IDMS Database Encryption

MC IDMS. Designed to protect IDMS data.

Easily encrypt and protect sensitive IDMS data.

MEGA Cryption idms™

IDMS Specific Encryption

MegaCryption IDMS provides a comprehensive and cost-effective solution for the encryption of sensitive IDMS data. It encrypts data-at-rest using the most secure non-proprietary and well-known algorithms such as AES-128, AES-256 and TRIPLE-DES. Encryption is transparent to users and typically requires no changes to your applications.

MegaCryption IDMS encrypts critical data at both the record and element level. A simple and flexible conversion utility is provided to handle common cryptographic tasks such as: initial data encryption, key rotation, removal of encryption, and data display.

As part of the MegaCryption product family, MegaCryption IDMS incorporates several of the most popular and strongest algorithms commercially available. Key management options enable the separation of duties between Key Managers and IDMS Administrators.

MegaCryption IDMS also supports the encryption of IDMS Non-SQL data in one of two basic modes - Data Mode and Record Mode. As the name implies, Data Mode involves the encryption of individual data elements [fields or groups of fields] residing in an IDMS record - allowing precise cusomization of the data to be encrypted. Conversely, Record Mode operates at the IDMS record level, allowing all fields beyond the last control item in a record to be encrypted.

Supported Algorithms

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

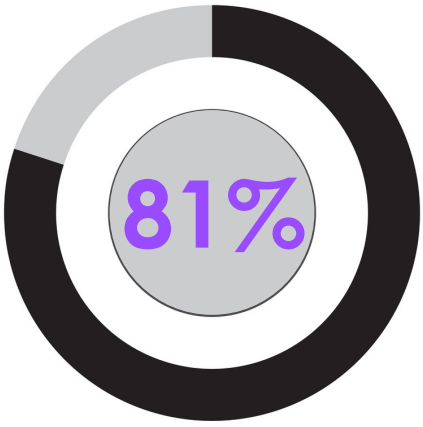
2 **AES 2** (Advanced Encryption Standard) is a Federal Information Processing Standard (FIPS) for use by US Government. MegaCryption makes use of 256 bit keys for AES (RIJNDAEL)

3 **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.

Compliancy

PCI, SOX, HIPAA, FERPA, GLB and more

Regardless of your industry, today's data centers are facing unprecedented pressure to comply with internal, state, federal, international 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 IDMS aids in compliancy with US government and International regulations such as SOX, PCI, HIPAA, FERPA, COPPA, HITECH, OMB M-06-16, Graham-Leach-Bliley, EU GDPR, UK DPA and more. MegaCryption IDMS provides mandate specific solutions to protecting data; Additionally, MegaCryption IDMS provides for AES-128 encryption and decryption operations using FIPS-197 validated cryptographic modules.

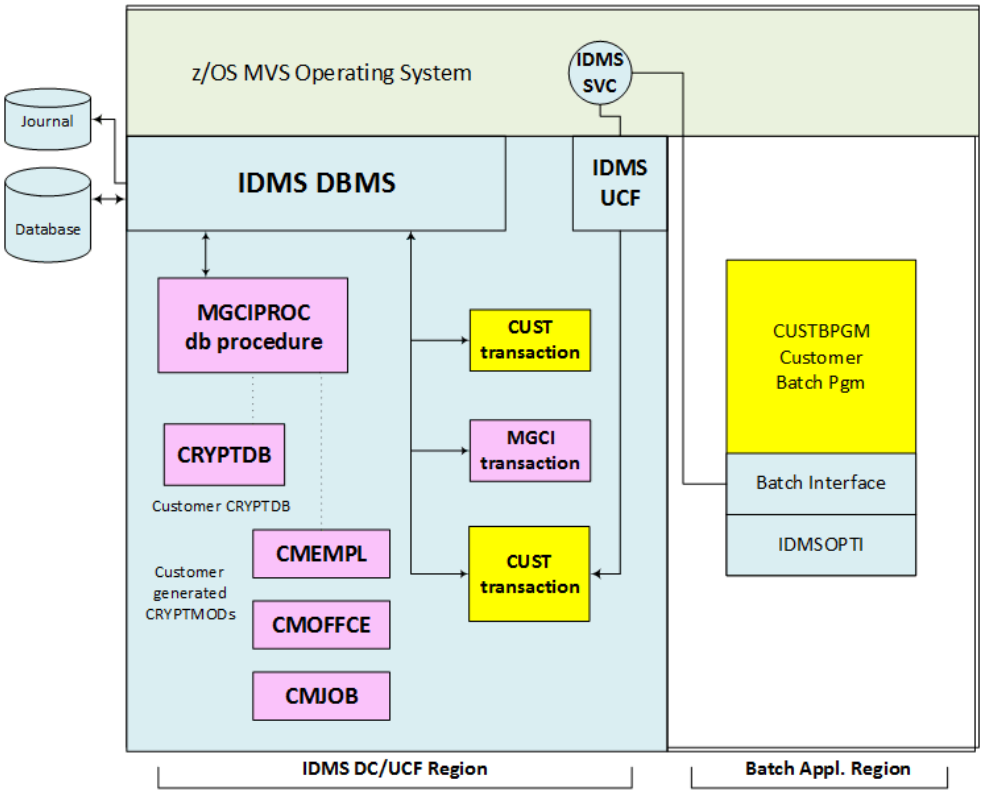


PCI compliancy is important. 81% of affected organizations subject to the Payment Card Industry Data Security Standard [PCI-DSS] had been found non-compliant prior to being breached.

Encrypting 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 confidential data they have stewardship responsibilities for. Although encrypting data in transit is important, encrypting data at rest in the data center is unquestionably just as, if not more, important. Although security management tools like RACF™, ACF2™ and Top Secret™ do a great job of controlling access to mainframe data, a recent national study showed that 70% of companies surveyed admitted to internal security breaches—making encryption of data at rest a necessity. Encrypting data at rest greatly reduces the likelihood of confidential information being disclosed to unauthorized individuals, especially for companies with a large mobile workforce. 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 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.

MegaCryption IDMS Architecture



MegaCryption z/OS

MegaCryption IDMS can be used as a stand-alone product, or in conjunction with MegaCrytion z/OS to provide a complete encryption solution protecting data across the entire enterprise.

Free 30-day Trial: www.aspg.com

800.662.6090 ● 239.649.1548 ● aspgsales@aspg.com

Fast Facts

- Encrypts sensitive IDMS data at rest, customizable at the field or record 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
- Run both field and record mode concurrently
- Multiple algorithms supported: AES, AES2, 3-DES
- Designed to be extremely flexible to accommodate a variety of requirements, encryption methods and existing security policies.
- Conversion utility provided to handle common cryptographic tasks
- Assist with internal and federal compliancy [HIPAA, SOX, PCI, FERPA, GLB, COPPA, GDPR, OMB M-06-16 and more]
- Fast and easy installation. Customers are ready to encrypt data immediately after installation
- MegaCryption PC/IX is provided at no cost as an enterprise companion for non-zSystem platforms
- All-in-one product, supported by one company, 24x7x365

MegaCryption IDMS

ADVANCED SOFTWARE PRODUCTS GROUP, INC.

www.aspg.com

800.662.6090 ● 239.649.1548
aspgsales@aspg.com