MEGA Cryption db™

DB2 Encryption

Advanced Software Products Group, Inc · 3185 Horseshoe Drive South, Naples, FL 34104 USA
T: 800-662-6090 **T:** 239-649-1548 · aspgsales@aspg.com · www.aspg.com

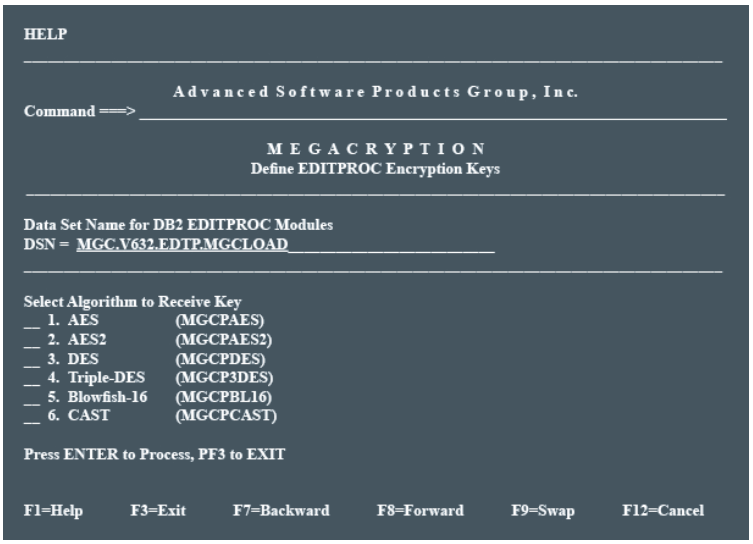
“Easily protect sensitive DB2 data using MegaCryption DB™”

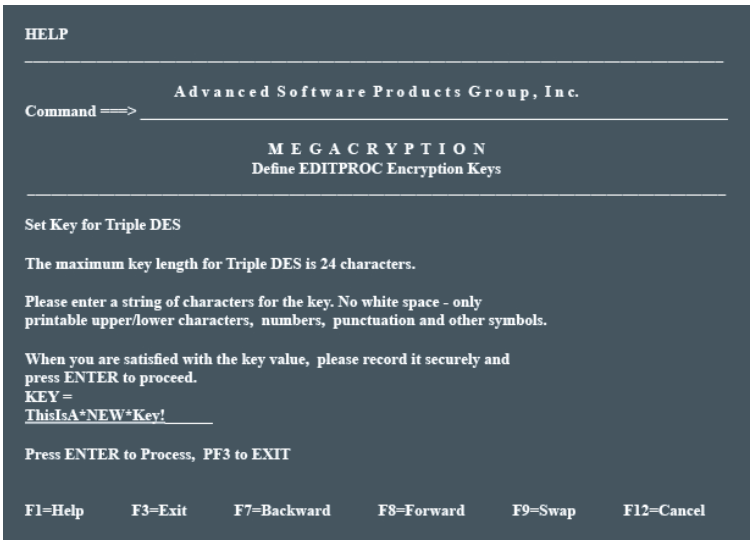
DB2 Cryptography

MegaCryption DB™ provides comprehensive and cost-effective encryption of sensitive DB2 data, customizable at the table [row] level. It encrypts data-at-rest using the most secure non proprietary and well-known algorithms such as AES-128, AES-256, Blowfish-16, CAST, DES, and Triple-DES. Encryption is transparent to applications / users and requires no changes to your applications.

MegaCryption DB complements any encryption process you may already have in place for other platforms. It does not require IBM's ICSF to encrypt your data and can take advantage of IBM's CPACF clear-key acceleration for speed. Designed to be extremely flexible to accommodate a variety of experience levels, encryption methods, and security policies companies have implemented. Additionally, a robust ISPF front-end allows for simple administration.

MegaCryption DB can be used as a stand-alone product, encrypting critical data at the DB2 table level, or can be used in conjunction with MegaCryption z/OS to provide a complete encryption solution protecting data across the enterprise. MegaCryption and MegaCryption DB also come with FREE companion products for use on Windows, UNIX or LINUX systems, which can be freely distributed internally and externally.





