IBM Encryption Facility for z/OS (5655-P97)

Proporcione transferencias de datos seguras a su negocio

Características principales

- Permite transferencias de datos muy seguras a socios comerciales, proveedores y clientes
- Permite el cifrado con gestión de claves para cinta y disco
- Permite el cifrado de grandes volúmenes de datos para el archivado en sitios remotos
- Aprovecha al máximo las funciones de gestión de claves de IBM® z/OS
- Permite gestión de claves a largo plazo para archivado de datos en sitios remotos
- Más flexibilidad con compatibilidad con el formato OpenPGP RFC 4880
- Admite la compresión mediante los algoritmos ZIP y ZLIB y el uso de z Data Compression (zEDC) cuando está disponible.

La protección de los datos confidenciales es una de las principales preocupaciones de las empresas de todo el mundo. La importancia de proteger los datos esenciales para el negocio y la información de los clientes ha llegado hasta las salas de juntas, porque los errores en la protección de estos activos pueden originar costes muy altos y, lo más importante, suponer una pérdida de confianza de clientes e inversores. Es posible que el sector, la normativa y las obligaciones contractuales con los business partners (BP) exijan ofrecer también esta protección. Tanto si los datos se transfieren a través de la red como si atraviesan la ciudad en una cinta dentro de un camión, deben protegerse frente a los accesos no autorizados y ser accesibles a los usuarios a los que están destinados.

IBM Encryption Facility for z/OS V1.2 puede aplicar servicios de cifrado de mainframe, que han contribuido a proteger los cajeros automáticos durante más de 20 años, para proteger los datos que no se utilizan. Los clientes pueden utilizar la gestión centralizada de claves de z/OS para ofrecer un intercambio de claves de cifrado extraordinariamente seguro. Si un contenido importante y destinado a un socio comercial de confianza cae en las manos incorrectas, los datos solo se podrán descifrar con la clave de cifrado privada del socio.

Con IBM Encryption Facility for z/OS, puede cifrar datos de su sistema z/OS para hacerlos llegar a sus socios o clientes, aunque no dispongan de un sistema z/OS. Los socios que dispongan de z/OS tendrán la opción de utilizar Encryption Facility, el cliente basado en Java™, Decryption Client for z/OS o un programa compatible con OpenPGP RFC 4880 para descifrar los datos. Los socios que no tengan

z/OS pueden utilizar el cliente basado en tecnología Java o un programa compatible con OpenPGP RFC 4880 para cifrar y descifrar datos.

Encryption Facility for z/OS consta de dos características opcionales de pago:

- La función **Encryption Services** admite el cifrado y el descifrado de determinados formatos de archivo en z/OS. Esto permite transferir archivos a sitios remotos dentro de la empresa, a socios y proveedores, o archivarlos. La función Encryption Services admite el formato de IBM z Systems (introducido originalmente en Encryption Facility for z/OS V1.1) y el formato OpenPGP (presentado con Encryption Facility for z/OS V1.2). El formato z Systems admite compresión acelerada por hardware antes del cifrado
- La función **DFSMSdss Encryption** permite el cifrado de conjuntos de datos de volcado DFSMSdss. Esta función admite la compresión acelerada por hardware antes del cifrado.

La capacidad de cifrado de última generación (SOTA) y de gestión centralizada de claves proporcionada por las funciones de z/OS y las características de los servidores z Systems contribuyen a proteger los datos.

Función Encryption Services

Formato z Systems

La función Encryption Services permite cifrar datos y le ayuda a compartir información confidencial entre distintas plataformas con socios, proveedores y clientes. También puede utilizar la función Encryption Services para cifrar determinados archivos para conservarlos. Esta función puede utilizar las funciones de gestión de claves de z/OS y de autenticación de acceso proporcionadas en Integrated Cryptographic Services Facility (ICSF), así como las capacidades de compresión y cifrado de hardware de los servidores z Systems.

La función Encryption Services admite cifrado de datos mediante claves TDES de triple longitud o claves Advanced Encryption Standard (AES) de 128 bits. Se pueden especificar claves públicas/privadas Rivest Shamir Adleman (RSA) para encapsular y desencapsular las claves de datos AES y TDES que se han utilizado para cifrar el archivo. Las claves desencapsuladas se almacenarán en un encabezado de archivo. Con esta técnica, se pueden generar muchos archivos utilizando distintas claves de cifrado y, en teoría, todos ellos podrán leerse incluso después de varios años de archivado. La función Encryption Services también admite el uso de un esquema de derivación de clave con contraseña.

