Guía del Usuario II

Módulo de Encriptación de Campos

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

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

Nota ATT

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

GUIA DEL USUARIO_I_Crypto Complete_Herramienta_de_Encriptación.pdf

GUIA DEL USUARIO_II_Crypto Complete_Encriptación_de_Campos.pdf

GUIA DEL USUARIO_III_Crypto Complete__Backup e IFS encriptados.pdf

GUIA DEL USUARIO_IV_Crypto Complete_Encriptación Automática carpetas IFS.pdf

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

Guía del Usuario II - Encriptación de Campos

1. Encriptación de Campos de Base de Datos

Los valores de los campos pueden ser encriptados y desencriptados usando una variedad de métodos de cifrado en Crypto Complete, proporcionando una gran flexibilidad para su empresa. Por cada campo de la base de datos, puede elegir la técnica a utilizar más apropiada para las necesidades de su aplicación.

La opción recomendada para la encriptación campos es el uso del innovador Registro de Encriptación de Campos de Crypto Complete. Permite señalar y registrar los campos de la base de datos a encriptar. Cuando un campo se "activa" en el Registro, Crypto Complete realizará una encriptación masiva de los valores actuales de ese campo. A partir de ese momento, Crypto Complete encriptará automáticamente los valores de campo según se vayan modificando y añadiendo nuevos.

La función de **encriptación automática** del Registro de Encriptación de Campos de Crypto Complete elimina la necesidad de realizar cambios en los programas de sus aplicaciones para la encriptación de campos.

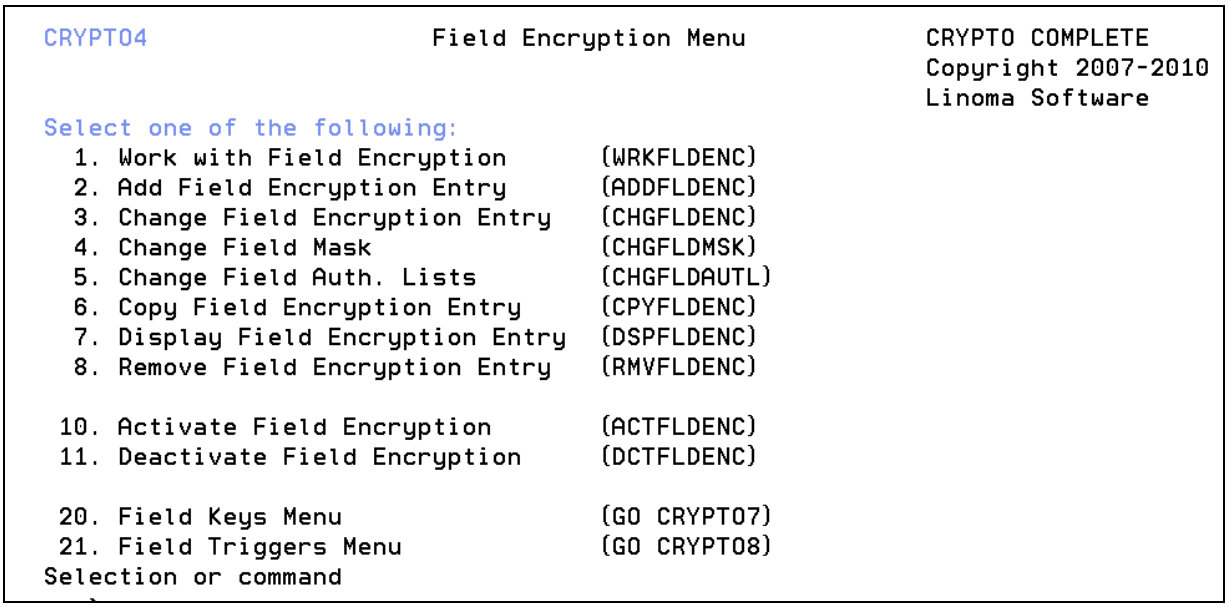
Si se utilizan los Procedimientos de campo de DB2 (disponibles en IBM i V7R1) , los valores también pueden ser automáticamente desencriptados sin cambios en sus programas.

En versiones de i/OS anteriores a la V7R1, en las que esta característica no está disponible **unos sencillos cambios en sus programas permitirán desencriptar los valores mediante las APIs de Crypto Complete.**

Si lo desea, también puede modificar sus aplicaciones para encriptar los datos a través de llamadas a los programas y procedimientos de encriptación de Crypto Complete. Crypto Complete incluye también procedimientos almacenados (stored procedures) y funciones SQL, que pueden ser llamadas desde dentro de las aplicaciones nativas o de otros clientes externos (es decir, interfaces gráficas o web) para la encriptación y desencriptación.

Dispone del mandato FNDDBFLD - Buscar Campos de la base de datos - que permite encontrar los campos de base de datos (en los archivos físicos y tablas) que contengan los valores que cumplan los criterios de búsqueda especificados. Es especialmente útil para encontrar los campos que contienen datos sensibles sin encriptar, como números de tarjetas de crédito, números de seguridad social…*(Ver más información en el apartado 4 de este manual)*

Desde la pantalla de Menú Principal de Crypto accedemos a la gestión de la encriptación de campos con la opción 4. Field Encryption Menu (GO CRYPTO4) y se obtiene la siguiente pantalla.



Pantalla del Menú de Encriptación de Campos

1.1 Conceptos Básicos de Encriptación

Los datos encriptados (texto cifrado) están en formato alfanumérico. Dado que los algoritmos de cifrado utilizan el conjunto completo de caracteres, verá los datos cifrados como una combinación de letras, caracteres especiales y números. Por ejemplo:

```
Sin encriptar:          The quick brown fox jumped over the lazy dog
Texto encriptados:      „OE \ËKä°BBY ý\åê·Ñ,C‹Ÿ^{F+rAÀJ[13]~()$j1Ï(¾Y½i›”®t
```

a) Algoritmos de encriptación

Crypto Complete utiliza los algoritmos de encriptación AES y TDES. Ambos algoritmos siguen las especificaciones (no propietarias) estándar publicadas en el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST).

El estándar TDES (Triple DES) fue introducido en 1998. Se llama así porque aplica el algoritmo de cifrado Data Encryption Standard (DES) tres veces para cada bloque de datos. El TDES tiende a desaparecer lentamente debido a problemas de rendimiento y tamaños de clave más débiles.

El algoritmo AES (Advanced Encryption Standard) estándar fue introducido en 2001. AES es el primer algoritmo de cifrado de acceso público y abierto aprobado por el Gobierno de los EE.UU. para información de alto secreto. AES ofrece un alto rendimiento y proporciona longitudes de clave de hasta 256 bits mucho más seguras. Gracias a estas características ha resultado tener una gran aceptación para el encriptado de datos.

b) Modos de encriptación

Los estándares AES y TDES ofrecen varios métodos de funcionamiento que puede escoger. **Crypto Complete contempla y soporta tres métodos CUSP, ECB y CBC.**

CUSP Mode (Cryptographic Unit Support Program)

- El modo CUSP es compatible con el algoritmo **AES**.
- Este es un modo stream-based. Esto significa que la longitud de los datos encriptados será igual a la longitud de los datos de entrada. Este modo **es útil si el dato del campo no es divisible por una longitud de bloque** y si usted desea almacenar los valores encriptados en el propio campo (si no se utiliza un procedimiento de campo de DB2).
- Con el modo de CUSP, si lo desea, puede especificar un **Vector de Inicialización (IV).** Un Vector de Inicialización (IV) es un valor arbitrario que puede introducir, el cual será utilizado como un **dato de entrada adicional para el algoritmo de encriptación**. Por lo tanto, la salida encriptada depende de la combinación del Vector de Inicialización, la clave de encriptación y el texto a encriptar.

ECB Mode (Electronic Code Book)

- El modo ECB es compatible y soportado por los algoritmos AES y TDES.
- Es un modo basado en bloques (block-based(*)).
- No puede especificarse un Vector de Inicialización.

CBC Mode (Cipher Block Chaining)

- El modo CBC es compatible y soportado por los algoritmos AES y TDES.
- Es un modo basado en bloques (block-based(*)).
- Puede especificarse un Vector de Inicialización opcionalmente.

(*) Notas sobre modo basado en bloques (block-based)

Si se utiliza el algoritmo AES con los modos CBC o EBC, la longitud de los datos encriptados será como mínimo de 16 de caracteres. Su longitud “block-based” será divisible por 16 o 24. Por ejemplo:

Original Field Length	Encrypted Length
10 bytes	16 bytes
16 bytes	16 bytes
17 bytes	24 bytes
24 bytes	24 bytes
31 bytes	32 bytes

Si se utiliza el algoritmo TDES con los modos CBC y ECB, la longitud de los datos encriptados será como mínimo de 8 caracteres de largo. Su longitud “block-based” será divisible por 8. Por ejemplo:

Original Field Length	Encrypted Length
5 bytes	8 bytes
8 bytes	8 bytes
9 bytes	16 bytes
16 bytes	16 bytes

Nota adicional: Para los modos ECB y CBC. Si la longitud de un campo alfanumérico no es divisible por la longitud del bloque, entonces puede elegir entre almacenar los valores encriptados en una archivo externo separado o bien utilizar el Procedimiento de Campo DB2.

Modo de Encriptación soportados por CC.	Algoritmo Encriptación	Stream Based	Block Based	Vector de Incialización
CUSP	AES	Si	-	Si
ECB	AES,TDES	-	Si	No
CBC	AES,TDES	-	Si	Si

2. Registro de Encriptación de Campos

El Registro de Encriptación de Campos de Crypto Complete permite especificar (registrar) los campos de la base de datos que requieren encriptación. Existen varias opciones configurables por cada campo de la base de datos agregados al Registro.

Una opción es que Crypto Complete cree **Triggers SQL** en el archivo de la base de datos automatizando así la encriptación de los valores de los campos de la base de datos cuando se introduzcan nuevos datos (insertar) y cuando los valores del campo se actualicen en la base de datos. Esto permite minimizar los cambios en la aplicación y centrarse solo en aquellos programas que tengan que recuperar valores desencriptándolos.

Para los clientes de IBM i V7R1 o superior, otra opción es que Crypto Complete establezca un Procedimiento de Campo DB2 en el campo de la base de datos, automatizando de este modo tanto la encriptación como la desencriptación de sus valores. Esta opción tiene el potencial de eliminar cualquier cambio de sus aplicaciones. (Ver Apéndice B de la Guía del Usuario I - Herramienta de Encriptación)

Campo tratado con:	Encriptación (Adición o actualización o adición)	Desencriptación (lectura)
Mediante APIs de Crypto Complete	Encriptación APIs y cambios en programas	Desencriptación APIs y cambios en programas
Triggers SQL creados por Crypto Complete	Encriptación Automática	Desencriptación APIs y cambios en programas
DB2 Field Procedures (solo para IBM i V7R1 o mayor)	Encriptación Automática	Desencriptación Automática

2.1 Almacenaje de los Valores Encriptados

El Registro de Encriptación de Campos proporciona una opción de usuario específico para indicar donde deberían almacenarse los valores de campo encriptados. Puede escoger entre almacenar los valores encriptados en la parte “codificada” del campo (mediante el Procedimiento de Campo DB2 - FieldProc), dentro del propio espacio del campo existente, o bien en un fichero externo separado. Está flexibilidad del registro permite especificar una opción de almacenaje distinta para cada campo que se ha encriptado.

a) Almacenar con DB2 Field Procedure (IBM i > V7R1)

Al definir un campo en el Registro de Encriptación de Campos, puede escoger el almacenar los valores encriptados dentro de la porción “codificada” del campo mediante el Procedimiento de Campo DB2 (FieldProc).Está opción es válida si trabaja con IBM i V7R1 o superior. Este enfoque funciona para campos del tipo alfanumérico, numérico, fecha, hora y timestamp.

Nota: Antes de usar los procedimientos de campo DB2 en un entorno de producción, por favor léase el Apéndice "B" para entender los problemas de rendimiento o posibles conflictos y soluciones.

Mismo Campo de Archivo con DB2 Field Procedure (a partir de V7R1)
Alfanuméricos, numéricos, fecha, hora y timestamp
Se almacena en la parte “codificada” del campo.

b) Almacenar en el campo existente

Al definir un campo en el Registro de Encriptación de Campos se puede optar por almacenar los valores encriptados en el espacio existente del campo, siempre y cuando:

- El tipo de campo sea alfanumérico (char)
- Cumpla con los siguientes requisitos de algoritmo, método y longitud:

  - Algoritmo AES con el modo CUSP.
  - Algoritmo AES con modos CBC o el ECB, siempre que la longitud máxima de los valores del campo sea divisible por la longitudes de los bloques, 16 o 24.
  - Algoritmo TDES, siempre que la longitud máxima de los valores en el campo sea divisible por la longitud de bloque de 8.

Mismo Campo de Archivo
Solo si campo es Alfanumérico
• AES y CUSP • AES con CBC o ECB, si longitud máxima del valor del campo es divisible por 16 o 24 • TDES si longitud máxima del valor del campo es divisible por 8.

c) Almacenar en un Archivo Externo

Al definir un campo en el Registro de Encriptación de Campos, puede especificar que los valores encriptados se almacenen en un archivo físico externo separado, que será creado y mantenido por Crypto Complete. El almacenamiento de valores encriptados de un campo en un fichero externo separado tiene las siguientes **ventajas:**

- Pueden encriptarse los campos de tipo numérico, además de los alfanuméricos.
- Si se utiliza el modo ECB o CBC no es necesario que las longitudes de los campos sean divisibles por la longitud del bloque de datos correspondiente según el algoritmo de encriptación.
- La clave de encriptación de datos (DEK) puede cambiarse en cualquier momento sin tener que reencriptar todos los valores de los campos. Pueden especificarse hasta 99.999 claves DEK para un campo.
- Se almacena información adicional en el archivo externo, como el registro de los id de usuario y timestamps en que los valores de los campos fueron actualizados (encriptado) o vistos (desencriptados).

En un archivo externo
Campos Alfanumérico y numéricos.
• Con CBC o ECB no es necesario que las longitudes de cmapos sean divisibles por la longitud de bloque según sea AES o TDES. • Se crea archivo externo con dato encriptado e información adiconal.

Cuando se utiliza la opción de almacenamiento en un archivo externo**, se creará un archivo físico distinto por cada campo de la base de datos que sea activado** en el Registro de Encriptación de Campos. El usuario puede especificar el nombre del archivo externo o bien, será generado por Crypto Complete.

En este último caso, Crypto utilizará la siguiente convención de nomenclatura: CRXXnnnnn, donde "CRXX" es constante y "nnnnn" es un número secuencial del 1 al 99999.

La descripción del objeto del fichero externo creado contendrá el nombre del archivo y biblioteca y el nombre del campo de la base de datos original, para el que está almacenando los valores encriptados. La disposición del registro en el archivo externo es la siguiente:

Field	Example value	Optional
Field Identifier	CREDIT_CARD	
Index number	7	
Key id	2	
Last updated by user	BILL	
Last updated time	2009-07-10-18.09.39.375000	
Last retrieved by user	MARY	Yes
Last retrieved time	2009-07-15-01.22.32.567000	Yes
Record hash	œôÊA·□	Yes
Encrypted value	{¥háö,q'M□™□TVà#	

Crypto Complete creará un registro en el archivo externo correspondiente a cada campo, por cada valor de campo encriptado. A cada registro del archivo externo se le asignará un Índice numérico secuencial único. Este Índice numérico, debe ser almacenado además en el campo existente en el archivo de la base de datos de su aplicación. Utilizando el ejemplo anterior, el índice numérico 7 debe ser almacenado en el campo existente en la base de datos.

Cuando se vaya a recuperar el valor del campo, la aplicación pasará el Índice numérico (almacenado en el campo existente en la base de datos) a un procedimiento del Crypto Complete. Crypto Complete que utilizará este índice numérico para recuperar el valor encriptado en el archivo externo. Crypto completa desencriptará el valor del campo y lo devolverá a la aplicación (si está autorizado).

Precaución: Si se almacenan los valores encriptados en un archivo externo, entonces el campo existente (el que vamos a encriptar) debería ser lo suficientemente largo para poder acoger los Índices Numéricos. Por ejemplo, si su archivo existente no contiene ni contendrá más de 999.999 registros, entonces el campo existente (a encriptar) debería tener una longitud mínima de 6 para poder contener un número de índice de 0 a 999999.

d) Almacenaje Externo - Archivo Lógico Opcional

Crypto Complete también puede crear opcionalmente un archivo lógico sobre el archivo físico externo si se utiliza la opción de almacenaje externo. Este archivo lógico estará indexado por el Identificador del Campo y el Valor Encriptado. Esto es útil si necesita recuperar un registro del (chain out to) archivo físico externo utilizando un valor de campo encriptado especificado por el usuario o una aplicación.

Archivo Externo creado por Crypto Complete
Numérico y Alfanumérico
No necesita cumplir con condiciones de longitud y división de ECB o CBC.
Permite rotar claves DEK sin tener que reencriptar todos los valores. Permite hasta 99.999 claves DEK por campo.
Características archivo externo: • Crea un archivo físico por cada campo activado en el Registro de Encriptación de Campos. • Crea un registro en el archivo externo de un campo por cada valor original que se encripta. • Cada registro tiene un Índice numérico secuencial único asociado que se almacenará en el archivo original. • La longitud del campo existente debe permitir almacenar un índice numérico igual al número total de registros que contenga el archivo original. • Almacena información sobre registro del id de usuario y timestamps cuando se actualizan los campos o se leen. • Se puede crear un archivo lógico sobre el archivo externo.

Cuadro resumen

	Almacenaje			
Tipo Dato	Manual	Internal	External	Field Procedures (V7R1)
Alfánumerico	**SI**	**SI**	**SI**	**SI**
Decimal	**SI**	**-**	**SI**	**SI**
Fecha	**SI**	**-**	**-**	**SI**
TimeStamp	**SI**	**-**	**-**	**SI**
Hora	**SI**	**-**	**-**	**SI**

Crypto Complete permite los almacenajes interno, externo y de Field Procedures según el tipo de dato y campo contemplados en la tabla. Ahora bien, se pueden realizar procesos manuales para realizar la encriptación de datos en archivos externos de fecha u hora.

