriptación de Campos. El FieldProc no se creará hasta que se haya realizado el proceso de Activación en el paso 2.

2. Cuando esté preparado para añadir el FieldProc al campo y realizar una encriptación masiva de los valores de los campos existentes, debe ejecutar en Batch el mandato ACTFLDENC (Activate Field Encryption). No debería haber bloqueos en el fichero en ese momento. Este mandato añadirá el FieldProc al archivo utilizando la sentencia SQL “Alter Table Alter Column Set FieldProc”, la cual añade el área de almacenaje interno al campo (para almacenar los valores encriptados) y encriptará los valores de los campos existentes.

3. Para comprobar si un FieldProc se añadió a su campo, puede ejecutar el mandato DSPFFD en el archivo. El campo debería mostrar el nombre del FieldProc en la biblioteca CRYPTO. Como en este ejemplo:



4. Puede verificar que los valores del campo han sido encriptados utilizando la función HEX_ENCODED de SQL para visualizar los valores hex. Por ejemplo, la sentencia:

   SELECT HEX_ENCODED(cmssno) FROM prdata/employee

   Mostrará los siguientes valores codificados en hex de los 4 primeros registros:

   F0F0F0F0F369D692FD4062D24680
   F0F0F0F0F3BED7758A5B145983FD
   F0F0F0F0F3C2178F6AE5073A83E4
   F0F0F0F0F3E801C9C44F84C16865

   Y vemos que el identificador de la clave ocupa los 5 primeros bytes (negrilla) y los valores encriptados aparecen representados por los bytes restantes.

12.2 Cosas a tener en cuenta sobre DB2 Field Procedures

A continuación enumeramos una serie de conceptos sobre los FieldProcs que es necesario conocer:

- Los FieldProcs son compatibles con los archivos físicos descritos con DDS o tablas SQL
- Varios campos del mismo archivo pueden tener FieldProcs.
- Los FieldProcs son compatibles para archivos con múltiples miembros.
- Nadie más puede utilizar el archivo cuando el FieldProc se está añadiendo al mismo, ya que requiere un bloqueo exclusivo para realizar la encriptación del campo.
- Añadir un FieldProc al archivo no cambiará el formato del identificador de nivel, de modo que no necesita recompilar los programas que utilizan ese archivo. No generará errores “level check” en los programas.
- Si duplica un archivo (CRTDUPOBJ), los FieldProcs también se duplicarán.

12.3 Rendimiento de DB2 Field Procedures

Cada vez que se actualice, lea o busque un campo se llamará a un exit program FieldProc (DB2 Field Procedure). A continuación enumeramos algunos de los eventos conocidos hasta la fecha que harán que se llame al exit program FieldProc.

Eventos que llaman al programa FieldProc cuando se ENCRIPTA un campo:

- Cuando se añada un nuevo registro. Sea cual sea el programa o método utilizado (RPG; Cobol, SQL, DFU…)
- Cuando se actualice un registro. Aún cuando no cambie el valor del campo.

- Cuando se realice una búsqueda/consulta SQL contra el campo encriptado con un FieldProc. Por ejemplo, si el usuario lanza una sentencia SQL “Select NAME where SSNO = ‘508998888’, entonces el se llamará al FieldProc para encriptar el valor ‘508998888’ y pueda realizar la búsqueda del campo SSNO encriptado con ese valor.
- Cuando se tenga que realizar una búsqueda sobre un campo clave encriptado utilizando operaciones a nivel de registro (SETLL, SETGT, CHAIN, READE). Por ejemplo, si el usuario ejecuta una operación RPG como SSNO CHAIN EMPMAST, entonces se llamará al FieldProc para encriptar el campo clave SSNO para que pueda buscar el campo que tiene ese valor encriptado.

