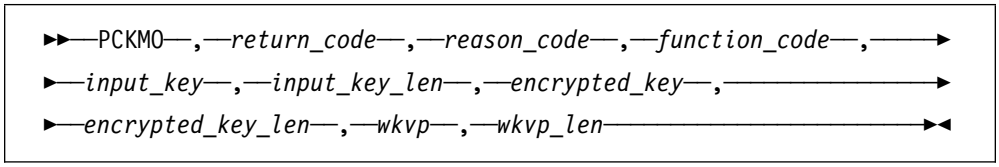
PCKMO - Perform Cryptographic Key Management Operation

Purpose

Encrypt DES, TDES or AES keys using the PCKMO ('B928') hardware instruction, with either the 192-bit DES wrapping-key register or the 256-bit AES wrapping-key register. The corresponding wrapping key verification pattern value is also returned.

Format



Parameters

PCKMO
(input, CHAR, 8) can be passed as a literal or in a variable.

return_code
(output, INT, 4) is a variable for the return code from PCKMO.

reason_code
(output, INT, 4) is a variable for the reason code from PCKMO.

function_code
(input, INT, 4) specifies which PCKMO key management function to preform. A list of valid codes is given in the Usage Notes.

input_key
(input, CHAR, *input_key_len*) is the key to be encrypted.

input_key_len
(input, INT, 4) is a variable containing the length of the preceding character parameter, *input_key*

encrypted_key
(output, CHAR, *encrypted_key_len*) contains the encrypted key value.

encrypted_key_len
(input, INT, 4) is a variable containing the length of the preceding character parameter, *encrypted_key*

wkvp
(input, CHAR, *wkvp_len*) the 24 or 32 byte wrapping key verification pattern.

wkvp_len
(input, INT, 4) is a variable containing the length of the wrapping key verification pattern It must be either 24 or 32

Usage

1. Valid function codes are:

Code	Function	Description
1	Encrypt_DEA_Key	Encrypt the 8 byte key using the hardware DES 24 byte wrapping key register, and return the wrapping key verification pattern value.
2	Encrypt_TDEA_128_Key	Encrypt the 16 byte key using the hardware DES 24 byte wrapping key register, and return the wrapping key verification pattern value.
3	Encrypt_TDEA_192_Key	Encrypt the 24 byte key using the hardware DES 24 byte wrapping key register, and return the wrapping key verification pattern value.
18	Encrypt_AES_128_Key	Encrypt the 16 byte key using the hardware AES 32 byte wrapping key register, and return the wrapping key verification pattern value.
19	Encrypt_AES_192_Key	Encrypt the 24 byte key using the hardware AES 32 byte wrapping key register, and return the wrapping key verification pattern value.
20	Encrypt_AES_256_Key	Encrypt the 32 byte key using the hardware AES 32 byte wrapping key register, and return the wrapping key verification pattern value.

All other function code values are unassigned.

2. Definitions of these functions for Rexx are in PCKMOREX COPY and for PL/I are in PCKMOPLI COPY.
3. This routine is only supported in the z/Architecture CMS[1] (ZCMS) environment.
4. Since both the wrapping key and wrapping key verification pattern registers are changed each time CMS, or zCMS, is IPL-ed, or the CP SYSTEM RESET command is issued in the virtual machine, using encrypted keys in this environment is problematic. Support for *wkvp* is included only for completeness.

Retrun codes and reason codes

Return codes:

Severity	Code	Meaning
OK	0	The operation was successful.
WARNING	4	The operation was successful, but a warning condition was encountered.
ERROR	8	The operation was unsuccessful.
SEVERE	12	The operation was unsuccessful, and the operation can no longer continue.

Reason codes:

Severity	Code	Description
ERROR	8	bad key length, key not 8, 16, 24, or 32 bytes long
ERROR	10	unknown function code specified
ERROR	15	bad wrapping key verification pattern length; this value must be either 24 or 32

[1] This environment is created via the IPL ZCMS command.