2.2 APIs suminstradas

En el caso en que **no se utilicen** Triggers SQL o bien Procedimientos de Campo DB2 para automatizar la encriptación de valores de campo, deberán modificarse las aplicaciones que mantienen registros en la base de datos para que **llamen a las API's de encriptación** del Crypto Complete.

APIs para encriptar si no se automatiza mediante Triggers SQL o procedimientos de campo DB2	
APIs si el almacenaje es externo	APIs si el almacenaje es en el campo existentes
• InsEncFld • UpdEncFld • DltEncFld	• EncFld

Si **no está utilizando** los Procedimientos de Campo DB2 (DB2 Field Procedures) para desencriptar automáticamente, entonces las aplicaciones que necesitan tener acceso a los valores de campo desencriptados deben modificarse para que **llamen a las APIs de desencriptación** de Crypto Complete.

APIs para Desencriptación no automatizada	
APIs si el almacenaje es externo	APIs si el almacenaje es en los campos existentes
• GetEncFld • GetEncFldMask • GetEncFldAuth	• DecFld • DecFldMask • DecFldAuth

Encontrará más información acerca de estas APIs en la Guía del Programador (Progammer's Guide).

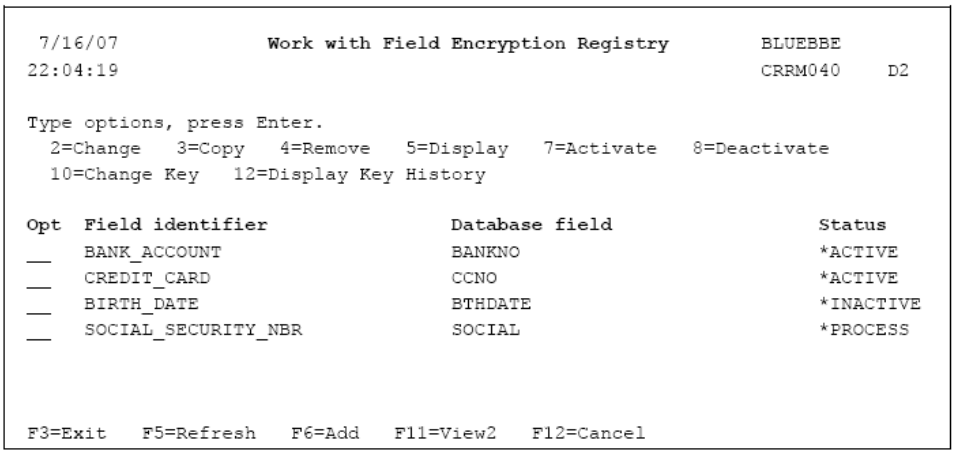
2.3 Mandatos del Registro de Encriptación de Campos

a) Trabajar con el Registro de Encriptación de Campos (WRKFLDENC)

El mandato **WRKFLDENC** permite a los usuarios autorizados trabajar con las entradas del Registro de Encriptación de Campos. La pantalla del mandato incluye funciones para añadir, cambiar, activar, desactivar y eliminar entradas de campos.

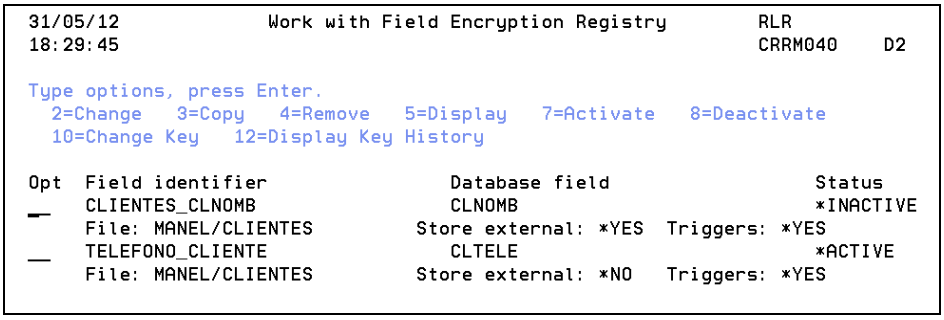
Realice los siguientes pasos para **trabajar con el Registro de Encriptación de Campos**:

1. Ejecute el mandato **CRYPTO/WRKFLDENC**
2. Se muestran la siguiente pantalla que contiene las entradas del Registro de Encriptación de Campos



Pantalla del mandato WRKFLDENC

Por cada entrada de campo listada, la pantalla del mandato WRKFLDENC muestra el Identificador de Campo asignado por el usuario, el Nombre del Campo en la base de datos original y su Estado. Pulse F11=View2 para ver más información sobre cada entrada.



Ejemplo de otra Pantalla del mandato WRKFLDENC -F11=View2

Estado del campo

A continuación se muestran los diferentes estados que pueden tener las diferentes entradas de campo que aparecen en el registro.

Status	Descripción
*ACTIVE	La entrada del campo SI está activada para la encriptación
*INACTIVE	La entrada del campo NO está activada para la encriptación
*PROCESS	La entrada del campo está siendo actualizada para activarse/desactivarse
*ERROR	El proceso de activación/desactivación fallo. Llame a American Top Tools.

Opciones de pantalla

Opción	Descripción
2	CAMBIAR la entrada de campo con el mandato CHGFLDENC
3	COPIAR la entrada de campo con el mandato CPYFLDENC
4	BORRAR la entrada de campo con el mandato RMVFLDENC (previa confirmación)
5	VER los valores de la entrada del campo con el mandato DSPFLDENC
7	ACTIVAR el campo de entrada para encriptar con el mandato ACTFLDENC
8	DESACTIVAR la encriptación del campo de entrada con el mandato DCTFLDENC
10	CAMBIAR la clave/s de encriptación/desencriptación de los valores correspondientes a la entrada del campo con el mandato CHGFLDKEY
12	Muestra un histórico de las claves utilizadas para encriptar/desencriptar los valores de la entrada de campo con el mandato WRKFLDKEY

Teclas de Función

Función	Descripción
F3	Salir de la pantalla WRKFLDENC
F5	Refrescar la lista de entradas de campo del Registro de Encriptación de Campos
F6	Añadir una entrada de campo nueva al registro con el mandato ADDFLDENC
F11	Muestra información adicional sobre la entrada del campo: nombre de la base de datos y la configuración del almacén externo y de los Triggers.

b) Añadir un campo en el Registro de Encriptación de Campos (ADDFLDENC)

El mandato **ADDFLDENC** permite a los usuarios autorizados añadir una nueva entrada en el Registro de Encriptación de Campos.

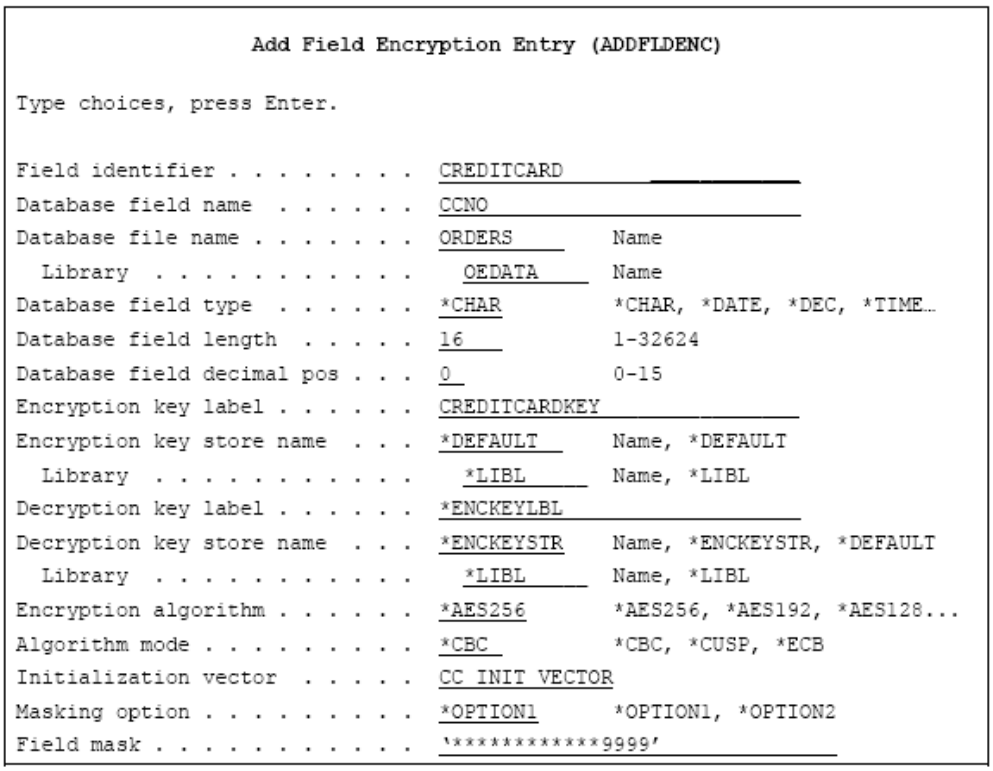
Los siguientes usuarios pueden utilizar este mandato:

- 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 Field Enc.Registry” (Mantener Registro de Encriptación de Claves) establecida en *YES

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL002, lista de validación *VLDL, el cual contiene el Registro de Encriptación de Campos.

Realice los siguientes pasos para **añadir una nueva entrada en el Registro de Encriptación de Campos:**

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



```
                    Add Field Encryption Entry (ADDFLDENC)

Type choices, press Enter.

Field identifier . . . . . .  CREDITCARD
Database field name  . . . . .  CCNO
Database file name . . . . . .  ORDERS       Name
  Library  . . . . . . . . . .    OEDATA     Name
Database field type  . . . . .  *CHAR        *CHAR, *DATE, *DEC, *TIME…
Database field length  . . . .  16           1-32624
Database field decimal pos . .  0            0-15
Encryption key label . . . . .  CREDITCARDKEY
Encryption key store name  . .  *DEFAULT     Name, *DEFAULT
  Library  . . . . . . . . . .    *LIBL      Name, *LIBL
Decryption key label . . . . .  *ENCKEYLBL
Decryption key store name  . .  *ENCKEYSTR   Name, *ENCKEYSTR, *DEFAULT
  Library  . . . . . . . . . .    *LIBL      Name, *LIBL
Encryption algorithm . . . . .  *AES256      *AES256, *AES192, *AES128...
Algorithm mode . . . . . . . .  *CBC         *CBC, *CUSP, *ECB
Initialization vector  . . . .  CC_INIT_VECTOR
Masking option . . . . . . . .  *OPTION1     *OPTION1, *OPTION2
Field mask . . . . . . . . . .  '************9999'
```

Pantalla del mandato ADDFLDENC - Página 1

Note: El mandato ADDFLDENC sólo añade la configuración del campo añadido en el registro. No se producirá ninguna acción sobre el campo del archivo de la base de datos. El campo no se activará para ser encriptado hasta que se utilice el mandato ACTFLDENC (Activate Field Encryption).

```
                    Add Field Encryption Entry (ADDFLDENC)

Type choices, press Enter.

Auth. list for full value  . . .  CCFULL       Name, *NONE
Auth. list for masked value  . .  CCMASKED     Name, *NONE
Auth. list caching . . . . . . .  *YES         *YES, *NO
Not authorized fill value  . . .  *            Character value
Store values in external file  .  *YES         *YES, *NO
External file name . . . . . . .  *GEN         Name, *GEN
  Library  . . . . . . . . . . .    *DBLIB      Name, *DBLIB
External logical file  . . . . .  *GEN_        Name, *GEN, *NONE
  Library  . . . . . . . . . . .    *DBLIB      Name, *DBLIB
Store hash for security check  .  *YES         *YES, *NO
Store last retrieved user/time    *YES         *YES, *NO
Index number alignment . . . . .  *LEFT        *LEFT, *RIGHT
Index number padding character    ' '          Character value
Last index number storage  . . .  *FLDREG      *FLDREG, *PF
Use triggers to auto encrypt . .  *YES         *YES, *NO
Trigger name for inserts . . . .  *GEN
_____________________________
  Library  . . . . . . . . . . .    *DBLIB___   Name, *DBLIB
Trigger name for updates . . . .  *GEN
_____________________________
  Library  . . . . . . . . . . .    *DBLIB      Name, *DBLIB
Trigger name for deletes . . . .  *GEN
_____________________________
  Library  . . . . . . . . . . .    *DBLIB      Name, *DBLIB
Trigger exit program type  . . .  *SRVPGM      *NONE, *PGM, *SRVPGM
Trigger exit program . . . . . .  SRV001       Name
  Library  . . . . . . . . . . .    OELIB       Name, *LIBL
Trigger exit *SRVPGM procedure .  EncExitProc
Use DB2 field procedure  . . . .  *NO          *YES, *NO
Field procedure return value . .  *FULL        *FULL, *AUTH
```

Pantalla del mandato ADDFLDENC - Página 2

Descripción de los campos del mandato ADDFLDENC

Field Identifier	Indica el identificador (nombre) único de la entrada de campo: - Máximo de 30 caracteres. - NO permite o caracteres especiales, excepto subrayado bajo (_). - NO es sensible a mayúsculas/minúsculas. Será almacenado en mayúsculas.
Database Field Name	Especifique uno de los siguientes: - El nombre actual del campo en la base de datos que se va a registrar. - Máximo de 30 caracteres. - Especifique *REMOTE para indicar que el campo está situado en una base de datos remota (no local). Crypto Complete gestionará la encriptación y almacenaje de los valores mediante la “Tokenization”. Vea más sobre Tokenización en el apartado 2.4 de esta guía.

Database File Name - Library	Indicar el nombre y biblioteca del archivo de la base de datos que contiene el campo que se va registrar.
Database field type	Indicar el tipo de datos del campo de la base de datos: *CHAR - El campo es tipo alfanumérico *DEC - El campo es del tipo decimal. Incluye la opción “Packed Decimal” y “Zoned Decimal”. También puede ser un tipo Integro si utiliza el procedimiento de campos DB2 (FieldProc). Si utiliza un FieldProc (DB2 Field Procedure) para encriptar/desencriptar los valores de los campos automáticamente, entonces los siguientes tipos de datos también son posibles: *DATE - El campo tiene formato de fecha *TIME - El campo tiene formato de de hora *TIMESTAMP - El campo tiene formato de TIMESTAMP
Database field length	Indica la longitud de los valores (a encriptar) dentro del campo de la base de datos. Tipo *CHAR, el máximo permitido es de 32624. Tipo *DEC el máximo permitido es de 30. Si no está utilizando el procedimiento de campo DB2 (FieldProc) y si solo quiere encriptar la porción izquierda de un campo alfanumérico, puede especificar una longitud menor a la longitud total real del campo. ATENCIÓN: Si especifica una longitud que es menor que la longitud del campo en la base de datos, cualquier byte remanente en el campo será borrado durante el proceso de activación del campo.
Database field decimal pos	Si ha especificado un tipo de campo *DEC, indique el número de posiciones decimales que contiene el campo. El máximo permitido es 4.
Encryption key label	Indica la Etiqueta de la Clave DEK inicial a utilizar para encriptar los valores de los campos.
Encryption key store name - Library	Indica el nombre y biblioteca del Almacén de Claves que contiene la Etiqueta de la Clave DEK de encriptación. Indique *DEFAULT para utilizar el nombre del Almacén de Claves especificado en la política de claves.
Decryption key label	Indique la Etiqueta de la Clave DEK a utilizar para desencriptar los valores de los campos. Indique *ENCKEYLBL para utilizar el mismo nombre de etiqueta que se introdujo en la Etiqueta de la Clave DEK de encriptación. ATENCIÓN: Si especifica una Etiqueta de la Clave DEK distinta a la Etiqueta especificada para la encriptación, entonces esa clave de desencriptación debería contener el mismo valor de clave que la clave de encriptación. (Ver Nota ATT)
Nota ATT: Para ello, realice una copia de la clave DEK utilizada para encriptar con el mandato CPYSYMKEY asignándole el mismo almacén de claves (cambiar nombre Etiqueta de la Clave DEK) u otro almacén de claves (Podría mantener mismo nombre de Etiqueta de la Clave DEK). De esta manera, el valor de la clave que se usa para encriptar y desencriptar es el mismo.	
Decryption key store name - Library	Indica el nombre y biblioteca del Almacén de Claves que contiene la Etiqueta de la Clave DEK de desencriptación. Indique *DEFAULT para utilizar el nombre del Almacén de Claves especificado en la política de claves. Indique *ENCKEYSTR para utilizar el mismo valor que se introdujo como Almacén de Claves de encriptación.
Encryption algorithm	Indicar el algoritmo que se usará para encriptar/desencriptar los valores de los campos de la base de datos. Los valores admitidos son: *AES256, *AES192, *AES128 y *TDES. Para mayor seguridad se recomienda utilizar *AES256.