La función Encryption Services admite entradas procedentes de archivos de entrada secuenciales físicos, de conjuntos de datos particionados (PDS), de conjuntos de datos particionados ampliados (PDSE) y de archivos almacenados en sistemas de archivos z/OS UNIX® System Services. Puede comprimir los archivos de entrada antes de cifrarlos y escribir los archivos de salida. Al utilizar la interfaz de grandes bloques con los archivos de salida escritos en cinta, la función Encryption Services puede contribuir también a optimizar el rendimiento y el espacio del soporte.

Formato OpenPGP RFC4880
Con la introducción de V1.2, Encryption Facility for z/OS ahora es compatible con el formato OpenPGP. La compatibilidad con OpenPGP proporciona más opciones y flexibilidad para realizar intercambios de datos entre BP. La compatibilidad con OpenPGP de Encryption Facility está pensada para cumplir con los requisitos del estándar OpenPGP y ser compatible con otros productos conformes con OpenPGP (RFC 4880). Le permitirá intercambiar un archivo cifrado, comprimido y firmado digitalmente entre sus centros de datos (DC) internos utilizando la compatibilidad de Encryption Facility con OpenPGP junto con sus socios comerciales externos y proveedores que tengan instalado un cliente conforme con OpenPGP (RFC 4880) que se ejecute en z/OS y otros sistemas operativos (SO). La compatibilidad de Encryption Facility con OpenPGP incluye una larga lista de capacidades, por ejemplo, el cifrado básico mediante contraseña de una clave de sesión generada de forma aleatoria, el cifrado asimétrico de claves simétricas generadas de forma aleatoria con algoritmos RSA y ElGamal, las firmas digitales de datos y otras funciones diversas que pueden ser importantes en función de su sistema operativo y necesidades.

La compatibilidad con el formato OpenPGP por parte de Encryption Facility for z/OS V1.2 consumirá más recursos de CP que la compatibilidad con el formato de Encryption Facility z Systems. Se puede configurar para utilizar varias CP a través de un incremento del proceso en paralelo. El impacto del mayor uso de la unidad central de proceso (CPU) por parte de la compatibilidad con OpenPGP de Encryption Facility se puede reducir con los procesadores z Integrated Information Processor (zIIP) en z13 y zIIP y los procesadores zEnterprise Application Assist Processors (zAAP) en las generaciones anteriores. Dado que la compatibilidad con el formato OpenPGP está escrita en Java y la carga de trabajo de Java es apta para procesadores especializados, puede obtener un ahorro de software teórico. Por lo tanto, con determinadas configuraciones, como las de cuatro o más CPU en línea, el tiempo necesario para la realización de una tarea por parte de la compatibilidad con OpenPGP es menor si lo comparamos con la compatibilidad con el formato de Encryption Facility z Systems.

Estas funciones pueden utilizar Integrated Cryptographic Service Facility (ICSF) y criptografía de hardware. La criptografía de hardware necesita el entorno correcto y es posible que requiera también que se haya instalado un módulo criptográfico.

Encryption Facility for z/OS V1.2 está disponible en las versiones de z Systems y z/OS admitidas actualmente.

Función DFSMSdss Encryption

La función Data Facility Storage Management Subsystem (DFSMSdss) permite cifrar conjuntos de datos de volcado DFSMSdss escritos en cinta y en disco. Esta función está diseñada para utilizar las funciones de gestión de claves de z/OS y autenticación de acceso, así como las funciones de criptografía de hardware y compresión de z Systems.

DFSMSdss Encryption admite cifrado de datos mediante claves TDES de triple longitud o claves AES de 128 bits. Al igual que la función Encryption Services, admite el uso de claves públicas/privadas RSA para encapsular y desencapsular las claves de datos AES y TDES utilizadas para cifrar archivos, así como la generación de claves AES y TDES mediante una contraseña especificada. También puede especificar que DFSMSdss comprima los datos antes de cifrarlos.

DFSMSdss Encryption incluye dos funciones: una para cifrar datos al tiempo que se procesan comandos DUMP y la otra para descifrarlos mientras se procesan comandos RESTORE.

