MEGA Cryption™ | Enterprise Cryptography Toolkit

MegaProtection. MegaCompression. MegaAwesome.

SERVING THE IT COMMUNITY SINCE 1986 • 86

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

Enterprise Cryptography

MegaCryption™ is a comprehensive cryptographic toolkit that not only encrypts for data confidentiality, 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 entire files or specific fields, on-site data or data transmissions, 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.

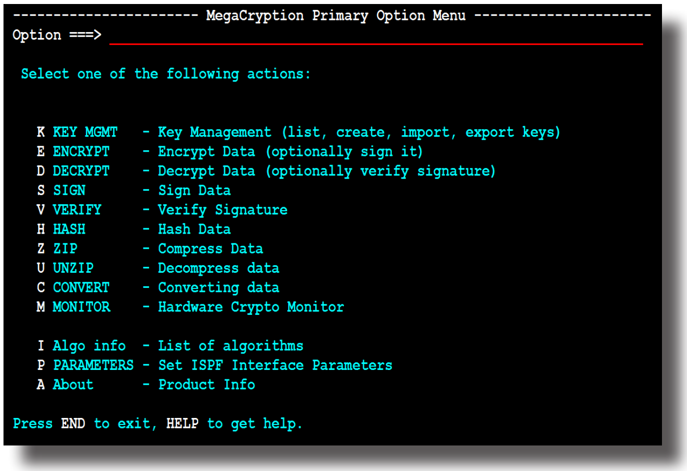
MegaCryption offers support for the most secure non-proprietary and well-known algorithms available today, ensuring security and compatibility with cryptography standards. Symmetric/asymmetric batch utilities or symmetric callable subroutines execute cryptography conforming to the OpenPGP standard (RFC4880), the OpenSSL standard, or for interoperation with other MegaCryption users. MegaCryption includes 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. 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 secure sharing of confidential data with 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 as a compliment to existing hardware system encryption.

High-performance compression for single or multiple-file archives is included. Multiple compression formats on z/OS including hardware compression, Gzip, Zip, and ZIP64 formats are supported. MegaCryption's compression can be used to create zipped files on the mainframe with or without encryption.

Users may choose to selectively encrypt specific fields/columns of data using a MegaCryption batch utility or their own custom application. MegaCryption includes a programming interface, providing the ability to call subroutines from application programs written in Assembler, PL/1, COBOL, & REXX. Users may optionally add cryptographic routines directly into their applications, databases, exits, online transactions & batch programs.