Continuación Descripción de los campos ADDFLDENC

Algorithm mode	Indicar el modo de algoritmo a utilizar para encriptar/desencriptar los valores de campo de la base de datos: *CUSP - (Cryptographic Unit Support Program)- Es un modo de encriptación stream-based, lo que significa que la longitud de los datos encriptados será igual a la longitud de los datos introducidos. Este modo es útil si el campo alfanumérico no es divisible por una longitud de bloque y si quiere almacenar los datos encriptados en el campo existente (si no se está utilizando un procedimiento de campo DB2). Este método permite el uso de un Vector de Inicialización. *CBC - (Cipher Block Chaining) - Es un modo de encriptación basado en bloques. Soporta los vectores de inicialización. (*) *ECB - (Electronic Code Book) - Es un modo de encriptación basado en bloques. No soporta los vectores de inicialización. (*) Consideraciones sobre los modos CBC y ECB: - Si utiliza el algoritmo AES, la longitud de los datos encriptados tendrá un mínimo de 16 bytes de largo. Su longitud de bloque será divisible por 16 o 24. - Si utiliza el algoritmo TDES, la longitud de los datos encriptados tendrá un mínimo de 8 bytes de largo. Su longitud de bloque será divisible por 8.
Initialization Vector	Opcional. El Vector de Inicialización (IV) es un valor arbitrario que puede introducir y que se empleará como un parámetro más en el algoritmo de encriptación. Por ello, el resultado encriptado será dependiente de la combinación del Vector de Inicialización, la Clave de Encriptación y el texto a encriptar. Este vector de inicialización se puede especificar solo con los modos *CBC y *CUSP.
Masking Option	Indicar la opción de máscara a utilizar en el campo cuando el valor de máscara sea requerido en una operación de desencriptación. *NONE - No se realiza enmascaramiento *OPTION1 - Puede mostrar o enmascarar posiciones exactas en el valor del campo. (Ver Field Mask) *OPTION2 - Se muestran a la izquierda/derecha del campo cierta cantidad de dígitos o caracteres especificados.
Field mask	Indicar el formato de máscara a aplicar al campo cuando sea requerido el valor enmascarado en una operación de desencriptación. Válido para la *OPTION1. Especifique el número 9 en las posiciones en las que quiera mostrar el valor subyacente en esa posición. Especifique cualquier otro carácter (incluido espacios) o número, en aquellas posiciones en las que se quiera enmascarar el valor subyacente. Por ejemplo, si se especifica una máscara como '**********9999' para una tarjeta de crédito, entonces la parte visible de un campo enmascarado que contiene un número de tarjeta de crédito sería '**********1234'. Otro ejemplo sería, '##99##999' como máscara de un campo que contiene un número de cuenta. Se vería '##76##541'.
Char/Digits to show on left	Indicar el número de caracteres o dígitos a mostrar en el lado izquierdo del valor de un campo. Válido para la *OPTION2 de enmascaramiento. Para un campo de caracteres, cualquier espacio en blanco al inicio de la cadena será ignorado al realizar el enmascaramiento. Para un campo decimal, los ceros al principio del número serán ignorados.

Char / Digits to show on right	Indicar el número de caracteres o dígitos a mostrar en el lado derecho del valor de un campo. Válido para la *OPTION2 de enmascaramiento. Para un campo de caracteres, cualquier espacio en blanco al final de la cadena será ignorado al realizar el enmascaramiento.
Masking Value	El valor a utilizar como valor de enmascaramiento de un carácter o número. Válido para la *OPTION2 de enmascaramiento. Si está utilizando los DB2 Field Procedures para enmascarar un campo numérico, el valor de enmascaramiento debe ser un número entre 0 y 9. Si NO está utilizando los DB2 Field Procedures, el valor de enmascaramiento, tanto para un campo de caracteres o un campo numérico, puede ser un carácter o número.
Auth.list for full value	Indicar la Lista de Autorizaciones del i5/OS que debe usarse para determinar que usuarios tienen autorización a los valores completos del campo en las operaciones de desencriptación. Esta lista de autorizaciones será utilizada por las APIs de desencriptación de campos de Crypto Complete y los procedimientos de campo DB2. Especifique *NONE para indicar que NO debe usarse una Lista de Autorizaciones para desencriptar. Por ello, el usuario puede acceder a los valores desencriptados totalmente, siempre que estos tengan autorización *USE sobre el Almacén de Claves, que contiene la Clave de Desencriptación. * Ver nota más abajo.

Continuación Descripción de los campos ADDFLDENC

Auth.list for masked value	Indique la Lista de Autorizaciones del i5/OS que debe usarse para determinar que usuarios tienen autorización a los valores del campo enmascarados en las operaciones de desencriptación. Esta lista de autorizaciones ser utilizada por las APIs de desencriptación de campos de Crypto Complete y por los procedimientos de campo DB2. Especifique *NONE para indicar que la lista de autorización NO debería utilizarse por las operaciones de desencriptación. Por ello, el usuario puede tener acceso a los valores enmascarados siempre que estos tengan autorización *USE al almacén de claves que contiene la Clave de Desencriptación. * Ver nota más abajo.
Auth.list caching	Especifique si los permisos sobre las Listas de Autorización deben ser guardadas en la memoria cache. Los valores posibles son: *YES - Se guardarán en la cache. Cuando se produzca una operación de desencriptación de un campo, los permisos sobre las Listas de Autorización se salvarán (en memoria) y utilizarán en futuras comprobaciones de autorización (en las operaciones de desencriptación) dentro del trabajo. Esta opción de cache favorece un mejor rendimiento. Nota: De cara a reconocer cualquier cambio de los permisos sobre las Listas de Autorizaciones, los trabajos, que están realizando operaciones de desencriptación) tendrán que ser reiniciadas. *NO - No se guardan en la cache. Con cada operación de desencriptación se comprobarán los permisos sobre las Listas de Autorización. Esta opción es útil cuando quiera que los cambios sobre las Listas de Autorización sean inmediatamente reconocidos por los trabajos que están realizando operaciones de desencriptación, o si quiere aprovechar las ventajas de la autorización adoptada de programa cuando determina los permisos sobre una Lista de Autorización.

***Nota:** Las Listas de Autorización se pueden crear con el mandato CRTAUTL. Los usuarios o grupos de usuarios que necesiten tener acceso a los valores desencriptados o enmascarados necesitarán al menos autorización *USE sobre la Lista de Autorización. Además, los usuarios que necesiten tener acceso a los valores desencriptados o enmascarados necesitarán al menos autorización *USE sobre el objeto Almacén de Claves que contiene la Clave de Desencriptación.	
Not authorized fill value	Especifique un valor de 1 byte que rellene el valor retornado en una solicitud de desencriptación (desde un FieldProc DB2 o una API 'auth' de Crypto Complete) cuando el usuario no esté autorizado a las Listas de Autorización de valores completos o de valores enmascarados. Por ejemplo, si el valor de relleno es un '9' y la longitud del campo es 7, entonces se devolverá el valor '9999999' en una solicitud de desencriptación no autorizada. Consideraciones: - El valor de relleno es necesario cuando se utiliza un FieldProc (DB2 Field Procedure) y el valor de retorno (FLDPROCOPT) se establece en *AUTH - Si el tipo de campo es *CHAR, entonces el valor de retorno puede ser un número, letra o carácter especial (#, *, %). - Si el tipo de campo es *DEC, entonces el valor de relleno puede ser un número de 1 a 9 si se está utilizando un DB2 Field Procedure. En caso contrario, puede ser un número de 0 a 9. - El valor de relleno no está permitido para tipos de campo *DATE, *TIME y *TIMESTAMP.
Store Values in external file	Indicar si los valores de campo encriptados deben almacenarse o no en un archivo externo: *YES - Se utilizará un fichero externo creado por Crypto Complete para almacenar los valores encriptados. Ver cuadro parámetros adicionales. *NO - Los valores encriptados se almacenan en el mismo campo del archivo de la base de datos. **Nota:** Los valores encriptados deben almacenarse en un archivo externo si no está utilizando un DB2 Field Procedure (Procedimiento de Campo DB2) y siempre que se cumpla alguna de estas situaciones: - Si el tipo de campo es *DEC - Cuando se utilizan los algoritmos *AES128, *AES192 o *AES256 en los modos ECB o CBC, si el tipo de campo es *CHAR y la longitud máxima de los valores del campo no es divisible por 16 o 24. - Cuando se utiliza el algoritmo *TDES, si el tipo de campo es *CHAR y la longitud máxima de los valores del campo no es divisible por 8.

Parámetros adicionales cuando "Store Values in external file = *YES"

External file name - Library	Indicar el nombre y biblioteca del archivo externo que se creará para contener los valores encriptados del campo. *GEN: Crypto Complete genera automáticamente el nombre del objeto utilizando la nomenclatura CRXXnnnnn (siendo CRXX una constante y 'nnnnn' un número secuencial entre 1 y 99999). *DBLIB - El archivo externo será creado en la misma biblioteca en la que reside el archivo de la base de datos. Este archivo fisico estará indexado por el Identificador de Campo (XXFLDID) y el Número de Índice (XXINDEX).
External logical file name - Library	Indicar el nombre y biblioteca del archivo lógico que se creará sobre el archivo fisico, que estará indexado por el Identificador de Campo (XXFLDID) y el Valor Encriptado (XXVALUE).

	*NONE - Para NO crear un archivo lógico sobre el archivo físico externo. *GEN- Para que Crypto Complete genere automáticamente el nombre del objeto, que utiliza la convención de nomenclatura CRXXnnnnnL, siendo CRXX una constante y 'nnnnn' un número secuencial entre 1 y 99999). *DBLIB - Para que el archivo lógico sea creado en la misma biblioteca en la que reside el archivo de base de datos cuyos campos estamos encriptando.
Store hash for security check	Indicar si debe almacenarse un valor HASH por cada registro en el archivo externo: *YES - Se almacenará un valor HASH por cada registro en el archivo externo. El valor HASH de un valor encriptado se calcula según el Identificador del Campo, el Número de Índice y el id de Clave para cada registro. Cuando Crypto Complete recupera un registro de un archivo externo, recalculará el HASH y lo comparará con el HASH almacenado. Si no coinciden los valores HASH se entiende que se ha producido un cambio no autorizado sobre el Identificador del Campo, y/o Número de Índice y/o id de Clave del registro del archivo externo. *NO - No se almacenará un valor HASH en el archivo externo.
Store last retrieved user/time	Indicar si debe almacenarse por cada registro del archivo externo, el id de Usuario y Timestamp, de la última vez que se desencriptó/recuperó un valor de un campo. Nota: Además puede iniciar un control de auditoría sobre una clave de desencriptación para que registre su uso.
Index number alignment	Indicar como debería alinearse en el campo el Número de Índice Externo, cuando se esté encriptando un campo de tipo carácter (alfanumérico) el cual se almacena en un archivo externo. *LEFT - El número índice debería alinearse en la parte izquierda del campo del archivo de base de datos. *RIGHT - El número de índice debería alinearse en la parte derecha del campo del archivo de base de datos.
Index number padding character	Indicar que carácter de relleno utilizar en las posiciones vacías del campo que se encripta y este sea de tipo carácter (alfanumérico). El carácter de relleno NO puede ser un número, ni comillas simples (') ni un guión (-). Por ejemplo, si se especifica '*' con alineación *LEFT, un valor de campo de 10 posiciones con un número de índice 895 aparecería como "895*******".
Last Index number storage	Indicar el tipo de objeto que almacenará el "last index number used" (el último número de índice utilizado). Cada vez que se escribe un registro (inserta) en el archivo externo, el "last index number used" se recupera del objeto, se incrementa en 1 unidad, se asigna al nuevo registro y se salva de nuevo en el objeto. Las opciones de almacenamiento válidas son: *FLDREG - Almacenar el "last index number used" en el objeto de Registro de Encriptación de Campos, que es una lista de validación *VLDL con el nombre CRVL002. Es la opción por defecto. *PF - Almacenar el "last index number used" en un archivo físico con el nombre CRPF002. Un archivo físico es más fácil de replicar que una lista de validación *VLDL en una herramienta de Alta Disponibilidad. También proporciona un mejor rendimiento (que una lista *VLDL) cuando se produce un alto volumen de inserciones en ese campo, porque el archivo físico maneja con más habilidad y eficiencia los bloqueos.

Continuación Descripción de los campos ADDFLDENC

Use Triggers to auto encrypt	Indicar si se deben crear Triggers SQL sobre el archivo de la base de datos los cuales encriptarán automáticamente los valores del campo de la base de datos sin tener que cambiar sus aplicaciones. **Nota:** Recuerde que los Triggers SQL no pueden utilizarse para la encriptación si se utiliza un DB2 Field Procedure. Los valores válidos son: *YES - Se crearán Triggers SQL sobre el fichero. *NO - No se crearán Triggers SQL. Deberá usar los DB2 Field Procedures o utilizar las APIs de encriptación de Crypto Complete desde los programas de la aplicación para encriptar los valores del campo.

Parámetros adicionales...si "Use Triggers to auto encrypt = *YES"

Trigger name for inserts - Libary	Indicar el nombre y biblioteca del _Trigger a crear. Este Trigger se utiliza para encriptar automáticamente el valor del campo, cuando se inserten (añadan) registros en la base de datos. *GEN- Crypto Complete genera automáticamente el nombre del Trigger con la nomenclatura "FILENAME_FIELDNAME_ CryptoInsert" *DBLIB- El Trigger se creará en la misma biblioteca en que reside la base de datos.
Trigger name for updates - Library	Indicar el nombre y biblioteca del Indicar el nombre y biblioteca del Trigger a crear. Este Trigger se utiliza para encriptar automáticamente el valor del campo, cuando se actualicen registros en la base de datos. Es un Trigger de columna, de modo que solo será llamado cuando el valor del campo en particular sea cambiado. *GEN- Crypto Complete genera automáticamente el nombre del Trigger con la nomenclatura "FILENAME_FIELDNAME_ CryptoUpdate" *DBLIB- El Trigger se creará en la misma biblioteca en que reside la base de datos.
Trigger name for deletes - Library	Solo es válido si se utiliza un archivo externo para almacenar los valores encriptados. Indicar el nombre y biblioteca del Trigger a crear. Este Trigger se utiliza para eliminar automáticamente el valor encriptado del campo (registro) del fichero externo, cuando se borre un registro del la base de datos. *GEN- Crypto Complete genera automáticamente el nombre del Trigger con la nomenclatura "FILENAME_FIELDNAME_ CryptoDelete" *DBLIB- El Trigger se creará en la misma biblioteca en que reside la base de datos.
Nota: Los Triggers SQL se salvan (Backup) junto con el archivo físico cuando se ejecutan los mandatos SAVOBJ, SAVCHGOBJ o SAVLIB. No es necesario hacer el Backup de los SQL Triggers de forma separada.	

Trigger Exit Program type	Indicar si los Triggers deben llamar a un Exit Program personalizado antes de añadir, actualizar o borrar el valor del campo. Mostramos unos ejemplos de cómo se podría utilizar un Exit Program como Trigger: 1. Escribir datos adicionales de auditoría en el archivo de journal de auditoría de Crypto Complete. 2. Hacer que Crypto Complete no procese (ignore) la inserción, actualización o borrado solicitado del valor del campo según ciertos criterios, como el id de usuario o la aplicación que realiza la solicitud. 3. Para realizar otro tipo de acción. Un Trigger Exit Program puede escribirse en RPG, Cobol, C en el IBMi. Encontrará ejemplos de programas Trigger RPG en los miembros TRGEXTPGM y TRGEXTSRV en el fuente CRYPTO/ QRPGLESSRC. Los valores válidos son: *NONE - No se utiliza un Trigger Exit Program *PGM - La salida del Trigger es un objeto programa (*PGM) *SRVPGM - La salida del Trigger es un objeto Service Program (*SRVPGM)
Trigger Exit Program - Libarary	Si el tipo de Trigger Exit Program es *PGM o *SRVPGM especifique el nombre y biblioteca donde se aloja el objeto Programa o Service Program al que llamar.
Trigger exit *SRVPGM procedure	Si el tipo de Trigger Exit Program es *SRVPGM, especificar el nombre del procedimiento a llamar dentro del propio *SRVPGM.

Continuación Descripción de los campos ADDFLDENC

Use DB2 field procedure (disponible a partir de IBMi V7R1)	Indicar si se va a utilizar un DB2 Field Procedure para encriptar y desencriptar automáticamente los valores de los campos. Es una aproximación alternativa al uso de los Triggers y la llamada a APIs. Un DB2 Field Procedure (FieldProc) también permite almacenar los valores encriptados “codificados” dentro del propio campo existente, lo que es especialmente útil para campos numéricos (No necesitará crear un archivo externo separado para almacenar los valores de los campos numéricos). Los DB2 Field Procedures están disponibles a partir de la versión de IBMi V7R1. Recomendamos la lectura del Apéndice B de la “GUIA DEL USUARIO_I_Crypto Complete - Herramienta de Encriptación” antes de introducir el uso de DB2 Field Procedures en un entorno de producción, para conocer los riesgos y conflictos sobre el rendimiento. Los valores válidos son: *YES - Se utiliza un DB2 Field Procedure para encriptar/desencriptar los valores del campo. *NO - No se utiliza un DB2 Field Procedure. Deberán usarse entonces los Triggers o APIs para encriptar los valores. Deberán usarse las APIs para desencriptar los valores.

Field procedure return value	Esta opción determina que valor del campo devolverá (según permisos de usuario) el DB2 Field Procedure a la aplicación en una operación de lectura. Los valores válidos son: *FULL - Devuelve el valor desencriptado completo si el usuario tiene como mínimo permisos *USE sobre la Lista de Autorización especificada en el parámetro AUTLDEC (o si se especifica *NONE en ese parámetro). En caso contrario, se genera un error con el id de mensaje CPF504D en la aplicación que realiza la lectura. La opción *FULL está disponible para los tipos de datos *CHAR, *DEC, *DATE, *TIME y *TIMESTAMP. *AUTH -Para los campos de caracteres (*CHAR) que tengan una longitud de hasta 30 bytes, esta opción devuelve: 1) *El valor completo* (full) si el usuario tiene al menos permisos *USE sobre la Lista de Autorización especificada en el parámetro AUTLDEC (o si se especifica *NONE en ese parámetro) 2) *El valor enmascarado* si el usuario tiene al menos autorización *USE a la Lista de Autorización especificada en el parámetro AUTLMASK (o si se especificó *NONE en ese parámetro) 3) *El valor de relleno* si el usuario no tiene al menos permisos *USE a alguna de las listas de autorización. - Para los campos decimales/numéricos (*DEC) o campos de caracteres cuya longitud sea mayor de 30 bytes, esta opción devuelve el valor completo si el usuario tiene al menos permisos *USE a la Lista de Autorización especificada en el parámetro AUTLDEC (o si se ha especificado *NONE en ese parámetro). En caso contrario (si no está autorizado) se devuelve el valor de relleno. - Esta opción *AUTH no es válida para los tipos de datos *DATE, *TIME y *TIMESTAMP.

c) Cambiar Entrada de Encriptación de Campo (CHGFLDENC)

El mandato **CHGFLDENC** permite a los usuarios autorizados cambiar la configuración de una entrada de campo *INACTIVE en el Registro de Encriptación de Campos.