Eventos que llaman al programa FieldProc cuando se DESENCRIPTA un campo:

- Cuando se lee un nivel de registro nativo desde RPG (READ, READE,CAHIN…) y Cobol.
- Cuando se lee un campo con sentencias SELECT y FETCH de SQL.
- Cuando se lee un campo en una Consulta o a través de Report Writer.
- Cuando se accede al campo a través de una herramienta de Transferencia de Archivos (Client Access, Surveyor/400…)
- Cuando se lee un archivo con un mandato CL como DSPPFM o CPYF (si no se está crando el arhchivo)

Importante: La llamada de los exit programs FieldProc como consecuencia de estos eventos mencionados anteriormente se consumen ciclos CPU. Si un campo que contiene un FieldProc es utilizado frecuentemente en sus aplicaciones, estas llamadas repetitivas del programa pueden incrementar los tiempos de respuesta de los trabajos interactivos y extender la duración de trabajos batch. El impacto en el rendimiento podría ser mayor si el archivo contiene varios campos con FieldProcs.

12.4 Precauciones a considerar sobre DB2 Field Procedures

Importante:

- Antes de implementar los DB2 Field Procedures (FieldProcs en el entorno de producción, debe conocer los posibles conflictos que pueden surgir por su uso. Ver la siguiente lista.
- Se recomienda también instalar las últimas PTFs de IBM

Archivos físicos y lógicos – No ordenados correctamente

Conflicto: Si el campo que tiene un FieldProc es un campo clave de un archivo físico o lógico, será buscado según el valor encriptado en cualquier operación READ.

Ejemplo: Si los registros son leídos en el orden de entrada 1,2,3,4,5…, el FieldProc puede que haga que se lean como 5,1,3,2,4…. Estos resultados "desordenados" pueden dar problemas en sus aplicaciones si sus aplicaciones están esperando el resultado ordenado por los valores desencriptados.

Solución: Para poder clasificar los registros apropiadamente, es decir, por sus valores desencriptados, debe usar una sentencia SELECT de SQL junto con la cláusula ORDER BY sobre los campos que está intentando ordenar. La cláusula ORDER BY llamará al exit program FieldProc asociado para desencriptar los valores para ordenarlos adecuadamente.

CHGPF – Eliminación de FieldProcs

Conflicto: El mandato CHGPF (utilizando los parámetros SRCFILE y SRCMBR) han sido utilizados comúnmente para añadir nuevos campos o cambiar definiciones de campos existentes en los archivos. Desafortunadamente, el uso de CHGPF eliminará cualquier FieldProc del archivo y devolverá cualquier valor encriptado a su valor original desencriptado, lo que podría dar lugar a una exposición no deseada de datos sensibles del archivo.

Solución: De cara a añadir un campo a un archivo o cambiar una definición de campo existente, se recomienda utilizar la sentencia ALTER TABLE de SQL ya que retendrá cualquier FieldProcs existente. Antes de que utilice ALTER TABLE en archivos descritos con DDS, debería convertir la sintaxis DDS del archivo a sintaxis DDL SQL mediante alguna herramienta como Surveyor/400. Consulte con American Top Tools.

Duplicar Archivos – Biblioteca del Registro de Encriptación de Campos

Conflicto: Dado que el nombre de la biblioteca donde se ubica el Registro de Encriptación de Campos se introduce a mano en los campos con FieldProcs, la duplicación del archivo (utilizando CRTDUPOBJ o CPYF CRTFILE(*YES)) en otro entorno también copiará los nombres de la biblioteca introducidos en el nuevo archivo. Esto podría hacer que los FieldProcs del nuevo archivo apunten al Registro en el entorno de biblioteca erróneo, dando lugar a resultados no esperados.

Solución: Cree primero el archivo en el entorno de destino desde cero, utilizando DDS o SQL. Luego añada el campo al Registro de Encriptación de Campos en el entorno de destino y active el campo. Ahora utilice el mandato CPYF para copiar los datos desde el archivo del entorno original al entorno de destino. Las funciones de encriptar y desencriptar funcionarán para cada registro y campo con FieldProcs.

