



Enterprise Cryptography Toolkit



Enterprise Cryptography

MegaCryption is a comprehensive cryptographic toolkit that not only encrypts data, but provides Data Integrity to assure that data has not been compromised, Data Authentication to verify the origin of the data, and Compression to provide the highest level of performance.

Whether your company chooses to secure their on-site data, data transmissions, entire files, or specific fields within the z/OS environment, MegaCryption can help. As a file-level cryptography tool, MegaCryption provides a comprehensive, cost-effective approach to encrypting virtually any file in your z/OS environment, while complementing any communication level encryption process you may already have in place. MegaCryption offers support of the most secure non-proprietary and well-known algorithms available today, ensuring security and compatibility with other standard implementations. Symmetric/asymmetric batch utilities or symmetric callable subroutines execute encryption conforming to either MegaCryption's documented format, the OpenPGP standard (RFC4880), or the OpenSSL standard. MegaCryption also comes with FREE companion products for non-z/OS systems, which can be freely distributed internally and externally for use on Windows, Unix or Linux systems; and are compatible with the OpenPGP standard. MegaCryption's user friendly ISPF panels and sample JCL libraries are ideal for all skill levels.

MegaCryption was designed to be extremely flexible in order to accommodate a variety of environments, experience levels, encryption methods, and security policies companies have implemented. Accordingly, MegaCryption fully exploits and compliments IBM's ICSF and CPACF cryptographic facilities by providing techniques that allow companies to achieve hardware-enhanced cryptographic processing, secure storage of cryptographic keys, and the ability to securely share confidential data with non-z/OS systems or business partners. Due to the non-proprietary format of MegaCryption encrypted files, compatibility with most PC or Unix encryption products is possible. MegaCryption can also be used in an environment that already uses hardware encryption by addressing the lack of interoperability and the lack of encryption outside of the hardware system.

```
----- MegaCryption Primary Option Menu -----
Option ==> |
Select one of the following actions:
                                                    DVLIP349
                                                    2007.065
                                                    14:35
                                                    ADCC
                                                    v6.1.2

K KEY MGMT - Key Management (list, create, import, export keys)
E ENCRYPT   - Encrypt Data (optionally sign it)
D DECRYPT   - Decrypt Data (optionally verify signature)
S SIGN     - Sign Data
H HASH     - Hash Data
Z ZIP      - Compress Data
I Algo info - List of algorithms
A About    - Product Info

V VERIFY   - Verify Signature
C CONVERT  - Converting data
U UNZIP    - Decompress data
M MONITOR  - Hardware Crypto Monitor
P PARAMETERS - Set ISPF Interface Parameters

Press END to exit, HELP to get help.
```

The MegaCryption ISPF Interface – Primary Option Menu

High-performance compression for single or multiple files is included. Multiple compression formats on z/OS including hardware compression, Gzip, ZIP64 & TAR formats are supported. The MegaCryption compression utility can also be used in stand-alone mode to create zipped files on the mainframe without using encryption services.

Encrypt only what you need to, such as specific fields or columns. Encryption routines can be written to maximize the amount of control and broaden performance. MegaCryption's API Interface [Application Programming Interface] provides the ability to call subroutines from application programs written in Assembler, PL/1, COBOL, & REXX. Implement cryptographic functions directly into applications, databases, exits, online transactions & batch programs. Both Callable API modules and processes that are already programmed are included in MegaCryption.

MegaCryption supports flat files, VSAM files and any type of database data without limitation. Additionally, MegaCryption supports cryptography in a DB2 database at the field/column level with three separate types of encryption: Transparent Encryption, Application Program Encryption, and End User Managed Encryption.

Compliance Mandates



Regardless of your industry, today's data centers are facing unprecedented pressure to comply with internal, state, federal, and industry compliance 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 aids in compliance with government regulations such as SOX, PCI, HIPAA, FERPA, Graham-Leach-Bliley and more. MegaCryption provides mandate specific solutions to protecting data; For example, encrypting data in process, providing security for data

as it is being created by your applications is just one way MegaCryption aids in PCI compliance. The Verizon Annual Data Breach Investigation report states, "PCI compliance 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 optionally provides for encryption and decryption operations using FIPS-140 and/or 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 reasonably 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.

Encryption: Data Transmissions

Transmitting data via FTP is a common and vital procedure in any data center. MegaCryption eliminates the exposure involved when downloading critical/sensitive mainframe data to another platform for FTP transmission. By encrypting data on the mainframe with MegaCryption, users can now securely FTP encrypted data directly from the z/OS platform. Since the data is stored in an encrypted format on the mainframe, the data remains secure before, during, and after the FTP transmission. Encrypting data to be transmitted via FTP completely eliminates reliance on a secure network path, and protects data even after it has landed at a destination that may or may not be secure.

Key Management

One of the most important aspects of cryptography is key management. MegaCryption offers a comprehensive, yet easy-to-use key management structure to allow a complete life cycle management of keys to take place.

MegaCryption provides comprehensive, secure key storage in ACF2, Top Secret, or IBM's RACF database, as well as using IBM's ICSF for adherence to the Common Cryptographic Architecture (CCA). All key storage methods supported by MegaCryption are backed by industry proven access control mechanisms that the mainframe is famous for. Keys are always stored separately from the encrypted data and can be up to 6,000 key bit size. In addition to supporting cryptographic keys in the z/OS environment, MegaCryption supports existing OpenPGP and OpenSSL cryptographic keys that may pre-exist on any platform.