Encryption Facility for z/OS Client con uso del formato z Systems
Encryption Facility for z/OS Client, un programa con licencia independiente (que se ofrece tal cual, sin garantía), se ha diseñado para permitir el intercambio de datos cifrados entre sistemas z/OS que tengan instalado Encryption Facility y sistemas que se ejecuten en z/OS o en otras plataformas que necesiten las funciones compatibles.

El programa Encryption Facility for z/OS Client consta de:

- **Un cliente basado en Java.** *El cliente basado en Java, escrito en Java, se puede utilizar en Z/OS y en cualquier plataforma que admita Java.* El cliente basado en Java admite el descifrado de datos creados en un sistema z/OS con el formato de Encryption Facility z Systems, así como el cifrado de datos para enviar a un sistema z/OS, donde el archivo se descifrará utilizando el formato de Encryption Facility z Systems. Nota: No se puede utilizar la compresión para crear los datos que se van a procesar con el cliente basado en Java
- **Decryption Client for z/OS.** *Decryption Client for z/OS solo es compatible con sistemas z/OS.* Decryption Client for z/OS admite el descifrado de datos creados en un sistema z/OS utilizando el formato de Encryption Facility z Systems. Se puede utilizar la compresión para crear los datos que se van a procesar con Decryption Client for z/OS. Decryption Client no admite el cifrado de datos para el viaje de vuelta. Esta opción puede reportar ventajas de rendimiento y necesitar menos espacio de soporte a efectos de intercambio, pero no permite a sus socios devolverle los datos con un formato cifrado.

El valor del cifrado del mainframe

Los servicios de cifrado del mainframe de IBM se basan en una integración del hardware y el software: de las tecnologías de cifrado y compresión de los servidores mainframe y de las funciones de gestión de claves centralizadas del sistema operativo z/OS.

El hardware para el cifrado de mainframe ofrece dos funciones fundamentales: una mayor aceleración del cifrado en comparación con el cifrado basado en software y, con las funciones adecuadas, proporciona también servicios Secure Key. La función CP Assist for Cryptographic Function (CPACF), integrada en los procesadores centrales en los servidores IBM z Systems, proporciona una aceleración del cifrado con un alto rendimiento. En el servidor IBM System z10 Enterprise Class (z10 EC) y posteriores, las nuevas mejoras incluyen compatibilidad con el algoritmo hash SHA-512 y con el estándar Advanced Encryption Standard (AES-256) de 256 bits, que se está convirtiendo rápidamente en el estándar de cifrado.

Las funciones opcionales Crypto Express2, Crypto Express3, Crypto Express4 y Crypto Express5 proporcionan tecnologías Secure Key que permiten realizar intercambios de confianza utilizando claves públicas/privadas. Secure Key es importante para las funciones bancarias, por ejemplo, las comunicaciones de host a cajero. Crypto Express2 admite Triple-DES y Trusted Key Entry, que ofrecen opciones Secure Key. Crypto Express3 admite Triple-DES y claves de cifrado de datos AES de 128, 192 y 256 bits. La última generación Crypto Express5 aporta un rendimiento mayor que z/OS Encryption Facility puede aprovechar junto con las mejoras de rendimiento proporcionadas por el z13 CPACF.

La función ICSF de z/OS proporciona la interfaz entre aplicaciones que buscan cifrado y servicios de cifrado de hardware. Con un historial de más de 20 años de uso eficaz por parte de clientes de mainframe en todo el mundo, ICSF ayuda a las empresas a proteger y gestionar claves de cifrado. Esto incluye generación de claves, gestión de claves basada en políticas de cliente y recuperación de claves. Otra característica importante de ICSF es la capacidad de proporcionar información para el cumplimiento de auditorías y los controles de acceso.

Estas funciones de cifrado se amplían con la flexibilidad y la disponibilidad del mainframe de IBM. La alta disponibilidad, la ampliación, la flexibilidad y las funciones de recuperación remota del mainframe hacen que resulte la opción más lógica para almacenar y gestionar claves de cifrado. Las funciones de cifrado proporcionadas por los servidores mainframe de IBM, junto con la seguridad integrada en el sistema operativo z/OS, ofrecen una base sólida para la gestión de claves a largo plazo. Encryption Facility for z/OS (V1.2) se ha diseñado para proporcionar un método integral para el cifrado de datos en cinta o en disco.

Otras funciones de IBM Encryption

IBM ahora ofrece una amplia gama de soluciones de cifrado diseñada para responder a sus necesidades de protección de los datos.