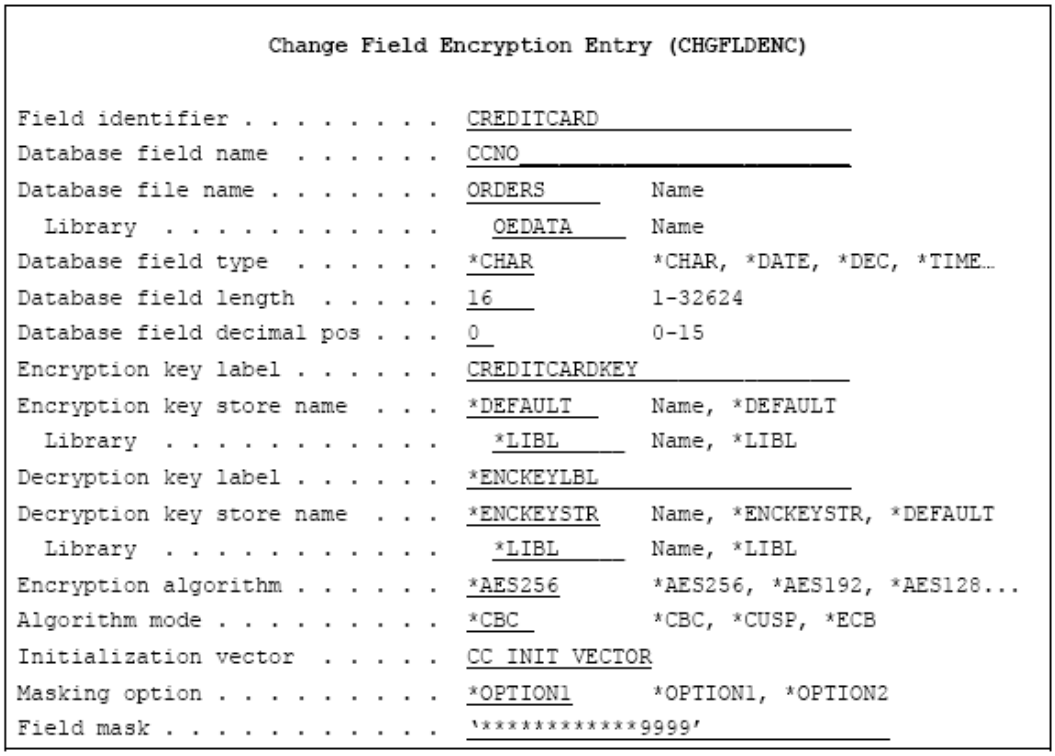
Los siguientes usuarios pueden utilizar este mandato:

- 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 Field Enc.Registry” (Mantener Registro de Encriptación de Claves) establecida en *YES

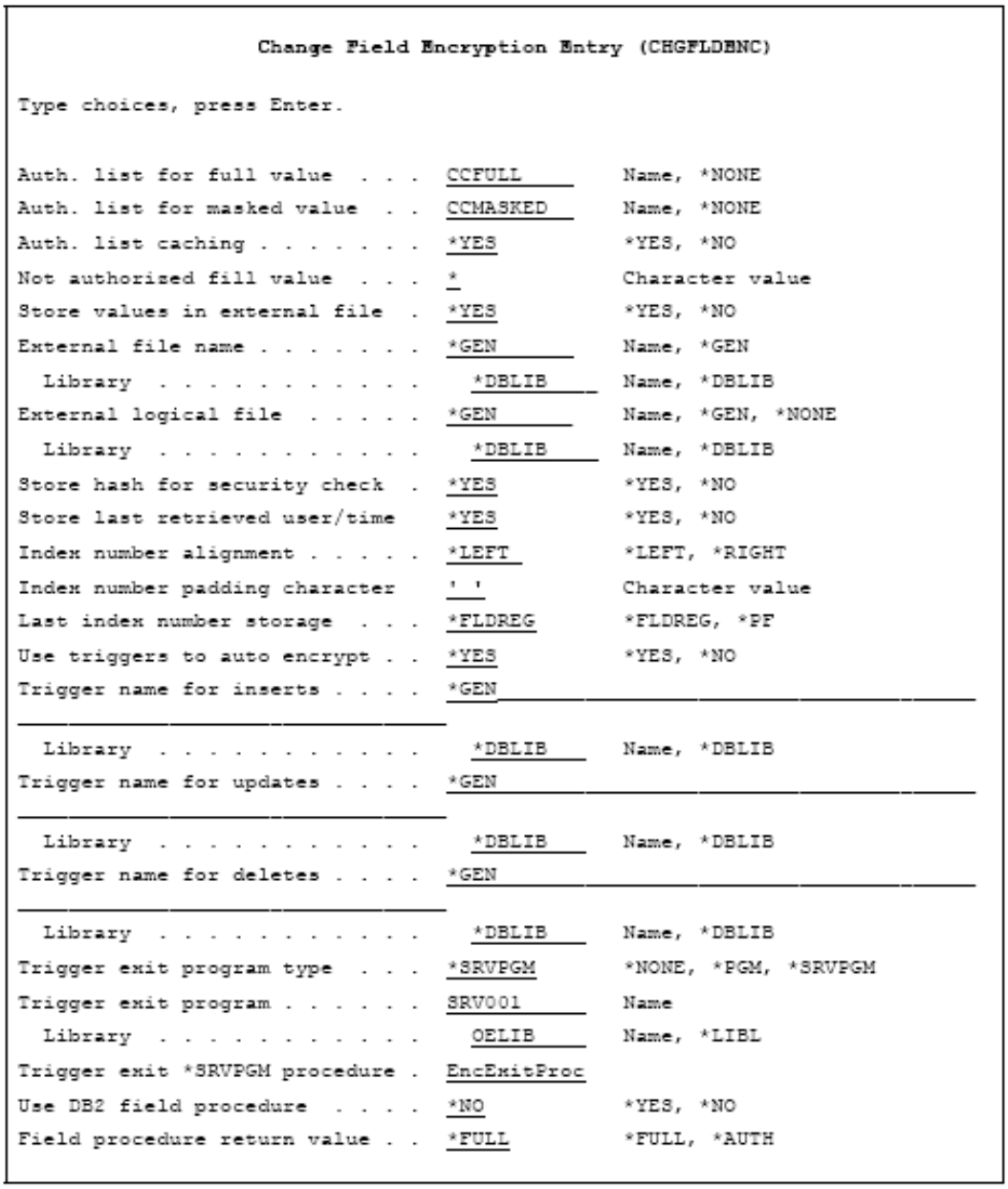
Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL002, lista de validación *VLDL, el cual contiene el Registro de Encriptación de Campos.

Realice los siguientes pasos para **cambiar una entrada de campo en el Registro de Encriptación de Campos:**

1. Introduzca el mandato **CRYPTO/CHGFLDENC** y haga F4
2. Introduzca el Identificador de Campo a cambiar y pulse Intro
3. Se mostrará la configuración actual de la entrada de campo (valores de los parámetros)
4. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line
5. Pulse Intro una vez se hayan cambiado los parámetros.



Ejemplo de Pantalla del mandato CHGFLDENC - Página 1



```
                    Change Field Encryption Entry (CHGFLDENC)

Type choices, press Enter.

Auth. list for full value  . . .  CCFULL        Name, *NONE
Auth. list for masked value  . .  CCMASKED      Name, *NONE
Auth. list caching . . . . . . .  *YES          *YES, *NO
Not authorized fill value  . . .  *             Character value
Store values in external file  .  *YES          *YES, *NO
External file name . . . . . . .  *GEN          Name, *GEN
  Library  . . . . . . . . . . .    *DBLIB       Name, *DBLIB
External logical file  . . . . .  *GEN          Name, *GEN, *NONE
  Library  . . . . . . . . . . .    *DBLIB       Name, *DBLIB
Store hash for security check  .  *YES          *YES, *NO
Store last retrieved user/time    *YES          *YES, *NO
Index number alignment . . . . .  *LEFT         *LEFT, *RIGHT
Index number padding character    ' '           Character value
Last index number storage  . . .  *FLDREG       *FLDREG, *PF
Use triggers to auto encrypt . .  *YES          *YES, *NO
Trigger name for inserts . . . .  *GEN
_____________________________
  Library  . . . . . . . . . . .    *DBLIB       Name, *DBLIB
Trigger name for updates . . . .  *GEN
_____________________________
  Library  . . . . . . . . . . .    *DBLIB       Name, *DBLIB
Trigger name for deletes . . . .  *GEN
_____________________________
  Library  . . . . . . . . . . .    *DBLIB       Name, *DBLIB
Trigger exit program type  . . .  *SRVPGM       *NONE, *PGM, *SRVPGM
Trigger exit program . . . . . .  SRV001        Name
  Library  . . . . . . . . . . .    OELIB        Name, *LIBL
Trigger exit *SRVPGM procedure .  EncExitProc
Use DB2 field procedure  . . . .  *NO           *YES, *NO
Field procedure return value . .  *FULL         *FULL, *AUTH
```

Ejemplo de Pantalla del mandato CHGFLDENC - Página 2

Nota: Para ver que significan estos parámetros, vea el apartado b) sobre el mandato ADDFLDENC.

Nota: El manato CHGFLDENC tan sólo cambia la configuración de una entrada de campo en el Registro de Encriptación de Campos. No dará lugar a ninguna acción sobre el campo del archivo de la base de datos.

d) Cambiar Máscara del Campo (CHGFLDMSK)

El mandato **CHGFLDSMSK** permite a los usuarios autorizados cambiar el carácter de enmascaramiento de una entrada de campo en el Registro de Encriptación de Campos.

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 Field Enc.Registry” (Mantener Registro de Encriptación de Claves) establecida en *YES

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL002, lista de validación *VLDL, el cual contiene el Registro de Encriptación de Campos.

Realice los siguientes pasos para **cambiar la máscara de una entrada de campo en el Registro de Encriptación de Campos:**

1. Introduzca el mandato **CRYPTO/CHGFLDMSK** y haga F4
2. Introduzca el Identificador de Campo al que se va a cambiar la máscara y pulse Intro
3. Se mostrará la máscara actual
4. Introduzca la nueva máscara y pulse Intro

```
                    Change Field Mask (CHGFLDMSK)

Type choices, press Enter.

Field identifier . . . . . .  CREDITCARD
Masking option . . . . . .  .  *OPTION1      *OPTION1, *OPTION2
Field mask . . . . . .  . . .  '************9999'
```

Ejemplo de Pantalla del mandato CHGFLDMSK - Página 2

Descripción de los campos del mandato CHGFLDMSK

Field identifier	Indicar el Identificador de Campo del que queremos cambiar la máscara.
Masking option	Indicar la opción de máscara a utilizar para el campo el cuándo se solicita el valor de enmascaramiento en una operación de desencriptación. *NONE – No ser realice el enmascaramiento. *OPTION1 – Ciertas posiciones dentro del valor del campo pueden ser mostradas o enmascaradas. *OPTION2 – Sólo un número especificado de dígitos o caracteres se muestran en el lado izquierdo o derecho del campo.
Field mask	Indicar la máscara a aplicar al valor de campo cuando sea desencriptado con las APIs de enmascaramiento de Crypto Complete. - Especifique el número 9 en una posición para que se muestre el valor subyacente para esa posición.

	- Especifique cualquier otro carácter (incluso espacios) o número en una posición para que enmascare el valor subyacente en esa posición. Ejemplo 1: Si se especifica una máscara como '**********9999' para un número de tarjeta de crédito, entonces el número de tarjeta de crédito se vería como '**********1234' a modo de ejemplo. Ejemplo 2: Si la máscara especificada fuera '##99##999' para un número de cuenta bancaria, entonces un ejemplo del número de cuenta enmascarado que se vería sería '##76##541'.
Char / Digits to show on left	Indicar el número de caracteres o dígitos a mostrar en el lado izquierdo del valor del campo. Válido para la opción *OPTION2 de enmascaramiento. Para un campo de caracteres, los caracteres en blanco al inicio serán ignorados al realizar el enmascaramiento. Para campos decimales, los ceros al inicio serán ignorados.
Char / Digits to show on right	Indicar el número de caracteres o dígitos a mostrar en el lazo derecho del valor del campo. Válido para la opción *OPTION2 de enmascaramiento. Para un campo de caracteres, los caracteres en blanco al inicio serán ignorados al realizar el enmascaramiento.
Masking value	El valor que se utilizará para realizar el enmascaramiento del carácter o número. Válido para la opción *OPTION2 de enmascaramiento. Si está utilizando los DB2 Field Procedures para enmascarar un campo numérico, el valor de enmascaramiento tiene que ser un número entre 0 y 9. Si no está utilizando los DB2 Field Procedures, el valor de enmascaramiento, tanto para un campo de caracteres o un campo numérico, puede ser un carácter o número.

Nota: Más información sobre las APIs de enmascaramiento de Crypto Complete en la Guía del Programador.

e) Cambiar Listas de Autorización del Campo (CHGFLDAUTL)

El mandato **CHGFLDAUTL** permite a los usuarios autorizados cambiar la configuración de las Listas de Autorización de una entrada de campo en el Registro de Encriptación de Campos.

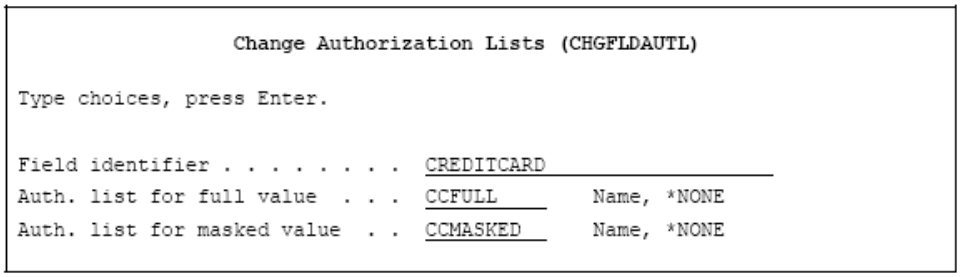
Los siguientes usuarios pueden utilizar este mandato:

- 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 Field Enc.Registry" (Mantener Registro de Encriptación de Claves) establecida en *YES

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL002, lista de validación *VLDL, el cual contiene el Registro de Encriptación de Campos.

Realice los siguientes pasos para **cambiar las Listas de Autorización de una entrada de campo en el Registro de Encriptación de Campos:**

1. Introduzca el mandato **CRYPTO/CHGFLDAUTL** y haga F4
2. Introduzca el Identificador de Campo y pulse Intro
3. Se mostrarán las listas de autorización del campo actuales
4. Especifique el nuevo nombre de las listas de autorización y pulse Intro



Ejemplo de Pantalla del mandato CHGFLDAUTL - Página 2

Descripción de los campos del mandato CHGFLDAUTL

Field identifier	Indicar el Identificador de campo del cual queremos modificar las listas de autorización.
Auth. list for full value	Indicar la Lista de Autorización del sistema IBMi que deben utilizar las APIs de desencriptación para comprobar los permisos de usuario sobre los valores completos desencriptados. Especifique *NONE para no usar una Lista de Autorización. Ver nota adicional(*)
Auth. list for masked value	Indicar la Lista de Autorización del sistema IBMi que deben utilizar las APIs de desencriptación para comprobar los permisos de usuario sobre los valores enmascarados desencriptados. Especifique *NONE para no usar una Lista de Autorización. Ver nota adicional(*)

(*)Nota: Las Listas de Autorización se crean con el mandato CRTAUTL del sistema i5/OS. Los usuarios o grupos de usuarios que necesitan tener acceso a los valores desencriptados o enmascarados necesitan tener como mínimo autorización *USE a la Lista de Autorización. Además Los usuarios o grupos de usuarios que necesitan tener acceso a los valores desencriptados o enmascarados necesitan tener al menos autorización *USE al objeto Almacén de Claves el cual contiene la Clave de Desencriptación.

f) Copiar Entrada de Encriptación de Campo (CPYFLDENC)

El mandato **CPYFLDENC** permite a los usuarios autorizados copiar las entradas del Registro de Encriptación de Campos.

Este mandato es especialmente útil para replicar entradas cuando está utilizando diferentes entornos (bibliotecas de datos) para controlar que Registro de Encriptación de Datos está utilizando sus aplicaciones.

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 Field Enc.Registry” (Mantener Registro de Encriptación de Claves) establecida en *YES

Este mandato requiere que el usuario tenga autorización *USE al Registro de Encriptación de Datos (Origen)(objeto CRVL002, lista de validación *VLDL) y autorización *CHANGE sobre el Registro de Encriptación de Datos (Destino)(objeto CRVL002, lista de validación *VLDL).

Realice los siguientes pasos para **copiar una entrada de la Encriptación de Campos:**

1. Introduzca el mandato **CRYPTO/CPYFLDENC** y haga F4
2. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line
3. Pulse Intro una vez se hayan cambiado los parámetros

```
                    Copy Field Encryption Entry (CPYFLDENC)

Type choices, press Enter.

From field registry library  . .  CRDATA1      Name
From field identifier  . . . . .  CREDITCARD
To field registry library  . . .  CRDATA2      Name, *FRMLIB
To field identifier  . . . . . .  *FRMFLDID
To field status  . . . . . . . .  *SAME        *SAME, *INACTIVE
Replace field id . . . . . . . .  *NO          *NO, *YES
Redirect key store library . . .  *NO          *NO, *YES
Key store library  . . . . . . .  *FLDREGLIB   Name, *FLDREGLIB
Redirect file library  . . . . .  *YES         *NO, *YES
File library . . . . . . . . . .  *FLDREGLIB   Name, *FLDREGLIB
```

Ejemplo de Pantalla del mandato CPYFLDENC

Descripción de los campos del mandato CPYFLDENC

From field registry library	Indicar la biblioteca que contiene el Registro de Encriptación de Campos (CRVL002) del cual queremos copiar una entrada de campo.
From field identifier	Indicar el nombre de la entrada de campo a copiar.
To field registry library	Indicar la biblioteca que contiene el Registro de Encriptación de Campos (CRVL002) al cual queremos copiar una entrada de campo. **Nota:** Los nombres de las bibliotecas (del archivo de la base de datos, del archivo externo y de los Triggers) en la nueva entrada de campo serán automáticamente modificados por la biblioteca especificada en este parámetro.
To Field Identifier	Indicar el nombre de la entrada de campo a crear en el registro de campos de destino. Utilice el valor *FRMFLDID para conservar el mismo nombre que figura en el campo “From field identifier”.
To field status	Indicar el estado a utilizar en el identificador de campo “To”. Los valores válidos son: *SAME – El estado en el campo “To” será el mismo que en el campo

	"From". *INACTIVE – El estado en el campo "To" se establecerá en *Inactive.
Replace field id	Indicar si cualquier identificador de campo existente (con el mismo nombre) debería ser reemplazado. La entrada "to" no puede ser reemplazada si su estado es *ACTIVE o *PROCESS.
Redirect key store library	Indicar si los nombres de las bibliotecas de los Almacenes de Claves de las nuevas entradas de campos deben cambiarse automáticamente por el nombre especificado en el parámetro "Key store library".
Key store library	Indicar el nombre de la biblioteca que contiene el almacén de claves a utilizar por la nueva entrada de campo en el registro, si se especificó *YES en el parámetro "Redirect key store library".
Redirect file library	Indicar si los nombres de la biblioteca del fichero a utilizar en la nueva entrada de campo del registro deberían cambiarse durante el proceso de copia. *YES - Especifique la biblioteca en el parámetro "File library". Cambiará las bibliotecas para el archive de base de datos y los archivos físicos externos y lógicos, así como los programas de los triggers (si aplica).
File library	Indicar el nombre de la biblioteca que contiene los archivos a utilizar por la nueva entrada de campo del registro, si se especificó *YES en el parámetro "Redirect file library".

g) Visualizar Entrada de Encriptación de Campo (DSPFLDENC)

El mandato **DSPFLDENC** permite a los usuarios autorizados visualizar la configuración de la entrada de un campo en el Registro de Encriptación de Campos.

