IBM Data Encryption for IMS and DB2 Databases, Version 1.1

Highlights

- ***Provides user-customizable precoded exits for encryption of IMS™ and DB2® data***
- ***Exploits zSeries™ Crypto Hardware features which results in low overhead encryption/ decryption***
- ***Uses the ANSI Data Encryption Algorithm (DEA) which is also known as the U.S. National Institute of Science and Technology (NIST) Data Encryption Standard (DES) algorithm***
- ***Works at and is customizable at the IMS segment level. For DB2, encryption and decryption is customizable at the row level***
- ***Conforms to the existing z/OS™ security model***

Data security is a top issue in today's world

Are you the person responsible for protecting your company's sensitive IMS and DB2 data? Are you investigating how to comply with security legislation in such industries as health care and finance? If so, IBM Data Encryption for IMS and DB2 Databases is the tool you need. It provides you with a data encryption tool for both IMS and DB2 for z/OS databases in a single product, enabling you to protect your sensitive and private data for IMS at the segment level and for DB2 at the row level.

No need to write and maintain encryption software

IBM Data Encryption for IMS and DB2 Databases is implemented via standard IMS and DB2 exits. The exit code invokes the zSeries Crypto Hardware to encrypt data for storage and decrypt data for application use thereby protecting sensitive data residing on various storage media.

In IMS, the data encryption tool implements encryption via the standard Segment Edit/Compression exit routine. Both IMS data and index databases can be encrypted and decrypted. In DB2, the data encryption tool implements encryption through the standard EDITPROC exit. This tool can help you save the time and effort required to write and maintain your own encryption software for use with such exits or within your applications.

Complying with regulatory legislation

Strong internal controls are needed to reduce operational risk and comply with active and pending legislative requirements faced by corporations, especially large multinationals. Examples of such legislation include Basel II, which puts in place financial risk management structures that address complex international banking relationships. Sarbanes-Oxley (SOX) imposes new standards for reliability in reporting financial results and establishing independent auditors. The Health Insurance Portability and Accountability Act (HIPAA) regulates the security of medical records.

In the United Kingdom, the Data Protection Act (DPA) requires that individuals' personal information be kept confidential. Twenty-five members of the European Union are Safe Harbor Certified to do business with US companies, agreeing to provide notice on how data is used and to guarantee security of that data. Canada has enacted PIPEDA (Personal Information Protection and Electronics Documents Act) which regulates how private sector companies can collect and use personal information in the course of commercial activities.

In Japan, the Personal Information Protection Law requires that companies appoint corporate privacy officers to enforce rules regarding privacy. Hong Kong, Taiwan and Singapore are among the growing number of countries which have enacted laws covering the protection of personal data.

An important first step in taking control of information and meeting regulatory requirements is encrypting sensitive data. IBM Data Encryption for IMS and DB2 Databases enables you to leverage the power of Storage Area Networks (SANs) safely while complying with these privacy and security regulations and many others being enacted worldwide. During encryption, IMS or DB2 application data is converted to database data that is unintelligible except to the person authorized by your security administrator. If you make decisions about protecting sensitive data to keep your company on the right track to compliance, find out more about how IBM's data encryption tool can help.

Hardware requirements

IBM Data Encryption for IMS and DB2 Databases supports any processor capable of operating all supported releases of IMS and DB2 Universal Database™ (UDB) Server for z/OS.

Software requirements

IBM Data Encryption for IMS and DB2 Databases requires IMS, Version 7 or higher and/or DB2 UDB Server for z/OS, Version 7 or higher. It also requires z/OS Integrated Cryptographic Service Facility (ICSF) which only runs on processors that support the IBM Cryptographic Coprocessor Feature (CCF). For example, these processors include G3, G4, G5, G6, Multiprise® 2000, Multiprise 3000, or @server zSeries. The hardware CCF modules must be enabled with configuration data that is a separately orderable feature and requires a processor Power-On-Reset to complete the loading of the data into the crypto modules.

z/OS ICSF additional information

Integrated Crypotographic Service Facility (ICSF) is an element of z/OS, so there are no additional operating system requirements. Before use of the hardware encryption can occur, the hardware modules must be loaded with at least host DES Master Keys. For details on Master Key entry, see the ICSF Administrator's Guide (SA22-7521-03) in the IBM Publication Center at http://www.elink.ibmlink.ibm.com/public/applications/publications/cgi-bin/pbi.cgi

For more information

Please contact your IBM marketing representative or an IBM Business Partner, or call 1 800-IBM CALL within the U.S.

Also, visit our Web site at **ibm.com**/software/data/db2imstools.

When ordering IBM Data Encryption for IMS and DB2 Databases, please specify program number 5655-P03.

IBM Corporation
Silicon Valley Laboratory
555 Bailey Avenue
San Jose, CA 95141

Produced in the United States of America
12-05
All Rights Reserved

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.