IBM System Storage Solution
El sistema IBM System Storage TS1120 o las unidades de cinta posteriores ofrecen un sistema de almacenamiento de datos flexible y de alto rendimiento compatible con el cifrado de datos. La función de cifrado se suministra de serie en todos los TS1120 solicitados recientemente o las unidades de cinta de modelos posteriores. El TS1120 y las unidades de cinta de modelos posteriores con cifrado se han diseñado para proporcionar una solución de protección de datos capaz de descargar la función de cifrado desde el servidor a la unidad de cinta (evitando de esta manera la sobrecarga del servidor) y ofrecer una solución de cifrado rentable para grandes volúmenes de datos utilizados en operaciones de copia de seguridad y archivado. Cuando se utilizan con z/OS, el TS1120 o las unidades de cintas de modelos posteriores aprovechan las ventajas de las extraordinarias funciones de cifrado y seguridad de z Systems para ofrecer una potente solución de almacenamiento y gestión de claves de cifrado en toda la empresa.

IBM Security Key Lifecycle Manager (ISKLM)
IBM Security Key Lifecycle Manager (ISKLM) para z/OS funciona con unidades de cinta que admiten cifrado y dispositivos de almacenamiento del sistema de IBM. ISKLM ayuda a generar, proteger, almacenar y mantener las claves de cifrado utilizadas para cifrar la información que se escribe en los dispositivos y descifrar la información que se lee de ellos. Existe una interfaz de línea de comandos (CLI) para gestionar el suministro de claves a estos dispositivos. Asimismo, ISKLM para z/OS es compatible con unidades de cinta Linear Tape-Open® (LTO®) y 3592 que admiten cifrado. Son compatibles los siguientes tipos de unidad:

- Unidades de cinta TS1120, TS1130 y TS1140 con cifrado de datos
- Unidades de cinta LTO Ultrium® 4 y LTO Ultrium 5 con cifrado de datos. El cifrado se realiza a velocidad máxima de línea en la unidad de cinta después de la compresión.

ISKLM for z/OS es también compatible con el sistema IBM DS8000 Storage Controller con la versión del paquete de microcódigos adecuada de DS8000 Storage Controller, nivel Licensed Internal Code (LIC) 64.2 o posterior.

Solución Data Encryption for IMS and DB2 Databases
IBM Data Encryption for IMS and DB2 Databases proporciona una herramienta de cifrado de datos para bases de datos IMS y DB2 para z/OS en un único producto. Este producto se ha concebido para permitirle proteger los datos confidenciales y privados de IMS en el nivel de segmento y para DB2 en el nivel de fila. IBM Data Encryption for IMS and DB2 Databases se implementa mediante opciones estándar IMS y DB2 que invocan el hardware criptográfico de z Systems para cifrar datos a fin de almacenarlos y descifrar datos para utilizarlos en aplicaciones.

Todas estas soluciones le ofrecen una amplia gama de funciones de cifrado, cada una de ellas diseñada para proteger determinados elementos de su entorno. Para poder evaluar y determinar las soluciones de cifrado más adecuadas para responder a sus necesidades de seguridad, póngase en contacto con su representante de ventas de IBM o business partner local para que le proporcionen más información.

Requisitos de hardware:

Las funciones Encryption Services y DFSMSdss Encryption de Encryption Facility for z/OS se ejecutan en los siguientes servidores IBM:

- IBM z13
- IBM zEnterprise EC12 (zEC12) o zBC12
- IBM zEnterprise 196 (z196) o z114
- IBM System z10 Enterprise Class (z10 EC) o z10 BC
- IBM System z9 Enterprise Class (z9 EC) o z9 BC.

El anuncio de IBM 207-008 para Estados Unidos del 16 de enero de 2007 especifica los siguientes requisitos mínimos para las opciones criptográficas de hardware.

Consulte el siguiente anuncio para obtener más detalles: **ibm.com**/common/ssi/rep_ca/8/897/ENUS207-008/ENUS207008.PDF

Para más información

Para obtener más información acerca de la seguridad del mainframe de IBM, visite: **ibm.com**/systems/z/security/

IBM España S.A.
Sta. Hortensia 26-28
28002 Madrid
España

El sitio web de IBM está disponible en **ibm.com**/es

Reciclar por favor

ZSD01450-ESES-04