Este mandato requiere que el usuario tenga autorización *USE sobre el objeto CRVL002, lista de validación *VLDL, el cual contiene el Registro de Encriptación de Campos.

Realice los siguientes pasos para **visualizar la configuración de una entrada de campo en el Registro de Encriptación de Campos:**

1. Introduzca el mandato **CRYPTO/DSPFLDENC** y haga F4
2. Introduzca el Identificador de Campo que quiere ver y pulse Intro
3. Se mostrarán los actuales valores de los parámetros de configuración junto con el nombre de usuario y timestamp de la última vez que se añadió o modificó la entrada
4. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line

A continuación se muestran ejemplos de la pantalla y parámetros del mandato DSPFLDENC.

```
                  Display Field Encryption Entry (DSPFLDENC)

Type choices, press Enter.

Field identifier . . . . . .  CREDITCARD
Database field name  . . . . .  CCNO
Database file name . . . . . .  ORDERS
  Library  . . . . . . . . . .    OEDATA
Database field type  . . . . .  *CHAR
Database field length  . . . . .  16
Database field decimal pos . . .
Encryption key label . . . . . .  CREDITCARDKEY
Encryption key store name  . . .  OEKEYS
  Library  . . . . . . . . . .    KEYLIB
Decryption key label . . . . . .  CREDITCARDKEY
Decryption key store name  . . .  OEKEYS
  Library  . . . . . . . . . .    KEYLIB
Encryption algorithm . . . . . .  *AES256
Algorithm mode . . . . . .  *CBC
Initialization vector  . . . . .  CC_INIT_VECTOR
Field mask . . . . . .  '************9999'
```

Ejemplo de Pantalla del mandato DSPFLDENC - Página 1

```
                  Display Field Encryption Entry (DSPFLDENC)

Type choices, press Enter.

Auth. list for full value  . . .  CCFULL
Auth. list for masked value  . .  CCMASKED
Auth. list caching . . . . . .  *YES
Not authorized fill value  . . .  *
Store values in external file  .  *YES
External file name . . . . . .  CRXX00009
  Library  . . . . . . . . . .    OEDATA
External logical file  . . . . .  CRXX00009L
  Library  . . . . . . . . . .    OEDATA
Store hash for security check  .  *YES
Store last retrieved user/time .  *YES
Index number alignment . . . . .  *LEFT
Index number padding character    '*'
Last index number storage  . . .  *FLDREG
```

```
Use triggers to auto encrypt . .   *YES
Trigger name for inserts . . . .   ORDERS_CCNO_CryptoInsert
  Library  . . . . . . . . . . .     OEDATA
Trigger name for updates . . . .   ORDERS_CCNO_CryptoUpdate
  Library  . . . . . . . . . . .     OEDATA
Trigger name for deletes . . . .   ORDERS_CCNO_CryptoDelete
  Library  . . . . . . . . . . .     OEDATA
Trigger exit program type  . . .   *SRVPGM
Trigger exit program . . . . . .   SRV001
  Library  . . . . . . . . . . .     OELIB
Trigger exit *SRVPGM procedure .   EncExitProc
Use DB2 field procedure  . . . .   *NO
Field procedure return value . .   *FULL
Last modified by user  . . . . .   MARY
Last modified date/time  . . . .   '2009-07-18-15.09.42.692000'
```

Ejemplo de Pantalla del mandato DSPFLDENC - Página 2

Nota: Para ver que significan estos parámetros, vea el apartado b) sobre el mandato ADDFLDENC.

h) Activar Encriptación de Campo (ACTFLDENC)

El mandato **ACTFLDENC** permite a los usuarios autorizados activar una entrada de campo del Registro de Encriptación de Campos.

Este mandato producirá un bloqueo del archivo de la base de datos y realizará una **encriptación masiva** de los valores actuales de los campos.

Ejecute este mandato sólo cuando NO haya aplicaciones utilizando el archivo de la base de datos.

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 Field Enc.Registry” (Mantener Registro de Encriptación de Claves) establecida en *YES

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL002, lista de validación *VLDL, el cual contiene el Registro de Encriptación de Campos.

Este mandato sólo puede utilizarse en las entradas de campo cuyo estado es *INACTIVE.

Se recomienda que el mandato se ejecute en modo BATCH.

INSTRUCCIONES ESPECIALES

Antes de utilizar el mandato ACTFLDENC para encriptar los datos de producción, realice lo siguientes pasos:

1. Asegúrese de tener autorización *ALL al archivo de la base de datos que contiene el campo que va a encriptar.
2. Si NO se utilizan Triggers SQL o DB2 Field Procedures para auto-encriptar los valores de los campos:

   Deben modificarse todos los programas que mantienen (añadir / cambiar / borrar) registros en el archivo de la base de datos para que llamen a las **APIs de encriptación** de Crypto Complete.

   Si está almacenando los valores encriptados de los campos en un archivo externo, lea más sobre las APIs (InsEncFld, UpdEncFld, DltEncFld) en la Guía del Programador,

   Si está almacenando los valores de campo encriptados en el campo existente, lea más sobre la API EncFld.
3. Si NO se utilizan los DB2 Field Procedure para auto-desencriptar los valores de los campos:

   Deben modificarse todos aquellos programas que necesitan acceder a los valores de campo desencriptados para que llamen a las **APIS de desencriptación** de Crypto Complete.

   Si está almacenando los valores encriptados de los campos en archivo externo, lea más sobre las APIs (GetEncFld, GetEncFldMask and GetEncFldAuth) en la Guía del Programador.

   Si está almacenando los valores encriptados en el campo existente, lea más sobre las APIs DecFld, DecFldMask y DecFldAuth.
4. Debería haber probado en un ENTORNO DE PRUEBAS, el mandato ACTFLDENC, probado las llamadas a APIs necesarias para encriptar y desencriptar y probado el funcionamiento de sus aplicaciones profundamente con los valores encriptados.
5. Ninguna aplicación o usuario debería estar utilizando en el momento de realizar la encriptación masiva el archivo de la base de datos que contiene los campos que se van a encriptar.
6. El mandato ACTFLDENC realizará una encriptación masiva de los valores de los campos actuales. Debería contar con un espacio de tiempo de inactividad suficiente de sus aplicaciones para ejecutar el mandato ACTFLDENC.

   Los tiempos de ejecución varían según la velocidad del procesador de su sistema, el número de registros en su archivo de base de datos, y otra actividad del sistema. Para poder estimar el tiempo de ejecución del mandato ACTFLDENC, debería ejecutar el mandato ACTFLDENC sobre algunos datos de prueba.
7. Compruebe la configuración de las entradas de campo con el mandato DSPFLDENC. Especialmente compruebe que el Nombre del archivo de la base de datos, el Nombre del Campo y el Tipo y Longitud del campo son correctas.
8. Vuelva a comprobar el paso 7.

Importante: Si activa un campo que utiliza un DB2 Field Procedure, y si ya existen otros DB2 Field Procedure en el archivo, debería tener como mínimo autorización *USE a las Listas de Autorización 'FULL' asignadas a esos otros campos, así como autorización *USE a los Almacenes de Claves que contienen las claves de encriptación y desencriptación utilizadas por esos campos.

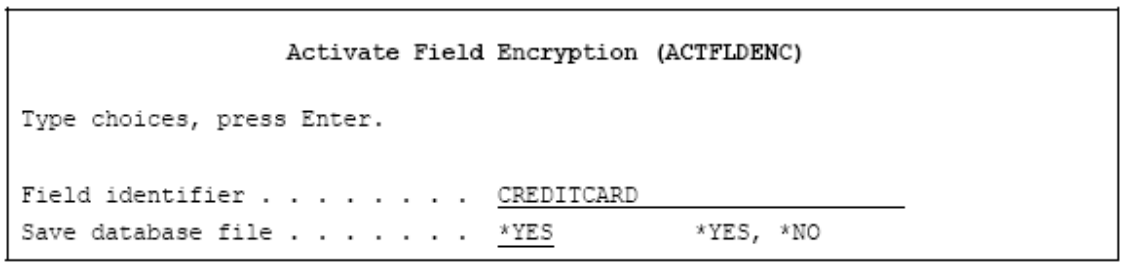
Esto se debe a que la sentencia ALTER TABLE de IBM (utilizada en el proceso de activación) ejecuta los procesos de encriptación y desencriptación para todos los campos que tienen un DB2 Field Procedure. **NO TENER LAS AUTORIZACIONES ADECUADAS CAUSARÁ LA PÉRDIDA DE DATOS.**

Recomendaciones sobre el mandato ACTFLDENC

- Ejecute el mandato en batch con el mandato SBMJOB
- Especifique *YES en el parámetro "Save Database File" para hacer una copia del archivo de la base de datos en un Save File, antes de la activación del proceso. Está opción es importante en caso de emergencia.
- Asegúrese de disponer del espacio suficiente para alojar esas copias.

Realice los siguientes pasos para **activar una entrada de campo en el Registro de Encriptación de Campos:**

1. Introduzca el mandato **CRYPTO/ACTFLDENC** y haga F4
2. Introduzca el Identificador del Campo a activar y pulse Intro



Ejemplo de Pantalla del mandato ACTFLDENC

Paso a paso del proceso ejecutado por el mandato ACTFLDENC

1. Produce un bloqueo exclusivo (*EXCL) sobre el archivo de la base de datos que contiene el campo a encriptar.
2. Si se utiliza un archivo externo para almacenar los valores encriptados, se creará un archivo de base de datos externo separado con el nombre y biblioteca especificado en la entrada de campo.
3. Opcional: Crea un Backup del archivo de la base de datos (que contiene el campo a encriptar) en un archivo de Salvado llamado BACKUPxxxxx, donde xxxxx es un número secuencial de 1 a 99999.
4. Realiza una encriptación masiva de los valores de los campos actuales del archivo de la base de datos. Si se especificó un DB2 Field Procedure para ese campo, entonces se añadirá al campo en ese momento.
5. Si se han especificado Triggers SQL para encriptar automáticamente los valores de los campos, entonces esos Triggers se crearán sobre el archivo.
6. Se desactivará el bloqueo exclusivo sobre el archivo de la base de datos que contiene el campo encriptado.
7. El estado de la entrada de campo en el Registro de Encriptación de Campos estará en *ACTIVE.

Notas sobre el ACTFLDENC:

- Una vez finalizado el mandato ACTFLDENC

  Una vez haya comprobado que sus aplicaciones están funcionando adecuadamente con los valores encriptados, puede eliminar el SAVE FILE creado en el paso 3 anterior, el cual contiene un Backup del archivo de la base de datos.

- Si se especificó un archivo externo para almacenar valores encriptados
  - El archivo externo se creará con las mismas autorizaciones que el archivo de la base de datos que contiene los campos a encriptar. Tras la finalización del mandato ACTFLDENC, puede ajustar las autorizaciones del archivo externo, si fuera necesario, mediante el mandato EDTOBJAUT.
  - El archivo externo se crea con el parámetro SIZE(*NOMAX), lo que permite al archivo externo contener un número ilimitado de registros. Una vez finalizado el mandato ACTFLDENC, puede ajustar el límite SIZE del archivo externo (si fuera necesario) mediante el mandato CHGPF.
  - Cualquier usuario que necesite encriptar los valores de campo tendrá que tener autorización *CHANGE sobre el objeto CRVL002 *VLDL , el cual contiene la información del registro de encriptación de campos.
  - Cualquier usuario que necesite desencriptar los valores de campo tendrá que tener al menos autorización *USE sobre el objeto CRVL002 *VLDL , el cual contiene el registro de encriptación de campos.

i) Cambiar Clave de Encriptación de Campo (CHGFLDKEY)

El mandato **CHGFLDKEY** permite a los usuarios autorizados cambiar (rotar) las claves utilizadas para encriptar y desencriptar datos de una entrada de campo del Registro de Encriptación de Campos.

Se pueden rotar hasta 99.999 claves para una misma entrada de campo.

Este mandato puede utilizarse cuando las entradas de campo en el Registro de encriptación de campos están en estado *INACTIVE. También con entradas de campo con estado *ACTIVE, siempre que los valores encriptados se estén almacenando en archivos externos para estas entradas de campo.

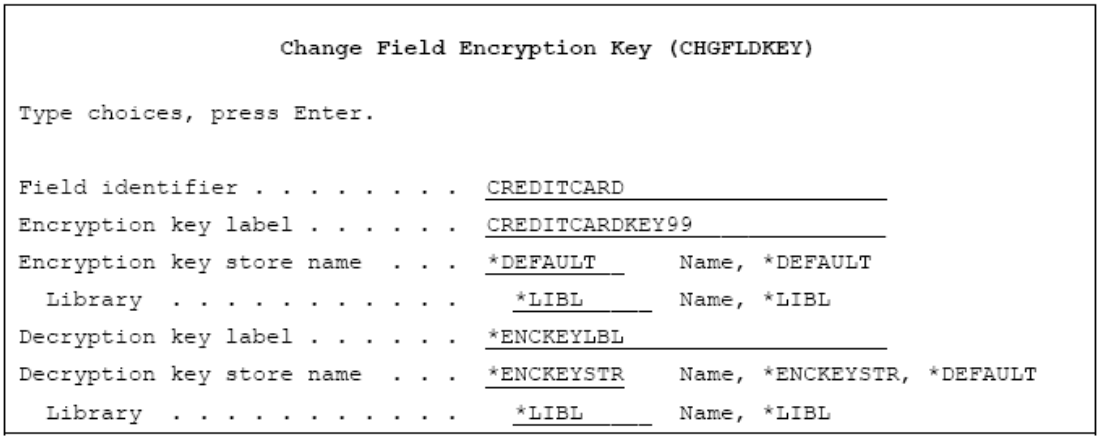
Los siguientes usuarios pueden utilizar este mandato:

- 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 Field Enc.Registry” (Mantener Registro de Encriptación de Claves) establecida en *YES

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL002, lista de validación *VLDL, el cual contiene el Registro de Encriptación de Campos.

Realice los siguientes pasos para **cambiar (rotar) las claves de una entrada de campo** en el Registro de Encriptación de Campos:

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



Ejemplo de Pantalla del mandato CHGFLDKEY

Descripción de los campos del mandato CHGFLDKEY

Field identifier	Indicar el Identificador único de la entrada de campo en el registro de encriptación de campos.
Encryption key label	Indicar la Etiqueta de la Clave DEK que se va a utilizar para encriptar los valores del campo
Encryption key store name - Library	Indicar el nombre y biblioteca del Almacén de Claves que contiene la Etiqueta de la Clave DEK de encriptación. Especifique *DEFAULT para utilizar el nombre de Almacén de Claves especificado en la Política de Claves.
Decryption key label	Indicar la Etiqueta de la Clave DEK a utilizar para desencriptar los valores de los campos. Especifique *ENCKEYLBL para utilizar el mismo valor que especificó para Encryption key label. **Atención:** Si especifica una Etiqueta de la Clave DEK diferente que la especificada para la encriptación, entonces la clave de desencriptación debería contener el mismo valor de clave que la clave de encriptación.
Nota ATT: Para ello, realice una copia de la clave DEK utilizada para encriptar con el mandato CPYSYMKEY asignándole el mismo almacén de claves (cambiar nombre Etiqueta de la Clave DEK) u otro almacén de claves (Podría mantener mismo nombre de Etiqueta de la Clave DEK). De esta manera, el valor de la clave que se usa para encriptar y desencriptar es el mismo.	
Decryption key store name - Library	Indicar el nombre y biblioteca del Almacén de Claves que contiene la Etiqueta de la Clave DEK de Desencriptación. Especifique *DEFAULT para utilizar el nombre del Almacén de Claves por defecto especificado en la Política de Claves. Especifique *ENCKEYSTR para utilizar el mismo valor que se introdujo para el nombre del Almacén de Claves de Encriptación.

i -1) Si almacena los valores de campo encriptados en un archivo externo

Cuando se utiliza un archivo externo para almacenar los valores encriptados de los campos, se almacena un Identificador de Clave numérico (Key id number) por cada valor del campo encriptado. Este id de Clave, es una referencia a la Etiqueta de la Clave DEK utilizada para encriptar los datos, así como la Etiqueta de la Clave DEK necesaria para desencriptar los datos.

Cuando se modifican las Etiquetas de Claves con el mandato CHGFLDKEY, se almacena un nuevo Identificador de clave numérico (Key id number), que hace referencia a las nuevas Etiquetas de Clave para cualquier nuevo valor del campo encriptado.

El id de Clave, permanecerá igual para los valores de campo encriptados ya existentes, lo que permite a Crypto Complete desencriptar esos valores de campo utilizando las Etiquetas de Claves anteriores. Está técnica permite rotar las claves con frecuencia, sin tener que reencriptar los valores de todos los campos existentes.