MegaCryption supports flat files, VSAM files, and any type of database data without limitation. Additionally, MegaCryption offers DB2™ cryptography. MegaCryption's symmetric encryption and decryption routines have been enhanced to run with DB2 Distributed Data Facility™.



```
---------------------- MegaCryption Primary Option Menu ---------------------
Option ===> ________________________________________________________________

 Select one of the following actions:


   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
   V VERIFY     - Verify Signature
   H HASH       - Hash Data
   Z ZIP        - Compress Data
   U UNZIP      - Decompress data
   C CONVERT    - Converting data
   M MONITOR    - Hardware Crypto Monitor

   I Algo info  - List of algorithms
   P PARAMETERS - Set ISPF Interface Parameters
   A About      - Product Info

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

The MegaCryption ISPF Interface – Primary Option Menu

SUPPORTED ALGORITHMS

MegaCryption supports strong, well-known, non-proprietary algorithms and provides both asymmetric and symmetric cryptography in multiple modes. MegaCryption uses **FIPS Validated Cryptography** certified by the 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 6080 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 6080 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.

ARC4 (also known as RC4) uses a 128-bit key and is used symmetrically with OpenSSL operations.

IDEA (International Data Encryption Algorithm) is a symmetric block cipher with a 128-bit key size.

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

SHA, SHA2, SHA5, MD2, MD5, HMAC-SHA-1,HMAC-SHA-2, CRC AND ADL are used for data integrity.

Data at Rest

Data lost or stolen outside the confines of the data center has made global headlines, forcing organizations to encrypt data that leaves their data center. While encrypting data in transit is important, encrypting data at rest 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. As data threats and technologies become more advanced, data at rest becomes much more than tape and back-up data: companies, especially those with mobile work forces, now have a multitude of laptops, USBs, and employee owned devices (BYOD) entering and leaving their data centers with critical data on a daily basis. Data can be left anywhere, so it must be protected everywhere. Encrypting data at rest greatly reduces the likelihood of confidential information being disclosed to unauthorized individuals, including internal threats. Internal breaches alone have made the encryption of data at rest a necessity. By combining encryption of data at rest and data in transit, organizations can be assured that data is secure before, during and after transmission.

Data Transmission

Transmitting data via FTP is a common and vital procedure in any data center. Data centers are also increasingly transmitting sensitive data into the cloud. MegaCryption eliminates the exposure involved when downloading critical/sensitive mainframe data to another platform for FTP transmission or transference into the cloud. By encrypting data on the mainframe with MegaCryption, users can securely FTP encrypted data directly from the z/OS platform into the cloud, to remote sites, business partners, disaster recovery centers, and more. 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, which greatly eases the sharing of critical data between your organization and outside vendors. The utilization of MegaCryption's cryptography also protects data even after it has landed in the cloud or another destination that may or may not be secure.

Key Management

One of the most important aspects of cryptography is key management; without proper management of encryption and decryption keys, the security of encryption is diminished. MegaCryption offers a comprehensive yet easy-to-use key management structure to allow for a complete life cycle management of keys.

Adhering to IBM's Common Cryptographic Architecture™ (CCA), MegaCryption provides secure key storage in ICSF or in ACF2, Top Secret, RACF, or data sets. Users of MegaCryption are provided the option of controlling the creation and access of keys by user or group administration. MegaCryption optionally detects and implements encryption operations using ICSF for key management and encryption/decryption processing by utilizing IBM's Cryptographic Coprocessor for FIPS-140-2 conforming security and fast processing. Through its utilization of existing RACF resources, MegaCryption provides additional security while preventing a key administrator from learning a new security product. For administrators of keys who may not be familiar with RACF, MegaCryption's optional ISPF Wizard supplies them with progressive steps for key management operations. All key storage methods supported by MegaCryption are backed by industry proven access control mechanisms that the mainframe is famous for.

In addition to supporting cryptographic keys within the z/OS environment, MegaCryption supports OpenPGP and OpenSSL cryptographic keys that may pre-exist on any platform, including keys from other vendors and keys currently in ICSF. 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. Due to the support of open cryptographic standards, MegaCryption specializes in key portability across the enterprise. This allows MegaCryption users to share cryptographic keys from a PC or Unix server's PKI or PGP™ facility, applying leverage to your existing key infrastructure.

MegaCryption's key management features and functions, coupled with its support of OpenPGP and OpenSSL, allow you the flexibility to securely and easily incorporate the product into any existing structure, independent of the platforms involved. MegaCryption also provides optional alerts for the pending expiration of cryptographic keys, optionally authorizes the use of an expired key in an emergency, implements user-friendly JCL and/or ISPF program for the listing of keys, and simplifies the key rotation process, enabling easy adherence to security mandates. For seasoned sites and sites just starting out, MegaCryption provides a secure, user-friendly key management scheme across your enterprise.

Compliancy

Regardless of industry, today's data centers are facing unprecedented pressure to comply with internal, state, and federal compliancy mandates. There are very few organizations which are not required to protect customer (PII) and/or operational data, yet everyday there are numerous organizations in the news for non-compliance and a lack of data protection. Cryptography is vital to the protection of sensitive data, which in turn is vital to the protection of your organization's credibility and finances. Through its use of non-proprietary, FIPS-140 and FIPS-197 validated cryptographic algorithms, MegaCryption provides data protection to ensure internal, state, and industry specific mandates are met. MegaCryption also aids in compliancy with government regulations such as SOX, PCI, HIPAA, FERPA, FISMA, GLBA, and more.

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, Gramm-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

ASPG
ADVANCED SOFTWARE PRODUCTS GROUP, INC.

FREE TRIAL DOWNLOAD • FREE EDUCATIONAL WEBINAR

800-662-6090   239-649-1548

aspgsales@aspg.com | www.aspg.com

*All trademarks are the property of their respective companies and not the property of Advanced Software Products Group, Inc. [ASPG, Inc.]

MEGA Cryption