13. Desinstalación de Crypto Complete

Importante: Antes de desinstalar Crypto Complete de su sistema, ASEGÚRESE DE QUE NO EXISTEN DATOS ENCRIPTADOS (que fueron encriptados con Crypto Complete).

Puede desinstalar Crypto Complete de su sistema con el mandato:

```
DLTLICPGM LICPGM(4CRYPTO)
```

El programa 4CRYPTO y la biblioteca CRYPTO serán eliminadas.

14. Terminología de Encriptación

Listed below are the primary encryption terms used throughout this manual.

AES	AES is the abbreviation for Advanced Encryption Standard. AES is an encryption algorithm which utilizes symmetric keys. It provides strong protection and is approved by the U.S. Government for protecting sensitive information. See http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf for more information on the AES encryption standard.
AES128	AES encryption using a key length of 128 bits.
AES192	AES encryption using a key length of 192 bits.
AES256	AES encryption using a key length of 256 bits.
Algorithm	A mathematical process used to scramble (encrypt) data.
Data Encryption Key (DEK)	A symmetric key used to encrypt and decrypt data.
CBC mode	CBC is the abbreviation for Cipher-Block Chaining. CBC mode is available in the AES and TDES algorithms. With CBC mode, you can alter the encryption algorithm by supplying an Initialization Vector (IV) value. Therefore, the same input Plain Text and Key can produce different output Cipher Text values, depending on the IV supplied.
Cipher	A pair of algorithms (mathematical processes) used to encrypt and decrypt data.
Cipher Text	The unintelligible (encrypted) text value generated (output) by an encryption algorithm.
Cryptology	The art and science of keeping data secret.
CUSP mode	CUSP is the abbreviation for Cryptographic Unit Support Program. CUSP mode is available in the AES algorithm. CUSP mode is a special type of CBC mode documented in the z/OS ICSF Application Programmer's Guide (SA22-7522). It is used for handling data that is not a multiple of the block length. The length of output Cipher Text in CUSP mode will always equal the length of the input Plain Text. With CUSP mode, you can alter the encryption algorithm by supplying an Initialization Vector (IV) value. Therefore, the same input Plain Text and Key can produce different output Cipher Text values, depending on the IV supplied.
Decryption	The process of converting Cipher Text (unintelligible code) into Plain Text (readable information).
ECB mode	ECB is the abbreviation for Electronic Codebook mode. ECB mode is available in the AES and TDES algorithms. You cannot use Initialization Vectors (IV) with ECB mode, so the same input Plain Text and Key will always produce the same output Cipher Text value.
Encryption	The process of converting Plain Text (readable information) into Cipher Text (unintelligible code).
Hash	An algorithm for calculating a value based on a block of data. If the data changes in any way, then the hash values will not match when it is recalculated. A hash will protect the integrity of data.

Initialization Vector (IV)	An additional value that can be supplied to alter the encryption algorithm in order to produce a different result. In other words, the same input Plain Text and Key can produce different output Cipher Text values, depending on the IV supplied. This is especially useful to ensure the security of small encrypted values.
Key	The information needed to control the detailed operations of the Cipher. In contrast to human-generated passwords, Keys are more secure since they are computer-generated and are represented as an obscure series of bits (1001110…).
Key Store	An object used to organize and store one or more keys.
Master Encryption Key (MEK)	A key used to protect (encrypt) other keys.
Passphrase	Alternative name for *password*. A string of characters (entered by the user or supplied by a program) that can be used to create a Key.
Plain Text	The readable (decrypted) text value generated (output) by a decryption algorithm.
Symmetric Key	A key which can be used to encrypt and decrypt data. The key must be kept secret or the security is compromised.
TDES	TDES is the abbreviation for Triple DES (Data Encryption Standard). TDES is an encryption algorithm which utilizes symmetric keys. TDES is slowly disappearing from use since AES is up to 6 times faster and offers higher protection than TDES.
Tokenization	Tokenization is the process of replacing sensitive data with unique identification numbers (e.g. tokens) and storing the original data on a central server, typically in encrypted form.