Consejo: El mandato TRNFLDKEY (Translate Field Keys) puede utilizarse para traducir (reencriptar) cualquier valor de campo existente a la clave más actual. **El mandato TRNFLDKEY solo debe ejecutarse después de realizar el mandato CHGFLDKEY.**

i-2) Si almacena los valores de campo encriptados en el campo existente de la base de datos

El mandato CHGFLDKEY NO puede utilizarse para una entrada de campo *ACTIVE que no almacene los valores encriptados del campo en un archivo externo. Para cambiar la clave para este tipo de entrada de campos, puede utilizar el mandato TRNFLDKEYI.

J) Traducir Claves de Encriptación de Campo - Almacenaje Externo (TRNFLDKEY)

El mandato **TRNFLDKEY** permite a los usuarios autorizados traducir (reencriptar) cualesquiera valores de un campo, que hubieran sido encriptados con claves anteriores, con la nueva clave para el Identificador de Campo especificado.

Este mandato puede utilizarse para entradas de campo con estado *ACTIVE siempre que almacenen el valor de campo encriptado en archivos externos.

El mandato TRNFLDKEY encontrará cualquier registro en el archivo externo (donde se encuentran almacenados los valores encriptados) que estén encriptados con las claves anteriores.

Por cada registro encontrado, TRNFLDKEY desencripta el valor con la antigua clave y lo vuelve a encriptar con la clave nueva (actual).

Nota: El mandato TRNFLDKEY SOLO DEBERIA EJECUTARSE si se ha ejecutado anteriormente el mandato CHGFLDKEY para ese campo.

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 Field Enc.Registry” (Mantener Registro de Encriptación de Claves) establecida en *YES

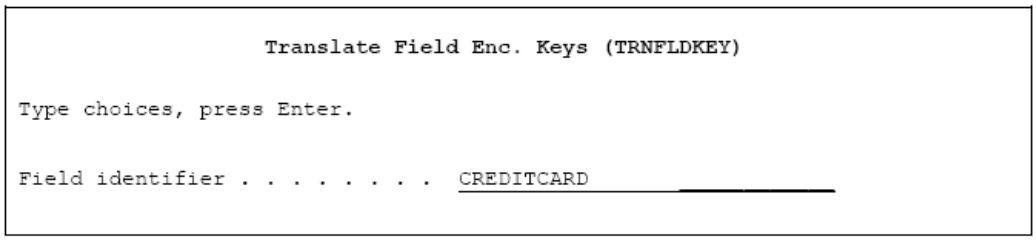
Este mandato requiere que usted tenga las siguientes autorizaciones de objeto:

Autorización	Objeto	Descripción
*USE	CRVLOO2 *VLDL (Lista de Validación)	Contiene el Registro de Encriptación de Campos.
*READ	Archivo de base de datos	Especificado en la entrada de campo del Registro.
*CHANGE	Archivo externo	Archivo de almacenaje externo que contiene valores encriptados
*USE	Almacenes de Claves	Contienen cualquier clave activa y las nuevas claves de encriptación/desencriptación

Se recomienda ejecutar este mandato en **batch** mediante el mandato SBMJOB.

Realice los siguientes pasos para **traducir (reencriptar) las claves de una entrada de campo** en el Registro de Encriptación de Campos, si el valor encriptado se almacena en archivo externo:

1. Introduzca el mandato **CRYPTO/TRNFLDKEY** y haga F4.
2. Especifique el identificador de campo y pulse Intro



Ejemplo de Pantalla del mandato TRNFLDKEY

Notas: - Se puede ejecutar el mandato TRNFLDKEY mientras los usuarios y aplicaciones están ACTIVAS en el sistema.
- El tiempo de ejecución del mandato TRNFLDKEY depende del número de registros que debe traducir (reencriptar) a la nueva clave.

k) Traducir Claves de Encriptación de Campo – Almacenaje Interno (TRNFLDKEYI)

El mandato **TRNFLDKEYI** permite a los usuarios autorizados traducir (reencriptar) cualesquiera valores del campo, que hubieran sido encriptados con claves anteriores, con la nueva clave para el Identificador de Campo especificado.

Este mandato puede utilizarse con entradas de campo *ACTIVE que almacenan los valores encriptados dentro del campo existente de la base de datos, y que no utilicen los DB2 Field Procedure.

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 Field Enc.Registry” (Mantener Registro de Encriptación de Claves) establecida en *YES

Este mandato requiere que el usuario tenga las siguientes autorizaciones de objeto:

Autorización	Objeto	Descripción
*CHANGE	CRVLOO2 *VLDL (Lista de Validación)	Contiene el Registro de Encriptación de Campos.
*CHANGE	Archivo de base de datos	Especificado en la entrada de campo del Registro.
*USE	Almacenes de Claves	Contienen cualquier clave activa y las nuevas claves de encriptación/desencriptación

Precaución: Ningún usuario o aplicación debe estar utilizando el archivo en el momento de ejecutar el mandato TRNFLDKEYI pues este intentará obtener un bloqueo exclusivo sobre el archivo.

Importante: La ejecución del mandato TRNFLDKEYI dará lugar a una reencriptación masiva de los valores actuales del campo. Debería contar con un espacio de tiempo de inactividad suficiente de sus aplicaciones para ejecutar el mandato TRNFLDKEYI. Los tiempos de ejecución varían según la velocidad del procesador de su sistema, el número de registros en su archivo de base de datos, y otra actividad del sistema. Para poder estimar el tiempo de ejecución del mandato TRNFLDKEYI, debería ejecutar el mandato TRNFLDKEYI sobre algunos datos de prueba.

Se recomienda ejecutar este mandato en **batch** mediante el mandato SBMJOB.

Realice los siguientes pasos para **traducir (reencriptar) la clave de una entrada de campo** en el Registro de Encriptación de Campos, si los valores encriptados se almacenan el campo existente y no se utilizan DB2 Field Procedure:

1. Introduzca el mandato **CRYPTO/TRNFLDKEYI** y haga F4.
2. Especifique el identificador de campo
3. Especifique las nuevas Etiquetas de Claves de encriptación y desencriptación
4. Especifique los Almacenes de Claves y pulse Intro.

```
                Translate Field Encryption Key (TRNFLDKEYI)

Type choices, press Enter.

Field identifier . . . . . .  CREDITCARD
Encryption key label . . . . .  CREDITCARDKEY99
Encryption key store name  . . .  *DEFAULT      Name, *DEFAULT
  Library  . . . . . .  *LIBL      Name, *LIBL
Decryption key label . . . . .  *ENCKEYLBL
Decryption key store name  . . .  *ENCKEYSTR    Name, *ENCKEYSTR, *DEFAULT
  Library  . . . . . .  *LIBL      Name, *LIBL
Save database file . . . . . .  *YES           *YES, *NO
```

Ejemplo de Pantalla del mandato TRNFLDKEYI

l) Traducir Claves de Encriptación de Campo – Field Procedure (TRNFLDKEYF)

El mandato **TRNFLDKEYF** permite a los usuarios autorizados traducir (reencriptar) cualesquiera valores del campo, que hubieran sido encriptados con claves anteriores, con la nueva clave para el Identificador de Campo especificado.

Este mandato puede utilizarse con entradas de campo *ACTIVE que utilicen los DB2 Field Procedure para la encriptación y desencriptación automática.

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 Field Enc.Registry” (Mantener Registro de Encriptación de Claves) establecida en *YES

Este mandato requiere que el usuario tenga las siguientes autorizaciones de objeto:

Autorización	Objeto	Descripción
*CHANGE	CRVLOO2 *VLDL (Lista de Validación)	Contiene el Registro de Encriptación de Campos.
*CHANGE	Archivo de base de datos	Especificado en la entrada de campo del Registro.
*USE	Almacenes de Claves	Contienen cualquier clave activa y las nuevas claves de encriptación/desencriptación

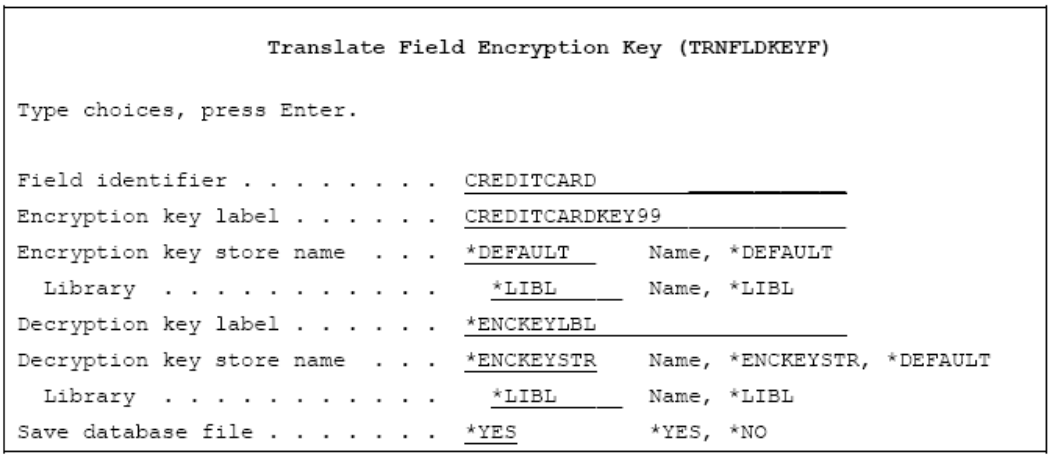
Precaución: Ningún usuario o aplicación debe estar utilizando el archivo en el momento de ejecutar el mandato TRNFLDKEYF pues este intentará obtener un bloqueo exclusivo sobre el archivo.

Importante: La ejecución del mandato TRNFLDKEYF dará lugar a una reencriptación masiva de los valores actuales del campo. Debería contar con un espacio de tiempo de inactividad suficiente de sus aplicaciones para ejecutar el mandato TRNFLDKEYF. Los tiempos de ejecución varían según la velocidad del procesador de su sistema, el número de registros en su archivo de base de datos, y otra actividad del sistema. Para poder estimar el tiempo de ejecución del mandato TRNFLDKEYF, debería ejecutar el mandato TRNFLDKEYF sobre algunos datos de prueba.

Se recomienda ejecutar este mandato en **batch** mediante el mandato SBMJOB.

Realice los siguientes pasos para **traducir (reencriptar) la clave de una entrada de campo** en el Registro de Encriptación de Campos, si utiliza los DB2 Field Procedures.

1. Introduzca el mandato **CRYPTO/TRNFLDKEYF** y haga F4.
2. Especifique el Identificador de Campo.
3. Especifique las nuevas Etiquetas de Claves de encriptación y desencriptación.
4. Especifique los Almacenes de Claves y pulse Intro.



Ejemplo de Pantalla del mandato TRNFLDKEYF

Paso a paso del proceso ejecutado por el mandato TRNFLDKEYF

1. Produce un bloqueo exclusivo (*EXCL) sobre el archivo de la base de datos que contiene el campo a encriptar.
2. Opcional: Crea un Backup del archivo de la base de datos (que contiene el campo a encriptar) en un archivo de salvado llamado BACKUPxxxxx, donde xxxxx es un número secuencial de 1 a 99999.
3. Cambia el estado del campo a *PROCESS.
4. Lee todos los registros en el archivo y reencripta los valores de campo con la nueva clave introducida.
5. Cambia las claves *CURRENT en el registro de encriptación de campos por las nuevas claves introducidas en el mandato.
6. Se elimina el bloqueo exclusivo sobre el archivo de la base de datos que contiene e campo encriptado.
7. El estado de la entrada de campo en el Registro de Encriptación de Campos se cambiará a *ACTIVE.

m) Eliminar Triggers del Campo (RMVFLDTRG)

El mandato **RMVFLDTRG** permite a los usuarios autorizados eliminar los Triggers SQL creados con Crypto Complete en el archivo de la base de datos para el Ientificador de Campo especificado, cuando se activó con ACTFLDENC.

Este mandato es útil para eliminar temporalmente los Triggers cuando se necesita realizar operaciones de mantenimiento sobre el archivo de la base de datos, como añadir un campo nuevo al archivo a través de una herramienta de gestión de cambios.

El mandato RMVFLDTRG solo puede utilizarse para las entradas de campo *ACTIVE, que se configuraron en el Registro de Encriptación de Campos para que utilizasen Triggers SQL.

Al ejecutar este mandato, no debería haber aplicaciones o usuarios utilizando el archivo de la base de datos, porque podría dar lugar a la adición o actualización de valores del campo en el archivo sin encriptar.

El mandato RMVFLDTRG solo elimina los Triggers SQL del archivo de la base de datos. Todos los campos que existieran antes de ejecutar el mandato RMVFLDTRG permanecerán encriptados. La entrada de campo mantendrá el estado de *ACTIVE en el Registro de Encriptación de Campos.

> **Precaución:** Si se eliminan los Triggers SQL del archivo, cualquier adición o actualización de valores del cmapo NO SERA ENCRIPTADA automáticamente por Crypto Complete. Solo debe usarse este mandato para eliminar temporalmente los triggers.

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 Field Enc.Registry” (Mantener Registro de Encriptación de Claves) establecida en *YES

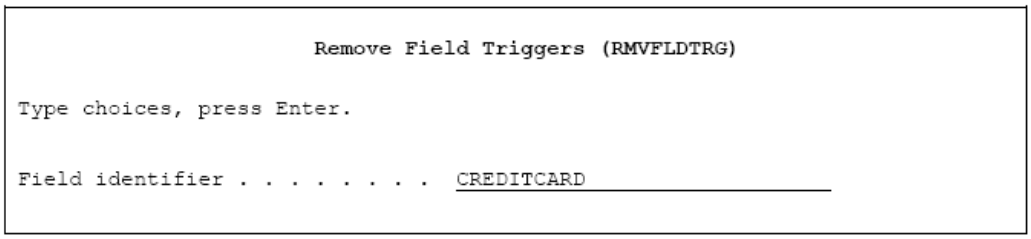
Este mandato requiere que el usuario tenga las siguientes autorizaciones de objeto:

Autorización	Objeto	Descripción
*USE	CRVLOO2 *VLDL (Lista de Validación)	Contiene el Registro de Encriptación de Campos.
*CHANGE	Archivo de base de datos	Especificado en la entrada de campo del Registro.

Realice los siguientes pasos para **eliminar los Triggers de una entrada de campo** en el Registro de Encriptación de Campos:

1. Compruebe que no existe ningún bloqueo sobre el archivo de la base de datos antes de continuar.
2. Introduzca el mandato **CRYPTO/RMVFLDTRG** y haga F4.

3. Especifique el identificador de campo y pulse Intro.



Ejemplo de Pantalla del mandato RMVFLDTRG

Nota: Utilice el mandato ADDFLDTRG para recrear los Triggers SQL en el archivo de la base de datos.

n) Añadir Triggers a un Campo (ADDFLDTRG)

El mandato **ADDFLDTRG** permite a los usuarios autorizados recrear cualquier Trigger SQL que haya sido eliminado con el mandato RMVFLDTRG.

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 Field Enc.Registry” (Mantener Registro de Encriptación de Claves) establecida en *YES

El mandato ADDFLDTRG sólo puede utilizarse con las entradas de campo *ACTIVE, que fueron configuradas inicialmente para utilizar Triggers SQL en el Registro de Encriptación de Campos.

Precaución: Este mandato ADDFLDTRG sólo debe utilizarse para recrear los Triggers SQL que fueron eliminados con el mandato RMVFLDTRG.

Realice los siguientes pasos para **recrear los Triggers de una entrada de campo** en el Registro de Encriptación de Campos:

1. Compruebe que no existe ningún bloqueo sobre el archivo de la base de datos antes de continuar.
2. Introduzca el mandato **CRYPTO/ADDFLDTRG** y haga F4.
3. Especifique el Identificador de Campo y pulse Intro.

```
                    Add Field Triggers (ADDFLDTRG)

Type choices, press Enter.

Field identifier . . . . . .  CREDITCARD
```

Ejemplo de Pantalla del mandato ADDFLDTRG

Notas: - El mandato ADDFLDTRG solo recrea los Triggers SQL del archivo de la base de datos. Todos los valores de campo, que existieran antes de la ejecución del mandato ADDFLDTRG, permanecerán como estén actualmente.
- La entrada de campo permanecerá en el estado *ACTIVE en el Registro de Encriptación de Campos.

o) Trabajar con Claves de Encriptación de Campo (WRKFLDKEY)

El mandato **WRKFLDKEY** permite a los usuarios autorizados ver la clave actual, así como la historia de las claves utilizadas para encriptar y desencriptar datos de una entrada de campo en el Registro de Encriptación de Campos.

Realice los siguientes pasos para **visualizar las claves de una entrada de campo** en el Registro de Encriptación de Campos.

1. Introduzca el mandato **CRYPTO/TWRKLDKEY** y haga F4.
2. Especifique el Identificador de Campo. y pulse Intro
3. Se mostrarán las claves para la entrada de campo

```
7/18/06              Work with Field Encryption Keys              MARY
1:57:19                                                           CRRM047     D2

Field identifier  . . . . . .  CREDITCARD

Key Id  Encryption Key Label            Key Store
    1   CREDITCARDKEY200601             KEYLIB/KEYSTORE
    2   CREDITCARDKEY200603             KEYLIB/KEYSTORE
    3   CREDITCARDKEY200606             KEYLIB/KEYSTORE
    4   CREDITCARDKEY200609             KEYLIB/KEYSTORE
    5   CREDITCARDKEY200701             KEYLIB/KEYSTORE
    6   CREDITCARDKEY200704             KEYLIB/KEYSTORE
    7   CREDITCARDKEY200707             KEYLIB/KEYSTORE         *CURRENT KEY




 F3=Exit    F5=Refresh    F11=View2    F12=Cancel
```

Ejemplo de Pantalla del mandato WRKFLDKEY

La clave mostrada con el comentario *CURRENT KEY es el id de Clave que se está utilizando actualmente para encriptar y desencriptar los valores de los campos.