This allows you to share your cryptographic keys from a PC or Unix server's PKI or PGP facility; for example, with MegaCryption on z/OS, applying leverage to your existing key infrastructure independent of platform. MegaCryption does not require import processing to use OpenPGP keys or X.509 certificates; allowing direct reading of binary or RADIX-64 (ASCII-armor) formats. Additionally, you have the ability to share MegaCryption-managed cryptographic keys with other facilities in your enterprise and with your business partners. MegaCryption key management features and functions, coupled with its support of OpenPGP and OpenSSL, allow you the flexibility to easily incorporate the product into any existing structure; independent of the platforms involved. Attributes of MegaCryption-managed cryptographic keys stored in RACF or keyfile data sets, may be easily displayed in detail from MegaCryption's ISPF interface. For sites just starting out, MegaCryption easily provides the basis for a secure key management scheme in your enterprise.

SUPPORTED ALGORITHMS

MegaCryption supports strong, well-known and preferred, non-proprietary algorithms and provides both asymmetric and symmetric cryptography in multiple modes. 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).

RSA is a widely-used public-key cryptosystem for encryption, authentication, and key exchange. MegaCryption utilizes key sizes up to 6000 bits.

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

DH-ELGAMAL is another popular public-key cryptographic system. MegaCryption enables interoperation with key sizes up to 6000 bits.

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.

DSS (Digital Signature Standard) algorithm is approved by the US National Institute of Standards and Technology (NIST) for applications requiring a digital signature.

SHA, SHA2, MD2, MD5, HMAC-SHA-1, HMAC-SHA-2, CRC AND ADL are used for data integrity.



MegaCryption is the #1 enterprise cryptography tool available. Encryption, Data Integrity, Data Authentication and Compression all in one tool, backed by 24x7x365 product support.



PRODUCT FEATURES

CRYPTOGRAPHY WHERE YOU NEED IT

- Encrypts data at rest, providing an additional layer of protection to SAF tools by encrypting any type of field/file level data directly on the mainframe
- Encrypts data in process, providing security for data as it is being created by your applications [a PCI requirement]
- Encrypts mainframe data for FTP and SSL, extending file confidentiality beyond a secure network.
- Encrypts tape and disk data
- Encrypts data at single or multiple field level
- Allows encryption and decryption for tape backups using DFSMSdss, CA-DISK, or FDR protecting data for transit offsite
- Application Programming Interface [API], providing the ability to call subroutines from application programs written in Assembler, PL/1, COBOL & REXX. Implement cryptographic functions directly into applications, databases, exits, online transactions & batch programs
- Self-Decrypting Archives (SDA) created by Mega Cryption on z/OS for delivery to Windows PC users
- Provides Courtesy software for your business partners so there is no expense to your partner in handling MegaCryption encrypted data (symmetric)

KEY MANAGEMENT

- Secure key storage: Comprehensive key management easily adapts to existing keys [ie ICSF, OpenSSL, OpenPGP, etc.]
- Secure key storage via mainframe security databases [RACF, ACF2, Top Secret & IBM's ICSF]
- Unique Key Update feature enables replacement of decryption keys for existing ciphertext, preventing the mass recovery of data when a cryptographic key is compromised

COMPREHENSIVE CUSTOMER SUPPORT

- All-in-one product, supported by one company, 24x7x365
- Fast & easy Installation in less than one hour. Customers are ready to encrypt data immediately after installation
- MegaCryption training is available on-site or online

PERFORMANCE & SECURITY

- Data authentication: digital signature verifies the origin of data
- Data Integrity identifies if data has been altered
- Online ISPF interface for automatic MegaCryption JCL generation and system status information. Also, includes sample executable JCL libraries
- Exploits IBM cryptographic hardware (ICSF & CPACF) for acceleration and added performance when available.
- Aides in compliancy with government regulations such as SOX, PCI, HIPAA, FERPA, Graham-Leach-Bliley and more
- Generates SMF records for tracking and auditing MegaCryption operations
- FREE utilities included for use with or without encryption are EBCDIC to ASCII translation, Compression/Decompression, Hashing & ASCII Armoring
- Single or multiple file high-performance compression. Supports multiple compression formats on z/OS including hardware compression, Gzip, ZIP64 & TAR formats
- Data-type Preserving Cryptography provides user control of ciphertext characters so encrypted data may conform to a specific data-type; such as numeric-only or text-only
- Text translation and conversion features utilize UNICODE services

INTEROPERATION FOR "OPEN" CRYPTOGRAPHY

- Cross-platform compatibility. OpenPGP (RFC4880) support. Compatible with PGP, OpenPGP, GnuPG, FileCrypt & CipherOps; in addition to any other product on any other platform that conforms to the OpenPGP standard
- Cross-platform compatibility. OpenSSL support. Use X.509 cert as public key; Generate PKCS-10 cert request from MegaCryption RSA or DSS key pair; Encrypt and decrypt PKCS-7 enveloped messages for exchange with an OpenSSL user
- MegaCryption/PC & MegaCryption/IX FREE enterprise companion products for your non-z/OS platforms; conforming to the OpenPGP standard (RFC4880). Includes graphical Windows interface, command-line interface, key generation, key import/export & Zip/Gzip compression

FREE TRIAL DOWNLOAD • FREE EDUCATIONAL WEBINAR



800-662-6090 239-649-1548
aspgsales@aspg.com | www.aspg.com