Compliancy Mandates

Regardless of your industry, today's data centers are facing unprecedented pressure to comply with internal, state, federal, and industry compliancy mandates. There are very few organizations that are not required to protect customer and/or operational data. Cryptography is vital to protecting sensitive data. MegaCryption DB aids in compliancy with government regulations such as SOX, PCI, HIPAA, FERPA, Graham-Leach-Bliley and more. MegaCryption DB provides mandate-specific solutions to protecting data; for example, for PCI compliancy, MegaCryption DB will encrypt data in process, and provide security for data as it is being created by your application. The Verizon Annual Data Breach Investigation report states, *"PCI compliancy is important. 81% of affected organizations subject to the Payment Card Industry Data Security Standard [PCI-DSS] had been found non-compliant prior to being breached."* Additionally, MegaCryption DB provides for AES-128 encryption and decryption operations using FIPS-197 validated cryptographic modules.

Encryption: Data at Rest

Data lost or stolen outside the confines of the data center has made global headlines in the last few years, forcing organizations to encrypt data that they are physically transporting. Although, encrypting data in transit is important, encrypting data at rest in the data center is unquestionably just as important. Although SAF tools like RACF™, ACF2™, & Top Secret™ have done a great job of securing mainframe data over the years, a recent national study showed that 70% of companies surveyed admitted to internal security breaches. Internal breaches alone, have made the encryption of data at rest a necessity. Encrypting data at rest greatly reduces the likelihood of confidential information being disclosed to unauthorized individuals, and when it comes to internal threats, encrypting data at rest provides an additional layer of security. By combining encryption of data at rest and data in transit, organizations can be assured that only the most sophisticated adversaries are a concern. Data at rest also represents a major security vulnerability for organizations with mobile work forces. Data can be left anywhere, so it must be protected everywhere. Legal requirements may also force organizations to encrypt data at rest as part of government mandated regulations.

PRODUCT FEATURES

- Encrypts sensitive DB2 data at rest, customizable at the table [row] level
- Encrypts data in process, providing security for data as it is being created by your applications [a PCI requirement]
- Encryption is transparent to applications / users
- Requires no changes to your applications
- EDITPROC Exit for DB2
- Row Level Encryption
- Multiple Algorithms Supported: AES, AES2, DES, 3-DES, CAST, BL16
- Robust ISPF Interface for simple administration
- Aides in compliancy with government regulations such as SOX, PCI, HIPAA, FERPA, Graham-Leach-Bliley and more
- Fast & easy Installation in less than one hour. Customers are ready to encrypt data immediately after installation
- MegaCryption/PC & MegaCryption/IX FREE enterprise companion products for your non-z/OS platforms
- MegaCryption training is available on-site or online
- All-in-one product, supported by one company, 24x7x365

SUPPORTED ALGORITHMS

MegaCryption DB supports strong, well-known and preferred, non-proprietary algorithms and provides symmetric cryptography. MegaCryption is FIPS validated & certified by National Institute of Standards & Technology [NIST].

AES (Advanced Encryption Standard) is a Federal Information Processing Standard (FIPS) for use by US Government. MegaCryption makes use of 128 & 256 bit keys for AES (RIJNDAEL).

CAST-5 uses 16-round with 128 bit key size and is commonly used by OpenPGP implementations.

DES is a 64-bit block cipher, symmetric algorithm also known as Data Encryption Algorithm (DEA and DEA-1) with a key size of 56 bits.

TRIPLE DES is an encryption configuration in which the DES algorithm is used three times with three different keys - producing the equivalent of a 168-bit key size.

BLOWFISH is a 64-bit symmetric block cipher that takes a variable-length key, from 32-bits to 448 bits.

ADVANCED SOFTWARE PRODUCTS GROUP, INC.

FREE TRIAL DOWNLOAD • FREE EDUCATIONAL WEBINAR

800-662-6090 239-649-1548

aspgsales@aspg.com | www.aspg.com