

VM/Encrypt-Tape™ for IBM z/VM

Summary: Protecting sensitive data from unauthorized access is now a major requirement in z/VM® data centers. VM/Encrypt-Tape™ protects such data by encrypting it, using strong, secure and robust data encryption algorithms, as it is written to and read from tape. Depending on the security requirements, different encryption algorithms can be employed, allowing each site to select the level of data protection required. VM/Encrypt-Tape™ provides for both hardware and software encryption, so data backed up on one processor type can be restored on another.

Technical Specifications: VM/Encrypt-Tape™ transparently works with any CMS tape handling application that uses the native CMS *tapeio* macro for tape input and output. Encryption parameters are specified on the VM/Encrypt-Tape™ CMS command, allowing the encryption algorithm and parameters to be easily changed to meet different data protection needs.

VM/Encrypt-Tape™ encrypts data written to tape using the following algorithms:

1. DES (Data Encryption Standard), a block cipher, employing a data block size of 8 bytes and a key length of 8 bytes (64 bits). Both [Electronic codebook \(ECB\)](#) and [Cipher-block chaining \(CBC\)](#) modes of encryptions are supported. For CBC mode, an initial chaining value of 8 bytes can be specified.
2. 3DES, employing a data block size of 8 bytes and a key length of either 16 bytes (128 bits) or 24 bytes (192 bits). Both [Electronic codebook \(ECB\)](#) and [Cipher-block chaining \(CBC\)](#) modes of encryption are supported; for CBC mode, an initial chaining value of 8 bytes can be specified.
3. AES (Advanced Encryption Standard), a block cipher, employing a data block size of 16 bytes and a key length of either 16 bytes (128 bits), 24 bytes (192 bits), or 32 bytes (256 bits). Both [Electronic codebook \(ECB\)](#) and [Cipher-block chaining \(CBC\)](#) modes of encryption are supported. For CBC mode, an initial chaining value of 16 bytes can be specified.
4. BlowFish, a block cipher, employing a data block size of 8 bytes and a key length of either 16 bytes (128 bits) or 32 bytes (256 bits). Both [Electronic codebook \(ECB\)](#) and [Cipher-block chaining \(CBC\)](#) modes of encryption are supported. For CBC mode, an initial chaining value of 8 bytes can be specified.
5. ARC4, a stream cipher, with a data block size of 1 byte (8 bits) and an arbitrary key length of up to 64 bytes (512 bits).

VM/Encrypt-Tape™ will detect at run time if the appropriate encryption hardware support is available, and exploit the hardware support automatically. This can be overridden by a user parameter forcing VM/Encrypt-Tape™ to use the software encryption algorithms instead.

For the block ciphers VM/Encrypt-Tape™ supports, data record padding to an integral of the encryption algorithm's block size is handled automatically. Padding bytes are automatically removed when the data from tape read back in and decrypted. The maximum record length VM/Encrypt-Tape™ block ciphers can process is 64K-2 bytes. For the ARC4 stream cipher, the data block size is one byte, and therefore no data record padding is required. It can be used to encrypt data records that are as large as the maximum record size CMS allows.

A set of Rexx-callable encryption routines, implementing the encryption algorithms listed above, is also provided with VM/Encrypt-Tape™. These routines allow the end user to employ advanced encryption data protection methods in situations where VM/Encrypt-Tape™ would not be directly applicable. The CMS PIPELINE environment is supported as well.

If the hardware supports the CP Assist for Cryptographic Function (CPACF, feature code 3863) option, VM/Encrypt-Tape™ can exploit the cryptographic hardware instructions to perform the actual data encryption and decryption for the following algorithms, with significant performance improvements:

1. DES
2. 3DES
3. AES



VM/Encrypt-Tape™ has not been FIPS 140-2 certified; however it is FIPS 140-2 conformant.

Requirements:

Software: VM/Encrypt-Tape™ requires:

IBM z/VM Version 6.1 (5741-A07) and later releases
IBM z/VM Version 5.1 (5741-A05) and later releases
IBM z/VM Version 4.1 (5739-A03) and later releases

Hardware: VM/Encrypt-Tape™ will operate on the following IBM platforms:

zEnterprise 196
System z10 (BC and EC models)
System z9 (BC and EC models)
IBM  zSeries 990 and 890 IBM  zSeries 900 and 800

Developed by:



Sold and Marketed by:

