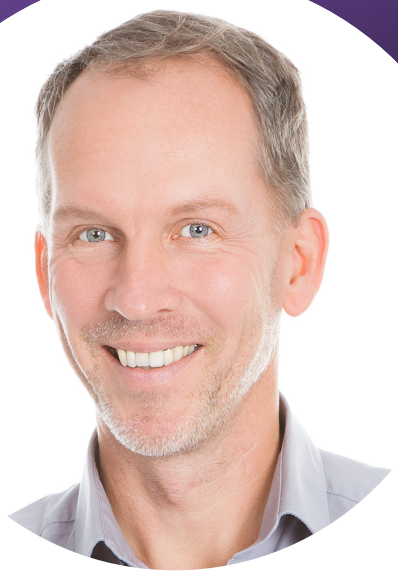
MEGACRYPTION

z / o s



THE #1 ENTERPRISE CRYPTOGRAPHY TOOL AVAILABLE

Mainframe Cryptography. Smarter Key Management. Superior Compression.

CRYPTOGRAPHY TOOLKIT FOR IBM Z / OS

SECURE PROTECTION DESIGNED FOR IBM Z

MegaCryption remains one of the industry's most trusted and versatile cross-platform cryptographic toolkits, delivering robust protection with enterprise-grade agility. By seamlessly integrating encryption, compression, text translation, data authenticity and key management into a single comprehensive suite, MegaCryption empowers organizations to secure data throughout its entire lifecycle without sacrificing performance or compatibility.

Whether securing data at rest, encrypting files for transmission, or protecting data in motion and in-process, MegaCryption delivers targeted cryptography exactly where it's needed, all within the convenience of a single tool.

For organizations that store or exchange sensitive information on a regular basis, MegaCryption offers comprehensive compliance with global standards including HIPAA, GDPR, PCI, and SOX, providing end-to-end data privacy and reducing the risk of exposure.

BUILT FOR YOUR ENVIRONMENT

Even in environments that already utilize encryption, vulnerabilities can still persist. MegaCryption addresses these gaps by supplementing existing cryptographic infrastructure with robust, interoperable tools that secures data from its origin to final destination. MegaCryption's open architecture ensures seamless communication with partners and systems that may rely on different encryption technologies, making it an ideal solution for enterprises with diverse ecosystems.

Designed to function across platforms, MegaCryption offers exceptional interoperability, working with OpenPGP, OpenSSL, S/MIME, CMS, PKCS, and built-in conversion of text from EBCDIC to ASCII.

MegaCryption is also fully compatible with ICSF and CPACF. Thanks to zEnterprise Data Compression (zEDC) MegaCryption significantly reduces file sizes, saving time and conserving resources.

MegaCryption is built to complement and extend IBM's pervasive encryption, allowing organizations to achieve true end-to-end encryption by offering batch and online interfaces across all points of data handling while enhancing operational flexibility and resolving compliance mandates.

Designed for ease of use, MegaCryption features intuitive ISPF panels and comprehensive JCL libraries that eliminates learning curves, making strong cryptography simple and accessible to teams of all skill levels.

"MegaCryption gave us the flexibility we needed to unify encryption across our entire infrastructure—z/OS to cloud."
– CTO, Global Tech Firm

"We needed a solution that met global compliance without slowing us down. MegaCryption delivered on every front."
– VP of Infrastructure, International Bank

"MegaCryption provided the cryptographic control and transparency our agency required—plus the support to back it up."
– Federal Systems Architect

MEGACRYPTION HIGHLIGHTS:

- **Secure file-level data encryption, compression, translation, and integrity checking**
- **Improve compression support up to 95%**
- **Cross-platform compatibility with WIN, Linux, UNIX, and more**
- **Complies with all worldwide data regulations**
- **Seamlessly works alongside existing encryption tools**
- **Protects critical data from origin all the way to destination**

ALSO AVAILABLE:

MEGACRYPTION FOR WINDOWS, DB2, IDMS, UNIX & LINUX

SUPPORTED ALGORITHMS:

AES, RSA, CAST-5, DH- ELGAMAL, DES, TRIPLE DES, BLOWFISH, ARC4, IDEA, DSS/DSA, SHA, SHA2, SHA5, MD2, MD5, HMAC-SHA-1, HMAC-SHA-2, CRC AND ADL

Z/OS COMPATIBILITY:

WORKS ALONGSIDE ALL RECENT RELEASES OF Z/OS

FREE 30 DAY TRIAL:
WWW.ASPG.COM

KEY FEATURES AND BENEFITS:

COMPREHENSIVE TOOLKIT	Encryption, Data Integrity, Key Management, Data Authentication and Compression all in one convenient tool.
EXTEND CONFIDENTIALITY	Encrypts mainframe data for FTP and SSL.
REGULATION COMPLIANCE	Complies with all worldwide and industry regulations including GDPR, SOX, HIPPA, EFTA, COPPA, PCI, etc.
NO LEARNING CURVE	User-friendly ISPF panels and sample JCL libraries for all skill levels.
COMPLETE PROTECTION	Secure on-site data, cloud-stored data, data transmissions, entire files, or specific fields within the z/OS environment.
KEY MANAGEMENT	Comprehensive key management easily adapts into existing keys including ICSF, OpenSSL, OpenPGP, etc.
SECURE KEY STORAGE	Via common mainframe security databases including RACF, ACF2, TopSecret and ICSF.
PARTNER SUPPORT	Courtesy software for business partners handling encrypted data.
INTEROPERATION	Compatible with PGP, OpenPGP, GnuPG, and any other OpenPGP conforming products.
HIGH PERFORMANCE COMPRESSION	zEnterprise Data Compression (zEDC) optimizes compression and boosts storage.
IMS CRYPTOGRAPHY	Protect databases containing classified or sensitive data.
AFFORDABLE AND EFFECTIVE	Protect your valuable data from security threats.
ASPG SUPPORT	World-class technical support available 24x7x365.

NEW CAPABILITIES ADDED:

EXPANDED ASYMMETRIC CRYPTOGRAPHY	Includes support for 7 new asymmetric algorithms and 7 elliptic curves such as X25519, Ed25519, X448, Ed448, as well as NIST and Brainpool curves.
ENHANCED AEAD SUPPORT	Adds support for OCB and GCM authenticated encryption algorithms with AES-192 hardware acceleration.
ADVANCED HASHING AND KEY DERIVATION	Now supports 6 new SHA2 and SHA3 variants and secure password-based encryption with Argon2 and Iterated + Salted derivations.
MODERN OPENPGP COMPLIANCE	Full support for the updated OpenPGP RFC9580 standard, while maintaining backward compatibility with RFC4880 and RFC2440.
DYNAMIC ENCRYPTION DEFAULTS	The new Default Algorithms and Algorithm Preferences framework lets teams enforce consistent cryptographic policies across systems. The MGCOPTNS utility simplifies per-site default configuration.
RECIPIENT ALGORITHM PREFERENCES	Dynamically selects the recipient's preferred algorithm from their certificate during encryption/signing, for optimal interoperability.
IMPROVED KEY STORAGE	ICSF PKDS records now support embedded certificate metadata. RACF/ACF2/TSS keys benefit from stronger AES-256 protection.
PUBLIC KEY VERSIONING	Public Key Versioning: Customize OpenPGP public key format versions with the new PGPKVER option when generating asymmetric keys.

FEATURED HIGHLIGHTS:

- Secure file-level data encryption, compression, translation, and integrity checking
- Interoperation with OpenPGP, OpenSSL, GnuPG, S/MIME, PKI, CMS, ZIP and ZLIB
- Compression improvements up to 95% with zEDC support
- Integrated data redaction and field-level encryption
- Seamless support for ICSF, CPACF, and hardware cryptography acceleration
- Dynamic key management and new default policies reduce human error
- Supports all global data compliance standards: HIPAA, GDPR, PCI, SOX, and more
- Compatible with all z/OS releases and major platforms including Windows, Unix and Linux.

THE WORLD'S LARGEST ORGANIZATIONS TRUST MEGACRYPTION TO PROTECT THEIR SENSITIVE DATA.
SHOULDN'T YOU?

ASPG
ADVANCED SOFTWARE PRODUCTS GROUP, INC.
www.aspg.com

PROUDLY SERVING THE GLOBAL IT COMMUNITY SINCE 1986

IBM Business Partner · Microsoft CERTIFIED Partner · McAfee SecurityAlliance

800.662.6090 • 239.649.1548 • aspgsales@aspg.com