Teclas de Función

Función	Descripción
F3	Salir de la pantalla WRKFLDKEY
F5	Refresca la lista de claves de la entrada de campo
F11	Muestra adicionalmente la descripción de la Etiqueta de la Clave DEK, el Almacén de Claves así como, el usuario y fecha del último cambio.

p) Desactivar Encriptación del Campo (DCTFLDENC)

El mandato **DCTFLDENC** permite a los usuarios autorizados desactivar una entrada de campo en el Registro de Encriptación de campos.

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 Field Enc.Registry” (Mantener Registro de Encriptación de Claves) establecida en *YES

El mandato solo puede utilizarse para entradas de campo que tengan el estado *ACTIVE. Se recomienda ejecutar este mandato en **batch.**

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL002, lista de validación *VLDL, el cual contiene el Registro de Encriptación de Campos.

 **Precaución:** Ningún usuario o aplicación debe estar utilizando el archivo en el momento de ejecutar el mandato DCTFLDENC pues bloqueará el archivo de la base de datos para llevar a cabo una desencriptación masiva de los valores actuales de los campos.

INSTRUCCIONES ESPECIALES

Antes de utilizar el mandato DCTFLDENC para desencriptar los datos de producción, realice lo siguientes pasos:

1. Asegúrese de tener autorización *ALL al archivo de la base de datos que contiene el campo que va a desencriptar.
2. Asegúrese de tener como mínimo autorización *USE sobre el Almacén de Claves que contiene las Claves de Encriptación (DEKs) que se utilizarán para desencriptar los datos.

   Puede utilizar el mandato WRKFLDKEY para saber que almacenes de claves y claves DEK se están utilizando para desencriptar los datos.

   Si usted es el propietario de una de las claves que creó, entonces debe establecer en *YES el parámetro “DEK Decrypt usage by owner” (se puede ver con DSPKEYPCY), para que pueda utilizarla.
3. Si no se utilizan Triggers SQL o DB2 Field Procedures para auto-encriptar los valores de los campos:

   Deben modificarse todos los programas que mantienen (añadir / cambiar / borrar) registros en el archivo de la base de datos para que NO llamen a las APIs de encriptación de Crypto Complete.
4. Si no se utilizan los DB2 Field Procedure para auto-desencriptar los valores de los campos:

   Deben modificarse todos aquellos programas que necesitan acceder a los valores de campo desencriptados para que NO llamen a las APIS de desencriptación de Crypto Complete.
5. Debería haber probado en un ENTORNO DE PRUEBAS, el mandato DCTFLDENC, y probado sus aplicaciones a fondo con los valores desencriptados.
6. Ninguna aplicación o usuario debería estar utilizando en este momento el archivo de la base de datos que contiene los campos que se van a desencriptar.
7. El mandato DCTFLDENC realizará una desencriptación masiva de los valores de los campos actuales. Debería contar con un espacio de tiempo de inactividad suficiente de sus aplicaciones para ejecutar el mandato DCTFLDENC.

   Los tiempos de ejecución varían según la velocidad del procesador de su sistema, el número de registros en su archivo de base de datos, y otra actividad del sistema. Para poder estimar el tiempo de ejecución del mandato DCTFLDENC, debería ejecutar el mandato DCTFLDENC sobre algunos datos de prueba.

Importante: Si desactiva un campo que utiliza un DB2 Field Procedure, y si ya existen otros DB2 Field Procedure en el archivo, debería tener al menos autorización *USE a las Listas de Autorización 'FULL' asignadas a esos otros campos, así como al menos autorización *USE a los Almacenes de Claves que contienen las claves de encriptación y desencriptación utilizadas por esos campos.

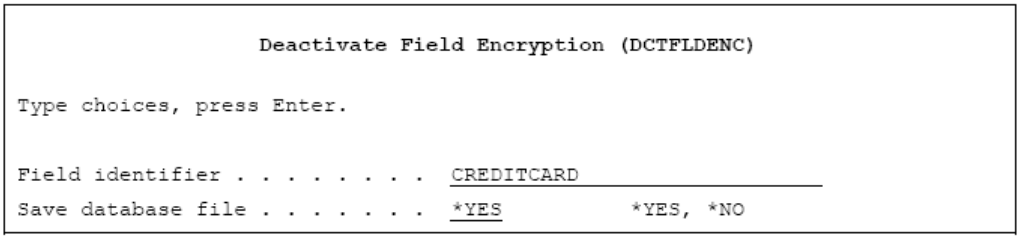
Esto se debe a que la sentencia ALTER TABLE de IBM (utilizada en el proceso de desactivación) ejecuta los procesos de encriptación y desencriptación para todos los campos que tienen un DB2 Field Procedure. **NO TENER LAS AUTORIZACIONES ADECUADAS CAUSARÁ LA PÉRDIDA DE DATOS.**

Recomendaciones sobre el mandato DCTFLDENC

- Ejecute el mandato en batch con el mandato SBMJOB
- Especifique *YES en el parámetro "Save Database File" para hacer una copia del archivo de la base de datos en un Save File, antes de la activación del proceso. Está opción es importante en caso de emergencia.
- Asegúrese de disponer del espacio suficiente para alojar esas copias.

Realice los siguientes pasos para **desactivar una entrada de campo en el Registro de Encriptación de Campos:**

3. Introduzca el mandato **CRYPTO/DCTFLDENC** y haga F4
4. Introduzca el Identificador del Campo a activar y pulse Intro



Ejemplo de Pantalla del mandato DCTFLDENC

Paso a paso del proceso ejecutado por el mandato DCTFLDENC

1. Produce un bloqueo exclusivo (*EXCL) sobre el archivo de la base de datos que contiene el campo a desencriptar.
2. Si se utiliza un archivo externo para almacenar los valores encriptados, se realizará un Backup del archivo externo en un Save File llamado BACKUPxxxxx, donde xxxxx es un número secuencial de 1 a 99999.

3. Opcional: Crea un Backup del archivo de la base de datos (que contiene el campo a desencriptar) en un Save File llamado BACKUPxxxxx, donde xxxxx es un número secuencial de 1 a 99999.
4. Realiza una desencriptación masiva de los valores de los campos actuales del archivo de la base de datos. Si se especificó un DB2 Field Procedure para ese campo, entonces se eliminará del campo en ese momento.
5. Si se han especificado Triggers SQL para encriptar automáticamente los valores de los campos, entonces esos Triggers SQL serán eliminados del archivo.
6. Si se empleó un archivo externo para almacenar los valores encriptados, el archivo externo será eliminado.
7. Se desactivará el bloqueo exclusivo sobre el archivo de la base de datos que contiene el campo desencriptado.
8. El estado de la entrada de campo en el Registro de Encriptación de Campos se cambiará a *INACTIVE.

Notas sobre el DCTFLDENC:

Una vez finalizado el mandato DCTFLDENC:

Una vez haya comprobado que sus aplicaciones están funcionando adecuadamente con los valores ya desencriptados, puede eliminar los archivos SAVE FILE creado en los pasos 2 y 3 anteriores, los cuales contienen los Backup del archivo externo y del archivo de datos.

q) Eliminar Entrada de Encriptación de Campo (RMVFLDENC)

El mandato **RMVFLDENC** permite a los usuarios autorizados eliminar una entrada de campo *INACTIVE del Registro de Encriptación de campos.

Los siguientes usuarios pueden utilizar este mandato:

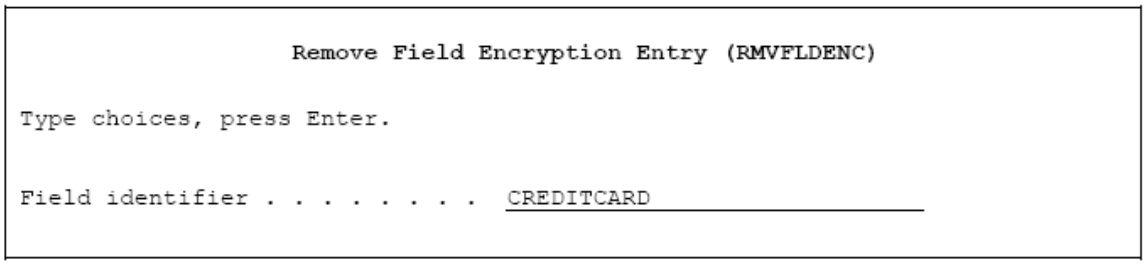
- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Perfil de usuario con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un Oficial de Claves que tenga la configuración de autorizaciones “Maintain Field Enc.Registry” (Mantener Registro de Encriptación de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

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL002, lista de validación *VLDL, el cual contiene el Registro de Encriptación de Campos.

> **Nota:** Solo se elimina la entrada del registro de encriptación de campos. No produce ninguna acción sobre el campo del archivo de la base de datos. La entrada en el registro tiene que estar *INACTIVE

Realice los siguientes pasos para **eliminar una entrada de campo del Registro de Encriptación de Campos:**

1. Introduzca el mandato **CRYPTO/RMVFLDENC** y haga F4
2. Introduzca el Identificador del Campo a eliminar y pulse Intro



Ejemplo de Pantalla del mandato RMVFLDENC

2.4 Tokenización

La "Tokenization" en el mundo de la seguridad de la información es el proceso de mover datos sensibles de su servidor a otra localización o servidor y sustituir por unos "token" los datos en su servidor originales, los cuales hacen referencia a los datos originales que se han trasladado a otro servidor o localización.

Nota: De aquí en adelante **Tokenization** se representará por **Tokenización**.

a) Tokenización para la Centralización de Datos Sensibles

La Tokenización debería considerarse cuando los datos sensibles se almacenan en múltiples sistemas a lo largo de la organización.

La Tokenización es el proceso de reemplazar la información sensible con Números de Identificación Únicos (Tokens) y almacenar los datos originales en un servidor central, normalmente de forma encriptada.

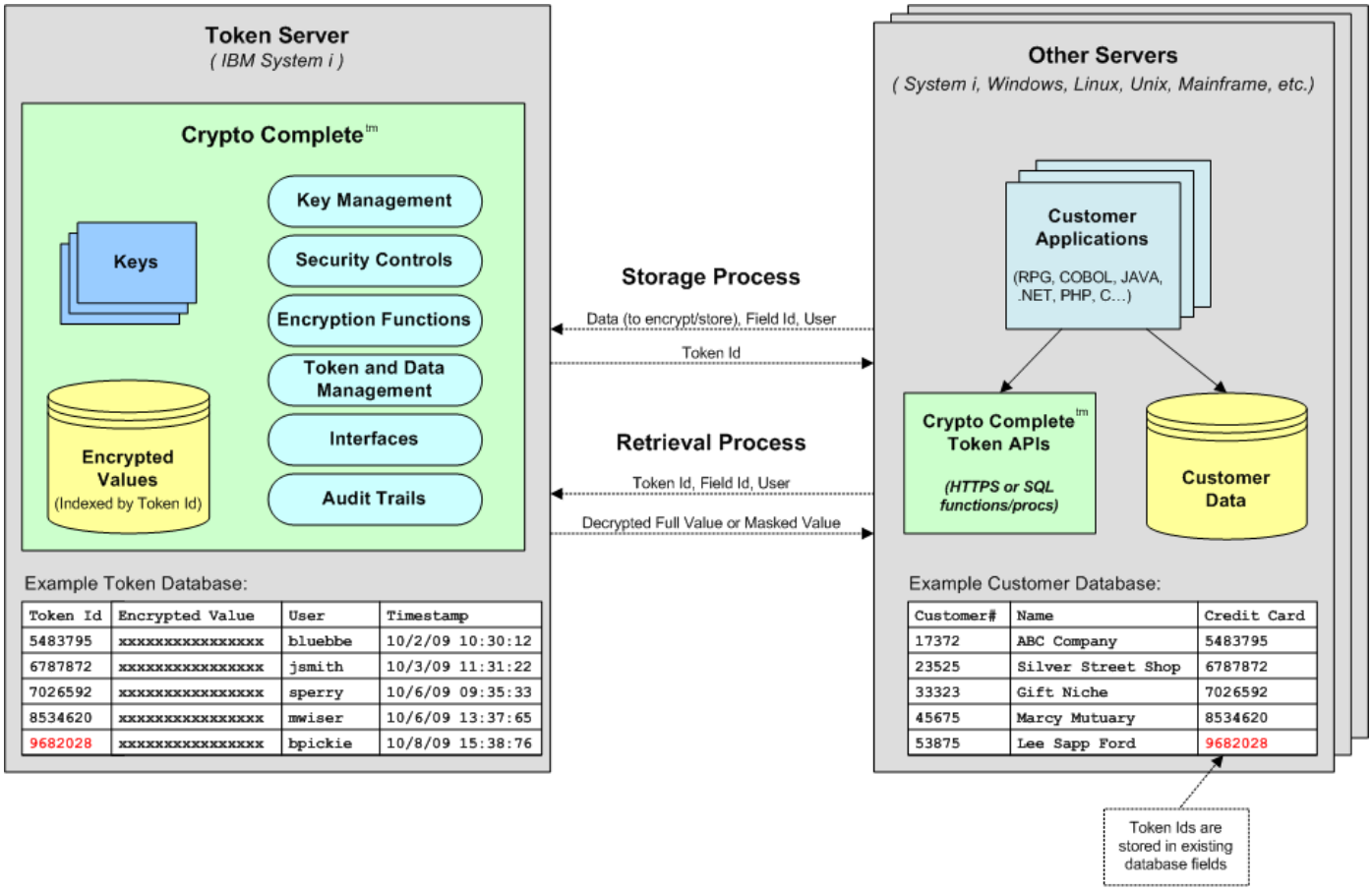
Al centralizar toda la información sensible en un solo sistema, la Tokenización puede ayudar a frustrar los ataques de hackers y ajustarse más a los requisitos de seguridad de obligado cumplimento, como las normas PCI.

En el caso de que necesite implantar la Tokenización en su empresa, Crypto Complete ofrece las siguientes **ventajas**:

- Centraliza la Gestión de Claves y Política de Claves en un solo servidor.
- Permite la Tokenización de información de datos procedente de diferentes sistemas (IBMi, Windows, Linux, Aix, etc…).
- Proporciona conexiones remotas a las funciones Token a través del protocolo HTTP(s).

- Asigna Identificadores de Tokens automáticamente desde el servidor central.
- Encripta y almacena los datos reemplazados por Tokens en archivos físicos de base de datos DB2 escalables.
- Permite asegurar los datos mediante Id de Usuario, Grupos de Usuarios y/ Listas de Autorización.
- Ofrece registros log de auditoría y mensajes de alerta centralizados.

En la siguiente página mostramos un diagrama que muestra cómo funciona Crypto Complete en un entorno de Tokenización.



Example Token Database:

Token Id	Encrypted Value	User	Timestamp
5483795	xxxxxxxxxxxxxxx	bluebbe	10/2/09 10:30:12
6787872	xxxxxxxxxxxxxxx	jsmith	10/3/09 11:31:22
7026592	xxxxxxxxxxxxxxx	sperry	10/6/09 09:35:33
8534620	xxxxxxxxxxxxxxx	mwiser	10/6/09 13:37:65
9682028	xxxxxxxxxxxxxxx	bpickie	10/8/09 15:38:76

Example Customer Database:

Customer#	Name	Credit Card
17372	ABC Company	5483795
23525	Silver Street Shop	6787872
33323	Gift Niche	7026592
45675	Marcy Mutuary	8534620
53875	Lee Sapp Ford	9682028

Diagrama del Proceso de Tokenización con Crypto Complete

b) Proceso de Almacenaje y de Recuperación

Introducción de datos

Cuando sea necesario almacenar información (normalmente una actualización o adición), el sistema remoto pasará los datos, junto con el Id de Campo y el Usuario al servidor de Tokens. Crypto Complete asignará un Id. de Token único y encriptará y almacenará los datos en un archivo físico DB2 en el servidor de Tokens.

El Id del Token es devuelto al sistema remoto, para que lo almacene en el mismo campo (o columna) en que los datos se encontraban originalmente.

Recuperación de datos

Cuando se necesita recuperar los datos, ahora alojados en el Token Server, el sistema remoto pasa el Id. del Token, el Id. del campo y el Usuario. Se recuperan los datos que corresponden al Id del Token y el Id. del campo. Siempre atendiendo a la autorización que tenga el usuario y a la función solicitada, Crypto Complete devolverá al sistema remoto el valor desencriptado ya sea en su versión completa, enmascarada o ningún valor si no está autorizado.

c) Configuración de la Tokenización

Los siguientes pasos permiten establecer la Tokenización con Crypto Complete para cada elemento de dato remoto:

Paso 1 - Cree una entrada en el Registro de Encriptación de Campos

En primer lugar, debería crear una entrada en el Registro de Encriptación de Campos mediante el mandato **ADDFLDENC**. A continuación se muestra un ejemplo con ciertos parámetros:

```
CRYPTO/ADDFLDENC FLDID(ORDERS_CREDITCARD_PRODSYS1)
        DBFLD(*REMOTE)
        DBFLDTYP(*CHAR) DBFLDLEN(16)
        ENCKEYLBL(ENCKEY1) ENCKEYSTR(KEYLIB/ORDERKEYS)
        FLDMASK('************9999')
        AUTLDEC(CCFULL) AUTLMASK(CCMASKED)
        STREXTFILE(*YES) EXTFILE(PRODLIB/CCFILE)
```

Sobre la pantalla del mandato ADDFLDENC puede hacer F1 sobre cualquier parámetro para obtener ayuda on-line. A continuación mostramos una lista de los parámetros que deben especificarse para configurar campos Tokenizados.

Descripción de los campos

FLDID	Se recomienda que el Identificador de Campo se componga del nombre del archivo/tabla, nombre del campo y nombre del sistema remoto en que se utilizará el Token. En el ejemplo anterior, el Identificador de Campo se compone del nombre de archivo ORDERS, del nombre de campo CREDITCARD en el sistema remoto cuyo nombre es PRODSYS1.
DBFLD	Especifique siempre *REMOTE para destacar que los datos son de un sistema remoto.
DBFLDTYP	Es tipo de dato del campo. *CHAR para caracteres y *DEC para decimales.
DBFLDLEN	Longitud de los datos.
ENCKEYLBL	Etiqueta de la Clave DEK de Encriptación de Datos (DEK)
ENCKEYSTR	Nombre del Almacén de Claves que contiene las claves DEK.

FLDMASK	El formato que se utilizará para enmascarar los valores.
AUTLDEC	La lista de autorización de los usuarios autorizados a ver los valores desencriptados completos.
AUTLMASK	La lista de autorización de usuarios autorizados a ver los valores desencriptados enmascarados.
STREXTFILE	Especifique *siempre *YES* para indicar que los valores encriptados se almacenarán en un archivo físico externo.
EXTFILE	Especifique el nombre y biblioteca del archivo físico externo que almacenará los valores encriptados.

Paso 2 - Activar el campo en el Registro de Encriptación de Campos

Una vez añadido el campo al registro, activar el campo con el mandato **ACTFLDENC**.

CRYPTO/ACTFLDENC FLDID(*ORDERS_CREDITCARD_PRODSYS1*)

El mandato ACTFLDENC creará el archivo físico externo que contendrá los datos Tokenizados encriptados para el Identificador de Campo y cambiará su estado a *ACTIVE. Tenga en cuenta que el archivo físico externo tendrá las mismas autorizaciones que las de la biblioteca en que se crea.

Paso 3 - Encriptar y Tokenizar los datos existentes

Se debe escribir un programa en el sistema remoto que pase por todos los registros (filas) del archivo (tabla) que contiene los datos a encriptar. Por cada registro que lee, el programa debe llamar a la función Insert http apropiada del servidor de Tokens, pasando el dato a encriptar/almacenar. Una vez llamada la función Insert HTTP, el Id del Token devuelto se debe almacenar en el archivo de base de datos. Vea la guía HTTP para ver saber más sobre los procedimientos de inserción.

Paso 4 - Encriptación y Recuperación automática

Vea la guía HTTP para ver saber más sobre los procedimientos a llamar desde su sistema remoto para almacenar y recuperar datos del servidor de Tokens.

d) Consideraciones sobre la Tokenización

Rendimiento

La Tokenización de datos no se ejecutará tan bien como la encriptación/almacenamiento nativa de datos, ya que los datos tienen que viajar entre diferentes sistemas por la red.

La velocidad de las transacciones Tokenizadas dependerá principalmente del rendimiento de su servidor Token IBM i así como la velocidad de su red. Se pueden realizar ajustes para mejorar el rendimiento consultando con su proveedor.

Failover

Debería tener un plan de contingencia por si se produjese un fallo en el servidor Token o se perdiesen las comunicaciones. Sin un servidor Token replicado o una conexión alternativa, los datos Tokenizados no estarán disponibles para sus sistemas remotos hasta que se restaure el servidor Token principal o la conexión. Por favor, consulte con su proveedor para ayudarle a preparar un plan de contingencia apropiado.

3. Control de Accesos a los Valores Desencriptados

Existen dos niveles de seguridad que pueden emplearse en Crypto Complete para controlar el acceso a los valores de los campos desencriptados.

En un primer nivel de seguridad, debería dar la autorización *USE sobre el objeto Almacén de Claves (que contiene las claves de desencriptación) sólo a aquellos usuarios o grupo de usuarios que pueden realizar la desencriptación.

En un segundo nivel, puede asignar Listas de Autorización a las entradas de campo en el Registro de Encriptación de Campos y utilizar las APIs convenientemente asignadas para retornar los valores autorizados.

3.1 Primer Nivel de Seguridad - Autorización al Almacén de Claves

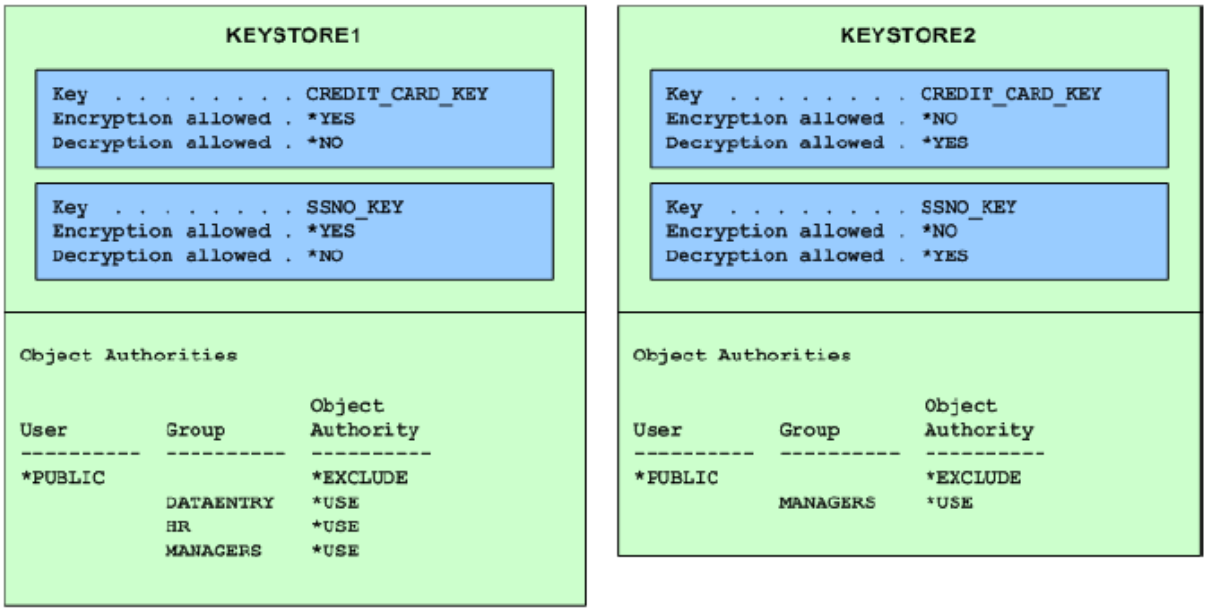
Cuando se solicita una clave para encriptar o desencriptar datos Crypto Complete comprobará en primer lugar si el usuario tiene como mínimo autorización *USE sobre el Almacén de Claves que contiene la clave. Si el usuario no está autorizado sobre el Almacén de Claves, se denegará la solicitud de clave y por tanto el usuario no podrá continuar con la encriptación o desencriptación de datos. El error de autorización también será registrado en el archivo de journal de auditoría.

Es posible que quiera tener un pequeño grupo de usuarios que pueda acceder a datos sensibles (desencriptar), frente a un grupo de usuarios más grandes que introduzca datos (encriptar). Se puede conseguir fácilmente utilizando dos Almacenes de Claves con sus respectivas autorizaciones. En el primer almacén de claves puede almacenar las claves necesarias para encriptar y dar a ese almacén un abanico de autorizaciones más amplio. En el segundo almacén de claves, puede guardar las claves necesarias para la desencriptación y limitar el número de autorizaciones sobre ese segundo almacén.

Por ejemplo, cualquier usuario de introducción de datos puede estar autorizado a introducir un número de tarjeta de crédito, y por tanto debe estar autorizado sobre el Almacén de Claves que contiene la clave de Encriptación. Sin embargo, quizás solo los Supervisores deberían poder ver los números de tarjeta de crédito y por tanto estar autorizados sobre el almacén que contiene la clave de desencriptación.

Cada clave dentro del Almacén de Claves puede ser designada para encriptación únicamente, desencriptación únicamente o ambas.

En el siguiente ejemplo, las Claves en el almacén de claves KEYSTORE1 pueden ser utilizadas sólo para encriptación y las claves en el almacén de claves KEYSTORE2 pueden ser utilizadas sólo para desencriptación. Observe que el almacén de claves KEYSTORE1 tiene más listas de autorización que el almacén KEYSTORE2.



Ejemplo paso a paso

Estos son los pasos, a modo de ejemplo, necesarios para **implementar dos Almacenes de Claves con autorizaciones diferentes:**

1. Cree el almacén de claves KEYSTORE1 para que contenga las claves de encriptación.

   CRYPTO/CRTKEYSTR KEYSTR(library/KEYSTORE1) MEKID(master-key-id)

2. Autorice con permiso *USE sólo a aquellos usuarios o grupos de usuarios sobre el almacén KEYSTORE1 que puedan encriptar.

   EDTOBJAUT OBJ(library/KEYSTORE1) OBJTYPE(*VLDL)

3. Cree el almacén de claves KEYSTORE2 para que contenga las claves de desencriptación.

   CRYPTO/CRTKEYSTR KEYSTR(library/KEYSTORE2) MEKID(master-key-id)

4. Autorice con permiso *USE sólo a aquellos usuarios o grupos de usuarios sobre el almacén KEYSTORE2 que puedan desencriptar.

   EDTOBJAUT OBJ(library/KEYSTORE2) OBJTYPE(*VLDL)

5. Cree la clave en el almacén de claves KEYSTORE1. Configurarla de modo que solo sirva para encriptación:

```
CRYPTO/CRTSYMKEY KEYLABEL(CREDIT_CARD_KEY) KEYSTR(library/KEYSTORE1)
ENCRYPTALW(*YES) DECRYPTALW(*NO)
```

6. Copie la clave del almacén de claves KEYSTORE1 al almacén de claves KEYSTORE2.

```
CRYPTO/CPYSYMKEY FRMLABEL(CREDIT_CARD_KEY) FRMKEYSTR(library/KEYSTORE1)
TOLABEL(*FRMLABEL) TOKEYSTR(library/KEYSTORE2)
```

 **Importante:** Dado que Crypto Complete utiliza encriptación Simétrica, los valores de las claves de encriptación y desencriptación deben ser iguales. Por eso se copia de un almacén a otro en lugar de volver a crearla.

7. Cambie la configuración de la clave en el almacén de claves KEYSTORE2 para que solo sirva para desencriptar.

```
CRYPTO/CHGSYMKEY KEYLABEL(CREDIT_CARD_KEY) KEYSTR(library/KEYSTORE2)
ENCRYPTALW(*NO) DECRYPTALW(*YES)
```

8. Si utiliza el Registro de Encriptación de Campos para encriptar los valores del campo, a continuación se muestra un ejemplo de cómo especificar la clave de encriptación en el almacén de claves KEYSTORE1 y la clave de desencriptación en el almacén de claves KEYSTORE2.

```
ADDFLDENC… ENCKEYLBL(CREDIT_CARD_KEY) ENCKEYSTR(library/KEYSTORE1)
DECKEYLBL(CREDIT_CARD_KEY) DECKEYSTR(library/KEYSTORE2)
```

3.2 Segundo Nivel de Seguridad - Listas de Autorización del Registro de Encriptación de Campos

La configuración de Listas de Autorización permite controlar que parte de los valores de los campos están disponibles para los usuarios y grupos de usuarios.

Por ejemplo, un grupo de usuarios podría estar autorizado a los valores de campo desencriptados completos, mientras que un segundo grupo podría estar autorizado a tan solo los valores enmascarados y un tercer grupo de usuarios podría tener restringido el acceso a cualquier valor del campo. Puede controlar este acceso a través de las Listas de Autorización del IBM i y del Registro de Encriptación de Campos de Crypto Complete.

A continuación mostramos, a modo de ejemplo, los pasos necesarios para crear Listas de Autorización y asociarlas a un campo del Registro de Encriptación de Campos:

Ejemplo paso a paso

1. Cree una Lista de Autorizaciones en el IBM i para controlar las autorizaciones sobre los valores desencriptados completos de un campo.

CRTAUTL AUTL(CCFULL) TEXT('Auth. List of Users with full access')

2. Autorice con permisos *USE a aquellos usuarios o grupo de usuarios que deben tener acceso a los valores desencriptados completos en la Lista de Autorización CCFULL.

EDTAUTL AUTL(CCFULL)

3. Cree otra Lista de Autorización para controlar las autorizaciones sobre los valores enmascarados de un campo.

CRTAUTL AUTL(CCMASK) TEXT('Auth. List of Users with masked access')

4. Autorice con permisos *USE a aquellos usuarios o grupo de usuarios que deben tener acceso a los valores enmascarados en la Lista de Autorización CCMASK.

EDTAUTL AUTL(CCMASK)

5. Si añade un campo en el Registro de Encriptación de Campos, a continuación mostramos un ejemplo de cómo especificar el formato de enmascaramiento y las Listas de Autorización para el campo.

ADDFLDENC… FLDMASK('**********9999')
AUTLDEC(CCFULL) AUTLMASK(CCMASK) NOTAUTHFV('#')

También puede especificar el valor de relleno a utilizar (con el parámetro NOTAUTHFV) si el usuarios no tiene autorización a ninguna de las Listas de Autorización.

Basándonos en los ejemplos anteriores, el valor de campo devuelto en una solicitud de desencriptación será una de las siguientes.

Valor Devuelto	Autorizaciones
Desencriptado completo	Si el usuario tiene como mínimo autorización *USE sobre la Lista de Autorización CCFULL
Enmascarado	Si el usuario tiene como mínimo autorización *USE sobre la Lista de Autorización CCMASK
Relleno	Si no tiene autorización *USE a ninguna de las Listas de Autorización CCFULL o CCMASK. Por ejemplo, si el valor de relleno es #, para un campo de 16 bytes devolverá ################

Nota: Adicionalmente el usuario necesita tener autorización *USE sobre el objeto Almacén de Claves que contiene la clave necesaria para la desencriptación.

Si está utilizando los DB2 Field Procedures (Procedimientos de Campo DB2 o FieldProc), los valores autorizados serán devueltos automáticamente a la aplicación o usuario en las operaciones de lectura.

Sino los utiliza, puede utilizar las APIs de Crypto Complete para acceder a los valores de campo autorizados para el usuario.

- Si está almacenando los valores encriptados de los campos en un archivo externo, lea más sobre la API **GetEncFldAuth** en la Guía del Programador
- Si está almacenando los valores encriptados dentro del campo existente, lea más sobre la API **DecFldAuth.**
- Estas dos APIs tienen además APIs de llamadas a programa correspondientes, funciones SQL y Procedimientos Almacenados que pueden utilizarse opcionalmente desde sus aplicaciones. Encontrará más documentación en la Guía del Programador.

4. Utilidad de Análisis de Campos

El mandato **FNDDBFLD** (Buscar Campos de la base de datos) permite encontrar campos de las bases de datos (en los archivos físicos y tablas) que contengan los valores que cumplan los criterios de búsqueda especificados.

Es especialmente útil para encontrar los campos que contienen datos sensibles sin encriptar, como números de tarjetas de crédito, números de seguridad social…

Por ejemplo, puede realizar una búsqueda de campos numéricos que contengan un número de 16 dígitos (por ejemplo, números de tarjetas de crédito) o realizar una búsqueda de cualquier campo alfanumérico que contenga un patrón numérico como 999-99-999 o 999999999 (por ejemplo, número de Seguridad Social).

Puede realizar la búsqueda en múltiples archivos y bibliotecas con el mandato FNDDBFLD. Y puede buscar campos numéricos como alfanuméricos. El mandato dispone de un menú con diversas opciones y parámetros para ayudar en la búsqueda de números de tarjeta de crédito desencriptados, números de seguridad social, etc.

Para acceder a este menú ejecute: GO CRYPTO/CRYPTO9.

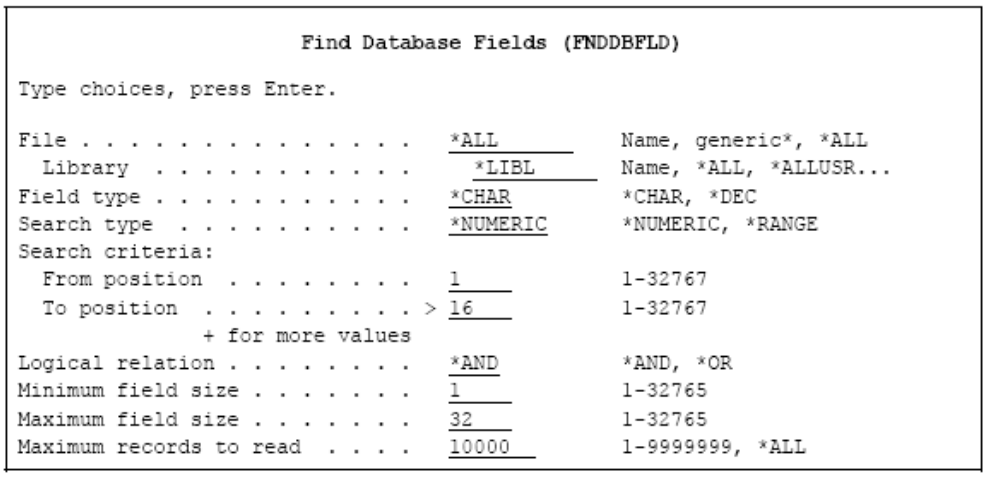
```
CRYPTO9                      Field Analysis Menu            CRYPTO COMPLETE
                                                            Copyright 2007-2010
Select one of the following:                                Linoma Software

 Credit Card Numbers:
   1. Find Alpha fields with a pattern of 9999999999999999 (left aligned)
   2. Find Alpha fields with a pattern of 9999-9999-9999-9999 (left aligned)
   3. Find Numeric fields containing 16 digits

 Social Security Numbers and Social Insurance Numbers:
  10. Find Alpha fields with a pattern of 999999999 (left aligned)
  11. Find Alpha fields with a pattern of 999-99-9999 (left aligned)
  12. Find Alpha fields with a pattern of 999-999-999 (left aligned)
  13. Find Numeric fields containing 9 digits

 Other:
  20. Find other types of data using custom search criteria (FNDDBFLD)
```

Pantalla de opción 9 del menú CRYPTO

Se recomienda ejecutar el mandato FNDDBFLD en **batch** con el mandato SBMJOB.

Realice los siguientes pasos para llamar al mandato de búsqueda FNDDBFLD:

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



Pantalla del mandato FNDDBFLD

Los resultados de la búsqueda se obtienen como un informe (archivo de spool). El informe contendrá la siguiente información por cada campo de la base de datos que concuerde con los criterios de la búsqueda:

- Nombre de archivo
- Nombre de biblioteca
- Nombre de campo
- Número de registro relativo RRN de los datos encontrados (para la primera coincidencia)
- El dato encontrado en el campo (para la primera coincidencia)

Importante: Durante la búsqueda de campos numéricos, el mandato FNDDBFLD ignorará los campos que contengan posiciones decimales. Si tiene archivos con varios miembros, tenga en cuenta que solo se buscará en el primer miembro.