

CRYPTO COMPLETE™



Crypto Complete™ provee procesos automatizados de cifrado de campos de Bases de Datos, archivos y backups, integrando un administrador de llaves (claves).

Suite de Cifrado para el sistema i de IBM

Beneficios de Crypto Complete:

- Cifrado automático de los campos de bases de datos, para IBM i (iSeries) sin Cambiar las aplicaciones.
- Protección de números de tarjetas de crédito (PAN), números de cuentas bancarias, números de documentos de identificación, pagos, y etc., etc.
- Cifrado de Bibliotecas/Objetos del IBM i, (Cifrado de Backup) y archivos del IFS.
- Crea, Administra y Protege las llaves con la solución completamente integrada de Administración de las mismas
- Rotación de las llaves de Cifrado sin tener que reenciptar los datos existentes o cambiar las aplicaciones.
- Cifrado utilizando los algoritmos más fuertes tales como: AES256, AES192, AES128 o TDES.
- Descifrado de valores únicamente para usuarios autorizados (No importa si es todo el valor o solamente la parte enmascarada).
- Uso de Tokens, cifra y almacena datos desde diversos sistemas, ejemplo (IBM i, Windows, Linux, Unix, etc.)
- Genera Seguimientos de auditoría y reportes fácilmente entendibles.

Crypto Complete protege datos sensibles utilizando cifrado fuerte, tokenización, administración de llaves integrada y auditoría.

Crypto Complete permite a las organizaciones cifrar campos de las bases de datos, backups y archivos del IFS de manera rápida y efectiva, a través de sus pantallas intuitivas y su tecnología comprobada.

Esta innovadora solución es fundamental para proteger información confidencial y cumplir rápidamente con los estándares PCI DSS, regulaciones federales (Ej, HIPPA, Sarbanes-Oxley) y leyes privadas del estado.

