IBM SecureWay Cryptographic Products
IBM 4758 PCI Cryptographic Coprocessor

Version 1 to Version 2, Major Differences

This paper describes major differences between the CCA Support Program Version 1 and Version 2 for the IBM 4758 PCI Cryptographic Coprocessor, Model 002 and Model 023.

Chapter 1. Version 1 to Version 2 Differences

This brief paper describes the major differences between the Version 1 and Version 2 CCA Support Program features.

Users of the IBM 4758, Model 1 or Model 13 should refer to the *IBM 4758 CCA Basic Services Reference and Guide, Version 1.31 for the IBM 4758-001*.

The CCA Support Program feature, Version 2, Release 1.0, includes functional enhancements and changes for verbs as listed in Figure 1-1 on page 1-2. There are also these changes in the CCA implementation that affect major portions of the support program:

1. The internal DES key token structure created by this release is changed to a version X'00' data structure. This release will accept both version X'00' and version X'03' key token data structures. However, this release will only output version X'00' key token data structures. The version X'00' token structure employs an 8-byte master key verification pattern (MKVP) whereas Version 1 supports a two-byte verification pattern.
2. New RSA key-token data structures are introduced for the private key sections. In the new private key-token sections, the private key information is encrypted by an *object protection key* (OPK). The object protection key is encrypted by the master key for asymmetric operations. The release will accept private keys contained within sections having section identifiers of X'02', X'05', and the new structures X'06', and X'08'. Internal key tokens are only created with the new section types. External modulus-exponent tokens employ section identifier X'02' for private keys. External CRT private keys are held in the new section identifier X'06'.

   The PKA_Key_Import verb is extended to process existing RSA private keys generated with IBM 4755 or IBM 4758 Model 1 or Model 13 products as well as keys generated in the newer formats used with the IBM 4758 Model 2 or Model 23. The verbs that use an RSA private key will operate with any of the RSA private key formats.

   The **RSA-OPT** keyword is not accepted in Version 2 implementations of PKA_Key_Token_Build since this keyword was previously used to create a section X'05' RSA key token.
3. An additional set of master keys (new, current, and old) are introduced to protect RSA private keys. Using new keywords, **ASYM-MK** and **SYM-MK**, you can operate on the master key for asymmetric key or symmetric key protection, respectively, in the Cryptographic_Facility_Query, Master_Key_Distribution, Master_Key_Process, and Key_Test verbs. If neither keyword is mentioned, then:
   - When introducing a master key value, the value is entered for both types of master keys.
   - When requesting information about a master key, information is only returned when the two types of master keys have the same value.
4. This release computes master key verification pattern information in several ways.

The key storage manager is extended to recognize the various key token types and associated master key verification patterns, and also accepts records that contain key tokens flagged as not containing a key value.

5. Additional DES key-type classes are included as well as double-length versions for certain key types. Additional keywords to designate these new types of keys are included. The Key_Token_Build verb is extended to support the additional control vectors. The Control_Vector_Generate verb is added. The Key_Token_Parse verb is added to enable you to disassemble DES key tokens.
6. Double-length variations of DES data keys are added. The Key_Generate verb can generate the added CIPHER-class keys, and now also double-length variations of DATA, CIPHER, and MAC/MACVER class keys. The Key_Export and Key_Import verbs will export and import these key types. You use the **TOKEN** keyword with the key-type variable to indicate the key type and other characteristics as specified by the control vector in the key token.
7. The Encipher and Decipher verbs are extended to support triple encryption of general data encryption based on a double-length DES key.
8. The PKA_Symmetric_Key_Generate, PKA_Symmetric_Key_Export, and PKA_Symmetric_Key_Import verbs are extended to support exchange of data keys, both single and double length, using RSA public key methods. Additional methods for formatting key information are added. Also, the PKA_Key_Encrypt and PKA_Key_Decrypt verbs are added to encrypt and decrypt clear-key information.
9. The Key_Token_Build and the Control_Vector_Generate verbs produce a different control vector for the keyword **CPINGEN** as compared to the Transaction Security System (TSS) implementation. Other changes from the TSS implementation exist because the control vectors and key tokens supported with the IBM 4758 CCA Support Program vary from those supported with TSS.
10. The value established using the **SET-MOFN** keyword in the Cryptographic_Facility_Control verb is no longer cleared when the master key is set using the Master_Key_Process verb.
11. The SET_Block_Decompose verb is extended to process an encrypted PIN-block in support of debit card transactions.

Figure 1-1 lists new and modified verbs.

Figure 1-1. New and Modified Verbs for Version 2, Release 1.0

Verb	Service Modification
Cryptographic_Facility_Query Master_Key_Distribution Master_Key_Process	Modified to accommodate a master key for the encryption of private keys in the asymmetric cryptography support.
PKA_Key_Token_Build PKA_Key_Generate PKA_Key_Import	Modifications and extensions to support the new RSA key tokens.
PKA_Key_Decrypt PKA_Key_Encrypt	Use RSA keys to decrypt and encrypt a symmetric key formatted in an RSA DSI PKDS #1 block type 2 structure. The unencrypted keys are in the clear.
Diversified_Key_Generate	Removal of the key-export restriction on the generated, diversified key.
Control_Vector_Generate Key_Token_Build Key_Token_Parse	Addition of the Control_Vector_Generate and Key_Token_Parse verbs and expanded support for additional key types and key usage options.
Multiple_Clear_Key_Import	Imports DES keys to form a single-length or double-length DES DATA key.
Prohibit_Export	Modifies the control vector and encryption on an operational DES key to prevent subsequent export of the associated key.
Key_Export Key_Generate Key_Import	Additional key-type keywords and key generation rules. Keys having an internal key token with the default DATA control vector for either single or double length will cause a single or double DES key to be exported or imported.
PKA_Symmetric_Key_Export PKA_Symmetric_Key_Generate PKA_Symmetric_Key_Import	Support of both single-length and double-length DATA key, MAC-class key, and CIPHER-class key distribution. Also additional formatting methods.
SET_Block_Decompose	The SET_Block_Decompose verb is extended to process an encrypted PIN-block in support of debit card transactions.

END OF DOCUMENT