Crypto Complete puede ser instalado en pocos minutos y no requiere realizar cambio en el código fuente para el proceso de cifrado. Los comandos en Crypto Complete tienen ayuda en línea que es accesible a través de menús intuitivos en el mismo formato de los menús del IBM i.

```
CRYPTO                               Main Menu

Select one of the following:

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

10. Product Information Menu          (GO CRYPTO10)

Selection or command
====> _____

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



(800) 949.4696

www.CryptoComplete.com

Menú Principal Crypto Complete

Cientes Satisfechos



Linoma Software: Sirviendo más de 3,000 Clientes alrededor del mundo

- BeautiControl Cosmetics
- Carolina Biological Supply
- CDW
- Certegy
- City of Ketchikan
- City of Redding
- Consolidated Telephone Companies
- CU*Answers
- Discovery Toys
- EOG Resources
- Fairmount Minerals
- Fidelity Express
- The Geo Group Inc.
- Hermann Sons
- Ingram Industries
- KOA Campgrounds of America
- Landau Uniforms
- Love's Travel Stops & Country Stores
- Mid-Continent Group
- Muscatine Foods Corporation
- Northwest Natural Gas
- Oneida Tribe of Indians of WI
- Permanent General Agency
- Rural Community Insurance Services
- Service Insurance Group
- Silverleaf Resorts
- Slomin's
- Sturm, Ruger & Company
- USA Mobility Wireless
- ViaTech Publishing Solutions

Administración de llaves

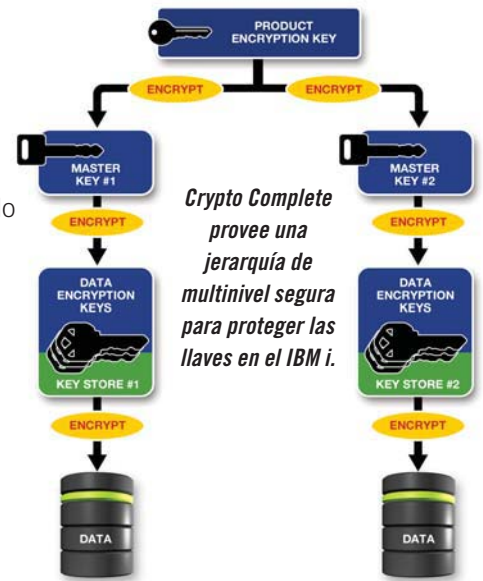
Crypto Complete incluye un avanzado sistema administrador de llaves el cual reside de forma nativa en el IBM i. Este sistema administrador de llaves se encuentra integrado de manera transparente con las políticas de control de Crypto Complete, funciones de cifrado y facilidades de auditoría para proveer una solución de protección de datos sencilla de manejar.

Junto con la seguridad integrada en el IBM i, las organizaciones pueden controlar de manera estricta el acceso a las actividades con las llaves (mantenimiento/uso) y el cumplimiento de requerimientos tales como PCI DSS.

Características:

- Proveen configuración de políticas para el cumplimiento de requerimientos
Ejemplos: Control Dual, separación de deberes
- Permiten controlar cuales usuarios están autorizados para administrar las llaves
- Generación de Llaves Fuertes con valores de hasta 256 bits de longitud
- Organización de las llaves dentro de uno o más objetos denominados repositorios de llaves
- Cifra el repositorio de llaves utilizando la llave maestra de cifrado (MEK)
- Controla el acceso a las llaves de acuerdo al perfil de usuario, perfil de grupo y/o listas de autorización
- Protege y evita que el valor de la llave sea recuperado
- Genera logs detallados de auditoría de todas las actividades de administración de las llaves

Crypto Complete provee también interfaces para compartir llaves de manera segura con otros sistemas tales sistemas de puntos de venta (POS), Windows, Linux y AIX.



Cifrado del Backup

Crypto Complete es una solución 100% Software que permite a los clientes de IBM i, cifrar sus Backups utilizando las mismas unidades de cinta que ya tienen. Los Backups pueden ser protegidos con una seguridad adicional utilizando llaves desde el sistema de administración de Crypto Complete. Se proveen comandos para cifrar/descifrar de cualquier dato dentro del IBM i, incluyendo bibliotecas, objetos y archivos del IFS.

Características:

- Utiliza AES para el proceso de cifrado (Advanced Encryption Standard)
- Cifra y guarda en las unidades de cinta existentes
- Se puede incorporar dentro de los procesos existentes de backup (Ej. Programas CL, BRMS, schedulers)
- Ahorra tiempo y espacio en disco al no generar "archivos de salvar" intermedios.
- Protege los Backups con cualquier "parafrase" (password) o llave
- Almacena etiquetas (identificador) de las llaves con el backup cifrado para facilitar los procesos de restauración
- Backup opcional del sistema integrado de archivos (IFS)
- Reducción de los costos de recuperación de desastres mientras no se requieran dispositivos especiales

Comandos Sencillos son dados para restaurar y descifrar Bibliotecas, objetos y archivos del IFS los cuales fueron guardados utilizando procesos de Backup de Crypto Complete. Estos comandos pueden ser restringidos, para que solo sean usados por usuarios autorizados.

Cifrado de campos

Crypto Complete podrá proteger campos sensitivos de Bases de datos dentro del IBM i utilizando algoritmos fuertes de cifrado tales como el AES o el TDES. Usted podrá cifrar campos de una base de datos con Crypto Complete, incluyendo:

- Números de Tarjetas de Crédito (PAN)
- Información relacionada con la salud
- Números de documentos de identificación
- Salarios
- Números de cuentas bancarias
- Datos Financieros

Con el registro innovador de cifrado de campos de Crypto Complete, usted podrá simplemente indicar los campos de la base de datos a cifrar. Cuando un campo es "Activado" en el registro, Crypto Complete realizara un cifrado masivo de los valores actuales para ese campo.

Crypto complete puede entonces automáticamente cifrar el campo y sus valores de una manera dinámica y permanente mientras nuevos registros son adicionados a la base de datos y aun cuando los valores existentes de campo son cambiados. Esta característica de automatización ahorra tiempo y dinero valioso para nuestros clientes, partiendo del hecho de que las aplicaciones no deben ser cambiadas debido al cifrado de los datos.



El acceso a los datos puede ser minuciosamente controlado a un nivel campo/usuario. Solamente los administradores de seguridad designados, pueden dar autoridad a los valores enmascarados o descifrados. El descifrado de cualquier dato puede ser completamente auditado en Crypto Complete, lo que dejara en el log el id del usuario, fecha, hora, información del trabajo (job) y llave utilizada.

Tokenización

La tokenización debería ser considerada cuando hay datos sensitivos almacenados en sistemas múltiples a lo largo de la organización.

Tokenización es el proceso de reemplazar datos sensitivos con números únicos de identificación, (Ej. Tokens) y almacenar los datos originales en un servidor central, generalmente de manera cifrada.

Al centralizar los datos sensitivos en un solo sistema, la tokenización puede ayudar a impedir ataques de hackers y minimizar el alcance de las auditorias de cumplimiento tales como PCI.

La tokenización puede ser utilizada para proteger cualquier dato sensitivo incluyendo números de Tarjetas de Crédito (PAN), números de cuentas bancarias, números de identificación, y cualquier otra información de uso personal.

Características:

- Centraliza en un solo Servidor la administración de las llaves y de políticas
- Soporta tokenización de los datos provenientes de diversos sistemas, incluyendo IBM i, Windows, Linux, AIX, etc.
- Provee conexiones remotas a las funciones token a través del protocolo seguro HTTPS
- Asigna de manera automática identificadores token desde el servidor central de tokens.
- Cifra y almacena datos tokenizados en archivos físicos expandibles de DB2
- Permite asegurar elementos de los datos por perfil de usuario, perfil de grupo y/o listas de autorización.
- Provee Logs de auditoría centralizados y mensajes de alerta

Auditorias



Crypto Complete incluye una completa auditoria para reunir los mas exigentes requerimientos de seguridad. Los logs de las entradas de auditoria son generados por los siguientes eventos:

- Cuando cualquier política de configuración de claves es cambiada.
- Cuando los oficiales de claves son cambiados, adicionados o borrados.
- Cuando las claves de Encriptación maestra son cargadas o configuradas.
- Cuando los almacenamientos de claves son creados o trasladados.
- Cuando las claves de Encriptación de datos son creadas, cambiadas o borradas.
- Cuando entradas en el registro de Encriptación de campos son adicionadas, cambiadas, removidas, activadas o desactivadas.
- Cuando cualquier función es denegada debido a autorización inapropiada.
- Cuando los datos son encriptados o descryptados con una clave que requiere registro de estos eventos.

Las entradas en los registros de los logs de auditoria pueden ser mostradas o impresas utilizando una variedad de criterios de selección amplia, incluyendo rangos de tiempo y/o fecha, usuario y tipo de auditoria.

Especificaciones Técnicas

Sistema Operativo: i5/OS V5R2 o mas reciente

Espacio en Disco: 75 MB

Cifrado de datos: Campos de Bases de Datos,
Archivos del IFS, Objetos,
Bibliotecas, Backups

Algoritmos de Cifrado: AES256, AES192,
AES128, TDES

Generación de Llaves: Randómico
Basado en Para frases
Importación Manual

Tipo de Llave: Simétrico

Laves de Cifrado Maestras: (MEK): Si

Llaves de Cifrado de Datos(DEK): Si

Número permitido de llaves almacenadas: Cantidad ilimitada

Número de Llaves Permitidas: Cantidad ilimitada

Control de Llaves Duales: Si

Separación de deberes: Si

Modos de cifrado de Campos: Automático o Manual

Cifrado de campos Alfanuméricos: Si

Cifrado de campos Numéricos: Si

Formatos personalizados de enmascaramiento: Si

Soporte de Tokenizacion: Si

Métodos de Protección del Backup: Llave o Password

Soporte para múltiples ambientes: Si

Trazabilidad de Auditoria: Si - (Dentro de un Journal)

Alertas de Seguridad: Email
Message Queue
Protegrity
QAUDJRN
QHST
QSYSOPR
SYSLOG
User Message

Acerca de Linoma Software

Fundada en 1994, Linoma Software provee constantemente tecnologías innovadoras dirigidas a las necesidades de desarrollo en lo referente a transmisión de datos, traducción, encriptación de datos y modernización de código.

Linoma Software tiene una diversa base de usuarios instalados, son más de 3,000 de ellos alrededor del mundo incluyendo corporaciones, organizaciones sin ánimo de lucro y entidades del gobierno. Con su dedicación a investigar, desarrollar y un servicio al cliente superior, Linoma Software es reconocido como un líder en el desarrollo de software.

Soporte al Cliente

El éxito que LINOMA software ha alcanzado es ampliamente basado en nuestro alcance al mercado que nosotros servimos, centrado en el cliente. Proveer el mas alto nivel de soporte al cliente es la prioridad numero uno en LINOMA. Linoma es capaz de rápida y eficientemente corregir o arreglar cualquier problema que pueda pasar a través de asistencia telefónica, correo electrónico, y conversaciones en línea.



LINOMA
SOFTWARE

1409 Silver Street
Ashland, Nebraska 68003
(402) 944.4242
(800) 949.4696
www.linomasoftware.com
email: sales@linomasoftware.com



Información del Distribuidor

Via Laietana 20
08003 Barcelona, Spain
93 319 16 12
www.att.es
email: att@att.es